# Albanian Journal of Mathematics

*Për një Shqipëri të shkencës dhe kulturës.*



**Volume 2, 2008**

www.albanian-j-math.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 3–6
ISSN 1930-1235: (electronic version)

# ON A QUESTION OF KAPLANSKY II

P.G. WALSH

(Communicated by F. Luca)

*This paper is dedicated to the memory of*
*Professor Irving Kaplansky*

Abstract. There is a question attributed to Irving Kaplansky concerning the solvability of the quadratic equation $x^2 - py^2 = a$ in the case that the prime $p = a^2 + (2b)^2$. This question was answered in the affirmative by Mollin [1], although according to [3], this result is implicit in the work of Gauss and Legendre. The proof appearing in [1] was later simplified in [4], and it was also shown therein that Kaplansky's question was a special case of a more general result. Using the method of proof in [4], Mollin [2] has recently extended the results of [4], but upon further consideration, it appears that there is a more general phenomenon occurring, and also, that one of the assumptions in the main theorem of [2] is unnecessary. In this paper we prove this generalization, and eliminate one of the assumptions stated in the main result of [2]. The proof is again based on the method described in [4].

## 1. Introduction

In an earlier article [4], the author generalized a result of Mollin, and at the same time, simplified the method of proof. Recently, Mollin has used this same elementary approach to further the results of [4]. The purpose of this present paper is to extend the results of [2]. The method remains the same as in [4], with the appropriate modifications described in [2] in order to deal with parity issues.

**Theorem 1.1.** *Let $d \equiv 1 \pmod 4$ be a positive integer, and assume that $n = a^2 + db^2$ for positive integers $a, b$ with $a$ odd and $(n, a) = 1$. Assume further that there is a positive integer $c$, with $(a, c) = 1$ for which the equation*

$$X^2 n - Y^2 d = c^2$$

*is solvable in coprime positive integers $X, Y$. Then there exists a (possibly trivial) factorization $rs$ of $nd$, and a divisor $f$ of $\sigma c$, for which the equation*

$$rx^2 - sy^2 = af$$

*is solvable in positive integers $x, y$, where $\sigma = 2$ if $n$ is odd and $c$ is even, and $\sigma = 1$ otherwise.*

Received by the editors August 16, 2007 and in revised form, September 11, 2007.
2000 *Mathematics Subject Classification.* Primary: 11D09, 11D85.
*Key words and phrases.* Pell equation.

For simplicity, Theorem 1 only deals with the case $d \equiv 1 \pmod 4$. A similar statement holds for the other cases, which we leave as an exercise for the reader.

We note that Theorem 1 not only extends the result of [2], which dealt with the particular case $d = 1$, but moreover removes an unnecessary assumption contained in the statement of the main theorem in [2]. Specifically, it is assumed therein that the quadratic equation $X^2 - nY^2 = -1$ is solvable. As the conclusion of the main theorem in [2] does not place any restriction on the constructed factors $r$ and $s$ of $n$, there is no need, during the course of the proof, to multiply by a unit of norm $-1$. Therefore, we do not need to include an analogous assumption (that the quadratic equation $x^2n - y^2d = 1$ be solvable in positive integers $x, y$) in the statement of Theorem 1 above.

## 2. Proof of Theorem 1

Let $(T, U)$ be coprime positive integers which satisfy $T^2n - U^2d = c^2$, and let $\alpha$ be defined $\alpha = T\sqrt{n} + U\sqrt{d}$. Let $\beta = \sqrt{n} + b\sqrt{d}$, and define integers $u$, by $u = Tn + Ubd, v = Tb + U$. Then

$$\alpha\beta = (Tn + Ubd) + (Tb + U)\sqrt{nd} = u + v\sqrt{nd}$$

is an element in $\mathbf{Z}[\sqrt{nd}]$ with norm $a^2c^2$.

Let $g = (u, v)$, then clearly $g$ divides $c^2$, but in fact, $g$ divides $c$. We provide the details for this assertion, as the reasoning in [2] appears to be flawed. Suppose that $p$ is a prime dividing $g$, with $p^\mu$ properly dividing $g$ ($\mu > 0$), and such that $p^\mu$ does not divide $c$. Note that $p$ divides $c$ because $p^\mu$ divides $c^2$. It follows that $p^\mu$ divides both $u$ and $v$, hence $p^{2\mu}$ divides $u^2 - v^2nd = a^2c^2$. By assumption, $p^{2\mu}$ does not divide $c^2$, and so $p$ must divide $a$, contradicting the fact that $(a, c) = 1$. We conclude that $g$ divides $c$, and from the equation $u^2 - v^2nd = a^2c^2$, we deduce that

$$(u/g)^2 - a^2(c/g)^2 = ((u/g) + a(c/g))((u/g) - a(c/g)) = (v/g)^2nd. \tag{1}$$

We now break up the argument into three cases, depending on the relative parities of $n$ and $c$. We note that $n$ and $c$ cannot both be even, as this would contradict either $(n, a) = 1$ or $(T, U) = 1$.

**Case 1:** $c$ even, $n$ odd.

In this case, as $n, a$ and $d$ are odd, and $n = a^2 + db^2$, it follows that $b$ is even. Also, the assumption that $c$ is even implies that $T$ and $U$ are odd (as they are coprime), whence it follows that both $u$ and $v$ are odd, which by equation (1) implies that there are integers $A, B, r, s$, with $v/g = AB$ and $nd = rs$, satisfying

$$(u/g) + a(c/g) = A^2r,\ (u/g) - a(c/g) = B^2s,$$

from which it follows that

$$A^2r - B^2s = af,$$

with $f = 2(c/g)$.

**Case 2:** $c$ odd, $n$ even.

In this case, since $d \equiv 1 \pmod 4$ and $(a, b) = 1$, it follows that $n \equiv 2 \pmod 4$, and that $b$ is odd. By considering the equation $T^2n - U^2d = c^2$ modulo 4, it is readily verified that both $T$ and $U$ are odd. We conclude that $u = Tn + Ubd$ is odd, and that $v = Tb + U$ is even. Therefore, there are integers $A, B, r, s$, with $nd = rs$ and $v/g = 2AB$, satisfying

$$(u/g) + a(c/g) = 2A^2r, \ (u/g) - a(c/g) = 2B^2s,$$

from which it follows that

$$A^2r - B^2s = af,$$

with $f = c/g$.

**Case 3:** $c$ odd and $n$ odd.

Since $d \equiv 1 \pmod 4$, it follows that $n \equiv 1 \pmod 4$, and again by considering the equation $T^2n - U^2d = c^2$ modulo 4 we deduce that $T$ is odd and that $U$ is even. Therefore, in this case we find again that $u = Tn+Ubd$ is odd and that $v = Tb+U$ is even, and the rest of the proof for this case follows as in the previous case.

**Acknowledgement** The author gratefully acknowledges support for his research from the Natural Sciences and Engineering Research Council of Canada

## References

[1] R.A. Mollin. *Proof of some conjectures by Kaplansky,* C.R. Math. Rep. Acad. Sci. Canada **23** (2001), 60-64.
[2] R.A. Mollin. *On a generalized Kaplansky conjecture,* Int. J. Contemp. Math. Sciences **2** (2007), 411-416.
[3] N. Tzanakis [M.R. 1913340 (2003g:11027)], Reviews of the A.M.S., 2003.
[4] P.G. Walsh, *On a conjecture of Kaplansky,* Amer. Math. Monthly **109** (2002), 60-61.

Department of Mathematics, University of Ottawa, 585 King Edward St., Ottawa, Ontario, Canada, K1N-6N5
*E-mail address*: gwalsh@mathstat.uottawa.ca

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 7–13
ISSN 1930-1235: (electronic version)

# ON THE INSTABILITY OF SOLUTIONS TO A CERTAIN CLASS OF NON-AUTONOMOUS AND NON-LINEAR ORDINARY VECTOR DIFFERENTIAL EQUATIONS OF SIXTH ORDER

CEMIL TUNÇ

Abstract. The aim of the present paper is to establish a new result, which guarantees the instability of zero solution to a certain class of non-autonomous ordinary differential equations of sixth order. Our result improves some known results in the literature for non- autonomous case (see, [20,Theorem 4], [31, Theorem 1]).

## 1. Introduction

Consider the non-autonomous and non-linear vector differential equation of sixth order:

$$X^{(6)}+AX^{(5)}+BX^{(4)}+C\dddot{X}+\Phi(t,X,\dot{X},\ddot{X},\dddot{X},X^{(4)},X^{(5)})\ddot{X}$$
$$+\Psi(X)\dot{X}+H(t,X,\dot{X},\ddot{X},\dddot{X},X^{(4)},X^{(5)})X=0, \tag{1}$$

in which $t\in\Re_+$ , $\Re_+=[0,\infty)$ and $X\in\Re^n$ ; $A$ , $B$ and $C$ are constant $n\times n$ -real symmetric matrices; $\Phi$ , $\Psi$ and $H$ are continuous $n\times n$ -symmetric real matrix functions depending, in each case, on the arguments shown in (1). Let $J\left(\Psi(X)X\,|X\right)$ denote the linear operator from the matrix function $\Psi(X)$ to the matrix

$$J\left(\Psi(X)X\,|X\right)=\left(\frac{\partial}{\partial x_j}\sum_{k=1}^{n}\psi_{ik}x_k\right)=\Psi(X)+\left(\sum_{k=1}^{n}\frac{\partial\psi_{ik}}{\partial x_j}x_k\right),$$

where $(x_1,x_2,...,x_n)$ and $(\psi_{ik})$ are components of $X$ and $\Psi$ , respectively. It is assumed that the matrix $J\left(\Psi(X)X\,|X\right)$ exists and is symmetric and continuous. From the relevant literature, it can be followed that, so far, many problems about the instability of solutions of various scalar and vector linear or nonlinear differential equations of third-, fourth-, fifth-, sixth-, seventh and eighth order have been investigated by researchers. For some papers carried out on the topic, one can refer to the book of Reissig et al [15] and the papers of Bereketoğlu [2], Ezeilo ([3], [4], [5], [6], [7]), Liao and Lu [9], Li and Yu [10], Li and Duan [11], Lu and Liao [12], Lu [13], Sadek ([16], [17]), Skrapek ([18], [19]), Tejumola [20], Tiryaki ([21], [22], [23]), Tunç ([24], [25], [26], [27], [28], [29], [30], [31], [32]), C.Tunç and E. Tunç ([33], [34], [35], [36]), C. Tunç and H. Sevli [37], E. Tunç [38] and the references listed therein. Throughout all the papers mentioned above the Lyapunov's second

2000 *Mathematics Subject Classification.* 34D05; 34D20.
*Key words and phrases.* Non-autonomous differential equation, sixth order, instability.

(or direct) method [14] is used as a basic tool to prove the result established there, and it will be also used to verify our result, which will be given hereafter. The motivation for the present work has been inspired especially by the papers in [20], [31] and the papers mentioned above. It should be noted that in [20], Tejumola investigated the instability of the trivial solution of the following sixth order scalar nonlinear differential equation of the type

$$x^{(6)}+a_1x^{(5)}+a_2x^{(4)}+a_3\dddot{x}+\varphi_4(x,\dot{x},\ddot{x},\dddot{x},x^{(4)},x^{(5)})\ddot{x}$$

$$+\varphi_5(x)\dot{x}+\varphi_6(x,\dot{x},\ddot{x},\dddot{x},x^{(4)},x^{(5)})=0.$$

He proved a result on the subject. Recently, in [31], Tunç investigated the instability of the trivial solution of sixth order nonlinear vector differential equation of the form

$$X^{(6)}+AX^{(5)}+BX^{(4)}+C\dddot{X}+\Phi(X,\dot{X},\ddot{X},\dddot{X},X^{(4)},X^{(5)})\ddot{X}$$

$$+\Psi(X)\dot{X}+H(X,\dot{X},\ddot{X},\dddot{X},X^{(4)},X^{(5)})X=0.$$

Clearly, (1) is a non-autonomous differential equation, that is, (1) is different from the above equations and ones considered in the literature, see also the papers mentioned above.

Throughout this paper, the symbol $\langle X,Y\rangle$ is used to denote the usual scalar product in $\Re^n$ , that is, $\langle X,Y\rangle=\sum_{i=1}^{n}x_iy_i$ , thus $\langle X,X\rangle=\|X\|^2$ , and $\lambda_i(A)$ , $(i=1,2,...,n)$ , are the eigenvalues of the $n\times n$ - matrix $A$ .

We take into consideration, in place of (1), the equivalent differential system

$$\dot{X}=Y,\dot{Y}=Z,\dot{Z}=S,\dot{S}=T,\dot{T}=U,$$

$$\dot{U}=-AU-BT-CS-\Phi(t,X,Y,Z,S,T,U)Z \tag{2}$$

$$-\Psi(X)Y-H(t,X,Y,Z,S,T,U)X,$$

which was obtained as usual by setting $\dot{X}=Y$ , $\ddot{X}=Z$ , $\dddot{X}=S$ , $X^{(4)}=T$ , $X^{(5)}=U$ by (1).

## 2. Preliminaries

In order to reach our main result, we will give a basic theorem for the general non-autonomous differential system and two well-known lemmas which play an essential role in the proof of our main result. Consider the differential system

$$\dot{x}=f(t,x),x(t_0)=x_0,t\geq 0, \tag{3}$$

where $f\in C[R_+\times S_{(\rho)},\ \Re^n]$ and $S_{(\rho)}=[x\in\Re^n:|x|<\rho]$ . Assume, for convenience that a solution $x(t)=x(t,t_0,x_0)$ of (3) exists and is unique for $t\geq t_0$ and $f(t,0)=0$ so that we have trivial solution $x=0$ . Let $K$ denote a class of the functions as $K=[\sigma\in C[[t_0,\rho),\Re_+]]$ such that $\sigma(t)$ is strictly increasing and $\sigma(0)=0$ .

Now, we state the following fundamental instability theorem.

**Theorem1.** Assume that there exists a $t_0\in\Re_+$ and an open set $U\subset S_{(\rho)}$ such that

$V\in C^1[[t_0,\infty)\times S_{(\rho)},\ \Re_+]$ for $(t,x)$ from $[t_0,\infty)\times U$ ,

**(i)** $0 < V(t,x) \leq a(|x|)$ , $a \in K$ ;

**(ii)** either $V'(t,x) \geq b(|x|)$ , $b \in K$ , $K = [\sigma \in C[[t_0,\rho),\Re_+]]$ such that $\sigma(t)$ is strictly increasing and $\sigma(0) = 0$ or $V'(t,x) = CV(t,x) + \omega(t,x)$ , where $C > 0$ and $\omega \in C[[t_0,\infty) \times U, \Re_+]$ ;

**(iii)** $V(t,x) = 0$ on $[t_0,\infty) \times (\partial U \bigcap S_{(\rho)})$ , $\partial U$ denotes boundary of $U$ and $0 \in \partial U$ .

Then the trivial solution $x = 0$ of system (3) is unstable.

**Proof.** See Lakshmikantham et al. [Theorem 1.1.9, 8].

**Lemma 1.** Let $A$ be a real symmetric $n \times n$ -matrix and
$a' \geq \lambda_i(A) \geq a > 0$ $(i = 1,2,...,n)$ , where $a'$ , $a$ are constants.
Then

$$a' \langle X, X \rangle \geq \langle AX, X \rangle \geq a \langle X, X \rangle$$

and

$$a'^2 \langle X, X \rangle \geq \langle AX, AX \rangle \geq a^2 \langle X, X \rangle$$

**Proof.** See Bellman[1].

**Lemma 2.** Let $Q$ , $D$ be any two real $n \times n$ commuting symmetric matrices. Then

**(i)** the eigenvalues $\lambda_i(QD)$ , $(i = 1,2,...,n)$ , of the product matrix $QD$ are real and satisfy
$\max\limits_{1\leq j,k\leq n} \lambda_j(Q)\lambda_k(D) \geq \lambda_i(QD) \geq \min\limits_{1\leq j,k\leq n} \lambda_j(Q)\lambda_k(D)$ ;

**(ii)** the eigenvalues $\lambda_i(Q+D)$ , $(i = 1,2,...,n)$ , of the sum of matrices $Q$ and $D$ are real and satisfy
$\left\{ \max\limits_{1\leq j\leq n} \lambda_j(Q) + \max\limits_{1\leq k\leq n} \lambda_k(D) \right\} \geq \lambda_i(Q+D) \geq \left\{ \min\limits_{1\leq j\leq n} \lambda_j(Q) + \min\limits_{1\leq k\leq n} \lambda_k(D) \right\}$ ,
where $\lambda_j(Q)$ and $\lambda_k(D)$ are, respectively, the eigenvalues of matrices $Q$ and $D$ .

**Proof.** See Bellman[1].

## 3. Main result

We establish the following theorem:

**Theorem 2.** In addition to the basic assumptions imposed on $A$ , $B$ , $C$ , $\Phi$ , $\Psi$ and $H$ that appeared in (2), we assume that the following conditions hold:There are constants $a_1$ , $a_2$ and $a_5$ such that
$\lambda_i(A) \geq a_1 > 0$ , $\lambda_i(B) \leq a_2 < 0$ , $|\lambda_i(\Psi(X)| \leq a_5$ , ( $a_5 > 0$ ),
and
$\lambda_i(H(t,X,Y,Z,S,T,U)) < \frac{1}{4a_2} [\lambda_i(\Phi(t,X,Y,Z,S,T,U))]^2$ , $(i = 1,2,...,n)$ ,
for all $t \in \Re_+$ and $X$ , $Y$ , $Z$ , $S$ , $T$ , $U \in \Re^n$ .
Then the zero solution of the system (2) is unstable.

**Remark.** It should be noted that there is no restriction on the eigenvalues of the matrix C in the system (2).

**Proof.** To prove Theorem 2, we construct a scalar differentiable Lyapunov function $V_0 = V_0(t, X, Y, Z, S, T, U)$ . This function, $V_0$ , is defined as follows:

$$\begin{aligned} V_0 = \quad & \langle X, U\rangle + \langle X, AT\rangle + \langle X, BS\rangle + \langle X, CZ\rangle \\ & - \langle Y, T\rangle - \langle Y, AS\rangle - \langle Y, BZ\rangle + \langle Z, S\rangle - \tfrac{1}{2}\langle Y, CY\rangle \\ & + \tfrac{1}{2}\langle Z, AZ\rangle + \int_0^1 \langle \Psi(\sigma X)X, X\rangle \, d\sigma. \end{aligned}$$

Clearly, $V_0(t, 0, 0, 0, 0, 0, 0) = 0$ on $[t_0, \infty)$ . Now, subject to the assumptions of Theorem 2, it is a straightforward calculation to see that

$$\begin{aligned} V_0(t, 0, 0, \varepsilon, \varepsilon, 0, 0) \quad & = \tfrac{1}{2}\langle \varepsilon, A\varepsilon\rangle + \langle \varepsilon, \varepsilon\rangle \\ & \geq \tfrac{1}{2}\langle \varepsilon, a_1\varepsilon\rangle + \langle \varepsilon, \varepsilon\rangle \\ & = (\tfrac{1}{2}a_1 + 1)\|\varepsilon\|^2 > 0 \end{aligned}$$

for all arbitrary, $\varepsilon \neq 0$ , $\varepsilon \in \Re^n$ . In view of the function $V_0 = V_0(t, X, Y, Z, S, T, U)$ , the assumptions of Theorem 2, the properties of symmetric matrices, Lemma 1, Lemma 2 and Cauchy-Schwarz inequality $|\langle X, Y\rangle| \leq \|X\| \ \ \|Y\|$ , one can easily obtain that there is a positive constant $K_1$ such that

$$V_0(t, X, Y, Z, S, T, U) \leq K_1 \left( \|X\|^2 + \|Y\|^2 + \|Z\|^2 + \|S\|^2 + \|T\|^2 + \|U\|^2 \right).$$

These show that assumption (i) of Theorem 1 holds.

Now, let $(X, Y, Z, S, T, U) = (X(t), Y(t), Z(t), S(t), T(t), U(t))$ be an arbitrary solution of system (2). By an elementary differentiation along the solution paths of the system (2), it can be verified that

$$\begin{aligned} \dot{V}_0 = \tfrac{d}{dt}V_0(t, X, Y, Z, S, T, U) = \quad & -\langle \Phi(t, X, Y, Z, S, T, U)Z, X\rangle \\ & -\langle H(t, X, Y, Z, S, T, U)X, X\rangle \\ & -\langle BZ, Z\rangle + \langle S, S\rangle - \langle \Psi(X)Y, X\rangle \\ & + \tfrac{d}{dt}\int_0^1 \langle \Psi(\sigma X)X, X\rangle \, d\sigma. \end{aligned} \tag{4}$$

Check that

$$\begin{aligned} \tfrac{d}{dt}\int_0^1 \langle \Psi(\sigma X)X, X\rangle \, d\sigma \quad & = \int_0^1 \langle \Psi(\sigma X)X, Y\rangle \, d\sigma + \int_0^1 \langle \sigma J\left(\Psi(\sigma X)X \,|\sigma X\,\right)Y, X\rangle \, d\sigma \\ & = \int_0^1 \langle \Psi(\sigma X)X, Y\rangle \, d\sigma + \int_0^1 \sigma \langle J\left(\Psi(\sigma X)X \,|\sigma X\,\right)X, Y\rangle \, d\sigma \\ & = \int_0^1 \langle \Psi(\sigma X)X, Y\rangle \, d\sigma + \int_0^1 \sigma \tfrac{\partial}{\partial\sigma}\langle \Psi(\sigma X)X, Y\rangle \, d\sigma \\ & = \sigma \langle \Psi(\sigma X)X, Y\rangle \,\big|_0^1 = \langle \Psi(X)X, Y\rangle. \end{aligned} \tag{5}$$

Combining the estimate (5) with (4), we deduce that

$$\begin{aligned}\dot{V}_0 = \quad & -\langle \Phi(t,X,Y,Z,S,T,U)Z,X\rangle - \langle H(t,X,Y,Z,S,T,U)X,X\rangle \\ & -\langle BZ,Z\rangle + \langle S,S\rangle\end{aligned}.$$

Hence, the assumptions of Theorem 2 and the fact $\langle S,S\rangle = \|S\|^2$ imply that

$$\begin{aligned}\dot{V}_0 \quad & \geq -\langle \Phi(t,X,Y,Z,S,T,U)Z,X\rangle - \langle H(t,X,Y,Z,S,T,U)X,X\rangle - a_2\langle Z,Z\rangle \\ & = -a_2\left\|Z+\tfrac{1}{2a_2}\Phi(t,X,Y,Z,S,T,U)X\right\|^2 - \langle H(t,X,Y,Z,S,T,U)X,X\rangle \\ & +\tfrac{1}{4a_2}\langle \Phi(t,X,Y,Z,S,T,U)X,\ \Phi(t,X,Y,Z,S,T,U)X\rangle \\ & \geq -\langle H(t,X,Y,Z,S,T,U)X,X\rangle \\ & +\tfrac{1}{4a_2}\langle \Phi(t,X,Y,Z,S,T,U)X,\Phi(t,X,Y,Z,S,T,U)X\rangle > 0.\end{aligned}$$

Thus, the assumptions of the theorem imply that $\dot{V}_0(t) \geq K_2\|X\|^2$ for all $t \geq 0$ , where $K_2$ is a positive constant, say infinite inferior limit of the function $\dot{V}_0$ . Besides, $\dot{V}_0 = 0$ $(t \geq 0)$ necessarily implies that $X = 0$ for all $t \geq 0$ , and therefore also that $Z = \dot{Y} = 0$ , $S = \ddot{Y} = 0$ , $T = \dddot{Y} = 0$ , $U = Y^{(4)} = 0$ for all $t \geq 0$ . Hence

$$X = Y = Z = S = T = U = 0 \text{ for all} \geq 0.$$

Therefore, subject to the assumptions of the theorem the function $V_0$ has the entire the criteria of Theorem 1, Lakshmikantham et al. [Theorem 1.1.9, 8]. Thus, the basic properties of the function $V_0(t,X,Y,Z,S,T,U)$ , which are proved just above verify that the zero solution of the system (2) is unstable, see also Lakshmikantham et al. [Theorem 1.1.9, 8]. The system of equations (2) is equivalent to differential equation (1) and the proof of Theorem 2 is now complete.

## References


[1] Bellman, R., "Introduction to matrix analysis". Reprint of the second (1970) edition. With a foreword by Gene Golub. Classics in Applied Mathematics, 19. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1997.

[2] Bereketoglu, H., "On the instability of trivial solutions of a class of eighth-order differential equations", *Indian J. Pure. Appl. Math.*, no.3, **22** (1991) 199-202.

[3] Ezeilo, J. O.C., "An instability theorem for a certain fourth order differential equation", *Bull. London Math. Soc.*, no. 2, **10**(1978) 184-185.

[4] Ezeilo, J. O.C., "Instability theorems for certain fifth-order differential equations", *Math. Proc. Cambridge Philos. Soc.*, no. 2, **84**(1978) 343-350.

[5] Ezeilo, J. O.C., "A further instability theorem for a certain fifth-order differential equation", *Math. Proc. Cambridge Philos. Soc.*, no. 3, **86**(1979) 491-493.

[6] Ezeilo, J. O.C., "Extension of certain instability theorems for some fourth and fifth order differential equations", *Atti. Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Natur.*, no. 4, (**8**) **66**(1979) 239-242.

[7] Ezeilo, J. O.C., "An instability theorem for a certain sixth order differential equation", *J. Austral. Math. Soc. Ser. A* , no.1, **32**(1982) 129-133.

[8] Lakshmikantham, V., Matrosov, V.M., Sivasundaram,S., Vector Lyapunov functions and stability analysis of nonlinear systems. Mathematics and its Applications, 63. Kluwer Academic Publishers Group, Dordrecht, 1991.

[9] Liao, Z.H. and Lu,D., "Instability of solution for the third order linear differential equation with varied coefficient", *Appl. Math. Mech.* (English Ed.), no. 10, **9** (1988) 969-984; translated from Appl. Math. Mech., no. 10, 9 (1988) 909-923 (Chinese).

[10] Li, W.J. and Yu, Y.H., "Instability theorems for some fourth-order and fifth-order differential equations", (Chinese) *J. Xinjiang Univ. Natur. Sci.*, no. 2, **7**(1990) 7-10.

[11] Li,W. J. and Duan, K.C., "Instability theorems for some nonlinear differential systems of fifth order", *J. Xinjiang Univ. Natur. Sci.*, no. 3, **17**(2000) 1-5.

[12] Lu, D. and Liao,Z.H., "Instability of solution for the fourth order linear differential equation with varied coefficient", *Appl. Math. Mech.* (English Ed.), no. 5, **14** (1993) 481-497; translated from Appl. Math. Mech., no. 5, 14 (1993) 455-469 (Chinese).

[13] Lu, D. "Instability of solution for a class of the third order nonlinear differential equation", *Appl. Math. Mech.* (English Ed.), no. 12, **16** (1995) 1185-1200; translated from Appl. Math. Mech., no. 12, 16 (1995) 1101-1114 (Chinese).

[14] Lyapunov, A.M., Stability of Motion,Academic Press, London, 1966.

[15] Reissig,R., Sansone, G. and Conti, R. Non-linear Differential Equations of Higher Order. Translated from the German, Noordhoff International Publishing, Leyden, 1974.

[16] Sadek, A.I. "An instability theorem for a certain seventh-order differential equation", *Ann. Differential Equations*, no. 1, **19** (2003) 1-5.

[17] Sadek, A.I. "Instability results for certain systems of fourth and fifth order differential equations", *Appl. Math. Comput.*, no. 2-3, **145** (2003) 541-549.

[18] Skrapek, W.A. "Instability results for fourth-order differential equations", *Proc. Roy. Soc. Edinburgh Sect. A* , no. 3-4, **85**(1980) 247-250.

[19] Skrapek, W.A. "Some instability theorems for third order ordinary differential equations", *Math. Nachr.*, **96**(1980) 113-117.

[20] Tejumola, H.O. "Instability and periodic solutions of certain nonlinear differential equations of orders six and seven", Ordinary Differential Equations (Abuja, 2000), 56-65, Proc. Natl. Math. Cent. Abuja Niger., 1.1, Natl. Math. Cent., Abuja, 2000.

[21] Tiryaki, A. "Extension of an instability theorem for a certain fourth order differential equation", *Bull. Inst. Math. Acad. Sinica.*, no.2, **16** (1988) 163-165.

[22] Tiryaki, A. "An instability theorem for a certain sixth order differential equation", *Indian J. Pure. Appl. Math.*, no.4, **21**(1990) 330-333.

[23] Tiryaki, A. "Extension of an instability theorem for a certain fifth order differential equation", National Mathematics Symposium (Trabzon, 1987), J. Karadeniz Tech. Univ. Fac. Arts Sci. Ser. Math. Phys., 11, (1988, 1989) 225-227.

[24] Tunc, C. "An instability theorem for a certain vector differential equation of the fourth order", *JIPAM. J. Inequal. Pure Appl. Math.* **5** (2004), no. 1, Article 5, 5 pp.

[25] Tunc, C. "An instability result for certain system of sixth order differential equations",*Appl. Math. Comput.*, no.2, **157** (2004) 477-481.

[26] Tunc, C. "On the instability of solutions of certain nonlinear vector differential equations of fifth order", *Panamer. Math. J.*, **14** (2004), no. 4, 25-30.

[27] Tunc, C. "On the instability of certain sixth-order nonlinear differential equations", *Electron. J. Diff. Eqns.*, Vol. **2004** , no. 117, (2004) 1-6.

[28] Tunc, C. "A further instability result for a certain vector differential equation of fourth order", *Int. J. Math. Game Theory Algebra* **15** (2006), no. 5, 489-495.

[29] Tunc, C. "An instability result for a certain non-autonomous vector differential equation of fifth-order", *Panamer. Math. J.* 15 (2005), no.3, 51-58.

[30] Tunc, C. "Instability of solutions of a certain non-autonomous vector differential equation of eighth-order", *Ann. Differential Equations* **22** (2006), no. 1, 7-12.

[31] Tunc, C. "New results about instability of nonlinear ordinary vector differential equations of sixth and seventh orders", *Dyn. Contin. Discrete Impuls. Syst. Ser. A Math. Anal.***14**(2007), no.1, 123-136.

[32] Tunc, C. "Some instability results on certain third order nonlinear vector differential equations", *Bull. Inst. Math. Acad. Sin.* (N.S.) **2** (2007), no. 1, 109-122.

[33] Tunc, C. and Tunc, E. "A result on the instability of solutions of certain non-autonomous vector differential equations of fourth order", *East-West J. Math.* **6** (2004), no. 2, 153-160.

[34] Tunc, C. and Tunc, E., "Instability of solutions of certain nonlinear vector differential equations of order seven", *Iran. J. Sci. Technol. Trans. A Sci.* **29** (2005), no. 3, 1-7.

[35] Tunc, C. andTunc, E., "An instability theorem for a class of eighth-order differential equations". (Russian) *Differ. Uravn.* **42** (2006), no. 1, 135-138, 143; translation in Differ. Equ. 42 (2006), no. 1, 150-154.

[36] Tunc, C. and Tunc, E., "Instability results for certain third order nonlinear vector differential equations", *Electron. J. Differential Equations* 2006, no. 109, 10 pp.

[37] Tunc, C. and Sevli, H. "On the instability of solutions of certain fifth order nonlinear differential equations", *Mem. Differential Equations Math. Phys.* **35** (2005), 147-156.

[38] Tunc, E. "Instability of solutions of certain nonlinear vector differential equations of third order", *Electron. J. Differential Equations*, no. 51, (2005) 1-6 (electronic).

Department of Mathematics, Faculty of Arts and Sciences, Yüzüncü Yil University 65080, Van -Turkey

*E-mail address*: cemtunc@yahoo.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 15–25
ISSN 1930-1235: (electronic version)

# IMPLICIT WIENER-HOPF EQUATIONS AND QUASI VARIATIONAL INEQUALITIES

MUHAMMAD ASLAM NOOR

(Communicated by E. Hashorva)

Abstract. In this paper, we introduce and consider a new class of Wiener-Hopf equations involving the nonlinear operator and nonexpansive operators, which is called the implicit Wiener-Hopf equations. Essentially using the projection technique, we establish the equivalence between the implicit Wiener-Hopf equations and quasi variational inequalities. Using this alternative equivalent formulation, we suggest and analyze an iterative method for finding the common element of the set of fixed points of nonexpansive mappings and the set of solutions of the quasi variational inequalities. We also study the convergence criteria of iterative methods under some mild conditions. Our results include the previous results as special cases and may be considered as an improvement and refinement of the previously known results.

## 1. Introduction

Quasi variational inequalities are being used as a mathematical programming tool in modelling various equilibrium problems in economics, operations research, optimization, regional, ecology and network analysis, see [1-33]. It is well known that the quasi variational inequalities include variational inequalities, implicit complementarity problems and optimization problems as special cases. It combines novel theoretical and algorithmic advances with new domain of applications. Analysis of these problems requires a blend of techniques from convex analysis, functional analysis and numerical analysis. As a result of such interaction between different branches of mathematical and engineering sciences, we now have a variety of techniques to suggest and analyze various numerical methods including projection technique and its variant forms, auxiliary principle and Wiener-Hopf equations for solving variational inequalities and related optimization problems. Essentially using the projection technique, one can establish the equivalence between the variational inequalities and the Wiener-Hopf equations. This equivalence has played an important and significant role in studying various problems associated with variational inequalities. Related to the quasi variational inequalities and the implicit Wiener-Hopf equations, we have the problem of finding the fixed points of the nonexpansive mappings, which is the subject of current interest in functional analysis. It is natural to consider a unified approach to these different problems.

Received by the editors January 22, 2008 and, in revised form, , 2008.
2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 90C33.
*Key words and phrases.* Wiener-Hopf equations; Nonexpansive mappings; Relaxed $(\gamma, r)$-Cocoercive mappings; Variational inequalities, Hilbert spaces.

Motivated and inspired by the research going on in this direction, we first introduce a new class of the Wiener-Hopf equations involving a nonexpansive operator $S$, which is called the implicit Wiener-Hopf equations. Using the projection technique, we show that the implicit Wiener-Hopf equations are equivalent to the quasi variational inequalities. We use this alternative equivalence to suggest and analyze an iterative scheme for finding the common solutions of the variational inequalities and nonexpansive mappings using the Wiener-Hopf equation technique. We also prove the convergence criteria of these new iterative schemes under some mild conditions. Since the quasi variational inequalities include variational inequalities and the implicit(quasi) complementarity problems **as** special cases, results proved in this paper continue to hold for these problems. In this respect, results proved in this paper may be viewed as significant and improvement of the previously known results.

## 2. Formulations and Basic Facts

Let $H$ be a real Hilbert space, whose inner product and norm are denoted by $\langle \cdot, \cdot \rangle$ and $\| \cdot \|$, respectively. Let $K(u)$ be a closed and convex-valued set in $H$ and $T : H \longrightarrow H$ be a nonlinear operator.

A *quasi variational inequality* consists in finding $u \in K(u)$, such that

$$\langle Tu, v - u \rangle \geq 0, \quad \forall v \in K(u). \tag{1}$$

It is well known [1- 28] that a large class of obstacle, unilateral, contact, free, moving, and equilibrium problems arising in economics, finance, physic**s**, mathematic**s**, engineering and applied sciences can be studied in the unifying and general framework of (1).

To convey an idea of the applications of the quasi variational inequalities, we consider the second-order implicit obstacle boundary value problem of finding $u$ such that

$$\left.\begin{array}{ll} -u'' \geq f(x) & \text{on } \Omega = [a,b] \\ u \geq M(u) & \text{on } \Omega = [a,b] \\ [-u'' - f(x)][u - M(u)] = 0 & \text{on } \Omega = [a,b] \\ u(a) = 0, \quad u(b) = 0. & \end{array}\right\} \tag{2}$$

where $f(x)$ is a continuous function and $M(u)$ is the cost (obstacle) function. The prototype encountered [2] is

$$M(u) = k + \inf_i \{u^i\}. \tag{3}$$

In (3), $k$ represents the switching cost. It is positive when the unit is turned on and equal to zero when the unit is turned off. Note that the operator $M$ provides the coupling between the unknowns $u = (u^1, u^2, \ldots, u^i)$. We study the problem (2) in the framework of the quasi variational inequality approach. To do so, we first define the set $K(u)$ as

$$K(u) = \{v : v \in H_0^1(\Omega) : v \geq M(u), \quad \text{on } \Omega\}, \tag{4}$$

which is a closed convex-valued set in $H_0^1(\Omega)$, where $H_0^1(\Omega)$ is a Sobolev (Hilbert) space. One can easily show that the energy functional associated with the problem

(2) is

$$\begin{aligned} I[v] &= -\int_a^b \left(\frac{d^2v}{dx^2}\right) v dx - 2\int_a^b f(x)\,(v)\,dx, \quad \forall v \in K(u) \\ &= \int_a^b \left(\frac{dv}{dx}\right)^2 dx - 2\int_a^b f(x)\,(v)\,dx \\ &= \langle Tv, v\rangle - 2\langle f, v\rangle \end{aligned} \tag{5}$$

where

$$\begin{aligned} \langle Tu, v\rangle &= \int_a^b \left(\frac{d^2u}{dx^2}\right)(v)\,dx = \int_a^b \frac{du}{dx}\frac{dv}{dx}dx \\ \langle f, v\rangle &= \int_a^b f(x)(v)dx. \end{aligned} \tag{6}$$

It is clear that the operator $T$ defined by (6) is linear, symmetric and positive. Using the technique of Noor [13,14,20], one can show that the minimum of the functional $I[v]$ defined by (5) associated with the problem (2) on the closed convex-valued set $K(u)$ can be characterized by the inequality of type (1). See also [1-29] for the formulation, applications, numerical methods and sensitivity analysis of the quasi variational inequalities.

If $K^\star(u)$ is the dual (polar) cone of the convex-valued cone $K(u)$, then the quasi variational inequalities (2.1) are equivalent to finding $u$ such that

$$u \in K(u), \quad Tu \in K^\star(u), \quad \text{and} \quad \langle u, Tu\rangle = 0, \tag{7}$$

which are called the quasi (implicit) complementarity problems. It is well known that a wide class of problems arising in various branches of pure and applied sciences can be studied via the implicit complementarity problems (7). For the applications, numerical methods and physical formulation, see the references.

If the convex-valued set $K(u)$ is independent of the solution $u$, that is, $K(u) = K$, a closed convex set, then problem (1) is equivalent to finding $u \in K$, such that

$$\langle Tu, v - u\rangle \geq 0, \quad \forall v \in K, \tag{8}$$

which is known as the classic variational inequality introduced and studied by Stampacchia [32] in 1964. For the state of the art in this theory; see [1- 33].

We also need the following well-known concepts and results.

**Lemma 2.1.** Let $K(u)$ be a closed convex-valued set in $H$. Then, for a given $z \in H$, $u \in K(u)$ satisfies the inequality

$$\langle u - z, v - u\rangle \geq 0, \quad \forall v \in K(u),$$

if and only if

$$u = P_{K(u)}z,$$

where $P_{K(u)}$ is the projection of $H$ onto the closed convex-valued set $K(u)$.

It is worth mentioning that the implicit projection operator $P_{K(u)}$ is not an nonexpansive operator. This fact motivates us to consider the following assumption on the projection operator $P_{K(u)}$ as:

**Assumption 2.1.** The projection operator $P_{K(u)}$ satisfies the following relation.

$$\|P_{K(u)}w - P_{K(v)}w\| \leq \nu\|u - v\|, \quad \forall v, u, w \in H,$$

where $\nu > 0$ is a constant.

We remark that Assumption 2.1 is true for the special case,

$$K(u) = m(u) + K, \tag{9}$$

which appears in many important applications [2], where $m$ is a point-to-point mapping and $K$ is a closed convex set in $H$. It is well known that

$$P_{K(u)}w = P_{m(u)+K}w = m(u) + P_K[w - m(u)], \quad \forall w, u \in H. \tag{10}$$

We remark that if the mapping $m(u)$ is a Lipschitz continuous with constant $\nu_1 > 0$, then, from (9) and (10), we have

$$\begin{aligned} \|P_{m(u)K}w - P_{m(v)+K}w\| &= \|m(u) - m(v) + P_K[w - m(u)] - P_K[w - m(v)]\| \\ &\leq 2\|m(u) - m(v)\| \leq 2\nu_1\|u - v\|. \end{aligned}$$

This shows that the projection operator $P_{m(u)+K}$ is Lipschitz continuous with constant $2\nu_1 > 0$. and satisfies the Assumption 2.1 with $\nu = 2\nu_1$.

We now show that the quasi variational inequalities (1) are equivalent to the implicit fixed point problem. This result can be proved by using Lemma 2.1. See also Noor [9].

**Lemma 2.2.** The function $u \in K(u)$ is a solution of the quasi variational inequality (1) if and only if $u \in K(u)$ satisfies the relation

$$u = P_{K(u)}[u - \rho Tu],$$

where $\rho > 0$ is a constant.

Lemma 2.2 implies that quasi variational inequalities and the fixed point problems are equivalent. This alternative equivalent formulation has played a significant role in the studies of the quasi variational inequalities and related optimization problems.

We now state the problem.

**Remark 2.3.** Let $S$ be a nonexpansive mapping. We denote the set of the fixed points of $S$ by $F(S)$ and the set of the solutions of the quasi variational inequalities (2.1) by $QVI(K,T)$. If $x^* \in F(S) \cap VI(K,T)$, then $x^* \in F(S)$ and $x^* \in VI(K,T)$. Thus from Lemma 2.2, it follows that

$$x^* = Sx^* = P_{K(u)}[x^* - \rho Tx^*] = SP_{K(u)}[x^* - \rho Tx^*], \tag{11}$$

where $\rho > 0$ is a constant.

This fixed point formulation is used to suggest the following iterative method for finding a common element of two different sets of solutions of the fixed points of the nonexpansive mappings and the variational inequalities.

**Algorithm 2.1.** For a given $u_0 \in K(u)$, compute the approximate solution $x_n$ by the iterative schemes

$$u_{n+1} = (1 - a_n)u_n + a_nSP_{K(u_n)}[u_n - \rho Tu_n],$$

where $a_n \in [0,1]$ for all $n \geq 0$ and $S$ is the nonexpansive operator. Algorithm 2.1 is also known as a Mann iteration. For the convergence analysis of Algorithm 2.1, see Huang and Noor [24] and Noor [16,17].

Related to the variational inequalities, we have the problem of solving the Wiener-Hopf equations. To be more precise, let $Q_{K(u)} = I - SP_{K(u)}$, where $P_{K(u)}$ is the

projection of $H$ onto the closed convex set $K(u)$, $I$ is the identity operator and $S$ is the nonexpansive operator. We consider the problem of finding $z \in H$ such that

$$TSP_{K(u)}z + \rho^{-1}Q_{K(u)}z = 0, \tag{12}$$

which is called the implicit Wiener-Hopf equation involving the nonexpansive operator $S$. For $S = I$, the identity operator, we obtain the implicit Wiener-Hopf equation, introduced by Noor [14]. If $S = I$, and $K(u) = K$, then the implicit Wiener-Hopf equations (12) reduce to the original Wiener-Hopf equations considered and studied by Shi [31] in relation with the classical variational inequalities. Using essentially the technique of the projection operator, one can establish the equivalence between the Wiener-Hopf equations and variational inequalities. This alternative equivalence has played a fundamental and basic role in developing some efficient and robust methods for solving variational inequalities and related optimization problems. The Wiener-Hopf equation technique has been used to study the sensitivity analysis and asymptotical stability of the variational inequalities, see [11-27,30,31]. It has been shown that the Wiener-Hopf equation technique is more flexible and general than the projection method and its variant form.

**Definition 2.1.** An operator $T : H \to H$ is called $\mu$-Lipschitzian if, there exists a constant $\mu > 0$, such that

$$||Tx - Ty|| \leq \mu||x - y||, \quad \forall x, y \in H.$$

**Definition 2.2.** An operator $T : H \to H$ is called $\alpha$-inverse strongly monotone (or co-coercive ) if, there exists a constant $\alpha > 0$, such that

$$\langle Tx - Ty, x - y\rangle \geq \alpha||Tx - Ty||^2, \quad \forall x, y \in H.$$

**Definition 2.3.** An operator $T : H \to H$ is called $r$-strongly monotone if, there exists a constant $r > 0$ such that

$$\langle Tx - Ty, x - y\rangle \geq r||x - y||^2, \quad \forall x, y \in H.$$

**Definition 2.4.** An operator $T : H \to H$ is called relaxed $(\gamma, r)$-cocoercive if, there exists constants $\gamma > 0, r > 0$, such that

$$\langle Tx - Ty, x - y\rangle \geq -\gamma||Tx - Ty||^2 + r||x - y||^2, \quad \forall x, y \in H.$$

**Remark 2.1.** Clearly a $r$-strongly monotone operator or a $\gamma$-inverse strongly monotone operator must be a relaxed $(\gamma, r)$-cocoercive operator, but the converse is not true. Therefore the class of the relaxed $(\gamma, r)$-cocoercive operators is the most general class, and hence definition 2.4 includes both the definition 2.2 and the definition 2.3 as special cases.

**Remark 2.2.** From definition 2.2, it follows that if $T$ is $\alpha$-inverse strongly monotone (or co-coercive), **then** $T$ is also Lipschitz continuous with constant $\frac{1}{\alpha}$.

**Lemma 2.3 [34].** Suppose $\{\delta_k\}_{k=0}^{\infty}$ is a nonnegative sequence satisfying the following inequality:

$$\delta_{k+1} \leq (1 - \lambda_k)\delta_k + \sigma_k, \ k \geq 0,$$

with $\lambda_k \in [0, 1]$, $\sum_{k=0}^{\infty} \lambda_k = \infty$, and $\sigma_k = o(\lambda_k)$. Then $\lim_{k\to\infty} \delta_k = 0$.

## 3. Main Results

In this section, we use the Wiener-Hopf equations to suggest and analyze an iterative method for finding the common element of the nonexpansive mappings and the variational inequalities QVI(T,K). For this purpose, we need the following result, which can be proved by using Lemma 2.2. However, for the sake of completeness, we include its proof.

**Lemma 3.1.** The element $u \in K(u)$ is a solution of quasi variational inequality (1) if and only if $z \in H$ satisfies the implicit Wiener-Hopf equation (12), where

$$u = P_{K(u)}z, \tag{13}$$

$$z = u - \rho Tu, \tag{14}$$

where $\rho > 0$ is a constant.

**Proof.** Let $u \in K(u)$ be a solution of VI(K,T). Then, from Lemma 2.3 and Remark 2.3, we have

$$u = SP_{K(u)}[u - \rho Tu]. \tag{15}$$

Let

$$z = u - \rho Tu. \tag{16}$$

Form (15) and (16), we have

$$u = SP_{K(u)}z, \qquad z = u - \rho Tu,$$

from which, we have

$$z = SP_{K(u)}z - \rho TSP_{K(u)}z,$$

which is exactly the implicit Wiener-Hopf equation (12), the required result. □

From Lemma 3.1, it follows that the quasi variational inequality (1) and the implicit Wiener-Hopf equation (12) are equivalent. This alternative equivalent formulation has been used to suggest and analyze a wide class of efficient and robust iterative methods for solving variational inequalities and related optimization problems, see [3-16] and the references therein. We denote the set of the solutions of the Wiener-Hopf equations by IWHE(H,T,S).

Using Lemma 3.1 and Remark 2.3, we now suggest and analyze a new iterative algorithm for finding the common element of the solution sets of the quasi variational inequalities and nonexpansive mappings $S$ and this is the main motivation of this paper.

**Algorithm 3.1.** For a given $z_0 \in H$, compute the approximate solution $z_{n+1}$ by the iterative schemes

$$u_n = SP_{K(u_n)}z_n \tag{17}$$

$$z_{n+1} = (1 - a_n)z_n + a_n\{u_n - \rho Tu_n\} \tag{18}$$

where $a_n \in [0, 1]$ for all $n \geq 0$ and $S$ is a nonexpansive operator. For $S = I$, the identity operator, Algorithm 3.1 reduces to the following iterative method for solving quasi variational inequalities (1) and appears to be a new one.

**Algorithm 3.2.** For a given $z_0 \in H$, compute the approximate solution $z_{n+1}$ by the iterative schemes

$$\begin{aligned} u_n &= P_{K(u_n)}z_n \\ z_{n+1} &= (1 - a_n)z_n + a_n\{u_n - \rho Tu_n\}. \end{aligned}$$

For $a_n = 1$ and $S = I$, the identity operator, Algorithm 3.1 collapses to the following iterative method for solving quasi variational inequalities (1).

**Algorithm 3.3.** For a given $z_0 \in H$, compute the approximate solution $z_{n+1}$ by the iterative schemes

$$\begin{aligned} u_n &= P_{K(u_n)} z_n \\ z_{n+1} &= u_n - \rho T u_n. \end{aligned}$$

If $K(u) = K$, the convex set in $H$, then Algorithms 3.1-3.3 reduce to the following algorithms for solving variational inequalities (8) and nonexpansive mapping, which are due to Noor and Huang [25].

**Algorithm 3.4.** For a given $z_0 \in H$, compute the approximate solution $z_{n+1}$ by the iterative schemes

$$\begin{aligned} u_n &= S P_K z_n \\ z_{n+1} &= (1 - a_n) z_n + a_n \{u_n - \rho T u_n\} \end{aligned}$$

where $a_n \in [0, 1]$ for all $n \geq 0$ and $S$ is a nonexpansive operator. For $S = I$, the identity operator, Algorithm 3.4 reduces to the following iterative method for solving variational inequalities (8) and appears to be a new one.

**Algorithm 3.5.** For a given $z_0 \in H$, compute the approximate solution $z_{n+1}$ by the iterative schemes

$$\begin{aligned} u_n &= P_K z_n \\ z_{n+1} &= (1 - a_n) z_n + a_n \{u_n - \rho T u_n\}. \end{aligned}$$

For $a_n = 1$ and $S = I$, the identity operator, Algorithm 3.4 collapses to the following iterative method for solving variational inequalities (2.8).

**Algorithm 3.6.** For a given $z_0 \in H$, compute the approximate solution $z_{n+1}$ by the iterative schemes

$$\begin{aligned} u_n &= P_K z_n \\ z_{n+1} &= u_n - \rho T u_n. \end{aligned}$$

We now study the conditions under the approximate solution obtained from Algorithm 3.1

**Theorem 3.1.** Let $T$ be a relaxed $(\gamma, r)$-cocoercive and $\mu$-Lipschitzian mapping and $S$ be a nonexpansive mapping such that $F(S) \cap IWHE(H, T, S) \neq \emptyset$. Let $\{z_n\}$ be a sequence defined by Algorithm 2.1, for any initial point $z_0 \in H$. If Assumption 2.1 holds and

$$\begin{aligned} |\rho - \frac{r - \gamma\mu^2}{\mu^2}| &\leq \frac{\sqrt{(r - \gamma\mu^2)^2 - \mu^2\nu(2 - \nu)}}{\mu^2}, \\ & r > \gamma\mu^2 + \mu\sqrt{\nu(2 - \nu)}, \quad \nu \in (0, 1), \end{aligned} \tag{19}$$

$a_n \in [0, 1]$ and $\sum_{n=0}^{\infty} a_n = \infty$, then $z_n$ converges strongly to $z^* \in F(S) \cap IWHE(H, T, S)$.

**Proof.** Let $z^* \in H$ be a solution of $F(S) \cap IWHE(H,T,S)$. Then, from Lemma 3.1, we have

$$u^* = a_n SPK_{(u^*)}z^* \tag{20}$$

$$z^* = (1-a_n)z^* + a_n\{u^* - \rho Tu^*\} \tag{21}$$

where $a_n \in [0,1]$ and $u^* \in K$ is a solution of QVI(K,I). To prove the result, we need first to evaluate $||z_{n+1} - z^*||$ for all $n \geq 0$. From (18) and (21), we have

$$\begin{aligned} ||z_{n+1} - z^*|| &= ||(1-a_n)z_n + a_n\{u_n - \rho Tu_n\} \\ &\quad -(1-a_n)z^* - a_n\{u^* - \rho Tu^*\}|| \\ &\leq (1-a_n)||z_n - z^*|| + a_n||u_n - u^* - \rho(Tu_n - Tu^*)||. \end{aligned} \tag{22}$$

From the relaxed $(\gamma, r)$-cocoercive and $\mu$-Lipschitzian definition on $T$, we have

$$\begin{aligned} &||u_n - u^* - \rho(Tu_n - Tu^*)||^2 \\ =\ &||u_n - u^*||^2 - 2\rho\langle Tu_n - Tu^*, u_n - u^*\rangle + \rho^2||Tu_n - Tu^*||^2 \\ \leq\ &||u_n - u^*||^2 - 2\rho[-\gamma||Tu_n - Tu^*||^2 + r||u_n - u^*||^2] \\ &+\rho^2||Tu_n - Tu^*||^2 \\ \leq\ &||u_n - u^*||^2 + 2\rho\gamma\mu^2||u_n - u^*||^2 - 2\rho r||u_n - u^*||^2 + \rho^2\mu^2||u_n - u^*||^2 \\ =\ &[1 + 2\rho\gamma\mu^2 - 2\rho r + \rho^2\mu^2]||u_n - u^*||^2 \\ =\ &\theta_1^2\|u_n - u^*\|^2, \end{aligned} \tag{23}$$

where

$$\theta_1 = \sqrt{1 + 2\rho\gamma\mu^2 - 2\rho r + \rho^2\mu^2}. \tag{24}$$

Combining (22) and (23), we have

$$\|z_{n+1} - z^*\| \leq (1-a_n)\|z_n - z^*\| + a_n\theta_1\|u_n - u^*\|. \tag{25}$$

From (17), (20) and the Assumption 2.1., we have

$$\begin{aligned} \|u_n - u^*\| &\leq a_n\|SP_{K(u_n)}z_n - SP_{K(u^*)}z^*\| \\ &\leq \|P_{K(u_n)}z_n - P_{K(u_n)}z^*\| + \|P_{K(u_n)}z^* - P_{K(u^*)}z^*\| \\ &\leq \nu\|u_n - u^*\| + \|z_n - z^*\|, \end{aligned}$$

which implies that

$$\|u_n - u^*\| \leq \frac{1}{1-\nu}\|z_n - z^*\|. \tag{26}$$

From (25) and (26), we obtain that

$$\begin{aligned} ||z_{n+1} - z^*|| &\leq (1-a_n)||z_n - z^*|| + a_n\theta\|z_n - z^*\| \\ &= [1 - a_n(1-\theta)]||z_n - z^*||, \end{aligned}$$

where

$$\theta = \frac{\sqrt{1 + 2\rho\gamma\mu^2 - 2\rho r + \rho^2\mu^2}}{1-\nu} < 1, \quad \text{using (19)},$$

and hence by Lemma 2.3, $\lim_{n\to\infty}||z_n - z^*|| = 0$, completing the proof. □

We now prove the strong convergence of Algorithm 3.1 under the $\alpha$-inverse strongly monotonicity.

**Theorem 3.2.** Let $K(u)$ be a closed convex subset of a real Hilbert space $H$. Let $T$ be an $\alpha$-inverse strongly monotonic mapping with constant $\alpha >$ . and $S$ be a nonexpansive mapping such that $F(S) \cap IWHE(H,T) \neq \emptyset$. If

$$|\rho - \alpha| \leq \alpha(1-\nu), \quad \nu \in (0,1), \tag{27}$$

then the approximate solution obtained from Algorithm 3.1 converges strongly to $z^* \in F(S) \cap IWHE(H,T)$.

**Proof.** Let $T$ be $\alpha$-inverse strongly monotone with the constant $\alpha > 0$, then $T$ is $\frac{1}{\alpha}$–Lipschitzian continuous. Consider

$$\begin{aligned}
& ||u_n - u^* - \rho[Tu_n - Tu^*]||^2 \\
= \; & ||u_n - u^*||^2 + \rho^2||Tu_n - Tu^*||^2 - 2\rho\langle Tu_n - Tu^*, u_n - u^*\rangle \\
\leq \; & ||u_n - u^*||^2 + \rho^2||Tu_n - Tu^*||^2 - 2\rho\alpha||Tu_n - Tu^*||^2 \\
= \; & ||u_n - u^*||^2 + (\rho^2 - 2\rho\alpha)||Tu_n - Tu^*||^2 \\
\leq \; & ||u_n - u^*||^2 + (\rho^2 - 2\rho\alpha) \cdot \frac{1}{\alpha^2}||u_n - u^*||^2 \\
= \; & \left(1 + \frac{(\rho^2 - 2\rho\alpha)}{\alpha^2}\right)||u_n - u^*||^2 = \theta_2\|u_n - u^*\|^2, \qquad (28)
\end{aligned}$$

where

$$\theta_2 = (1 + \frac{(\rho^2 - 2\rho\alpha)}{\alpha^2})^{1/2}. \tag{29}$$

From (27), (28) and (29), we have

$$\begin{aligned}
||z_{n+1} - z^*|| &\leq (1-a_n)||z_n - z^*|| + a_n||u_n - u^* - \rho(Tu_n - Tu^*)\| \\
&\leq (1-a_n)||x_n - x^*|| + a_n\theta_2||u_n - u^*|| \\
&= [1 - a_n(1-\theta_3)]||z_n - z^*||,
\end{aligned}$$

where

$$\theta_3 = \frac{\sqrt{1 + \frac{\rho^2 - 2\rho\alpha}{\alpha^2}}}{1-\nu} < 1, \quad \text{using (26).}$$

Therefore, it follows $\lim_{n\to\infty}||z_n - z^*|| = 0$ from Lemma 2.3, completing the proof. □

## 4. Computational Aspects

In this paper, we have shown that the variational inequalities are equivalent to a new class of Wiener-Hopf equations involving the nonexpansive operator. This equivalence is used to suggest and analyze an iterative method for finding the common element of set of the solutions of the variational inequalities and the set of the fixed-points of the nonexpansive operator. It is worth mentioning that Pitonyak, Shi and Schiller [30] and Noor, Wang and Xiu [28] used the Wiener-Hopf equations technique to develop some very efficient and numerically implementable iterative methods for solving variational inequalities and related optimization problems. The results are encouraging and perform better than other methods. It is interesting to use the techniques and ideas of this paper to develop other new iterative methods for solving the quasi variational inequalities involving the nonexpansive operators. This is another direction for future work.

**Acknowledgement.** I wish to express my deepest gratitude to Prof. Dr. Enkelejd Hashorva, Editor, Albanian Journal of Mathematics for his invitation. I am also grateful to Dr. S. M. Junaid Zaidi, Rector, CIIT, for the excellent research facilities.

## References

[1] C. Baiocchi, A. Capelo, Variational and Quasi Variational Inequalities, Wiley, New York, 1984.

[2] G. L. Blankenship and J. L. Menaldi, Optimal stochastic scheduling of power generation system with scheduling delays and large cost differentials, SIAM J. Control Optim. **22**(1984), 121-132.

[3] J. Cranks, Free and Moving Boundary Problems, Clarendon Press, Oxford, UK, 1984.

[4] P. Daniele, F. Giannessi, A. Maugeri, Equilibrium Problems and Variational Models, Kluwer Academic Publishers, United Kingdom, 2003.

[5] F. Giannessi and A. Magueri, Variational Inequalities and Network Equilibrium Problems, Plenum Press, New York, NY, 1995.

[6] F. Giannessi, A. Magure and M. S. Pardalos, Equilibrium Problems: Nonsmooth Optimization and Variational Inequality Models, Kluwer Academic Publishers, Dordrecht, Holland, 2001.

[7] R. Glowinski, J. L. Lions and R. Tremolieres, Numerical Analysis of Variational Inequalities, North-Holland, Amsterdam, Holland, 1981.

[8] M. B. Lignola, Well-posedness and L-well-posedness for quasivariational inequalities, J. Optim. Theory Appl. **128**(2006), 119-138.

[9] M. Aslam Noor, An iterative schemes for a class of quasi variational inequalities, J. Math. Anal. Appl. **110**(1985), 463-468.

[10] M. Aslam Noor, Quasi variational inequalities, Appl. Math. Letters, **1**(1988), 367-370.

[11] M. Aslam Noor, Wiener-Hopf equations and variational inequalities, J. Optim. Theory Appl. 79(1993) 197-206.

[12] M. Aslam Noor, Some recent advances in variational inequalities, Part I: Basic concepts, New Zealand J. Math. 26(1997) 53-80.

[13] M. Aslam Noor, Some recent advances in variational inequalities, Part II: Other concepts, New Zealand J. Math. 26(1997) 229-255.

[14] M. Aslam Noor, Sensitivity analysis for quasi variational inequalities, J. Optim. Theory Appl. 95(1997) 399-407.

[15] M. Aslam Noor, Generalized quasi variational inequalities and implicit Wiener-Hopf equations, Optimization, **45**(1999), 197-222.

[16] M. Aslam Noor, New approximation schemes for general variational inequalities, J. Math. Anal. Appl. 251 (2000) 217-229.

[17] M. Aslam Noor, Implicit dynamical systems and quasi variational inequalities, Appl. Math. Computation, **134**(2002), 216-226.

[18] M. Aslam Noor, A Wiener-Hopf dynamical system for variational inequalities, New Zealand J. Math. 31(2002) 173-182.

[19] M. Aslam Noor, Sensitivity analysis framework for general quasi variational inequalities, Computer Math. Appl. **44**(2002), 216-226.

[20] M. Aslam Noor, Some developments in general variational inequalities, Appl. Math. Comput. 152 (2004) 199-277.

[21] M. Aslam Noor, General variational inequalities and nonexpansive mappings, J. Math. Anal. Appl.**331**(2007), 810-822.

[22] M. Aslam Noor, On merit functions for quasi variational inequalities, J. Math. Inequal. **1**(2007), 259-268.
[23] M. Aslam Noor, Existence results for quasi variational inequalities, Banach J. Math. Anal. **1**(2007), 186-194.
[24] M. Aslam Noor and Z. Huang, Quasi variational inequalities and nonexpansive mappings, Inter. J. Appl. Math. Eng. Sciences, **1**(2007), 1-10.
[25] M. Aslam Noor and Z. Huang, Wiener-Hopf equations technique for variational inequalities and nonexpansive mappings, Appl. Math. Computation, **191**(2007), 504-510..
[26] M. Aslam Noor and Zhenyu Huang, Three-step methods for nonexpansive mappings and variational inequalities, Appl. Math. Comput. **187**(2007), 680-685.
[27] M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Some aspects of variational inequalities, J. Comput. Appl. Math. 47(1993) 285-312.
[28] M. Aslam Noor, Y. J. Wang and N. Xiu, Some new projection methods for variational inequalities, Appl. math. Comput. 137(2003) 423-435.
[29] M. Patriksson, Nonlinear Programming and Variational Inequalities: A Unified Approach, Kluwer Academic Publishers, Dordrecht, 1998.
[30] A. Pitonyak, P. Shi and M. Shiller, On an iterative method for variational inequalities, Numer. Math. 58(1990) 231-242.
[31] P. Shi, Equivalence of variational inequalities with Wiener-Hopf equations, Proc. Amer. Math. Soc. 111(1991) 339-346.
[32] G. Stampacchia, Formes bilineaires coercivites sur les ensembles convexes,Comptes Rendus de l'Academie des Sciences, Paris, 258 (1964) 4413-4416.
[33] W. Takahashi and M. Toyoda, Weak convergence theorems for nonexpansive mappings and monotone mappings, J. Optim. Theory Appl. 118 (2) (2003) 417-428.
[34] X.L. Weng, Fixed point iteration for local strictly pseudocontractive mappings, Proc. Amer. Math. Soc. 113 (1991) 727-731.

Mathematics Department, COMSATS Institute of Information Technology, Islamabad, Pakistan
*E-mail address*: noormaslam@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 27–32
ISSN 1930-1235: (electronic version)

# SOME VANISHING SUMS INVOLVING BINOMIAL COEFFICIENTS IN THE DENOMINATOR

S.PURKAIT AND B.SURY

Abstract. We obtain expressions for sums of the form $\sum_{j=0}^{m}(-1)^j \frac{j^d\binom{m}{j}}{\binom{n+j}{j}}$ and deduce, for an even integer $d \geq 0$ and $m = n > d/2$, that this sum is 0 or $\frac{1}{2}$ according as to whether $d > 0$ or not. Further, we prove for even $d > 0$ that $\sum_{l=1}^{d} c_{l-1}\frac{(-1)^l\binom{n}{l}l!}{(l+1)\binom{2n}{l+1}} = 0$ where $c_r = \frac{1}{r!}\sum_{s=0}^{r}(-1)^s\binom{r}{s}(r-s+1)^{d-1}$. Similarly, we show when $d > 0$ is even that $\sum_{r=0}^{d} a_r \frac{r!\binom{n}{r+1}}{\binom{2n}{r+1}} = 0$ where $a_r = \frac{(-1)^{d+r}}{r!}\sum_{s=0}^{r}(-1)^s\binom{r}{s}(r-s+1)^d$.

## Introduction

Identities involving binomial coefficients usually arise in situations where counting is carried out in two different ways. For instance, some identities obtained by William Horrace [1] using probability theory turn out to be special cases of the Chu-Vandermonde identities. Here, we obtain some generalizations of the identities observed by Horrace and give different types of proofs; these, in turn, give rise to some other new identities. In particular, we evaluate sums of the form $\sum_{j=0}^{m}(-1)^j j^d \frac{\binom{m}{j}}{\binom{n+j}{j}}$ and deduce that they vanish when $d$ is even and $m = n > d/2$. It is well-known [2] that sums involving binomial coefficients can usually be expressed in terms of the hypergeometric functions but it is more interesting if such a function can be evaluated explicitly at a given argument. Identities such as the ones we prove could perhaps be of some interest due to the explicit evaluation possible. The papers [3], [4] are among many which deal with identities for sums where the binomial coefficients occur in the denominator and we use similar methods here.

## 1. Horrace's identities - other proofs and generalizations

We start with the identities in Horrace's paper which he deduced using probability theory.

2000 *Mathematics Subject Classification.* 11B65, 05A19.
*Key words and phrases.* Binomial coefficients, difference operators.

**Lemma 1.1.** *For $m \geq 1, n \geq 0$; we have*
$\sum_{j=0}^{m}(-1)^j \frac{\binom{m}{j}}{\binom{n+j}{j}} = \frac{n}{n+m}$; *and*
$\sum_{j=1}^{m}(-1)^{j-1} j \frac{\binom{m}{j}}{\binom{n+j}{j}} = \frac{mn}{(n+m)(n+m-1)}$.

The lemma can be easily deduced by induction or using the method of [3].

**Remark 1.2.** *We give another expression for the left hand sides of these identities. Recall the forward difference operator $\Delta$ defined on a function $f$ by $(\Delta f)(x) = f(x+1) - f(x)$. As usual, one defines $\Delta^{k+1} f = \Delta(\Delta^k f)$ etc. It is easily seen by induction on $m$ that*

$$(\Delta^m f)(x) = \sum_{r=0}^{m}(-1)^r \binom{m}{r} f(x+m-r).$$

*Now, the left hand side of the first identity of Lemma 1.1 is*

$$\sum_{j=0}^{m}(-1)^j \frac{\binom{m}{j}}{\binom{n+j}{j}}$$

*which is $(\Delta^m g)(0)$ where*

$$g(x) = \frac{n!}{(m+1-x)(m+2-x)\cdots(m+n-x)}.$$

*Now, one can express $g(x)$ as a partial fraction $\sum_{i=1}^{n} \frac{a_i}{m+i-x}$. Also, each $a_j$ can be found by multiplying both sides by the product $(m+1-x)(m+2-x)\cdots(m+n-x)$ and evaluating at $x = m+j$; we have $a_j \prod_{i \neq j}(i-j) = n!$ for each $j \leq n$. Now, we compute $(\Delta^m g)(x) = \sum_{i=1}^{n}(\Delta^m g_i)(x)$ where $g_i(x) = \frac{a_i}{m+i-x}$. Computing, we see that*

$$(\Delta^m g)(0) = n! \sum_{i=1}^{n} \sum_{r=0}^{m} \prod_{j \leq n; j \neq i} \frac{1}{j-i} \frac{(-1)^r \binom{m}{r}}{r+i}$$

*which easily simplifies to*

$$(\Delta^m g)(0) = n \sum_{i=1}^{n} \sum_{r=0}^{m} \frac{(-1)^{r+i-1} \binom{n-1}{i-1} \binom{m}{r}}{r+i}.$$

*It is worth noting that although the left hand sides of these identities can be thought of as the action by the $(m+n)$-th difference operator, it does not give anything new and merely reproduces the left hand sides again. Now, by Lemma 1.1, we get $(\Delta^m g)(0) = \frac{n}{m+n}$ and we have the following corollary.*

**Corollary 1.3.**

$$\sum_{i=1}^{n} \sum_{r=0}^{m} \frac{(-1)^{r+i-1} \binom{n-1}{i-1} \binom{m}{r}}{r+i} = \frac{1}{m+n}.$$

Doing the same process with the second identity in Lemma 1.1, we have :

$$\sum_{i=1}^{n} \sum_{r=0}^{m} \frac{(-1)^{r+i-1} i \binom{n-1}{i-1} \binom{m}{r}}{r+i} = \frac{mn}{(m+n)(m+n-1)}.$$

As a matter of fact, the identity of Corollary 1.3 can be proved in a much more general form by another manner as follows.

**Lemma 1.4.**

$$\sum_{i_1,\cdots,i_k} \frac{(-1)^{i_1+\cdots+i_k}\binom{n_1}{i_1}\cdots\binom{n_k}{i_k}}{i_1+i_2+\cdots+i_k+1} = \frac{1}{n_1+n_2+\cdots+n_k+1}.$$

*Proof.* Writing $(1-t)^{n_1+\cdots+n_k} = (1-t)^{n_1}\cdots(1-t)^{n_k}$ and integrating both sides from 0 to 1 after expanding the right side binomially, we have the identity asserted. □

## 2. A vanishing theorem

A natural generalization of Lemma 1.1 would be to consider the sums of the form $\sum_{j=1}^{m}(-1)^{j-1}j^d\frac{\binom{m}{j}}{\binom{n+j}{j}}$ for various $d>1$. We have the following result which first shows how the roles of $m$ and $n$ are interchanged and then implies a vanishing result when $m=n$. In between, we also adopt a method used in [3] for evaluating sums where binomial coefficients appear in the denominator.

**Theorem 2.1.** *Let $\theta$ be a polynomial and let $m+n>deg(\theta)$. Then, the sum*

$$P_{m,n}(\theta) := \sum_{j=0}^{m}(-1)^j\frac{\theta(j)\binom{m}{j}}{\binom{n+j}{j}}$$

*satisfies*

$$\binom{m+n}{n}P_{m,n}(\theta) = \sum_{j=0}^{m}(-1)^j\theta(j)\binom{m+n}{m-j} = \sum_{i=0}^{n}(-1)^{i-1}\theta(-i)\binom{m+n}{n-i} + \theta(0).$$

*Further, if $\theta$ is an even function and if $m=n$, then $P_{m,n}(\theta)=\theta(0)/2$.*
*In particular, for $n>2k\geq 0$, $\sum_{j=0}^{n}(-1)^j\frac{j^{2k}\binom{n}{j}}{\binom{n+j}{j}}=0$ if $k>0$ and $=\frac{1}{2}$ if $k=0$.*

*Proof.* Now $P_{m,n}(\theta)=\sum_{j=0}^{m}(-1)^j\frac{\theta(j)\binom{m}{j}}{\binom{n+j}{j}} = (\Delta^m\Phi)(0)$ where

$$\Phi(x) = \frac{\theta(m-x)n!}{(m+1-x)(m+2-x)\cdots(m+n-x)}.$$

Now, we divide $\theta(x)$ by the polynomial $\prod_{i=1}^{n}(x+i)$ and write

$$\theta(x) = u(x)\prod_{i=1}^{n}(x+i) + v(x)$$

and $\deg(v)<n$.
Note that if $u$ is not the zero polynomial, we have $\deg(u)<m$ by hypothesis. In particular, $(\Delta^m u)$ is the zero polynomial.
Now, we expand in partial fractions as in Remark 1.2 :

$$\frac{v(m-x)n!}{(m+1-x)(m+2-x)\cdots(m+n-x)} = \sum_{r=1}^{n}\frac{c_r}{m+r-x}.$$

The coefficients $c_r$ are obtained easily as before; we get

$$c_i = \frac{v(-i)n!}{(-1)^{i-1}(i-1)!(n-i)!}.$$

Note that $v(-i) = \theta(-i)$ for all $i = 1, \cdots, n$. Thus,

$$P_{m,n}(\theta) = (\Delta^m \Phi)(0) = (\Delta^m w)(0)$$

where $w(x) = \frac{v(m-x)n!}{(m+1-x)(m+2-x)\cdots(m+n-x)} = \sum_{r=1}^{n} \frac{c_r}{m+r-x}$.

For $i = 1, \cdots, n$ we evaluate $(\Delta^m \frac{1}{m+i-x})(0) = \sum_{r=0}^{m} (-1)^r \frac{\binom{m}{r}}{r+i}$ as in [3] as follows.

$$\sum_{r=0}^{m} (-1)^r \frac{\binom{m}{r}}{r+i} = \sum_{r=0}^{m} (-1)^r \binom{m}{r} \int_0^1 (1-t)^{r+i-1} dt$$

$$= \int_0^1 t^{i-1}(1-t)^m dt = \beta(i, m+1) = \frac{(i-1)!m!}{(m+i)!}.$$

Therefore,

$$P_{m,n}(\theta) = \sum_{i=1}^{n} c_i \frac{(i-1)!m!}{(m+i)!} = \sum_{i=1}^{n} \frac{v(-i)n!}{(-1)^{i-1}(i-1)!(n-i)!} \frac{(i-1)!m!}{(m+i)!}$$

$$= \frac{1}{\binom{m+n}{n}} \sum_{i=1}^{n} (-1)^{i-1} v(-i) \binom{n+m}{n-i} = \frac{1}{\binom{m+n}{n}} \sum_{i=1}^{n} (-1)^{i-1} \theta(-i) \binom{n+m}{n-i}$$

because $v(-i) = \theta(-i)$ for all $i = 1, \cdots, n$. which is Adding and subtracting the term corresponding to $i = 0$, we get the expression asserted in the theorem, viz.,

$$P_{m,n}(\theta) = \frac{1}{\binom{m+n}{n}} \sum_{i=0}^{n} (-1)^{i-1} \theta(-i) \binom{m+n}{n-i} + \theta(0).$$

Adding this expression and the expression $\frac{1}{\binom{m+n}{n}} \sum_{j=0}^{m} (-1)^j \theta(j) \binom{m+n}{m-j}$, it is evident that when $m = n$ and $\theta(i) = \theta(-i)$ for all $i$, the sum is $\theta(0)$. Taking $\theta(x) = x^{2k}$, the last statement follows. The proof is complete.

□

**Remark 2.2.** *It is important to note that although $P_{m,n}(\theta)$ can be re-expressed as a multiple of $\sum_{j=0}^{m} (-1)^j \theta(j) \binom{m+n}{m-j}$, and hence, can be viewed as the effect of the $(m+n)$-th order difference operator on a certain function, this does not give any new information but merely reproduces the expression. Thus, it is indeed worthwhile to view $P_{m,n}(\theta)$ rather as the effect of the $m$-th order difference operator on a certain function.*

We proved the vanishing of $P_{m,n}(\theta)$ when $m = n$ and $\theta(j) = j^{2k}$, but did not evaluate it for general $m, n$. As we will see, a natural method to evaluate it is to evaluate and use the following sums:

**Proposition 2.3.** *For $m, n \geq 1, d \geq 0$ we have*

$$T_d := \sum_{j=0}^{m} (-1)^j (j+1)(j+2)\cdots(j+d) \frac{\binom{m}{j}}{\binom{n+j}{j}} = \frac{d! \binom{n}{d+1}}{\binom{m+n}{d+1}}.$$

*We also have*

$$S_d := \sum_{j=0}^{m} (-1)^j j(j-1)\cdots(j-d+1) \frac{\binom{m}{j}}{\binom{n+j}{j}} = \frac{(-1)^d n \binom{m}{d} d!}{(d+1)\binom{m+n}{d+1}}.$$

*As usual, the convention is that the empty product (when $d = 0$ here) is understood to be equal to 1.*

*Proof.* As we did in the proof of Theorem 2.1, we express the denominator $\binom{n+j}{j}$ in terms of the beta function and evaluate the sums. We omit details.

□

**Corollary 2.4.**

$$\sum_{j=0}^{m}(-1)^j j^d \frac{\binom{m}{j}}{\binom{n+j}{j}} = \sum_{l=1}^{d} c_{l-1}\frac{(-1)^l n\binom{m}{l} l!}{(l+1)\binom{m+n}{l+1}}$$

*where* $c_r = \frac{1}{r!}\sum_{s=0}^{r}(-1)^s\binom{r}{s}(r-s+1)^{d-1}$ *for all* $0 \le r < d-1$.
*In particular, if* $d > 0$ *is even and* $< 2n$, *then*

$$\sum_{l=1}^{d} c_{l-1}\frac{(-1)^l\binom{n}{l} l!}{(l+1)\binom{2n}{l+1}} = 0$$

*with* $c_l$*'s as above.*
*Similarly, we have*

$$\sum_{j=0}^{m}(-1)^j j^d \frac{\binom{m}{j}}{\binom{n+j}{j}} = \sum_{r=1}^{d} a_r \frac{r!\binom{n}{r+1}}{\binom{m+n}{r+1}}$$

*where* $a_r = \frac{(-1)^{d+r}}{r!}\sum_{s=0}^{r}(-1)^s\binom{r}{s}(r-s+1)^d$ *for all* $0 \le r < d$.
*In particular, if* $d > 0$ *is even and* $< 2n$, *then*

$$\sum_{r=1}^{d} a_r \frac{r!\binom{n}{r+1}}{\binom{2n}{r+1}} = 0$$

*with* $a_r$*'s as above.*

*Proof.* Now $\sum_{j=0}^{m}(-1)^j j^d \frac{\binom{m}{j}}{\binom{n+j}{j}} = \sum_{l=1}^{d} c_{l-1}S_l$ where $S_l$ is as above and where $c_l$' s are defined by $j^d = \prod_{k=0}^{d-1} c_k j(j-1)\cdots(j-k)$.
If we write

$$x^d = \prod_{k=0}^{d-1} c_k x(x-1)\cdots(x-k)$$

then it is easy to determine $c_k$'s recursively and we find that for $0 \le r < d-1$, we have

$$r!c_r = \sum_{s=0}^{r}(-1)^s\binom{r}{s}(r-s+1)^{d-1}.$$

Thus, Proposition 2.3 implies the first assertion.
Similarly, if we express $x^d = \sum_{r=0}^{d} a_r(x+1)(x+2)\cdots(x+r)$, then we have $\sum_{j=0}^{m}(-1)^j j^d \frac{\binom{m}{j}}{\binom{n+j}{j}} = \sum_{r=1}^{d} a_r T_r$. We may compute the $a_r$'s recursively and find that for $0 \le r < d$, we get

$$(-1)^{d+r} r! a_r = \sum_{s=0}^{r}(-1)^s\binom{r}{s}(r-s+1)^d.$$

□

**Acknowledgements:** We are indebted to William Horrace for communicating to us his identities which use probability theory and for pointing out (thanks to George Andrews) that they are special cases of the Chu-Vandermonde identities. We are

also grateful to the referee who pointed out that some similar results due to A.Sofo appear in the paper titled 'Sums of binomial coefficients in integral form' published in the Proceedings of the 12th International Conference on Fibonacci numbers and their application in July 2006 - San Francisco, using different methods.

## References

[1] W.C.Horrace - *On the difference of maxima from independent uniform samples and a hypergeometric identity*, Preprint.
[2] M.Petkovsek, H.S.Wilf and D.Zeilberger - *"A=B"*, A.K.Peters 1996.
[3] B.Sury - *Sum of the reciprocals of the binomial coefficients*, European J. Combin. 14 (1993) 351-353.
[4] B.Sury, T.Wang and F-Z.Zhao - *Identities involving reciprocals of binomial coefficients, Journal of Integer Sequences, Vol.7 (2004), Article 04.2.8*

Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560059, India.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 33–43
ISSN 1930-1235: (electronic version)

# THE NUMBER AND SUM OF NEAR $m-$EXTREMES

ENKELEJD HASHORVA AND JÜRG HÜSLER
ALLIANZ SUISSE & UNIVERSITY OF BERN

ABSTRACT. Let $\{X_n, n \geq 1\}$ be a sequence of independent random variables with common continuous distribution function $F$. In this article we discuss distributional and asymptotical properties of the point process $N_{n,m}(\cdot) = \sum_{i=1}^{n} \mathbf{1}(X_{n-m+1:n} - X_i \in \cdot)$ driven by the $m$th upper order statistic $X_{n-m+1:n}$. Further we derive some limiting results for related sums, which are of some interest in insurance applications.

## 1. INTRODUCTION

Let $\{X_n, n \geq 1\}$ be a sequence of independent random variables with common continuous distribution function $F$. By $X_{1:n} < \cdots < X_{n:n}$ we denote the order statistics of $X_1, \ldots, X_n$. Define the number of near $m-$extremes $K_n(a, m), a > 0, m \in \mathbb{N}$ by

$$K_n(a, m) := \sum_{i=1}^{n} \mathbf{1}(X_{n-m+1:n} - a < X_i \leq X_{n-m+1:n}),$$

with $\mathbf{1}(\cdot)$ the indicator function. More generally, let

$$N_{n,m}(\cdot) := \sum_{i=1}^{n} \mathbf{1}(X_{n-m+1:n} - X_i \in \cdot) \tag{1}$$

denote the related point process defined on $[0, \infty)$ driven by the $m$th upper order statistics. The marginal random variable $N_{n,m}(T)$ with $T$ a Borel set of $[0, \infty)$ is in other words the number of $m-$extremes falling into the Borel set $T$. Setting $T = [0, a)$ we have $N_{n,m}(T) = K_n(a, m)$.

The number of near $m-$extremes is dealt with in several papers. It was introduced and carefully examined by Pakes and Steutel (1997) and Khmaladze et al. (1997) (considering $m = 1$ only). Hashorva (2003, 2004) showed that studying $K_n(a, m)$ for dependent samples is of some relevance for insurance applications. Estimation of the tail coefficient based on the number of near $m-$extremes is further discussed in Hashorva and Hüsler (2004). Recent papers on the topic are Balakrishnan and Stepanov (2004, 2005), Dembinska et al. (2007), where new ideas and results in connection with near extremes have been presented.

Point process approach was considered by Hashorva and Hüsler (2000) deriving both distributional and asymptotical results for $N_{n,1}(\cdot)$.

Received by the editors November 11, 2007 and, in revised form, February 27, 2008.
2000 *Mathematics Subject Classification.* Primary 60F15; Secondary 60G70.
*Key words and phrases.* The number of near $m-$extremes, upper order statistics; point processes; weak and almost sure limit results.

The main topic of this paper is the asymptotic behaviour of the near $m-$extreme point process $N_{n,m}(\cdot)$. Special attention is given to $K_n(a,m)$; we show weak convergence of $K_n(a_n,m), n\geq 1$ without supposing the iid assumption. Further we discuss some asymptotic properties of sums of the near $m-$extremes (dealt with initially in Pakes (2000)) defined by

$$S_n(a,m) \quad := \quad \sum_{i=1}^{n} X_i \mathbf{1}\Big(X_i \in (X_{n-m+1:n}-a, X_{n-m+1:n}]\Big). \tag{2}$$

It is well-known that asymptotic properties of the $m$th upper order statistic are in some sense invariant to $m$. For example $X_{n-m+1:n}$ converges almost surely for any $m>1$ to the upper endpoint of the distribution function $F$. We show in this paper that similar invariance properties are demonstrated by the number of near $m-$extremes.

Brief outline of the paper: We continue next with some preliminary results followed by Section 3 where several asymptotical results for the iid setup are presented. In Section 4 we show that convergence in distribution for $K_n(a_n,m)$ with $a_n\to a\geq 0$ and $m\in\mathbb{N}$ holds under certain dependence assumptions on the random sequence $X_i, i\geq 1$.

## 2. Preliminaries

Write in the following $l_F, u_F$ for the lower and the upper endpoint of the distribution function $F$, respectively. We state now the following obvious lemma:

**Lemma 1.** *Let $\{X_n, n\geq 1\}$ be independent random variables with common continuous distribution function $F$. The random variable $N_{n,m}(T)-1(0\in T)$ with $T$ some Borel set of $[0,\infty)$ and $n>m\geq 1$ has a mixed binomial distribution $B(n-m,p(T,x))$ with mixing random variable $X_{n-m+1:n}$ where*

$$p(T,x) := \boldsymbol{P}\{x-W\in T | W\leq x\}, \quad l_F<x<u_F,$$

*with $W$ a random variable with distribution function $F$.*

It is also easy to see that the joint conditional distribution of

$$N_{n,m}(T_1)-1(0\in T_1),\ldots, N_{n,m}(T_k)-1(0\in T_k), \quad k\geq 2,$$

with $T_1,\ldots,T_k$ Borel sets of $[0,\infty)$ given the $m$th upper order statistic is multinomial. This fact is crucial when dealing with both distributional and asymptotical propertied of the point process $N_{n,m}(\cdot)$.

The law of the point process $N_{n,m}(\cdot)$ can be described via Markov kernels (see Reiss (1993) for basic properties of Markov kernels). We have

$$L(N_{n,m}(\cdot)-\mathbf{1}(0\in\cdot)) \quad = \quad \int_{\mathbb{R}} G_n(\cdot,x)\, dL(X_{n-m+1:n})(x), \tag{3}$$

where $G_{n,m}(\cdot,x)\stackrel{d}{=} B(n-m,p(\cdot,x))$, $L(\cdot)$ denotes the law of the corresponding random element, and $\stackrel{d}{=}$ stands for equality of distribution functions. Referring to Theorem 1.5.1 of Reiss (1989) the $m$th upper order statistic $X_{n-m+1:n}$ possess the $F$-density

$$\frac{n!F^{n-m}(x)(1-F(x))^{m-1}}{(n-m)!(m-1)!}. \tag{4}$$

Application of Fubini's Theorem for Markov kernels (see Reiss (1993)) yields further

$$\begin{aligned}\boldsymbol{E}\{N_{n,m}(T)\} &= \mathbf{1}(0\in T)+\int_{\mathbb{R}}\left(\int_{\mathbb{R}} y\, dL(B(n-m,p(T,x)))(y)\right) dL(X_{n-m+1:n})(x)\\ &= \mathbf{1}(0\in T)+(n-m)\boldsymbol{E}\{p(T,X_{n-m+1:n})\}\\ &= \mathbf{1}(0\in T)+\frac{n!}{(n-m-1)!(m-1)!}\\ &\quad\times\int_{\mathbb{R}}\boldsymbol{P}\{x-X_1\in T|X_1\le x\}F^{n-m}(x)(1-F(x))^{m-1}\,dF(x). \qquad (5)\end{aligned}$$

Substituting we have

$$\begin{aligned}\boldsymbol{E}\{K_n(a,m)\} &= 1+\frac{n!}{(n-m-1)!(m-1)!}\\ &\quad\times\int_{\mathbb{R}}[F(x)-F(x-a)]F^{n-m-1}(x)(1-F(x))^{m-1}\,dF(x) \qquad (6)\end{aligned}$$

for all $n>m\ge 1$.

Alternatively, moments of the random variable $N_{n,m}(T), T\subset[0,\infty)$ can be easily derived from the expression of probability generating function (p.g.f) given below.

**Lemma 2.** *Under the assumptions and the notation of Lemma 1 we have for any integer $m,n>m$ and $s\in(0,1)$*

$$\boldsymbol{E}\{s^{N_{n,m}(T)-\mathbf{1}(0\in T)}\}=\int_{\mathbb{R}}[1-(1-s)p(T,x)]^{n-m}\,dL(X_{n-m+1:n})(x), \qquad (7)$$

*where the distribution of the mth largest order statistic has $F$-density as in* (4).

Certain assumptions on the tail asymptotic behaviour of the distribution function $F$ allow us to derive several limiting results. If $F$ has upper endpoint $u_F=\infty$, and the following limit

$$\lim_{x\to\infty}\frac{1-F(x+a)}{1-F(x)} = l(a)\in[0,1] \qquad (8)$$

exists for any $a>0$, then as in Pakes and Steutel (1997) we call $F$ a thin-tailed, a thick-tailed, or a medium-tailed distribution whenever $l(a), a>0$, is equal to 0, 1, or is strictly between 0 and 1 for all $a>0$, respectively. Note in passing that Balakrishnan and Stepanov (2005) mention that (8) holds for all $a>0$ if and only if (iff) it holds for two distinct constants $a_1,a_2$ such that $a_1/a_2$ is an irrational number.

Examples of thin-tailed distribution functions are the half Normal law or the Weibull one with parameter $\alpha>1$. Gamma family belongs to the medium-tailed class, whereas Pareto distribution is a thick-tailed one.

The above tail asymptotic behaviour of $F$ is related to the max-domain of attraction of $F$ (see Pakes and Steutel (1997)).
It is well known (see e.g. Galambos (1987), Resnick (1987), Reiss (1989), Falk et al. (2004), Kotz and Nadarajah (2005), de Haan and Ferreira (2006)) that the distribution function $F$ belongs to the max-domain of attraction of an extreme value distribution function $H$ (write $F\in\mathrm{MDA}(H)$) if

$$\lim_{t\to\infty}\sup_{x\in\mathbb{R}}\left|F^t(q(t)x+r(t))-H(x)\right| = 0, \qquad (9)$$

with $q(t) > 0, r(t), t > 0$, two measurable functions. The univariate distribution functions $H$ is either the Gumbel distribution $\Lambda(x) = \exp(-\exp(-x)), x \in \mathbb{R}$, the Weibull distribution $\Psi_\alpha(x) = \exp(-|x|^\alpha), x < 0, \alpha > 0$, or the Fréchet distribution $\Phi_\alpha(x) = \exp(-x^{-\alpha}), x > 0, \alpha > 0$.

## 3. Asymptotics in the IID-Setup

In this section we consider the iid-setup, i.e., $X_i, i \geq 1$ are independent with common continuous distribution function $F$. Convergence in distribution for both $K_n(a,m)$ and $S_n(a,m)$ can be shown utilising the explicit expression in the right hand side of (7), provided that $F$ satisfies certain asymptotic conditions. For instance Pakes and Steutel (1997), Li (1999), Balakrishnan and Stepanov (2004, 2005) make extensive use of (8).

We split this section in three parts beginning with some equivalent conditions for (8). In the second part we discuss almost sure convergence and CLT for the sum of near $m-$extremes $S_n(a,m)$. In the last part we derive an approximation of the point process for the interesting cases that $F$ is in the Gumbel or the Weibull max-domain of attraction.

### 3.1. Condition (8).

We give next a general result which provides several equivalent conditions to (8). Previous partial results can be found in Proposition 2.5.3 in Hashorva (1999), Theorem 1.1. of Li (1999), Theorem 2.1 in Balakrishnan and Stepanov (2005).

**Proposition 3.** *Let $\{X_n, n \geq 1\}$ be a sequence of iid random variables with continuous distribution function $F$ with upper endpoint $u_F = \infty$. Then the following four statements are equivalent:*
*i) For any $a > 0$ the limit in (8) exists and $l(a) \in (0,1]$.*
*ii) For any $a > 0$ and any integer $m$, the discrete random variable $K_n(a,m)$ converges in distribution to some random variable $K^*_{a,m}$, where $K^*_{a,m} - 1$ has a negative binomial distribution with p.g.f*

$$\boldsymbol{E}\{s^{K^*_{a,m}-1}\} = \left(\frac{l(a)}{1-s(1-l(a))}\right)^m, \quad l(a) \in (0,1]. \tag{10}$$

*iii) For any $a > 0$ and any integer $m$*

$$\lim_{n\to\infty} \boldsymbol{E}\{K_n(a,m)\} = m[1-l(a)]/l(a) + 1, \quad l(a) \in (0,1] \tag{11}$$

*holds.*
*iv) For any $a > 0$ we have*

$$\lim_{n\to\infty} \boldsymbol{P}\{K_n(a,1) = 1\} = l(a) \in (0,1]. \tag{12}$$

*Moreover, for any $a > 0$ and any integer $m$ we have $K_n(a,m) \xrightarrow{p} \infty$ iff $l(a) = 0$.*

*Proof.* First note that

$$\boldsymbol{P}\{K_n(a,1) = 1\} = n \int_R F^{n-1}(x-a)\, dF(x), \quad \forall a > 0, n > 1.$$

Transforming the expression of the expectation in (5) we obtain

$$\begin{aligned} \boldsymbol{E}\{K_n(a,m)\}-1 &= (n-m)\boldsymbol{E}\{[1-F(X_{n-m+1:n}-a)/F(X_{n-m+1:n})]\} \\ &= n-m-(n-m)\boldsymbol{E}\{F(X_{n-m+1:n}-a)/F(X_{n-m+1:n})\} \\ &= n\boldsymbol{E}\{[1-F(X_{n-m:n-1}-a)]\}-m \\ &= n\boldsymbol{E}\{F_{n-m:n-1}(X_1+a)\}-m. \end{aligned} \tag{13}$$

Statement $i)$ implies that $F$ is in the Gumbel max-domain of attraction. Furthermore, the scaling function $q(t)$ can be choose to be constant in $t$. The proof follows now using (7), the Gumbel max-domain of attraction of $F$, and applying Lemma 4 below with the function $\chi(\cdot)$ constant and $\rho=1$. □

The following lemma follows immediately form Lemma 2.5.1 in Hashorva (1999) which is stated for multivariate distribution functions.

**Lemma 4.** *Let $F,G$ be two continuous univariate distribution functions with upper endpoint $\infty$, and let $\rho\geq 1, C\in[0,\infty]$ be two given constants. If $\chi:[0,\infty)\to[0,\infty)$ is a measurable function such that $\lim_{x\to 0}\chi(tx)/\chi(x)=1, \forall t>0$, then the following two statements are equivalent:*
*i) As $n\to\infty$ we have for any $c\in[0,\infty)$*

$$n\int_{\mathbb{R}} G^{n-c}(x)\,dF(x) = (1+o(1))\frac{C}{n^{\rho-1}}\chi(1/n). \tag{14}$$

*ii) As $x\to\infty$*

$$\frac{1-F(x)}{(1-G(x))^{\rho}\chi(1-G(x))} = (1+o(1))\frac{C}{\Gamma(\rho+1)}. \tag{15}$$

**Remark 1.** a) Imposing an additional technical condition on the distribution function $F$ Balakrishnan and Stepanov (2005) show in Theorem 2.2 therein that the almost sure convergence $K_n(a,m)\to 1$ is equivalent to $l(a)=1$ for all $a>0$. Note that if $l(a)=1$, then statement ii) in Proposition 3 means convergence in probability to 1.
b) Lemma 4 is motivated by Lemma 1.3 in Maller and Resnick (1984).

Our next result concerns the asymptotic approximation of the ratio of the number and sum of near $m-$extremes. It subsumes Theorem 7.1 in Pakes (2000).

**Proposition 5.** *Under the assumptions and the notation of Proposition 3*

$$S_n(a,m)/X_{n-m+1:n} \xrightarrow{d} 1+K^*_{a,m}, \quad n\to\infty \tag{16}$$

*holds for any $a>0$ and any integer $m$, iff either of the statements $i),ii),iii),iv)$ in Proposition 3 hold.*
*Furthermore, for any $a>0$ and any integer $m$ the convergence in probability*

$$S_n(a,m)/X_{n-m+1:n} \xrightarrow{p} \infty, \quad n\to\infty \tag{17}$$

*is valid iff $l(a)=0$, and*

$$S_n(a,m)/X_{n-m+1:n} \xrightarrow{p} 1, \quad n\to\infty \tag{18}$$

*holds iff $l(a)=1$.*

*Proof.* For any positive $a$ and any integer $m$

$$[X_{n-m+1:n} - a]K_n(a,m) \leq S_n(a,m) \leq X_{n-m+1:n}K_n(a,m)$$

holds almost surely. Furthermore the almost sure convergence

$$X_{n-m+1:n} \to \infty, \quad n \to \infty$$

implies

$$a/X_{n-m+1:n} \to 0, \quad n \to \infty,$$

thus the proof follows using Proposition 3. □

3.2. **Almost Sure Convergence and CLT.** Hashorva (1999) shows the convergence in probability of

$$K_n(a,m)/n \quad \stackrel{p}{\to} \quad 1 - F(u_F - a), \quad n \to \infty,$$

provided that the upper endpoint $u_F$ of $F$ is finite. Since

$$\lim_{n\to\infty} \boldsymbol{E}\{K_n(a,m)/n\} \quad = \quad 1 - F(u_F - a)$$

the convergence holds also in the $r$th ($r > 0$) mean. Almost sure convergence and CLT for $K_n(a,m)$ are stated in Hashorva and Hüsler (2004).
Next, we discuss some asymptotic properties for the sum of near $m-$extremes.

**Proposition 6.** *Let $\{X_n, n \geq 1\}$ be a positive sequence of independent random variables with continuous distribution function $F$. If both the lower and the upper endpoint $l_F, u_F$ of the distribution function $F$ are finite, then for any $a > 0$ and any integer $m$ we have the almost sure convergence*

$$S(a,m)/n \quad \stackrel{a.s.}{\to} \quad \boldsymbol{E}\{X_1\mathbf{1}(X_1 > u_F - a)\}, \quad n \to \infty. \tag{19}$$

*Proof.* Since for any $\varepsilon > 0$

$$X_i\mathbf{1}(u_F - X_{n-m+1:n} > \varepsilon) \leq u_F\mathbf{1}(u_F - X_{n-m+1:n} > \varepsilon) \to 0, \quad n \to \infty$$

almost surely, we have for all large $n$

$$S(a,m)/n \quad \leq \quad \sum_{i=1}^{n} X_i\mathbf{1}(X_i > u_F - a - \varepsilon)/n + u_F\mathbf{1}(u_F - X_{n-m+1:n} > \varepsilon)$$

and

$$S(a,m)/n \quad \geq \quad \sum_{i=1}^{n} X_i\mathbf{1}(X_i > u_F - a)/n - u_F(m-1)/n,$$

hence the proof follows by the Strong Law of Large Numbers. □

We show next the CLT for the sum of near $m-$extremes.

**Proposition 7.** *Let $\{X_n, n \geq 1\}$ be as in Proposition 6 and suppose further that the lower endpoint of $F$ is non-negative and the upper endpoint $u_F$ is finite. Assume that there exists a positive sequence $\{c_n, n \geq 1\}$ such that*

$$\lim_{n\to\infty} n \ln F(u_F - c_n) \quad = \quad -\infty, \tag{20}$$

*and for some positive constant $a$ we have*

$$\lim_{n\to\infty} \sqrt{n}[F(u_F - a) - F(u_F - a - c_n)] \quad = \quad 0, \tag{21}$$

*with* $F(u_F - a) \in (0,1)$. *If further* $\sigma_a^2 := Var(X_1 \mathbf{1}(u_F - a \le X_1 \le u_F)) \in (0,\infty)$, *then the convergence in distribution*

$$[S_n(a,m) - n\boldsymbol{E}\{X_1 \mathbf{1}(X_1 > u_F - a)\}]/\sqrt{n} \quad \stackrel{d}{\to} \quad W, \quad n \to \infty \tag{22}$$

*holds with* $W$ *a mean zero Gaussian random variable with variance* $\sigma_a^2$.

*Proof.* For any $m \ge 1$, condition (20) implies $\sqrt{n}\mathbf{1}(X_{n-m+1:n} < u_F - c_n) = o_p(1)$ as $n \to \infty$. Consequently (recall $u_F < \infty$)

$$S_n(a,m)/\sqrt{n} \le \sum_{i=1}^{n} X_i \mathbf{1}(u_F - X_i < a + c_n)/\sqrt{n} + o_p(1)$$

and

$$S_n(a,m)/\sqrt{n} \ge \sum_{i=1}^{n} X_i \mathbf{1}(u_F - X_i < a)/\sqrt{n} - u_F(m-1)/\sqrt{n}.$$

By (21)

$$\sum_{i=1}^{n} X_i \mathbf{1}(a \le u_F - X_i < a + c_n)/\sqrt{n} = o_p(1), \quad \text{as } n \to \infty,$$

thus the proof follows easily by applying the CLT for the random sequence $X_i \mathbf{1}(u_F - X_i < a), i \ge 1$ (see e.g. Kallenberg (1997)). □

3.3. **Asymptotics for the point process.** Finally we consider the asymptotic behaviour of the point process $N_{n,m}(\cdot)$. Since this point process is driven by the $m$th upper extreme order statistics, in order to deal with its asymptotic behaviour we consider the case when $F$ is in a max-domain of attraction of a univariate distribution function $H$, assuming (9) holds with norming functions $q(t), r(t)$.

We show first weak convergence of the scaled point process

$$N_{n,m}^*(\cdot) := \sum_{i=1}^{n} \mathbf{1}((X_{n-m+1:n} - X_i)/q_n \in \cdot),$$

with $q_n := q(n)$ the norming constant from (9). The asymptotics for $m = 1$ is dealt with in Hashorva (1999). As in that case, utilising the same arguments (see also Theorem 1.2 in Hashorva and Hüsler (2000)) the scaled point process $N_{n,m}^*$ can be approximated ($n \to \infty$) by a Cox process plus a point at 0. We have the following result:

**Proposition 8.** *Let* $\{X_n, n \ge 1\}$ *be a sequence of iid random variables with continuous distribution function* $F$ *satisfying condition* (9). *If the univariate distribution function* $H$ *is standard Gumbel or Weibull, then for all* $m \ge 1$

$$N_{n,m}^*(\cdot) \quad \stackrel{d}{\to} \quad N_m(\cdot) + \mathbf{1}(0 \in \cdot), \quad n \to \infty, \tag{23}$$

*where* $N_m(\cdot)$ *is a Cox process with stochastic intensity*

$$\nu([a,b), X_*^{(m)}) = \ln\left(\frac{H(X_*^{(m)} - a)}{H(X_*^{(m)} - b)}\right)$$

*for $0 < a < b < \infty$. The mixing random variable $X_*^{(m)}$ has continuous distribution function $H_m$ given by*

$$H_m(x) \quad = \quad H(x) \sum_{r=0}^{m-1} \frac{(-\ln H(x))^m}{m!}, \quad \forall x \in \mathbb{R}.$$

The following corollary is immediate:

**Corollary 9.** *Let $\{X_n, n \geq 1\}$ be a sequence of iid random variables with continuous distribution function $F$ such that for all $a > 0$ condition (8) holds with $l(a) \in (0,1)$. Then (9) holds with $q(t) = q \in (0,\infty), r(t), t > 0$ and further for all $m \geq 1$*

$$N_{n,m}(\cdot) \quad \stackrel{d}{\to} \quad N_m(\cdot) + \mathbf{1}(0 \in \cdot), \quad n \to \infty, \tag{24}$$

*where $N_m(\cdot)$ is a Cox process with stochastic intensity*

$$\nu([a,b), X_*^{(m)}) = \ln\left(\frac{H(X_*^{(m)} - a/c)}{H(X_*^{(m)} - b/c)}\right), \quad 0 < a < b < \infty$$

*and the mixing random variable $X_*^{(m)}$ as in Proposition 8.*

Note in passing that weak convergence of the unscaled point process $N_{n,m}(\cdot)$ follows by the above result, since the scaling function is constant in Corollary 9.

## 4. Approximations in the case of dependence

Since we want to drop the iid assumption (which implies (7)), we follow here a different approach which we motivate below. If the distribution function $F$ satisfies (9) with functions $q(t) > 0, r(t), t \in \mathbb{R}$, we have the joint convergence in distributions ($n \to \infty$)

$$\Big((X_{n:n} - r_n)/q_n, \ldots, (X_{n-l+1:n} - r_n)/q_n\Big) \quad \stackrel{d}{\to} \quad (X_*^{(1)}, \ldots, X_*^{(l)}), \tag{25}$$

where $q_n = q(n) > 0, r_n := r(n), n \geq 1$, and the random vector $(X_*^{(1)}, \ldots, X_*^{(l)})$ has the distribution function $\mathbf{H}_l$ with density function $\mathbf{h}_l$ given by

$$\mathbf{h}_l(\mathbf{x}) \quad = \quad H(x_l) \prod_{i=1}^{l} \frac{H'(x_i)}{H(x_i)}, \quad \text{with } x_l < \cdots < x_2 < x_1 \tag{26}$$

and $x_1, x_l$ are such that $H(x_1), H(x_l) \in (0,1)$ (see e.g. Reiss (1989)). Hence for $0 < k \leq n - m - 1$, $a_n = c_a q_n (1 + o(1)), n \geq 1$, with $c_a > 0$ some constant, we have

$$\begin{aligned}
&\boldsymbol{P}\{K_n(a_n, m) > k\} \\
&\quad = \quad \boldsymbol{P}\{X_{n-m+1:n} - X_{n-m+1-k:n} < a_n\} \\
&\quad = \quad \boldsymbol{P}\{(X_{n-m+1:n} - r_n)/q_n - (X_{n-m+1-k:n} - r_n)/q_n < c_a(1 + o(1))\} \\
&\qquad [\text{ since the convergence holds locally uniformly, we get }] \\
&\quad \to \quad \boldsymbol{P}\{X_*^{(m)} - X_*^{(m+k)} \leq c_a\} =: 1 - \mathbf{H}^{(m)}(c_a, k), \quad n \to \infty. \qquad (27)
\end{aligned}$$

In deriving (27) we only needed (25), consequently at this point dropping the iid assumption is possible. We need however to introduce mixing type conditions $D$ and $D'$ as in Leadbetter et al. (1983), see Corollary 3.2.

The next result generalises Theorem 2 and Theorem 3 of Li and Pakes (1998b). We denote in the sequel by $\alpha_H$ the lower endpoint of the distribution function $H$.

**Proposition 10.** *Assume that condition* (25) *holds for the sequence of random variables* $\{X_n, n \geq 1\}$ *with continuous distribution function* $F$*, with constants* $q_n > 0$*,* $r_n$ *and* $\mathbf{H}_m$ *as in* (26)*. If* $a_n \sim c_a q_n$*,* $c_a > 0$*, then for* $m, l \geq 1$ *and any* $x \in \mathbb{R}$ *such that* $H(x) \in (0,1)$ *we have*

$$\begin{aligned} &\lim_{n\to\infty} \boldsymbol{P}\{K_n(a_n, m) \leq k, (X_{n-l+1:n} - r_n)/q_n \leq x\} \\ &= \boldsymbol{P}\{X_*^{(m)} - X_*^{(m+k)} > c_a, X_*^{(l)} \leq x\} \\ &=: \mathbf{H}^{(m)}(c_a, x, k, l), \quad k \in \mathbb{N}. \end{aligned} \tag{28}$$

*The random sequence* $K_n(a_n, m)$ *converges weakly to a positive non-degenerate random variable* $K^*_{a,m}$ *with distribution function* $\mathbf{H}^{(m)}(c_a, k)$ *iff* $\alpha_H = -\infty$*.*
*Further if for some* $j > m-1$

$$(X_{j-m+1:n} - r_n)/q_n \quad \xrightarrow{p} \quad x_0, \quad n \to \infty \tag{29}$$

*then we have*

$$\lim_{n\to\infty} \boldsymbol{P}\{K_n(a_n, m) > n - j\} \quad = \quad H(c_a + x_0) \sum_{r=0}^{m-1} (-\ln H(c_a + x_0))^r / r!. \tag{30}$$

*Proof.* By the assumptions we have

$$\begin{aligned} &\lim_{n\to\infty} \boldsymbol{P}\{K_n(a_n, m) \leq k, (X_{n-l+1:n} - r_n)/q_n \leq x\} \\ &= \boldsymbol{P}\{X_*^{(m)} - X_*^{(m+k)} > c_a, X_*^{(l)} \leq x\}, \end{aligned}$$

hence the weak convergence of $K_n(a_n, m)$ to a non-degenerated random variable follows if we show further that

$$\lim_{k\to\infty} \boldsymbol{P}\{X_*^{(m)} - X_*^{(m+k)} > c_a\} = 1.$$

Since $H$ is continuous, in light of (26) the limit distribution of the $i$th largest order statistic is

$$\boldsymbol{P}\{X_*^{(i)} \leq x\} = H(x) \sum_{r=0}^{i-1} \frac{(-\ln H(x))^r}{r!} =: H_i(x), \quad x : H(x) > 0,$$

hence we get for all $x \in \mathbb{R}$ such that $H(x) > 0$

$$\lim_{i\to\infty} \boldsymbol{P}\{X_*^{(i)} \leq x\} = \lim_{i\to\infty} H(x) \sum_{r=0}^{i-1} \frac{(-\ln H(x))^r}{r!} = H(x) \exp(-\ln H(x)) = 1.$$

Consequently, the monotonicity of the random sequence $\{X_*^{(i)}, i \geq 1\}$ implies

$$X_*^{(i)} \xrightarrow{a.s.} \alpha_H, \quad \text{as } i \to \infty$$

and thus

$$\lim_{k\to\infty} \boldsymbol{P}\{X_*^{(m)} - X_*^{(m+k)} > c_a\} \quad = \quad 1 - \boldsymbol{P}\{X_*^{(m)} \leq c_a + \alpha_H\} < 1$$

if and only if we have $\alpha_H > -\infty$. Finally by (29) for any $j$ fixed

$$\begin{aligned} &\boldsymbol{P}\{K_n(a_n, m) > n - j\} \\ &= \boldsymbol{P}\{X_{n-m+1:n} - X_{j-m+1:n} < a_n\} \\ &= \boldsymbol{P}\{(X_{n-m+1:n} - r_n)/q_n - (X_{j-m+1:n} - r_n)/q_n < c_a(1 + o(1))\} \\ &\to \boldsymbol{P}\{X_*^{(m)} \leq c_a + x_0\}, \quad n \to \infty, \end{aligned}$$

hence the proof is complete. □

In the above theorem we do not assume the independence of $X_i$, but only condition (25). Next, we focus attention to stationary random sequences which satisfy certain mixing type conditions. For the extreme value theory the distributional mixing conditions $D_3(\boldsymbol{u}_n)$ for the long range dependence and $D'(u_n)$ for the local dependence are sufficient to assume (see Leadbetter et al. (1983)). Here $\boldsymbol{u}_n = (u_{ni}) \in \mathbb{R}^3$ with $u_{ni} = q_n x_i + r_n$ and any $x_i \in \mathbb{R}, i \leq 3$, where $q_n$ and $r_n$ are from (5). We mention these conditions which imply (25).

**Condition** $D_3(\boldsymbol{u}_n)$: For any fixed $p, q$ and integers $1 \leq i_1 < i_2 < \cdots < i_p < j_1 < j_2 < \cdots < j_q \leq n$ with $j_1 - i_p > \ell$, and any $k_h, k'_{h'} \in \{1, 2, 3\}$ for $h \leq p, h' \leq q$, assume that

$$\Big| \boldsymbol{P}\Big\{ X_{i_h} \leq u_{n,k_h}, h \leq p, X_{j_{h'}} \leq u_{n,k'_{h'}}, h' \leq q \Big\} - \boldsymbol{P}\Big\{ X_{i_h} \leq u_{n,k_h}, h \leq p \Big\} \times \boldsymbol{P}\Big\{ X_{j_{h'}} \leq u_{n,k'_{h'}}, h' \leq q \Big\} \Big| \leq \alpha_{n,\ell},$$

where $\alpha_{n,\ell} \to 0$ for some sequence $\ell = \ell(n) = o(n)$.

**Condition** $D'(u_n)$: Assume that for $k \to \infty$

$$\limsup_{n\to\infty} \sum_{1<i\leq n/k} P\{X_1 > u_n, X_i > u_n\} \to 0.$$

**Proposition 11.** *Let $\{X_n, n \geq 1\}$ be a stationary random sequence with distribution function $F$ so that (9) holds. If also the conditions $D_3(\boldsymbol{u}_n)$ and $D'(u_n)$ are satisfied for any $x$ with $H(x) \in (0, 1)$ and $u_n = u_n(x) = q_n x + r_n$, then (28) holds.*

*Proof.* The proof follows immediately from Theorem 5.5.1 of Leadbetter et al. (1983). □

## References


[1] Balakrishnan, N., and Stepanov, A. (2004) A note on the paper of Khmaladze et al. *Statist. Probab. Lett.* **68**(4): 415-419.

[2] Balakrishnan, N., and Stepanov, A. (2005) A note on the number of observations near an order statistic. *J. Statist. Planning Infer.* **134**(1): 1–14.

[3] De Haan, L., and Ferreira, A. (2006) *Extreme Value Theorey. An Introdution.* Springer, New York.

[4] Dembinska, A. Stepanov, A., and Wesolowski, J. (2007) How many observations fall in a neighbourhood of an order statistic? *Comm. Stat. - Theory Meth.* **36**(5): 851–868.

[5] Falk, M., Hüsler, J., and Reiss, R-D. (1994) *Laws of Small Numbers: Extremes and Rare Events.* DMV Seminar Vol. **23**, Birkhäuser, Basel.

[6] Galambos, J. (1987) *The Asymptotic Theory of Extreme Order Statistics.* Second Edition, Malabar: Krieger.

[7] Hashorva, E., and Hüsler, J. (2000) On the number of near-maxima. *Supplemento ai rendiconti del Circolo Matematico di Palermo,* Serie II, **65**: 121–136.

[8] Hashorva, E. (2003) On the number of near-maximum insurance claim under dependence. *Insurance: Mathematics and Economics*, **33**(1): 37–49.

[9] Hashorva, E. (2004) Bivariate maximum insurance claim and related point processes. *Statist. Probab. Lett.*, **69**(2): 117–128.

[10] Kallenberg, O. (1997) *Foundations of modern probability.* New York, Springer.

[11] Khmaladze, E., Nadareishvili, M., and Nikabadze, A. (1997) Asymptotic behaviour of a number of repeated records. *Statist. Probab. Lett.*, **35**(1): 49–58.

[12] Kotz, S., and Nadarajah, S. (2005) *Extreme Value Distributions, Theory and Applications.* Imperial College Press, London, United Kingdom. (Second Printing).

[13] Leadbetter, M.R., Lindgren, G., and Rootzén, H. (1983) *Extremes and Related Properties of Random Sequences and Processes.* Springer-Verlag, Berlin.
[14] Li, Y. (1999) A note on the number of records near the maximum. *Statist. Probab. Lett.*, **43**(2): 153–158.
[15] Maller, R.A., and Resnick, S.I. (1984) Limiting behaviour of sums and the term of the maximum modulus. *Proc. London Math. Soc.* **49**(3): 385-422.
[16] Pakes, A. G. (2000) The number and sum of near-maxima for thin-tailed populations. *Adv. Appl. Prob.*, **32**(4): 1100–1116.
[17] Pakes, A. G. and Steutel, F. W. (1997) On the number of records near the maximum. *The Austral. J. Statist.* **39**, 172–192.
[18] Reiss, R-D. (1989) *Approximate Distributions of Order Statistics: With Applications to Non-parametric Statistics.* Springer, New York.
[19] Reiss, R-D. (1993) *A Course on Point Processes.* Springer, New York.
[20] Resnick, S.I. (1987) *Extreme Values, Regular Variation and Point Processes.* Springer, New York.

University of Bern, Institute of Mathematical Statistics and Actuarial Sciences,, Sidlerstrasse 5, CH-3012 Bern, Switzerland, and, Allianz Suisse Insurance Company, Laupenstrasse 27, CH-3001 Bern, Switzerland
*E-mail address*: enkelejd@stat.unibe.ch
*E-mail address*: enkelejd.hashorva@Allianz-Suisse.ch

University of Bern, Institute of Mathematical Statistics and Actuarial Sciences,, Sidlerstrasse 5, CH-3012 Bern, Switzerland
*E-mail address*: huesler@stat.unibe.ch

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 47–55
ISSN 1930-1235: (electronic version)

# INVERSE LIMITS OF H-CLOSED SPACES

IVAN LONČAR

Abstract. The main purpose of this paper is to study the non-emptiness and H-closeness of inverse limits of H-closed spaces.

## 1. Introduction

An *inverse system* $\mathbf{X} = \{X_a, p_{ab}, A\}$ [4, p. 135] over a directed set $A$ is a function which attaches to each $a \in A$ a space $X_a$ and to each pair $a, b \in A$ such that $a \leq b$ a mapping $p_{ab} : X_b \to X_a$ such that

$$\begin{aligned} p_{aa} &= \text{identity}, \qquad a \in A, \\ p_{ab}p_{bc} &= p_{ac}, \qquad a \leq b \leq c. \end{aligned}$$

The *inverse limit* $\lim \mathbf{X}$ of the inverse system $\mathbf{X} = \{X_a, p_{ab}, A\}$ is the set of all points $\{x_a\}$ of the Cartesian product $\Pi\{X_a : a \in A\}$ satisfying $p_{ab}(x_b) = x_a$ for every $a \leq b$.

For each inverse system $\mathbf{X} = \{X_a, p_{ab}, A\}$ we define [4, Proposition 2.5.1, p.135]

$$X_{ab} = \{\{x_a\} \in \Pi\{X_a : a \in A\} : p_{ab}(x_b) = x_a,\ a \leq b\}.$$

**Proposition 1.** [4, Proposition 2.5.1, p.135]. *The limit of an inverse system* $\mathbf{X} = \{X_a, p_{ab}, A\}$ *of a Hausdorff spaces* $X_a$ *is closed subset of the Cartesian product* $\Pi\{X_a : a \in A\}$.

For each inverse system $\mathbf{X} = \{X_a, p_{ab}, A\}$ we define [4, Theorem 3.2.13, p.188]

$$Z_a = \{\{x_a\} \in \Pi\{X_a : a \in A\} : p_{ba}(x_a) = x_b,\ b \leq a\}$$

In [4, Theorem 3.2.13, p.188] it is used that $Z_a$ is closed in $\Pi\{X_a : a \in A\}$. This is true if each $X_a$ is Hausdorff.

**Proposition 2.** *The family* $\{Z_a : a \in A\}$ *has the finite intersection property.*

*Proof.* This follows from the fact that for each pair $a, b$ there is a $c \in A$ such that $Z_c \subset Z_a \cap Z_b$ [4, The proof of Theorem 3.2.13, p. 188]. □

Let $(X, \tau)$ be an arbitrary topological space. According to [17], a point $x \in X$ is said to be a *$\theta$-cluster point* of a set $A \subset X$ if and only if $\operatorname{Cl} V \cap A \neq \emptyset$ whenever $V$ is an open neighbourhood of $x$. Let $|A|_\theta$ denote the set of all $\theta$-cluster points of $A$; $A$ is said to be *$\theta$- closed* if and only if $|A|_\theta = A$. The above concepts are generally used in the literature (see e.g. [14] and [2]).

1991 *Mathematics Subject Classification.* Primary 54F15, 54F50; Secondary 54B35.
*Key words and phrases.* Inverse limit, H-closed, $\theta$-closed.

**Proposition 3.** [3, (2.3)]. *A space $X$ is Hausdorff if and only if for each $p \in X$, $|\{p\}|_\theta = \{p\}$.*

**Proposition 4.** [3, (2.4)]. *A space is regular if and only if for every $A \subset X$, $|A|_\theta = Cl\ A$.*

In the sequel the following theorem frequently will be used.

**Theorem 1.1.** [6, Theorem 2]. *In any topological space:*

**(a):** *the empty set and the whole space are $\theta$-closed,*
**(b):** *arbitrary intersection and finite unions of $\theta$-closed sets are $\theta$-closed,*
**(c):** *$Cl\ K \subset |K|_\theta$ for each subset $K$,*
**(d):** *a $\theta$-closed subset is closed.*

A subset $A \subset X$ is said to be *$\theta$-open* if $X \setminus A$ is $\theta$-closed.A subset $A \subset X$ is said to be *regular- open* provided $\text{Int}\ (\ \text{Cl}\ (A)) = A$.

A Hausdorff space $X$ is *H-closed* [1] if it is closed in any Hausdorff space in which it is embedded.

The following two characterizations are given in [1].

**Proposition 5.** [1, Theorem 1]. *A Hausdorff space $X$ is H-closed if and only if every family $\{U_\mu : U_\mu$ is open in $X$, $\mu \in \Omega\}$ with the finite intersection property has the property $\cap\{\ Cl\ U_\mu : \mu \in \Omega\} \neq \emptyset$.*

**Proposition 6.** [1, Theorem 2]. *A Hausdorff space $X$ is H-closed if for each open cover $\{U_\mu : \mu \in M\}$ of $X$ there exists a finite subfamily $\{U_{\mu_1}, ..., U_{\mu_k}\}$ such that $\{\ Cl\ U_{\mu_1}, ...,\ Cl\ U_{\mu_k}\}$ is a cover of $X$.*

**Proposition 7.** [6]. *A Hausdorff space $X$ is H-closed if and only if for every family $\{A_\mu : A_\mu \subset X,\ \mu \in \Omega\ \}$ with the finite intersection property there exists a point $x \in X$ such that $Cl\ V \cap A \neq \emptyset$ for every open set $V$ containing $x$ and every $A_\mu$.*

The point $x$ is called *$\theta$-accumulation point*. From this characterizations it follows the following lemma frequently used in the paper.

**Lemma 1.2.** *If $X$ is H-closed, then every family $\{A_\mu,\ \mu \in \Omega\ \}$ of $\theta$-closed subsets of $X$ with the finite intersection property has a non-empty intersection $\cap\{A_\mu,\ \mu \in \Omega\ \}$.*

*Proof.* Let $X$ be H-closed and let $\{A_\mu,\ \mu \in \Omega\ \}$ be a family of $\theta$-closed subsets of $X$ with the finite intersection property. By Proposition 7 we infer that there exists a $\theta$-accumulation point $x$ such that $\text{Cl}\ V \cap A \neq \emptyset$ for every open set $V$ containing $x$ and every $A_\mu$. This means that $x \in \cap\{A_\mu :,\ \mu \in \Omega\ \}$ since each $A_\mu$ is $\theta$-closed. □

**Theorem 1.3.** [2, (2.4), p.410]. *Disjoint $\theta$-closed subsets of an H-closed space are contained in disjoint open subsets.*

**Lemma 1.4.** *If $f : X \to Y$ is a continuous mapping, then $f^{-1}(F)$ is $\theta$-closed in $X$ if $F$ is $\theta$-closed in $Y$.*

*Proof.* If $x \in X \setminus f^{-1}(F)$, then $f(x) \notin F$. There exists an open set $U$ such that $f(x) \in U$ and $\text{Cl}\ U \cap F = \emptyset$ since $F$ is $\theta$-closed in $Y$. The open set $f^{-1}(U)$ contains $x$ and $\text{Cl}\ f^{-1}(U) \cap f^{-1}(F) = \emptyset$ since $f^{-1}(\ \text{Cl}\ U) \cap f^{-1}(F) = \emptyset$. Hence, if $x \in X \setminus f^{-1}(F)$, then $x \in X \setminus \left|f^{-1}(F)\right|_\theta$, and, consequently, $f^{-1}(F)$ is $\theta$-closed in $X$. □

A net $\{x_\mu : \mu \in M\}$ is *eventually* in a set $A$ if and only if there exists a $\mu \in M$ such that $x_\nu \in A$ for each $\nu \geq \mu$ [12, p. 65].

A net $\{x_\mu : \mu \in M\}$ is *frequently* in a set $A$ if and only if for each $\mu \in M$ there is a $\nu \geq \mu$ such that $x_\nu \in A$.

A net in a topological space is said to *$\theta$-converge* (*$\theta$-accumulate*) [6, Definition 3] to a point $x$ in the space if then net is eventually (frequently) in $\mathrm{Cl}\,(V)$ for each open set $V$ about $x$.

The following two theorems are proved in [17, Lemmas 1, 2, 3]. See also [9].

**Theorem 1.5.** *A point $x$ in a topological space is in $\theta$-closure of a subset $K$ if and only if there is a net $x_a$ in $K$ which $\theta$-converges to $x$ ($x_a \xrightarrow[\theta]{} x$).*

**Theorem 1.6.** *A Hausdorff space is H-closed if and only if each net in the space has a $\theta$-convergent subnet.*

In the sequel the following Proposition will be frequently used.

**Proposition 8.** [3, (2.7), p. 45]. *A $\theta$-closed subset of an H-closed space is H-closed.*

## 2. Inverse limit of H-closed spaces and mappings with $\theta$-closed graphs

In this Section we consider inverse limit of inverse systems $\mathbf{X} = \{X_a, p_{ab}, A\}$ of H-closed spaces $X_a$ and bonding mappings $p_{ab}$ with $\theta$-closed graphs. Such bonding mappings $p_{ab}$ are special case of multifunction considered in [11].

Let $f : X \to Y$ be a mapping. The graph $G(f)$ of $f$ is

$$G(f) = \{(x, y) \in X \times Y : y = f(x)\}.$$

**Theorem 2.1.** [11, Theorem 2.3]. *The following statements are equivalent for spaces $X, Y$, and multifunction $\Phi : X \to Y$:*

- **(a):** *The multifunction $\Phi$ has a $\theta$-closed graph $G(\Phi)$,*
- **(b):** *For each $(x, y) \in (X \times Y) - G(\Phi)$ there are sets $V \ni x$ in $X$ and $W \ni y$ in $Y$ with $\Phi(\ Cl\ (V)) \cap\ Cl\ (W) = \emptyset$.*

Now we shall prove the following result concerning inverse limit of inverse systems $\mathbf{X} = \{X_a, p_{ab}, A\}$ of H-closed spaces $X_a$ and bonding mappings $p_{ab}$ with $\theta$-closed graph.

**Theorem 2.2.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty H-closed spaces $X_a$ and bonding mappings $p_{ab}$ with $\theta$-closed graphs. Then $X = \lim \mathbf{X}$ is non-empty, $\theta$-closed in $\Pi\{X_a : a \in A\}$ and H-closed.*

*Proof.* It is known that $\Pi\{X_a : a \in A\}$ is H-closed [4, Problem 3.12.5 (d), p. 283]. Let us prove that $Z_a = \{(x_b) \in \Pi X_a : p_{ab}(x_a) = x_b\}$ is $\theta$-closed for each $a \in A$. To do this we shall prove that $\Pi\{X_a : a \in A\} \setminus Z_a$ is $\theta$ -open. Let $y = (y_a) \in \Pi\{X_a : a \in A\} \setminus Z_a$. There exists $b \leq a$ such that $p_{ab}(x_a) \neq x_b$. It follows from Theorem 2.1 that there exists a pair $U, V$ of open sets such that $x_a \in U$, $x_b \in V$ and $p_{ba}(\ \mathrm{Cl}\ U) \cap\ \mathrm{Cl}\ V = \emptyset$ since $p_{ba}$ has a $\theta$-closed graph.

Now $Z = U \times V \times \Pi\{X_c : c \neq a, b\}$ is open set containing $y$ with the property $\mathrm{Cl}\ Z \subset \Pi\{X_a : a \in A\} \setminus Z_a$ . This means that $\Pi\{X_a : a \in A\} \setminus Z_a$ $\theta$-open, and, consequently, $Z_a$ is $\theta$-closed. In order to prove that $X = \lim \mathbf{X}$ is non-empty consider the family $\{Z_a : a \in A\}$ of $\theta$-closed sets $Z_a$. This family has the finite intersection property (Proposition 2). By Lemma 1.2 we infer that $\cap\{Z_a : a \in A\}$ $= \lim \mathbf{X}$ is non-empty. Now, (b) of Theorem 1.1 implies that $\lim \mathbf{X}$ is $\theta$-closed. Finally, from Proposition 8 it follows that $\lim \mathbf{X}$ is H-closed. □

## 3. Inverse limit of H-closed spaces and strongly continuous bonding mappings

A mapping $f : X \to Y$ is said to be *strongly continuous at* $x \in X$ [15] provided for each neighborhood $U$ of $f(x)$ there is a neighborhood $V$ of $x$ such that $f(\text{ Cl } V) \subset U$. A mapping $f : X \to Y$ is said to be *strongly continuous* provided $f$ is strongly continuous at each point $x \in X$.

If $Y$ is a regular space, then each continuous mapping $f : X \to Y$ is strongly continuous.

**Proposition 9.** *Let $Y$ be a Hausdorff space. Every strongly continuous mapping $f : X \to Y$ has a $\theta$-closed graph.*

*Proof.* Let $x \in X$ and $y \in Y$ such that $y \neq f(x)$. There are open disjoint sets $U, V$ in $Y$ such that $y \in U$ and $f(x) \in V$. It is clear that $\text{Cl } U \cap V = \emptyset$. Moreover, there is an open set $W$ containing $x$ such that $p_{ab}(\text{ Cl } W) \subset V$ since $f$ is strongly continuous. Now, for $(x, y) \in (X \times Y) - G\{f\}$ there are sets $W \ni x$ in $X$ and $U \ni y$ in $Y$ with $f(\text{ Cl } (W)) \cap \text{ Cl } (U) = \emptyset$. By Theorem 2.1 the proof is completed. □

Theorem 2.2 and Proposition 9 imply the following result.

**Theorem 3.1.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty H-closed spaces $X_a$ and strongly continuous bonding mappings. Then $X = \lim \mathbf{X}$ is non-empty. Moreover, $X = \lim \mathbf{X}$ is $\theta$-closed in $\Pi\{X_a : a \in A\}$ and H-closed.*

## 4. Inverse limit of H-closed spaces and $\theta$-closed bonding mappings

In this section we study the inverse systems $\mathbf{X} = \{X_a, p_{ab}, A\}$ with H-closed spaces $X_a$ and $\theta$-closed bonding mappings $p_{ab}$.

A mapping $f : X \to Y$ is said to be $\theta$-closed if $f(F)$ is $\theta$-closed for each $\theta$-closed subset $F \subset X$.

**Remark 4.1.** *In* [16, Definition 4.1, p. 490] *is given the following definition. A function $f$ is said to be $\theta$-open if the image of every open set is $\theta$-open. Similarly, a function $f$ is said to be $\theta$ -closed if the image of every closed set is $\theta$-closed.*

**Lemma 4.2.** *Let $f : X \to Y$ be a continuous mapping. The following conditions are equivalent:*

- **(a):** *$f$ is $\theta$-closed,*
- **(b):** *for every $B \subset Y$ and each $\theta$-open set $U \supseteq f^{-1}(B)$ there exists a $\theta$-open set $V \supseteq B$ such that $f^{-1}(V) \subset U$.*

*Proof.* The proof is similar to the proof of the corresponding theorem for closed mappings [4, p. 52]. □

Now we are ready to prove the following theorem.

**Theorem 4.3.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty H-closed spaces $X_a$ and $\theta$-closed bonding mappings $p_{ab}$. Then $X = \lim \mathbf{X}$ is non-empty and*

$$p_a(X) = \cap\{p_{ab}(X_b) : b \geq a\}$$

*where $p_a : X \to X_a, a \in A$, is a natural projection.*

*Proof.* Let $\theta_a$ be a family of all non-empty $\theta$-closed subsets of $X_a$ and let $\mathcal{Y}$ be a family of all collections $Y = \{Y_a : Y_a \in \theta_a, a \in A\}$ such that $p_{ab}(Y_b) \subset Y_a$. The family $\mathcal{Y}$ is non-empty since $\mathbf{X} \in \mathcal{Y}$. For two collections $Y = \{Y_a : Y_a \in \theta_a, a \in A\}$ and $Z = \{Z_a : Z_a \in \theta_a, a \in A\}$ we shall write $Y \geq Z$ if $Y_a \subset Z_a$ for every $a \in A$. It is clear that $(\mathcal{Y}, \geq)$ is a partially ordered set. The remaining part of the proof consists of several steps.

**Step 1**. *There exists a maximal element in* $(\mathcal{Y}, \geq)$. It suffices to prove that $(\mathcal{Y}, \geq)$ is inductive, i.e., if $L = \{Y^\lambda : \lambda \in \Lambda\}$ is a strictly increasing chain in $(\mathcal{Y}, \geq)$, then there is an element $M \in (\mathcal{Y}, \geq)$ such that $M \geq Y^\lambda$ for every $\lambda \in \Lambda$. We define $M = \{M_a : M_a \in \theta_a, a \in A\}$ such that $M_a = \cap\{Y_a^\lambda : \lambda \in \Lambda\}$. From Lemma 1.2 and Theorem 1.1 it follows that the set $M_a$ is non-empty $\theta$-closed subset of $X_a$. Moreover, $p_{ab}(M_b) \subset M_a$.

**Step 2**. *If* $Y = \{Y_a : Y_a \in \theta_a, a \in A\}$ *is a maximal element of* $(\mathcal{Y}, \geq)$, *then* $Y_a = p_{ab}(Y_b)$ *for every pair* $a, b \in A$ *such that* $a \leq b$. Let $Z = \{Z_a : Z_a \in \theta_a, a \in A\}$ be a collection such that $Z_a = \cap\{p_{ab}(Y_b) : b \geq a\}$. Each $p_{ab}(Y_b)$ is $\theta$-closed since $p_{ab}$ is $\theta$-closed and $Y_b \in \theta_b$. By Lemma 1.2 and Theorem 1.1 it follows that the set $Z_a$ is non-empty $\theta$-closed subset of $X_a$. In order to prove that $Z \in (\mathcal{Y}, \geq)$ it suffices to prove that $p_{ab}(M_b) \subset M_a$. If $a \leq b$ then $p_{ab}(Z_b) \subset \cap\{p_{ab}(p_{bc}(Y_c)) : b \leq c\} = \cap\{p_{ac}(Y_c) : c \geq b\}$. On the other hand, for every $d \geq a$ there is a $c \in A$ such that $c \geq b, d$. It follows that $p_{ac}(Y_c) \subset p_{ad}(Y_d)$. This means that

$$\cap\{p_{ac}(Y_c) : c \geq b\} = \cap\{p_{ad}(Y_d) : c \geq b\} = Z_a.$$

Finally, we have $Z \in (\mathcal{Y}, \geq)$. Moreover, $Z_a \subset Y_a$ for each $a \in A$. This means that $Z = Y$ since $Y$ is maximal.

**Step 3**. *If* $Y = \{Y_a : Y_a \in \theta_a, a \in A\}$ *is a maximal element of* $(\mathcal{Y}, \geq)$, *then* $Y_a$ is *one-point set for every* $a \in A$. Let $x_a \in Y_a$. Define

$$Z_b = \begin{cases} Y_b \cap p_{ab}^{-1}(x_a) & \text{if} \quad b \geq a, \\ Y_b & \text{if} \quad b \not\leq a. \end{cases}$$

Let us prove that $Z = \{Z_a : Z_a \in \theta_a, a \in A\}$. From Proposition 3 and Lemma 1.4 it follows that $p_{ab}^{-1}(x_a)$ is $\theta$-closed. Then, by Theorem 1.1, we infer that each $Y_b \cap p_{ab}^{-1}(x_a)$ is $\theta$-closed. It is easy to prove that $p_{ab}(Z_b) \subset Z_a$. Hence, $Z \in (\mathcal{Y}, \geq)$. Now, $Z = Y$ since $Z \geq Y$ and $Y$ is maximal. This means $Y_a = \{x_a\}$.

**Step 4**. $\lim \mathbf{X}$ *is non-empty.* From Step 3 we have $Z = \{Z_a : Z_a \in \theta_a, a \in A\} = \{x_a : a \in A\}$ such that $p_{ab}(x_b) = x_a$ for every pair $a, b$ such that $b \geq a$.

**Step 5**. *Let us prove* $p_a(X) = \cap\{p_{ab}(X_b) : b \geq a\}$. It is clear that $p_a(X) \subset \cap\{p_{ab}(X_b) : b \geq a\}$. Let us prove that $p_a(X) \supset \cap\{p_{ab}(X_b) : b \geq a\}$. Let $x_a \in \cap\{p_{ab}(X_b) : b \geq a\}$. This means that $Y_b = p_{ab}^{-1}(x_a)$ is non-empty for each $b \geq a$. Moreover, $Y_b$ is $\theta$-closed (Proposition 3 and Lemma 1.4). For each $b$ non-comparable with $a$, let $Y_b = X_b$. Now, we have a collection $Y = \{Y_a : Y_a \in \theta_a, a \in A\}$ which is evidently in $(\mathcal{Y}, \geq)$. There exists a maximal element $Z = \{Z_a : Z_a \in \theta_a, a \in A\}$ in $(\mathcal{Y}, \geq)$ such that $Z \geq Y$. It follows that each $Y_a$ is some $Z_a$ which is a point $z_a \in X_a$ (Step 3) since $Z$ is maximal. The collections $(z_a)$ is a point of $\lim \mathbf{X}$. Hence, $p_a(X) = \cap\{p_{ab}(X_b) : b \geq a\}$. □

**QUESTION 1**. Is it true that $X = \lim \mathbf{X}$ in Theorem 4.3 is H-closed?

**QUESTION 2**. Is every projection $p_a : \lim \mathbf{X} \to \mathbf{X}_a$ $\theta$-closed?

At the end of this section we consider the special kinds of $\theta$-closed mappings.

A mapping $f : X \to Y$ has the *inverse property* provided $f^{-1}(\operatorname{Cl} V) = \operatorname{Cl} f^{-1}(V)$ for every open set $V \subset Y$.

**Lemma 4.4.** *If $f : X \to Y$ is a closed mapping with the inverse property and if $X$ and $Y$ are H-closed, then $f$ is $\theta$-closed.*

*Proof.* Let $F$ be a $\theta$-closed subset of $X$. In order to prove that $f(F)$ is $\theta$-closed we shall prove that $Y \setminus f(F)$ is $\theta$-open. Let $y \in Y \setminus f(F)$. Now, $f^{-1}(y)$ is $\theta$-closed subset of $X$ (Lemma 1.4). Using Theorem 1.3 we obtain disjoint open sets $U$ and $V$ such that $F \subset U$ and $f^{-1}(y) \subset V$. It follows that $\operatorname{Cl} V \cap U = \emptyset$. The closeness of $f$ imply the existence of an open set $W$ about $y$ such that $f^{-1}(W) \subset V$. We infer that $\operatorname{Cl} f^{-1}(W) \subset \operatorname{Cl} V$. Moreover, $f^{-1}(\operatorname{Cl} W) \subset \operatorname{Cl} V$. It follows that $f^{-1}(\operatorname{Cl} W) \cap F = \emptyset$, i.e., $\operatorname{Cl} W \cap f(F) = \emptyset$. Hence, if $y \in Y \setminus f(F)$, then $y$ has a neighborhood $W$ such that $\operatorname{Cl} W \subset Y \setminus f(F)$, i.e., $Y \setminus f(F)$ is $\theta$-open and $f(F)$ is $\theta$-closed. □

Each open mapping has the inverse property [4, Exercise 1.4.C., p. 57] . Hence, we have the following corollary.

**Corollary 4.5.** *If $f : X \to Y$ is a closed and open mapping and if $X$ and $Y$ are H-closed, then $f$ is $\theta$-closed.*

**Lemma 4.6.** *If $X$ and $Y$ are H-closed, then each strongly continuous mapping $f : X \to Y$ is $\theta$-closed.*

*Proof.* Let us recall that $f : X \to Y$ is said to be strongly continuous at $x \in X$ [15] provided for each neighborhood $U$ of $f(x)$ there is a neighborhood $V$ of $x$ such that $f(\operatorname{Cl} V) \subset U$. A mapping $f : X \to Y$ is said to be strongly continuous provided $f$ is strongly continuous at each point $x \in X$. Now, let us prove Lemma.

Let $F$ be a $\theta$-closed subset of $X$. We have to prove that $f(F)$ is a $\theta$-closed subset of $Y$. Suppose that it is not $\theta$-closed. There is a point $y \in |f(F)|_\theta \setminus f(F)$. By Theorem 1.5 we infer that there is a net $\{y_a : y_a \in f(F), a \in A\}$ which $\theta$-converges to $y$. Now there is a net $\{x_a : x_a \in F, f(x_a) = y_a\}$. By Theorem 1.6 we may assume that this net is $\theta$-convergent to some point $x \in X$. From Theorem 1.5 it follows that $x \in F$ since $F$ is $\theta$-closed. It is clear that $f(x)$ is $\theta$-limit of $\{f(x_a) : x_a \in F\} = \{y_a : y_a \in f(F), a \in A\}$. We infer that $f(x) = y$ since, in the opposite case, $f(x)$ and $y$ have disjoint neighborhoods $U$ and $V$ such that $f(x) \in U$ and there is a neighborhood $W$ such that $f(\operatorname{Cl} W) \subset U$. This means that a net $\{y_a : y_a \in f(F), a \in A\}$ is not eventually in $\operatorname{Cl} V$. This is impossible. Hence, $f(x) = y$ From $x \in F$ it follows that $f(x) \in f(F)$. Hence $y \in f(F)$ and $f(F)$ is $\theta$-closed. The proof is completed. □

**Lemma 4.7.** *If $Y$ is Urysohn and $X$ H-closed, then each continuous mapping $f : X \to Y$ is $\theta$-closed.*

*Proof.* Let $F$ be a $\theta$-closed subset of $X$. We have to prove that $f(F)$ is a $\theta$-closed subset of $Y$. Suppose that it is not $\theta$-closed. There is a point $y \in |f(F)|_\theta \setminus f(F)$. By Theorem 1.5 we infer that there is a net $\{y_a : y_a \in f(F), a \in A\}$ which $\theta$-converges to $y$. Now there is a net $\{x_a : x_a \in F, f(x_a) = y_a\}$. By Theorem 1.6 we may assume that this net is $\theta$-convergent to some point $x \in X$. From Theorem 1.5 it follows that $x \in F$ since $F$ is $\theta$-closed. It is clear that $f(x)$ is $\theta$-limit of $\{f(x_a) : x_a \in F\}$ $= \{y_a : y_a \in f(F), a \in A\}$. We infer that $f(x) = y$ since in Urysohn space a net

has only one $\theta$-limit. From $x \in F$ it follows that $f(x) \in f(F)$. Hence $y \in f(F)$ and $f(F)$ is $\theta$-closed. The proof is completed □

A function $f : X \to Y$ is *almost closed* [2] if for any set $A \subset X$ we have $f(|A|_\theta) = |f(A)|_\theta$.

Now we shall prove the following theorem.

**Theorem 4.8.** *Each almost closed function is $\theta$-closed.*

*Proof.* If $A$ is $\theta$-closed, then $A = |A|_\theta$. Now we have $f(|A|_\theta) = |f(A)|_\theta$ or $f(A) = |f(A)|_\theta$. This means that $f(A)$ is $\theta$-closed. Hence $f$ is $\theta$-closed. □

**Corollary 4.9.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty H-closed spaces $X_a$ and closed bonding mappings $p_{ab}$ with the inverse property. Then $X = \lim \mathbf{X}$ is non-empty and H-closed.*

*Proof.* Lemma 4.4 and Theorem 4.3 imply the Corollary. H-closenes of $\lim \mathbf{X}$ it follows from Theorems 3.3 and 3.7 of [5]. □

## 5. Inverse systems of nearly-compact spaces

We say that a space $X$ is an *Urysohn space* ([7], [10]) if for every pair $x, y, x \neq y$, of points of $X$ there exist open sets $V$ and $W$ about $x$ and $y$ such that $\operatorname{Cl} V \cap \operatorname{Cl} W = \emptyset$.

A Hausdorff space is *nearly-compact* [8] if every open cover if every open cover $\{U_\mu : \mu \in M\}$ has a finite subcollection $\{U_{\mu_1}, ..., U_{\mu_n}\}$ such that $\operatorname{Int} \operatorname{Cl} U_{\mu_1} \cup ... \cup \operatorname{Int} \operatorname{Cl} U_{\mu_n} = X$. Every nearly-compact space is H-closed.

**Lemma 5.1.** [8]. *A space $X$ is nearly-compact if and only if it is H-closed and Urysohn.*

If $\mathbf{X} = \{X_a, p_{ab}, A\}$ is an inverse system of nearly-compact spaces, then $\theta$-closeness of bonding mappings $p_{ab}$ in Theorem 4.3 follows from Lemma 4.7, but we shall give the alternate proof of the following theorem.

**Theorem 5.2.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty nearly-compact spaces $X_a$. Then $X = \lim \mathbf{X}$ is non-empty, $\theta$-closed in $\Pi\{X_a : a \in A\}$ and nearly-compact.*

*Proof.* Let us observe that $\Pi\{X_a : a \in A\}$ is H-closed [4, Problem 3.12.5 (d), p. 283]. Let us prove that $Y_a = \{(x_b) \in \Pi X_a : p_{ab}(x_a) = x_b\}$ $\theta$-closed for each $a \in A$. To do this we shall prove that $\Pi X_a \setminus Y_a$ $\theta$-open. Let $y = (y_a) \in \Pi X_a \setminus Y_a$. There exists $b \leq a$ such that $p_{ab}(x_a) \neq x_b$. It follows that there exists a pair $U, V$ of open sets such that $x_b \in U$, $p_{ab}(x_a) \in V$ and $\operatorname{Cl} U \cap \operatorname{Cl} V = \emptyset$ since $X_b$ is Urysohn. Moreover, there is an open set $W$ containing $x_a$ such that $p_{ab}(\operatorname{Cl} W) \subset \operatorname{Cl} V$. Now $Z = U \times W \times \Pi\{X_c : c \neq a, b\}$ is open set containing $y$ with the property $\operatorname{Cl} Z \subset \Pi X_a \setminus Y_a$. This means that To $\Pi X_a \setminus Y_a$ $\theta$-open, and, consequently, $Y_a$ is $\theta$-closed. In order to prove that $X = \lim \mathbf{X}$ is non-empty consider the family $\{Y_a : a \in A\}$ of $\theta$-closed sets $Y_a$. This family has the finite intersection property (Proposition 2). By Lemma 1.2 we infer that $\cap\{Y_a : a \in A\} = \lim \mathbf{X}$ is non-empty. It is $\theta$-closed by Theorem 1.1 and H-closed by Proposition 8. Moreover, $\lim \mathbf{X}$ is Urysohn and, consequently, nearly-compact. □

## 6. Inverse systems with semi-open bonding mappings

A mapping $f : X \to Y$ is said to be *semi-open* provided $\text{Int } f(U) \neq \emptyset$ for each non-empty open $U \subset X$.

**Theorem 6.1.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty H-closed spaces $X_a$ and semi-open bonding mappings. Then $X = \lim \mathbf{X}$ is non-empty and H-closed.*

*Proof.* The proof is broken into several steps.

**Step 1**. By virtue of [13, Theorem 2, p. 10] we can assume that $A$ is cofinite, i.e., for each $a \in A$ the set of all predecessors of $a$ is finite set.

**Step 2**. *The sets*

$$Z_a = \{\{x_a\} \in \Pi X_a : p_{ab}(x_b) = x_a,\ a \leq b\}$$

*have non-empty interior.* Let $a_1, ..., a_k$ be a set of all predecessors of $a$. If $U \subset X_a$ is open set, then $\text{Int } p_{a_1a}(U) \times ... \times \text{Int } p_{a_ka}(U) \times U \times \Pi\{X_b : b \notin \{a_1, ..., a_k, a\}\}$ is an open set contained in $Z_a$. Hence, $\text{Int } Z_a$ is non-empty for each $a \in A$.

**Step 3**. *The family $\{\text{Int } Z_a : a \in A\}$ has the finite intersection property.* This follows from the fact that for each pair $a, b$ there is a $c \in A$ such that $Z_c \subset Z_a \cap Z_b$ and, consequently, $\text{Int } Z_c \subset \text{Int } Z_a \cap \text{Int } Z_b$.

**Step 4**. $\cap\{\text{Cl Int } Z_a : a \in A\}$ is non-empty. This follows from Proposition 5.

**Step 5**. Now $\lim \mathbf{X} = \cap\{Z_a : a \in A\} \supset \cap\{\text{Cl Int } Z_a : a \in A\}$. This means that $\lim \mathbf{X}$ is non-empty and the proof of non-emptiness is completed.

**Step 6**. *$X = \lim \mathbf{X}$ is H-closed.* Let $\mathcal{U} = \{U_\mu : \mu \in M\}$ be a maximal family of open sets of $X$ with the finite intersection property. From the definition of topology on $X$ it follows that there is an $a(\mu) \in A$ such that $\text{Int } f_{a(\mu)}(U_\mu)$ is non-empty. By virtue of the semi-openness of $p_{ab}$ we infer that $\text{Int } f_a(U_\mu) \neq \emptyset$ for every $a \in A$ and every $\mu \in M$. This means that a family $\{\text{Int } f_a(U_\mu) : \mu \in M\}$ is a family with the finite intersection property. Let us prove that this family is maximal. If $U$ is an open set which intersects every set $\text{Int } f_a(U_\mu), \mu \in M$, then $p_a^{-1}(U) \in \mathcal{U}$ since $p_a^{-1}(U)$ intersects every $U_\mu$. This means that $U \in \{\text{Int } f_a(U_\mu) : \mu \in M\}$. Hence, $\{\text{Int } f_a(U_\mu) : \mu \in M\}$ is maximal. From the H-closeness of $X_a$ and Proposition 5 it follows that there is a point $x_a = \cap\{\text{Cl Int } f_a(U_\mu) : \mu \in M\}$. It is obvious that $p_{ab}(x_b) = x_a$ for every $b \geq a$.Now, $x = (x_a : a \in A)$ is a point of $\lim \mathbf{X}$ and $x \in \cap\{\text{Cl } U_\mu) : \mu \in M\}$. By Proposition 5 $\lim \mathbf{X}$ is H-closed and the proof is completed. □

We close this Section with some corollaries of Theorem 6.1.

**Corollary 6.2.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty H-closed spaces $X_a$ and open bonding mappings. Then $X = \lim \mathbf{X}$ is non-empty and H-closed.*

**Remark 6.3.** *For another proof of this corollary see* [18].

A mapping $f : X \to Y$ is an *irreducible mapping* if the set $f^{\#}(U) = \{y \in Y : f^{-1}(y) \subset U\}$ is non-empty for every non-empty open se $U \subset X$. If $f : X \to Y$ is a closed and irreducible mapping, then $f^{\#}(U)$ is open and non-empty. Hence, a closed and irreducible mapping is semi-open. Theorem 6.1 now gives the following corollary.

**Corollary 6.4.** *Let $\mathbf{X} = \{X_a, p_{ab}, A\}$ be an inverse system of non-empty H-closed spaces $X_a$ and closed irreducible bonding mappings. Then $X = \lim \mathbf{X}$ is non-empty and H-closed.*

**Acknowledgement**. The author is very grateful to the referee for his/her help and valuable suggestions.

## References

[1] P. S. Aleksandroff et P. S. Urysohn, *Mémoire sur les espaces topologiques compacts*, Verh. Akademie Amsterdam, Deel XIV, Nr. 1 (1929), 1-96.
[2] R. F. Dickman, Jr. and J. R. Porter, *$\theta$ -closed subsets of Hausdorff spaces*, Pac. J. Math. 59 (1975), 407-415.
[3] R. F. Dickman, Jr. and J. R. Porter, *$\theta$ -perfect and $\theta$-absolutely closed function,* Illinois J. Math 21 (1977), 42-60.
[4] R. Engelking, *General Topology*, PWN,Warszawa, 1977.
[5] L. M. Friedler and D. H. Pettey, *Inverse limits and mappings of minimal topological spaces*, Pac. J. Math. 71 (1977), 429-448.
[6] L. L. Herrington and P. E. Long, *Characterizations of H-closed spaces*, Proc. Amer. Math. Soc. 48 (1975), 469-475.
[7] L. L. Herrington, *Characterizations of Urysohn-closed spaces*, Proc. Amer. Math. Soc. 55 (1976), 435-439.
[8] L. L. Herrington, *Properties of nearly-compact spaces*, Proc. Amer. Math. Soc. 45 (1974), 431-436.
[9] J. E. Joseph, *On H-closed spaces*, Proc. Amer. Math. Soc. 55 (1976), 223-226.
[10] J. E. Joseph, *On Urysohn-closed and minimal Urysohn spaces*, Proc. Amer. Math. Soc. 68 (1978), 235-242.
[11] J. E. Joseph, *Multifunctions and graphs*, Pacific J. Math, Vol. 79, 1978, 509-529.
[12] J. L. Kelley, General topology, D. van Nostrand 1963.
[13] S. Mardesic and J. Segal, Shape theory. The inverse system approach, North-Holland Publishing Company, (1982).
[14] T. Noiri, *Strongly $\theta$-precontinuous functions*, Acta Math. Hungar., 90 (2001), 307-316.
[15] M. Saleh, *On $\theta$-Continuity And Strong $\theta$-Continuity*, Applied Mathematics E-Notes 3 (2003), 42-48.
[16] M. Saleh, *On $\theta$-closed sets and some forms of continuity*, Archivum Mathematicum (Brno), 40 (2004), 383-393.
[17] N. V. Veličko, *H-closed topological spaces*, Mat. Sb., 70 (112) (1966), 98-112.
[18] T. O. Vinson, Jr. and R. F. Dickman, Jr., *Inverse limits and absolutes of H-closed spaces*, Proc. Amer. Math. Soc. 66 (1977), 351-358.

Faculty of Organizations and Informatics Varaždin, Croatia
*E-mail address*: ivan.loncar@foi.hr or ivan.loncar1@vz.htnet.hr

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 57–60
ISSN 1930-1235: (electronic version)

# ON GENERALIZED QUASI-CONVEX FUNCTIONS

KHALIDA INAYAT NOOR

Abstract. In this paper, we introduce and study a class $\tilde{Q}_k(\alpha,\beta,\rho,\gamma)$ of analytic functions in the unit disc. This class generalizes the concept of quasi-convexity. Inclusion results, distortion theorem and some other properties of this class are investigated.

## 1. Introduction

Let $\tilde{P}(\gamma)$ denote the class of functions $p$ of the form

$$p(z) = 1 + c_1 z + c_2 z^2 + \ldots, \tag{1}$$

which are analytic in the unit disc $E = \{z : |z| < 1\}$ and which satisfy the condition $|\arg p(z)| \leq \frac{\pi\gamma}{2}$ for some $\gamma(\gamma > 0)$ in $E$. We note that $\tilde{P}(1) \equiv P$ is the class of analytic functions with positive real part. It can easily be shown that the class $\tilde{P}(\gamma)$ is a convex set.

Let $V_k(\rho), k \geq 2, 0 \leq \rho < 1$, be the class of functions of analytic and locally univalent in $E$, $f(0) = 0$, $f'(0) = 1$ and satisfying the condition

$$\int_0^{2\pi} \left| \{Re \frac{(zf'(z))'}{f'(z)} - \rho\}/(1-\rho) \right| d\theta \leq k\pi. \tag{2}$$

When $\rho = 0$, we obtain the class $V_k$, $(k \geq 2)$ of functions of bounded boundary rotation. It can easily be shown that $f \in V_k(\rho)$ if and only if there exists a function $f_1 \in V_k$ such that

$$f'(z) = (f_1'(z))^{1-\rho}. \tag{3}$$

We note that $V_2 \equiv C \subset S^\star$, where $C$ and $S^\star$ are respectively the classes of convex and starlike univalent functions in $E$.

We now introduce the following classes of analytic functions.

**Definition 1.1.** Let $f : f(z) = z + \sum_{n=2}^{\infty} a_n z^n$ be analytic in $E$. Then, for $0 \leq \rho < 1$, $0 \leq \gamma \leq 1$, $f \in T_k^\star(\rho,\gamma)$ if and only if there exists a function $g \in V_k(\rho)$ such that, for $z \in E$, $\frac{f'(z)}{g'(z)} \in \tilde{P}(\gamma)$.

We note that $T_2^\star(\rho,\gamma) = \tilde{K}(\rho,\gamma) \subset \tilde{K}(\gamma)$, where $\tilde{K}(\gamma)$ is the class of strongly close-to-convex functions.

**Definition 1.2.** Let $\alpha, \beta \geq 0$, $(\alpha + \beta \neq 0)$, and let $f$ be analytic in $E$ with $f(0) = 0$, $f'(0) = 1$. Then $f \in \tilde{Q}_k(\alpha,\beta,\rho,\gamma)$ for $z \in E$, if and only if there

1991 *Mathematics Subject Classification.* Primary 30C45; Secondary 30C50.
*Key words and phrases.* Quasi-convex functions, convolution, integral operator.

exists a $g \in V_k(\rho)$ such that

$$\left\{\frac{\alpha}{\alpha+\beta}\frac{f'(z)}{g'(z)}+\frac{\beta}{\alpha+\beta}\frac{(zf'(z))'}{g'(z)}\right\}\in\tilde{P}(\rho),\quad \text{for some}\quad \gamma>0. \tag{4}$$

The class $\tilde{Q}_2(\alpha,0,0,\gamma)$ consists of strongly close-to-convex functions. Also $\tilde{Q}_2(0,1,0,1)\equiv C^\star$ is the class of quasi-convex functions introduced in [1]. Also see [2,3]. For $\beta=(1-\alpha),\quad g\in V_2(0)\equiv C$, we obtain the class of strongly $\alpha$-quasi-convex functions discussed in [7]. The case $\rho=\beta=0,\quad \alpha=\gamma=1$ gives us the class $T_k$ which was introduced and investigated in [4]. We also refer to [5] for more details.

## 2. Main Results

**Theorem 2.1.** *Let $f$ be analytic in $E$ with $f(0)=f'(0)-1=0$. Then $f\in\tilde{Q}_k(\alpha,\beta,\rho,\gamma)$ if and only if*

$$\left\{\frac{\alpha}{\alpha+\beta}f(z)+\frac{\beta}{\alpha+\beta}zf'(z)\right\}\in T_k^\star(\rho,\gamma),\quad \textit{for}\quad z\in E.$$

*Proof.* The proof follows immediately from the definition of these classes. □

**Theorem 2.2.** *For $\beta>0,\quad f\in\tilde{Q}_k(\alpha,\beta,\rho,\gamma)$ if and only if there exists $F\in T_k^\star(\rho,\gamma)$ such that*

$$f(z)=\frac{\alpha+\beta}{\beta}z^{\frac{-\alpha}{\beta}}\int_0^z t^{\frac{\alpha}{\beta}-1}F(t)dt. \tag{5}$$

*Proof.* From (2.1), we have

$$F(z)=\frac{\alpha}{\alpha+\beta}f(z)+\frac{\beta}{\alpha+\beta}zf'(z),$$

and, using Theorem 2.1, we prove the result. □

**Theorem 2.3.** *Let $f\in\tilde{Q}_k(\alpha,\beta,\rho,\gamma),\quad \alpha,\beta>0$. Then, for $|z|=r\quad(0<r<1)$, we have*

$$|f(z)|\geq\frac{\alpha+\beta}{2A}\left[\frac{1}{\alpha}-\frac{r^{\frac{-\alpha}{\beta}}}{\beta}G(\left(\frac{\alpha}{\beta},A,B,-r\right)\right],$$

*where*

$$A=\left(\frac{k}{2}-1\right)(1-\rho)+\gamma+1,\quad B=A+\frac{\alpha}{\beta}, \tag{6}$$

*$G$ denotes the hypergeometric function and it is known to be analytic in $E$. This result is sharp as can be seen from the function $f_0\in\tilde{Q}_k(\alpha,\beta,\rho,\gamma),\alpha,\beta>$ defined by*

$$f_0(z)=\frac{(\alpha+\beta)}{\beta(k+2\gamma)}z^{\frac{-\alpha}{\beta}}\int_0^z\xi^{\frac{\alpha}{\beta}-1}\left\{1-\left(\frac{1-\xi}{1+\xi}\right)^{\frac{k}{2}+\gamma}\right\}d\xi. \tag{7}$$

*Proof.* We consider the straight line $\Gamma$ joining 0 to $f(z)=Re^{i\phi}$. $\Gamma$ is the image of a Jordan arc $\Gamma$ in $E$ connecting 0 to $z=re^{i\theta}$. The image of $\Gamma$ under the mapping $\left|z^{\frac{\alpha}{\beta}}f(z)\right|$ will consist of many line-segments emanating from the origin each of length

$$r^{\frac{\alpha}{\beta}}R=\left|z^{\frac{\alpha}{\beta}}f(z)\right|\quad=\quad\int_\Gamma\left|\frac{d}{d\xi}[\xi^{\frac{\alpha+\beta}{\beta}}f(\xi)]\right||d\xi|.$$

Since $f$ is in $\tilde{Q}_k(\alpha,\beta,\rho,\gamma)$, there exists $F \in T_k^\star(\rho,\gamma)$ such that

$$\frac{d}{d\xi}\left[\xi^{\frac{\alpha}{\beta}} f(\xi)\right] = \frac{1}{\beta} f^{\frac{\alpha}{\beta}-1} F(\xi).$$

Thus, if $t = |\xi|$, we deduce that

$$r^{\frac{\alpha}{\beta}} R = \frac{\alpha+\beta}{\beta} \int_\Gamma \left|\xi^{\frac{\alpha}{\beta}-1} F(\xi)\right| |d\xi|. \tag{8}$$

Now, for $F \in T_k^\star(\rho,\gamma)$, we have

$$|F(z)| \geq \frac{1}{2A}\left[1 - \left(\frac{1-r}{1+r}\right)^A\right], \tag{9}$$

where $A$ is defined by (2.2) and we have used (1.3) together with a result proved in [7]. Using (2.5) in (2.4), we have

$$\begin{aligned} R = |f(z)| &\geq \frac{r^{\frac{-\alpha}{\beta}}(\alpha+\beta)}{-2\beta A} \int_0^r t^{\frac{\alpha}{\beta}-1}\left[1 - \left(\frac{1-t}{1+t}\right)^A\right] dt \\ &= \frac{(\alpha+\beta)}{2A}\left[\frac{1}{\alpha} - \frac{1}{\beta} r^{\frac{-\alpha}{\beta}} \int_0^r t^{\frac{\alpha}{\beta}-1}(1-t)^A (1+t)^{-A} dt\right] \\ &= \frac{(\alpha+\beta)}{2A}\left[\frac{1}{\alpha} - \frac{r^{\frac{-\alpha}{\beta}}}{\beta}.G(\frac{\alpha}{\beta}, A, B, -r)\right]. \end{aligned}$$

This completes the proof. □

Letting $r \longrightarrow 1$ in Theorem 2.3, we obtain the following result.

**Theorem 2.4.** *Let $f \in \tilde{Q}_k(\alpha,\beta,\rho,\gamma)$, $(\alpha,\beta > 0)$. Then $f(E)$ contains the schliht disc*

$$|z| < \frac{\alpha+\beta}{(k-2)(1-\rho)+2\gamma+2}.$$

We now have the following.

**Theorem 2.5.** *A function $f \in \tilde{Q}_k(\alpha,\beta,0,\gamma)$ for $\alpha,\gamma >, \beta \geq 0$ belongs to $T_2^\star(0,\gamma)$ for $z \in E$.*

*Proof.* For $\beta = 0$, $\tilde{Q}_2(\alpha,0,0,\gamma) = T_2^\star(0,\gamma)$ and the result is obvious. We shall assume that $\beta > 0$.

Form (2.1), we note that, for $f \in \tilde{Q}_2(\alpha,0,0,\gamma)$,

$$f(z) = \phi_{\alpha,\beta}(z) \star F(z),$$

where $F \in T_2^\star(0,\gamma)$ and

$$\phi_{\alpha,\beta}(z) = \sum_{n=1}^{\infty}\left[\frac{(\alpha+\beta)}{\beta(n-1)+\alpha+\beta}\right] z^n.$$

Since $\phi_{\alpha,\beta}(z)$ is convex in $E$, see [8] and it is known that the class $T_2^\star(0,\gamma)$ is closed under convolution with convex functions [6], we conclude that $f \in T_2^\star(0\gamma)$. □

Using Theorem 2.1 and Theorem 2.5, we can easily show that the class $\tilde{Q}_2(\alpha,\beta,0,\gamma)$ is also closed under convolution with convex functions.

**Theorem 2.6.** *Let*

$$\frac{\alpha_1}{\alpha_1+\beta_1} < \frac{\alpha}{\alpha+\beta}, \quad \frac{\beta_1}{\alpha_1+\beta_1} < \frac{\beta}{\alpha_1+\beta_1}.$$

*Then, for* $z \in E$, $\quad \tilde{Q}_2(\alpha,\beta,0,\gamma) \subset \tilde{Q}_2(\alpha_1,\beta_1,0,\gamma)$.

*Proof.* Let $f \in \tilde{Q}_2(\alpha,\beta,0,\gamma)$. Then , for $z \in E$,

$$\begin{aligned}\frac{\alpha_1}{\alpha_1+\beta_1}\frac{f'(z)}{g'(z)} \quad + \quad & \frac{\beta_1}{\alpha_1+\beta_1}\frac{(zf'(z))'}{g'(z)} = \left(1-\frac{\beta_1(\alpha+\beta)}{\beta(\alpha_1+\beta_1)}\right)\frac{f'(z)}{g'(z)} \\ & +\frac{\beta_1(\alpha+\beta)}{\beta(\alpha_1+\beta_1)}\left[\frac{\alpha}{\alpha+\beta}\frac{f'(z)}{g'(z)}+\frac{\beta}{\alpha+\beta}\frac{(zf'(z))'}{g'(z)}\right] \\ = \quad & 1-\frac{\beta_1(\alpha+\beta)}{\beta(\alpha_1+\beta_1)}H_1(z)+\frac{\beta_1(\alpha+\beta)}{\beta(\alpha_1+\beta_1)}H_2(z) = H(z),\end{aligned}$$

and since $\tilde{P}(\gamma)$ is a convex set, it follows that $\quad H \in \tilde{P}(\gamma), z \in E$. This implies that $f \in \tilde{Q}_2(\alpha,\beta,0,\gamma)$. □

**Acknowledgement.** We would like to thank Dr. S. M. Junaid Zaidi, Rector, CIIT, for providing excellent research facilities.

## References

[1] K. Inayat Noor,*On Close-to-Convex and Related Functions,* PhD Thesis, University of Wales, Swansea, UK, 1972.
[2] K. Inayat Noor and D. K. Thomas, Quasi-convex univalent functions, *Inter. J. Math. Math. Sci.,* **3**(1980), 755-758.
[3] K. Inayat Noor, On quasi-convex functions and related topics, *Inter. J. Math. Math. Sci.,* **10**(1987), 241-258.
[4] K. Inayat Noor, On a generalization of close-to-convexity,*Inter. J. Math. Math. Sci.,* **6**(1983), 327-334.
[5] K. Inayat Noor, Higher order close-to-convex functions, *Math. Japonica,* **37**(1992), 1-8.
[6] K. Inayat Noor, On strongly close-to-convex functions, *Mathematics (Cluj),* **44(67)**(2002), 25-29.
[7] K. Inayat Noor, On a class related with strongly close-to-convex functions, *Mathematica (Cluj),* **44(67)**(2002), 191-199.
[8] S. Ruscheweyh, New criteria for univalent functions, *Proc. Amer. Math. Soc.,* **49**(1975), 109-115.

Mathematics Department,, COMSATS Institute of Information Technology,, Islamabad, PAKISTAN
*E-mail address*: khalidanoor@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 61–79
ISSN 1930-1235: (electronic version)

# RIEMANN HYPOTHESIS: A NUMERICAL TREATMENT OF THE RIESZ AND HARDY-LITTLEWOOD WAVE

STEFANO BELTRAMINELLI AND DANILO MERLINI

Abstract. We present the results of numerical experiments in connection with the Riesz and the Hardy-Littlewood criteria for the truth of the Riemann Hypothesis (RH). The coefficients $c_k$ of the Pochhammer expansion for the reciprocal of the Riemann Zeta function depend in our model on two parameters. The "critical functions" $c_k k^a$ (where $a$ is some constant), whose behaviour is concerned with the possible truth of the RH, are analysed at relatively large values of $k$. Some cases are numerically investigated up to larger values of $k$, i.e. $k = 10^9$ and more.

The $c_k$ we obtain in such a region have an oscillatory behaviour, which we call the Riesz and the Hardy-Littlewood wave. A special case is then studied numerically in some range of the critical strip. The numerical results give some evidence that the critical function is bounded for $\Re(s) > \frac{1}{2}$ and such an "evidence" is stronger in the region $\Re(s) > \frac{3}{4}$ where the wave seems to decay slowly. This give further support in favour of the absence of zeros of the Riemann Zeta function in some regions of the critical strip ($\Re(s) > \frac{3}{4}$) and a (weaker) support in the direction to believe that the RH may be true ($\Re(s) > \frac{1}{2}$).

The amplitudes and the wavelength of the wave obtained by our numerical treatment are then compared with those formulated by Baez-Duarte in his analytical approach. The agreement is satisfactory.

Finally for another special case we found that the wave appears to be bounded even though one parameter in our model grows to infinity. Our analysis suggests that RH may barely be true and it is argued that an absolute bound on the amplitudes of the waves in all cases, should be given by $|\frac{1}{\zeta(\frac{1}{2}+\epsilon)} - 1|$, with $\epsilon$ arbitrarily small positive, i.e. equal to 1.68477....

## 1. Introduction

Following recent works concerning the study of some well known functions appearing in the original criteria of Riesz, Hardy and Littlewood and involving the Riemann Hypothesis (RH), there is new interest in the direction of numerical experiments, where the calculations use the ideas of some modern works on the subject. These ideas concern the expansion of the reciprocal of the Riemann Zeta function in terms of the so called Pochhammer polynomials $P_k$, whose coefficients $c_k$ play a central role also in the asymptotic region of very large $k$.

1991 *Mathematics Subject Classification.* 11M26.

*Key words and phrases.* Riemann's Zeta function, Riemann Hypothesis, Criteria of Riesz, Hardy-Littlewood and Baez-Duarte, Pochhammer's polynomials.

Here we are concerned with the discrete version of the Riesz criterion which has also been studied numerically: the first numerical experiments have been announced and reported for the Riesz case. It has been found that the function $c_k$ has an oscillatory behaviour in a region of relatively high $k$, in agreement with an asymptotic formula given by Baez-Duarte and involving the non-trivial zeros of the Zeta function. The agreement appears satisfactory even if only the contribution of few non-trivial zeros has been used.

In our previous paper, appeared in the first Number of this Journal, a two parameters family (parameter $\alpha$ and $\beta$) of Pochhammer's polynomials was introduced. This allowed the starting investigation of $c_k$ at low values of $k$, but in various cases and in the so called "strong coupling" regime (high $\beta$). After the initial study at low $k$, our computations using the formula containing the Möbius function were easily extended to larger and larger $k$ (up to a billion) in the strong coupling limit, with the appearance of macro-oscillations in $c_k$ extending to larger $k$. This is a symptom that using such a limit the RH may eventually barely be true. In this paper we continue the numerical experiments partially using our Poisson formula already established in and which is well suited for numerical purposes.

After the formulation of the model and the definition of the statement "critical function" in Section 2, we then give in Section 3 an asymptotic formula (the Baez-Duarte formula) to compute it. This formula involves the trivial and not-trivial zeros of the Riemann Zeta function. The next three sections are dedicated to the numerical experiments. Our aim is twofold: first we will analyse the correctness of this asymptotic formula and second we will investigate the behaviour of the critical function whose boundedness will ensure the truth of the RH. In Section 4 the amplitudes of what we call the Riesz and Hardy-Littlewood wave are calculated in some cases using the Baez-Duarte formula. We then present our results for these different models up to values of $k$ equal to one billion and observe oscillations in all cases. These oscillations are compatible with the calculated amplitudes: the agreement with the asymptotic formula of Baez-Duarte is satisfactory. In Section 5, we concentrate our study in more details by considering a special new model already proposed where $\alpha = \frac{7}{2}$ and $\beta$ is increasing starting with the value equal to 4. The results show in a concrete way the "transition" from the low coupling to the "strong coupling regime": at low values of $\beta$ ($\beta = 4$) we obtain up to 7 oscillation with values of $k$ extending up to a billion. These start to deform continuously with increasing values of $\beta$ approaching the infinite $\beta$ limit. In such a regime, the wave is absorbed in a macroscopic region with an amplitude whose strength should be finite as already noted in our previous work. Also in these cases the agreement with the asymptotic formula is satisfactory. In Section 6 we analyse the behaviour of the critical function in the critical strip and the contribution to it of the non-trivial zeros. Moreover, the possibility that in an ideal numerical experiment (using an arbitrarily large but finite maximum value of $n$, say $N$ in the formula with the Möbius function) the amplitude of the waves at finite $\beta$ values should be bounded, is commented in Section 7.

## 2. The model

The starting point of this work is the representation of the reciprocal of the Riemann Zeta function by means of the Pochhammer polynomials $P_k(s)$ (where $s$ is

a complex variable, $s = \sigma + it$), whose coefficients $c_k$ have been introduced by Baez-Duarte for the Riesz case ($\alpha = \beta = 2$). For the study of the coefficients $c_k$, some recent analytical as well as numerical results have been obtained [1, 2, 3, 4, 5, 6, 7].

Using the Baez-Duarte approach, the representation of $\frac{1}{\zeta(s)}$ may be obtained for a family of two parameters Pochhammer polynomials (parameters $\alpha > 1$ and $\beta > 0$) and by [3] we have:

$$\frac{1}{\zeta(s)} = \sum_{k=0}^{\infty} c_k(\alpha, \beta) P_k(s; \alpha, \beta) \tag{2.1}$$

where

$$P_k(s; \alpha, \beta) \quad := \prod_{r=1}^{k} \left(1 - \frac{\frac{s-\alpha}{\beta}+1}{r}\right) \tag{2.2}$$

$$c_k(\alpha, \beta) \quad := \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}} \left(1 - \frac{1}{n^{\beta}}\right)^k \tag{2.3}$$

and $P_0(k; \alpha, \beta) = 1$.

In (2.3) the Möbius function of argument $n$ is given by:

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1 \\ (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ 0, & \text{if } n \text{ contains a square.} \end{cases}$$

One has for $\Re(s) = \sigma > 1$:

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \tag{2.4}$$

so another explicit formula for the $c_k(\alpha, \beta)$ is obtained from (2.3) using the binomial coefficients and reads:

$$c_k(\alpha, \beta) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \frac{1}{\zeta(\alpha + \beta j)} \tag{2.5}$$

As $\beta$ is increasing, one may also use (especially) in the context of numerical experiments, the formula recently obtained [3] and given by:

$$c_k(\alpha, \beta) \cong \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}} e^{-\frac{k}{n^{\beta}}} \tag{2.6}$$

In such an approximation we have that

$$c_k(\alpha, \beta) \cong \sum_{p=0}^{\infty} c_p(\alpha, \beta) \frac{k^p}{p!} e^{-k} \tag{2.7}$$

which shows the emergence of a Poisson like distribution for the coefficients $c_k(\alpha, \beta)$. This should be a very satisfactory approximation [3].

We recall that an important inequality due to Baez-Duarte [1, 2] concerning the Pochhammer polynomials of complex argument $z$ is given by:

$$|P_k(z)| \leq C k^{-\Re(z)} \tag{2.8}$$

TABLE 1. The expected decay of $c_k$ for different values of $\alpha$ and $\beta$ ($\sigma = \frac{1}{2}$)

| $\alpha$ | $\beta$ | decay of $\lvert c_k \rvert$ | Note |
|---|---|---|---|
| 2 | 2 | $k^{-\frac{3}{4}}$ | The case of Riesz |
| 1 | 2 | $k^{-\frac{1}{4}}$ | The case of Hardy-Littlewood |
| 2 | 6 | $k^{-\frac{1}{4}}$ | Same decay as the Hardy-Littlewood case but numerically more convenient |
| $\frac{7}{2}$ | 4 | $k^{-\frac{3}{4}}$ | Same decay as the Riesz case, intensive calculations are given below |
| 3 | 3 | $k^{-\frac{5}{6}}$ | If the Zeta function has no zero for $\Re(s) > \frac{3}{4}$ then $c_k(3,3)$ should decay at least as $k^{-\frac{3}{4}}$ |
| 4 | 4 | $k^{-\frac{7}{8}}$ | Since from the Prime Number Theorem there is no zero for $\Re(s) \geq 1$ the $c_k(4,4)$ decays at least as $k^{-\frac{3}{4}}$ |
| 2 | 4 | $k^{-\frac{3}{8}}$ | Another interesting case for calculations |

The above inequality applied to our two parameters family of Pochhammer's polynomials with complex argument $z = \frac{s-\alpha}{\beta} + 1$ gives:

$$\left| P_k(\frac{s-\alpha}{\beta} + 1; \alpha, \beta) \right| \leq C k^{-\left(\frac{\sigma-\alpha}{\beta}+1\right)} \tag{2.9}$$

So that $\zeta(s)$ in (2.1) will be different from zero and thus the RH will be true for $\Re(s) = \sigma > \frac{1}{2}$ if the sequence $c_k$ decays, at large $k$, as (see [3]):

$$|c_k| \leq A k^{-\frac{\alpha-\sigma}{\beta}} \tag{2.10}$$

We will also consider the "critical function" $\psi$ defined by:

$$\psi(k; \alpha, \beta, \sigma) := c_k k^{\frac{\alpha-\sigma}{\beta}} \tag{2.11}$$

which from (2.10) is expected to be bounded by a constant $A$.

We now recall two original cases given in pionnering works by Riesz [8] and by Hardy-Littlewood [9]. Setting $\sigma = \frac{1}{2}$ in (2.10), for $\alpha = \beta = 2$ (Riesz case) we have that $|c_k| \leq A k^{-\frac{3}{4}}$ and for $\alpha = 1$, $\beta = 2$ (Hardy-Littlewood case), $|c_k| \leq A k^{-\frac{1}{4}}$. Other interesting cases for which we will carry out intensive numerical experiments to be presented below are summarized in Table 1.

A limiting delicate case analysed in [3] is the one where $\alpha = \frac{1}{2} + \delta$ and $\beta$ grows to infinity. Here of course we do not have absolute convergence to $\frac{1}{\zeta(s)}$ ($c_k$ may nevertheless be analysed) and from (2.10) we have that the $c_k$ should be smaller than a constant for all $k$. This is what we verified with numerical experiments (not presented here) with values of $k$ up to a billion. The value of the constant has been proposed in our previous work [3] and the conjecture was that $|c_k| \leq |\frac{1}{\zeta(\frac{1}{2})} - 1| \cong 1.68477$. However the situation is delicate ($\alpha < 1$) since Littlewood [9] has shown that, assuming RH is true, $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\frac{1}{2}+\epsilon}}$ is convergent for all $\epsilon$ strictly greater than zero.

The general situation is that the "critical function" $c_k k^{\frac{\alpha-\sigma}{\beta}}$ should be bounded by a constant in absolute value as $k \to \infty$. In fact the sequence starts at zero

for $k = 0$, reaches a minimum, then starts to increase and then begins to oscillate with a "constant " amplitude as $k \to \infty$ as we will see in the experiments. In the previous work [3] we have analysed $c_k$ in various cases but only for moderately values of $k$, i.e. for $k$ not exceeding 1000, with exception of some cases at large values of $\beta$, where $k$ reached the value of a half billion. $c_k$ was found to have only negative values in the range considered and increasing with $k$. Presently, we know of recent numerical experiments in the Riesz case carried out by K. Maslanka [6] ($k$ up to $10^6$), J. Cislo and M. Wolf [4] ($k$ up to $10^6$) and M. Wolf ($k$ up to $10^9$) where the calculations indicate that the sequence $c_k$ becomes of oscillatory type, thus assuming positive and negative values. In fact two or three oscillations with a wavelength related in first approximation to the first zero of the Riemann Zeta function has been seen. Here it should be remarked that this situation for the Riesz case is not in contraddiction with our strong coupling limit ($\beta$ large) cited above (see discussion below for the case $\alpha = \frac{7}{2}$ and $\beta$ increasing).

In few of these new finding, we want first analyse (in an analytical context) such a behaviour and we call this general phenomena the Riesz and the Hardy-Littlewood wave. This will be analysed using an interesting result of Baez-Duarte, i.e. an expression giving $c_k$ for $k \to \infty$.

## 3. The Riesz and the Hardy-Littlewood wave

For the Riesz case, in connection with the Mellin inversion formula, the Riesz function is given (see [8] and [10]) explicitly by:

$$F(x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1} x^k}{(k-1)!\zeta(2k)} \tag{3.1}$$

Using the calculus of residues *F(x)* is obtained by an integration and is given by:

$$F(x) = \frac{i}{2\pi} \int_{a-i\infty}^{a+i\infty} \frac{\Gamma(1-s)x^s}{\zeta(2s)} ds \tag{3.2}$$

where $\frac{1}{2} < a < 1$.

Recently Baez-Duarte [2], with an ingenious method found in particular an expression for the reciprocal of the Pochhammer polynomial given by:

$$\frac{1}{P_k(s)} = \sum_{j=1}^{k} (-1)^j \binom{k}{j} \frac{j}{s-j} \tag{3.3}$$

and one has uniformely on compact subsets:

$$\lim_{k \to \infty} P_k(s) k^s = \frac{1}{\Gamma(1-s)} \tag{3.4}$$

Moreover he was able to obtain an explicit formula connecting $c_k$ and the set of all trivial and non-trivial zeros (let $\rho$ denote a complex Zeta zero) under the assumption of simple zeros. For the Riesz case and for sufficiently large $k$ the expression is given by:

$$-2kc_{k-1} = \sum_{\rho} \frac{1}{\zeta'(\rho) P_k(\frac{\rho}{2})} + o(1) \tag{3.5}$$

TABLE 2. The "amplitude" of $\psi$ for different values of $\alpha$ and $\beta$, calculated with (3.8)

| $\alpha$ | $\beta$ | The function | The amplitude |
|---|---|---|---|
| 2 | 2 | $\lvert\psi(k;2,2,\frac{1}{2})\rvert = \lvert k^{\frac{3}{4}} c_k\rvert$ | 0.0000777506 |
| 1 | 2 | $\lvert\psi(k;1,2,\frac{1}{2})\rvert = \lvert k^{\frac{1}{4}} c_k\rvert$ | 0.0000292558 |
| 2 | 6 | $\lvert\psi(k;2,6,\frac{1}{2})\rvert = \lvert k^{\frac{1}{4}} c_k\rvert$ | 0.0210433 |
| $\frac{7}{2}$ | 4 | $\lvert\psi(k;\frac{7}{2},4,\frac{1}{2})\rvert = \lvert k^{\frac{3}{4}} c_k\rvert$ | 0.00841095 |
| 3 | 3 | $\lvert\psi(k;3,3,\frac{1}{2})\rvert = \lvert k^{\frac{5}{6}} c_k\rvert$ | 0.00215622 |
| 4 | 4 | $\lvert\psi(k;4,4,\frac{1}{2})\rvert = \lvert k^{\frac{7}{8}} c_k\rvert$ | 0.00984936 |
| 2 | 4 | $\lvert\psi(k;2,4,\frac{1}{2})\rvert = \lvert k^{\frac{3}{8}} c_k\rvert$ | 0.00524454 |

$o(1)$ can be written explicitly in terms of the trivial zeros. It should be said that formula (3.5) of Baez-Duarte is very nice and may be used to control our numerical computations at large $k$ to be presented below. Apparently (3.5), with some precautions, may be extended to our general model with parameters $\alpha$, $\beta$ (2.1) and should read:

$$-\beta k c_{k-1} = \sum_{\rho} \frac{1}{\zeta'(\rho) P_k(\frac{\rho-\alpha}{\beta}+1)} + o(1) \tag{3.6}$$

Then using (3.4) in (3.6) we can compute for large $k$ the following approximated expression for the "critical function" (we call it the Riesz and the Hardy-Littlewood wave) $\psi$:

$$\psi(k;\alpha,\beta,\sigma) = k^{\frac{\alpha-\sigma}{\beta}} c_k \cong \psi_{nt}(k;\alpha,\beta,\sigma) + \psi_t(k;\alpha,\beta,\sigma) \tag{3.7}$$

where $\psi_{nt}$ and $\psi_t$ are the contributions of the non-trivial respectively trivial zeros of the Zeta function. They are given by:

$$\psi_{nt}(k;\alpha,\beta,\sigma) = \frac{1}{\beta} \sum_{\rho} \frac{k^{\frac{\rho-\sigma}{\beta}} \Gamma(\frac{\alpha-\rho}{\beta})}{\zeta'(\rho)} \tag{3.8}$$

and

$$\psi_t(k;\alpha,\beta,\sigma) = \frac{1}{\beta} \sum_{n=1}^{\infty} \frac{k^{-\frac{2n+\sigma}{\beta}} \Gamma(\frac{\alpha+2n}{\beta})}{\zeta'(-2n)} \tag{3.9}$$

We concentrate our numerical research on three topics: the amplitude of the Riesz and the Hardy-Littlewood wave in the long wavelength limit ($k$ large) for the special case $\sigma = \frac{1}{2}$, the case where we steadily increase the parameter $\beta$ and finally its behaviour for different values of $\sigma$ (that is inside the critical strip).

## 4. NUMERICAL EXPERIMENTS: THE "AMPLITUDE" OF THE CRITICAL FUNCTION

In the limit of large $k$, one may consider to neglect the contribution of the trivial zeros in (3.7) [2]. To prepare the comparison of (3.8) with the numerical results we write it explicitly for the various cases we will treat. In order to obtain an estimate for the amplitude of the wave in the long wavelength limit ($k$ large) we will use in (3.8) only the first zero and its complex conjugate up to 10 decimals ($\beta$ small). Setting the first derivative of (3.8) to zero and solving the equation with *Mathematica*, we obtain the data in Table 2.

The values for the amplitude of the waves in Table 2 will be compared with the results of the numerical experiments performed for the various cases using (2.3).

Our numerical experiments was carried out in more cases using the Möbius function in (2.3) up to $n = 10^6$ and we calculated $c_k$ until $k = 10^6$ or $k = 10^8$ with a sample interval of 2500 for the $k$-axis. The general situation is that at moderately values of $k$ (until some thousand) the wave given by the experimental results starts with zero amplitude, after a minimum with a negative value, increases and seems to stabilize at large values of $k$ with oscillations displaced at larger and larger wavelength (proportional to $\log k$) and with an amplitude which seems to saturate to a constant value (given in a good approximation) by the values in Table 2. Below (Figure 1) we first give the plot of the wave for the Riesz case ($\alpha = \beta = 2$). As already remarked in [2], the first intensive calculations by K. Maslanka, J. Cislo and M. Wolf indicate the appearance of oscillations with the first one in the region $k = 20000$. Our results obtained with (2.3) confirm for such values the asymptotic limit for the wave with an amplitude in agreement with the constant obtained above ($A \cong 0.000078$).

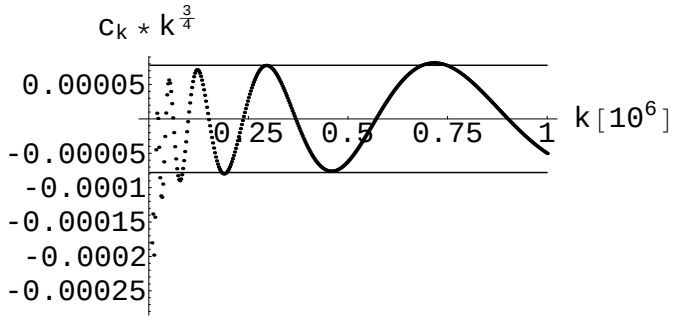



FIGURE 1. The wave $k^{\frac{3}{4}}c_k$ for the Riesz case $\alpha = \beta = 2$

Figure 2 and Figure 3 concern two cases of special interest since the decays of $c_k$ are expected to be the same as for the Hardy-Littlewood case and for the Riesz case. In both cases there is agreement with the "amplitude" $A \cong 0.0210433$ and $A \cong 0.008411$ given above but the amplitudes are respectively 1000 and 100 time bigger than in the first case.

In Figure 4 and Figure 5 we give the plots of $k^{\frac{5}{6}}c_k(3,3)$ and $k^{\frac{7}{8}}c_k(4,4)$ where the amplitudes are still found to be in agreement with the theoretical values given above in Table 2.

The next special case is the one with $\alpha = 2$ and $\beta = 4$. Again, the experimentally detected amplitude agrees well with the theoretical value calculated above, i.e. $A = 0.0052445$ (Figure 6).

## 5. Numerical experiments: $\beta$ increasing

For $\alpha = \frac{7}{2}$ we will now present the plots of the waves for an increasing sequence of $\beta$ values i.e. 4, 8, 12, and 20 (in order to investigate the "infinite beta limit"

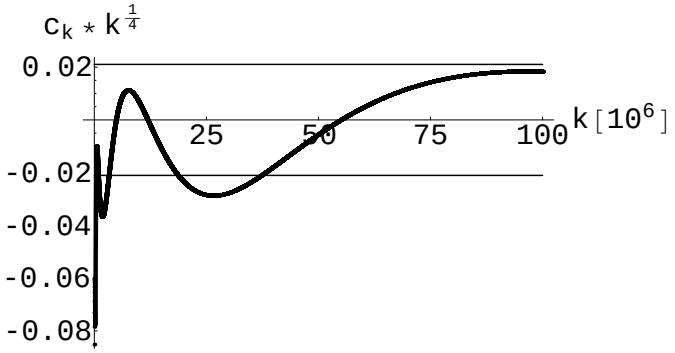



FIGURE 2. The wave $k^{\frac{1}{4}}c_k$ for the case $\alpha = 2, \beta = 6$

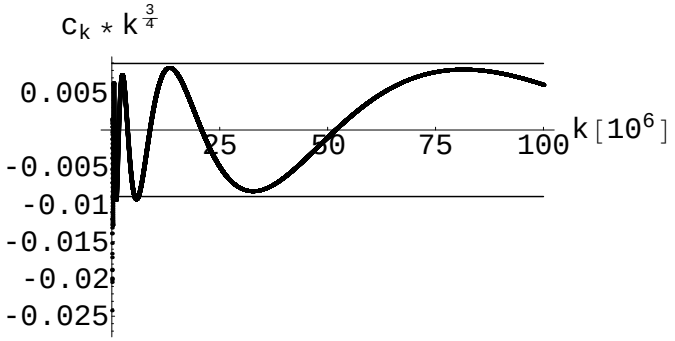



FIGURE 3. The wave $k^{\frac{3}{4}}c_k$ for the case $\alpha = \frac{7}{2}, \beta = 4$

already introduced in our previous work [3]). We will compute the function

$$\psi(k; \frac{7}{2}, \beta, \frac{1}{2}) = k^{\frac{3}{\beta}} c_k(\frac{7}{2}, \beta) \tag{5.1}$$

which will also be compared with the expression given by the Baez-Duarte formula (3.8) in the asymptotic region $k \to \infty$, i.e. $\psi_{nt}(k; \frac{7}{2}, \beta, \frac{1}{2})$. Here we will take into account only the contribution of the groundstate of the spectrum i.e. $\rho = \frac{1}{2} + 14.134725141i$ and its complex conjugate $\overline{\rho}$. It is then convenient to introduce the new variable $x = \log k$. This allow us to control more efficiently the wavelength and the amplitude of the wave in the region to be considered ($x$ runs from 8 to 22, so $k$ up to $3.6 \times 10^9$).

In the Figures 7-10 we present our numerical results for increasing $\beta$ values, which we call the "strong coupling limit". In the range $\log k > 10$ the two waves are walking close together arm in arm at least for $\beta = 4$ (Figure 7). This confirms

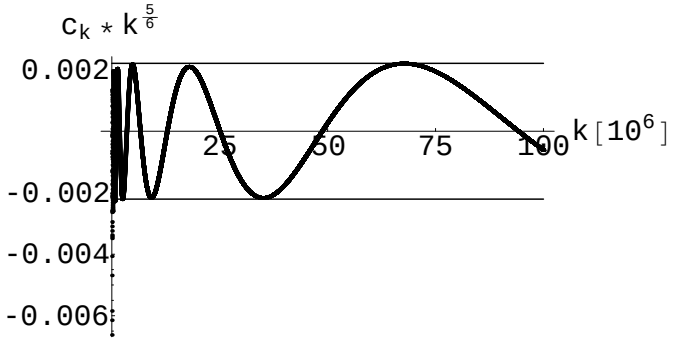



FIGURE 4. The wave $k^{\frac{5}{6}}c_k$ for the case $\alpha = \beta = 3$

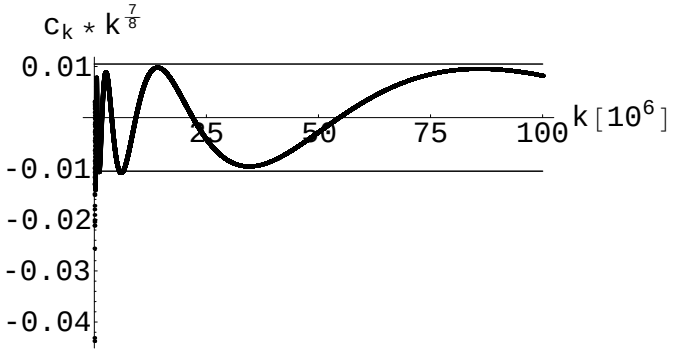



FIGURE 5. The wave $k^{\frac{7}{8}}c_k$ for the case $\alpha = \beta = 4$

that the contribution of the first zero ($\rho = \frac{1}{2} + 14.134725141i$ and $\overline{\rho}$) appears to be dominant at low values of $\beta$.

At the same time one can see that in this case $|c_k|$ itself is smaller than ($c_k$ is not the critical function!):

$$\left| \frac{1}{\zeta(\frac{7}{2})} - 1 \right| \cong 0.11247897 \tag{5.2}$$

at least for the case $\beta = 4$ as already discussed in our previous work [3] concerning only very low values of $k$. Figure 11 confirms this behaviour also for large values of $k$. In this example the region of annihilation of the "eincoming" wave extends up to larger and larger values of $k$. It should be noted that for the critical function $\psi$ (5.1) the situation is more delicate since the value of a possible bound on $\psi$ depends on $\beta$.

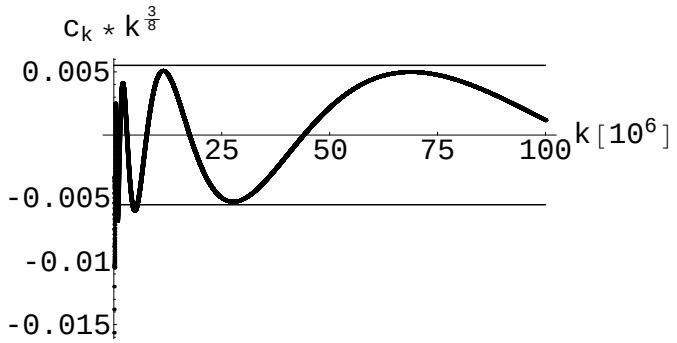



FIGURE 6. The wave $k^{\frac{3}{8}}c_k$ for the case $\alpha = 2, \beta = 4$

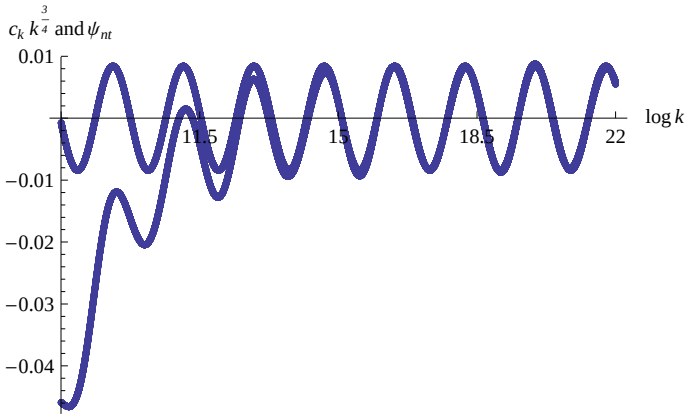



FIGURE 7. The wave $k^{\frac{3}{4}}c_k$ (lowest curve) and the approximation $\psi_{nt}$ (highest curve), $\alpha = \frac{7}{2}$ and $\beta = 4$

## 6. Numerical experiments: the critical function in the critical strip

As above, in this numerical study it is convenient to introduce the variable $x = \log k$, in term of which we define the critical function corresponding to $\alpha$ and $\beta$. With the help of (2.6), this is given in the next calculations by:

$$\psi(x;\alpha,\beta,\sigma) = e^{\frac{\alpha-\sigma}{\beta}x}\sum_{n=1}^{2000}\frac{\mu(n)}{n^{\alpha}}e^{-\frac{e^x}{n^{\beta}}} =: \psi_{\sigma}(x) \tag{6.1}$$

2000 is the maximum argument $N$ used in these experiments. For the special case we treat ($\alpha = \frac{15}{2}$ and $\beta = 4$) $\psi$ will be calculated up to $x = 30$ (this corresponds to $k = e^{30} = 1.06865 \times 10^{13}$).

Before we present the results of our numerical experiments for various values of $\sigma$ (for $\sigma = 1, \frac{7}{8}, \frac{3}{4}, \frac{5}{8}, \frac{1}{2}, \frac{3}{8}, \frac{3}{10}$) it is important to give the explicit expression of the contribution of the non-trivial ($\psi_{nt}$) and also of the trivial zeros ($\psi_t$) to the critical

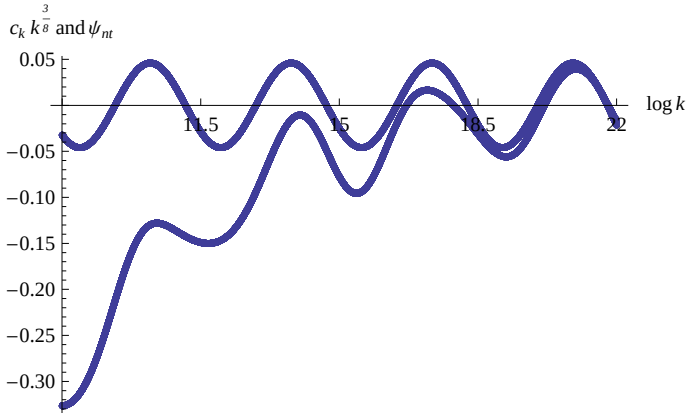



FIGURE 8. The wave $k^{\frac{3}{8}}c_k$ (lowest curve) and the approximation $\psi_{nt}$ (highest curve), $\alpha = \frac{7}{2}$ and $\beta = 8$

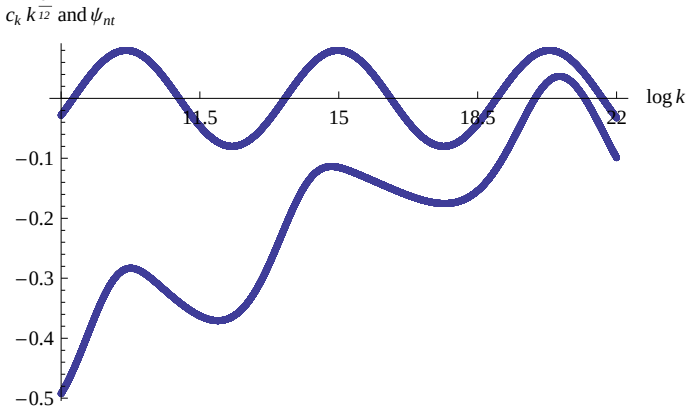



FIGURE 9. The wave $k^{\frac{3}{12}}c_k$ (lowest curve) and the approximation $\psi_{nt}$ (highest curve), $\alpha = \frac{7}{2}$ and $\beta = 12$

function defined above for the general case $\alpha$ and $\beta$. For the non-trivial zeros at $\sigma$, it is given by:

$$\psi_{nt}(x;\alpha,\beta,\sigma) = \frac{1}{\beta}\sum_{j=1}^{2}\frac{e^{\frac{i\Im(\rho_j)}{\beta}x}\Gamma(-\frac{\rho_j-\alpha}{\beta})}{\zeta'(\rho_j)} \tag{6.2}$$

where $\rho_j$ is a non-trivial zero of $\zeta(s)$. In our experiments we will limit to the contribution of the first two lower zeros given experimentally by $\rho_1 = \frac{1}{2}+14.134725i$ and $\rho_2 = \frac{1}{2} + 21.022040i$ and the complex conjugate of them. The corresponding contribution will be denoted by $r_1(x)$ (from $\rho_1$ and $\overline{\rho}_1$) and $r_2(x)$ (from $\rho_2$ and $\overline{\rho}_2$).

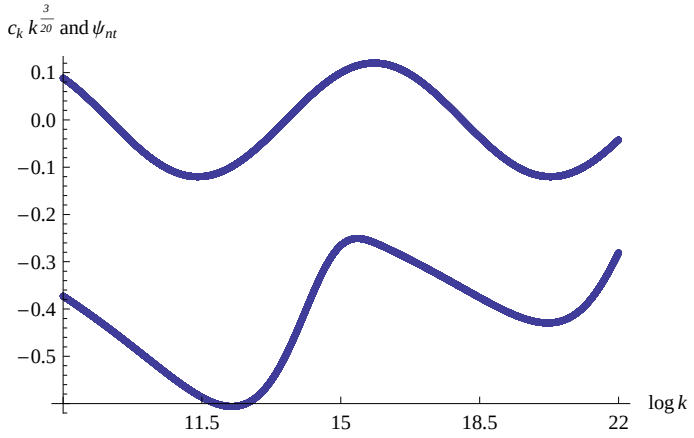



FIGURE 10. The wave $k^{\frac{3}{20}}c_k$ (lowest curve) and the approximation $\psi_{nt}$ (highest curve), $\alpha = \frac{7}{2}$ and $\beta = 20$

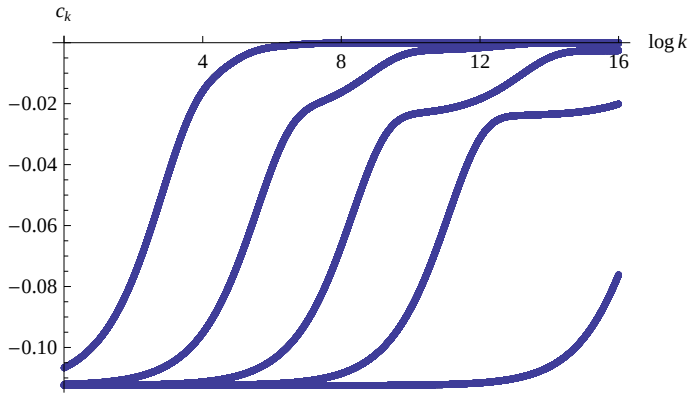



FIGURE 11. $c_k(\frac{7}{2}, \beta)$ for $\beta = 4, 8, 12, 16, 24$ (from left to right)

The contribution of the trivial zeros $\rho = -2n$ to the critical function is given by:

$$\psi_t(x; \alpha, \beta, \sigma) = \frac{1}{\beta} \sum_{n=1}^{20} \frac{e^{-\frac{2n+\sigma}{\beta}x} \Gamma(\frac{\alpha+2n}{\beta})}{\zeta'(-2n)} \tag{6.3}$$

where a summation until $N = 20$ will be sufficient.

So, in our calculations we will set $\alpha = \frac{15}{2}$ and $\beta = 4$ in the above formulas, for any value of $\sigma$ we shall consider. The contribution $\psi_t$ for $\sigma$ will be indicated with $g_\sigma(x)$. Below we present the results of our numerical experiments performed using *Mathematica*. The fluctuation's errors in the Möbius function around the maximum index $N = 2000$ will be specified in Section 7.

In Figure 12 we present the plot of the two functions $\psi(x; \frac{15}{2}, 4, \frac{1}{2}) - g_{1/2}(x)$ and $r_1(x) + r_2(x)$ up to $x = 30$ which shows not only a good agreement but also the oscillatory behaviour of the contribution of the first two non-trivial zeros. Note

that for the Riesz case ($\alpha = \beta = 2$), the contribution of the trivial zeros to the $c_k$ have been treated by K. Maslanka using the Rice integrals [6].

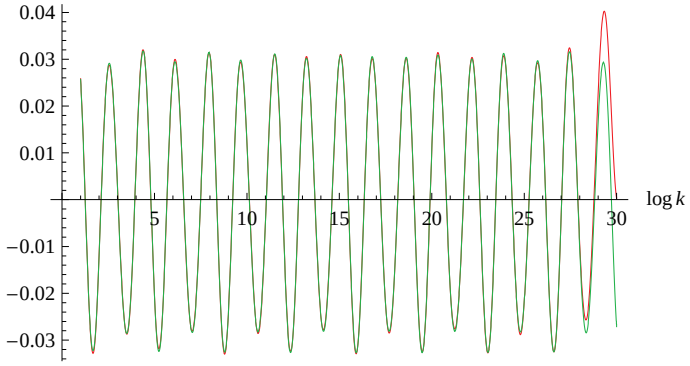



FIGURE 12. Plot of $\psi_{1/2}(x) - g_{1/2}(x)$ [red] and $r_1(x) + r_2(x)$ [green] up to $x = 30$

In the next Figure 13 we present the plots of some critical functions $\psi_\sigma$ corresponding to different values of $\sigma$ using (6.1) and this without any comparison with the Baez-Duarte asymptotic expansion considered above. It is to be noted that all functions $\psi_\sigma$ has the same zeros and we observe that there is a well marked evidence that for $\sigma > \frac{1}{2}$ increasing to 1 the amplitudes decay while for $\sigma < \frac{1}{2}$ the amplitudes grow. These functions have been indicated with $\psi_1$, $\psi_{7/8}$, $\psi_{3/4}$, $\psi_{5/8}$, $\psi_{1/2}$, $\psi_{3/8}$, $\psi_{3/10}$ respectively.

It should be said that $\psi_{3/8}$ and $\psi_{3/10}$, we have considered, have no relation with the representation of $\frac{1}{\zeta(s)}$ which is valid only for $\Re(s) > \frac{1}{2}$. The two functions help only to visualize that $\psi_{1/2}$ is the borderline for the critical functions decaying for $\Re(s) > \frac{1}{2}$ as suggested by our numerical experiments up to $x = 30$. It should also be added that from the duality relation (Riemann's symmetry of the Zeta function), given by:

$$\frac{1}{\zeta(1-s)} = \pi^{s-\frac{1}{2}} \frac{\Gamma(\frac{1-s}{2})}{\Gamma(\frac{s}{2})} \frac{1}{\zeta(s)} \tag{6.4}$$

it follows that the right hand side of (6.4) ensures a representation of $\frac{1}{\zeta(s)}$ via the Pochhammer polynomials in the region $0 < \Re(s) < \frac{1}{2}$.

Here there is more evidence that the amplitude of the wave at $\sigma = \frac{1}{2}$ is decreasing with $x = \log k$. The experiments of Figure 13 give in any cases a stronger evidence: for $\sigma > \frac{3}{4}$ the amplitudes of the waves are decaying, and thus are bounded in amplitude by a constant. This is a symptom of the absence of non-trivial zeros in the critical segment $\frac{3}{4} < \sigma < 1$.

In Figure 14 we present the result for a special case where we allow a slower decrease in the critical function (see addendum in the exponent of the critical function), which is the same as to say that we ask only for a slower decay of $c_k$, at $\sigma = \frac{1}{2}$ i.e. of the type $c_k = \frac{A \log k}{k^{\frac{7}{4}}}$ for the case considered. This is not the same as to ask that the RH is true or that the RH is true with non-trivial zeros which are simple [2]. It is a case in between the two.

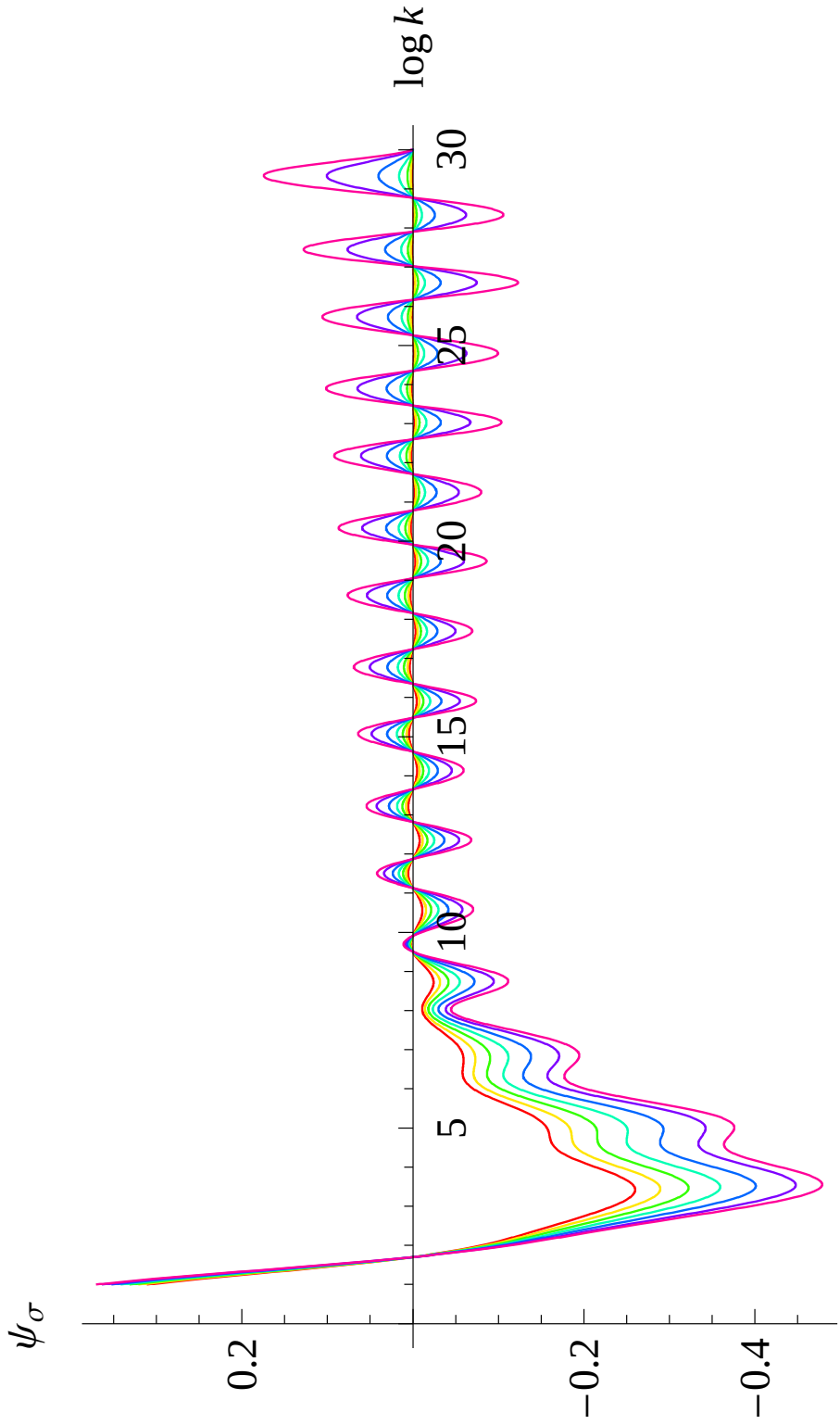



FIGURE 13. Plot of $\psi_\sigma$ for $\sigma = 1, \frac{7}{8}, \frac{3}{4}, \frac{5}{8}, \frac{1}{2}, \frac{3}{8}, \frac{3}{10}$ up to $x = 30$, in order of increasing amplitudes

In this case the critical function (indicated with $\psi_{1/2+}$) is explicitly given by:

$$\psi_{1/2+}(x) = e^{\frac{7}{4}x - \log x} \sum_{n=1}^{2000} \frac{\mu(n)}{n^{\frac{15}{2}}} e^{-\frac{e^x}{n^4}} \tag{6.5}$$

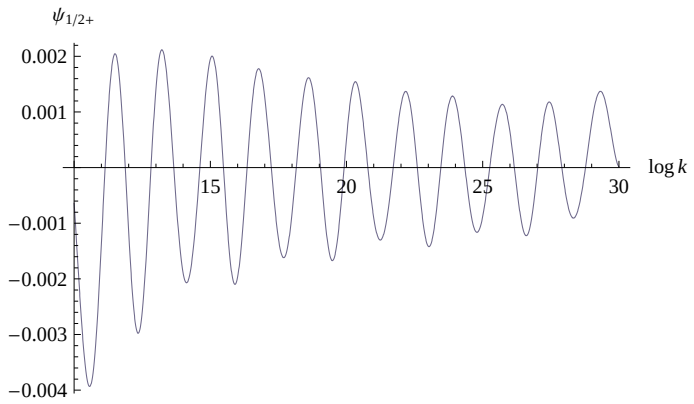



FIGURE 14. Plot of $\psi_{1/2+}$

In the last experiment we set $\sigma = \frac{3}{4}$ and compare $\psi_{3/4}$ with the asymptotic expression of Baez-Duarte: for the trivial zeros we set $\sigma = \frac{3}{4}$ in the above formula, for the non-trivial zeros (the two we consider) we keep the same value of $\Im(\rho_{1,2})$ but we assume that their real part is $\Re(\rho_{1,2}) = \frac{3}{4}$. The plot in Figure 15 of the function $\psi_{3/4}(x)$ and of $g_{3/4}(x) + r_1(x) + r_2(x)$ are clearly different: in $\psi_{3/4}$ there is the trace via the Möbius function of where the non-trivial zeros are located and thus the amplitude is decaying. In the second function, the two considered zeros are supposed to have $\Re(s) = \frac{3}{4}$ and the wave which appears seems to have a constant amplitude as in the case $\psi_{1/2}$ which of course would be sufficient to ensure the truth of the RH.

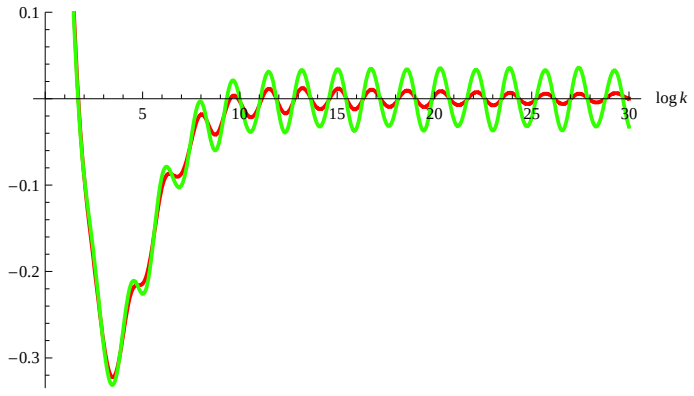



FIGURE 15. Plots of the functions $\psi_{3/4}(x)$ [red] and $g_{3/4}(x) + r_1(x) + r_2(x)$ [green]

In the next Section we analyse a (weak) stability property of our results obtained with $N = 2000$ in the Möbius function and give some indications why the waves for $\sigma = \frac{3}{4}$ should be decaying, thus ensuring more credibility on the absence of zeros of the Riemann Zeta function in the segment $\frac{3}{4} < \sigma < 1$.

## 7. Numerical considerations

In the context of the numerical experiments performed so far, it is helpful to obtain a crude inequality concerning a bound on the critical function. This is simply obtained by setting $|\mu(n)| = 1$ in (2.3). We consider the critical function for $\sigma = \frac{1}{2}$ given by:

$$k^{\frac{\alpha-\frac{1}{2}}{\beta}} c_k \cong k^{\frac{\alpha-\frac{1}{2}}{\beta}} \sum_{n=1}^{N} \frac{\mu(n)}{n^\alpha} \left(1 - \frac{1}{n^\beta}\right)^k =: \psi_k(\alpha, \beta, N)$$

where $N$ is the maximum value of the argument in the Möbius function considered in an ideal numerical experiment ($N$ finite). Introducing the variable $x = \log k$ we have that:

$$|\psi_k(\alpha, \beta, N)| \leq e^{\frac{\alpha-\frac{1}{2}}{\beta} x} (\zeta(\alpha) - 1) e^{\log(1-\frac{1}{N^\beta}) e^x}$$

For large $N$ we have:

$$|\psi_k(\alpha, \beta, N)| \leq (\zeta(\alpha) - 1)\, e^{\frac{\alpha-\frac{1}{2}}{\beta} x - \frac{1}{N^\beta} e^x}$$

As an example we consider the case $\alpha = \frac{7}{2}$ and $\beta = 4$ (Section 4). Remembering that from Table 2 the amplitude calculated only with the first non-trivial zero is about 0.008411, we may ask: for what $N$ and $k$, $|\psi_k(\alpha, \beta, N)|$ is bounded by the value 0.008411? For example the inequality is satisfied for the followig pairs:

$N = 1000$ and $x > 31$, or
$N = 10^6$ and $x > 60$.

As a second example we consider the Riesz case ($\alpha = \beta = 2$). From Table 2, the amplitude (still restricting to the contribution of the first zero) is 0.000078. The inequality is satisfied as follows:

$N = 1000$ and $x > 17$, or
$N = 10^6$ and $x > 31$, or
$N = 10^9$ and $x > 87.2$.

This inequality may be helpful to control the numerical computations in the experiments.

Another numerical consideration will be the following. We consider the critical function $\psi_{3/4}(x)$ obtained with $N = 2000$ (maximum argument in the Möbius function appearing in the Baez-Duarte definition of the $c_k$). We will suppose that the numerical results are given with good accuracy. We now ask: if we increase $N$ from 2000 up to $10^6$ in a ideal experiment, what will be the change of the critical function in the range $x < 30$?

$$\psi_{3/4}(x; N = 2000) = e^{\frac{27}{16} x} \sum_{n=1}^{2000} \frac{\mu(n)}{n^{\frac{15}{2}}} e^{-\frac{e^x}{n^4}}$$

$$\psi_{3/4}(x; N = 10^6) = e^{\frac{27}{16} x} \sum_{n=1}^{10^6} \frac{\mu(n)}{n^{\frac{15}{2}}} e^{-\frac{e^x}{n^4}}$$

The difference $\Delta$ between the two functions is bounded by:

$$\Delta \leq e^{\frac{27}{16}x} \sum_{n=2000}^{10^6} \frac{1}{n^{\frac{15}{2}}} e^{-\frac{e^x}{10^{24}}}$$

If we ask that $\Delta$ will be smaller than say $10^{-6}$ time 0.015 which is about the value of the amplitude of the wave in the range $x \leq 30$, obtained with $N = 2000$, we have:

$$\Delta \leq e^{\frac{27}{16}x} e^{-\frac{e^x}{10^{24}}} (\zeta(\frac{15}{2}) - \zeta(\frac{15}{2}; N = 2000)) \leq 0.015 \cdot 10^{-6}$$

The difference between the Zetas is estimated to:

$$\int_{2000}^{\infty} \frac{1}{x^{\frac{15}{2}}} dx = \frac{2}{13} 2000^{-\frac{13}{2}} = \frac{2}{65} 10^{-26}$$

and the inequality takes the form:

$$\frac{27}{16}x - e^{\frac{x}{10^{24}}} + \log(\frac{2}{65}) - 26\log(10) + 6\log(10) - \log(0.015) \leq 0$$

with the solution $x \leq 27$. Thus for $x \leq 27$, the amplitudes will change at most $10^{-6}$ time of its value 0.015. This shows some stability in the numerical experiments as $N$ increases in a ideal experiment. Of course this is independent of how many zeros are employed in the Baez-Duarte estimation.

The third remark deals with the formula for the $c_k$ we have used in our experiments and given by [3]:

$$\hat{c}_k = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}} e^{-\frac{k}{n^{\beta}}}$$

instead of the correct formula:

$$c_k = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}} \left(1 - \frac{1}{n^{\beta}}\right)^k$$

Again, as above, the crude inequality $|\mu(n)| \leq 1$ may be used to show that the difference between the two sequences becomes smaller as $k$ get bigger and depends on $\alpha$ and $\beta$. In fact it behaves unconditionally as:

$$\frac{C}{k^{\frac{\alpha+\beta-1}{\beta}}} \tag{7.1}$$

To see this, let $\Delta = |\hat{c}_k - c_k|$ then:

$$\Delta \leq \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^{\alpha}} \left(e^{-\frac{k}{n^{\beta}}} - \left(1 - \frac{1}{n^{\beta}}\right)^k\right) \leq \sum_{n=1}^{\infty} \frac{1}{n^{\alpha}} \left(e^{-\frac{k}{n^{\beta}}} - \left(1 - \frac{1}{n^{\beta}}\right)^k\right)$$

since $e^{-\frac{k}{n^{\beta}}} \geq (1 - \frac{1}{n^{\beta}})^k$. Passing to the continuous variable $x$, the contribution of the second integral is given by [3]:

$$\int_1^{\infty} \frac{1}{x^{\alpha}} \left(1 - \frac{1}{x^{\beta}}\right)^k dx = \frac{1}{\beta} \frac{\Gamma(\frac{\alpha-1}{\beta})\Gamma(k+1)}{\Gamma(\frac{\alpha-1}{\beta} + k + 1)}$$

while the first is given by:

$$\int_1^\infty \frac{e^{-\frac{k}{x^\beta}}}{x^\alpha} dx = \frac{1}{\beta k^{\frac{\alpha-1}{\beta}}} \Gamma(\frac{\alpha-1}{\beta})$$

Using Stirling's formula, at large $k$ the difference behaves like:

$$\Delta \leq \frac{C}{k^{\frac{\alpha+\beta-1}{\beta}}}.$$

For the model under consideration the decay is as $\frac{C}{k^{\frac{21}{8}}}$ and is stronger then in the usual Riesz case ($\alpha = \beta = 2$) where an early more detailed calculation gives a decay like $\frac{C}{k^{\frac{3}{2}}}$ [4].

Finally it should be added that the general upper bound for $\Delta$ is related to the discrete derivative of the Baez-Duarte coefficients given by:

$$\begin{aligned} c_k(\alpha,\beta) - c_{k+1}(\alpha,\beta) &= \sum_{n=1}^\infty \frac{\mu(n)}{n^\alpha} \left( \left(1 - \frac{1}{n^\beta}\right)^k - \left(1 - \frac{1}{n^\beta}\right)^{k+1} \right) \\ &= \sum_{n=1}^\infty \frac{\mu(n)}{n^\alpha} \left(1 - \frac{1}{n^\beta}\right)^k \left(1 - 1 + \frac{1}{n^\beta}\right) = c_k(\alpha+\beta,\beta) \end{aligned}$$

which unconditionally are bounded by $\frac{C}{k^{\frac{\alpha+\beta-1}{\beta}}}$ as above.

In the same way

$$-\frac{d}{dk} \sum_{n=1}^\infty \frac{\mu(n)}{n^\alpha} e^{-\frac{k}{n^\beta}} = \sum_{n=1}^\infty \frac{\mu(n)}{n^{\alpha+\beta}} e^{-\frac{k}{n^\beta}}$$

which gives the same decay since the function is equal to $c_k(\alpha+\beta,\beta)$ as above.

At large $k$ we also have [3]:

$$c_k \approx \sum_{p=0}^\infty \frac{c_p k^p e^{-k}}{p!}$$

a Poisson like distribution for the coefficients $c_k$.

## 8. Conclusions

In this work, we have used the expansion in terms of the Pochhammer polynomials for the reciprocal of the Zeta function. Our expansion contains two parameters $\alpha$ and $\beta$ so that our analysis was possible for different functions, called "critical functions". The boundedness of the critical function would ensure the truth of the RH.

In a numerical context we have first presented an extensive treatment of the critical functions via the Möbius function. Then we have compared the amplitudes of the "Riesz, Hardy and Littlewood waves" using an extension of the formula of Baez-Duarte (the formula contains the contribution of the trivial and non-trivial zeros of the Riemann Zeta function): the agreement with the treatment using the Möbius function seems satisfactory even if we have considered only very few zeros in the Baez-Duarte formula for the coefficients $c_k$.

For a special case where $\alpha = \frac{7}{2}$ and $\beta = 4$, we have then considered different values of $\Re(s)$, i.e. values in the critical segment from 1 to $\frac{3}{10}$: the critical functions

appear decaying, starting from the right border $\Re(s) = 1$ to reach near $\Re(s) = \frac{1}{2}$ a behaviour still bounded, with oscillations of a nearby constant amplitude. This is not in contradiction with the possible truth of the RH. Finally we have remarked some stability property of the amplitudes of the waves involved in the experiments in the asymptotic region (increasing values of $\log k$).

The numerical results up to a maximum value of $\log k = 30$ (i.e. $k = 1.06865 \times 10^{13}$) go more in the direction to believe that the critical functions do not increase with $\log k$ and that they should reach a behaviour with a stable amplitude of the waves which is smaller that the maximum conjectured value given by $1.68477\ldots$.

In the context of validity of our numerical results, our analysis gives further indication that the RH may barely be true as indicated by our two parameter models in the week as well as in the "strong coupling regime".

So the open question is still the following: the critical function at large value of $k$ is growing, stabilizing to a "periodic pure wave" with constant amplitude or decaying with a zero amplitude? From the results of our numerical treatment we are more in favour of the last two cases.

## References


[1] L. Baez-Duarte, A new necessary and sufficient condition for the Riemann Hypothesis, *arXiv:math.NT/0307215*, 2003

[2] L. Baez-Duarte, A sequential Riesz-like criterion for the Riemann Hypothesis, *International Journal of Mathematical Sciences*, 2005, 3527-3537

[3] S. Beltraminelli and D. Merlini, The criteria of Riesz, Hardy-Littlewood et al. for the Riemann Hypothesis revisited using similar functions, *Alb. Jour. Math.* **1**, 2007, 17-30

[4] J. Cislo, M. Wolf, Equivalence of Riesz and Baez-Duarte criterion for the Riemann Hypothesis, *arXiv:math.NT/0607782,* 2006

[5] M. Coffey, On the coefficients of the Baez-Duarte criterion for the Riemann Hypothesis and their extensions, *arXiv:math-ph/0608050*, 2006

[6] K. Maslanka, Baez-Duarte criterion for the Riemann Hypothesis and Rice's integrals, *arXiv:math.NT/0603713*, 2006

[7] M. Wolf, Evidence in favor of the Baez-Duarte criterion for the Riemann Hypothesis, *arXiv:math.NT/0605485*, 2006

[8] M. Riesz, *Acta Math.* **40**, 1916, 185-190

[9] G.H. Hardy and J.E. Littlewood, *Acta Math.* **41**, 1918, 119-196

[10] E.C. Titchmarsh, The Theory of the Riemann Zeta-function,*Oxford: Clarendon Press*, 1986, p. 374 and p. 382



S. Beltraminelli, CERFIM, Research Center for Mathematics and Physics, PO Box 1132, 6600 Locarno, Switzerland

*E-mail address*: stefano.beltraminelli@ti.ch

D. Merlini, CERFIM, Research Center for Mathematics and Physics, PO Box 1132, 6600 Locarno, Switzerland

*E-mail address*: merlini@cerfim.ch

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 81–89
ISSN 1930-1235: (electronic version)

# OSCILLATION OF NONAUTONOMOUS SECOND ORDER NEUTRAL DELAY DYNAMIC EQUATIONS ON TIME SCALES

H. A. AGWO

Abstract. In this paper, we establish some new oscillation criteria for nonautonomous second order neutral delay dynamic equation with several delays

$$(x(t) - r(t)x(\tau(t)))^{\Delta\Delta} + H(t, x(h(t))) + G(t, x(g(t))) = 0,$$

on a time scale $\mathbb{T}$. The results not only can be applied on neutral differential equations when $\mathbb{T} = \mathbb{R}$, neutral delay difference equations when $\mathbb{T} = \mathbb{N}$ and for neutral delay $q-$ difference equations when $\mathbb{T} = q^{\mathbb{N}}$ for $q > 1$, but also improved most previous results.

## 1. Introduction

A time scale $\mathbb{T}$ is an arbitrary nonempty closed subset of the real numbers $\mathbb{R}$. On any time scale $\mathbb{T}$, we defined the *forward* and *backward jump* operators by

$$\sigma(t) := \inf\{s \in \mathbb{T} : s > t\} \text{ and } \rho(t) := \sup\{s \in \mathbb{T} : s < t\}, \tag{1.1}$$

A point $t \in \mathbb{T}$, $t > \inf \mathbb{T}$ is said to be *left-dense* if $\rho(t) = t$, *right-dense* if $t > \sup \mathbb{T}$ and $\sigma(t) = t$, *left-scattered* if $\rho(t) < t$ and *right-scattered* if $\sigma(t) > t$. The graininess function $\mu : \mathbb{T} \to [0, \infty)$, is defined by $\mu(t) := \sigma(t) - t$. For the function $f : \mathbb{T} \to \mathbb{R}$ the $(delta)$ derivative is defined by

$$f^{\Delta}(t) := \frac{f(\sigma(t)) - f(t)}{\sigma(t) - t}, \tag{1.2}$$

$f$ is said to be differentiable if its derivative exists. A useful formula is

$$f^{\sigma} := f(\sigma(t)) = f(t) + \mu(t) f^{\Delta}(t), \tag{1.3}$$

If $f, g$ are differentiable, then $fg$ and the quotient $\frac{f}{g}$ (where $gg^{\sigma} \neq 0$) are differentiable with

$$(fg)^{\Delta} = f^{\Delta} g + f^{\sigma} g^{\Delta} = f g^{\Delta} + f^{\Delta} g^{\sigma}, \tag{1.4}$$

and

$$\left(\frac{f}{g}\right)^{\Delta} := \frac{f^{\Delta} g - f g^{\Delta}}{g g^{\sigma}}. \tag{1.5}$$

If $f^{\Delta}(t) \geq 0$, then $f$ is nondecreasing.

A function $f : [a, b] \to \mathbb{R}$ is said to be *right-dense continuous* if it right continuous at each right-dense point and there exists a finite left limit at all left-dense

1991 *Mathematics Subject Classification.* Primary 34K11; Secondary 39A10; 39A99.
*Key words and phrases.* Oscillation, Time scales, Neutral delay, dynamic equation.

points. The set of all right-dense continuous functions is denoted by $C_{rd}$ . A function $f : \mathbb{T} \to \mathbb{R}$ is called regressive, if $1 + \mu(t)f(t) \neq 0$ for all $t \in \mathbb{T}$. The set of all functions $f : \mathbb{T} \to \mathbb{R}$ which are regressive and $rd-$continuous will be denoted by $\mathcal{R}$. We define the set $\mathcal{R}^+$ of all positively regressive elements of $\mathcal{R}$ by $\mathcal{R}^+ = \{f \in \mathcal{R} : 1 + \mu(t)f(t) \neq 0,\ t \in \mathbb{T}\}$. A function $F$ with $F^{\triangle} = f$ is called an antiderivative of $f$ and then we define

$$\int_a^b f(t)\triangle t = F(b) - F(a), \tag{1.6}$$

where $a, b \in \mathbb{T}$. It is well known that rd-continuous functions possess antiderivatives. A simple consequence of formula (2.3) is

$$\int_t^{\sigma(t)} f(s)\triangle s = \mu(t)f(t), \tag{1.7}$$

and infinite integrals are defined as

$$\int_a^{\infty} f(t)\triangle t = \lim_{b\to\infty} \int_a^b f(t)\triangle t. \tag{1.8}$$

In the recent years, the theory of time scales has received a lot of attention which was introduced by Stefan Hilger in his Ph.D. thesis in 1988 in order to unify continuous and discrete analysis (see [10]). In fact there has been much activities concerning the oscillation and nonoscillation of solutions of dynamic equations on time scales (or measure chains). We refer the reader to recent papers [1-3, 7, 11, 13-18] and the references cited therein. A book on the subject of time scales, by Bohner and Peterson [5] summarizes and organizes much of time scales calculus, see also the book by Bohner and Peterson [4] for advances in dynamic equations on time scales. For oscillation of first-order neutral delay dynamic equations with a negative coefficient on the neutral term, Mathsen et. al. [14] considered the equation

$$(x(t) - r(t)x(\tau(t)))^{\triangle} + \alpha(t)x(h(t)) = 0. \tag{1.9}$$

and the authors posed the following question. What can be said about even order equations

$$(x(t) - r(t)x(\tau(t)))^{\triangle^{2n}} + \alpha(t)x(h(t)) = 0$$

and various generalization?. Recently Saker in [16] considered the equation

$$(x(t) - r(t)x(\tau(t)))^{\triangle\triangle} + \alpha(t)x(h(t)) = 0. \tag{1.10}$$

Also, recently Liu et. al. [13] considered the equation

$$(x(t) - r(t)x(\tau(t)))^{\triangle} + H(t, x(h(t))) + G(t, x(g(t))) = 0 \tag{1.11}$$

on a time scale $\mathbb{T}$ and established some oscillation criteria, which in the special case when $\mathbb{T} = \mathbb{R}$ involve some oscillation criteria for neutral delay differential equations.

In this paper, we are concerned with the oscillation of the second-order nonlinear dynamic equation

$$(x(t) - r(t)x(\tau(t)))^{\triangle\triangle} + H(t, x(h(t))) + G(t, x(g(t))) = 0 \tag{1.12}$$

on a time scale $\mathbb{T}$. Since we are interest in asymptotic behavior of solutions, we will suppose that the time scale $\mathbb{T}$ under consideration is not bounded above, i.e. it is a time scale interval of the form $[t_0, \infty)_{\mathbb{T}} = [t_0, \infty) \cap \mathbb{T}$. Through this paper, we assume that:

$(H_1)$ $r \in C_{rd}(\mathbb{T}, \mathbb{R}^+)$, $h$ and $g \in C_{rd}(\mathbb{T}, \mathbb{T}), \tau(t) < t, h(t) < t$, $g(t) < t$ , $\lim_{t\to\infty} \tau(t) = \infty$, $\lim_{t\to\infty} h(t) = \infty$, $\lim_{t\to\infty} g(t) = \infty$ and $0 \leq r(t) \leq r < 1$, $C_{rd}(\mathbb{T}, \mathbb{S})$ denotes the set of all functions $f : \mathbb{T} \to \mathbb{S}$ -( $\mathbb{S}$ is a time scale)- which are *right-dense continuous* on $\mathbb{T}$.

$(H_2)$ $H(t, u), G(t, v) \in C(\mathbb{T} \times \mathbb{R}, \mathbb{R})$ for each $t \in \mathbb{T}$ which are nondecreasing in $\mathfrak{u}$ and $v, uH(t, u) > 0$ for $u \neq 0$ and $vG(t, v) > 0$ for $v \neq 0$.

$(H_3)$ $|H(t, u)| \geq \alpha(t) |u|^{\lambda}$ and $|G(t, v)| \geq \beta(t) |v|^{\lambda}$, where $\alpha(t), \beta(t) \geq 0$ and $0 \leq \lambda = \frac{p}{q} \leq 1$ with $p, q$ are odd integers.

By a solution of equation (1.12), we mean a nontrivial real value function $x(t)$ which has the properties $(x(t) - r(t)x(\tau(t)) \in C^2_{rd}[t_x, \infty), t_x > t_0$ and satisfying equation (1.12) for all $t > t_x$. Our attention is restricted to those solutions of equation (1.12) which exist on some half line $[t_x, \infty)$ and satisfy $\sup\{|x(t)| : t > t_1\} > 0$ for any $t_1 > t_x$.

A solution $x(t)$ of (1.12) is said to be oscillatory if it is neither eventually positive nor eventually negative. Otherwise it is called nonoscillatory. The equation itself is called oscillatory if all its solutions are oscillatory.

Note that if $\mathbb{T} = \mathbb{R}$, we have $\sigma(t) = \rho(t) = t$, $f^{\triangle}(t) = f^{'}(t)$, and (1.10), (1.12) become respectively, the second-order neutral delay differential equations

$$[x(t) - r(t)x(\tau(t)]^{''} + \alpha(t)x(h(t)) = 0 \tag{1.13}$$

and

$$[x(t) - r(t)x(\tau(t)]^{''} + H(t, x(h(t))) + G(t, x(g(t))) = 0. \tag{1.14}$$

For oscillation of equation (1.13) Graef et.al. [8] proved that , if $\alpha > 0, 0 \leq r(t) < 1$ and

$$\int_{t_0}^{\infty} \alpha(s)ds = \infty \tag{1.15}$$

then every unbounded solution of (1.13) oscillates. Note that condition (1.15) can not be applied for the second order neutral equation

$$[x(t) - r(t)x(\tau(t)]^{''} + \frac{\gamma}{(t-h)^2}x(t-h) = 0,$$

where $\gamma > 0, 0 \leq r(t) < 1$. Also, Dzurina and Mihalikova in [6] considered the equation (1.5) when $r(t) = r$ where $r$ is constant and gave the following oscillation criteria. If

$$\int_{t_0}^{\infty}(\alpha(s)h(s)\frac{1-r^{n+1}}{1-r}-\frac{1}{4h(s)})ds=\infty, \tag{1.16}$$

then, every solution of equation (1.13) oscillates.

If $\mathbb{T}=\mathbb{Z}$, we have $\sigma(t)=t+1$, $\mu(t)=1$, $f^{\Delta}=\Delta f$, and (1.12) becomes the second-order neutral delay difference equation

$$\Delta^2\left[x(t)-r(t)x(\tau(t))\right]+H(t,x(h(t)))+G(t,x(g(t)))=0. \tag{1.17}$$

If $\mathbb{T}=h\mathbb{Z}$, $h>0$, we have $\sigma(t)=t+h$, $\mu(t)=h$, $f^{\Delta}=\Delta_h f=\frac{f(t+h)-f(t)}{h}$ and (1.4) becomes the second-order neutral delay difference equation

$$\Delta_h^2\left[x(t)-r(t)x(\tau(t))\right]+H(t,x(h(t)))+G(t,x(g(t)))=0. \tag{1.18}$$

If $\mathbb{T}=q^{\mathbb{N}}=\{t:t=q^n,\ n\in\mathbb{N},\ q>1\}$, we have $\sigma(t)=qt$, $\mu(t)=(q-1)t$, $x_q^{\Delta}(t)=\frac{x(qt)-x(t)}{(q-1)t}$, and (1.3) becomes the second order $q-$neutral delay difference equation

$$\Delta_q^2\left[x(t)-r(t)x(\tau(t))\right]+H(t,x(h(t)))+G(t,x(g(t)))=0. \tag{1.19}$$

This paper is organized as follows: In Section 2, we establish some new sufficient conditions for oscillation of (1.12). In Section 3, we present some illustrative examples to show that our results are not only new but also improved many previous results.

## 2. Main results

In this section, we establish some sufficient conditions for the oscillation of equation (1.12). For the remainder of the paper we assume that $\delta^{-1}(t)$ is the inverse of the function $\delta(t)$ exists and satisfies $\delta^{-(n+1)}(t)=t+n\delta$

**Theorem 2.1.** *Assume that $H_1-H_3$ hold. Then every solution of (1.12) oscillates, if*

$$\int_{t_5}^{\infty}\{\alpha(s)(r(h(s))\tau(h(s)))^{\lambda}+\beta(s)(r(g(s))\tau(g(s)))^{\lambda}\}\triangle s=\infty. \tag{2.1}$$

**Proof.** Suppose to the contrary that equation (1.12) has a nonoscillatory solution $x(t)$. We may assume without loss of generality that there exists $t_1\geq t_0$ such that $x(t)>0$, $x(\tau(t))>0$ and $x(\delta(t))>0$ where $\delta=\min\{h,g\}$ for all $t>t_1$. Set

$$y(t)=x(t)-r(t)x(\tau(t)), \tag{2.2}$$

Then, it follows from equation (1.12) we have

$$y^{\triangle\triangle}(t)=-H(t,x(h(t)))-G(t,x(g(t)))\ for\ all\ t>t_1. \tag{2.3}$$

Now $(H_2)$ with $x(\delta(t))>0$ implies that $y^{\Delta\Delta}(t)<0$. Thus $y^{\Delta}(t)$ is strictly decreasing. Now, we prove that $y^{\Delta}(t)>0$ on the interval $[t_1,\infty)_{\mathbb{T}}$. Assume not. Then there exists $t_2\geq t_1$ such that $y^{\Delta}(t_2)=C<0$. Then, since $y^{\Delta\Delta}(t)<0$, we have

$$y^{\Delta}(t)\leq y^{\Delta}(t_2)=C,\quad \text{for}\ \ t\geq t_2, \tag{2.4}$$

and therefore

$$y^{\Delta}(t)\leq C\quad for\ all\ \ t\geq t_2. \tag{2.5}$$

Integrating the last inequality from $t_2$ to $t$, we obtain

$$y(t) = y(t_2) + \int_{t_2}^{t} y^{\Delta}(s)\Delta s \leq y(t_2) + C(t - t_2), \tag{2.6}$$

and consequently $y(t) \to -\infty$ as $t \to \infty$ which implies that there exists $c > 0$ and $t_3 \geq t_2$ such that $y(t) < -c$ for $t \geq t_3$. Then, we have from (3.2) that

$$x(t) < -c + r(t)x(\tau(t)) \leq -c + rx(\tau(t)),\ for\ t \geq t_3, \tag{2.7}$$

which implies that $x(\delta^{-1}(t_3)) < -c + rx(t_3)$. Thus

$$x(\delta^{-(n+1)}(t_3)) \leq -c\sum_{i=0}^{n} r^i + r^{n+1}x(t_3) \leq -c + r^{n+1}x(t_3), \tag{2.8}$$

and so $x(\delta^{-(n+1)}(t_3)) < 0$ for large $n$, which contradicts the fact that $x(t) > 0$ for all $t \geq t_1$. Hence $y^{\Delta}(t) > 0$ and this implies that $y(t)$ is strictly increasing on $[t_1, \infty)$. We prove now that $y(t) > 0$ for $t \geq t_2$ where $t_2$ is large enough. Suppose not. Then there exists a $t_3 \geq t_1$ with $y(t_3) < 0$. Now, since $y(t)$ is strictly increasing then $y(t) > 0$ for $t \geq t_3$ (for if there exists a $t_4 > t_3$ with $y(t_4) > 0$, then $y(t) > 0$ for $t \geq t_4$, but we are assuming that $y(t) > 0$ for $t$ large enough is not true). Then from (2.2) that $x(t) < rx(\tau(t))$, for $t \geq t_3$. Thus $x(\tau^{-1}(t)) \leq rx(t)$ and this implies after iteration that $x(\delta^{-(n+1)}(t)) \leq r^{n+1}x(t) \to 0$ for large $n$, since $0 < r < 1$ and so $x(\delta^{-(n+1)}(t)) < 0$ again, which contradicts the fact that $x(t) > 0$ for all $t \geq t_1$. Then, we have

$$y(t) > 0,\ y^{\Delta}(t) > 0,\ y^{\Delta\Delta}(t) < 0\ for\ t \geq t_1. \tag{2.9}$$

Since $y^{\Delta\Delta}(t) < 0$ and $y(t) > 0$, then

$$\begin{aligned} y(t) &= y(t_4) + \int_{t_4}^{t} y^{\triangle}(s)\triangle s > (t - t_4)y^{\triangle}(t) > kty^{\triangle}(t) \ \text{ for } t > \frac{t_4}{(1-k)} := t_5, \\ 0 &< k < 1. \end{aligned}$$

Now $y(t) > 0$ implies that $y(t) < x(t)$ and $x(t) > r(t)x(\tau(t))$.Since $H(t, x)$ and $G(t, x)$ are nondecreasing in $x$ , we get

$$\begin{aligned} 0 &= y^{\Delta\Delta}(t) + H(t, x(h(t))) + G(t, x(g(t))) \\ &\geq y^{\Delta\Delta}(t) + H(t, r(h(t))x(\tau(h(t)))) + G(t, r(g(t))x(\tau(g(t)))) \\ &\geq y^{\Delta\Delta}(t) + H(t, r(h(t))y(\tau(h(t)))) + G(t, r(g(t))y(\tau(g(t)))) \\ &\geq y^{\Delta\Delta}(t) + \alpha(t)(r(h(t))y(\tau(h(t))))^{\lambda} + \beta(t)(r(g(t))y(\tau(g(t))))^{\lambda} \\ &\geq y^{\Delta\Delta}(t) + \alpha(t)(kr(h(t))\tau(h(t))y^{\triangle}(\tau(h(t))))^{\lambda} \\ &\quad +\beta(t)(kr(g(t))\tau(g(t))y^{\triangle}(\tau(g(t))))^{\lambda} \end{aligned}$$

From nondecreasing property of $\tau(t)$, we have $\tau(h(t)) < \tau(t) < t$ and nonincreasing of $y^{\triangle}(t)$ implies that

$$y^{\triangle}(\tau(h(t))) \geq y^{\triangle}(\tau(t)) \geq y^{\triangle}(t).$$

and

$$y^{\triangle}(\tau(h(t))) \geq y^{\triangle}(\tau(t)) \geq y^{\triangle}(t).$$

Hence,

$$
\begin{aligned}
0 &\geq y^{\Delta\Delta}(t) + \alpha(t)(kr(h(t))\tau(h(t))y^{\triangle}(\tau(h(t))))^{\lambda} \\
&+ \beta(t)(kr(g(t))\tau(g(t))y^{\triangle}(\tau(g(t))))^{\lambda} \qquad (2.10) \\
&\geq y^{\Delta\Delta}(t) + [\alpha(t)(kr(h(t))\tau(h(t)))^{\lambda} + \beta(t)(kr(g(t))\tau(g(t)))^{\lambda}](y^{\triangle}(t))^{\lambda}.
\end{aligned}
$$

Then

$$
\alpha(t)(kr(h(t))\tau(h(t)))^{\lambda} + \beta(t)(kr(g(t))\tau(g(t)))^{\lambda} \leq -\frac{y^{\triangle\triangle}(t)}{(y^{\triangle}(t))^{\lambda}}.
$$

Integrating the above inequality from $t_5$ to $\infty$, we get

$$
\begin{aligned}
& \int_{t_5}^{\infty} \{\alpha(s)(r(h(s))\tau(h(s)))^{\lambda} + \beta(s)(r(g(s))\tau(g(s)))^{\lambda}\}\triangle s \\
\leq & -\int_{t_5}^{\infty} \frac{y^{\triangle\triangle}(s)}{(y^{\triangle}(s))^{\lambda}}\triangle s. \\
= & \lim_{t\to\infty} \int_{y^{\triangle}(t_5)}^{y^{\triangle}(t)} \frac{\triangle s}{s^{\lambda}} \\
= & \int_{y^{\triangle}(t_5)}^{0} \frac{\triangle s}{s^{\lambda}} < \infty.
\end{aligned}
$$

But

$$
\int_{t_5}^{\infty} \{\alpha(s)(r(h(s))\tau(h(s)))^{\lambda} + \beta(s)(r(g(s))\tau(g(s)))^{\lambda}\}\triangle s = \infty,
$$

so, equation (1.12) has no eventually positive solution. Similarly, we can prove that equation (1.12) has no eventually negative solution. Thus equation (1.12) is oscillatory.

**Theorem 2.2.** *Assume that $H_1 - H_3$ hold. Then every solution of (1.12) oscillates, if the inequality*

$$
z^{\triangle}(t) + [\alpha(t)(kr(h(t))\tau(h(t)))^{\lambda} + \beta(t)(kr(g(t))\tau(g(t)))^{\lambda}]z^{\lambda}(\tau(t)) \leq 0, \qquad (2.11)
$$

*has no eventually positive solution.*

**Proof**. Assume to the contrary that equation (1.12) has a nonoscillatory solution $x(t)$. Following the same steps used in the proof of Theorem 2.1, until to get (1.10). Putting $z(t) = y^{\triangle}(t)$ in (2.10) we get (2.11) which have a positive solution. Consequently if (2.11) has no eventually positive solution, then all solutions of (1.12) are oscillatory. This completes the proof of the theorem.

Theorem 2.2 reduces the question of oscillation of (1.12) to that of the absence of eventually positive solutions of the dynamic inequality (2.11).

**Theorem 2.3** *Assume that $H_1 - H_2$ hold and $|H(t,u)| \geq \alpha(t)\,|u|$ and $|G(t,v)| \geq \beta(t)\,|v|$ ,where $\alpha(t), \beta(t) \geq 0$. If*

$$
\int_{t_5}^{\infty} \{\alpha(s)(r(h(s))\tau(h(s))) + \beta(s)(r(g(s))\tau(g(s)))\}\triangle s = \infty. \qquad (2.12)
$$

*Then , every solution of*

$$(x(t) - r(t)x(\tau(t)))^{\triangle\triangle} + \alpha(t)x(h(t)) + \beta(t)x(g(t)) = 0 \tag{2.13}$$

*is oscillatory.*

**Proof**. The proof follows directly from the Theorem 2.1. So we omitted it.

## 3. Examples

In this section, we give some examples to illustrate our main results.

**Example 3.1.** Consider the following second order neutral delay dynamic equation

$$(x(t) - \frac{1}{c}x(\gamma_1 t))^{\triangle\triangle} + \frac{(2+\sin t)}{t^{\alpha}}x^{\lambda}(\gamma_2 t) + \frac{(3+\cos t)}{t^{\beta}}x^{\lambda}(\gamma_3 t) = 0, t \in \mathbb{T}, \tag{3.1}$$

where $\mathbb{T}$ is a time scale, with $c > 1, 0 \leq \lambda = \frac{p}{q} \leq 1$ , $p, q$ are odd integers, $\alpha_1, \alpha_2 \in [\lambda, \lambda + 1]$ and $\gamma_1, \gamma_2, \gamma_3 \in (0, 1)$. In equation (1.12) $r(t) = \frac{1}{c}, \tau(t) = \gamma_1 t, h(t) = \gamma_2 t, g(t) = \gamma_2 t, H(t, x(h(t)) = \frac{(2+\sin t)}{t^{\alpha_1}}x^{\lambda}(h(t))$ and $G(t, x(g(t)) = \frac{(3+\cos t)}{t^{\alpha_2}}x^{\lambda}(g(t))$. (i.e. $\alpha(t) = \frac{(2+\sin t)}{t^{\alpha_1}}$ and $\beta = \frac{(3+\cos t)}{t^{\alpha_2}}$). Then we have

$$\begin{aligned}
& \int_{t_5}^{\infty} \{\alpha(s)(r(h(s))\tau(h(s)))^{\lambda} + \beta(s)(r(g(s))\tau(g(s)))^{\lambda}\}\triangle s \\
= & \int_{t_5}^{\infty} \{\frac{(2+\sin s)}{s^{\alpha_1}}((\frac{1}{c})(\gamma_1\gamma_2 s))^{\lambda} + \frac{(3+\cos s)}{s^{\alpha_2}}((\frac{1}{c})(\gamma_1\gamma_3 s))^{\lambda}\}\triangle s \\
\geq & \int_{t_5}^{\infty} \{\frac{1}{s^{\alpha_1}}((\frac{1}{c})(\gamma_1\gamma_2 s))^{\lambda} + \frac{1}{s^{\alpha 2}}((\frac{1}{c})(\gamma_1\gamma_3 s))^{\lambda}\}\triangle s \\
= & (\frac{\gamma_1\gamma_2}{c})^{\lambda}\int_{t_5}^{\infty}\frac{\triangle s}{s^{\alpha_1-\lambda}} + (\frac{\gamma_1\gamma_3}{c})^{\lambda}\int_{t_5}^{\infty}\frac{\triangle s}{s^{\alpha_2-\lambda}} = \infty \text{ for } \alpha_1, \alpha_2 \in [\lambda, \lambda+1].
\end{aligned}$$

Hence, by Theorem (2.1) every solution of equation (3.1) oscillates.

**Example 3.2.** Consider the following second order neutral delay dynamic equation

$$(x(t) - e^{-\frac{1}{\lambda}(t-\tau)}x(t-\tau))^{\triangle\triangle} + x^{\lambda}(t-h_1) + \frac{1}{e^{-t}+1}x^{\lambda}(t-h_2) = 0, t \in \mathbb{T}, \tag{3.2}$$

where $\mathbb{T}$ is a time scale, where $0 \leq \lambda = \frac{p}{q} \leq 1$ , $p, q$ are odd integers, $\tau, h_1, h_2 > 0$, $r(t) = e^{-\frac{1}{\lambda}(t-\tau)}, \tau(t) = t - \tau, h(t) = t - h_1, g(t) = t - h_2, H(t, x(h(t)) = x^{\lambda}(h(t))$ and $G(t, x(g(t)) = \frac{1}{e^{-t}+1}x^{\lambda}(g(t))$. (i.e. $\alpha(t) = 1$ and $\beta = \frac{1}{e^{-t}+1}$). Then we have

$$\begin{aligned}
& \int_{t_5}^{\infty} \{\alpha(s)(r(h(s))\tau(h(s)))^{\lambda} + \beta(s)(r(g(s))\tau(g(s)))^{\lambda}\}\triangle s \\
= & \int_{t_5}^{\infty} \{e^{-\frac{1}{\lambda}(t-\tau-h_1)}(t-\tau-h_1)\}^{\lambda}\triangle s \\
& + \int_{t_5}^{\infty} \frac{1}{e^{-s}+1}(e^{-\frac{1}{\lambda}(t-\tau-h_2)}(t-\tau-h_2))^{\lambda}\}\triangle s \\
\geq & \frac{3}{2}(\frac{\lambda}{e})^{\lambda}\int_{t_5}^{\infty}\triangle s = \infty.
\end{aligned}$$

Therefore, by Theorem (2.1), equation (3.2) is oscillatory.

**Example 3.3.** Consider the following specific second order neutral delay dynamic equation

$$(x(t)-\frac{1}{2}x(t-\tau))^{\triangle\triangle}+\frac{\gamma}{(t-h)^2}x^{\lambda}(t-h)=0, t\in\mathbb{T}, \tag{3.3}$$

where $\mathbb{T}$ is a time scale, where $\tau, h > 0$, $r(t) = \frac{1}{2}, \tau(t) = t-\tau, h(t) = t-h, H(t, x(h(t)) = x(h(t))$ and $G(t, x(g(t)) = 0$.(i.e. $\alpha(t) = \frac{\gamma}{(t-h)^2}, \gamma > 0$ and $\beta(t) = 0$). Then we have

$$\begin{aligned}
&\int_{t_5}^{\infty}\{\alpha(s)(r(h(s))\tau(h(s))) + \beta(s)(r(g(s))\tau(g(s)))\}\triangle s\\
=\ &\int_{t_5}^{\infty}\frac{\gamma(s-\tau-h)}{2(s-h)^2}\triangle s\\
=\ &\frac{\gamma}{2}\int_{t_5}^{\infty}\frac{1}{s-h}(1-\frac{\tau}{s-h})\triangle s=\infty.
\end{aligned}$$

Hence, by Theorem 2.3, every solution of equation (3.3) is oscillatory. This example shows that the results by Dzurina and Mihalikova [6] in the case when $\mathbb{T}=\mathbb{R}$, is not sharp, since by choosing $n=\infty$, we have

$$\begin{aligned}
\int_{t_0}^{\infty}\left[\alpha(s)h(s)\frac{1-r^{n+1}}{1-r}-\frac{1}{4h(s)}\right]ds &= \int_{t_0}^{\infty}\left[\frac{\gamma}{s-h}(\frac{1}{1-\frac{1}{2}})-\frac{1}{4(s-h)}\right]ds\\
&= \int_{t_0}^{\infty}\left[\frac{2\gamma-\frac{1}{4}}{(s-h)}\right]ds=\infty,\ \text{if } \gamma>\frac{1}{2}.
\end{aligned}$$

Also, the result by Saker not sharp for equation (3.3). For, in his results [Example 2.2, 16 ], it was proved that this equation is oscillatory if $\gamma > \frac{1}{4}$ and Graef et. al. [8] condition (1.15) can not be applied. Therefore our results are not only new but also improve some previous results.

## References


[1] R P. Agarwal, Donal O'Regan and S. H. Saker, Oscillation criteria for second order neutral delay dynamic equations, *J. Math. Anal. Appl,* 300 (2004) 203-217.

[2] H. A. Agwo, On the oscillation of second order neutral delay dynamic equations with several delays and variable coefficients, *International J. Appl. Math. & Stat.* 5(6) (2006) 65-73.

[3] H. A. Agwo, On the oscillation of second order nonlinear neutral delay dynamic equations, *Georgian Math. J.* 14(2007) 597-606.

[4] M. Bohner and A. Peterson, *Advances in Dynamic Equations on Time Scales*, Birkhäuser, Boston, MA, 2003.

[5] M. Bohner and A. Peterson, *Dynamic Equations on Time Scales : An Introduction with Application*, Birkhäuser, Boston, MA, 2001.

[6] J. Dzurina and Mihalikova, Oscillation criteria for second order neutral differential equations, *Math. Bohemica* 125 (2000), 145-153.

[7] L. Erbe, A. Peterson and S. H. Saker, Kamenev-type oscillation criteria for second-order linear delay dynamic equations, *Dynamic Syst. & Appl.* 15 (2006), 65-78.

[8] J. R. Graef, M. K. Grammatikopoulos and P. W. Spikes, Asymptotic properties of solutions of nonlinear delay differential equations of second, *Radovi Mat.* 4 (1988), 133-149.

[9] I. Györi, G. Ladas, *Oscillation Theory of Delay Differential Equations with Applications*, Clarendon Press, Oxford, 1991.

[10] S. Hilger, Analysis on measure chains - a unified approach to continuous and discrete calculus, *Results Math.* 18 (1990) 18- 56.
[11] J. Jiang, X. Li, Oscillation of second order nonlinear neutral differential equations, *Appl. Math. Comput.* 135 (2003) 531-540.
[12] G. S. Ladde, V. Lakshmikantham and B. G. Zhang, *Oscillation Theory of Differential Equations with Deviating Arguments*, Marcel Dekker, New York, 1987.
[13] Liu Ailian, Wu Hongwu, Zhu Siming and R. M. Mathsen, Oscillation for nonautonomous neutral dynamic delay equations scales, *Acta Math. Sci.* 26 B(1), (2006), 99-106.
[14] R. M. Mathsen, QI-RU Wang and Hong-Wu Wu, Oscillation for neutral dynamic functional equations on time scales, *J. Diff. Eqns. Appl.* 10 (2004), 651-659.
[15] Y. Sahiner, On oscillation of second-order neutral type delay differential equations, *Appl. Math. Comput.* 150 (2004) 697-706.
[16] S. H. Saker, Oscillation of second order neutral delay dynamics equations on time scales, (accepted)..
[17] S. H. Saker, Oscillation of second-order nonlinear neutral delay dynamic equations on time scales, *J. Comp. Appl. Math.* 187 , (2006), 123-141.
[18] S. H. Saker, Oscillatory behavior of linear neutral delay dynamic equations on time scales, *Kyungpook Math. J.* (accepted).

Department of Mathematics, Ain Shams University, Faculty of Education, Roxy, Cairo, Egypt.
*E-mail address*: hassanagwa@yahoo.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 91–99
ISSN 1930-1235: (electronic version)

# BOUNDARY VALUE PROBLEMS FOR SECOND ORDER CONVEX AND NONCONVEX DIFFERENTIAL INCLUSIONS WITH INTEGRAL BOUNDARY CONDITIONS

MUSTAPHA LAKRIB

Abstract. We prove existence results for boundary value problems for second order convex and nonconvex differential inclusions with integral boundary conditions. The proofs use nonlinear alternatives of Leray-Schauder type and a selection theorem due to Bressan and Colombo.

## 1. Introduction

This paper is concerned with the boundary value problem for a second order ordinary differential inclusion with integral boundary conditions

$$x''(t) \in F(t, x(t)), \quad \text{a.e. } t \in J := [0, 1], \tag{1.1}$$

$$x(0) - k_1 x'(0) = \int_0^1 h_1(x(s))ds, \qquad x(1) + k_2 x'(1) = \int_0^1 h_2(x(s))ds. \tag{1.2}$$

In problem (1.1)-(1.2), $F : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ is a multivalued function with nonempty compact values, $\mathcal{P}(\mathbb{R})$ is the class of all subsets of $\mathbb{R}$ and, for $i = 1, 2$, $h_i : \mathbb{R} \to \mathbb{R}$ are given functions and $k_i$ are nonnegative constants.

Boundary value problems with integral boundary conditions constitute an important class of problems, because they include as special cases two, three, multi-point and nonlocal boundary value problems. Such problems for second order differential equations have been considered by many authors, for instance, see [3, 6, 8, 10, 12, 13] and the references therein. As far as we know, there are few authors who study the existence of solutions in the case of differential inclusions, among them we would like to cite Brykalov [2] and Halidias and Papageorgiou [7]. In [2], existence results for boundary value problems for differential inclusions with nonconvex right-hand sides and monotone nonlinear (integral) boundary conditions was studied. The technique of continuous selections of multivalued functions with decomposable values coupled with the method of monotone boundary conditions are used in these investigations. In [7], the authors use the method of upper and lower solutions with fixed point theorems to establish some existence results for second order differential inclusions with Sturm-Liouville and periodic boundary conditions.

Recently, Rahmat in [12] have used the method of upper and lower solutions with the method of generalized quasilinearization to study the existence of solutions of

2000 *Mathematics Subject Classification.* 34A60, 34B15.
*Key words and phrases.* Differential inclusions, integral boundary value problems, fixed point theorems, continuous selection, existence results.

the boundary value problem for a second order differential equation with integral boundary conditions of the form (1.2)

$$x''(t) = f(t, x(t)), \quad \text{a.e. } t \in J := [0,1], \tag{1.3}$$

$$x(0) - k_1 x'(0) = \int_0^1 h_1(x(s))ds, \qquad x(1) + k_2 x'(1) = \int_0^1 h_2(x(s))ds. \tag{1.4}$$

Motivated by this work, we consider problem (1.1)-(1.2) which is the multivalued form of problem (1.3)-(1.4). Our goal is to give some existence results for problem (1.1)-(1.2). Our method of study is to convert problem (1.1)-(1.2) into a fixed point problem. Then, we first apply the nonlinear alternative of Leray-Schauder type for multivalued functions [11] to prove an existence result when $F$ has convex values. Next, we combine a continuous selection theorem [1] due to Bressan and Colombo with the nonlinear alternative of Leray-Schauder type for single valued functions [4] to prove the second existence result of this paper for $F$ with nonconvex values. In both cases, the conditions established on the multivalued function $F$ are common in the literature on differential equations and inclusions. In our main results, the only condition we require on the functions $h_i$, $i = 1, 2$, is continuity.

Let $C(J, \mathbb{R})$ and $L^1(J, \mathbb{R})$ denote the Banach spaces of continuous and Lebesgue integrable functions on $J$ equipped with the normes $\|x\| = \max\{|x(t)| : t \in J\}$ and $\|x\|_{L^1} = \int_0^1 |x(t)|dt$, respectively. Consider $AC^1(J, \mathbb{R})$ the space of all continuous functions whose first derivatives exist and are absolutely continuous on $J$.

By a solution of (1.1)-(1.2) we mean a function $x \in AC^1(J, \mathbb{R})$ whose second derivative $x''$ exists and is a member of $L^1(J, \mathbb{R})$, that is, there exists a function $v \in L^1(J, \mathbb{R})$, $v(t) \in F(t, x(t))$ for almost every $t \in J$ such that $x''(t) = v(t)$ almost everywhere in $J$ and $x$ satisfies the conditions (1.2)

## 2. Preliminaries

In what follows we will enumerate some notions and results regarding single valued and multivalued functions. Although many of these are available in a more general framework, we will mention them only in the form we need in the present paper.

We say that a subset $A$ of $L^1(J, \mathbb{R})$ is decomposable if for all $u, v \in A$ and all $I \subset J$ measurable, the function $u\chi_I + v\chi_{J-I} \in A$, where $\chi_I$ stands for the characteristic function of $I$.

For $X$ a Banach space, $\mathcal{P}(X)$ is the class of all subsets of $X$.

Let $X_1$ and $X_2$ be Banach spaces and $G : X_1 \to \mathcal{P}(X_2)$ be a multivalued function. $G$ is said to be closed (resp. convex and compact) valued if $G(x)$ is closed (resp. convex and compact) subset of $X_2$ for each $x \in X_1$. We say that $G$ is lower semi-continuous (in brief l.s.c.) if for every open subset $A$ of $X_2$, the set $\{x \in X_1 : G(x) \cap A \neq \emptyset\}$ is open. We say that $G$ is upper semi-continuous (in brief u.s.c.) if for every closed subset $A$ of $X_2$, the set $\{x \in X_1 : G(x) \cap A \neq \emptyset\}$ is closed. $G$ is called continuous when it is l.s.c and u.s.c.

A multivalued function $G : X_1 \to \mathcal{P}(X_2)$ (resp. A function $G : X_1 \to X_2$) is said to be completely continuous if $\overline{G(A)}$ is compact for all bounded subsets $A$ of $X_1$. If $X_1 = X_2$, we say that $G$ has a fixed point if there is $x \in X_1$ such that $x \in G(x)$ (resp. $x = G(x)$).

A multivalued function $G : J \to \mathcal{P}(\mathbb{R})$ with nonempty compact convex values is said to be measurable if for every $y \in \mathbb{R}$, the function $t \to d(y, G(t)) = \inf\{|y - x| : x \in G(t)\}$ is measurable.

A multivalued function $G : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ (resp. A function $G : J \times \mathbb{R} \to \mathbb{R}$) is said to satisfy Carathéodory's conditions if

(i) $t \mapsto G(t, x)$ is measurable for each $x \in \mathbb{R}$,
(ii) $x \mapsto G(t, x)$ is continuous almost everywhere in $J$.

Moreover, $G$ is called $L^1$-Carathéodory, if, in addition,

(iii) for each real number $r > 0$, there exists a function $h_r \in L^1(J, \mathbb{R})$ such that

$$\|G(t,x)\| = \sup\{|v| : v \in G(t,x)\} \leq h_r(t) \text{ (resp. } |G(t,x)| \leq h_r(t)) \text{ a.e. } t \in J$$

for all $x \in \mathbb{R}$ with $|x| \leq r$.

For each $x \in C(J, \mathbb{R})$, define the set of selections of a multivalued function $G : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ that belong to $L^1(J, \mathbb{R})$ by

$$S^1_G(x) = \{v \in L^1(J, \mathbb{R}) : v(t) \in G(t, x(t)) \text{ a.e. } t \in J\}. \tag{2.1}$$

Then we have the following lemma [9] due to Lasota and Opial.

**Lemma 2.1.** *Let $G : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ be an $L^1$-Carathéodory multivalued function with nonempty compact convex values. Then $S^1_G(x) \neq \emptyset$ for each $x \in \mathbb{R}$.*

The following hypotheses on the multivalued function $F : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ and the functions $h_i$, $i = 1, 2$, in problem (1.1)-(1.2) will be used throughout this work:

(C1) $F$ is Carathéodory.
(C2) Each function $h_i : \mathbb{R} \to \mathbb{R}$, $i = 1, 2$, is continuous.
(C3) There exists an $L^1$-Carathéodory function $\psi : J \times \mathbb{R}_+ \to \mathbb{R}_+$ such that
  (i) $|F(t, x)| \leq \psi(t, |x|)$, for almost all $t \in J$ and all $x \in \mathbb{R}$,
  (ii) $\psi(t, x)$ is nondecreasing in $x$ for almost all $t \in J$,
  as well as a constant $M^* > 0$ such that
  (iii) $M^* > \sup_{|u| \leq M^*} |h_1(u)| + \sup_{|u| \leq M^*} |h_2(u)| + C_0 \|\psi(\cdot, M^*)\|_{L^1}$, where

$$C_0 := \frac{(1 + k_1)(1 + k_2)}{1 + k_1 + k_2}.$$

**Remark 2.2.** *From conditions (C1) and (C3)-(i) we deduce that the multivalued function $F$ is $L^1$-Carathéodory.*

## 3. Main results

3.1. **Convex case.** In this section, we are concerned with the existence of solutions for the problem (1.1)-(1.2) when the right hand side has convex values. So, we suppose that $F : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ in (1.1) is a multivalued function with nonempty compact convex values.

We need the following result in the sequel.

**Lemma 3.1.** [9] *Let $F : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ be an $L^1$-Carathéodory multivalued function with nonempty compact convex values, and $\mathcal{K} : L^1(J, \mathbb{R}) \to C(J, \mathbb{R})$ be a linear continuous function. Then the operator, with nonempty compact convex values, $\mathcal{K} \circ S^1_F : C(J, \mathbb{R}) \to \mathcal{P}(C(J, \mathbb{R}))$ has a closed graph in $C(J, \mathbb{R}) \times C(J, \mathbb{R})$.*

Our main existence theorem in this section (i.e. Theorem 3.3) is obtained via the following nonlinear alternative of Leray-Schauder type for multivalued functions [11].

**Theorem 3.2.** *Let $X$ be a Banach space, $U$ an open and bounded subset of $X$ with $0 \in U$ and $\Gamma : \overline{U} \to \mathcal{P}(X)$ a multivalued function. Suppose that*

(i) *$\Gamma x$ is nonempty, convex and closed for each $x \in \overline{U}$,*
(ii) *$\Gamma$ has closed graph,*
(iii) *$\Gamma$ is completely continuous.*

*Then, either*

(A1) *$\Gamma$ has a fixed point in $\overline{U}$, or*
(A2) *there exists $x \in \partial U$ (the boundary of $U$) and $\lambda \in (0,1)$ with $x \in \lambda \Gamma x$.*

Now, we are able to state and prove our main theorem.

**Theorem 3.3.** *Suppose that conditions (C1)-(C3) are satisfied. Then problem (1.1)-(1.2) has a solution on $J$.*

*Proof.* To establish our result, we will apply Theorem 3.2 to the operator $\Gamma : C(J,\mathbb{R}) \to \mathcal{P}(C(J,\mathbb{R}))$ defined, for any $x \in C(J,\mathbb{R})$, by $\Gamma x$ the set of functions $y \in C(J,\mathbb{R})$ such that

$$y(t) = P(t) + \int_0^1 G(t,s)v(s)ds, \quad t \in J, \quad v \in S_F(x),$$

where the function $P : J \to \mathbb{R}$ is defined, for any $t \in J$, by

$$P(t) = \frac{1}{1+k_1+k_2}\left[(1-t+k_2)\int_0^1 h_1(x(s))ds + (k_1+t)\int_0^1 h_2(x(s))ds\right] \tag{3.1}$$

and $G : J \times J \to \mathbb{R}$, the Green function associated with problem (1.1)-(1.2), is given by

$$G(t,s) = \frac{-1}{1+k_1+k_2}\begin{cases}(k_1+t)(1-s+k_2), & 0 \le t < s \le 1,\\ (k_1+s)(1-t+k_2), & 0 \le s < t \le 1.\end{cases} \tag{3.2}$$

Note that $|G(t,s)| \le C_0$ on $J \times J$, where $C_0$ is given in condition (C3)-(iii).

It is clear that $\Gamma$ is well defined. By standard argument one can check that fixed points of $\Gamma$ are solutions to problem (1.1)-(1.2). It remains to show that $\Gamma$ satisfies all the conditions of Theorem 3.2.

**Claim 1:** *$\Gamma x$ is nonempty and convex for each $x \in C(J,\mathbb{R})$.* This is an immediate consequence of the fact that $S_F(x)$ is nonempty (see Lemma 2.1) and $F(x)$ is convex, respectively.

**Claim 2**: *$\Gamma$ has closed graph.* So, let $(x_n)_n$ be a sequence in $C(J,\mathbb{R})$ and $x \in C(J,\mathbb{R})$ such that $x_n \to x$. Let $y_n \in \Gamma x_n$ such that $y_n \to y$. We will show that $y \in \Gamma x$.

Define the operator $\mathcal{K} : L^1(J,\mathbb{R}) \to C(J,\mathbb{R})$ by

$$(\mathcal{K}v)(t) = \int_0^1 G(t,s)v(s)ds, \quad v \in L^1(J,\mathbb{R}), \quad t \in J.$$

We can easily see that $\mathcal{K}$ is well defined, linear and continuous. Let $n \in \mathbb{N}$ and $v_n \in S_F(x_n)$ such that

$$y_n(t) = P_n(t) + \int_0^1 G(t,s)v_n(s)ds, \quad t \in J.$$

We have $y_n - P_n \in \mathcal{K} \circ S_F(x_n)$ and $y_n - P_n \to y - P$. By Lemma 3.1, $\mathcal{K} \circ S_F$ has a closed graph, so that $y - P \in \mathcal{K} \circ S_F(x)$, that is,

$$y(t) = P(t) + \int_0^1 G(t,s)v(s)ds$$

for some $v \in S_F(x)$, which proves that $y \in \Gamma x$.

**Claim 3**: $\Gamma x$ *is closed for each* $x \in C(J,\mathbb{R})$. This assertion follows from Claim 2 by setting $x_n \equiv x$.

**Claim 4**: $\Gamma$ *is completely continuous on* $C(J,\mathbb{R})$. To show this, we first show that $\Gamma$ maps bounded sets into bounded sets. Let $B$ be a bounded subset of $C(J,\mathbb{R})$. Then there exists a constant $r > 0$ such that $\|x\| \leq r$ for all $x \in B$. Let $x \in B$, $y \in \Gamma x$ and $v \in S_F(x)$ such that, for $t \in J$,

$$y(t) = P(t) + \int_0^1 G(t,s)v(s)ds.$$

Conditions (C2) and (C3) yield

$$\begin{aligned} |y(t)| &\leq |P(t)| + C_0 \int_0^1 |F(s,x(s))|ds \\ &\leq \sup_{|u|\leq r} |h_1(u)| + \sup_{|u|\leq r} |h_2(u)| + C_0\|\psi(\cdot,r)\|_{L^1} := \eta, \end{aligned}$$

which implies that $y$ is uniformly bounded with a uniform bound $\eta$. This finish to prove that $\Gamma B$ is bounded.

Next we show that $\Gamma$ maps bounded sets into equicontinuous sets. Let $B$ be a bounded subset of $C(J,\mathbb{R})$ as above. Let $x \in B$, $y \in \Gamma x$ and $t, \tau \in J$. Then

$$\begin{aligned} |y(t) - y(\tau)| &\leq |P(t) - P(\tau)| + \int_0^1 |G(t,s) - G(\tau,s)||F(s,x(s))|ds \\ &\leq |P(t) - P(\tau)| + \int_0^1 |G(t,s) - G(\tau,s)|\psi(s,q)ds \\ &\leq |P(t) - P(\tau)| + \|G(t,\cdot) - G(\tau,\cdot)\|_{L^1}\|\psi(\cdot,q)\|_{L^1}. \end{aligned}$$

In view of the continuity of $P$ and $G$, and by use of the Lebesgue's convergence theorem, the right hand side tends to zero as $\tau \to t$. So $\Gamma B$ is equicontinuous.

The results above, together with the Arzelá-Ascoli Theorem, allow us to conclude that, for any bounded subset $B$ of $C(J,\mathbb{R})$, $\Gamma B$ is relatively compact. Hence, $\Gamma$ is completely continuous.

Now take $M^*$ as in condition (C3)-(iii), set

$$U = \{x \in C(J,\mathbb{R}) : \|x\| < M^*\}$$

and consider the operator $\Gamma : \overline{U} \to \mathcal{P}(C(J,\mathbb{R}))$. From Theorem 3.2 it follows that either the operator inclusion $x \in \Gamma x$ has a solution (i.e. problem (1.1)-(1.2) has a solution) or there exists $x \in \partial U$ and $\lambda \in (0,1)$ such that $x \in \lambda\Gamma x$.

**Claim 5:** *The second alternative above does not occur.* Let $x$ be a solution of $x \in \lambda\Gamma x$ with $\lambda \in (0,1)$ and suppose that $\|x\| = M^*$. Then, for $t \in J$ and some

$v \in S_F(x)$,

$$\begin{aligned}|x(t)| &= \left|\lambda\left(P(t) + \int_0^1 G(t,s)v(s)ds\right)\right| \\ &\leq \int_0^1 |h_1(x(s))|ds + \int_0^1 |h_2(x(s))|ds + C_0\int_0^1 \psi(s,|x(s)|)ds \\ &\leq \sup_{|u|\leq M^*}|h_1(u)| + \sup_{|u|\leq M^*}|h_2(u)| + C_0\|\psi(\cdot,M^*)\|_{L^1}.\end{aligned}$$

Consequently

$$M^* \leq \sup_{|u|\leq M^*}|h_1(u)| + \sup_{|u|\leq M^*}|h_2(u)| + C_0\|\psi(\cdot,M^*)\|_{L^1},$$

which contradicts condition (C3)-(iii). The conclusion of our theorem is straightforward from Theorem 3.2. □

Hereafter, we discuss a special case to illustrate how condition (C3)-(iii) can be satisfied.

Let us suppose that, for each $i = 1, 2$, the function $h_i$ is continuous and there exist $\alpha_i, \beta_i, x_i \geq 0$, with $\alpha_1 + \alpha_2 < 1$, such that $|h_i(x)| \leq \alpha_i x + \beta_i$, for all $x \geq x_i$. Also, suppose that there exist a nondecreasing continuous eventually $\alpha_3$-sublinear function $\overline{\psi} : \mathbb{R}_+ \to \mathbb{R}_+$, with $\alpha_3 < \frac{1-(\alpha_1+\alpha_2)}{C_0\|p\|_{L^1}}$, and a function $p \in L^1(J, \mathbb{R}_+)$ such that $\psi(t,x) = p(t)\overline{\psi}(x)$, for all $x \geq 0$.

Let $\varepsilon > 0$ be such that

$$\alpha_3 < \frac{1-(\alpha_1+\alpha_2)-\varepsilon}{C_0\|p\|_{L^1}}$$

and set

$$q(x) = \beta_1 + \beta_2 + (\alpha_1 + \alpha_2 - 1)x + C_0\|p\|_{L^1}\overline{\psi}(x), \quad x \geq 0.$$

As $\overline{\psi}$ is eventually $\alpha_3$-sublinear, there exists $x_3 > 0$ such that, for all $x \geq x_3$, $\overline{\psi}(x) \leq \alpha_3 x$ and then

$$\begin{aligned}q(x) &\leq \beta_1 + \beta_2 + (\alpha_1 + \alpha_2 - 1)x + C_0\|p\|_{L^1}\alpha_3 x \\ &\leq \beta_1 + \beta_2 + (\alpha_1 + \alpha_2 - 1)x + C_0\|p\|_{L^1}\frac{1-(\alpha_1+\alpha_2)-\varepsilon}{C_0\|p\|_{L^1}}x \\ &= \beta_1 + \beta_2 - \varepsilon x.\end{aligned}$$

Thus, for $x > \max\{x_3, \frac{\beta_1+\beta_2}{\varepsilon}\}$, we see that $q(x) < 0$, i.e.

$$q(x) = \beta_1 + \beta_2 + (\alpha_1 + \alpha_2 - 1)x + C_0\|p\|_{L^1}\overline{\psi}(x) < 0$$

or

$$x > \beta_1 + \beta_2 + (\alpha_1 + \alpha_2)x + C_0\|p\|_{L^1}\overline{\psi}(x).$$

This implies that

$$x > \sup_{|u|\leq x}|h_1(u)| + \sup_{|u|\leq x}|h_2(u)| + C_0\|\psi(\cdot,x)\|_{L^1},$$

whenever

$$x > \max\left\{x_1, x_2, x_3, \frac{\beta_1+\beta_2}{\varepsilon}\right\}.$$

Therefore, if $h_i$, $i = 1, 2$ and $\psi$ are as above, we can always find a constant $M^* > 0$ satisfying condition (C3)-(iii). Hence, we have the following corollary.

**Corollary 3.4.** *Assume that (C1) holds. In addition, assume that the following conditions (C2') and (C3') are satisfied.*

(C2') *Each function $h_i : \mathbb{R} \to \mathbb{R}$, $i = 1, 2$, is continuous and there exist constants $\alpha_i$, $\beta_i$, $x_i \geq 0$, with $\alpha_1 + \alpha_2 < 1$, such that $|h_i(x)| \leq \alpha_i x + \beta_i$, for all $x \geq x_i$.*

(C3') *There exist a continuous nondecreasing function $\overline{\psi} : \mathbb{R}_+ \to \mathbb{R}_+$ which is eventually $\alpha_3$-sublinear, with $\alpha_3 < \frac{1-(\alpha_1+\alpha_2)}{C_0\|p\|_{L^1}}$, and a function $p \in L^1(J, \mathbb{R}_+)$ such that*

$$|F(t, x)| \leq p(t)\overline{\psi}(|x|), \text{ for almost all } t \in J \text{ and all } x \in \mathbb{R}.$$

*Then problem (1.1)-(1.2) has a solution on $J$.*

3.2. **Nonconvex case.** Suppose that the multivalued function $F : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ in (1.1) has nonempty compact (nonconvex) values. We assign to $F$ the multivalued operator $\mathcal{F} : C(J, \mathbb{R}) \to \mathcal{P}(L^1(J, \mathbb{R}))$ defined by $\mathcal{F}(x) = S^1_F(x)$, where $S^1_F(x)$ is given by (2.1). We say that $F$ is of lower semi-continuous type (in brief l.s.c. type) if the operator $\mathcal{F}$ has property (BC), that is,

1) $\mathcal{F}$ is l.s.c.,
2) $\mathcal{F}$ has nonempty closed and decomposable values.

The following selection result [1] due to Bressan and Colombo and Lemma 3.6 below are of great importance in the proof of Theorem 3.8.

**Lemma 3.5.** *Let $\mathcal{F} : C(J, \mathbb{R}) \to \mathcal{P}(L^1(J, \mathbb{R}))$ be a multivalued operator which has property (BC). Then $\mathcal{F}$ has a continuous selection, that is, there exists a continuous function (single valued) $f_0 : C(J, \mathbb{R}) \to L^1(J, \mathbb{R})$ such that $f_0(x) \in \mathcal{F}(x)$ for all $x \in C(J, \mathbb{R})$.*

**Lemma 3.6.** [5] *Let $F : J \times \mathbb{R} \to \mathcal{P}(\mathbb{R})$ be a multivalued function with nonempty compact values. Assume (C1) and (C3)-(i) hold. Then $F$ is of l.s.c. type.*

For the proof of Theorem 3.8, we rely on the well-known Leray-Schauder nonlinear alternative for single valued functions [4].

**Theorem 3.7.** *Let $X$ be a Banach space and $U$ an open and bounded subset of $X$ with $0 \in U$. Suppose that $\Gamma : \overline{U} \to X$ is a continuous and completely continuous operator. Then, either*

(i) *$\Gamma$ has a fixed point in $\overline{U}$, or*
(ii) *there exists a $x \in \partial U$ (the boundary of $U$) and a $\lambda \in (0, 1)$ with $x = \lambda\Gamma x$.*

Now, our main result of this section reads as follows.

**Theorem 3.8.** *Assume that conditions (C1), (C2) and (C3) hold. Then problem (1.1)-(1.2) has a solution on $J$.*

*Proof.* By Lemma 3.6 together with Lemma 3.5, the multivalued operator $\mathcal{F}$ defined above has a continuous selection $f_0 : C(J, \mathbb{R}) \to L^1(J, \mathbb{R})$ such that $f_0(x) \in \mathcal{F}(x)$ for all $x \in C(J, \mathbb{R})$. By analogy with the single valued case, we denote $f(\cdot, x(\cdot)) = f_0(x)(\cdot)$, for any $x \in C(J, \mathbb{R})$.

Consider then the problem

$$x''(t) = f(t, x(t)), \quad \text{a.e. } t \in J, \tag{3.3}$$

$$x(0) - k_1 x'(0) = \int_0^1 h_1(x(s))ds, \qquad x(1) + k_2 x'(1) = \int_0^1 h_2(x(s))ds. \tag{3.4}$$

It is clear that if $x \in AC^1(J,\mathbb{R})$ is a solution of (3.3)-(3.4), then $x$ is a solution to the problem (1.1)-(1.2).

Integrating (3.3) on $[0,t]$ for $t \in J$, problem (3.3)-(3.4) becomes equivalent to the integral equation $x(t) = (\Gamma x)(t)$ where the operator $\Gamma : C(J,\mathbb{R}) \to C(J,\mathbb{R})$ is given by

$$(\Gamma x)(t) = P(t) + \int_0^1 G(t,s) f(s,x(s)) ds, \quad x \in C(J,\mathbb{R}), \quad t \in J,$$

where the functions $P$ and $G$ are as in (3.1) and (3.2), respectively.

We will prove that $\Gamma$ fulfills the hypotheses of Theorem 3.7.

We first show that $\Gamma$ is continuous. To this end, let $\{x_n\}$ with $x_n \to x$ in $C(J,\mathbb{R})$. After some standard calculations we obtain, for $t \in J$,

$$\begin{aligned} |(\Gamma x_n)(t) - (\Gamma x)(t)| \leq \|h_1(x_n(\cdot)) - h_1(x(\cdot))\|_{L^1} + \|h_2(x_n(\cdot)) - h_2(x(\cdot))\|_{L^1} \\ + C_0 \|f(\cdot, x_n(\cdot)) - f(\cdot, x(\cdot))\|_{L^1}. \end{aligned} \tag{3.5}$$

Let $B = \{u \in C(J,\mathbb{R}) : \|u\| \leq r\}$ for some $r > 0$ such that $\|x_n\|, \|x\| \leq r$, for all $n \in \mathbb{N}$. Since, by (C3)-(i),

$$|f(s,x_n(s)) - f(s,x(s))| \leq 2\psi(s,r), \text{ a.e. on } J,$$

then by the continuity of $h_1$, $h_2$ and $f$ in its second variable and the Lebesgue's convergence theorem, from (3.5) we deduce that $\Gamma x_n \to \Gamma x$; which completes the proof that $\Gamma$ is continuous.

Now, as the proofs that $\Gamma$ is completely continuous and that the second alternative in Theorem 3.7 is deactivate follow the same lines as in the proof that the operator $\Gamma$ in the proof of Theorem 3.3 possesses the same property and that the second alternative in Theorem 3.2 does not occur, they are omitted.

The conclusion of our theorem follows immediately by Theorem 3.7. □

## References


[1] A. Bressan and G. Colombo, *Extensions and selections of maps with decomposable values*, Studia Math. **90** (1988), 70-85.

[2] S. A. Brykalov, *Nonconvex differential inclusions with nonlinear monotone boundary conditions*, Georgian Math. J. **4** (1997), No. 6, 501-508.

[3] S. A. Brykalov, *A second order nonlinear problem with two-point and integral boundary conditions*, Georgian Math. J. **1** (1994), No.3, 243-249.

[4] J. Dugundji and A. Granas, *Fixed Point Theory*, Springer Monographs in Mathematics, Springer, New York, 2003.

[5] M. Frigon and A. Granas, *Théorèmes d'existence pour des inclusions différentielles sans convexité*, C.R. Acad. Sci. Paris Ser. I Math. **310** (12) (1990), 819-822.

[6] J. M. Gallardo, *Second order differential operators with integral boundary conditions and generation of semigroups*, Rocky Mountain J. Math. **30** (2000), 1265-1292.

[7] N. Halidias and N. S. Papageorgiou, *Second order multivalued boundary value problems*, Arch. Math. (Brno) **34** (1998), No. 2, 267-284.

[8] G. L. Karakostas and P. Ch. Tsamatos, *Multiple positive solutions of some Fredholm integral equations arisen from nonlocal boundary-value problems*, Electron. J. Diff. Eqns., Vol. 2002 (2002), **30**, 1-17.

[9] A. Lasota and Z. Opial, *An application of the Kakutani-Ky Fan theorem in the theory of ordinary differential equations*, Bull. Acad. Pol. Sci. Ser. Sci. Math. Astronom. Phys. **13** (1965), 781-786.

[10] A. Lomtatidze and L. Malaguti, *On a nonlocal boundary-value problems for second order nonlinear singular differential equations*, Georg. Math. J. **7** (2000), 133-154.

[11] D. O'Regan, *Nonlinear alternatives for multivalued maps with applications to operator inclusions in abstract spaces*, Proc. Amer. Math. Soc., Vol. 127, **12** (1999) 3557-3564.

[12] A. K. Rahmat, *The generalized method of quasilinearization and nonlinear boundary value problems with integral boundary conditions*, Electron. J. Qual. Theo. Diff. Eqns. (2003), **10**, 1-15.

[13] B. Rudolf, *Method of lower and upper solutions for a generalized boundary value problem*, Arch. Math. (Brno) **36** (2000), No. 4, 595-602.

Laboratoire de Mathématiques, Université de Sidi Bel Abbès, BP 89, 22000, Sidi Bel Abbès, Algérie

*E-mail address*: mlakrib@univ-sba.dz

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 101–109
ISSN 1930-1235: (electronic version)

# A NOTE ON INEQUALITIES IN MULTIFUNCTIONAL ANALYTIC SPACES

SONGXIAO LI AND ROMI SHAMOYAN

Abstract. A general method"weighted method" will be presented which allows to extend various inequalities for one function case to inequalities for multifunctional case in the unit disk, unit ball and polydisk.

## 1. Introduction

Let $n \in \mathbb{N}$ and $\mathbb{C}^n = \{z = (z_1, ..., z_n) \ |z_k \in \mathbb{C}, 1 \leq k \leq n\}$ be the n-dimensional space of complex coordinates. Let $U^n$ be the unit polydisk of $\mathbb{C}^n$, i.e. $U^n = \{z \in \mathbb{C}^n| \ |z_k| < 1, 1 \leq k \leq n\}$, $T^n$ the distinguished boundary of $U^n$. We use $m_{2n}$ to denote the volume measure on $U^n$ given by $m_{2n}(U^n) = 1$. We use $m_{2n,\alpha} = \prod_{i=1}^n (1-|z_i|^2)^\alpha m_{2n}$ to denote the weighted measure on $U^n$. $dm_1$ is the standard Lebesgue measure on $T$. Let $H(U^n)$ be the space of all bounded holomorphic functions on $U^n$. We write as usual (see [1,10]) $z \cdot w = (z_1 w_1, \dots, z_n w_n)$, $z, w \in \mathbb{C}^n$; $e^{i\theta} = (e^{i\theta_1}, \dots, e^{i\theta_n})$, $d\theta = d\theta_1 \cdots d\theta_n$. When we write $0 \leq \vec{r} < 1$, where $\vec{r} = (r_1, \dots, r_n)$, this means that $0 \leq r_i < 1$ $(i = 1, \dots, n)$. The Hardy space $H^p(U^n)\,(0 < p < \infty)$ on $U^n$ can be defined in a standard way as following:

$$H^p(U^n) = \{f \in H(U^n) : \ \frac{1}{(2\pi)^n} \sup_{0 \leq \vec{r} < 1} \int_{[0,2\pi]^n} |f(\vec{r} \cdot e^{i\theta})|^p d\theta < \infty\}.$$

For $\vec{\alpha} > -1, 0 < p < \infty$, recall that the weighted Bergman space $A^p_{\vec{\alpha}}(U^n)$ consists of all holomorphic functions on the polydisk satisfying the condition

$$\|f\|^p_{A^p_{\vec{\alpha}}} = \int_{U^n} |f(z)|^p \prod_{i=1}^n (1-|z_i|^2)^{\alpha_i} dm_{2n} < \infty.$$

Let $\mathbb{B}_n$ be the unit ball in $\mathbb{C}^n$ and $dv$ be the normalized Lebesgue measure of $\mathbb{B}_n$ (i.e. $v(\mathbb{B}_n) = 1$). The boundary of $\mathbb{B}_n$ will be denoted by $S$ and is called the unit sphere in $\mathbb{C}^n$. The surface measure on $S$ will be denoted by $d\sigma$. We denote the class of all holomorphic functions on the unit ball by $H(\mathbb{B}_n)$. Let $z = (z_1, \dots, z_n)$ and $w = (w_1, \dots, w_n)$ be points in $\mathbb{C}^n$, we write

$$\langle z, w\rangle = z_1\overline{w}_1 + \cdots + z_n\overline{w}_n, \ |z| = \sqrt{|z_1|^2 + \cdots + |z_n|^2}.$$

The Hardy space $H^p(\mathbb{B}_n)\,(0 < p < \infty)$ on $\mathbb{B}_n$ is defined by (see [16])

$$H^p(\mathbb{B}_n) = \{f \in H(\mathbb{B}_n) : \|f\|_{H^p(\mathbb{B}_n)} = \sup_{0 \leq r < 1} M_p(f, r) < \infty\},$$

---

1991 *Mathematics Subject Classification.* 47B35 and 30H05.

This research is supported in part by the NSF of Guangdong Province of China (No.73006147).

where

$$M_p(f,r)=\left(\int_S |f(r\zeta)|^p d\sigma(\zeta)\right)^{1/p},\ r\in(0,1).$$

For real parameter $\alpha>-1$ we consider the weighted volume measure $dv_\alpha(z)=(1-|z|^2)^\alpha dv(z)$. Suppose $0<p<\infty$ and $\alpha>-1$, recall that the weighted Bergman space $A^p_\alpha$ on the unit ball consists of those functions $f\in H(\mathbb{B}_n)$ for which

$$\|f\|^p_{A^p_\alpha}=\int_{\mathbb{B}_n}|f(z)|^p dv_\alpha(z)<\infty.$$

For $f\in C^1(\mathbb{B}_n)$, the invariant gradient $\widetilde{\nabla}f$ is defined by $(\widetilde{\nabla}f)(z)=\nabla(f\circ\varphi_z)(0)$, where $\nabla f$ is the complex gradient of $f$, i.e.

$$\nabla f(z)=\left(\frac{\partial f}{\partial z_1}(z),\dots,\frac{\partial f}{\partial z_n}(z)\right).$$

For $f\in H(\mathbb{B}_n)$ and $z\in B$, set

$$Q_f(z)=\sup_{w\in\mathbb{C}^n\setminus\{0\}}\frac{|\langle\nabla f(z),\bar{w}\rangle|}{(H_z(w,w))^{1/2}},$$

where $H_z(w,w)$ is the Bergman metric on $\mathbb{B}_n$, i.e.

$$H_z(w,w)=\frac{n+1}{2}\frac{(1-|z|^2)|w|^2+|\langle w,z\rangle|^2}{(1-|z|^2)^2}.$$

The Bloch space $\mathcal{B}$, which was introduced by Timoney (see [14, 15]), is the space of all $f\in H(\mathbb{B}_n)$ for which

$$\|f\|_{\mathcal{B}}=\sup_{z\in\mathbb{B}_n}Q_f(z)<\infty.$$

It is well known that $f\in\mathcal{B}$ if and only if $\sup_{z\in\mathbb{B}_n}(1-|z|^2)\,|\nabla f(z)|<\infty$.

For $1<p<\infty$, recall that the Möbius invariant Besov space $B_p$ consists of those holomorphic functions $f$ for which $Q_f$ is $p$-integrable function with respect to the invariant measure $d\lambda(z)$. Here $d\lambda(z)=(1-|z|^2)^{-n-1}dv(z)$ is a Möbius invariant measure, that is for any $\psi\in Aut(\mathbb{B}_n)$ and $f\in L^1(\mathbb{B}_n)$,

$$\int_{\mathbb{B}_n}f(z)d\lambda(z)=\int_{\mathbb{B}_n}f\circ\psi(z)d\lambda(z).$$

From [2], we know that for $n\geq 2$, the Besov space is nontrivial if and only if $p>2n$.

The following inequality is a direct consequence of diagonal-mapping Theorem (see [1,12]) and the subharmonicity of $|f(z)|^p$,

$$\int_U|f(z,\cdots,z)|^p(1-|z|^2)^{\alpha_1+\cdots+\alpha_n+2n-2}dm_2(z)\leq C\|f\|^p_{A^p_{\vec{\alpha}}},\tag{1}$$

where $0<p<\infty$, $\vec{\alpha}=(\alpha_1,\cdots,\alpha_n)>-1$, $j=1,\cdots,n$, $f\in H(U^n)$.

If we put $f=f_1\cdots f_n$ in (1), then we get new inequality, i.e.

$$\begin{aligned}&\int_U\prod_{i=1}^n|f_i(z)|^p(1-|z|^2)^{\alpha_1+\cdots+\alpha_n+2n-2}dm_2(z)\\ &\leq\ C\int_{U^n}\prod_{i=1}^n|f_i(z_i)|^p\prod_{k=1}^n(1-|z_k|^2)^{\alpha_k}dm_{2n}(z).\end{aligned}\tag{2}$$

Running from one function to $n$ different functions in this simple example we see, the appearance of the certain weight. More concretely the additional weight $(1-$

$|z|^2)^{2n-2}$ appeared in our inequality with the addition of the amount of functions. The main goal of this note is to try to understand the connection of this weight with the structure of the Bergman space or other holomorphic function spaces, then try to generalize this effect and to find other cases where the similar change will occur during the very natural process of addition of the amount of functions in various inequalities for one holomorphic function, i.e. to generalize (2) and get various generalizations of the known theorem from one functional case to multifunctional case, that is to get estimate for more general expression of the type $|f_1|^{q_1}\cdots|f_k|^{q_k}, 0 < q_j < \infty, j = 1, \cdots, k$.

Throughout this paper, constants are denoted by $C$, they are positive and may differ from one occurrence to the other. The notation $A \asymp B$ means that there is a positive constant $C$ such that $B/C \le A \le CB$.

## 2. Main result

We propose a general method which we call "weight method". The main tool is the following vital theorem.

**Theorem A.** *Let $\mu$ be a positive Borel measure on $Y$, $X_i, Y$ be any quasi normed spaces, $\beta, q_i \in (0, \infty)$, $i = 1, \cdots, k$. If*

$$\sup_{z\in Y} |f_i|^{q_i}(1-|z|^2)^{\beta} \le C\|f_i\|^{q_i}_{X_i}, i = 1, 2, \cdots, k. \tag{3}$$

*and*

$$\int_Y |f_1(z)|^{q_1} d\mu(z) \le C\|f_1\|^{q_1}_{X_1},$$

*then*

$$\int_Y \prod_{i=1}^{k} |f_i|^{q_i}(1-|z|^2)^{\beta k-\beta} d\mu(z) \le C\|f_1\|^{q_1}_{X_1} \cdots \|f_k\|^{q_k}_{X_k}. \tag{4}$$

*Proof.* We use induction. For $k = 1$, we are lead to have the estimate

$$\int_Y |f_1|^{q_1} d\mu(z) \le C\|f_1\|^{q_1}_{X_1}.$$

This is obvious. Assume that (4) is true for $k$, let us prove that (4) is also true for $k + 1$. We have

$$\begin{aligned}
&\int_Y \prod_{i=1}^{k+1} |f_i(z)|^{q_i}(1-|z|^2)^{\beta k-\beta}(1-|z|^2)^{\beta} d\mu(z)\\
\le\ & \Big(\sup_{z\in Y} |f_{k+1}(z)|^{q_{k+1}}(1-|z|^2)^{\beta}\Big)\Big(\int_Y \prod_{i=1}^{k} |f_i|^{q_i}(1-|z|^2)^{\beta k-\beta} d\mu(z)\Big)\\
\le\ & C\Big(\sup_{z\in Y} |f_{k+1}(z)|^{q_{k+1}}(1-|z|^2)^{\beta}\Big)\prod_{i=1}^{k} \|f_i\|^{q_i}_{X_i}\\
\le\ & C\prod_{i=1}^{k+1} \|f_i\|^{q_i}_{X_i}.
\end{aligned}$$

**Remark 1.** Uniform estimates are known for functions from many holomorphic spaces in the unit disk, polydisk, unit ball (see [1, 3, 10, 16] and references therein).

Hence we can put instead of $X_i$ various spaces including Bergman, Hardy, BMOA, $Q_p$, mixed norm spaces, Lipschitz and holomorphic Lizorkin Triebel classes (see [7, 8, 9, 11, 13]). Using these uniform estimates(analogues of (3)) and the one functional result we will get the multifunctional generalization of many concrete one functional inequalities (for example from recent Zhu's book [16]) by simple induction as we did in Theorem A. On that way a certain weight of the type $(1-|z|^2)^t$, with some fixed $t$, depending on the structure of the quasi norm of the space, will appear. We will give below two simple concrete examples for Hardy and weighted Bergman spaces in the unit disk, then turning our attention to the case of the unit ball $\mathbb{B}_n$.

For $0 < p < \infty,\ \alpha > -1,\ f \in A^p_\alpha,\ z \in U$, we have (see [3])

$$|f(z)| \leq \frac{C\|f\|_{A^p_\alpha}}{(1-|z|^2)^{(2+\alpha)/p}}.$$

Let $Y = U$. From Theorem A, we obtain the following corollaries immediately.

**Corollary 1.** *Assume that $f_i \in A^{q_i}_\alpha,\ q_i \in (0,\infty),\ \alpha \in (-1,\infty), i = 1,\cdots,k, i \in \mathbb{N}$. Then the following inequality holds.*

$$\int_U \Big(\prod_{i=1}^k |f_i(z)|^{q_i}\Big)(1-|z|^2)^{2k-2}(1-|z|^2)^{k\alpha} dm_2(z) \leq C\prod_{i=1}^k \|f_i\|^{q_i}_{A^{q_i}_\alpha}. \tag{5}$$

**Corollary 2.** *Assume that $f_i \in H^{p_i},\ p_i \in (0,\infty),\ i = 1,\cdots,k, i \in \mathbb{N}$. Then the following inequality holds.*

$$\int_U \prod_{i=1}^k |f_k(z)|^{p_i}(1-|z|^2)^{k-1} dm_1(z) \leq C\prod_{i=1}^k \|f_i\|^{p_i}_{H^{p_i}}. \tag{6}$$

**Remark 2.** As we noticed in Corollary 1 for Bergman spaces the transferring from one function case to $k$ function case needs the addition of $(1-|z|^2)^{2k-2}$, for Hardy space as the Corollary 2 shows the weight is $(1-|z|^2)^{k-1}$.

## 3. Multifunctional inequalities in higher dimension

The same approach can be developed much further, clearly we can easily note that the main part of our method is based on uniform estimates of function $|f(z)|,\ f \in X \subset H(U)$ (or even in more general form $X \subset H(\Omega)$, where $\Omega$ is the unit ball or the polydisk in $\mathbb{C}^n$). The next aim is to show that Corollaries 1 and 2 are also true for the unit ball and polydisk, uniform estimates that we used in the disk for Hardy space $H^p$ and Bergman space $A^p_\alpha$ should be transferred to unit ball. The following inequalities are well known.

$$|f(z)| \leq \frac{C\|f\|_{A^p_\alpha}}{(1-|z|^2)^{(n+1+\alpha)/p}},\ 0 < p < \infty,\ \alpha > -1,\ f \in A^p_\alpha,\ z \in \mathbb{B}_n$$

and

$$|f(z)| \leq \frac{C\|f\|_{H^p}}{(1-|z|)^{n/p}},\ 0 < p < \infty,\ f \in H^p,\ z \in \mathbb{B}_n.$$

A big amount of results in the unit ball from [16] can be extended from one functional case to multifunctional case using addition of some weight and induction

and some simple multifunction of ideas that we used above. For $f \in H(\mathbb{B}_n)$, $0 < p < \infty,\ \alpha > -1$, we have (see, e.g. [16])

$$\int_{\mathbb{B}_n} |f(z)|^p dv_\alpha(z) \le C \int_{\mathbb{B}_n} |\widetilde{\nabla} f(z)|^p dv_\alpha(z) = A_1(f);$$

$$\int_{\mathbb{B}_n} |f(z)|^p dv_\alpha(z) \le C \int_{\mathbb{B}_n} |\nabla f(z)|^p (1-|z|^2)^p dv_\alpha(z) = A_2(f);$$

$$\int_{\mathbb{B}_n} |f(z)|^p dv_\alpha(z) \le C \int_{\mathbb{B}_n} |\mathcal{R} f(z)|^p (1-|z|^2)^p dv_\alpha(z) = A_3(f).$$

Here $\mathcal{R}f$ denotes the radial derivative of $f$, that is, $\mathcal{R}f(z) = \sum_{j=1}^n z_j \frac{\partial f}{\partial z_j}(z)$. Now we have the following generalization.

**Theorem 1.** *The following equalities hold.*

$$\int_{\mathbb{B}_n} |f_1|^{p_1} \cdots |f_k|^{p_k} (1-|z|^2)^{k(n+1)-(n+1)} \times (1-|z|^2)^{\alpha_1} \cdots (1-|z|^2)^{\alpha_k} dv(z)$$

$$(7) \le \quad C \prod_{i=1}^k A_j(f_i),\ j = 1, 2, 3,$$

*where* $0 < p_i < \infty,\ \alpha_i > -1,\ f_i \in A^{p_i}_{\alpha_i}, i = 1, \cdots, n.$

*Sketch of Proof.* All inequalities in theorem 1 can be proved similarly. We use induction and the estimate

$$|f(z)| \le \frac{C\|f\|_{A^{p_i}_{\alpha_i}}}{(1-|z|^2)^{(n+1+\alpha_i)/p_i}},\ 0 < p_i < \infty,\ \alpha_i > -1,\ f_i \in A^{p_i}_{\alpha_i}, i = 1, \cdots, n$$

and proceed similarly as in the proof of Theorem A. Note that in the unit disk we have weight $2k-2$ and in ball $k(n+1)-(n+1)$.

The following inequality is contained in [16]. For every $p \in (1, \infty)$ there exists a positive constant $C$ such that

$$(8)\ \int_S |f(\tau\xi)|^p d\sigma(\xi) \le C \int_S |f(\xi)|^p d\sigma(\xi) \le C \int_S |Ref(\xi)|^p d\sigma(\xi),\ \tau \in (0,1)$$

for all $f \in H^p(\mathbb{B}_n)$ with $f(0) = 0$. Again based on induction and the one functional result we have the following extension of (8).

**Theorem 2.** *For every $p_i \in (1, \infty)$, there exists a positive constant $C$ such that*

$$(9) \qquad \Big( \int_S \prod_{i=1}^k |f_i(\tau\xi)|^{p_i} d\sigma(\xi) \Big) (1-\tau)^{n(k-1)} \le C \prod_{i=1}^k \int_S |Ref_i(\xi)|^{p_i} d\sigma(\xi),$$

*for all $f_i \in H^{p_i}$ with $f_i(0) = 0, i = 1, \cdots, k$, where $\tau \in (0,1)$.*

*Proof.* Let $k = 1$. Then we have one functional result, i.e. (8). Suppose the result is true for the case of $k$, let us prove the case of $k+1$. Since for any $f \in H^{p_i}, i = 1, \cdots, k+1$,

$$\sup_{z \in \mathbb{B}_n} |f(z)|(1-|z|^2)^{n/p_i} \le C\|f\|_{H^{p_i}} \asymp C \int_S |f(\xi)|^p d\sigma(\xi),$$

we have

$$\begin{aligned}
&\Big(\int_S \prod_{i=1}^{k+1} |f_i(\tau\xi)|^{p_i} d\sigma(\xi)\Big)(1-\tau)^{nk} \\
\leq\ & C\Big(\sup_{\xi\in S} |f_{k+1}(\tau\xi)|^{p_{k+1}}(1-|\tau\xi|^2)^n\Big)\cdot\Big(\int_S \prod_{i=1}^{k} |f_i(\tau\xi)|^{p_i} d\sigma(\xi)\Big)(1-\tau)^{n(k-1)} \\
\leq\ & C\Big(\sup_{z\in\mathbb{B}_n} |f_{k+1}(z)|^{p_{k+1}}(1-|z|^2)^n\Big)\cdot\Big(\prod_{i=1}^{k}\int_S |Ref_i|^{p_i} d\sigma(\xi)\Big) \\
\leq\ & C\int_S |f_{k+1}(\xi)|^{p_{k+1}} d\sigma(\xi)\cdot\Big(\prod_{i=1}^{k}\int_S |Ref_i|^{p_i} d\sigma(\xi)\Big) \\
\leq\ & C\prod_{i=1}^{k+1}\int_S |Ref_i|^{p_i} d\sigma(\xi),\ \tau\in(0,1).
\end{aligned}$$

The following result is also contained in [16]. For every $p\in[1,\infty)$ and $\alpha>-1$, there exists a positive constant $C$ such that

$$\int_{\mathbb{B}_n} |f(z)|^p dv_\alpha(z) \leq C\int_{\mathbb{B}_n} |Ref(z)|^p dv_\alpha(z) \tag{10}$$

for all $f\in H(\mathbb{B}_n)$ with $f(0)=0$. Again based on induction and the one functional result we have the following extension of (10).

**Theorem 3.** *For every $p_i\in[1,\infty)$, there exists a positive constant $C$ such that*

$$\int_{\mathbb{B}_n} \prod_{i=1}^{k} |f_i(z)|^{p_i}(1-|z|^2)^{\frac{n+1+\alpha}{p}(k-1)} dv(z) \leq C\prod_{i=1}^{k}\int_{\mathbb{B}_n} |Ref_i(z)|^{p_i} dv_\alpha(z), \tag{11}$$

*for all $f_i\in H(\mathbb{B}_n)$ with $f_i(0)=0, i=1,\cdots,k$.*

Let

$$\beta(z,w)=\frac{1}{2}\log\frac{1+|\varphi_z(w)|}{1-|\varphi_z(w)|}$$

be the Bergman metric between two points $z$ and $w$ in $\mathbb{B}_n$. The following results can be found in [16].

**Lemma 1.** *Let $f\in H(\mathbb{B}_n)$ and $1\leq p\leq\infty$. Then $f\in B_p$ if and only if*

$$|f(z)-f(w)|\leq C_p(\beta(z,w))^{1/q},$$

*where $1/p+1/q=1$.*

Using Lemma 1 and ideas we used on Theorem A we can get various multifunctional generalizations of theorems from [16]. We give several examples for Besov spaces.

**Theorem 4.** *Let*

$$\lambda_n=\begin{cases} 1 & , \quad n=1 \\ 2n & , \quad n>1 \end{cases}.$$

*Let $f_i\in H(\mathbb{B}_n), i=1,\ldots,k$, $k\in\mathbb{N}$, $\lambda_n<p<\infty$, $0<q<\infty$ such that $\frac{1}{p}+\frac{1}{q}=1$. Then the following statements holds.*

*(1)*

$$\int_{\mathbb{B}_n}\int_{\mathbb{B}_n}\frac{\prod_{i=1}^k|f_i(z)-f_i(w)|^p(1-|z|^2)^{p/2}(1-|w|^2)^{p/2}(\beta(z,w))^{(pk-p)/q}}{|w-P_w(z)-(1-|w|^2)^{1/2}Q_w(z)|^p}d\lambda(z)d\lambda(w)$$
$$\leq C\prod_{i=1}^k\|f_i\|_{B_p}^p,$$

*where $P_w$ is the orthogonal projection into the space spanned by $w$ and $Q_w=I-P_w$.*

*(2)*

$$\int_{\mathbb{B}_n}\int_{\mathbb{B}_n}\frac{\prod_{i=1}^k|f_i(z)-f_i(w)|^p(1-|z|^2)^{p/2}(1-|w|^2)^{p/2}(\beta(z,w))^{(pk-p)/q}}{|w-z|^p}d\lambda(z)d\lambda(w)$$
$$\leq C\prod_{i=1}^k\|f_i\|_{B_p}^p.$$

*(3)*

$$\int_{\mathbb{B}_n}\int_{\mathbb{B}_n}\frac{\prod_{i=1}^k|f_i(z)-f_i(w)|^p(1-|z|)^{\alpha}(1-|w|)^{\alpha}(\beta(z,w))^{(pk-p)/q}}{|1-\langle z,w\rangle|^{2(n+1+\alpha)}}dv(z)dv(w)$$
$$\leq C\prod_{i=1}^k\|f_i\|_{B_p}^p,$$

*where $\alpha>-1$.*

*(4) Let $w_r(f)(z)=\sup\{|f(z)-f(w)|:w\in D(z,r)\}$, where $D(z,r)=\{w\in\mathbb{B}_n:\beta(w,z)<r\}$. If $r>0$, then*

$$w_r(f_1\cdots f_k)(z) = \sup_{w\in D(z,r)}|f_1(z)-f_1(w)|\cdots|f_k(z)-f_k(w)|\times(\beta(z,w))^{(k-1)/q}$$
$$\leq C\prod_{i=1}^k\|f_i\|_{B_p}.$$

**Remark 3.** When $k=1$, the results in (1), (3) and (4) were proved in [6] (or see [16]) and the result in (2) was proved in [5].

It should be noted that many so called multifunctional inequalities can be delivered in a prepared form from various inequalities from polydisk function theory (see, e.g. [1]). The simple idea is to cut one analytic function in the polydisk to $n$ pieces, $f(z_1,\cdots,z_n)=f_1(z_1)\cdots f_n(z_n)$. But in this case the amount of functions will always be equal to the dimension and all $q_i$ in $|f_1|^{q_1}\cdots|f_n|^{q_n}$ will be equal to each other. We will give two examples.

**Proposition 1.** *(Extension of Riesz inequality) Let $2\leq p\leq q<\infty$, $k=(k_1,\cdots,k_n)$, $k_j\in\mathbb{N}$, $j=1,\cdots,n$. Then*

$$\int_0^1\cdots\int_0^1\prod_{i=1}^n(1-|z_i|)^{k_iq+qp-1}\left|\frac{\partial^{k_1}f_1(z_1)}{\partial z_1^{k_1}}\right|^q\cdots\left|\frac{\partial^{k_n}f_n(z_n)}{\partial z_n^{k_n}}\right|^q d|z_1|\cdots d|z_n|$$
$$\leq \prod_{i=1}^n\int_T|f_i(\xi)|^p dm_1(\xi).$$

The proof of Proposition 1 is a direct consequence of a polydisk version of M. Riesz inequality (see [1]).

**Theorem 5.** *Let $\mu$ be a Borel measure in $U^n$, $k=(k_1,k_2,\cdots,k_n)\in\mathbb{Z}_+^n$, $k_j\neq 0$, $1\leq j\leq n$, $\triangle_l(w)=\{z\in U^n : 1-l_j<|z_j|<1; |argw_j-argz_j|<l_j/2\}$, $l=(l_1,\cdots,l_n)$, $0<l_j<1$, $j=1,\cdots,n$, $w\in T^n$. Then the following two assertions are equivalent*

*1)*

$$\int_{U^n}|\frac{\partial^{k_1}}{\partial z_1^{k_1}}f_1(z_1)|^p\cdots|\frac{\partial^{k_n}}{\partial z_n^{k_n}}f_n(z_n)|^p d\mu(z)\leq C\prod_{k=1}^n\int_T|f_k(\xi)|^p dm_1(\xi),$$

*if $f_k\in H^p(U), 2\leq p<\infty$, $k=1,\cdots,n$.*

*2) $\mu(\triangle_l(w))\leq Cl_1^{k_1p+1}\cdots l_n^{k_np+1}, 2\leq p<\infty$, $k_j\in\mathbb{Z}_+$, $j=1,\cdots,n$.*

*Proof.* The implication *1)* $\Rightarrow$ *2)* is a direct consequence of using test function

$$f_j(z_j)=\big(\frac{1-\tau_j^2}{1-\tau_j z_j}\big)^{1/p},\ 0<|\tau_j|<1,\ z_j\in U,\ 1\leq j\leq n.$$

The reverse was proved in a book of Djrbashian and Shamoian (see [1]) even for all $f\in H^p(U^n)$(we need only those $f\in H^p(U^n)$ such that $f=f_1\cdots f_n$, where $f_k\in H^p(U), k=1,\cdots,n.$).

**Remark 4.** It should be point out that there are concrete cases when the addition of the amount of functions does not change the structure of the equalities and inequalities, so we just add functions without any additional weight. For example, since

$$\int_{\mathbb{B}_n}|\widetilde{\nabla}f(z)|^p dv_\alpha(z)\leq C\int_{\mathbb{B}_n}|f(z)|^p dv_\alpha(z),\ 0<p<\infty,\ \alpha>-1, f\in H(\mathbb{B}_n),$$

we get

$$\int_{\mathbb{B}_n}|\widetilde{\nabla}(f_1(z)\cdots f_n(z))|^p dv_\alpha(z)\leq C\int_{\mathbb{B}_n}\prod_{i=1}^n|f_i(z)|^p dv_\alpha(z),\ 0<p<\infty,\ \alpha>-1.$$

Hence the addition of the amount of functions does not mean that the addition weight will always appear.

**Remark 5.** Apparently(since these all ideals and proofs are not complicated) the similar "weight effects" will also appear in inequalities for several functions for Hardy, Bergman classes in various domains $G$ in $\mathbb{C}^n$, the classical weight $(1-|z|^2)^t$ must be replaced in this case by $dist(z,\partial G)$, the distance from a point in $G$ to the boundary of the domain, see [4].

## References


[1] A. E. Djrbashian and F. A. Shamoian, *Topics in the Theory of $A^p_\alpha$ Spaces*, Leipzig, Teubner, 1988.

[2] K. T. Hahn and E. H. Youssfi, Möbius invariant Besov $p$-spaces and Hankel operators in the Bergman space on the unit ball, *Complex Variables,* **17** (1991), 89-104.

[3] H. Hedenmalm, B. Korenblum and K. Zhu, *Theory of Bergman Spaces*, Graduate Texts in Mathematics, 199. Springer-Verlag, New York, 2000.

[4] S. G. Krantz, *Function Theory of Several Complex Variables*, Pure and Applied Mathematics, A Wiley-Interscience Publication. John Wiley Sons, Inc., New York, 1982.

[5] S. Li and H. Wulan, Besov space on the unit ball of $\mathbb{C}^n$, *Indian J. Math.* **48** (2) (2006), 177-186.

[6] M. Nowak, Bloch space and Möbius invariant Besov spaces on the unit ball on $\mathbb{C}^n$, *Complex Variables,* **44** (2001), 1-12.

[7] J. M. Ortega and J. Fabrega, Holomorphic Triebel-Lizorkin spaces, *J. Funct. Anal.* **151** (1) (1997), 177-212.

[8] J. M. Ortega and J. Fabrega, Hardy's inequality and embeddings in holomorphic Triebel-Lizorkin spaces, *Illinois J. Math.* **43** (4) (1999), 733-751.

[9] C. H. Ouyang, W. S. Yang and R. Zhao, $\mathcal{M}$öbius invariant $Q_p$ spaces associated with the Green function on the unit ball, *Pacific J. Math.* **182** (1998), 69-99.

[10] W. Rudin, *Function Theory in the Polydisk*, Benjamin, New York, 1969.

[11] F. A. Shamoyan, Applications of Dzhrbashyan integral representations to some problems of analysis, *Doklady Acad. Nauk USSR*, **261** (3) (1981), 557-561.

[12] F. A. Shamoyan, Diagonal mapping and problems of representation in anisotropic spaces of functions that are holomorphic in a polydisk, *Sibirsk. Mat. Zh.* **31** (2) (1990), 197-15.

[13] R. F. Shamoyan, Lizorkin-Triebel-type spaces of functions holomorphic in the polydisk, *Izv. Nats. Akad. Nauk Armenii Mat.* **37** (3)(2002), 57-78.

[14] R. M. Timoney, Bloch functions in several complex variables I, *Bull. London Math. Soc.* **12** (1980), 241-267.

[15] R. M. Timoney, Bloch functions in several complex variables II, *J. Reine Angew. Math.* **319** (1980), 1-22.

[16] K. Zhu, *Spaces of Holomorphic Functions in the Unit Ball*, New York, 2005.



Songxiao Li, Department of Mathematics, JiaYing University, MeiZhou, China
*E-mail address*: jyulsx@163.com

Hasi Wulan, Department of Mathematics, Bryansk State Pedagogical University, Russian
*E-mail address*: rsham@mail.ru

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 111–124
ISSN 1930-1235: (electronic version)

# NUMERICAL BLOW-UP AND ASYMPTOTIC BEHAVIOR FOR A SEMILINEAR PARABOLIC EQUATION WITH A NONLINEAR BOUNDARY CONDITION

DIABATE NABONGO AND THÉODORE K. BONI

Abstract. This paper concerns the study of the numerical approximation for the following initial-boundary value problem:

$$(P)\begin{cases} u_t(x,t) = u_{xx}(x,t) + au^p(x,t), \quad 0 < x < 1,\ t > 0, \\ u_x(0,t) = 0, \quad u_x(1,t) + bu^q(1,t) = 0, \quad t > 0, \\ u(x,0) = u_0(x) > 0, \quad 0 \le x \le 1, \end{cases}$$

where $a > 0$, $b > 0$ and $p > q > 1$. We show that under some conditions, the solution of a semidiscrete form of $(P)$ either decays uniformly to zero or blows up in a finite time. When the blow-up occurs, we estimate the semidiscrete blow-up time and prove that under some assumptions, the semidiscrete blow-up time converges to the real one when the mesh size goes to zero. When the semidiscrete solution goes to zero as $t$ goes to infinity, we give its asymptotic behavior. Finally, we give some numerical experiments to illustrate our analysis.

## 1. Introduction

Consider the following initial-boundary value problem:

$$u_t(x,t) = u_{xx}(x,t) + au^p(x,t), \quad 0 < x < 1, \quad t > 0, \tag{1}$$

$$u_x(0,t) = 0, \quad u_x(1,t) + bu^q(1,t) = 0, \quad t > 0, \tag{2}$$

$$u(x,0) = u_0(x) > 0, \quad 0 \le x \le 1, \tag{3}$$

where $a > 0$, $b > 0$, $p > q > 1$, $u_0 \in C^2([0,1])$,

$$u_0''(x) + au_0^p(x) > 0 \quad \text{in} \quad [0,1], \tag{4}$$

$$u_0'(0) = 0, \quad u_0'(1) + bu_0^q(1) = 0. \tag{5}$$

The particularity of this kind of problem is that the solution $u$ of (1)–(3) may develop singularities in a finite time. In other words, under some assumptions, there exists a finite time $T$ such that $\|u(\cdot,t)\|_\infty < +\infty$ for $t \in (0,T)$ but $\lim_{t\to T} \|u(\cdot,t)\|_\infty = +\infty$ where $\|u(\cdot,t)\|_\infty = \sup_{x\in[0,1]} |u(x,t)|$. In this case, we say that the solution $u$ blows up in a finite time and the time $T$ is called the blow-up time of the solution $u$. When $T$ is infinite, we say that the solution $u$ exists globally. The theoretical study of blow-up and asymptotic behavior of solutions for semilinear parabolic equations

1991 *Mathematics Subject Classification.* 35B40, 35B50, 35K60, 65M06.
*Key words and phrases.* semidiscretizations, semilinear parabolic equation, asymptotic behavior, convergence.

with nonlinear boundary conditions has been the subject of investigation of many authors (see [2]–[5], [7], [13], [14] and the references cited therein).
The fact that $p > 1$, $q > 1$ and the condition (5) ensure the local in time existence and the uniqueness of the solution of (1)–(3) which is regular (see for instance [2], [3], [7], [9], [13]).
Since $a > 0$, $b > 0$, $p > q > 1$, under the condition given in (4), it is also proved that the solution u of (1)–(3) blows up in a finite time and we have an upper bound of the blow-up time (see [2], [3], [7]).
Finally, it is shown that the solution u of (1)–(3) exists globally and decays uniformly to zero for small initial data (see [2], [4], [7]).

In this paper, we are interesting in the numerical study of (1)–(3). Let I be a positive integer and define the grid $x_i = ih$, $0 \leq i \leq I$, where $h = 1/I$. We approximate the solution u of the problem (1)–(3) by the solution $U_h(t) = (U_0(t), U_1(t), \ldots, U_I(t))^T$ of the following semidiscrete equations

$$\frac{d}{dt}U_i(t) = \delta^2 U_i(t) + a(U_i(t))^p, \quad 0 \leq i \leq I-1, \quad t > 0, \tag{6}$$

$$\frac{d}{dt}U_I(t) = \delta^2 U_I(t) + a(U_I(t))^p - \frac{2b}{h}(U_I(t))^q, \quad t > 0, \tag{7}$$

$$U_i(0) = \varphi_i > 0, \quad 0 \leq i \leq I, \tag{8}$$

where

$$\delta^2 U_i(t) = \frac{U_{i+1}(t) - 2U_i(t) + U_{i-1}(t)}{h^2}, \quad 1 \leq i \leq I-1,$$

$$\delta^2 U_0(t) = \frac{2U_1(t) - 2U_0(t)}{h^2}, \quad \delta^2 U_I(t) = \frac{2U_{I-1}(t) - 2U_I(t)}{h^2}.$$

For the initial data $\varphi_h = (\varphi_0, ..., \varphi_I)^T$, one may take $\varphi_i = u_0(x_i)$, $0 \leq i \leq I$ but this is not necessary. In fact, we shall see later that if $\varphi_h$ is close to $u_0(x)$, then the semidiscrete solution $U_h(t)$ approaches the continuous one (see Theorem 3.2 below).

We need the following definition.

**Definition 1.1.** *We say that the solution $U_h$ of (6)–(8) blows up in a finite time if there exists a finite time $T_h$ such that*

$$\|U_h(t)\|_\infty < +\infty \text{ for } t \in [0, T_h) \text{ but } \lim_{t \to T_h} \|U_h(t)\|_\infty = +\infty,$$

*where $\|U_h(t)\|_\infty = \max_{0 \leq i \leq I} |U_i(t)|$. The time $T_h$ is called the semidiscrete blow-up time of the solution $U_h(t)$.*

In this paper, under some assumptions on the initial data, we show that the solution $U_h(t)$ of (6)–(8) either blows up in a finite time or exists globally and decays uniformly to zero. In the case where the blow-up occurs, we show that the semidiscrete blow-up time converges to the real one when the mesh size goes to zero. When the solution decays uniformly to zero, we give its asymptotic behavior.

Our work was motived by the papers in [1], [6] and [11]. In [1] and [11], the authors have studied numerical blow-up for semilinear parabolic equations with Dirichlet boundary conditions. In this paper, the results obtained in the case of blow-up solutions generalize those found in [1] and [11] but this is not a simple generalization because of the nonlinearity of boundary conditions. Let us illustrate this fact. In the case where the semidiscrete solution blows up in a finite time, for

the convergence of the semidiscrete blow-up time, our proof is based on an idea of Friedman and McLeod in [8] and on the construction of an upper solution. In [1], an upper solution has been also used to prove the convergence of the semidiscrete blow-up time but in the present paper, because of the nonlinearity of boundary conditions, the upper solution constructed is not usual. Indeed, we construct a continuous upper solution and show after a semidiscretization that the discrete version of the above solution is a good candidate as an upper solution for the semidiscrete problem. Let us also notice that in [11], the author has proved the convergence of the discrete blow-up time for a solution which blows up in $L^p$ norm with $1 \leq p < +\infty$. This condition is restrictive because in general, one deals with solutions which blow up in $L^\infty$ norm. In [6], the phenomenon of extinction is investigated using some semidiscrete and discrete schemes (we say that a solution extincts in a finite time if it reaches the value zero in a finite time).

The rest of the paper is written in the following manner. In the next section, we prove some lemmas about the discrete maximum principle. In the third section, we show that under some assumptions, the solution $U_h(t)$ of (6)–(8) blows up in a finite time and estimate its semidiscrete blow-up time. We also prove that the blow-up time of the semidiscrete problem converges to the one of the continuous problem when the mesh size goes to zero. In the fourth section, we show that the solution of the semidiscrete problem goes to zero for small initial data and determine its asymptotic behavior. Finally in the last section, we construct two schemes and give some numerical results.

## 2. Properties of the semidiscrete scheme

In this section, we give some lemmas which will be used later.
The following lemma is a semidiscrete form of the maximum principle.

**Lemma 2.1.** *Let $a_h(t) \in C^0([0,T),\mathbb{R}^{I+1})$ and let $V_h(t) \in C^1([0,T),\mathbb{R}^{I+1})$ such that*

$$\frac{d}{dt}V_i(t) - \delta^2 V_i(t) + a_i(t)V_i(t) \geq 0, \quad 0 \leq i \leq I, \quad t \in (0,T), \tag{9}$$

$$V_i(0) \geq 0, \quad 0 \leq i \leq I. \tag{10}$$

*Then we have $V_i(t) \geq 0$ for $0 \leq i \leq I$, $t \in (0,T)$.*

*Proof.* Let $T_0 < T$ and introduce the vector $Z_h(t) = e^{\lambda t}V_h(t)$ where $\lambda$ is such that $a_i(t) - \lambda > 0$, $0 \leq i \leq I$, $t \in [0,T_0]$. Let $m = \min_{0\leq i\leq I, 0\leq t\leq T_0} Z_i(t)$. Since for $i \in \{0,...,I\}$, $Z_i(t)$ is a continuous function, there exists $t_0 \in [0,T_0]$ such that $m = Z_{i_0}(t_0)$ for a certain $i_0 \in \{0,...,I\}$. It is not hard to see that

$$\frac{dZ_{i_0}(t_0)}{dt} = \lim_{k\to 0} \frac{Z_{i_0}(t_0) - Z_{i_0}(t_0-k)}{k} \leq 0, \tag{11}$$

$$\delta^2 Z_{i_0}(t_0) = \frac{2Z_1(t_0) - 2Z_0(t_0)}{h^2} \geq 0 \quad \text{if} \quad i_0 = 0, \tag{12}$$

$$\delta^2 Z_{i_0}(t_0) = \frac{Z_{i_0+1}(t_0) - 2Z_{i_0}(t_0) + Z_{i_0-1}(t_0)}{h^2} \geq 0 \quad \text{if} \quad 1 \leq i_0 \leq I-1, \tag{13}$$

$$\delta^2 Z_{i_0}(t_0) = \frac{2Z_{I-1}(t_0) - 2Z_I(t_0)}{h^2} \geq 0 \quad \text{if} \quad i_0 = I. \tag{14}$$

Using (9), a straightforward computation reveals that

$$\frac{dZ_{i_0}(t_0)}{dt} - \delta^2 Z_{i_0}(t_0) + (a_{i_0}(t_0) - \lambda)Z_{i_0}(t_0) \geq 0. \tag{15}$$

According to (11)–(15), we arrive at $(a_{i_0}(t) - \lambda)Z_{i_0}(t_0) \geq 0$, which implies that $m = Z_{i_0}(t_0) \geq 0$. Therefore, $V_h(t) \geq 0$ for $t \in [0, T_0]$ and we have the desired result. □

Another version of the maximum principle for semidiscrete equations is the following comparison lemma.

**Lemma 2.2.** *Let $V_h(t)$, $U_h(t) \in C^1([0,\infty), \mathbb{R}^{I+1})$ and $f \in C^0(\mathbb{R}\times\mathbb{R}, \mathbb{R})$ such that for $t \in (0,\infty)$*

$$\frac{dV_i(t)}{dt} - \delta^2 V_i(t) + f(V_i(t), t) < \frac{dU_i(t)}{dt} - \delta^2 U_i(t) + f(U_i(t), t), \quad 0 \leq i \leq I, \tag{16}$$

$$V_i(0) < U_i(0), \quad 0 \leq i \leq I. \tag{17}$$

*Then we have $V_i(t) < U_i(t)$, $0 \leq i \leq I$, $t \in (0,\infty)$.*

*Proof.* Define the vector $Z_h(t) = U_h(t) - V_h(t)$. Let $t_0$ be the first $t > 0$ such that $Z_h(t) > 0$ for $t \in [0, t_0)$ but $Z_{i_0}(t_0) = 0$ for a certain $i_0 \in \{0, ..., I\}$. We observe that

$$\frac{dZ_{i_0}(t_0)}{dt} = \lim_{k\to 0} \frac{Z_{i_0}(t_0) - Z_{i_0}(t_0 - k)}{k} \leq 0,$$

$$\delta^2 Z_{i_0}(t_0) = \frac{Z_{i_0+1}(t_0) - 2Z_{i_0}(t_0) + Z_{i_0-1}(t_0)}{h^2} \geq 0 \quad \text{if} \quad 1 \leq i_0 \leq I-1,$$

$$\delta^2 Z_{i_0}(t_0) = \frac{2Z_1(t_0) - 2Z_0(t_0)}{h^2} \geq 0 \quad \text{if} \quad i_0 = 0,$$

$$\delta^2 Z_{i_0}(t_0) = \frac{2Z_{I-1}(t_0) - 2Z_I(t_0)}{h^2} \geq 0 \quad \text{if} \quad i_0 = I,$$

which implies that $\frac{dZ_{i_0}(t_0)}{dt} - \delta^2 Z_{i_0}(t_0) + f(U_{i_0}(t_0), t_0) - f(V_{i_0}(t_0), t_0) \leq 0$. But this inequality contradicts (16) and the proof is complete.

□

## 3. Blow-up solutions

In this section, under some assumptions, we show that the solution $U_h$ of (6)–(8) blows up in a finite time and estimate its semidiscrete blow-up time. In addition, we prove that the semidiscrete blow-up time converges to the real one when the mesh size goes to zero.
We need the following result.

**Lemma 3.1.** *Let $U_h \in \mathbb{R}^{I+1}$ such that $U_h \geq 0$. Then we have*

$$\delta^2 U_i^q \geq q U_i^{q-1} \delta^2 U_i, \quad 0 \leq i \leq I.$$

*Proof.* Apply Taylor's expansion to obtain

$$\delta^2 U_0^q = q U_0^{q-1} \delta^2 U_0 + (U_1 - U_0)^2 \frac{q(q+1)}{h^2} \theta_0^{q-2},$$

$$\delta^2 U_i^q = q U_i^{q-1} \delta^2 U_i + (U_{i+1} - U_i)^2 \frac{q(q+1)}{2h^2} \theta_i^{q-2} + (U_{i-1} - U_i)^2 \frac{q(q+1)}{2h^2} \eta_i^{q-2}$$
$$if \quad 1 \leq i \leq I-1,$$

$$\delta^2 U_I^q = qU_I^{q-1}\delta^2 U_I + (U_{I-1} - U_I)^2 \frac{q(q+1)}{h^2}\eta_I^{q-2},$$

where $\theta_i$ is an intermediate value between $U_i$ and $U_{i+1}$ and $\eta_i$ the one between $U_{i-1}$ and $U_i$. Use the fact that $U_h \geq 0$ to complete the proof.

□

Now let us state a result on blow-up.

**Theorem 3.1.** *Let $U_h$ be the solution of (6)–(8). Suppose that there exists a positive constant $A$ such that*

$$\delta^2 \varphi_i + a\varphi_i^p \geq A\varphi_i^q, \quad 0 \leq i \leq I. \tag{18}$$

*Then the solution $U_h$ of (6)–(8) blows up in a finite time $T_b^h$ with the following estimation*

$$T_b^h \leq \frac{1}{A}\frac{\|\varphi_h\|_\infty^{1-q}}{(q-1)}. \tag{19}$$

*Proof.* Let $(0, T_b^h)$ be the maximal time interval on which $\|U_h(t)\|_\infty < +\infty$. Our aim is to show that $T_b^h$ is finite and satisfies the above inequality. Introduce the vector $J_h(t)$ defined as follows

$$J_i = \frac{d}{dt}U_i - AU_i^q, \quad 0 \leq i \leq I. \tag{20}$$

A direct calculation yields

$$\frac{d}{dt}J_i - \delta^2 J_i = \frac{d}{dt}(\frac{d}{dt}U_i - \delta^2 U_i) - AqU_i^{q-1}\frac{d}{dt}U_i + A\delta^2 U_i^q.$$

From Lemma 3.1 $\delta^2 U_i^q \geq qU_i^{q-1}\delta^2 U_i$ which implies that

$$\frac{d}{dt}J_i - \delta^2 J_i \geq \frac{d}{dt}(\frac{d}{dt}U_i - \delta^2 U_i) - AqU_i^{q-1}(\frac{d}{dt}U_i - \delta^2 U_i),\ 0 \leq i \leq I.$$

It follows from (6)–(7) that

$$\frac{d}{dt}J_i - \delta^2 J_i \geq apU_i^{p-1}J_i, \quad 0 \leq i \leq I-1,$$

$$\frac{d}{dt}J_I - \delta^2 J_I \geq (-2qb\frac{U_I^{q-1}}{h} + apU_I^{p-1})J_I.$$

The relation (18), implies that $J_h(0) \geq 0$. It follows from Lemma 2.1 that $J_h(t)$ is nonnegative, which implies $\frac{d}{dt}U_i \geq AU_i^q$, $0 \leq i \leq I$. We observe that

$$\frac{dU_i}{U_i^q} \geq Adt, \quad 0 \leq i \leq I. \tag{21}$$

Integrating these inequalities over $(t, T_b^h)$, we arrive at

$$T_b^h - t \leq \frac{1}{A}\frac{(U_i(t))^{1-q}}{(q-1)}, \quad 0 \leq i \leq I. \tag{22}$$

Let $i_0$ such that $\|U_h(t)\|_\infty = U_{i_0}(t)$. If we replace $i$ by $i_0$ and the time $t$ by 0 in the above inequalities, we get the following estimation $T_b^h \leq \frac{1}{A}\frac{\|U_h(0)\|_\infty^{1-q}}{(q-1)}$. This implies that the solution $U_h(t)$ blows up in a finite time because the quantity on the right hand side of the above inequality is finite. Use the fact that $\|U_h(0)\|_\infty = \|\varphi_h\|_\infty$ to complete the rest of the proof. □

**Remark 3.1.** *The inequalities (22) imply that*

$$T_b^h - t_0 \leq \frac{1}{A}\frac{\|U_h(t_0)\|_\infty^{1-q}}{(q-1)} \quad \text{if} \quad 0 < t_0 < T_b^h.$$

**Remark 3.2.** *Let us notice that the condition (18) is the discrete version of the one given in (4) for the continuous solution.*

In the following theorem, we show that for each fixed time interval $[0, T]$ where u is defined, the solution $U_h(t)$ of (6)–(8) approximates u when the mesh parameter h goes to zero.

**Theorem 3.2.** *Assume that (1)-(3) has a solution $u \in C^{4,1}([0,1] \times [0,T])$ and the initial condition at (8) satisfies*

$$\|\varphi_h - u_h(0)\|_\infty = o(1) \quad \text{as} \quad h \to 0, \tag{23}$$

*where $u_h(t) = (u(x_0,t), ..., u(x_I,t))^T$. Then, for h sufficiently small, the problem (6)–(8) has a unique solution $U_h \in C^1([0,T], \mathbb{R}^{I+1})$ such that*

$$\max_{0\leq t\leq T} \|U_h(t) - u_h(t)\|_\infty = O(\|\varphi_h - u_h(0)\|_\infty + h^2) \quad \text{as} \quad h \to 0. \tag{24}$$

*Proof.* The problem (6)–(8) has for each $h$, a unique solution $U_h \in C^1([0, T_q^h), \mathbb{R}^{I+1})$. Let $t(h)$ the greatest value of $t > 0$ such that

$$\|U_h(t) - u_h(t)\|_\infty < 1 \quad \text{for} \quad t \in (0, t(h)). \tag{25}$$

The relation (23) implies that $t(h) > 0$ for h sufficiently small. Let $t^*(h) = \min\{t(h), T\}$. By the triangle inequality, we obtain

$$\|U_h(t)\|_\infty \leq \|u(\cdot,t)\|_\infty + \|U_h(t) - u_h(t)\|_\infty \quad \text{for} \quad t \in (0, t^*(h)),$$

which implies that $U_h(t)$ is bounded on the interval $(0, t^*(h))$. Let $e_h(t) = U_h(t) - u_h(x,t)$ be the error of discretization. Using Taylor's expansion, we have for $t \in (0, t^*(h))$,

$$\frac{d}{dt}e_i(t) - \delta^2 e_i(t) = \frac{h^2}{12}u_{xxxx}(\widetilde{x}_i, t) + ap\xi_i^{p-1}e_i(t),$$

$$\frac{d}{dt}e_I(t) - \delta^2 e_I(t) = \frac{2}{h}q\theta_I^{q-1}e_I + \frac{2h^2}{3}u_{xxx}(\widetilde{x}_I, t) + \frac{h^2}{12}u_{xxxx}(\widetilde{x}_I, t) - ap\xi_I^{p-1}e_I(t),$$

where $\theta_I$ is an intermediate value between $U_I(t)$ and $u(x_I, t)$ and $\xi_i$ the one between $U_i(t)$ and $u(x_i, t)$. Since $U_i(t)$ is bounded and $u \in C^{4,1}$, there exist two positive constants $K$ and $L$ such that

$$\frac{d}{dt}e_i(t) - \delta^2 e_i(t) \leq L|e_i(t)| + Kh^2, \quad 0 \leq i \leq I-1, \tag{26}$$

$$\frac{de_I(t)}{dt} - \delta^2 e_I(t) \leq \frac{L|e_I(t)|}{h} + L|e_I(t)| + Kh^2. \tag{27}$$

Consider the function $z(x,t) = e^{((M+1)t+Cx^2)}(\|\varphi_h - u_h(0)\|_\infty + Qh^2)$ where $M$, $C$, $Q$ are constants which will be determined later. A direct calculation yields

$$z_t(x,t) - z_{xx}(x,t) = (M + 1 - 2C - 4C^2x^2)z(x,t),$$

$$z_x(0,t) = 0, \quad z_x(1,t) = 2Cz(1,t),$$

$$z(x,0) = e^{Cx^2}(\|\varphi_h - u_h(0)\|_\infty + Qh^2).$$

By a semidiscretization of the above problem, we may choose $M$, $C$, $Q$ large enough that

$$\frac{d}{dt}z(x_i,t) - \delta^2 z(x_i,t) > L|z(x_i,t)| + Kh^2, \quad 0 \le i \le I-1, \tag{28}$$

$$\frac{d}{dt}z(x_I,t) - \delta^2 z(x_I,t) > \frac{L}{h}|z(x_I,t)| + L|z(x_I,t)| + Kh^2, \tag{29}$$

$$z(x_i,0) > e_i(0), \quad 0 \le i \le I. \tag{30}$$

It follows from Lemma 2.2 that $z(x_i,t) > e_i(t)$ for $t \in (0,t^*(h))$, $0 \le i \le I$. By the same way, we also prove that $z(x_i,t) > -e_i(t)$ for $t \in (0,t^*(h))$, $0 \le i \le I$, which implies that

$$\|U_h(t) - u_h(t)\|_\infty \le e^{(Mt+C)}(\|\varphi_h - u_h(0)\|_\infty + Qh^2), \quad t \in (0,t^*(h)).$$

Let us show that $t^*(h) = T$. Suppose that $T > t(h)$. From (25), we obtain

$$1 = \|U_h(t(h)) - u_h(t(h))\|_\infty \le e^{(MT+C)}(\|\varphi_h - u_h(0)\|_\infty + Qh^2). \tag{31}$$

Since the term in the right hand side of the above inequality goes to zero as $h$ goes to zero, we deduce that $1 \le 0$, which is impossible. Consequently $t^*(h) = T$, and we obtain the desired result. □

**Remark 3.3.** *Let us notice that if for the semidiscrete scheme in (6)–(8) we take as initial data $\varphi_i = u_0(x_i)$, $0 \le i \le I$, then we easily see that*

$$u_h(0) = (u(x_0,0),...,u(x_I,0))^T = (u_0(x_0),...,u_0(x_I))^T = \varphi_h.$$

*In this case $\|\varphi_h - u_h(0)\|_\infty = 0$ and the condition (23) is valid. We also observe that if we take $\varphi_i = u_0(x_i) + ih^2$, $0 \le i \le I$ then the condition (23) remains valid. The advantage to choose this kind of initial data is that if for instance the initial data $u_0$ of the continuous problem is nondecreasing, taking $\varphi_i = u_0(x_i) + ih^2$, $0 \le i \le I$, we remark that $\varphi_{i+1} > \varphi_i$, $0 \le i \le I-1$. This is sometimes very important when we want to treat certain problems.*

Now, we are in a position to prove the main result of this section

**Theorem 3.3.** *Suppose that the problem (1)–(3) has a solution $u$ which blows up in a finite time $T_b$ such that $u \in C^{4,1}([0,1] \times [0,T_b))$ and the initial condition at (8) satisfies*

$$\|\varphi_h - u_h(0)\|_\infty = o(1) \quad \text{as} \quad h \to 0.$$

*Assume that there exists a constant $A > 0$ such that*

$$\delta^2 \varphi_i + a\varphi_i^p \ge A\varphi_i^q, \quad 0 \le i \le I.$$

*Then the problem (6)–(8) has a solution $U_h$ which blows up in a finite time $T_b^h$ and*

$$\lim_{h \to 0} T_b^h = T_b.$$

*Proof.* Letting $\varepsilon > 0$, there exists a positive constant N such that

$$\frac{1}{A}\frac{x^{1-q}}{(q-1)} \le \frac{\varepsilon}{2} < \infty \quad \text{for} \quad x \in (N, +\infty). \tag{32}$$

Since $u$ blows up at the time $T_b$, there exists $T_1$ such that $|T_1 - T_b| \le \frac{\varepsilon}{2}$ and $\|u(\cdot,t)\|_\infty \ge 2N$ for $t \in [T_1, T_b]$. Let $T_2 = \frac{T_1+T_b}{2}$, then $\sup_{t\in[0,T_2]} |u(\cdot,t)| < \infty$. It follows from Theorem 3.2 that the problem (6)–(8) has a solution $U_h(t)$

and $\sup_{t\in[0,T_2]}|U_h(t)-u_h(t)|_\infty \leq N$. Applying the triangle inequality, we get $\|U_h(t)\|_\infty \geq \|u_h(t)\|_\infty - \|U_h(t)-u_h(t)\|_\infty$, which leads to $\|U_h(t)\|_\infty \geq N$ for $t\in[0,T_2]$. From Theorem 3.1, $U_h(t)$ blows up at the time $T_b^h$. We deduce from Remark 3.1 and (32) that

$$|T_b^h - T_b| \leq |T_b^h - T_2| + |T_2 - T_b| \leq \frac{\varepsilon}{2} + \frac{1}{A}\frac{\|U_h(T_2)\|_\infty^{1-q}}{(q-1)} \leq \varepsilon,$$

and the proof is complete. □

## 4. Asymptotic behavior

In this section, we show that for small initial data, the solution $U_h$ of (6)–(8) goes to zero as $t\to+\infty$ and give its asymptotic behavior.

**Theorem 4.1.** *Let $U_h(t)$ be the solution of (6)–(8). There exists a constant $C>0$ such that if the initial condition defined in (8) satisfies $\|\varphi_h\|_\infty \leq C$ then $U_h(t)$ goes to zero as $t\to+\infty$. Moreover, the following relation holds*

$$\lim_{t\to\infty} t^{\frac{1}{q-1}}\|U_h(t)\|_\infty = C_0,$$

*where $C_0 = (\frac{1}{b(q-1)})^{\frac{1}{q-1}}$.*

The proof of the above theorem is based on the lemmas below. Introduce the function

$$\mu(x) = -\lambda(C_0+\varepsilon) + b(C_0+\varepsilon)^q,$$

where $\lambda = \frac{1}{q-1}$. This function is crucial for the proof of the above theorem.
Let us state our first lemma which gives us an upper bound of the semidiscrete solution.

**Lemma 4.1.** *Let $U_h$ be the solution of (6)-(8). There exists a positive constant $C$ such that if the initial condition defined in (8) satisfies $\|\varphi_h\|_\infty \leq C$, then $U_h$ goes to zero when $t$ tends to infinity. In addition for any $\varepsilon>0$, there exist two positive times $T$ and $\tau$ such that*

$$U_i(t+\tau) \leq (C_0+\varepsilon)(t+T)^{-\lambda} + \varphi_i(t+T)^{-\lambda-1}, \quad 0\leq i\leq I,$$

*where $\varphi_i = -\frac{b}{2}(C_0+\varepsilon)^q i^2 h^2$.*

*Proof.* Since $\mu(0)=0$ and $\mu'(0)=1$, let $\eta>0$ such that $\mu(\eta)>0$. Define the vector $W_h$ such that

$$W_i(t) = (C_0+\eta)t^{-\lambda} + \varphi_i t^{-\lambda-1}, \quad 0\leq i\leq I.$$

Our idea is to show that the vector $W_h$ is an upper solution of (6)-(8). A direct calculation reveals that

$$\begin{aligned}\frac{dW_i}{dt} - \delta^2 W_i + aW_i^p &= -\lambda(C_0+\eta)t^{-\lambda-1} - (\lambda+1)t^{-\lambda-2}\varphi_i \\ &+ at^{-\lambda p}((C_0+\eta)+t^{-\lambda-1})^p - t^{-\lambda-1}\delta^2\varphi_i,\ 0\leq i\leq I-1,\end{aligned}$$

$$\begin{aligned}\frac{dW_I}{dt}-\delta^2 W_I+aW_I^P-\frac{2b}{h}W_I^q &= -\lambda(C_0+\eta)t^{-\lambda-1}-(\lambda+1)t^{-\lambda-2}\varphi_I\\ &+ at^{-\lambda p}((C_0+\eta)+\varphi_I t^{-1})^p+\\ &+ t^{-\lambda-1}\delta^2\varphi_I\\ &- \frac{2b}{h}t^{-\lambda-1}(C_0+\eta+\varphi_I t^{-1})^q,\end{aligned}$$

because $\lambda q=\lambda+1$. By the mean value theorem, we get
$(C_0+\eta+\varphi_I t^{-1})^q=(C_0+\eta)^q+\chi_I t^{-1}$ where $\chi_I(t)$ is a bounded function. We deduce that

$$\begin{aligned}\frac{dW_i}{dt}-\delta^2 W_i+aW_i^p &= t^{-\lambda-1}(\mu(\eta)-(\lambda+1)t^{-1}\varphi_i\\ &+ at^{-\lambda p+\lambda+1}(C_0+\eta+t^{-1}\varphi_i)^p),\end{aligned}$$

$$\begin{aligned}\frac{dW_I}{dt}-\delta^2 W_I+aW_I^p-\frac{2b}{h}W_I^q &= t^{-\lambda-1}(-\lambda\mu(\eta)-(\lambda+1)t^{-1}\varphi_I\\ &+ at^{-\lambda p+\lambda+1}(C_0+\eta+t^{-1}\varphi_I)^p+\frac{2b}{h}\chi_I t^{-1}),\end{aligned}$$

we observe that $-\lambda p+\lambda+1=\frac{q-p}{q-1}<0$. Since $\mu(\eta)>0$, there exists a time $T>0$ such that

$$\frac{dW_i}{dt}-\delta^2 W_i+aW_i^p>0,\quad 0\le i\le I-1,\quad t\ge T,$$

$$\frac{dW_I}{dt}-\delta^2 W_I+aW_I^p-\frac{2b}{h}W_I^q>0,\quad t\ge T,$$

$$W_i(T)>\frac{T^{-\lambda}C_0}{2}.$$

Suppose that $U_i(0)<\frac{T^{-1}C_0}{2}<W_i(T)$. Let us introduce the vector $Z_h(t)$ such that $Z_h(t)=U_h(t-T)$. It is not hard to see that

$$\frac{dZ_i}{dt}-\delta^2 Z_i+aZ_i^p=0,\quad 0\le i\le I-1,\quad t\ge T,$$

$$\frac{dZ_I}{dt}-\delta^2 Z_I+aZ_I^p-\frac{2b}{h}Z_I^q=0,\quad t\ge T,$$

$$Z_i(T)=U_i(0)<W_i(T),\quad 0\le i\le I.$$

We deduce from Comparison Lemma 2.2 that $U_h(t-T))\le W_h(t)$ for $t\ge T$. Since $W_h(t)$ decays to zero when $t$ tends to infinity, we deduce that $U_h(t)$ goes to zero when $t$ approaches infinity. Now introduce the vector $V_h(t)$ defined as follows

$$V_i(t)=(C_0+\varepsilon)t^{-\lambda}+\varphi_i t^{-\lambda-1},\quad 0\le i\le I.$$

By an analogous argument as in the proof of the first part of the lemma, we obtain

$$\begin{aligned}\frac{dV_i}{dt}-\delta^2 V_i+aV_i^p &= t^{-\lambda-1}(\mu(\varepsilon)-(\lambda+1)t^{-1}\varphi_i\\ &+ at^{-\lambda p+\lambda+1}(C_0+\varepsilon+t^{-1}\varphi_i)^p),\ 0\le i\le I-1,\end{aligned}$$

$$\begin{aligned}\frac{dV_I}{dt} - \delta^2 V_I + aV_I^p - \frac{2b}{h}V_I^q &= t^{-\lambda-1}(-\lambda\mu(\varepsilon) - (\lambda+1)\varphi_I \\ &+ at^{-\lambda p+\lambda+1}(C_0+\varepsilon+t^{-1}\varphi_i)^p + \frac{2b}{h}\chi_i t^{-1}).\end{aligned}$$

Since $\mu(\varepsilon) > 0$ and $-p\lambda + \lambda + 1 < 0$, there exists a positive time $T$ such that

$$\frac{dV_i}{dt} - \delta^2 V_i + aV_i^p > 0, \quad 0 \le i \le I-1, \quad t \ge T,$$

$$\frac{dV_I}{dt} - \delta^2 V_I + aV_I^p - \frac{2b}{h}V_I^q > 0, \quad t \ge T,$$

$$V_i(T) > \frac{T^{-\lambda}C_0}{2}.$$

Since $U_h(t)$ goes to zero as $t$ approaches infinity, there exists a time $\tau > T$ such that $U_i(\tau) < \frac{T^{-1}C_0}{2} < V_i(T)$. Let the vector $Z_h(t)$ such that $Z_h(t) = U_h(t+\tau-T)$. A routine computation reveals that

$$\frac{dZ_i}{dt} - \delta^2 Z_i + aZ_i^p = 0, \quad 0 \le i \le I-1, \quad t \ge T,$$

$$\frac{dZ_I}{dt} - \delta^2 Z_I + aZ_I^p - \frac{2b}{h}Z_I^q = 0, \quad t \ge T,$$

$$Z_i(T) = V_i(\tau) < U_i(T).$$

It follows from Comparison Lemma 2.2 that $U_h(t-T) \ge V_h(t)$, $t \ge T$, which leads us to the result. □

The following lemma establishes a lower bound of the solution $U_h(t)$ of (6)–(8)

**Lemma 4.2.** *For any $\varepsilon > 0$ there exists a positive time $\tau$ such that*

$$U_i(t+1) \ge (C_0-\varepsilon)(t+\tau)^{-\lambda} + \psi_i(t+\tau)^{-\lambda-1}, \quad 0 \le i \le I,$$

*where $\psi_i = \frac{-b(C_0-\varepsilon)^q}{2}i^2h^2$.*

*Proof.* Define the vector $W_h$ such that

$$W_i(t) = (C_0-\varepsilon)t^{-\lambda} + \psi_i t^{-\lambda-1}, \quad 0 \le i \le I.$$

As in the proof of Lemma 4.1, we find that

$$\begin{aligned}\frac{dW_i}{dt} - \delta^2 W_i + aW_i^p &= t^{-\lambda-1}(\mu(-\varepsilon) - (\lambda+1)t^{-1}\psi_i \\ &+ at^{-\lambda p+\lambda+1}(C_0-\varepsilon+t^{-1}\psi_i)^p),\ 0 \le i \le I-1,\end{aligned}$$

$$\begin{aligned}\frac{dW_I}{dt} - \delta^2 W_I + aW_I^p - \frac{2b}{h}W_I^q &= t^{-\lambda-1}(\mu(-\varepsilon) - (\lambda+1)\varphi_I t^{-1} \\ &+ at^{-\lambda p+\lambda+1}(C_0-\varepsilon+t^{-1}\psi_I)^p + \frac{2b}{h}\chi_I t^{-1}),\end{aligned}$$

where $\chi_I(t)$ is a bounded function. Since $\mu(0) = 0$ and $\mu^{'}(0) = 1$, we observe that $\mu(-\varepsilon) < 0$. Using the fact that $-p\lambda + \lambda + 1 < 0$, we deduce that there exists a positive time $\tau$ such that

$$\frac{dW_i}{dt} - \delta^2 W_i + aW_i^p < 0, \quad 0 \le i \le I-1, \quad t \ge \tau,$$

$$\frac{dW_I}{dt} - \delta^2 W_I + aW_I^p - \frac{2b}{h}W_I^q < 0, \quad t \geq \tau,$$

Since $W_h(t)$ goes to zero when $t$ approaches infinity, there exists a time $T \geq \tau$ such that $W_h(T) < U_h(1)$. Introduce the vector $Z_h(t)$ such that $Z_h(t) = U_h(t - \tau + 1)$. A straightforward computation gives

$$\frac{dZ_i}{dt} - \delta^2 Z_i + aZ_i^p = 0, \quad 0 \leq i \leq I-1, \quad t \geq \tau,$$

$$\frac{dZ_I}{dt} - \delta^2 Z_I + aZ_I^p - \frac{2b}{h}Z_I^q = 0, \quad t \geq \tau,$$

$$Z_i(\tau) = U_i(1) > W_h(T).$$

It follows from Comparison Lemma 2.2 that $U_h(t - \tau + 1)) \geq W_h(t)$, $t \geq \tau$, which leads us to the result. □

With the above lemmas, we are ready to prove the main result of this section.

**Proof of Theorem 4.1.** From Lemmas 4.1 and 4.2, we deduce that

$$(C_0 - \varepsilon) \leq \lim_{t\to\infty} \inf(\frac{U_i(t)}{t^\lambda}) \leq \lim_{t\to\infty} \sup(\frac{U_i(t)}{t^\lambda}) \leq (C_0 + \varepsilon),$$

for any $\varepsilon > 0$ and we have the desired result. □

## 5. Numerical results

In this section, we give some numerical results. Firstly, we approximate the solution $u(x,t)$ of (1)–(3) by the solution $U_h^{(n)} = (U_0^{(n)}, U_1^{(n)}, \ldots, U_I^{(n)})^T$ of the following explicit scheme

$$\frac{U_i^{(n+1)} - U_i^{(n)}}{\Delta t_n} = \delta^2 U_i^{(n)} + a(U_i^{(n)})^p, \quad 0 \leq i \leq I-1, \tag{33}$$

$$\frac{U_I^{(n+1)} - U_I^{(n)}}{\Delta t_n} = \frac{2U_{I-1}^{(n)} - 2U_I^{(n)}}{h^2} - \frac{2b}{h}(U_I^{(n)})^{q-1}U_I^{(n+1)} + a(U_I^{(n)})^p, \tag{34}$$

$$U_i^{(0)} = \phi_i > 0, \quad 0 \leq i \leq I, \tag{35}$$

where $n \geq 0$, $\Delta t_n = \min\{\frac{h^2}{2}, \frac{h^2}{\|U_h^{(n)}\|_\infty^{p-1}}\}$. Let us notice that the restriction on the time step $\Delta t_n \leq \frac{h^2}{2}$ guarantees the positivity of the discrete solution.

Secondly, we approximate the solution $u(x,t)$ of (1)–(3) by the solution $U_h^{(n)} = (U_0^{(n)}, U_1^{(n)}, \ldots, U_I^{(n)})^T$ of the following implicit scheme

$$\delta_t U_i^{(n)} = \delta^2 U_i^{(n+1)} + a(U_i^{(n)})^p, \quad 0 \leq i \leq I-1, \tag{36}$$

$$\delta_t U_I^{(n)} = \delta^2 U_I^{(n+1)} - \frac{2b}{h}(U_I^{(n)})^{q-1}U_I^{(n+1)} + a(U_I^{(n)})^p, \tag{37}$$

$$U_i^{(0)} = \phi_i > 0, \quad 0 \leq i \leq I, \tag{38}$$

where $n \geq 0$, $\Delta t_n^i = \frac{h^2}{\|U_h^{(n)}\|_\infty^{p-1}}$.

The above equations may be rewritten in the following form

$$A^{(n)}U_h^{(n+1)} = a(U_h^{(n)})^p$$

where $A^{(n)}$ is a tridiagonal matrix defined as follows

$$A^{(n)} = \begin{pmatrix} d_0 & \frac{-2\Delta t_n}{h^2} & 0 & 0 & \cdots & 0 & 0 \\ \frac{-\Delta t_n}{h^2} & d_1 & \frac{-\Delta t_n}{h^2} & 0 & \cdots & 0 & 0 \\ 0 & \frac{-\Delta t_n}{h^2} & d_2 & \frac{-\Delta t_n}{h^2} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \frac{-\Delta t}{h^2} & d_{I-2} & \frac{-\Delta t_n}{h^2} & 0 \\ 0 & 0 & 0 & \cdots & \frac{-\Delta t_n}{h^2} & d_{I-1} & \frac{-\Delta t_n}{h^2} \\ 0 & 0 & 0 & \cdots & 0 & \frac{-2\Delta t_n}{h^2} & d_I \end{pmatrix},$$

with

$$d_i = 1 + 2\frac{\Delta t_n}{h^2}, \quad 0 \leq i \leq I-1,$$

$$d_I = 1 + 2\frac{\Delta t_n}{h^2} + \frac{2b}{h}|U_I^{(n)}|^{q-1}\Delta t_n.$$

We remark that the tridiagonal matrix $A^{(n)}$ satisfies the following properties

$$A_{ii}^{(n)} > 0, \quad A_{ij}^{(n)} < 0, \quad i \neq j,$$

$$|A_{ii}^{(n)}| > \sum_{i \neq j} |A_{ij}^{(n)}|.$$

These properties imply that $U_h^{(n)}$ exists for all $n$ and $U_h^{(n)} \geq 0$ (See for instance [6]).
We suppose that $p = 3$, $q = 2$, $a = 1$, $b = 1$. In the following tables, in rows, we present the numerical blow-up times or numerical times, the numbers of iterations, CPU times and the orders of the approximations corresponding to meshes of 16, 32, 64, 128. The order(s) of the method is computed from

$$s = \frac{\log((T_{4h} - T_{2h})/(T_{2h} - T_h))}{\log(2)}.$$

5.1. **Blow-up solutions.** Here we take $U_i^{(0)} = 2 * (hi)^4$. The numerical blow-up time $t_n = \sum_{j=0}^{n-1} \Delta t_j$ is computed at the first time when $\Delta t_n = |t_n - t_{n-1}| \leq 10^{-16}$.

**Table 1:** Numerical blow-up times, numbers of iterations, CPU times (seconds) and orders of the approximations obtained with the implicit Euler method.

| $I$ | $T^n$ | $n$ | $CPU_t$ | $s$ |
|---|---|---|---|---|
| 16 | 0.0012719 | 3150 | 0.6 | - |
| 32 | 0.0012669 | 11879 | 3 | - |
| 64 | 0.0012657 | 44690 | 31.6 | 2.06 |
| 128 | 0.0012654 | 167504 | 839.7 | 2.01 |

**Table 2:** Numerical blow-up times, numbers of iterations, CPU times (seconds) and orders of the approximations obtained with the explicit Euler method.

| $I$ | $T^n$ | $n$ | $CPU_t$ | $s$ |
|---|---|---|---|---|
| 16 | 0.00126726 | 3138 | 1.40 | - |
| 32 | 0.00126571 | 11868 | 6.9 | - |
| 64 | 0.00126545 | 44680 | 11.4 | 2.58 |
| 128 | 0.00126539 | 167490 | 256.2 | 2.12 |

5.2. **Solutions which go to zero.** Here we take $U_i^{(0)} = \frac{1}{2} * (hi)^{\frac{1}{4}}$. The numerical time $t_n = \sum_{j=0}^{n-1} \Delta t_j$ is computed at the first time when $\|t_n^{\frac{1}{q-1}} U_h^{(n)} - 1\|_\infty < 10^{-2}$.

**Table 3:** Numerical times, numbers of iterations, CPU times (seconds), and orders of the approximations obtained with the implicit Euler method.

| $I$ | $T^n$ | $n$ | $CPU_t$ | $s$ |
|---|---|---|---|---|
| 16 | 0.655822 | 335 | - | - |
| 32 | 0.654190 | 1339 | 0.5 | - |
| 64 | 0.654048 | 5358 | 3 | 3.53 |
| 128 | 0.653946 | 21431 | 55 | 0.47 |

**Table 4:** Numerical times, numbers of iterations, CPU times (seconds) and orders of the approximations obtained with the explicit Euler method.

| $I$ | $T^n$ | $n$ | $CPU_t$ | $s$ |
|---|---|---|---|---|
| 16 | 0.654296 | 334 | 0.12 | - |
| 32 | 0.653808 | 1338 | 1 | - |
| 64 | 0.653730 | 5356 | 11.4 | 2.65 |
| 128 | 0.653661 | 21429 | 179 | 0.17 |

## References


[1] L. Abia, J. C. López-Marcos and J. Martinez, *On the blow-up time convergence of semidiscretizations of reaction-diffusion equations*, Appl. Numer. Math., **26** (1998), 399-414.

[2] H. Amann, *Dynamics theory of quasilinear parabolic systems*, Math. Z., **202** (1989), 219-250.

[3] H. Amann, *Parabolic evolution equations and nonlinear boundary conditions*, J. Diff. Equat., **72** (1988), 201-269.

[4] T. K. Boni, *On the asymptotic behavior of solutions for some semilinear parabolic and elliptic equation of second order with nonlinear boundary conditions*, Nonl. Anal. TMA, **45** (2001), 895-908.

[5] T. K. Boni, *On blow-up and asymptotic behavior of solutions to a nonlinear parabolic equation of second order with nonlinear boundary conditions*, Comment. Math. Univ. Comeniae., **40** (1999), 457-475.

[6] T. K. Boni, *Extinction for discretizations of some semilinear parabolic equations*, C.R.A.S, Serie I, **333** (2001), 795-800.

[7] J. Escher, *Global existence and nonexistence for semilinear parabolic systems with nonlinear boundary conditions*, Math. Anal., **284** (1989), 289-305.

[8] A. Friedman and B. McLeod, *Blow-up of positive solutions of semilinear heat equations*, Indiana Univ. Math. J., **34**, (1985), 425-477.

[9] O. A. Ladyzenskaya, V. A. Solonnikov, and N. N. Ural'ceva, *Linear and quasilinear equations of parabolic type*, Trans. Math. Monogr., **23**, AMS, Providence, RI, (1988) (English translation from Russian 1967).

[10] R. E. Mickens, *Relation between the time and space step-sizes in nonstandard finite difference schemes for the fisher equation*, Num. Methods Part. Diff. Equat., **13** (1997), 51-55.

[11] T. Nakagawa, *Blowing up on the finite difference solutions to* $u_t = u_{xx} + u^2$, Appl. Math. Optim., **2** (1976), 337-350.

[12] M. H. Protter and H. F. Weinberger, *Maximum principles in differential equations*, Prentice Hall, Englewood Cliffs, NJ, (1967).
[13] A. Samarski, V. A Galaktionov, S. P. Kurdyunov and A. P. Milailov, *Blow-up in quasilinear parabolic equations*, Walter de Gruyter, Berlin, (1995).
[14] P. Quittner and P. Souplet, *Superlinear parabolic problems blow-up, Global existence and steady states series: Birkhuser Advanced texts*, Basler Lehbcher, (2007).
[15] W. Walter, *Differential-und Integral-Ungleichungen*, Springer, Berlin, (1964).

Université d'Abobo-Adjamé, UFR-SFA, Département de Mathématiques et Informatiques, 16 BP 372 Abidjan 16, (Cote d'Ivoire)
*E-mail address*: nabongo_diabate@yahoo.fr

Institut National Polytechnique Houphouet-Boigny de Yamoussoukro, BP 1093 Yamoussoukro, (Cote d'Ivoire)
*E-mail address*: theokboni@yahoo.fr.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 1, Pages 125–138
ISSN 1930-1235: (electronic version)

# EXTRAGRADIENT METHOD FOR EQUILIBRIUM PROBLEMS AND VARIATIONAL INEQUALITIES

MUHAMMAD ASLAM NOOR, YONGHONG YAO, AND YEONG-CHENG LIOU

Abstract. In this paper, we suggest and analyze a new extragradient method for finding a common element of the set of solutions of an equilibrium problem, the set of fixed points of a nonexpansive mapping and the set of solutions of some variational inequality. Furthermore, we prove that the proposed iterative algorithm converges strongly to a common element of the above three sets. Our result includes the main result of Bnouhachem, Noor and Hao [A. Bnouhachem, M.A. Noor and Z. Hao, Some new extragradient methods for variational inequalities, Nonlinear Analysis (2008), doi:10.1016/j.na.2008.02.014] as a special case.

## 1. Introduction

Equilibrium problems, which were introduced by Blum and Oettli [21] and Noor and Oettli [22] in 1994, are being used as mathematical model for studying a wide class of problems arising in various branches of pure and applied sciences. It has been shown that equilibrium problems include variational inequalities, fixed point problems and Nash equilibrium problems as special cases. In recent years, several iterative methods including extragradient method and auxiliary technique have been developed for solving equilibrium problems and variational inequalities, see [16-25] and the references therein. Bnouhachem, Noor and Hao [15] has suggested and analyzed an extragradient type method for solving variational inequalities. Motivated and inspired by the on going research in this direction, we suggest and analyze a new extragradient type method for finding the common element of the set of solutions of the equilibrium problems, variational inequalities and fixed point problems of nonexpansive mapping. The proposed iterative method is quite general and include the recent methods as special cases. Our results can be viewed as a significant improvement of the recently obtained results.

Let $C$ be a nonempty closed convex subset of a real Hilbert space $H$. Let $T : C \to H$ be a nonlinear mapping. The classical variational inequality, denoted by $VI(T, C)$, is to find $u^* \in C$ such that

$$\langle T(u^*), u - u^* \rangle \geq 0, \forall u \in C,$$

which was introduced by Stampacchia [1] in 1964. Since then, the variational inequality has been extensively studied in the literature. See, e.g., [2-11] and the

Received by the editors May 13, 2008 and, in revised form, June 10, 2008.
2000 *Mathematics Subject Classification.* Primary 49J30; Secondary 47H09, 47J20, 49M05.
*Key words and phrases.* Nonexpansive mapping; equilibrium problem; fixed point; variational inequality.
The third author is partially supposed by the grant NSC 96-2221-E-230-003.

references therein. Recall that a mapping $T$ of $C$ into $H$ is called $\alpha$-inverse-strongly monotone if there exists a positive real number $\alpha$ such that

$$\langle T(u) - T(v), u - v\rangle \geq \alpha\|T(u) - T(v)\|^2, \forall u, v \in C.$$

It is obvious that any $\alpha$-inverse-strongly monotone mapping $T$ is $\frac{1}{\alpha}$ Lipschitz continuous. A mapping $S : C \to H$ is said to be nonexpansive if

$$\|S(u) - S(v)\| \leq \|u - v\|, \quad \forall u, v \in C.$$

Denote the set of fixed points of $S$ by $Fix(S)$.

For finding an element of $Fix(S) \cap VI(T, C)$ under the assumption that a set $C \subset H$ is closed and convex, a mapping $S$ of $C$ into itself is nonexpasive and a mapping $T$ of $C$ into $H$ is $\alpha$-inverse-strongly monotone, Takahashi and Toyoda [12] introduced the following iterative scheme:

$$u^{k+1} = \alpha_k u^k + (1 - \alpha_k)S(P_C[u^k - \rho_k T(u^k)]), \forall k \geq 0, \tag{1}$$

where $P_C$ is the metric projection of $H$ onto $C$, $u^0 = u \in C$, $\{\alpha_k\}$ is a sequence in $(0, 1)$, and $\{\rho_k\}$ is a sequence in $(0, 2\alpha)$. They showed that, if $Fix(S) \cap VI(T, C)$ is nonempty, then the sequence $\{u^k\}$ generated by (1) converges weakly to some $z \in Fix(S) \cap VI(T, C)$. Recently, Nadezhkina and Takahashi [13] introduced a so-called extragradient method motivated by the idea of Korpelevich [14] for finding a common element of the set of fixed points of a nonexpansive mapping and the set of solutions of a variational inequality problem. Zeng and Yao [11] introduced another extragradient method for finding a common element of the set of fixed points of a nonexpansive mapping and the set of solutions of a variational inequality problem. Further, Bnouhachem, Noor and Hao [15] introduced the following extragradient iterative method:

$$\begin{cases} \tilde{u}^k = P_C[u^k - \rho_k T(u^k)], \\ u^{k+1} = \beta_k u^k + (1 - \beta_k)S(\alpha_k u + (1 - \alpha_k)P_C[u^k - \rho_k T(\tilde{u}^k)]). \end{cases} \tag{2}$$

Under mild assumptions, they proved a strong convergence theorem for finding a common element of the fixed points of a nonexpansive mapping $S$ and the solution set of the variational inequality for an $\alpha$-inverse strongly monotone mapping $T$ in a Hilbert space.

Let $F$ be an equilibrium bifunction of $C \times C$ into $\mathbf{R}$, where $\mathbf{R}$ is the set of real numbers. The equilibrium problem for $F : C \times C \to \mathbf{R}$ is to find $u \in C$ such that

$$EP: \quad F(u, v) \geq 0 \text{ for all } v \in C.$$

The set of solutions of the equilibrium problem is denoted by EP(F).

For solving the above equilibrium problem, some efforts have been made by many authors. For the more details, please refer to [15-18] and the references therein.

Motivated and inspired by the works in the literature, in this paper, we introduce an iterative algorithm based on extragradient method for finding a common element of the set of solutions of an equilibrium problem, the set of fixed points of a nonexpansive mapping and the set of solutions of some variational inequality. Furthermore, we prove that the proposed iterative algorithm converges strongly to a common element of the above three sets. Our result includes the main result of Bnouhachem, Noor and Hao [A. Bnouhachem, M.A. Noor and Z. Hao, Some

new extragradient methods for variational inequalities, Nonlinear Analysis (2008), doi:10.1016/j.na.2008.02.014] as a special case.

## 2. Preliminaries

Let $H$ be a real Hilbert space with inner product $\langle\cdot,\cdot\rangle$ and norm $\|\cdot\|$ and let $C$ be a closed convex subset of $H$. It is well known that, for any $u \in H$, there exists unique $y_0 \in C$ such that

$$\|u - y_0\| = \inf\{\|u - y\| : y \in C\}.$$

We denote $y_0$ by $P_C[u]$, where $P_C$ is called the metric projection of $H$ onto $C$. The metric projection $P_C$ of $H$ onto $C$ has the following basic properties:

(i) $\|P_C[u] - P_C[v]\| \le \|u - v\|$ for all $u, v \in H$,

(ii) $\langle u - v, P_C[u] - P_C[v]\rangle \ge \|P_C[u] - P_C[v]\|^2$ for every $u, v \in H$,

(iii) $\langle u - P_C[u], v - P_C[u]\rangle \le 0$ for all $u \in H, v \in C$,

(iv) $\|u - v\|^2 \ge \|u - P_C[u]\|^2 + \|v - P_C[u]\|^2$ for all $u \in H, v \in C$.

Let $T$ be a monotone mapping of $C$ into $H$. In the context of the variational inequality problem, it is easy to see from (iv) that

$$u \in VI(T, C) \Leftrightarrow u = P_C[u - \lambda T(u)], \quad \forall \lambda > 0.$$

A set-valued mapping $A : H \to 2^H$ is called monotone if, for all $u, v \in H$, $f \in Au$ and $g \in Av$ imply $\langle u - v, f - g\rangle \ge 0$. A monotone mapping $A : H \to 2^H$ is maximal if its graph $G(A)$ is not properly contained in the graph of any other monotone mapping. It is known that a monotone mapping $A$ is maximal if and only if, for $(u, f) \in H \times H$, $\langle u - v, f - g\rangle \ge 0$ for every $(v, g) \in G(A)$ implies $f \in Au$. Let $T$ be a monotone mapping of $C$ into $H$ and let $N_C v$ be the normal cone to $C$ at $v \in C$; i.e.,

$$N_C v = \{w \in H : \langle v - u, w\rangle \ge 0, \forall u \in C\}.$$

Define

$$Av = \begin{cases} T(v) + N_C v, & \text{if } v \in C, \\ \emptyset, & \text{if } v \notin C. \end{cases}$$

Then $A$ is maximal monotone and $0 \in Av$ if and only if $v \in VI(T, C)$.

In this paper, for solving the equilibrium problems for an equilibrium bifunction $F : C \times C \to \mathbf{R}$, we assume that $F$ satisfies the following conditions:

(C1) $F(u, u) = 0$ for all $u \in C$;

(C2) $F$ is monotone, i.e., $F(u, v) + F(v, u) \le 0$ for all $u, v \in C$;

(C3) for each $u, v, w \in C$, $\lim_{t \downarrow 0} F(tw + (1 - t)u, v) \le F(u, v)$;

(C4) for each $u \in C$, $v \mapsto F(u, v)$ is convex and lower semicontinuous.

If an equilibrium bifunction $F : C \times C \to \mathbf{R}$ satisfies conditions (C1)-(C4), then we have the following two important results. You can find them in [16].

**Lemma 2.1** Let $C$ be a nonempty closed convex subset of $H$ and let $F$ be an equilibrium bifunction of $C \times C$ into $\mathbf{R}$ satisfies conditions (C1)-(C4). Let $r > 0$ and $u \in C$. Then, there exists $v \in C$ such that

$$F(v, w) + \frac{1}{r}\langle w - v, v - u\rangle \ge 0 \text{ for all } w \in C.$$

**Lemma 2.2** Assume that $F$ satisfies the same assumptions as Lemma 2.1. For $r > 0$ and $u \in C$, define a mapping $\Gamma_r : H \to C$ as follows:

$$\Gamma_r(u) = \{v \in C : F(v, w) + \frac{1}{r}\langle w - v, v - u\rangle \geq 0, \forall w \in C\}.$$

Then the following hold:

(1) $\Gamma_r$ is single-valued;

(2) $\Gamma_r$ is firmly nonexpansive, i.e., for any $u, v \in H$,

$$\|\Gamma_r u - \Gamma_r v\|^2 \leq \langle \Gamma_r u - \Gamma_r v, u - v\rangle;$$

(3) $Fix(\Gamma_r) = EP(F)$;

(4) $EP(F)$ is closed and convex.

We also need the following lemmas for proving our main results.

**Lemma 2.3**([19]) Let $\{u^k\}$ and $\{v^k\}$ be bounded sequences in a Banach space $X$ and let $\{\beta_k\}$ be a sequence in $[0, 1]$ with $0 < \liminf_{k\to\infty} \beta_k \leq \limsup_{k\to\infty} \beta_k < 1$. Suppose $u^{k+1} = (1 - \beta_k)v^k + \beta_k u^k$ for all integers $k \geq 0$ and

$$\limsup_{k\to\infty}(\|v^{k+1} - v^k\| - \|u^{k+1} - u^k\|) \leq 0.$$

Then, $\lim_{k\to\infty} \|v^k - u^k\| = 0$.

**Lemma 2.4**([20]) Assume $\{a^k\}$ is a sequence of nonnegative real numbers such that $a^{k+1} \leq (1 - \gamma_k)a^k + \delta^k$, where $\{\gamma_k\}$ is a sequence in $(0, 1)$ and $\{\delta^k\}$ is a sequence such that

(1) $\sum_{k=1}^{\infty} \gamma_k = \infty$;

(2) $\limsup_{k\to\infty} \delta^k/\gamma_k \leq 0$ or $\sum_{k=1}^{\infty} |\delta^k| < \infty$.

Then $\lim_{k\to\infty} a^k = 0$.

## 3. Iterative algorithms

In this section, we suggest and analyze an iterative algorithm for finding a common element of the set of solutions of an equilibrium problem, the set of fixed points of a nonexpansive mapping and the set of solutions of some variational inequality. Let $C$ be a nonempty closed convex subset of a real Hilbert space $H$. Let $F$ be a bifunction from $C \times C \to \mathbf{R}$ satisfying (C1)-(C4). Let $T$ be an $\alpha$-inverse-strongly monotone mapping of $C$ into $H$ and let $S$ be a nonexpansive mapping of $C$ into itself such that $Fix(S) \cap VI(T, C) \cap EP(F) \neq \emptyset$.

**Algorithm 3.1** For fixed $u \in C$ and given $u^0 \in C$ arbitrarily, find the approximate solution $\{u^{k+1}\}$ by the iterative schemes:

$$(3) \quad \begin{cases} F(v^k, w) + \frac{1}{r_k}\langle w - v^k, v^k - u^k\rangle \geq 0, \forall w \in C, \\ \tilde{u}^k = P_C[v^k - \rho_k T(v^k)], \\ u^{k+1} = \beta_k u^k + (1 - \beta_k)S(\alpha_k u + (1 - \alpha_k)P_C[v^k - \rho_k T(\tilde{u}^k)]), \end{cases}$$

where $\{\alpha_k\}$ and $\{\beta_k\}$ are two sequences in $(0, 1)$, $\{\rho_k\}$ is a sequence in $[0, 2\alpha]$ and $\{r_k\}$ is a sequence in $(0, \infty)$.

If we put $F(u, v) \equiv 0$ for all $u, v \in C$ and $r_k = 1$ for all $k \geq 0$ in Algorithm 3.1, then we have $v^k = P_C[u^k] = u^k$. Then we obtain the following iterative algorithm

**Algorithm 3.2** For fixed $u \in C$ and given $u^0 \in C$ arbitrarily, find the approximate solution $\{u^{k+1}\}$ by the iterative schemes:

$$\begin{cases} \tilde{u}^k = P_C[u^k - \rho_k T(u^k)], \\ u^{k+1} = \beta_k u^k + (1-\beta_k) S(\alpha_k u + (1-\alpha_k) P_C[u^k - \rho_k T(\tilde{u}^k)]), \end{cases}$$

where $\{\alpha_k\}$ and $\{\beta_k\}$ are two sequences in $(0,1)$, $\{\rho_k\}$ is a sequence in $[0, 2\alpha]$ and $\{r_k\}$ is a sequence in $(0,\infty)$.

If we put $S \equiv I$ the identity operator in Algorithm 3.2. Then we obtain the following iterative algorithm

**Algorithm 3.3** For fixed $u \in C$ and given $u^0 \in C$ arbitrarily, find the approximate solution $\{u^{k+1}\}$ by the iterative schemes:

$$\begin{cases} \tilde{u}^k = P_C[u^k - \rho_k T(u^k)], \\ u^{k+1} = \beta_k u^k + (1-\beta_k)(\alpha_k u + (1-\alpha_k) P_C[u^k - \rho_k T(\tilde{u}^k)]), \end{cases}$$

where $\{\alpha_k\}$ and $\{\beta_k\}$ are two sequences in $(0,1)$, $\{\rho_k\}$ is a sequence in $[0, 2\alpha]$ and $\{r_k\}$ is a sequence in $(0,\infty)$.

Let $\{u^k\}$ be a sequence defined by (3). In the sequence, we will assume that the algorithm parameters satisfy the following restrictions:

(R1) $\lim_{k\to\infty} \alpha_k = 0$ and $\sum_{k=0}^{\infty} \alpha_k = \infty$;
(R2) $0 < \liminf_{k\to\infty} \beta_k \le \limsup_{k\to\infty} \beta_k < 1$;
(R3) $\lim_{k\to\infty} \rho_k = 0$;
(R4) $\liminf_{k\to\infty} r_k > 0$ and $\lim_{k\to\infty}(r_{k+1} - r_k) = 0$.

In order to prove the strong convergence of Algorithm 3.1, we first prove the following lemmas.

**Lemma 3.1** The sequence $\{u^k\}$ is bounded.

**Proof.** Let $u^* \in Fix(S) \cap VI(T,C) \cap EP(F)$. Then, it is clear that $u^* = P_C[u^* - \rho_k T(u^*)] = \Gamma_{r_k} u^*$. First, we note that $I - \rho_k T$ is nonexpansive for all $\rho_k \in [0, 2\alpha]$. Indeed, by the $\alpha$-inverse-strongly monotonicity of $T$, we have

$$\begin{aligned} \|(I-\rho_k T)u - (I-\rho_k T)v\|^2 &= \|u-v\|^2 - 2\rho_k\langle T(u) - T(v), u - v\rangle \\ &\quad + \rho_k^2 \|T(u) - T(v)\|^2 \\ &\le \|u-v\|^2 + \rho_k(\rho_k - 2\alpha)\|T(u) - T(v)\|^2 \\ &\le \|u-v\|^2, \end{aligned}$$

which implies that $I - \rho_k T$ is nonexpansive. Set $w^k = P_C[v^k - \rho_k T(\tilde{u}^k)]$ for all $k \ge 0$. From the property (iv) of $P_C$, we have

$$\begin{aligned} \|w^k - u^*\|^2 &\le \|v^k - \rho_k T(\tilde{u}^k) - u^*\|^2 - \|v^k - \rho_k T(\tilde{u}^k) - w^k\|^2 \\ &= \|v^k - u^*\|^2 - 2\rho_k\langle T(\tilde{u}^k), v^k - u^*\rangle + \rho_k^2\|T(\tilde{u}^k)\|^2 \\ &\quad - \|v^k - w^k\|^2 + 2\rho_k\langle T(\tilde{u}^k), v^k - w^k\rangle - \rho_k^2\|T(\tilde{u}^k)\|^2 \\ &= \|v^k - u^*\|^2 - \|v^k - w^k\|^2 + 2\rho_k\langle T(\tilde{u}^k), u^* - w^k\rangle \\ &= \|v^k - u^*\|^2 - \|v^k - w^k\|^2 + 2\rho_k\langle T(\tilde{u}^k) - T(u^*), u^* - \tilde{u}^k\rangle \\ &\quad + 2\rho_k\langle T(u^*), u^* - \tilde{u}^k\rangle + 2\rho_k\langle T(\tilde{u}^k), \tilde{u}^k - w^k\rangle. \end{aligned} \tag{4}$$

Using the fact that $T$ is monotonic and $u^*$ is a solution of the variational inequality problem $VI(T,C)$, we have $\langle T(\tilde{u}^k) - T(u^*), u^* - \tilde{u}^k\rangle \le 0$ and $\langle T(u^*), u^* - \tilde{u}^k\rangle \le 0$.

This together with (4) implies that

$$\begin{aligned}\|w^k-u^*\|^2 &\le \|v^k-u^*\|^2-\|v^k-w^k\|^2+2\rho_k\langle T(\tilde{u}^k),\tilde{u}^k-w^k\rangle\\ &=\|v^k-u^*\|^2-\|v^k-\tilde{u}^k\|^2-2\langle v^k-\tilde{u}^k,\tilde{u}^k-w^k\rangle\\ &\quad-\|\tilde{u}^k-w^k\|^2+2\rho_k\langle T(\tilde{u}^k),\tilde{u}^k-w^k\rangle\\ &=\|v^k-u^*\|^2-\|v^k-\tilde{u}^k\|^2+2\langle v^k-\rho_kT(\tilde{u}^k)-\tilde{u}^k,w^k-\tilde{u}^k\rangle\\ &\quad-\|\tilde{u}^k-w^k\|^2.\end{aligned}\tag{5}$$

By using the property (iii) of $P_C$, we have $\langle v^k-\rho_kT(v^k)-\tilde{u}^k,w^k-\tilde{u}^k\rangle\le 0$. Therefore, we get

$$\begin{aligned}\langle v^k-\rho_kT(\tilde{u}^k)-\tilde{u}^k,w^k-\tilde{u}^k\rangle &=\langle v^k-\rho_kT(v^k)-\tilde{u}^k,w^k-\tilde{u}^k\rangle\\ &\quad+\rho_k\langle T(v^k)-T(\tilde{u}^k),w^k-\tilde{u}^k\rangle\\ &\le \rho_k\langle T(v^k)-T(\tilde{u}^k),w^k-\tilde{u}^k\rangle\\ &\le \rho_k\|T(v^k)-T(\tilde{u}^k)\|\|w^k-\tilde{u}^k\|\\ &\le \frac{\rho_k}{\alpha}\|v^k-\tilde{u}^k\|\|w^k-\tilde{u}^k\|.\end{aligned}\tag{6}$$

Combining (5) and (6), we obtain

$$\begin{aligned}\|w^k-u^*\|^2 &\le \|v^k-u^*\|^2-\|v^k-\tilde{u}^k\|^2-\|\tilde{u}^k-w^k\|^2\\ &\quad+2\frac{\rho_k}{\alpha}\|v^k-\tilde{u}^k\|\|w^k-\tilde{u}^k\|\\ &\le \|v^k-u^*\|^2-\|v^k-\tilde{u}^k\|^2-\|\tilde{u}^k-w^k\|^2\\ &\quad+\frac{\rho_k^2}{\alpha^2}\|v^k-\tilde{u}^k\|^2+\|w^k-\tilde{u}^k\|^2\\ &=\|v^k-u^*\|^2+(\frac{\rho_k^2}{\alpha^2}-1)\|v^k-\tilde{u}^k\|^2.\end{aligned}\tag{7}$$

Note that $\lim_{k\to\infty}\rho_k=0$, we may assume without loss of generality that $\rho_k<\alpha$. Hence, from (7), we have

$$\|w^k-u^*\|^2\le\|v^k-u^*\|^2=\|\Gamma_{r_k}u^k-\Gamma_{r_k}u^*\|^2\le\|u^k-u^*\|^2.$$

From (3), we deduce that

$$\begin{aligned}\|u^{k+1}-u^*\| &=\|\beta_k(u^k-u^*)+(1-\beta_k)(S(\alpha_ku+(1-\alpha_k)w^k)-u^*)\|\\ &\le \beta_k\|u^k-u^*\|+(1-\beta_k)\|\alpha_k(u-u^*)+(1-\alpha_k)(w^k-u^*)\|\\ &\le \beta_k\|u^k-u^*\|+(1-\beta_k)(\alpha_k\|u-u^*\|+(1-\alpha_k)\|w^k-u^*\|)\\ &\le (1-\beta_k)\alpha_k\|u-u^*\|+(1-(1-\beta_k)\alpha_k)\|u^k-u^*\|.\end{aligned}\tag{8}$$

It follows from (8) induction that

$$\|u^k-u^*\|\le\max\{\|u-u^*\|,\|u^0-u^*\|\},\quad k\ge 0.$$

Therefore $\{u^k\}$ is bounded. It is easy to prove that $\{\tilde{u}^k\}$, $\{v^k\}$ and $\{w^k\}$ are all bounded.

**Lemma 3.2** $\lim_{k\to\infty}\|u^{k+1}-u^k\|=0$.

**Proof.** First, we estimate $\|w^{k+1} - w^k\|$. Noting that $P_C$ and $I - \rho_k T$ is nonexpansive, we have

$$\begin{aligned}
\|w^{k+1} - w^k\| &= \|P_C[v^{k+1} - \rho_{k+1}T(\tilde{u}^{k+1})] - P_C[v^k - \rho_k T(\tilde{u}^k)]\| \\
&\le \|(v^{k+1} - \rho_{k+1}T(\tilde{u}^{k+1})) - (v^k - \rho_k T(\tilde{u}^k))\| \\
&= \|(v^{k+1} - \rho_{k+1}T(v^{k+1})) - (v^k - \rho_{k+1}T(v^k)) \\
&\quad + \rho_{k+1}(T(v^{k+1}) - T(\tilde{u}^{k+1}) - T(v^k)) + \rho_k T(\tilde{u}^k)\| \qquad (9) \\
&\le \|(v^{k+1} - \rho_{k+1}T(v^{k+1})) - (v^k - \rho_{k+1}T(v^k))\| \\
&\quad + (\rho_{k+1} + \rho_k)M_1 \\
&\le \|v^{k+1} - v^k\| + (\rho_{k+1} + \rho_k)M_1,
\end{aligned}$$

where $M_1$ is some constant such that

$$\sup\{\|T(v^{k+1}) - T(\tilde{u}^{k+1}) - T(v^k)\| + \|T(\tilde{u}^k)\|, \quad k \ge 0\} \le M_1.$$

On the other hand, from $v^k = \Gamma_{r_k} u^k$ and $v^{k+1} = \Gamma_{r_{k+1}} u^{k+1}$, we have

$$F(v^k, w) + \frac{1}{r_k}\langle w - v^k, v^k - u^k\rangle \ge 0, \quad \forall w \in C \qquad (10)$$

and

$$F(v^{k+1}, w) + \frac{1}{r_{k+1}}\langle w - v^{k+1}, v^{k+1} - u^{k+1}\rangle \ge 0, \quad \forall\ w \in C. \qquad (11)$$

Putting $w = v^{k+1}$ in (10) and $w = v^k$ in (11), we have

$$F(v^k, v^{k+1}) + \frac{1}{r_k}\langle v^{k+1} - v^k, v^k - u^k\rangle \ge 0, \qquad (12)$$

and

$$F(v^{k+1}, v^k) + \frac{1}{r_{k+1}}\langle v^k - v^{k+1}, v^{k+1} - u^{k+1}\rangle \ge 0. \qquad (13)$$

From the monotonicity of $F$, we have

$$F(v^k, v^{k+1}) + F(v^{k+1}, v^k) \le 0.$$

So, from (12) and (13), we can conclude that

$$\langle v^{k+1} - v^k, \frac{v^k - u^k}{r_k} - \frac{v^{k+1} - u^{k+1}}{r_{k+1}}\rangle \ge 0$$

and hence

$$\langle v^{k+1} - v^k, v^k - v^{k+1} + v^{k+1} - u^k - \frac{r_k}{r_{k+1}}(v^{k+1} - u^{k+1})\rangle \ge 0.$$

Since $\liminf_{k\to\infty} r_k > 0$, without loss of generality, we may assume that there exists a real number $b$ such that $r_k > b > 0$ for all $k \in N$. Then, we have

$$\begin{aligned}
\|v^{k+1} - v^k\|^2 &\le \langle v^{k+1} - v^k, u^{k+1} - u^k + (1 - \frac{r_k}{r_{k+1}})(v^{k+1} - u^{k+1})\rangle \\
&\le \|v^{k+1} - v^k\|\{\|u^{k+1} - u^k\| + |1 - \frac{r_k}{r_{k+1}}|\|v^{k+1} - u^{k+1}\|\}
\end{aligned}$$

and hence

$$\|v^{k+1} - v^k\| \le \|u^{k+1} - u^k\| + \frac{M_2}{b}|r_{k+1} - r_k|, \qquad (14)$$

where $M_2$ is a constant such that $\sup\{\|v^{k+1} - u^{k+1}\|, k \geq 0\} \leq M_2$. Substituting (14) into (9), we have

$$\begin{aligned} \|w^{k+1} - w^k\| &\leq \|u^{k+1} - u^k\| + (\rho_{k+1} + \rho_k)M_1 \\ &\quad + \frac{M_2}{b}|r_{k+1} - r_k|. \end{aligned} \tag{15}$$

Define $u^{k+1} = \beta_k u^k + (1 - \beta_k)x^k, \forall k \geq 0$. It follows that

$$\begin{aligned} x^{k+1} - x^k &= \frac{u^{k+2} - \beta_{k+1}u^{k+1}}{1 - \beta_{k+1}} - \frac{u^{k+1} - \beta_k u^k}{1 - \beta_k} \\ &= S(\alpha_{k+1}u + (1 - \alpha_{k+1})w^{k+1}) - S(\alpha_k u + (1 - \alpha_k)w^k). \end{aligned} \tag{16}$$

It follows from (15) and (16) that

$$\begin{aligned} &\|x^{k+1} - x^k\| - \|u^{k+1} - u^k\| \\ &\leq \|(\alpha_{k+1}u + (1 - \alpha_{k+1})w^{k+1}) - (\alpha_k u + (1 - \alpha_k)w^k)\| \\ &\quad - \|u^{k+1} - u^k\| \\ &\leq \alpha_{k+1}(\|u\| + \|w^{k+1}\|) + \alpha_k(\|u\| + \|w^k\|) \\ &\quad + (\rho_{k+1} + \rho_k)M_1 + \frac{M_2}{b}|r_{k+1} - r_k|, \end{aligned}$$

which implies that $\limsup_{k\to\infty}(\|x^{k+1} - x^k\| - \|u^{k+1} - u^k\|) \leq 0$. This together with Lemma 2.3 implies that $\lim_{k\to\infty} \|x^k - u^k\| = 0$. Consequently $\lim_{k\to\infty} \|u^{k+1} - u^k\| = \lim_{k\to\infty}(1 - \beta_k)\|x^k - u^k\| = 0$.

**Lemma 3.3** $\lim_{k\to\infty} \|S(\tilde{u}^k) - \tilde{u}^k\| = 0$.

**Proof.** Since $u^{k+1} = \beta_k u^k + (1 - \beta_k)S(\alpha_k u + (1 - \alpha_k)w^k)$, we have

$$\begin{aligned} \|u^k - S(w^k)\| &\leq \|u^k - u^{k+1}\| + \|u^{k+1} - S(w^k)\| \\ &\leq \|u^k - u^{k+1}\| + \beta_k\|u^k - S(w^k)\| + (1 - \beta_k)\alpha_k\|u - w^k\|, \end{aligned}$$

that is

$$\|u^k - S(w^k)\| \leq \frac{1}{1 - \beta_k}\|u^k - u^{k+1}\| + \alpha_k\|u - w^k\|.$$

It follows that

$$\lim_{n\to\infty} \|u^k - S(w^k)\| = 0. \tag{17}$$

Since $\Gamma_{r_k}$ is firmly nonexpansive, we have

$$\begin{aligned} \|v^k - u^*\|^2 &= \|\Gamma_{r_k}u^k - \Gamma_{r_k}u^*\|^2 \\ &\leq \langle \Gamma_{r_k}u^k - \Gamma_{r_k}u^*, u^k - u^* \rangle \\ &= \langle v^k - u^*, u^k - u^* \rangle \\ &= \frac{1}{2}(\|v^k - u^*\|^2 + \|u^k - u^*\|^2 - \|u^k - v^k\|^2) \end{aligned}$$

and hence

$$\|v^k - u^*\|^2 \leq \|u^k - u^*\|^2 - \|u^k - v^k\|^2. \tag{18}$$

By (3), we have

$$
\begin{aligned}
\|u^{k+1}-u^*\|^2 &= \|\beta_k(u^k-u^*)+(1-\beta_k)[S(\alpha_k u+(1-\alpha_k)w^k)-u^*]\|^2 \\
&\le \beta_k\|u^k-u^*\|^2+(1-\beta_k)\|\alpha_k u+(1-\alpha_k)w^k-u^*\|^2 \\
&\le \beta_k\|u^k-u^*\|^2+(1-\beta_k)(\alpha_k\|u-u^*\|^2 \\
&\quad +(1-\alpha_k)\|w^k-u^*\|^2) \\
&= \beta_n\|u^k-u^*\|^2+(1-\beta_k)\alpha_k\|u-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)\|w^k-u^*\|^2.
\end{aligned} \tag{19}
$$

From (7) and (19), we have

$$
\begin{aligned}
\|u^{k+1}-u^*\|^2 &\le \beta_k\|u^k-u^*\|^2+(1-\beta_k)\alpha_k\|u-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)\|v^k-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)(\frac{\rho_k^2}{\alpha^2}-1)\|v^k-\tilde{u}^k\|^2 \\
&\le \beta_k\|u^k-u^*\|^2+(1-\beta_k)\alpha_k\|u-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)\|u^k-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)(\frac{\rho_k^2}{\alpha^2}-1)\|v^k-\tilde{u}^k\|^2.
\end{aligned}
$$

Then we derive

$$
\begin{aligned}
&(1-\beta_k)(1-\alpha_k)(1-\frac{\rho_k^2}{\alpha^2})\|v^k-\tilde{u}^k\|^2 \\
&\le \beta_k\|u^k-u^*\|^2+(1-\beta_k)\alpha_k\|u-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)\|u^k-u^*\|^2-\|u^{k+1}-u^*\|^2 \\
&\le (1-\beta_k)\alpha_k\|u-u^*\|^2+\|u^k-u^*\|^2-\|u^{k+1}-u^*\|^2 \\
&\le (1-\beta_k)\alpha_k\|u-u^*\|^2+(\|u^k-u^*\|+\|u^{k+1}-u^*\|)\|u^k-u^{k+1}\|.
\end{aligned} \tag{20}
$$

It is clear that $\liminf_{k\to\infty}(1-\beta_k)(1-\alpha_k)(1-\frac{\rho_k^2}{\alpha^2})>0$. So, from (R1) and (20), we have

$$
\lim_{k\to\infty}\|v^k-\tilde{u}^k\|=0. \tag{21}
$$

From (18) and (19), we have

$$
\begin{aligned}
\|u^{k+1}-u^*\|^2 &\le \beta_k\|u^k-u^*\|^2+(1-\beta_k)\alpha_k\|u-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)\|v^k-u^*\|^2 \\
&\le \beta_k\|u^k-u^*\|^2+(1-\beta_k)\alpha_k\|u-u^*\|^2 \\
&\quad +(1-\beta_k)(1-\alpha_k)(\|u^k-u^*\|^2-\|u^k-v^k\|^2) \\
&\le \|u^k-u^*\|^2+(1-\beta_k)\alpha_k\|u-u^*\|^2 \\
&\quad -(1-\beta_k)(1-\alpha_k)\|u^k-v^k\|^2,
\end{aligned}
$$

that is

$$\begin{aligned}&(1-\beta_k)(1-\alpha_k)\|u^k-v^k\|^2\\&\leq(1-\beta_k)\alpha_k\|u-u^*\|^2+\|u^k-u^*\|^2-\|u^{k+1}-u^*\|^2\\&\leq(1-\beta_k)\alpha_k\|u-u^*\|^2+(\|u^k-u^*\|+\|u^{k+1}-u^*\|)\times\|u^{k+1}-u^k\|,\end{aligned}$$

which implies that

$$\lim_{k\to\infty}\|u^k-v^k\|=0. \tag{22}$$

Since

$$\begin{aligned}\|S(\tilde{u}^k)-\tilde{u}^k\|&\leq\|S(\tilde{u}^k)-S(w^k)\|+\|S(w^k)-u^k\|+\|u^k-v^k\|+\|v^k-\tilde{u}^k\|\\&\leq\|\tilde{u}^k-w^k\|+\|S(w^k)-u^k\|+\|u^k-v^k\|+\|v^k-\tilde{u}^k\|\\&=\|P_C[v^k-\rho_kT(v^k)]-P_C[v^k-\rho_kT(\tilde{u}^k)]\|+\|S(w^k)-u^k\|\\&\quad+\|u^k-v^k\|+\|v^k-\tilde{u}^k\|\\&\leq\rho_k\|T(v^k)-T(\tilde{u}^k)\|+\|S(w^k)-u^k\|\\&\quad+\|u^k-v^k\|+\|v^k-\tilde{u}^k\|.\end{aligned}$$

This together with (R3), (17), (21) and (22) implies that $\lim_{k\to\infty}\|S(\tilde{u}^k)-\tilde{u}^k\|=0$.

**Lemma 3.4** $\limsup_{k\to\infty}\langle u-z^0,w^k-z^0\rangle\leq 0$, where $z^0=P_\Omega(u)$ and $\Omega=Fix(S)\cap VI(T,C)\cap EP(F)$.

**Proof.** First, we show that $\limsup_{k\to\infty}\langle u-z^0,S(\tilde{u}^k)-z^0\rangle\leq 0$. To show this inequality, we can choose a subsequence $\{\tilde{u}^{k_j}\}$ of $\{\tilde{u}^k\}$ such that

$$\lim_{j\to\infty}\langle u-z^0,S(\tilde{u}^{k_j})-z^0\rangle=\limsup_{k\to\infty}\langle u-z^0,S(\tilde{u}^k)-z^0\rangle.$$

Since $\{\tilde{u}^{k_j}\}$ is bounded, there exists a subsequence $\{\tilde{u}^{k_{j_i}}\}$ of $\{\tilde{u}^{k_j}\}$ which converges weakly to $z$. Without loss of generality, we can assume that $\tilde{u}^{k_j}\to z$ weakly. From $\|S(\tilde{u}^k)-\tilde{u}^k\|\to 0$, we obtain $S(\tilde{u}^{k_j})\to z$ weakly.

First we show $z\in EP(F)$. By $v^k=\Gamma_{r_k}u^k$, we have

$$F(v^k,w)+\frac{1}{r_k}\langle w-v^k,v^k-u^k\rangle\geq 0,\quad\forall w\in C.$$

From the monotonicity of $F$, we have $\frac{1}{r_k}\langle w-v^k,v^k-u^k\rangle\geq -F(v^k,w)\geq F(w,v^k)$ and hence $\langle w-v^{k_j},\frac{v^{k_j}-u^{k_j}}{r_{k_j}}\rangle\geq F(w,v^{k_j})$. Since $\frac{v^{k_j}-u^{k_j}}{r_{k_j}}\to 0$ and $v^{k_j}\to z$ weakly, from the lower semi-continuity of $F(u,v)$ on the second variable $v$, we have

$$F(w,z)\leq 0,\forall w\in C.$$

For $t$ with $0<t\leq 1$ and $w\in C$, let $w_t=tw+(1-t)z$. Since $w\in C$ and $z\in C$, we have $w_t\in C$ and hence $F(w_t,z)\leq 0$. So, from the convexity of equilibrium bifunction $F(u,v)$ on the second variable $v$ , we have

$$0=F(w_t,w_t)\leq tF(w_t,w)+(1-t)F(w_t,z)\leq tF(w_t,w).$$

Hence $F(w_t,w)\geq 0$. Then, we have $F(z,w)\geq 0,\forall w\in C$. This indicates that $z\in EP(F)$.

Second, we show that $z \in VI(T, C)$. Set

$$Av = \begin{cases} T(v) + N_C v, & \text{if } v \in C, \\ \emptyset, & \text{if } v \notin C. \end{cases}$$

Then $A$ is maximal monotone. Let $(v, u) \in G(A)$. Since $u - T(v) \in N_C v$ and $\tilde{u}^k \in C$, we have

$$\langle v - \tilde{u}^k, u - T(v)\rangle \geq 0.$$

On the other hand, from $\tilde{u}^k = P_C[v^k - \rho_k T(v^k)]$, we have

$$\langle v - \tilde{u}^k, \tilde{u}^k - (v^k - \rho_k T(v^k))\rangle \geq 0$$

and hence

$$\langle v - \tilde{u}^k, \frac{\tilde{u}^k - v^k}{\rho_k} + T(v^k)\rangle \geq 0.$$

It follows that

$$\begin{aligned} \langle v - \tilde{u}^{k_j}, u\rangle &\geq \langle v - \tilde{u}^{k_j}, T(v)\rangle \\ &\quad - \langle v - \tilde{u}^{k_j}, \frac{\tilde{u}^{k_j} - v^{k_j}}{\rho_{k_j}} + T(v^{k_j})\rangle \\ &= \langle v - \tilde{u}^{k_j}, T(v) - \frac{\tilde{u}^{k_j} - v^{k_j}}{\rho_{k_j}} - T(v^{k_j})\rangle \\ &= \langle v - \tilde{u}^{k_j}, T(v) - T(\tilde{u}^{k_j})\rangle + \langle v - \tilde{u}^{k_j}, T(\tilde{u}^{k_j}) - T(v^{k_j})\rangle \\ &\quad - \langle v - \tilde{u}^{k_j}, \frac{\tilde{u}^{k_j} - v^{k_j}}{\rho_{k_j}}\rangle \\ &\geq \langle v - \tilde{u}^{k_j}, T(\tilde{u}^{k_j}) - T(v^{k_j})\rangle - \langle v - \tilde{u}^{k_j}, \frac{\tilde{u}^{k_j} - v^{k_j}}{\rho_{k_j}}\rangle \end{aligned}$$

which implies that $\langle v - z, u\rangle \geq 0$. We have $z \in A^{-1}(0)$ and hence $z \in VI(T, C)$.

Thirdly, we prove that $z \in Fix(S)$. Assume that $z \notin Fix(S)$. Since $\tilde{u}^{k_j} \rightharpoonup z$ and $z \neq S(z)$, by Opial's condition we have

$$\begin{aligned} \liminf_{j\to\infty} \|\tilde{u}^{k_j} - z\| &< \liminf_{j\to\infty} \|\tilde{u}^{k_j} - S(z)\| \\ &\leq \liminf_{j\to\infty} (\|\tilde{u}^{k_j} - S(\tilde{u}^{k_j})\| + \|S(\tilde{u}^{k_j}) - S(z)\|) \\ &\leq \liminf_{j\to\infty} \|\tilde{u}^{k_j} - z\|, \end{aligned}$$

which is a contradiction. Then we get $z \in Fix(S)$. Hence, we deduce that $z \in Fix(S) \cap VI(T, C) \cap EP(F)$. Therefore, from the property (iii) of $P_C$, we have

$$\begin{aligned} \limsup_{k\to\infty} \langle u - z^0, w^k - z^0\rangle &= \limsup_{k\to\infty} \langle u - z^0, S(\tilde{u}^k) - z^0\rangle \\ &= \lim_{j\to\infty} \langle u - z^0, S(\tilde{u}^{k_j}) - z^0\rangle \\ &= \langle u - z^0, z - z^0\rangle \leq 0. \end{aligned} \tag{23}$$

## 4. Strong convergence

Now we prove the strong convergence of Algorithm 3.1.

**Theorem 4.1** The sequence $\{u^k\}$ defined by (3) converges strongly to $z^0 = P_\Omega(u)$.

**Proof.** From (3), we have

$$
\begin{aligned}
\|u^{k+1} - z^0\|^2 &\le \beta_k \|u^k - z^0\|^2 + (1-\beta_k)\|S(\alpha_k u + (1-\alpha_k)w^k) - z^0\|^2 \\
&\le \beta_k \|u^k - z^0\|^2 + (1-\beta_k)\|\alpha_k(u - z^0) + (1-\alpha_k)(w^k - z^0)\|^2 \\
&\le \beta_k \|u^k - z^0\|^2 + (1-\beta_k)[(1-\alpha_k)\|w^k - z^0\|^2 \\
&\quad + 2\alpha_k \langle u - z^0, \alpha_k(u - z^0) + (1-\alpha_k)(w^k - z^0)\rangle] \\
&\le \beta_k \|u^k - z^0\|^2 + (1-\beta_k)[(1-\alpha_k)\|u^k - z^0\|^2 \\
&\quad + 2\alpha_k \langle u - z^0, \alpha_k(u - z^0) + (1-\alpha_k)(w^k - z^0)\rangle] \\
&= [1 - (1-\beta_k)\alpha_k]\|u^k - z^0\|^2 + 2(1-\beta_k)\alpha_k^2 \|u - z^0\|^2 \\
&\quad + 2(1-\beta_k)\alpha_k(1-\alpha_k)\langle u - z^0, w^k - z^0\rangle \\
&= [1 - (1-\beta_k)\alpha_k]\|u^k - z^0\|^2 + (1-\beta_k)\alpha_k \Big\{ 2\alpha_k \|u - z^0\|^2 \\
&\quad + 2(1-\alpha_k)\langle u - z^0, w^k - z^0\rangle \Big\}.
\end{aligned} \tag{24}
$$

Note that $\limsup_{k\to\infty} \Big\{ 2\alpha_k \|u - z^0\|^2 + 2(1-\alpha_k)\langle u - z^0, w^k - z^0\rangle \Big\} \le 0$. Hence, by Lemma 2.4 and (24), we conclude that the sequence $\{u^k\}$ converges strongly to $z^0$. This completes the proof.

It is clear that the following conclusion holds.

**Theorem 4.2** Let $C$ be a nonempty closed convex subset of a real Hilbert space $H$. Let $T$ be an $\alpha$-inverse-strongly monotone mapping of $C$ into $H$ and let $S$ be a nonexpansive mapping of $C$ into itself such that $Fix(S) \cap VI(T, C) \neq \emptyset$. Let $\{u^k\}$ be the sequence defined by Algorithm 3.2. If the algorithm parameters satisfy conditions (R1)-(R3), then the sequence $\{u^k\}$ converge strongly to $P_{Fix(S)\cap VI(T,C)}(u)$. □

## References


1. G. Stampacchia, *Formes bilineaires coercitives sur les ensembles convexes*, C. R. Acad. Sci. Paris, **258** (1964), 4413-4416.
2. A. Bnouhachem and M. Aslam Noor, *Numerical comparison between prediction correction methods for general variational inequalities*, Appl. Math. Computation, **186** (2007), 496-505.
3. B.S. He and L.Z. Liao, *Improvement of some projection methods for monotone variational inequalities*, J. Optim. Theory Appl. **112** (2002), 111-128.
4. B.S. He, Z.H. Yang and X.M. Yuan, *An approximate proximal-extragradient type method for monotone variational inequalities*, J. Math. Anal. Appl. **300** (2004), 362-374.
5. M. Aslam Noor, *New extragradient-type methods for general variational inequalities*, J. Math. Anal. Appl. **277** (2003), 379-395.
6. M. Aslam Noor, *Some developments in general variational inequalities*, Appl. Math. Computation, **152** (2004), 199-277.

7. M. Aslam Noor and A. Bnouhachem, *On an iterative algorithm for general variational inequalities*, Appl. Math. Comput.**185** (2007), 155-168.
8. J.C. Yao, *Variational inequalities with generalized monotone operators*, Math. Operations Research, **19** (1994), 691-705.
9. L.C. Zeng, *On a general projection algorithm for variational inequalities*, J. Optim. Theory Appl. **97** (1998), 229-235.
10. O. Chadli, S. Schaible and J.C. Yao, *Regularized equilibrium problems with an application to noncoercive hemivariational inequalities*, J. Optim. Theory Appl. **121** (2004), 571-596.
11. L.C. Zeng and J.C. Yao, *Strong convergence theorem by an extragradient method for fixed point problems and variational inequality problems*, Taiwanese J. Math. **10** (2006), 1293-1303.
12. W. Takahashi, and M. Toyoda, *Weak convergence theorems for nonexpansive mappings and monotone mappings*, Journal of Optimization Theory and Applications, **118** (2003), 417-428.
13. N. Nadezhkina, and W. Takahashi, *Weak convergence theorem by an extragradient method for nonexpansive mappings and monotone mappings*, Journal of Optimization Theory and Applications, **128** (2006), 191-201.
14. G.M. Korpelevich, *An extragradient method for finding saddle points and for other problems*, Ekonomika i Matematicheskie Metody, **12** (1976), 747-756.
15. A. Bnouhachem, M.A. Noor and Z. Hao, *Some new extragradient methods for variational inequalities*, Nonlinear Analysis (2008), doi:10.1016/j.na.2008.02.014.
16. P.L. Combettes, S.A. Hirstoaga, *Equilibrium programming using proximal-like algorithms*, Math. Program , **78** (1997), 29-41.
17. S. Takahashi and W. Takahashi, *Viscosity approximation methods for equilibrium problems and fixed point problems in Hilbert spaces*, J. Math. Anal. Appl. **331** (2007), 506-515.
18. S. Plubtieng and R. Punpaeng, *A new iterative method for equilibrium problems and fixed point problems of nonexpansive mappings and monotone mappings*, Appl. Math. Comput. **197** (2008), 548-558.
19. T. Suzuki, *Strong convergence of Krasnoselskii and Mann's type sequences for one-parameter nonexpansive semigroups without Bochner integrals*, J. Math. Anal. Appl. **305** (2005), 227-239.
20. H.K. Xu, *Viscosity approximation methods for nonexpansive mappings*, J. Math. Anal. Appl. **298** (2004), 279-291.
21. E. Blum and W. Oettli, *From optimization and variational inequalities*, Math. Student, **63** (1994), 123-145.
22. M. Aslam Noor and W. Oettli, *On general nonlinear complementarity problems and quasi equilibria*, Le Math. **49** (1994), 313-331.
23. M. Aslam Noor, *Fundamentals of equilibrium problems*, Math. Inequal. Appl.**9** (2006), 529-566.
24. M. Aslam Noor, *Invex equilibrium problems*, J. Math. Anal. Appl. **302** (2005), 463-475.
25. M. Aslam Noor and K. Inayat Noor, *Hemiequilibrium-like problems*, Nonl. Anal. **64** (2006), 2631-2642.

COMSATS Institute of Information Technology, Mathematics Department, Islamabad, Pakistan
*E-mail address*: noormaslam@gmail.com

Tianjin Polytechnic University, Department of Mathematics, Tianjin 300160, China
*E-mail address*: yaoyonghong@yahoo.cn

Cheng Shiu University, Department of Information Management, Kaohsiung 833, Taiwan
*E-mail address*: simplex_liou@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 141–144
ISSN 1930-1235: (2008)

# ALGEBRAIC ASPECTS OF DIGITAL COMMUNICATIONS

T. Shaska

*Department of Mathematics and Statistics*
*Oakland University,*
*Rochester, MI, USA*
*shaska@oakland.edu*

M. Qarri

*Department of Computer Science and Electrical Engineering*
*University of Vlora,*
*Vlora, Albania*
*mbifsha@univlora.edu.al*

Developments of the last few decades in digital communications have created a close link between mathematics and areas of computer science and electrical engineering. A collaboration between such areas now seems very natural due to problems which require deep knowledge and expertise in each area. A special role in such collaboration has played algebra and some of its branches such as algebraic geometry, computational algebra, group theory, etc. As a result of such cooperation now we have disciplines such as coding theory and cryptography which are considered a mix of mathematics, computer science, and electrical engineering.

Coding theory is one of the most important and direct applications of information theory. It is a branch of electrical engineering, digital communication, mathematics, and computer science designing efficient and reliable data transmission methods, so that redundancy in the data can be removed and errors induced by a noisy channel can be corrected. It started with Shannon, Hamming, and many others in the mid 20-th century and became one of the most active areas of research for most of the second half of the 20-th century. Algebraic coding theory was the main direction of coding theory, even though recently other ways of coding have been developed. For more details in coding theory a wonderful source is [2] among many other publications.

Cryptology, is the science of hiding information, and historically has received much attention from the public. As a science was also put in solid background in the second half of the 20-th century. It is a mixture of theoretical mathematics and computer science which focuses more in areas such as number theory, algebraic geometry, graph theory, algorithm analysis, etc. There have been many conferences and publications which have explored the common ground among such areas; some of the more recent ones are [6, 7].

This special issue came out of the conference "New Challenges in Digital Communications" which was organized at the University of Vlora, during April 27 - May 9, 2008. This was funded by a NATO grant as a "Advanced Study Institute"; see [4], [5] for details. The conference focused precisely on connections between algebra, algebraic geometry, number theory, graph theory, and related areas of mathematics with coding theory and cryptography.

There were over 130 participants in the conference from all over the world. We want to thank NATO, the University of Vlora, and the Albanian Ministry of Science and Education for providing the funding of such conference. Special thanks to all the staff of the University of Vlora who were involved in all organizational tasks of the conference, especially the Department of Mathematics and the Department of Computer Science and Electrical Engineering, and the Vlora Conference Center at the University of Vlora.

Most of the papers focus on coding theory and some others in cryptography. While such topics were the main focus of the conference, we did accept papers which explore more theoretical aspects such as computational group theory, computational algebraic geometry, etc. There are overall 13 papers in this volume which cover a wide range of topics. There is also a proceedings volume of the conference which will be published by NATO. This volume will contain all the lectures which were held during the Advanced Study Institute; see [3].

We hope that such collection of papers will serve the scientific community in mathematics, computer science, and electrical engineering and foster closer relations among such communities. It is our intention to organize yearly conferences in Vlora in similar topics and with similar goals.

**Acknowledgements:** We sincerely thank all the authors for their contributions of this special issue. We also thank the anonymous referees for all their work going through all the papers. Our final thanks to NATO for sponsoring such conference.

## 1. Aspektet algjebrike te komunikacioneve dixhitale

Zhvillimet e dekadave të fundit në fushën e komunikimit dixhital kanë krijuar një lidhje të ngushtë midis matematikës dhe fushave të inxhinierisë kompjuterike dhe elektrike. Një bashkëpunim ndërmjet këtyre fushave tashmë duket tepër natyral në sajë të problemeve që kërkojnë njohuri të thella dhe ekspertizë në secilën fushë. Një rol të vecantë në një bashkëpunim të tillë ka luajtur algjebra dhe disa nga degët e saj të tilla si gjeometria algjebrike, algjebra kompjuterike, teoria e grupeve, etj. Si rezultat i një bashkëpunimi të tillë tani disponojmë disiplina të tilla si teoria e kodeve dhe kriptografia, të cilat janë konsideruar si përzierje e matematikës, inxhinierisë se shkencave kompjuterike dhe elektrike.

Teoria e kodeve është një nga aplikimet më të rëndësishme dhe të drejtpërdrejta të teorisë së infomacionit. Ajo është një degë e inxhinierisë elektrike, komunikimit dixhital, matematikës dhe shkencave kompjuterike, që përdor metoda eficente dhe të besueshme të transmetimit të të dhënave, në mënyrë që të eleminohen humbjet në informacionet dhe të korrigjohen gabimet e induktuara nga një kanal zhurme. Kjo degë ka filluar me Shannon, Hamming dhe shumë të tjerë në mes të shekullit XX dhe u bë një nga fushat më aktive të kërkimit për pjesën më të madhe të gjysmës së shekullit XX. Teoria e kodeve algjebrike ishte një nga drejtimet kryesore të teorisë së kodeve, edhe pse së fundmi mënyra të tjera kodimi janë zhvilluar. Për

më shumë detaje në teorinë e kodeve një burim i mrekullueshëm është : [2] midis publikimeve të tjera.

Kriptologjia është shkenca e fshehjes së informacionit, dhe historikisht ka qenë në vëmendjen e publikut. Si shkencë gjithashtu ka marrë formën e plotë në gjysmën e dytë të shekullit XX. Ajo është një kombinim i matematikës teorike dhe shkencës kompjuterike, e cila fokusohet me shumë në fusha të tilla si teoria e numrave, gjeometria algjebrike, teoria e grafeve, analiza algoritmike, etj. Janë zhvilluar shumë konferenca dhe ka patur mjaft publikime të cilat kanë eksploruar bazën e përbashkët midis këtyre fushave; ndër më të fundit janë [6,7].

Ky numër i vecantë i revistës *Albanian J. Math.* rezultoi nga konferenca "Sfida të reja në Komunikimin Dixhital", e cila u organizua pranë Universitetit të Vlorës, gjatë periudhës 27 Prill- 9 Maj, 2008. Ajo u financua nga një grant i NATO-s si "Instituti i Studimeve të Avancuara"; për detaje shih [4], [5]. Konferenca u përqëndrua saktësisht në lidhjet midis algjebrës, gjeometrisë algjebrike, teorisë së numrave, teorisë së grafeve, dhe fushave të tjera të matematikës të lidhura me teorinë e kodeve dhe kriptografinë.

Në konferencë kishte më shumë se 130 pjesëmarrës nga e gjithë bota. Ne duam të falënderojmë NATO-n, Universitetin e Vlorës dhe Ministrinë e Arsimit dhe Shkencës shqiptare që na siguruan fondet për një konferencë të tillë. Një falënderim i vecantë shkon për gjithë stafin e universitetit të Vlorës që mori pjesë në detyrat organizative, vecanërisht Departamentin e Matematikës dhe të Shkencave Kompjuterike dhe Elektrike, dhe Qendrën e Konferencave Vlorë pranë Universitetit të Vlorës.

Pjesa më e madhe e artikujve përqëndrohen tek teoria e kodeve dhe disa prej tyre në kriptografi. Ndërsa këto tema ishin fokusi kryesor i konferencës, ne pranuam edhe artikuj që eksploronin më shumë aspekte teorike të tilla si toeria e grupeve llogaritëse, gjeometria algjebrike llogaritëse, etj. Janë gjithsej 13 artikuj në këtë volum që mbulojnë një gamë të gjerë cështjesh. Gjithashtu, ekziston një volum i punimeve të konferencës që do të publikohet nga NATO. Ky volum do të përmbajë gjithë leksionet që u mbajtën gjatë Institutit të Studimeve të Avancuara; shih [3].

Ne shpresojmë që ky koleksion artikujsh do t'i shërbejë komunitetit shkencor të matematikës. Shkencave kompjuterike dhe inxhinerisë elektrike dhe do t'i japë zhvillim marrëdhënieve të ngushta midis këtyre komuniteteve. Qëllimi ynë është që të organizojmë në Vlorë cdo vit konferenca të tilla me tema të ngjashme dhe me objektiva të ngjashëm.

Ne falënderojmë sinqerisht të gjithë autorët për kontributin e tyre në këtë cështje të vecantë. Ne falënderojmë gjithashtu shkruarësit anonimë të referencave për punën e tyre mbi gjithë këto artikuj. Dhe falënderimi ynë final shkon tek NATO për sponsorizimin e kësaj konference.

## References


[1] W. Cary Huffman, *Codes and groups*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1345–1440. MR1667953

[2] V. S. Pless, W. C. Huffman, and R. A. Brualdi (eds.), *Handbook of coding theory. Vol. I, II*, North-Holland, Amsterdam, 1998. MR1667936 (2000h:94001)

[3] T. Shaska, *New Challenges in Digital Communications*, IOS Press, Brussels, 2008.

[4] *NATO Science for Peace and Security Programme.* Website: http://www.nato.int/science/index.html.

[5] *NATO Advanced Study Institute New Challenges in Digital Communications.* Directors:T. Shaska, E. Hasimaj; April 27 - May 9, 2008, Vlora, Albania.

[6] Tanush Shaska (ed.), *Computational aspects of algebraic curves*, Lecture Notes Series on Computing, vol. 13, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005. Papers from the conference held at the University of Idaho, Moscow, ID, May 26–28, 2005. MR2182657 (2006e:14003)

[7] T. Shaska, W. C. Huffman, D. Joyner, and V. Ustimenko (eds.), *Advances in Coding Theory and Cryptography*, Developments in Mathematics, vol. 12, World Scientific, Hackensack, NJ:, 2007.

[8] Helmut Voelklein and Tanush Shaska (eds.), *Progress in Galois theory*, Developments in Mathematics, vol. 12, Springer, New York, 2005. MR2150438 (2006a:00014)

[9] W. Cary Huffman and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003. MR1996953 (2004k:94077)

[10] V. A. Ustimenko, *On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography*, Albanian J. Math. **1** (2007), no. 4, 283–295. MR2367220 (2008k:05111)

[11] Arnaldo Garcia and Henning Stichtenoth (eds.), *Topics in geometry, coding theory and cryptography*, Algebras and Applications, vol. 6, Springer, Dordrecht, 2007. MR2265387 (2007h:11003)

[12] Gary L. Mullen, Henning Stichtenoth, and Horacio Tapia-Recillas (eds.), *Finite fields with applications to coding theory, cryptography and related areas*, Springer-Verlag, Berlin, 2002. MR1995324 (2004c:11003)

[13] D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger, and J. R. Wall, *Coding theory and cryptography: the essentials*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 234, Marcel Dekker Inc., New York, 2000. Second edition, revised and expanded. MR1792696 (2002h:94091)

[14] David Joyner (ed.), *Coding theory and cryptography*, Springer-Verlag, Berlin, 2000. From Enigma and Geheimschreiber to quantum theory; Papers from the Conference on Coding Theory, Cryptography, and Number Theory (Cryptoday) held in Annapolis, MD, October 25–27, 1998. MR1747832 (2000k:94042)

[15] T. Shaska and G. S. Wijesiri, *Codes over rings of size four, Hermitian lattices, and corresponding theta functions*, Proc. Amer. Math. Soc. **136** (2008), no. 3, 849–857 (electronic). MR2361856 (2008m:11132)

[16] A. Elezi and T. Shaska, *Special issue on algebra and computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 175–177. MR2367211

[17] Tanush Shaska and Quanlong Wang, *On the automorphism groups of some AG-codes based on $C_{a,b}$ curves*, Serdica J. Comput. **1** (2007), no. 2, 193–206. MR2363086 (2008m:94029)

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 145–158
ISSN 1930-1235: (2008)

# THE COMBINATORICS OF DEGENERATE COVERS AND AN APPLICATION FOR GENERAL CURVES OF GENUS 3

Kay Magaard

*School of Mathematics,Watson Building,*
*University of Birmingham,*
*Edgbaston, Birmingham B15 2TT, UK*

Helmut Völklein

*Institute for Experimental Mathematics,*
*Universität Essen, Germany*

Götz Wiesend

*Institute for Experimental Mathematics,*
*Universität Essen, Germany*

Abstract. Let $C_g$ be a general curve of genus $g$. If $g \geq 4$ then the monodromy group of a primitive cover $C_g \to \mathbb{P}^1$ of degree $n$ is either $S_n$ or $A_n$, and both cases actually occur (under suitable conditions on $n$ for fixed $g$). For $g = 3$ also the groups $GL_3(2)$ and $AGL_3(2)$ occur. In the present paper we settle the last possible case of $AGL_4(2)$. This requires new methods (which may be of independent interest) studying the combinatorial structure of degenerate covers.

## 1. Introduction

Let $C_g$ be a general curve of genus $g \geq 2$ (over $\mathbb{C}$). Then $C_g$ has a cover to $\mathbb{P}^1$ of degree $n$ if and only if $2(n-1) \geq g$. This is a classical fact of algebraic geometry. If $C_g$ has a cover to $\mathbb{P}^1$ of degree $n$, then there is such a cover that is simple, i.e., has monodromy group $S_n$ and all inertia groups are generated by transpositions. The question arises whether $C_g$ admits other types of covers to $\mathbb{P}^1$.

If there is a cover $C_g \to \mathbb{P}^1$ branched at $r$ points of $\mathbb{P}^1$ and $g \geq 2$ then $r \geq 3g$ (see Remark 2.2 below). Zariski [Za] used this to show that if $g > 6$ then there is no such cover with solvable monodromy group. The condition $r \geq 3g$ was further used by Guralnick to restrict the possibilities for the monodromy group $G$ of a cover $C_g \to \mathbb{P}^1$ of degree $n$. Assume the cover does not factor non-trivially, i.e., $G$ is a primitive subgroup of $S_n$. (Knowledge of this case is sufficient to know all types of covers $C_g \to \mathbb{P}^1$; this was already observed by Zariski [Za], see [GM]). If further

$g > 3$, then $G = S_n$ or $G = A_n$. For $g = 3$ there are 3 additional cases, with $n = 7, 8, 16$ and $G = GL_3(2), AGL_3(2), AGL_4(2)$, respectively. This was proved by Guralnick and Magaard [GM] and Guralnick and Shareshian [GS], using the classification of finite simple groups.

As noted in [GM], it was not known whether the case $G = A_n$ actually occurs. This was answered in the affirmative in [MV]. Also the cases $GL_3(2)$ and $AGL_3(2)$ in genus 3 were settled in [MV]. Here we show that also the last remaining case $G = AGL_4(2)$ occurs in genus 3. This case is more difficult and requires new techniques which may be of independent interest.

Our proof is based on studying degenerations of covers of $\mathbb{P}^1$, i.e., coalescing of branch points. In the usual description using the stable compactification of $\mathcal{M}_{0,r}$, coalescing of branch points means that the lower $\mathbb{P}^1$ degenerates into a tree of genus 0 curves. We describe certain such degenerations of $\mathbb{P}^1$ by the notion of a **multi-list**. The multi-list describes how the branch points are grouped together (in various levels of degeneration) such that the topological model of the degenerate $\mathbb{P}^1$ is obtained by shrinking to a point certain standard paths around blocks of branch points. The points of the degenerate $\mathbb{P}^1$ that arise from the shrinking of such a path are the **nodes**. In our formal approach we actually do not refer to this operation of shrinking paths, but we use the reverse operation of **replacing a node by a tube**.

Recall the usual group-theoretic data associated with a cover of $\mathbb{P}^1$ of degree $n$: The tuple of branch cycles $\sigma = (\sigma_1, \ldots, \sigma_r)$, where the $\sigma_i$ are permutations in $S_n$ associated with the branch points (local monodromy). This data depends only on the choice of a homotopy basis of $\mathbb{P}^1$ minus the branch points, and is therefore uniquely determined up to braid group action. Given the degeneration of $\mathbb{P}^1$ (described by a multi-list) and the tuple $\sigma$ of branch cycles of the original cover of $\mathbb{P}^1$, there is canonically associated a cover of the degenerate $\mathbb{P}^1$. This degenerate cover is constructed recursively in section 3.7. We have transformed this construction into a [GAP4] program which computes the combinatorial structure of this degenerate cover: The genera of the irreducible components, and the way these components are linked together. We further compute the analogous information for the stable model of this covering surface. This is the information actually used in the third part of the paper. We reproduce the GAP code in the appendix of this paper. Thus section 2 is purely topological, extending parts of the usual topological theory of covers of $\mathbb{P}^1$ to the case of covers a tree of $\mathbb{P}^1$'s. Section 2 together with the GAP code in the Appendix is independent of the rest of the paper and may be of interest or usefulness in itself.

In section 3 we complete the proof of our main result by a detailed study of a descending chain of subvarieties in the boundary of the moduli space $\mathcal{M}_3$. These subvarieties classify stable curves of topological type given by the above stable models of covering surfaces.

## 2. Moduli dimension of a tuple in $S_n$

2.1. **The Hurwitz space classifying covers of type $\sigma$.** Let $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{C}}$ the Riemann sphere. Let $\mathcal{U}^{(r)}$ be the open subvariety of $(\mathbb{P}^1)^r$ consisting of all $(p_1, ..., p_r)$ with $p_i \neq p_j$ for $i \neq j$, and $\mathcal{U}_r$ the quotient of $\mathcal{U}^{(r)}$ by the action of $S_r$ permuting $p_1, \ldots, p_r$. Thus $\mathcal{U}_r$ is the **configuration space**, consisting of unordered $r$-tuples of distinct points from $\mathbb{P}^1$. Consider a cover $f : X \to \mathbb{P}^1$ of degree $n$,

with branch points $p_1, ..., p_r \in \mathbb{P}^1$. Pick $p \in \mathbb{P}^1 \setminus \{p_1, ..., p_r\}$, and choose loops $\gamma_i$ around $p_i$ such that $\gamma_1, ..., \gamma_r$ is a standard generating system of the fundamental group $\Gamma := \pi_1(\mathbb{P}^1 \setminus \{p_1, ..., p_r\}, p)$ (see [V], Thm. 4.27); in particular, we have $\gamma_1 \cdots \gamma_r = 1$. Such a system $\gamma_1, ..., \gamma_r$ is called a homotopy basis of $\mathbb{P}^1 \setminus \{p_1, ..., p_r\}$. The group $\Gamma$ acts on the fiber $f^{-1}(p)$ by path lifting, inducing a transitive subgroup $G$ of the symmetric group $S_n$ (determined by $f$ up to conjugacy in $S_n$). It is called the **monodromy group** of $f$. The images of $\gamma_1, ..., \gamma_r$ in $S_n$ form a tuple of permutations called a tuple of **branch cycles** of $f$.

Let $\sigma_1, ..., \sigma_r$ be elements $\neq 1$ of the symmetric group $S_n$ with $\sigma_1 \cdots \sigma_r = 1$, generating a transitive subgroup. Let $\sigma = (\sigma_1, ..., \sigma_r)$. We call such a tuple **admissible**. We say a cover $f : X \to \mathbb{P}^1$ of degree $n$ **is of type** $\sigma$ if it has $\sigma$ as tuple of branch cycles relative to some homotopy basis of $\mathbb{P}^1$ minus the branch points of $f$. The genus $g$ of $X$ depends only on $\sigma$ (by the Riemann-Hurwitz formula); we write $g = g_\sigma$. The **braid orbit** of $\sigma$ is the smallest set of tuples in $S_n$ that contains $\sigma$ and is closed under (component-wise) conjugation and under the braid operations

$$(g_1, ..., g_r)^{Q_i} \quad = \quad (g_1, \ldots, \ g_{i+1}, \ g_{i+1}^{-1} g_i g_{i+1} \ , \ldots, g_r)$$

for $i = 1, ..., r-1$.

Let $\mathcal{H}_\sigma$ be the set of equivalence classes of covers of type $\sigma$. (We use the usual notion of equivalence of covers, see [V], p. 67.) Let $\sigma$, $\sigma'$ be admissible tuples in $S_n$ of length $r$. Let $f : X \to \mathbb{P}^1$ be a cover of type $\sigma$. Then $f$ is of type $\sigma'$ if and only if $\sigma'$ lies in the braid orbit of $\sigma$. In other words, we have $\mathcal{H}_\sigma = \mathcal{H}_{\sigma'}$ if and only if $\sigma'$ lies in the braid orbit of $\sigma$ (see [FrV], [V], Ch. 10).

Let $\Psi_\sigma : \mathcal{H}_\sigma \to \mathcal{U}_r$ be the map that maps the equivalence class of a cover to the set of branch points. The **Hurwitz space** $\mathcal{H}_\sigma$ carries a natural structure of irreducible quasiprojective variety such that $\Psi_\sigma$ is an algebraic morphism, and an unramified covering in the complex topology (see [FrV],[V], [BeRo]). We also have the morphism

$$\Phi_\sigma : \ \mathcal{H}_\sigma \quad \to \quad \mathcal{M}_g$$

mapping the equivalence class of a cover $f : X \to \mathbb{P}^1$ to the class of $X$ in the moduli space $\mathcal{M}_g$ (where $g = g_\sigma$). Hence the image of $\Phi_\sigma$, i.e., the locus of genus $g$ curves admitting a cover to $\mathbb{P}^1$ of type $\sigma$, is irreducible.

**Definition 2.1.** *The moduli dimension of $\sigma$, denoted by* **mod-dim**$(\sigma)$*, is the dimension of the image of $\Phi_\sigma$; i.e., the dimension of the locus of genus $g$ curves admitting a cover to $\mathbb{P}^1$ of type $\sigma$. We say $\sigma$ has* **full moduli dimension** *if* **mod-dim**$(\sigma) = \dim \mathcal{M}_g$*. Obviously, the moduli dimension of $\sigma$ depends only on the braid orbit of $\sigma$, hence we call it* **the moduli dimension of the braid orbit**.

A curve is called a **general curve of genus** $g$ if it corresponds to a point of $\mathcal{M}_g$ that does not lie in any proper closed subvariety of $\mathcal{M}_g$ defined over $\bar{\mathbb{Q}}$ (the algebraic closure of the rationals). Clearly, an admissible tuple $\sigma$ has full moduli dimension if and only if each general curve of genus $g_\sigma$ admits a cover to $\mathbb{P}^1$ of type $\sigma$.

The following Remark gives the necessary condition for full moduli dimension used by Guralnick, Fried and Zariski (cf. [MV], Remark 2.2).

**Remark 2.2.** *Let $\sigma$ be an admissible tuple of length $r$ in $S_n$, and $g := g_\sigma \geq 2$. If $\sigma$ has full moduli dimension then $r \geq 3g$.*

2.2. **Group-theoretic consequences of the necessary criterion for full moduli dimension.** Let $\sigma = (\sigma_1, ..., \sigma_r)$ be an admissible tuple in $S_n$, and $g := g_\sigma \geq 3$. Assume $\sigma$ satisfies the necessary condition $r \geq 3g$ for full moduli dimension. Assume further $\sigma$ generates a primitive subgroup $G$ of $S_n$. If $g \geq 4$ then $G = S_n$ or $G = A_n$ by [GM] and [GS]. If $g = 3$ and $G$ is not $S_n$ or $A_n$ then one of the following holds (see [GM], Theorem 2):

(1) $n = 7$, $G \cong GL_3(2)$
(2) $n = 8$, $G \cong AGL_3(2)$ (the affine group)
(3) $n = 16$, $G \cong AGL_4(2)$

The affine group $AGL_m(2)$ is the semi-direct product of $GL_m(2)$ with the group of translations. We view it as permutation group on the $2^m$ points of the affine space $(\mathbb{F}_2)^m$, on which it acts triply transitively. A **transvection** of $AGL_m(2)$ is an involution that fixes a hyperplane of the corresponding affine space pointwise.

In cases (1) and (3), the tuple $\sigma$ consists of 9 transvections of the respective linear or affine group. In case (2), either $\sigma$ consists of 10 transvections or it consists of 8 transvections plus an element of order 2,3 or 4 (where the element of order 2 is a translation).

2.3. **Braid orbits of full moduli dimension.**

2.3.1. *Braid orbits of 2-cycle tuples and 3-cycle tuples.* Admissible tuples in $S_n$ of fixed length that consist only of transpositions form a single braid orbit (by Clebsch 1872, see [V], Lemma 10.15). They correspond to the so-called **simple covers**. Their braid orbit has full moduli dimension if and only if $2(n-1) \geq g$, where $g = g_\sigma$ (see the remarks in the Introduction).

Now consider admissible tuples in $S_n$, $n \geq 6$, of fixed length that consist only of 3-cycles. Such tuples generate $A_n$. Fried [Fr1] proved that such tuples exist and form exactly two braid orbits (resp., one braid orbit) if $g > 0$ (resp., $g = 0$). In the case $g > 0$, both braid orbits have full moduli dimension by [MV, Theorem 4.1].

It is to be expected that there is a wealth of braid orbits of full moduli dimension whose tuples generate $S_n$ or $A_n$. A classification seems hopeless.

2.3.2. *Braid orbits of the exceptional tuples in genus 3.* It was proved in [MV, Remark 5.1] that the tuples in case (1) (i.e. 9 double transpositions in $S_7$ generating a group isomorphic to $GL_3(2)$) form a single braid orbit. This braid orbit has full moduli dimension by [MV, Theorem 5.2].

## 3. Covers of pinched surfaces

3.1. **Pinched surfaces.** A pinched surface $R$ is a topological space which is obtained from a disjoint union of compact Riemann surfaces $R_1, \ldots, R_s$ by identifying finitely many pairs of points $(q_\mu, q'_\mu)$ (i.e., we identify $q_\mu$ with $q'_\mu$ for each $\mu$). These pairs are mutually disjoint. The common image of $q_\mu$ and $q'_\mu$ in $R$ is denoted by $p_\mu$. We denote the image of $R_\nu$ in $R$ by $\bar{R}_\nu$. Each $p_\mu$ is contained in at most two $\bar{R}_\nu$. It is allowed that $\bar{R}_\nu$ is linked to itself. The $\bar{R}_\nu$ are called the irreducible components of $R$, and the $p_\mu$ are called the nodes. A node is called to be a node of the **first**, (resp. of the **second**) **kind**, if it lies on exactly one (resp. two) irreducible components of $R$. A pinched surface is called non-singular if it has no nodes.

3.2. **Replacing a node by a tube.** Let $R$ be a pinched surface and $p$ a node of $R$. Then $p$ has a neighborhood $U$ that is homeomorphic to the union of two discs $D_1$ and $D_2$ that are linked at their midpoints. Let $\tilde{R}$ be the pinched surface obtained by replacing $U$ by a cylinder $\mathcal{T}$ whose two boundary circles coincide with the boundary circles of $D_1$ and $D_2$. Obviously, the homeomorphism type of $\tilde{R}$ depends only on $R$ and $p$. We say $\tilde{R}$ is obtained by replacing the node $p$ by a tube. There is a natural continuous map $\pi : \tilde{R} \to R$ mapping $\pi^{-1}(R \setminus \{p\})$ homeomorphically onto $R \setminus \{p\}$. Furthermore, $\pi^{-1}(p)$ is a circle which we call the **waist-line** of $\mathcal{T}$.

3.3. **The genus of a pinched surface.** We return to the set-up of section 3.1. The **genus** $g_\nu$ of the irreducible component $\bar{R}_\nu$ is the genus of the compact Riemann surface $R_\nu$. The **arithmetic genus** $g$ of a connected pinched surface is the genus of the non-singular surface obtained by replacing the nodes by tubes. This genus can be computed from the $g_\nu$ by the following formula. Let $t$ be the number of nodes. Then

$$g \;=\; t \;+\; 1 \;+\; \sum_{\nu=1}^{s} (g_\nu - 1) \tag{1}$$

3.4. **Stable pinched surfaces.** An irreducible component of a pinched surface is called **exceptional**, if it has genus 0, is linked to at most two other irreducible components and has no node of the first kind.

A connected pinched surface $R$ of genus $g \geq 2$ is called **stable** if it has no exceptional component. Such a surface of genus $g = 1$ is called stable, if it has no exceptional component and at least one node.

The **stable model** of a pinched surface $R$ of genus $\geq 2$ is obtained by repeating the following procedure until we obtain a stable pinched surface: Take an exceptional irreducible component and replace one of its nodes by a tube. The stable model has the same genus.

3.5. **Covers of pinched surfaces.** Let $S$ be a connected pinched surface and $\hat{S}$ the non-singular surface obtained from $S$ by replacing all nodes by tubes. Let $\hat{f} : \hat{R} \to \hat{S}$ be a cover of non-singular surfaces such that no branch point of $\hat{f}$ maps to a node of $S$. Let $\mathcal{T}$ be a cylinder on $\hat{S}$ coming from a node of $S$. By our assumption on $\hat{f}$, we may assume that $\mathcal{T}$ contains no branch point of $\hat{f}$. The inverse image of $\mathcal{T}$ in $\hat{R}$ is the disjoint union of cylinders $\mathcal{T}_i$ (because a cylinder is homotopic to a circle). The waist-line $\mathcal{W}$ of $\mathcal{T}$ is homotopic to $\mathcal{T}$, hence each $\mathcal{T}_i$ contains exactly one component $\mathcal{W}_i$ of the inverse image of $\mathcal{W}$. This $\mathcal{W}_i$ is a circle. Shrinking each $\mathcal{W}_i$ to a point results in a pinched surface $R$. The cover $\hat{f} : \hat{R} \to \hat{S}$ induces a map $f : R \to S$. Each map $R \to S$ obtained in this way is called a cover of pinched surfaces. There is also a direct definition, see [BeRo, Def. 4.4].

Let $\tilde{S}$ be the pinched surface obtained by replacing a single node $p$ of $S$ by a tube. Let $\tilde{R} \to \tilde{S}$ be the cover obtained from $\hat{R} \to \hat{S}$ as in the previous paragraph. In this situation we say that the cover $\tilde{R} \to \tilde{S}$ is obtained from $R \to S$ by **replacing the node $p$ by a tube**.

3.6. **Multi-lists.** Let $k$ be a non-negative integer. A multi-list $P$ of level $k$ is defined as follows: If $k = 0$, then $P$ is a positive integer. If $k > 0$, then $P = (P_1, \ldots, P_t)$, where $P_i$ is a multi-list of level $< k$ and one of the $P_i$ has level $k - 1$.

The integer tuple associated to $P$ is defined as follows: If $k = 0$, then it is the tuple $(P)$. If $k > 0$ and $P = (P_1, \dots, P_t)$ then the integer tuple associated with $P$ is the concatenation of the integer tuples associated with the $P_i$. We demand that the integer tuple associated to $P$ is a tuple of consecutive integers.

A multi-list of level 0 is called stable. A multi-list $P = (P_1, \dots, P_t)$ of level $k > 0$ is called **stable**, if $t \geq 2$ and the $P_i$ are stable for $i = 1, \dots, t$.

3.7. **The cover associated to a multi-list and a tuple of permutations.** Let $\sigma = (\sigma_1, \dots, \sigma_r)$ be a tuple of permutations in $S_n$.

Let $P = (P_1, \dots, P_t)$ be a stable multi-list of level $k \geq 1$ with associated integer tuple $(m, m+1, \dots, m')$, where $1 \leq m < m' \leq r$. We define an associated cover of pinched surfaces $R \to S$, where $S$ has genus 0 and carries a distinguished point $s_0$ which is not a node. This point $s_0$ is ramified if and only if $\tau \neq 1$, where $\tau = (\sigma_m \cdots \sigma_{m'})^{-1}$.

Let $P_{i_1}, \dots, P_{i_s}$ be the entries of $P$ of level $\geq 1$. For $j = i_1, \dots, i_s$ let $R^{(j)} \to S^{(j)}$ be the covering associated with the multi-list $P_j$ of level $\leq k-1$ (defined by induction).

Let $S^{(0)}$ be an additional sphere and choose $t+1$ distinct points $p_1, \dots, p_{t+1}$ on $S^{(0)}$. The last of these points is the distinguished point $s_0 = p_{t+1}$. For $i = 1, \dots, t$ define $\tau_i = \sigma_k \cdots \sigma_{k'}$, where $(k, k+1, \dots, k')$ is the integer tuple associated with $P_i$.

Let $R^{(0)}$ be a cover of $S^{(0)}$ of type $(\tau_1, \dots, \tau_t, \tau)$ (see [V]), that restricts to an unramified cover of $S^{(0)} \setminus \{p_1, \dots, p_t, p_{t+1}\}$.

Define the cover $R \to S$ as follows:

(1) The space $S$ is obtained from the disjoint union of the $S^{(j)}$ (for $j = 0, i_1, \dots, i_s$) by identifying the distinguished point of each $S^{(j)}$ with $p_j \in S^{(0)}$.
(2) The space $R$ is obtained from the disjoint union of the $R^{(j)}$ (for $j = 0, i_1, \dots, i_s$) by linking $R^{(0)}$ to each $R^{(j)}$, $j = i_1, \dots, i_s$, in the following way: The points over $p_j$, on $R^{(0)}$ as well as $R^{(j)}$, correspond to the orbits of $\tau_j$ on $\{1, \dots, n\}$. We identify the points corresponding to the same orbit.

If $P$ has associated integer tuple $(1, \dots, r)$, then the associated cover $R \to S$ arises from a cover $\hat{R} \to \hat{S}$ of type $\sigma$ (of non-singular surfaces) as in section 3.2.

**Lemma 3.1.** *If $\sigma$ generates a transitive subgroup of $S_n$, then $R$ is connected.*

*Proof.* By induction the connected components of $R^{(i)}$ are the orbits of the group $H_i$, generated by $\sigma_k, \dots, \sigma_{k'}$, where $(k, k+1, \dots, k')$ is the integer tuple associated with $P_i$. The points over $p_i$ correspond to the orbits of $\tau$. Those of these points which lie in the same $H_i$-orbit belong to the same connected component. As $H_i$ is generated by $\sigma_k, \dots, \sigma_{k'}$, this shows that the connected components correspond to the orbits of the group generated by all of the $\sigma_i$. When this subgroup acts transitive, then $R$ is connected. ∎

**Remark 3.2.** *We have written a program in* [GAP4] *which computes the combinatorial structure of the covering surface $R$ and its stable model $R'$. The input of the program is the tuple $\sigma$ and the multi-list $P$. The output yields the following information for $R$ as well as $R'$: The genera of the irreducible components, and the links given by nodes of the first and second kind. For the convenience of the reader,*

*we reproduce the GAP code in the appendix of this paper. For computing the genera of the components of $R$ and $R'$, we proceed as indicated in the following remark.*

**Remark 3.3.** *(Genus of the connected surface $R$)*

Assume $\sigma$ generates a transitive subgroup of $S_n$. Then the genus of the connected pinched surface $R$ can be computed by the formula (1) once the genera of the irreducible components of $R$ and the incidence relations are known. The incidence relations can be read off from the algorithm constructing the cover $R \to S$ in section 3.7. The genera can be computed step by step from the following procedure which computes the genera of the components of $R^{(0)}$.

Let $H$ be the subgroup of $S_n$ generated by $\tau_1, \ldots, \tau_t, \tau$. The components of $R^{(0)}$ correspond to the $H$-orbits on $\{1, \ldots, n\}$. Consider the component $\Omega$ corresponding to the $H$ orbit $\mathcal{O}$. Let $\nu_1, \ldots, \nu_{t+1}$ be the restrictions of the generators of $H$ to $\mathcal{O}$. By the Riemann-Hurwitz formula, the genus $g_\Omega$ of $\Omega$ is given by

$$2(|\mathcal{O}| + g_\Omega - 1) \quad = \quad \sum_{i=1}^{t+1} \mathrm{Ind}(\nu_i)$$

where the index $\mathrm{Ind}(\nu_i)$ is $|\mathcal{O}|$ minus the number of orbits of this permutation.

3.8. **An example in genus 3: the group $AGL_4(2)$.**

3.8.1. *The tuple $\sigma$.* Consider the following tuple $\sigma = (\sigma_1, \ldots, \sigma_9)$ in $S_{16}$, where

$$\begin{aligned}
\sigma_1 &:= (2,6)(3,7)(10,14)(11,15)\\
\sigma_2 &:= (2,6)(3,7)(10,14)(11,15)\\
\sigma_3 &:= (2,7)(3,6)(9,16)(12,13)\\
\sigma_4 &:= (1,3)(6,8)(10,12)(13,15)\\
\sigma_5 &:= (2,7)(4,5)(10,15)(12,13)\\
\sigma_6 &:= (2,16)(4,14)(6,12)(8,10)\\
\sigma_7 &:= (1,13)(3,15)(6,10)(8,12)\\
\sigma_8 &:= (1,10)(2,9)(5,14)(6,13)\\
\sigma_9 &:= (1,15)(2,16)(3,13)(4,14)
\end{aligned}$$

We have $\sigma_1 \cdots \sigma_9 = 1$ and $\sigma$ generates the group $G = AGL_4(\mathbb{F}_2)$ in its natural action on $\mathbb{F}_2^4$, i.e. on 16 points. By the Riemann-Hurwitz formula we have $g_\sigma = 3$ (cf. section 2.1 and section 2.2).

3.8.2. *The multi-lists $P_i$.* Consider the multi list

$$P \quad = \quad (((1,2),3),((4,5),6),((7,8),9))$$

The following sequence of multi-lists removes the singularities step by step

$$\begin{aligned}
P_0 &:= (((1,2),3),((4,5),6),((7,8),9))\\
P_1 &:= ((1,2,3),((4,5),6),((7,8),9))\\
P_2 &:= ((1,2,3),(4,5,6),((7,8),9))\\
P_3 &:= ((1,2,3),(4,5,6),(7,8,9))\\
P_4 &:= (1,2,3,(4,5,6),(7,8,9))\\
P_5 &:= (1,2,3,4,5,6,(7,8,9))\\
P_6 &:= (1,2,3,4,5,6,7,8,9)
\end{aligned}$$

3.8.3. *The associated covers.* The construction of section 3.7 associates a sequence of covers of pinched surfaces $R_i \to S_i, \quad i = 1, \ldots, 6$. The surface $S_i$ is a tree of $7 - i$ projective lines (i.e., spheres). $S_{i+1}$ arises from $S_i$ by replacing a node by a tube (two spheres of $S_i$ are joined by a tube and thereby merge into one sphere). This implies the corresponding relation between the covering surfaces.

**Remark 3.4.** *The cover $R_{i+1} \to S_{i+1}$ arises from the cover $R_i \to S_i$ by the process of "replacing a node by a tube" (see section 3.5).*

For $i = 0, \ldots, 6$ let $R_i'$ be the stable model of $R_i$. All $R_i$ and $R_i'$ have (arithmetic) genus 3 (see section 3.3 and 3.4).

$R_0'$ : one component of genus 0 with 3 nodes of the second kind linking it to 3 other components (which are mutually disjoint); each of the latter has genus 0 and carries a node of the first kind.
$R_1'$ : one component of genus 0 with 3 nodes of the second kind linking it to 3 other components (which are mutually disjoint); two of the latter have genus 0 and carry a node of the first kind; the third has genus 1.
$R_2'$ : one component of genus 0 with 3 nodes of the second kind linking it to 3 other components (which are mutually disjoint); one of the latter has genus 0 and carries a node of the first kind; the two others have genus 1.
$R_3'$ : three disjoint components of genus 1 linked by three nodes to a component of genus 0
$R_4'$ : three components of genus 1 linked by two nodes
$R_5'$ : two components of genus 1, resp. 2, linked by a node
$R_6'$ : one nonsingular component of genus 3

This information was computed by the program reproduced in the appendix (cf. Remark 3.2). The combinatorial structure of the non-stable covering surfaces $R_i$ is much more complicated. From this it becomes apparent that it would have been extremely tedious to do this computation by hand (although the final result, i.e., the structure of the $R_i'$, is reasonably simple).

We describe the case $i = 0$. The surface $R_0$ has 58 components of genus 0, the maximal number of nodes on a component is 10. (Note that for any $i$, the surface $R_i$ has only nodes of the second kind. This is clear from the construction.)

## 4. The moduli-space of stable curves of genus $g$

The moduli space $\overline{\mathcal{M}_g}$ classifies stable curves over $\mathbb{C}$ of genus g. It is a projective variety over $\mathbb{C}$. We consider the set of complex points.

### 4.1. **Covers of pinched surfaces and of algebraic curves.**

**Lemma 4.1.** *Let $R \to S$ be a cover of pinched surfaces. Let $e$ be a node of $S$. We replace $e$ by a tube and also all nodes of $R$ which lie over $e$ (as in section 3.2). This gives a covering $R' \to S'$ of pinched surfaces of the same genera. Assume $\mathfrak{R} \to \mathfrak{S}$ is a cover of algebraic curves over $\mathbb{C}$ of topological type $R \to S$. Then there are covers $\mathfrak{R}_t \to \mathfrak{S}_t, t \in [0,1]$ of algebraic curves $/\mathbb{C}$ such that $\mathfrak{R}_t \to \mathfrak{S}_t$ is of topological type $R' \to S'$ for $t \neq 0, |t| < 1$ and the following holds: Let $p_t$ be the point of $\overline{\mathcal{M}_g}$ that corresponds to the stable model of $\mathfrak{R}_t$. Then $p_0 = \lim_{t \to 0} p_t$ in the complex topology.*

Proof: Because of [Man, III.2.7(a),(b), 2.8 (d)], we get a family $\mathfrak{S}_t, t \in [0,1]$, such that $\mathfrak{S}_t$ is of type $S$ for $t = 0$ and type $S'$ for $t > 0$. Because of the specialisation theorem for the Kummerian fundamental group [BeRo, Proposition 7.14] or [AsMaOd], the covering $\mathfrak{R} \to \mathfrak{S}$ deforms into a unique family $\mathfrak{R}_t \to \mathfrak{S}_t, t \in [0,1]$. Then $\mathfrak{R}_t$ is of type $R'$ for $t > 0$.

4.2. **The stratification of $\overline{\mathcal{M}_g}$ by pinched surfaces.** There is a stratification of $\overline{\mathcal{M}_g}$ by the topological type. Let $R$ be a pinched surface of genus $g$. The stable curves of genus $g$ whose associated pinched surface is homeomorphic to $R$ correspond to the points of a locally closed subset $\overline{\mathcal{M}_g}(R)$ of $\overline{\mathcal{M}_g}$ (see [Man, III.2.8(d)]; that reference uses "modular graphs" [Man, III Definition 2.4] instead of pinched surfaces to describe the topological type of a stable curve).

Let $R$ be a pinched surface of genus $g$. For any component $c$ of $R$ we define $v(c)$ as the number of nodes on $c$, with self-intersections counted twice. Then there is a finite morphism

$$\prod_c \mathcal{M}_{g(c),v(c)} \to \overline{\mathcal{M}_g}(R)$$

(see [Man, III.2.8]). This shows that $\overline{\mathcal{M}_g}(R)$ is irreducible and its dimension is given by

$$\dim\overline{\mathcal{M}_g}(R) \quad = \quad \sum_c \left(3g(c) - 3 + v(c)\right)$$

Here we have used $\dim\mathcal{M}_{g,r} = 3g - 3 + r$.

For the genus $g$ we have the formula (1)

$$g \quad = \quad 1 \; + \; \sum_c \left(g(c) - 1\right) \; + \; 1/2 \sum_c v(c)$$

For $g \geq 2$ this implies

$$\dim\mathcal{M}_g = 3g - 3 = \sum_c (3g(c) - 3 + 3/2 v(c))$$

**Corollary 4.2.**

$$codim\overline{\mathcal{M}_g}(R) = 1/2 \sum_v c(v) = \textit{number of nodes of } R.$$

**Lemma 4.3.** [Man, III.2.7(a),(b), 2.8 (d)] *Let $R$ and $T$ be two pinched surfaces. Then $\overline{\mathcal{M}_g}(R)$ is contained in the boundary of $\overline{\mathcal{M}_g}(T)$ if $T$ can be obtained from $R$ by replacing some nodes of $R$ by tubes.*

4.3. **Full moduli dimension for $AGL_4(2)$.** Let $\sigma = (\sigma_1, \ldots, \sigma_9)$, $P$, $R_i$ and $R_i'$ as in section 3.8. Let $\mathcal{M}^{(i)} := \overline{\mathcal{M}_3}(R_i')$, the locally closed, irreducible subset of $\overline{\mathcal{M}_3}$ classifying stable curves of topological type $R_i'$. By Corollary 4.2 we have dim $\mathcal{M}^{(i)} = i$, $i = 0, \ldots, 6$.

By inspection we see that $R_{i+1}'$ arises from $R_i'$ by replacing a node by a tube. Therefore, $\mathcal{M}^{(i)}$ is contained in the boundary of $\mathcal{M}^{(i+1)}$ by Lemma 4.3.

Let $\Omega$ be the image in $\mathcal{M}_3$ of the Hurwitz space $\mathcal{H}_\sigma$ (see section 2.1). Let $\bar{\Omega}$ be the Zariski-closure of $\Omega$ in $\overline{\mathcal{M}_3}$. We want to show $\bar{\Omega} = \overline{\mathcal{M}_3}$.

**Lemma 4.4.** *Assume $\mathfrak{R} \to \mathfrak{S}$ is a cover of algebraic curves over $\mathbb{C}$ of topological type $R_i \to S_i$ for some $i = 0, \ldots, 6$. Then the stable model of $\mathfrak{R}$ corresponds to a point of $\bar{\Omega}$.*

**Proof.** For $i = 6$ this follows directly from the definition of $\Omega$. Now assume $i = 5$. By Remark 3.4 and Lemma 4.1, there are covers $\mathfrak{R}_t \to \mathfrak{S}_t, t \in [0,1]$ of algebraic curves $/\mathbb{C}$ such that the following holds: $\mathfrak{R}_t \to \mathfrak{S}_t$ is of topological type $R_6 \to S_6$ for $t \neq 0, |t| < 1$ and equals the given cover $\mathfrak{R} \to \mathfrak{S}$ for $t = 0$. Furthermore, if $p_t$ denotes the point of $\overline{\mathcal{M}_3}$ that corresponds to the stable model of $\mathfrak{R}_t$, then $p_0 = \lim_{t\to 0} p_t$ in the complex topology. This proves the claim for $i = 5$. By iterating this argument we conclude the proof.

**Theorem 4.5.** *Each general curve of genus 3 has a cover to $\mathbb{P}^1$ with monodromy group $AGL_4(2)$. More precisely, the tuple $\sigma$ from section 3.8.1 (of nine transvections in $AGL_4(2)$) has full moduli dimension.*

*Proof.* It suffices to show that $\bar{\Omega} = \overline{\mathcal{M}_3}$ (cf. section 2.1). Recall that $\dim \mathcal{M}^{(i)} = i$. By Riemann's Existence Theorem, there is a cover of algebraic curves over $\mathbb{C}$ of topological type $R_0 \to S_0$. It follows by Lemma 4.4 that $\mathcal{M}^{(0)} \subset \bar{\Omega}$. By Lemma 4.1 and because $\dim \mathcal{M}^{(1)} = 1$ it follows that there is a Zariski-dense subset $\mathcal{D}$ of points of $\mathcal{M}^{(1)}$ which correspond to the stable model of an algebraic curve $/\mathbb{C}$ covering another algebraic curve of type $R_1 \to S_1$. By Lemma 4.4 we conclude that $\mathcal{M}^{(1)} \cap \bar{\Omega}$ is Zariski-dense in $\mathcal{M}^{(1)}$. It follows that $\mathcal{M}^{(1)} \subset \bar{\Omega}$.

Assume $\mathcal{M}^{(2)}$ is not contained in $\bar{\Omega}$. Then the maximal dimension $d$ of a component of $\mathcal{L} := \mathcal{M}^{(2)} \cap \bar{\Omega}$ satisfies $d < \dim \mathcal{M}^{(2)} = 2$. Since $\mathcal{L}$ is a locally closed subset of $\overline{\mathcal{M}_3}$, each component of the complement of $\mathcal{L}$ in its closure has dimension strictly less than $d$. Thus the closure of $\mathcal{L}$ would intersect $\mathcal{M}^{(1)}$ in a Zariski-closed proper subset. However, it follows from Lemma 4.1 and Lemma 4.4 that every point of $\mathcal{D}$ lies in the closure of $\mathcal{L}$. This contradiction shows that $\mathcal{M}^{(2)} \subset \bar{\Omega}$.

Continuing like this it finally follows that $\mathcal{M}^{(6)} \subset \bar{\Omega}$. However, $\mathcal{M}^{(6)} = \mathcal{M}_3$, and we are done.

∎

## APPENDIX: Computing the combinatorial structure of a (pinched) covering surface given by a tuple of permutations and a multi-list

### Appendix A. Auxiliary subroutines

The first of the following subroutines computes the index of a permutation (i.e., the permutation degree minus the number of cycles). The second subroutine computes the genus of any cover of $\mathbb{P}^1$ of type $t$ (cf. section 2.1), where $t$ generates a transitive permutation group of degree $n$.

```
PermIndex:=function(p,deg)
  return deg - Length(Orbits(Group(p),[1..deg]));
end;


OrbitGenus:=function(t,n)
  if not IsTransitive(Group(t),[1..n]) then Print("Group intransitive");
  return;
    fi;
  return 1-n+ Sum(List([1..Length(t)],
    i->PermIndex(t[i],n)))/2 ;
```

```
end;
```

## Appendix B. The combinatorial structure of certain pinched surfaces arising as coverings

Here we transform the recursive construction of the covering $R \to S$ from section 3.7 into a GAP program (cf. Remark 3.2). Let $T$ be an $r$-tuple of permutations of degree $n$.

If $P$ is a multi-list with associated integer tuple $1, \ldots, r$, the command `IncidMatrix`$(n, T, P)$ produces the following output: A pair whose first entry is the genus of $R$, where $R \to S$ is the covering constructed from $T$ and $P$ in section 3.7. The second entry is a list $I$ of records, with each record corresponding to a component $C$ of $R$. The attributes of the record yield the genus of $C$, and the positions in $I$ of the components linked with $C$.

The main construction occurs in the subroutine `RecursiveIncidMatrix`, which performs the recursive construction from section 3.7. Most users will not need to call the routine
`RecursiveIncidMatrix`, because it is called automatically by `IncidMatrix`. For completeness, we remark that in `RecursiveIncidMatrix`, the multi-list $P$ is more generally allowed to have integer tuple $(m, m+1, \ldots, m')$, where $1 \leq m < m' \leq r$.

```
RecursiveIncidMatrix:=function(n,T,P)
  local dist, G, g, B, record, Perm, Perm1, perm, Orbs, Inc, I, Comp,
  Laengen, ii, i, j, k, l, m, aux, NewOrb, R, s;
  Perm:=[]; Orbs:=[]; Comp:=[]; Laengen:=[];
  if not IsList(P) then return [ T[P], [], [] ];
    fi;
  s:=Length(P);
  for i in [1..s] do
    R:=RecursiveIncidMatrix(n,T,P[i]);
    Add(Perm,R[1]);
    Add(Orbs,R[2]);
    Append(Comp, R[3]); Add(Laengen,Length(R[3]));
    od;
  perm:=Product(Perm);
  Add(Perm, perm^-1);
  G:=Group(Perm);
  NewOrb:= Orbits(G,[1..n]);
  Construction of Comp = list of records, one for each component of the curve
  It has attributes genus and I=list of back distances to incident entries of Comp
  m:=Length(NewOrb);
  for j in [1..m] do
    B:=NewOrb[j];
    g:=1-Length(B)+
      Sum(List([1..s+1],
      i->PermIndex(GeneratorsOfGroup(Action(G,B))[i],Length(B))))/2;
    record:=rec(genus:=g, Inc:= []);
    for i in [1..s] do
```

```
      dist:=0;
      for ii in [i+1..s] do
        dist:=dist+ Laengen[ii];
        od;
      l:=Length(Orbs[i]);
      for k in [1..l] do
        I:=Intersection(NewOrb[j],Orbs[i][k]);
        for aux in Orbits(Group(Perm[i]),I) do
          Add(record.Inc,j+dist+l-k);
          od;
        od;
      od;
    Add(Comp,record);
    od;
  return [perm, NewOrb, Comp];
end;

------------------------------------------------------------------------
IncidMatrix:=function(n,T,P)
  local k, I, II, j, s, r;
  I:=RecursiveIncidMatrix(n,T,P)[3];
  s:=Length(I);
  for j in [1..s] do
    II:= I[j].Inc;
    r:=Length(II);
    for k in [1..r] do
      II[k]:= j-II[k];
      Add(I[II[k]].Inc,j);
   Incidence relation is made symmetric and absolute (i.e., no relative pointers)
      od;
    od;
  return [ OrbitGenus(T,n), I];
end;
```

## Appendix C. Computing the stable model of the covering surface

The routine `StabMatrix` has the same input as `IncidMatrix`. It computes the same information with $R$ replaced by its stable model $R'$.

```
StabMatrix:=function(n,T,P)
  local g, f, flag, k, I, J, II, j, s, m;
  II:= IncidMatrix(n,T,P);
  I:= II[2];
  s:=Length(I);
  flag:=1;
   now we make the corresponding curve stable if its arithmetic genus is > 1
  if II[1]<2 then Print("Curve has genus <2, cannot be made stable");
    fi;
```

```
  while flag=1 do
    flag:=0;
    for j in [1..s] do
      if I[j].genus=0 and Length(I[j].Inc)=1 then
        k:=I[j].Inc[1];
        I[k].Inc:= Filtered(I[k].Inc, x-> not x=j);
        I[j].Inc:=[]; flag:=1;
        fi;
      if I[j].genus=0 and Length(I[j].Inc)=2 then
        k:=I[j].Inc[1];
        m:=I[j].Inc[2];
        I[k].Inc:= Filtered(I[k].Inc, x-> not x=j);
        I[m].Inc:= Filtered(I[m].Inc, x-> not x=j);
        Add(I[k].Inc,m);
        Add(I[m].Inc,k);
        I[j].Inc:=[]; flag:=1;
        fi;
      od;
    od;
   now we delete those components with no incidences left
   and re-label the other components and incidence lists
  J:=[];
  f:=[];
  for j in [1..s] do
    if (not I[j].Inc= []) or I[j].genus>0 then
      Add(J,I[j]);
      f[j]:= Length(J);
      fi;
    od;
  m:=Length(J);
  for k in [1..m] do
    J[k].Inc:= List(J[k].Inc, x-> f[x] );
    od;
   now we compute the arithmetic genus of the stable curve
   as a consistency check (It has to equal II[1]).
   We use the formula in Harris-Morrison, p. 48.
  g:= Sum(List(J, x-> -1 + x.genus + Length(x.Inc)/2)) + 1;
  if g= II[1] then Print(" Arithmetic genus is correct");
    else Print(" Mistake:  Arithmetic genus is wrong");
    fi;
  return [ II[1], J];
end;
```

## References

[AsMaOd] M. Asada, M. Matsumoto, T. Oda: *Local monodromy on the fundamental groups of algebraic curves along a degenerate stable curve*, J. Pure and Applied Algebra **103** (1995), 235 – 283

[BeRo] J. Bertin, M. Romagny: Champs de Hurwitz, preprint
[Fr1] M. Fried, Alternating groups and lifting invariants, Preprint as of 07/01/96.
[Fr2] M. Fried, Combinatorial computations of moduli dimension of Nielsen classes of covers, Contemp. Math. **89** (1989), 61–79.
[FrGu] M. Fried and R. Guralnick, On uniformization of generic curves of genus $g < 6$ by radicals, unpublished manuscript.
[FrV] M. Fried and H. Völklein, The inverse Galois problem and rational points on moduli spaces, *Math. Annalen* **290** (1991), 771-800.
[GAP4] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.2; 2000. `(http://www.gap-system.org)`
[GM] R. Guralnick and K. Magaard, On the minimal degree of a primitive permutation group, J. Algebra 207 (1998), 127–145.
[GS] R. Guralnick and J. Shareshian, Alternating and Symmetric Groups as Monodromy Groups of Curves I, preprint.
[MV] K. Magaard and H. Völklein, The monodromy group of a function on a general curve, Israel J. Math. 141 (2004), 355–368.
[MSV] K. Magaard, S. Sphectorov and H. Völklein, A GAP package for braid orbit computation, and applications, Experimental Math. 12 (2003), 385– 393.
[Man] Y. Manin: *Frobenius manifolds, quantum cohomology, and moduli spaces* (1999), Colloquium Publications AMS.
[V] H. Völklein, Groups as Galois Groups – an Introduction, Cambr. Studies in Adv. Math. 53, Cambridge Univ. Press 1996.
[Za] O. Zariski, Collected papers vol. III, p. 43–49, MIT Press 1978.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 159–169
ISSN 1930-1235: (2008)

# CLIFFORD-WEIL GROUPS OF QUOTIENT REPRESENTATIONS.

Annika Günther

*Lehrstuhl D für Mathematik,*
*RWTH Aachen University*
*52056 Aachen, Germany*
*annika.guenther@math.rwth-aachen.de*

Gabriele Nebe

*Lehrstuhl D für Mathematik,*
*RWTH Aachen University*
*52056 Aachen, Germany*
*nebe@math.rwth-aachen.de*

Eric M. Rains

*Department of Mathematics,*
*California Institute of Technology,*
*Pasadena, CA 91125, U.S.A.,*
*rains@caltech.edu*

Abstract. This note gives an explicit proof that the scalar subgroup of the Clifford-Weil group remains unchanged when passing to the quotient representation filling a gap in [3]. For other current and future errata to [3] see http://www.research.att.com/∼njas/doc/cliff2.html/.

## 1. Introduction

All notations in this paper are introduced in detail in [3] and we refer to this book for their definitions. One main goal of the book is to introduce a unified language to describe the Type of self-dual codes combining the different notions of self-duality and Types, that are well established in coding theory. The Type of a code is a finite representation $\rho = (V, \rho_M, \rho_\Phi, \beta)$ of a finite form ring $\mathcal{R} = (R, M, \psi, \Phi)$. The finite alphabet $V$ is a left module for the ring $R$ and the biadditive form $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ defines the notion of duality. A code $C$ of length $N$ is then an $R$-submodule of $V^N$ and the dual code is

$$C^\perp = \{v \in V^N \mid \sum_{i=1}^{N} \beta(v_i, c_i) = 0 \ \forall c \in C\}.$$

Additional properties of codes of a given Type are encoded in the $R$-qmodule $\rho_\Phi(\Phi)$ which is a certain subgroup of the group of quadratic mappings $V \to \mathbb{Q}/\mathbb{Z}$. A code $C \leq V^N$ is *isotropic*, if $C \leq C^\perp$ and

$$\sum_{i=1}^{N} \rho_\Phi(\phi)(c_i) = 0 \quad \text{for all } \phi \in \Phi \text{ and for all } c \in C.$$

Given a finite representation $\rho$, one associates a finite subgroup $\mathcal{C}(\rho)$ of $\mathrm{GL}(\mathbb{C}[V])$, called the associated Clifford-Weil group (see Section 2). For certain finite form rings (including direct products of matrix rings over finite Galois rings) it is shown in [3, Theorem 5.5.7] that the ring of polynomial invariants of $\mathcal{C}(\rho)$ is spanned by the complete weight-enumerators of self-dual isotropic codes of Type $\rho$. We conjecture that this theorem holds for arbitrary finite form rings. It is shown in [3, Theorem 5.4.13, 5.5.3] that in general the order of the scalar subgroup

$$\mathcal{S}(\mathcal{C}(\rho)) = \mathcal{C}(\rho) \cap \mathbb{C}^* \,\mathrm{id}_{\mathbb{C}[V]}$$

is exactly the greatest common divisor of the lengths of self-dual isotropic codes of Type $\rho$. The proof of this theorem uses the fact that the scalar subgroup of $\mathcal{C}(\rho)$ remains unchanged when passing to the quotient representation. The aim of the present note is to give a full proof of this statement, Theorem 1.

Throughout the note we fix an isotropic code $C \leq C^\perp \leq V$ in $\rho$. Then the quotient representation $\rho/C$ is defined by

$$\rho/C := (C^\perp/C, \rho_M/C, \rho_\Phi/C, \beta/C),$$

where $(\rho_M/C(m))(v+C, w+C) = \rho_M(m)(v,w)$, $(\rho_\Phi/C(\phi))(v+C) = \rho_\Phi(\phi)(v)$, and $\beta/C(v+C, w+C) = \beta(v,w)$ for all $v, w \in C^\perp, m \in M, \phi \in \Phi$.

**Theorem 1.** *Let $\mathcal{R} = (R, M, \psi, \Phi)$ be a finite form-ring and let $\rho = (V, \rho_M, \rho_\Phi, \beta)$ be a finite representation of $\mathcal{R}$. Let $C$ be an isotropic self-orthogonal code in $\rho$. Then*

$$\mathcal{S}(\mathcal{C}(\rho)) \cong \mathcal{S}(\mathcal{C}(\rho/C)).$$

## 2. Clifford-Weil groups and hyperbolic counitary groups

The Clifford-Weil group $\mathcal{C}(\rho)$ associated to the finite representation $\rho$ acts linearly on the space $\mathbb{C}[V]$ with basis $[b_v : v \in V]$. It is generated by

| | |
|---|---|
| $m_r : b_v \mapsto b_{rv}$ | for $r \in R^*$ |
| $d_\phi : b_v \mapsto \exp(2\pi i \rho_\Phi(\phi)(v)) b_v$ | for $\phi \in \Phi$ |
| $h_{e,u_e,v_e} : b_v \mapsto \frac{1}{\lvert eV\rvert^{1/2}} \sum_{w \in eV} \exp(2\pi i \beta(w, v_e v)) b_{w+(1-e)v}$ | $e^2 = e \in R$ symmetric. |

Recall that the form-ring structure defines an involution $^J$ on $R$. Then an idempotent $e \in R$ is called *symmetric*, if $eR$ and $e^J R$ are isomorphic as right $R$-modules, which means that there are $u_e \in eRe^J, v_e \in e^J Re$ such that $e = u_e v_e$ and $e^J = v_e u_e$.

The Clifford-Weil group $\mathcal{C}(\rho)$ is a projective representation of the hyperbolic counitary group

$$\mathcal{U}(R, \Phi) = U(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \mathrm{Mat}_2(R), \Phi_2).$$

The elements of $\mathcal{U}(R, \Phi)$ are of the form

$$X = \left( \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) \in \mathrm{Mat}_2(R) \times \Phi_2 \tag{1}$$

such that

$$\begin{pmatrix} \gamma^J\alpha & \gamma^J\beta \\ \delta^J\alpha - 1 & \delta^J\beta \end{pmatrix} = \psi_2^{-1}\begin{pmatrix} \lambda(\phi_1) & m \\ \tau(m) & \lambda(\phi_2) \end{pmatrix}.$$

A more detailed definition of $\mathcal{U}(R,\Phi)$ can be found in [3, Chapter 5.2].

It is shown in the book that $\mathcal{U}(R,\Phi)$ is generated by the elements

$$d((r,\phi)) = \left(\begin{pmatrix} r^{-J} & r^{-J}\psi^{-1}(\lambda(\phi)) \\ 0 & r \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & \phi \end{pmatrix}\right)$$

with $r \in R^*, \phi \in \Phi$ and

$$H_{e,u_e,v_e} = \left(\begin{pmatrix} 1-e^J & v_e \\ -\epsilon^{-1}u_e^J & 1-e \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon e) \\ & 0 \end{pmatrix}\right),$$

where $e = u_e v_e$ runs through the symmetric idempotents of $R$.

To formalize the proofs we let $\mathcal{F}(R,\Phi)$ denote the free group on

$$\{\tilde{d}(r,\phi), \tilde{H}_{e,u_e,v_e} \mid r \in R^*, \phi \in \Phi, e = u_e v_e \text{ symmetric idempotent in } R\}.$$

On these generators there are two group epimorphism:

$$\pi : \mathcal{F}(R,\Phi) \to \mathcal{U}(R,\Phi), \tilde{d}(r,\phi) \mapsto d((r,\phi)), \tilde{H}_{e,u_e,v_e} \mapsto H_{e,u_e,v_e}$$

and

$$p : \mathcal{F}(R,\Phi) \to \mathcal{C}(\rho); \quad \tilde{d}(r,\phi) \mapsto m_r d_\phi, \quad \tilde{H}_{e,u_e,v_e} \mapsto h_{e,u_e,v_e}. \tag{2}$$

**Theorem 2.** $p(\ker(\pi)) \subseteq \mathcal{S}(\mathcal{C}(\rho))$.
*If $\rho$ is faithful (i.e.* $\mathrm{Ann}_R(V) = 0 = \ker(\rho_\Phi)$*), then* $p(\ker(\pi)) = \mathcal{S}(\mathcal{C}(\rho))$.

This is essentially [3, Theorem 5.3.2]. However the calculations there were omitted so we take the opportunity to give them here for completeness (also since there are a few typos in the proof there). As in [3, Theorem 5.3.2] we define the associated Heisenberg group $\mathcal{E}(V) := V \times V \times \mathbb{Q}/\mathbb{Z}$ with multiplication

$$(z,x,q)\cdot(z',x',q') = (z+z', x+x', q+q'+\beta(x',z)).$$

Then $\mathcal{E}(V)$ acts linearly on $\mathbb{C}[V]$ by

$$(z,x,q)\cdot b_v = \exp(2\pi i(q+\beta(v,z)))b_{v+x}, \ \ (z,x,q) \in \mathcal{E}(V), \ v \in V.$$

This yields an absolutely irreducible faithful representation $\Delta : \mathcal{E}(V) \to GL_{|V|}(\mathbb{C})$.

**Lemma 3.** *The hyperbolic counitary group $\mathcal{U}(R,\Phi)$ acts as group automorphisms on $\mathcal{E}(V)$ via*

$$\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix}\right)(z,x,q)$$
$$= (\alpha z + \beta x, \gamma z + \delta x, q + \rho_\Phi(\phi_1)(z) + \rho_\Phi(\phi_2)(x) + \rho_M(m)(z,x)).$$

*If $\rho$ is a faithful representation, then this action is faithful.*

Also the associated Clifford-Weil group $\mathcal{C}(\rho) \leq \mathrm{GL}(\mathbb{C}[V])$ acts on $\Delta(\mathcal{E}(V)) \cong \mathcal{E}(V)$ by conjugation.

**Lemma 4.** *For $r \in R^*, \phi \in \Phi$ and $(z,x,q) \in \mathcal{E}(V)$ we have*

$$\Delta(d((r,\phi))(z,x,q)) = (m_r d_\phi)\Delta((z,x,q))(m_r d_\phi)^{-1}.$$

*Proof.* The proof is an easy calculation.

$$d((r,\phi))(z,x,q) = (r^{-J}z + r^{-J}\psi^{-1}(\lambda(\phi))x, rx, q + \rho_\Phi(\phi)(x))$$

maps the basis element $b_v$ ($v \in V$) to

$$\exp(2\pi i(q + \rho_\Phi(\phi)(x) + \beta(v, r^{-J}z + r^{-J}\psi^{-1}(\lambda(\phi))x)))b_{v+rx}.$$

On the other hand

$$\begin{aligned}
&(m_r d_\phi)\Delta((z,x,q))(m_r d_\phi)^{-1}(b_v) = \\
&= m_r d_\phi \exp(2\pi i(q - \rho_\Phi(\phi)(r^{-1}v) + \beta(r^{-1}v, z))(b_{r^{-1}v+x}) \\
&= \exp(2\pi i(q - \rho_\Phi(\phi)(r^{-1}v) + \beta(r^{-1}v, z) + \rho_\Phi(\phi)(r^{-1}v + x)))(b_{v+rx}) \\
&= \exp(2\pi i(q + \beta(r^{-1}v, z) + \rho_M(\lambda(\phi))(r^{-1}v, x)))(b_{v+rx})
\end{aligned}$$

which is the same as the above, since $\beta(r^{-1}v, z) = \beta(v, r^{-J}z)$ by definition of the involution $J$ and

$$\rho_M(\lambda(\phi))(r^{-1}v, x) = \beta(r^{-1}v, \psi^{-1}(\lambda(\phi))x) = \beta(v, r^{-J}\psi^{-1}(\lambda(\phi))x).$$

□

**Lemma 5.** *For $e = u_e v_e$ a symmetric idempotent in $R$ and $(z,x,q) \in \mathcal{E}(V)$*

$$\Delta(H_{e,u_e,v_e}(z,x,q)) = h_{e,u_e,v_e}\Delta((z,x,q))h^{-1}_{e,u_e,v_e}.$$

*Proof.* The group $\mathcal{E}(V)$ is generated by $(z,0,0), (0,x,0), (0,0,q)$ where $z \in e^J V \cup (1-e^J)V$, $x \in eV \cup (1-e)V$, $q \in \mathbb{Q}/\mathbb{Z}$ and it is enough to check the lemma for these 5 types of generators. For $(0,0,q)$ this is clear. Similarly, if $z \in (1-e^J)V$ and $x \in (1-e)V$, then both sides yield $\Delta((z,x,q))$ as one easily checks. For $z \in e^J V$, $x \in eV$, $q \in \mathbb{Q}/\mathbb{Z}$

$$H_{e,u_e,v_e}(z,x,q) = (v_e x, -\epsilon^{-1}u_e^J z, q + \beta(z, -\epsilon x)).$$

To calculate the right hand side, we note that according to the decomposition

$$V = eV \oplus (1-e)V$$

the space $\mathbb{C}[V] = \mathbb{C}[eV] \otimes \mathbb{C}[(1-e)V]$ is a tensor product and

$$h_{e,u_e,v_e} = (h_{e,u_e,v_e})_{\mathbb{C}[eV]} \otimes \mathrm{id}_{\mathbb{C}[(1-e)V]}.$$

Moreover, the permutation matrix $\Delta((0,x,0)) : b_v \mapsto b_{v+x}$ for $x \in eV$ is a tensor product $p_x \otimes \mathrm{id}$ and similarly the diagonal matrix $\Delta((z,0,0))$ for $z \in e^J V$ is a tensor product $d_z \otimes \mathrm{id}$. It is therefore enough to calculate the action on elements of $\mathbb{C}[eV]$. For $z = e^J z \in e^J V$, $x = ex \in eV$ and $v = ev \in eV$, we get

$$\begin{aligned}
&h_{e,u_e,v_e} \circ \Delta((e^J z, 0, 0)) \circ h^{-1}_{e,u_e,v_e} b_v = \\
&= h_{e,u_e,v_e}(|eV|^{-1/2} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1}v_e^J \epsilon v, w) + \beta(w, e^J z)))b_w) \\
&= |eV|^{-1} \sum_{w' \in eV} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1}v_e^J \epsilon v, w) + \beta(w, e^J z) + \beta(w', v_e w)))b_{w'}.
\end{aligned}$$

Now $\beta(-\epsilon^{-1}v_e^J \epsilon v, w) + \beta(w, e^J z) + \beta(w', v_e w) = \beta(-\epsilon^{-1}v_e^J \epsilon v + \epsilon^{-1}z + \epsilon^{-1}v_e^J \epsilon w', w)$. Hence the sum over all $w$ is non-zero, only if $-v_e^J \epsilon v + z + v_e^J \epsilon w' = 0$ which implies

that $w' = v - \epsilon^{-1}u_e^J z$. Hence $h_{e,u_e,v_e} \circ \Delta((e^J z, 0, 0)) \circ h^{-1}_{e,u_e,v_e} b_v = b_{v-\epsilon^{-1}u_e^J z}$. A similar calculation yields

$$\begin{aligned}
&h_{e,u_e,v_e} \circ \Delta((0, ex, 0)) \circ h^{-1}_{e,u_e,v_e} b_v = \\
&= h_{e,u_e,v_e}(|eV|^{-1/2} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1}v_e^J \epsilon v, w)))b_{w+ex}) \\
&= h_{e,u_e,v_e}(|eV|^{-1/2} \sum_{w \in eV} \exp(2\pi i(\beta(-\epsilon^{-1}v_e^J \epsilon v, w - ex)))b_w) \\
&= h_{e,u_e,v_e} \circ h^{-1}_{e,u_e,v_e}(\exp(2\pi i(\beta(\epsilon^{-1}v_e^J \epsilon v, ex)))b_v) \\
&= \exp(2\pi i(\beta(v, v_e x)))b_v.
\end{aligned}$$

□

*Proof.* (of Theorem 2) That $p(\ker(\pi)) \subseteq \mathcal{S}(\mathcal{C}(\rho))$ follows from Lemma 4 and 5. Assume now that $\rho$ is faithful. Then by Lemma 3 the action of $\mathcal{U}(R, \Phi)$ on $\mathcal{E}(V)$ is faithful: Let $s \in \mathcal{S}(\mathcal{C}(\rho))$. Then there is some $f \in \mathcal{F}(R, \Phi)$ with $p(f) = s$ since $p$ is surjective. Moreover the action of $\pi(f) \in \mathcal{U}(R, \Phi)$ and $p(f) \in \mathcal{C}(\rho)$ on $\mathcal{E}(V)$ coincide, so $\pi(f)$ acts trivially on $\mathcal{E}(V)$ and therefore $f \in \ker(\pi)$.

□

**Remark 6.** *Let $\rho$ be faithful. Lemma 4 and 5 show that every element $a \in \mathcal{C}(\rho)$ induces an automorphism $\alpha$ on $\mathcal{E}(V)$ that is in $\mathcal{U}(R, \Phi)$. The latter group acts faithfully on $\mathcal{E}(V)$ by Lemma 3 hence $\alpha \in \mathcal{U}(R, \Phi)$ is uniquely determined. This defines a group epimorphism*

$$\nu : \mathcal{C}(\rho) \to \mathcal{U}(R, \Phi),\ a \mapsto \alpha.$$

*The kernel of $\nu$ is precisely the scalar subgroup $\mathcal{S}(\mathcal{C}(\rho))$. The inverse homomorphism is*

$$\theta : \mathcal{U}(R, \Phi) \to \mathcal{C}(\rho)/\mathcal{S}(\mathcal{C}(\rho)),\ u \mapsto p(\pi^{-1}(u))$$

*which is well defined by Theorem 2.*

For the calculations in Section 5 we need the following lemma.

**Lemma 7.** *Let $X \in \mathcal{U}(R, \Phi)$ be as in (1). If $\delta^2 = \delta$ then $\iota := 1 - \delta$ is a symmetric idempotent of $R$.*

**Proof.** We define $u_\iota = -\iota\gamma^J\iota^J,\ v_\iota = \iota^J\beta\iota$ and calculate

$$\begin{aligned}
u_\iota v_\iota &= -(1-\delta)\epsilon^{-1}\gamma^J(1-\delta^J)\beta(1-\delta) \\
&= -(1-\delta)\epsilon^{-1}\underbrace{\gamma^J\beta}_{=\alpha^J\epsilon\delta-\epsilon}(1-\delta) + (1-\delta)\epsilon^{-1}\gamma^J\underbrace{\delta^J\beta}_{=\beta^J\epsilon\delta}(1-\delta) \\
&= (1-\delta)\epsilon^{-1}\epsilon(1-\delta) = 1-\delta = \iota
\end{aligned}$$

and

$$\begin{aligned}
v_\iota u_\iota &= -(1-\delta^J)\beta(1-\delta)\epsilon^{-1}\gamma^J(1-\delta^J) \\
&= -(1-\delta^J)\underbrace{\beta\epsilon^{-1}\gamma^J}_{=\alpha\delta^J-1}(1-\delta^J) + (1-\delta^J)\beta\underbrace{\delta\epsilon^{-1}\gamma^J}_{=\gamma\delta^J}(1-\delta^J) \\
&= -(1-\delta^J)(-1)(1-\delta^J) = 1-\delta^J = \iota^J.
\end{aligned}$$

□

3. $\mathcal{S}(\mathcal{C}(\rho)) \leq \mathcal{S}(\mathcal{C}(\rho/C))$

The Clifford-Weil group $\mathcal{C}(\rho/C)$ can be derived from $\mathcal{C}(\rho)$ by restricting the operation of $\mathcal{C}(\rho)$ to a submodule of $\mathbb{C}[V]$.

**Lemma 8.** *The group $\mathcal{C}(\rho)$ acts on a submodule of $\mathbb{C}[V]$ isomorphic to $\mathbb{C}[C^\perp/C]$. This yields a representation*

$$\mathrm{res} : \mathcal{C}(\rho) \to \mathrm{GL}(\mathbb{C}[C^\perp/C])$$

*with* $\mathrm{res}(\mathcal{C}(\rho)) \leq \mathcal{C}(\rho/C)$. *For the scalar subgroups we get* $\ker(\mathrm{res}) \cap \mathcal{S}(\mathcal{C}(\rho)) = \{1\}$ *and hence $\mathcal{S}(\mathcal{C}(\rho))$ is isomorphic to a subgroup of $\mathcal{S}(\mathcal{C}(\rho/C))$.*

**Proof.** Let Rep denote a set of coset representatives of $C^\perp/C$. We define a subspace

$$U := \{ \sum_{v \in \mathrm{Rep}} \sum_{c \in C} a_v b_{v+c} \mid a_v \in \mathbb{C}\} \leq \mathbb{C}[V].$$

This subspace is isomorphic to $\mathbb{C}[C^\perp/C]$ via

$$f : \mathbb{C}[C^\perp/C] \to U, \ \sum_{v \in \mathrm{Rep}} a_v b_{v+C} \mapsto \sum_{v \in \mathrm{Rep}} \sum_{c \in C} a_v b_{v+c}.$$

So we have

$$\mathrm{res}(x) = f \circ x \circ f^{-1} \in GL(U)$$

for $x \in \mathcal{C}(\rho)$. Particularly, if $x = s \cdot \mathrm{id}_{\mathbb{C}[V]}$ then $\mathrm{res}(x) = s \cdot \mathrm{id}_{\mathbb{C}[C^\perp/C]}$ and hence the restriction of res to the scalar subgroup of $\mathcal{C}(\rho)$ is injective.

We now will show that

$$\star_H \qquad f \circ p(\tilde{H}_{e,u_e,v_e}) \circ f^{-1} = p/C(\tilde{H}_{e,u_e,v_e})$$

and

$$\star_d \qquad f \circ p(\tilde{d}((r,\phi))) \circ f^{-1} = p/C(\tilde{d}((r,\phi)))$$

where $p : \mathcal{F}(R,\Phi) \to \mathcal{C}(\rho)$ and $p/C : \mathcal{F}(R,\Phi) \to \mathcal{C}(\rho/C)$ denote the group homomorphisms as defined (2). So we have $\mathrm{Im}(\mathrm{res}) \leq \mathcal{C}(\rho/C) = \mathrm{Im}(p/C)$ which shows the lemma.

To prove $\star_H$ let $v + C \in C^\perp/C$ and let $T$ denote a set of coset representatives of $eC^\perp/eC \cong eC^\perp/C$. Then

$$
\begin{aligned}
f^{-1}\circ p(\tilde{H}_{e,u_e,v_e})\circ f(b_{v+C}) &= f^{-1}\circ p(\tilde{H}_{e,u_e,v_e})(\sum_{c\in C} b_{v+c})\\
=&f^{-1}(\sum_{c\in C}|eV|^{-\frac{1}{2}}\sum_{w\in eV}\exp(2\pi i\beta(w,v_e(v+c)))b_{w+(1-e)(v+c)})\\
=&f^{-1}(|eV|^{-\frac{1}{2}}\sum_{w\in eV}\exp(2\pi i\beta(w,v_ev))\sum_{c'\in(1-e)C}\cdot\\
&\underbrace{\cdot\sum_{c\in eC}\exp(2\pi i\beta(w,v_ec))}\ b_{w+(1-e)(v+c')})\\
&=\begin{cases}|eC|, & w\in eC^{\perp},\\ 0 & \text{otherwise.}\end{cases}\\
=&f^{-1}(\frac{|eC|}{|eV|^{\frac{1}{2}}}\sum_{w\in eC^{\perp}}\sum_{c'\in(1-e)C}\exp(2\pi i\beta(w,v_ev))b_{w+(1-e)(v+c')})\\
=&f^{-1}(\frac{|eC|}{|eV|^{\frac{1}{2}}}\sum_{w\in T}\sum_{c'\in(1-e)C}\sum_{c\in eC}\exp(2\pi i\beta(w,v_ev))b_{w+c+(1-e)(v+c')})\\
=&f^{-1}(\frac{|eC|}{|eV|^{\frac{1}{2}}}\sum_{w\in T}\exp(2\pi i\beta(w,v_ev))\sum_{c\in C}b_{w+(1-e)v}+c)\\
=&|eC^{\perp}/C|^{-\frac{1}{2}}\sum_{w\in eC^{\perp}/C}\exp(2\pi i\beta/C(w,v_e(v+C)))b_{w+(1-e)(v+C)}\\
=&p/C(\tilde{H}_{e,u_e,v_e})(b_{v+C}).
\end{aligned}
$$

To show $\star_d$ we note that $\rho_\Phi(\phi)(c)=0$ for all $c\in C$ and for all $\phi\in\Phi$ and obtain

$$
\begin{aligned}
f^{-1}\circ p(\tilde{d}((r,\phi)))\circ f(b_{v+C}) &= f^{-1}\circ p(\tilde{d}((r,\phi)))(\sum_{c\in C}b_{v+c})\\
&= f^{-1}(p(\tilde{d}((r,0)))\sum_{c\in C}\exp(2\pi i\rho_\Phi(\phi)(v+c))b_{v+c})\\
&= f^{-1}(\sum_{c\in C}\exp(2\pi i\rho_\Phi(\phi)(v))b_{rv+rc})\\
&= f^{-1}(\sum_{c\in C}\exp(2\pi i\rho_\Phi(\phi)(v))b_{rv+c})\\
&= \exp(2\pi i\rho_\Phi/C(\phi)(v+C))b_{r(v+C)})\\
&= p/C(\tilde{d}((r,\phi)))(b_{v+C}).
\end{aligned}
$$

□

## 4. The strategy.

Without loss of generality we now assume that $\rho$ is faithful, that is,

$$\ker(\rho)=(\mathrm{Ann}_R(V),\ker(\rho_\Phi))=(0,0)$$

and let $(I,\Gamma)=\ker(\rho/C)$. We then define $\overline{\mathrm{res}}:\mathcal{U}(R,\Phi)\to\mathcal{U}(R/I,\Phi/\Gamma)$ by

$$\overline{\mathrm{res}}(\left(\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix},\begin{pmatrix}\phi_1&m\\ &\phi_2\end{pmatrix}\right))=\left(\begin{pmatrix}\alpha+I&\beta+I\\ \gamma+I&\delta+I\end{pmatrix},\begin{pmatrix}\phi_1+\Gamma&m+\psi(I)\\ &\phi_2+\Gamma\end{pmatrix}\right)).$$

By Remark 6 the epimorphism

$$\nu : \mathcal{C}(\rho) \to \mathcal{U}(R,\Phi) \text{ by } \nu(m_r d_\phi) = d((r,\phi)),\ \ \nu(h_{e,u_e,v_e}) = H_{e,u_e,v_e}$$

for $r \in R^*, \phi \in \Phi$ and symmetric idempotents $e = u_e v_e \in R$ is well defined and its kernel is $\mathcal{S}(\mathcal{C}(\rho))$. Similarly $\overline{\nu} : \mathcal{C}(\rho/C) \to \mathcal{U}(R/I, \Phi/\Gamma)$. Then $\nu \circ p = \pi$ and $\overline{\nu} \circ p/C = \pi/C$, where $\pi/C : \mathcal{F}(R/I,\Phi/\Gamma) \to \mathcal{U}(R/I,\Phi/\Gamma)$ is the analogous group epimorphism. Again the representation $\rho/C$ of $(R/I,\Phi/\Gamma)$ is faithful so by Remark 6 the kernel of $\overline{\nu}$ is $\mathcal{S}(\mathcal{C}(\rho/C))$.

We then have the following commutative diagram with exact rows and columns

$$\begin{array}{ccccccccccc}
 & & & & 1 & & 1 & & & & \\
 & & & & \downarrow & & \downarrow & & & & \\
 & & 1 & \to & \ker(\mathrm{res}) & \overset{\nu|_{\ker(\mathrm{res})}}{\to} & \ker(\overline{\mathrm{res}}) & \to & \mathcal{Y}' & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
1 & \to & \mathcal{S}(\mathcal{C}(\rho)) & \to & \mathcal{C}(\rho) & \overset{\nu}{\to} & \mathcal{U}(R,\Phi) & \to & 1 & & \\
 & & \downarrow & & \downarrow \mathrm{res} & & \downarrow \overline{\mathrm{res}} & & & & \\
1 & \to & \mathcal{S}(\mathcal{C}(\rho/C)) & \to & \mathcal{C}(\rho/C) & \overset{\overline{\nu}}{\to} & \mathcal{U}(R/I,\Phi/\Gamma) & \to & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
 & & \mathcal{Y} & & 1 & & 1 & & & & \\
 & & \downarrow & & & & & & & & \\
 & & 1 & & & & & & & &
\end{array}$$

To see that all sequences are exact, we note that $\nu_{|\ker(\mathrm{res})}$ is injective, since $\ker(\mathrm{res}) \cap \mathcal{S}(\mathcal{C}(\rho)) = 1$. The homomorphisms $\overline{\mathrm{res}}$ and res are surjective, since idempotents and units of $R/I$ lift to idempotents and units of $R$. Moreover $\overline{\mathrm{res}} \circ \nu = \overline{\nu} \circ \mathrm{res}$ as one checks on the generators.

The claim of Theorem 1 is that $\mathcal{Y}$ is trivial. But this is fulfilled if and only if $\mathcal{Y}'$ is trivial, that is, if $\nu|_{\ker(\mathrm{res})}$ is an isomorphism since

$$|\mathcal{Y}| = \frac{|\mathcal{S}(\mathcal{C}(\rho/C))|}{|\mathcal{S}(\mathcal{C}(\rho))|} = \frac{|\mathcal{C}(\rho/C)| \cdot |\mathcal{U}(R,\Phi)|}{|\mathcal{U}(R/I,\Phi/\Gamma)| \cdot |\mathcal{C}(\rho)|} = \frac{|\ker(\overline{\mathrm{res}})|}{|\ker(\mathrm{res})|} = |\mathcal{Y}'|.$$

## 5. The surjectivity of $\nu|_{\ker(\mathrm{res})}$

During the proof of Theorem 1 some results on lifting symmetric idempotents are needed, which are stated in the next two lemmata.

**Lemma 9.** *Let $R$ be an Artinian ring and $I$ an ideal of $R$. If $e \in I + \operatorname{rad} R \subseteq R$ such that $e^2 \equiv e \mod \operatorname{rad} R$ then there exists an idempotent $e' \in I$ such that $e' \equiv e \mod \operatorname{rad} R$.*

**Proof.** We choose $x_0 \in \operatorname{rad} R$ such that $e_0 := e + x_0 \in I$. Then $e_0 + \operatorname{rad} R$ is an idempotent in $R/\operatorname{rad} R$. Since $\operatorname{rad} R$ is a nilpotent ideal of $R$ [2, Theorem 4.9] constructs an idempotent $e' = f(e_0) \in I$ for some polynomial $f \in \mathbb{Z}[X]$ with $f(0) = 0$ such that $e' + \operatorname{rad} R = e_0 + \operatorname{rad} R$. □

By [2, Theorem 4.5] applied to an idempotent $e \in R$, the right-modules $eR$ and $e^J R$ are isomorphic, if and only if their quotients modulo $\operatorname{rad} R$ are isomorphic. Hence we find

**Lemma 10.** *Let $e + \operatorname{rad} R \in R/\operatorname{rad} R$ be a symmetric idempotent such that*

$$e + \operatorname{rad} R = u_e v_e + \operatorname{rad} R,\ \ e^J + \operatorname{rad} R = v_e u_e + \operatorname{rad} R,$$

$u_e + \operatorname{rad} R \in (eRe^J) + \operatorname{rad} R$, $v_e \in (e^J Re) + \operatorname{rad} R$. *If $e \in R$ is an idempotent then $e$ is symmetric as well. More precisely, there exist $\tilde{u}_e \in eRe^J$, $\tilde{v}_e \in e^J Re$ such that*

$$e = \tilde{u}_e \tilde{v}_e,\ e^J = \tilde{v}_e \tilde{u}_e$$

*and $\tilde{v}_e \equiv v_e \mod \operatorname{rad} R$.*

For the rest of this note, let

$$X := \left( \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \begin{pmatrix} \phi_1 & m \\ & \phi_2 \end{pmatrix} \right) \in \ker(\overline{\text{res}}) \tag{3}$$

and let $(I, \Gamma) := \ker(\rho/C)$. In particular, $\alpha, \delta \in 1 + I$, $\beta, \gamma \in I$, $\phi_1, \phi_2 \in \Gamma$ and $m \in \psi(I)$. We have to find some $x \in \ker(\text{res})$ such that $\nu(x) = X$.

**Lemma 11.** *We have $d(P(R, \Phi)) \cap \ker(\overline{\text{res}}) \subseteq \operatorname{Im}(\nu|_{\ker(\text{res})})$.*

**Proof.** Let $r \in R^*, \phi \in \Phi$ such that $d((r, \phi)) = \nu(m_r d_\phi) \in \ker(\overline{\text{res}})$. Then $r \in 1 + I$ and $\phi \in \Gamma$. In particular $r$ acts as the identity on $C^\perp/C$ and $\rho_\Phi/C(\phi) = 0$. This implies that both $m_r$ and $d_\phi \in \ker(\text{res})$. □

**Lemma 12.** *Let $\delta$ be a unit. Then there exists $x \in \ker(\text{res})$ such that $\nu(x) = X$.*

**Proof.** Since $\ker(\text{res})$ is a normal subgroup of $\mathcal{C}(\rho)$ it suffices to show that $X$ is contained in the normal subgroup of $\mathcal{U}(R, \Phi)$ generated by the elements $d(P(R, \Phi)) \cap \ker(\overline{\text{res}})$. We show that there is $\phi \in \Gamma$ such that

$$X = d((\delta, \phi_2)) H_{1,1,1} d((1, \phi)) H_{1,1,1}^{-1}.$$

We have $d((\delta, \phi_2)) = \left( \begin{pmatrix} \delta^{-J} & \beta \\ 0 & \delta \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & \phi_2 \end{pmatrix} \right)$ and hence

$$d((\delta, \phi_2))^{-1} = \left( \begin{pmatrix} \delta^J & -\delta^J \beta \delta^{-1} \\ 0 & \delta^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ & -\phi_2[\delta^{-1}] \end{pmatrix} \right).$$

We therefore find

$$d((\delta, \phi_2))^{-1} X = \left( \begin{pmatrix} \delta^J \alpha - \delta^J \beta \delta^{-1} \gamma & 0 \\ \delta^{-1} \gamma & 1 \end{pmatrix}, \begin{pmatrix} -\phi_2[\delta^{-1}\gamma] + \phi_1 & \tilde{m} \\ & 0 \end{pmatrix} \right)$$

for some $\tilde{m} \in M$. Since the upper right entry in the first matrix of this element of $\mathcal{U}(R, \Phi)$ is 0 we obtain $\tilde{m} = 0$ and similarly $\delta^J \alpha - \delta^J \beta \delta^{-1} \gamma = 1$ and we get

$$d((\delta, \phi_2))^{-1} X = \left( \begin{pmatrix} 1 & 0 \\ \delta^{-1}\gamma & 1 \end{pmatrix}, \begin{pmatrix} -\phi_2[\delta^{-1}\gamma] + \phi_1 & 0 \\ & 0 \end{pmatrix} \right)$$

Furthermore,

$$H_{1,1,1} = \left( \begin{pmatrix} 0 & 1 \\ -\epsilon^J & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon) \\ & 0 \end{pmatrix} \right),\ H_{1,1,1}^{-1} = \left( \begin{pmatrix} 0 & -\epsilon \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(-\epsilon) \\ & 0 \end{pmatrix} \right).$$

Then we have

$$(d((\delta, \phi_2))^{-1} X)^{H_{1,1,1}} = \left( \begin{pmatrix} 1 & -\epsilon \delta^{-1} \gamma \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & m' \\ & \phi \end{pmatrix} \right),$$

with some $m' \in M$ and

$$\phi = \{\!\{ \psi(-\epsilon \delta^{-1} \gamma) \}\!\} - \phi_2[\delta^{-1}\gamma] + \phi_1 \in \Gamma,$$

since $-\epsilon \delta^{-1} \gamma \in I$ and $\phi_1, \phi_2 \in \Gamma$. Again $m' = 0$ since the lower left entry in the first matrix is 0. Hence

$$H_{1,1,1}^{-1} d((\delta, \phi_2))^{-1} X H_{1,1,1} = d((1, \phi)) \in \ker(\overline{\text{res}})$$

as claimed. □

We now conclude the proof of Theorem 1 by showing

**Lemma 13.** *The map $\nu|_{\ker(\mathrm{res})}$ is surjective, that is,* $\mathrm{Im}(\nu|_{\ker(\mathrm{res})}) = \ker(\overline{\mathrm{res}})$.

**Proof.** We show that there exists a symmetric idempotent $\iota \in I$ such that

$$X = \underbrace{\left(\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}, \begin{pmatrix} \phi_1' & \mu' \\ & \phi_2' \end{pmatrix}\right)}_{=:X'} H_{\iota,u_\iota,v_\iota}$$

and $\delta' \in R^*$. Since $\iota \in I = \ker(\rho/C)$ the set $\iota(C^\perp/C) = \{0\}$ and hence $h_{\iota,u_\iota,v_\iota} \in \ker(\mathrm{res})$. By Lemma 12 $X' \in \mathrm{Im}(\nu|_{\ker(\mathrm{res})})$, so the same holds for $X$.

Now let us construct $\iota$. The ring $R/\operatorname{rad} R$ is a direct sum of matrix rings over skew fields. Thus there exist $u_1, u_2 \in R^*$ such that $u_1\delta u_2$ is an idempotent modulo $\operatorname{rad} R$. After conjugating with $u_2$ we obtain an idempotent $\tilde{u}\delta + \operatorname{rad} R \in R/\operatorname{rad} R$ with $\tilde{u} \in R^*$. Since $\tilde{u}\delta + (I + \operatorname{rad} R) \in R/(I + \operatorname{rad} R)$ is an idempotent as well and $\delta \in 1 + I$ is a unit modulo $I + \operatorname{rad} R$, it follows that $\tilde{u} \in 1 + (I + \operatorname{rad} R)$. We can even assume that $\tilde{u} \in 1 + I$. If $\tilde{u} = 1 + i + r$ with $i \in I$ and $r \in \operatorname{rad} R$ then $(1 + i)\delta = (\tilde{u} - r)\delta$ is an idempotent $\mod \operatorname{rad} R$. Additionally, from $\tilde{u} \in R^*$ we get $1 + i \in R^*$, so we can assume $\tilde{u} = 1 + i$. Now $d((\tilde{u}, 0)) \in \ker(\overline{\mathrm{res}})$, thus

$$\begin{aligned} X \in \ker(\overline{\mathrm{res}}) &\Leftrightarrow d((\tilde{u},0))X \in \ker(\overline{\mathrm{res}}) \\ &\Leftrightarrow \left(\begin{pmatrix} \tilde{u}^{-J}\alpha & \tilde{u}^{-J}\beta \\ \tilde{u}\gamma & \tilde{u}\delta \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix}\right) \in \ker(\overline{\mathrm{res}}) \end{aligned}$$

Thus we can assume that $\delta + \operatorname{rad} R \in R/\operatorname{rad} R$ is an idempotent.

In the hyperbolic counitary group $\mathcal{U}(R/\operatorname{rad} R, \Phi/\tilde{\Gamma})$ there is

$$\tilde{X} := \left(\begin{pmatrix} \alpha + \operatorname{rad} R & \beta + \operatorname{rad} R \\ \gamma + \operatorname{rad} R & \delta + \operatorname{rad} R \end{pmatrix}, \begin{pmatrix} \phi_1 + \tilde{\Gamma} & \mu + \psi(\operatorname{rad} R) \\ & \phi_2 + \tilde{\Gamma} \end{pmatrix}\right)$$

Lemma 7 says that $e := (1 - \delta) + \operatorname{rad} R$ is a symmetric idempotent of $R/\operatorname{rad} R$; more precisely, we may write $e = u_e v_e$ with

$$\begin{aligned} u_e &= -e\epsilon^{-1}\gamma^J e^J + \operatorname{rad} R, \\ v_e &= e^J \beta e^J + \operatorname{rad} R. \end{aligned}$$

By Lemma 9 we obtain a symmetric idempotent

$$\iota := e + x = 1 - \delta + x \in I$$

with $x \in \operatorname{rad} R \cap I$. We calculate the projection on the first component

$$\pi(XH^{-1}_{\iota,u_\iota,v_\iota}) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \delta^J - x^J & -v_\iota^J\epsilon \\ u_\iota^J & \delta - x \end{pmatrix} = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

with $\delta' = -\gamma v_\iota^J \epsilon + \delta - \delta x$. It remains to show that $\delta' \in R^*$. Lemma 10 gives $v_\iota \equiv (1 - \delta^J)\beta(1 - \delta) \mod \operatorname{rad} R$. Also $\delta x \in \operatorname{rad}(R)$, so it remains to show that

$$\widetilde{\delta'} := -\gamma(1 - \delta^J)\beta^J\epsilon(1 - \delta) + \delta \in R^*.$$

We observe that $\widetilde{\delta'}\delta = -\gamma(1-\delta^J)\beta^J\epsilon\underbrace{(1-\delta)\delta}_{=0}+\delta^2 = \delta$ and

$$\begin{aligned}(1-\delta)\widetilde{\delta'} &= -(1-\delta)\gamma(1-\delta^J)\beta^J\epsilon(1-\delta) = \\ -(1-\delta)\gamma\beta^J\epsilon(1-\delta) + \underbrace{(1-\delta)\gamma\delta^J\beta^J\epsilon(1-\delta)}_{=0,\text{ since }\gamma\delta^J=\delta\epsilon^J\gamma^J} &= -(1-\delta)\gamma\beta^J\epsilon + (1-\delta)\gamma\underbrace{\beta^J\epsilon\delta}_{=\delta^J\beta} = \\ -(1-\delta)\underbrace{\gamma\beta^J\epsilon}_{=\delta\epsilon^J\alpha^J\epsilon-1} + \underbrace{(1-\delta)\gamma\delta^J\beta}_{=0} &= 1-\delta.\end{aligned}$$

Particularly, $(1-\delta)(2-\widetilde{\delta'}) = 1-\delta$. Now we see that $\widetilde{\delta'}$ is a unit since

$$\widetilde{\delta'}(2-\widetilde{\delta'}) = \widetilde{\delta'}(\delta+(1-\delta))(2-\widetilde{\delta'}) = \widetilde{\delta'} - \delta\widetilde{\delta'} + \delta = 1-\delta+\delta = 1.$$

□

## References


[1] A. Günther, *Self-dual group ring codes.* PhD Thesis, RWTH Aachen University, in preparation

[2] H. Nagao, Y. Tsushima, *Representations of finite groups.* Academic Press (1988)

[3] G. Nebe, E.M. Rains, N.J.A. Sloane, *Self-dual codes and invariant theory.* Springer (2006)

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 171–178
ISSN 1930-1235: (2008)

# CT BURST ERROR WEIGHT ENUMERATOR OF ARRAY CODES

IRFAN SIAP

*Education Faculty,*
*Adıyaman University,*
*Adıyaman, Turkey.*
*isiap@adiyaman.edu.tr*

Abstract. Recently, CT burst errors originally defined for block codes have been generalized to CT burst errors for array codes [6]. In order to establish a Rieger's type bound for array codes with respect to CT burst errors. Here, we introduce a CT burst error weight enumerator whose coefficients represent the number of CT burst errors of a particular weight. The method of obtaining the CT burst error weight enumerator is obtained by generating function like approach and it does not involve solving equations as presented in [6].

## 1. Introduction

In classical algebraic coding theory, block codes and their properties have been investigated intensively. On the other hand, array codes have proven to be a good resource for burst error correction. A burst error definition for block codes is given in [1]. Burst error definitions for array codes as two dimensional objects differ. Recently, Jain in [7] has introduced a type of burst error for two dimensional arrays. Later, a new approach on enumerating for these type of errors is introduced in [9]. Recently, Jain in [6] has further generalized this definition for array codes and named these burst errors as CT (Chien-Tang) burst errors in [6]. Jain has investigated these array codes with respect to newly introduced non Hamming metric called Rosenbloom-Tsfasmann (or shortly RT) metric and established a Rieger's type bound. In [6], enumeration of CT burst errors is based on solving some linear equations and further for each weight computation the computations have to be carried out separately. Here in this paper, we introduce a novel approach for computing the number of CT bursts that avoids solving equations and separate computations. We introduce so called CT burst error weight enumerator and the way how to obtain it. The coefficients of CT burst error weight enumerator give the number of CT burst errors of a particular weight. This approach avoids solving equations and repetition of computations.

**Definition 1.1.** *A linear subspace of $Mat_{m\times s}(F_q)$ (the set of all $m \times s$ matrices over the finite field with $q$ elements) is called an array code.*

*Key words and phrases.* Matrix Array Codes, Non Hamming Metric, CT Burst Errors, Weight enumerator.

**Definition 1.2.** [6] *A CT burst of order pr or $p \times r$ ($1 \leq p \leq m, 1 \leq r \leq s$) in the space $Mat_{m\times s}(F_q)$ is an $m \times s$ matrix in which all the nonzero entries are confined to some $p \times r$ submatrix which has non zero first row and column.*

**Definition 1.3.** *(Non Hamming-RT weight)*[10]
*Let $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$. The RT weight (or $\rho$-weight) of $\boldsymbol{v}$ is defined by*

$$w_N(\boldsymbol{v}) = \begin{cases} max\{i|v_i \neq 0\}, & \boldsymbol{v} \neq 0 \\ 0, & \boldsymbol{v} = 0. \end{cases}$$

Let $A \in Mat_{m\times s}(F_q)$, and $A_i$ be the $i$th row of the matrix $A$. Then the RT weight of the matrix $A$ is the sum of the RT weight of its rows in other words $w_N(A) = \sum_{i=1}^{m} w_N(A_i)$.

The *RT* (non Hamming) metric for codes over fields is defined in [10] and some bounds for the minimum distance are established. Some applications of this metric to uniform distributions are given in [11]. Some recent work related to RT metric has appeared in [2],[4],[5].

Let $T_{m\times s}^{p\times r}(F_q)$ be the number of CT bursts of order $pr$. This number with a direct computation is given in the following theorem.

**Theorem 1.1.** [6]

$$T_{m\times s}^{p\times r}(F_q) = \begin{cases} ms(q-1), & p = 1, r = 1, \\ m(s-r+1)(q-1)q^{r-1}, & p = 1, r \geq 2 \\ (m-p+1)s(q-1)q^{p-1}, & p \geq 2, r = 1, \\ (m-p+1)s(q-1)q^{r(p-1)}[q^r - 1 - (q^{r-1}-1)q^{1-p}], & p \geq 2, r \geq 2. \end{cases}$$

Further, in [6] a formula for the number of *CT* bursts of a particular order and $\rho$-weight less than or equal to a number is stated and proved in the following theorem. It is also shown that this theorem enables to establish a Rieger's type bound for array codes with respect to CT burst errors.

**Theorem 1.2.** [6] *The number of CT bursts of order $pr$ ($1 \leq p \leq m, 1 \leq r \leq s$) in $Mat_{m\times s}(F_q)$ having $\rho$-weight $w$ or less ($1 \leq w \leq ms$) is given by*

$$T_{m\times s}^{p\times r}(F_q, w) = \begin{cases} m \times \min(w, s) \times (q-1), & p = 1, r = 1, \\ m \times \min(w-r+1, s-r+1) \times (q-1)q^{r-1}, & p = 1, r \geq 2, \\ (m-p+1)T_3, & p \geq 2, r = 1, \\ (m-p+1)T_4, & p \geq 2, r \geq 2. \end{cases}$$

*where*

$$T_3 = \sum_{j=1}^{\min(w,s)} \sum_{\eta=0:\eta j \leq w-j}^{p-1} \binom{p-1}{\eta} (q-1)^{\eta+1},$$

$$T_4 = \sum_{j=1}^{\min(w-r+1, s-r+1)} (Q_{j,r}^{p} - Q_{j,r}^{p-1} - Q_{j+1,r-1}^{p} + Q_{j+1,r-1}^{p-1}),$$

*and*

$$(1) \qquad Q_{j,r}^{p} = \sum_{k_j, k_{j+1}, \ldots, k_{j+r-1}} \frac{p! q^{\sum l=0^{r-1}(l+1)k_{j+l}}}{\prod_{l=0}^{r-1} k_{j+1}! \left(p - \sum_{l=0}^{r-1} k_{j+l}\right)!} \left(\frac{q-1}{q}\right)^{\sum_{l=0}^{r-1} k_{j+l}}$$

*where* $k_j, k_{j+1}, \ldots, k_{j+r-1}$ *being nonnegative integers such that*

$$\sum_{l=0}^{r-1} k_{j+l} \leq p$$

$$\sum_{l=0}^{r-1} (j+l)k_{j+l} \leq w. \tag{2}$$

In Theorem 1.2, computing the number of CT burst errors of a particular order is still a challenging task. In Equation 2, the two inequalities are first to be solved in the set of natural numbers, then by using these $k_i$ solutions the numbers $Q_{j,r}^{p}$ are to be computed by the formulas in (1) and finally after having found the necessary values, the formula in Theorem 1.2 is applied. In [6], some examples using this approach are worked out explicitly. In the next sections, we introduce a new method that is simpler than the method introduced in [6] and explained above. Further, by using the new method, it does not only give the number of a particular CT burst error weight but it also gives all spectra of the weights in a single computation. The spectra of the number of burst errors shall be called the burst error weight enumerator.

In Section 2, we give the computation method of burst errors of order $p \times r$ in the space $Mat_{p\times r}(F_q)$. In Section 3, we give the computation method of burst errors of order $p \times r$ in the space $Mat_{m\times s}(F_q)$ where $1 \leq p \leq m, 1 \leq r \leq s$ by making use of the results obtained in Section 2. We conclude by several remarks.

## 2. Burst Error Weight Enumerator

In order to introduce the new counting approach for $T_{m\times s}^{p\times r}(F_q)$ of CT burst errors we need couple definitions.

We shall work on the space $Mat_{p\times r}(F_q)$ and consider only burst errors of order $p \times r$. Later, we shall consider burst errors of order $p \times r$ in the larger space $Mat_{m\times s}(F_q)$ where $1 \leq p \leq m, 1 \leq r \leq s$.

In this section, first we introduce the concept of generic burst errors. Next, we present the method of computing the number of generic burst errors. Then, we introduce a method for computing the number of burst errors by making use of generic burst errors.

**Definition 2.1.** *If* $A \in Mat_{m\times s}(F_q)$ *and* $w_N(A_i) = \alpha_i$*, then the matrix* $A$ *is said to have a weight distribution of type* $(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

**Definition 2.2.** *( Hamming weight) If an element of* $F_q$ *is not equal to zero than its Hamming weight is equal to 1, otherwise 0.* $w(a) = 1$ *if* $a \neq 0$ *or else* $w(a) = 0$. *Hamming weight of a codeword is the sum of Hamming weights of its coordinates.*

**Definition 2.3.** *A generic burst error* $A = (a_{ij})$ *of order* $p \times r$ *: A burst error of order* $p \times r$ *with the following conditions:*

1. *All entries are equal to* 0 *or* 1.
2. *If the first entry of a row is nonzero then the Hamming weight of that row is equal to* 1 *or* 2.
3. *If the first entry of a row is zero then the Hamming weight of that row is equal to* 1.

Let $A = (a_{ij}) \in Mat_{p\times r}(F_q)$ and $A_i$ be the $i$th row of the matrix $A$. Let $A_i = (a_{i1}, a_{i2}, \dots, a_{ir})$. Since in our method of representing a matrix as a multivariable term and also carrying information for the first column entries of the matrix is crucial we associate a multivariable term $x_i^{w(a_{i1})} X_i^{w_N(A_i)}$ where $w(a_{i1}) = 1$ if $a_{i1} \neq 0$ and $w(a_{i1}) = 0$ if $a_{i1} = 0$. We use capital letter variables for the entries different from the first entry and small letter variable for the first entry only. In a natural way, we extend this representation to the matrix $A$ by taking the product of all terms corresponding to the rows of $A$.

For example, the representation of the following matrices are given below:

**Example 2.1.**

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \leftrightarrow \quad X_1^2 x_2 X_3^3, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \leftrightarrow \quad x_1 X_3^2.$$

Since there is a correspondence between $p$ multivariable polynomials and generic burst errors of order $p \times r$, it is possible to list these errors via multivariable polynomials.

For simplification purpose, we set $(x_1, \dots, x_p, X_1, \dots, X_p) = (\tilde{x}, \tilde{X})$.

**Theorem 2.1.** *Let $\overline{X}_j = 1 + \sum_{i=2}^{r} X_j^i$ for all $1 \leq j \leq p$. All generic bursts of order $p \times r$ are obtained as terms of the following multi variable polynomial, say generic polynomial:*

$$G(\tilde{x}, \tilde{X}) = x_1 \overline{X}_1 \prod_{j=2}^{r} (1 + x_j)\overline{X}_j + \left(\overline{X}_1 - 1\right) \sum_{j=2}^{r} \frac{x_j \prod_{i=2}^{r} (1 + x_i)\overline{X}_i}{(1 + x_j)}.$$

**Proof:** Let $A = (a_{ij}) \in Mat_{p\times r}(F_q)$ be a generic burst error. We split the proof into two parts. First, if $a_{11} = 1$, then the corresponding $p$-variable terms must all contain the multiples of $x_1$ of order one. Thus, for the first row all possible terms that contain $x_1$ and a power of $X_2$ greater than one are represented by $x_1 \left(1 + \sum_{i=2}^{r} X_j^i\right)$. Since there is no restriction on the rest of terms, these are all obtained from the terms $x_1 \overline{X}_1 \prod_{j=2}^{r} (1 + x_j)\overline{X}_j$. In the second case, if $a_{11} = 0$, then, by definition of a generic burst, there must exist $a_{1j} = 1$, for some $2 \leq j \leq p$. Since the term $x_1$ does not exist, any multiple of the terms in the sum $\sum_{i=2}^{r} X_1^i = \overline{X}_1 - 1$ can exist and further at least one of $x_j$ $(j \geq 2)$ must exist. Hence, the corresponding $p$-variable terms are obtained from the terms of $\left(\overline{X}_1 - 1\right) \sum_{j=2}^{r} \frac{x_j \prod_{i=2}^{r} (1+x_i)\overline{X}_i}{(1+x_j)}$. Therefore, by adding these two group of possible terms, we have the result. □

**Example 2.2.** *By applying Theorem 2.1, the following generic polynomial $G$ gives the term representation of $A \in M_{2\times 3}(F_2)$ generic burst errors of order $2 \times 3$ : $(X_1 = X, X_2 = Y, x_1 = x, x_2 = y)$*

$$G(x, y, X, Y) = x(1 + X^2 + X^3)(1 + y)(1 + Y^2 + Y^3) + (X^2 + X^3)y(1 + Y^2 + Y^3).$$

*Hence,*

$$G(x,y,X,Y) = x + xY^2 + xY^3 + xy + xyY^2 + xyY^3 + xX^2 + xX^2Y^2 + xX^2Y^3 + xX^2y + xX^2yY^2 + xX^2yY^3 + xX^3 + xX^3Y^2 + xX^3Y^3 + xX^3y + xX^3yY^2 + xX^3yY^3 + X^2y + X^2yY^2 + X^2yY^3 + X^3y + X^3yY^2 + X^3yY^3.$$

**Theorem 2.2.** *Let $G(x_1,\dots,x_p,X_1,\dots,X_p)$ be the generic polynomial of generic bursts of order $p\times r$. Let $x_1^{a_1}x_2^{a_2}\cdots x_p^{a_p}X_1^{b_1}X_2^{b_2}\cdots X_p^{b_p}$ be a term of the generic polynomial $G$ where $a_i=0$ or $a_i=1$ and $2\le b_i\le r$. Then, by substituting*

$$(q-1)^{\sum(a_i+b_i)}q^{\sum\max(b_i-2,0)}x_1^{a_1}x_2^{a_2}\cdots x_p^{a_p}X_1^{b_1}X_2^{b_2}\cdots X_p^{b_p}$$

*for $x_1^{a_1}x_2^{a_2}\cdots x_p^{a_p}X_1^{b_1}X_2^{b_2}\cdots X_p^{b_p}$, we obtain a multivariable polynomial, say $K$. Next, by substituting $X_j^{c_j}$ for $x_jX_j^{c_j}$ if $c_j\neq 0$ and $X_j$ for $x_j$ otherwise in $K$, we obtain a multivariable polynomial say $H(X_1,\dots,X_p)$. The coefficients of $H$ corresponding to the term $X_1^{c_1}X_2^{c_2}\cdots X_p^{c_p}$ give the number of all burst errors of order $p\times r$ and type $(c_1,c_2,\dots,c_p)$ in the space $Mat_{p\times r}(F_q)$.*

**Proof:** Let $x_1^{a_1}x_2^{a_2}\cdots x_p^{a_p}X_1^{b_1}X_2^{b_2}\cdots X_p^{b_p}$ be a term of the generic polynomial $G$. The $i$th row is determined by the variables $x_i$ and $X_i$ corresponding the first and the last entries. If $a_i=1$, then the first entry of the $i$th row is not equal to zero. Hence, there are $q-1$ non zero elements in $F_q$ for this entry. Similarly, if $b_j\neq 0$, then the entry $(j,b_j)$ of the burst error is not equal to zero. Hence, there are $q-1$ non zero elements in $F_q$ for this entry, too. The entries between the first and the last entry of the $i$th row can take any value of $F_q$. Thus, considering the case $b_i=0$, there are $q^{\max(b_i-2,0)}$ choices for these entries. Altogether, for the $i$th row, there are $(q-1)^{a_i+b_i}q^{\max(b_i-2,0)}$ choices. Multiplying all terms corresponding to the rows of the burst error, we obtain the coefficients of a polynomial $K$. Since the term $x_jX_j^{c_j}$ when $c_j\neq 0$ corresponds to the $j$th row with the first and the $c_j$th entry nonzero, the $\rho$ weight of the $j$th row is equal to $c_j$, hence substituting $X_j$ for the term $x_jX_j^{c_j}$ will protect this information when considered as a new term of a polynomial. On the other hand if $c_j=0$, then only the term $x_j$ will appear, and in this case by substituting $X_j$ for $x_j$ will serve for our purpose. It is clear that after these substitutions, the coefficients of the term $X_1^{c_1}X_2^{c_2}\cdots X_p^{c_p}$ in the new multivariable polynomial say $H$ will give the number of burst errors of order $p\times r$ and type $(c_1,c_2,\dots,c_p)$ in the space $Mat_{p\times r}(F_q)$.

**Definition 2.4.** *The multivariable polynomial $H(X_1,\dots,X_p)$ obtained in Lemma 2.2 is said to be the weight spectra burst error enumerator of burst errors of order $p\times r$.*

**Example 2.3.** *Let $G$ be given as in Example 2.2. Then, by making necessary substitutions given in Theorem 2.2, we have*

$$H(X,Y) = XY + 3X^2Y^2 + 6X^2Y^3 + 4X^3Y + 12X^3Y^3 + 2XY^2 + 6X^3Y^2 + X + 2X^2Y + 2X^3 + 4Y^3X + X^2.$$

**Definition 2.5.** *Let $\mathbb{B}$ be the set of all burst errors of order $p\times r$. The polynomial, $B^{p\times r}(t)=\sum_{A\in\mathbb{B}}t^{w_N(A)}=\sum_{i=1}^{p\cdot r}b_it^i$ is said to be the burst error weight enumerator of bursts of order $p\times r$ in the space $Mat_{p\times r}(F_q)$.*

The following corollary is straightforward:

**Corollary 2.1.** *Let $H(X_1,\dots,X_p)$ be the weight spectra burst error enumerator of burst errors of order $p\times r$. By setting $X_1=X_2=\cdots=X_p=t$ in $H(X_1,\dots,X_p)$ we obtain $B^{p\times r}(t)$.*

**Example 2.4.** *Substituting $t$ for both $X$ and $Y$ in Example 2.2, we obtain the burst error weight enumerator*

$$B^{2\times 3}(t)=12t^6+12t^5+11t^4+6t^3+2t^2+t.$$

**Example 2.5.** *Let $\boldsymbol{B}$ be the set of all burst errors of order $4\times 2$ in the space $Mat_{4\times 2}(F_2)$. Let $X_1=X, X_2=Y, X_3=Z$ and $X_4=W$. Then,*

$$\begin{aligned}G(\tilde{x},\tilde{X}) &= x(1+X^2)(1+y)(1+Y^2)(1+z)(1+Z^2)(1+w)(1+W^2)\\ &+X^2(y(1+Y^2)(1+z)(1+Z^2)(1+w)(1+W^2)+z(1+Z^2)(1+y)(1+Y^2)\cdot\\ &\cdot(1+w)(1+W^2)+(1+y)(1+Y^2)w(1+W^2)(1+z)(1+Z^2)).\end{aligned}$$

*Further, by applying necessary substitutions as pointed out in Corollary 2.1, we obtain the burst error weight enumerator*

$$B_{4\times 2}(t)=20t^8+44t^7+57t^6+52t^5+31t^4+15t^3+4t^2+t.$$

*It is clear that the sum of the coefficients of order three or less it is equal to $T^{4\times 2}_{4\times 2}(F_2,3)=20$.*

This example is also worked out in [6]. In order to compute the value of $T^{4\times 2}_{4\times 2}(F_2,w)$ for a particular value of $w$, we need to apply the formula given in [6] for each case separately. However, with this novel approach, we can compute each value of $w$ quite easily by adding the related coefficients of the weight enumerator of burst errors. For instance, $T^{4\times 2}_{4\times 2}(F_2,4)=51$. This fact can be formalized easily by the following corollary:

**Corollary 2.2.**

$$T^{p\times r}_{p\times r}(F_q,w)=\sum_{i=0}^{w}w_i$$

*where $w_i$ correspond to the coefficients of burst error weight enumerator.*

## 3. Bursts in Larger Space

In this section we consider burst of errors of order $p\times r$ in the space $Mat_{m\times s}(F_q)$ where $1\le p<m$ and $1\le r<s$.

**Lemma 3.1.** *Let $A$ be a burst of order $p\times r$ in the space $Mat_{m\times s}(F_q)$ where $1\le p<m$ and $1\le r<s$. If $T^{p\times r}(F_q)$ is the number of burst of order $p\times r$ in the space $Mat_{p\times r}(F_q)$, then $T^{p\times r}_{m\times s}(F_q)=(s-r+1)(m-p+1)T^{p\times r}_{p\times r}(F_q)$ gives the number of burst of order $p\times r$ in the space $Mat_{m\times s}(F_q)$.*

**Proof:** A burst of order $p\times r$ in the space $Mat_{m\times s}(F_q)$ is an $A$ submatrix of a matrix in $Mat_{m\times s}(F_q)$ with confined non zero entries in a submatrix of size $p\times r$ with a nonzero first row and column. Hence, placing $A$ as a submatrix of a matrix of size $m\times s$ is possible in $s-r+1$ ways moving from the left to the right starting from the position $(1,1)$ for both the matrix and the submatrix. Also, given any possible position obtained above, there exist also $m-p+1$ movements downwards for obtaining all possible submatrices. Thus, there exist $(s-r+1)(m-p+1)$

positions that give raise to new submatrices for each burst error of order $p \times r$ in the space $Mat_{p\times r}(F_q)$. Therefore, the number of burst of order $p \times r$ in the space $Mat_{p\times s}(F_q)$ is $(s-r+1)(m-p+1)T^{p\times r}_{p\times r}(F_q)$.□

We naturally extend the definition of a generic burst error of order $p \times r$ in the space $Mat_{p\times r}(F_q)$ to the space $Mat_{m\times s}(F_q)$. Further, we associate a multivariable term $x_i^{jw(a_{ij})}X_i^{w_N(A_i)}$ where $a_{ik} = 0$ for all $1 \le k < j$ to the $i$th row of matrix $A$. Again, we extend this definition to a matrix as in Section 2.

For example, the representation of the following matrices via polynomial terms are given below:

**Example 3.1.**

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \leftrightarrow \quad x_2^3x_3^2x_4^3, \quad B = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \leftrightarrow \quad x_1^3X_1^4x_2^2X_2^3x_3^2.$$

**Lemma 3.2.** *Let $A$ be a burst of order $p \times r$ in the space of matrices $Mat_{p\times r}(F_q)$. Let the term $x_1^{a_1}x_2^{a_2}\cdots x_p^{a_p}X_1^{b_1}X_2^{b_2}\cdots X_p^{b_p}$ represent the burst error $A$ of type*

$(\max(a_1, b_1), \max(a_2, b_2), \ldots, \max(a_p, b_p))$. *If $s-r+1 > 0$, then multiplying the term $x_1^{a_1}\cdots x_p^{a_p}X_1^{b_1}\cdots X_p^{b_p}$ by $x_1^{w(a_1)}\cdots x_p^{w(a_p)}X_1^{w(b_1)}\cdots X_p^{w(b_p)}$ gives a new burst error in the space $Mat_{m\times s}(F_q)$.*

**Definition 3.1.** *Let*

$$H(X_1, X_2, \ldots, X_p) = \sum_{(i_1,i_2,\ldots,i_p)} h(i_1, i_2, \ldots, i_p)X_1^{i_1}X_2^{i_2}\cdots X_p^{i_p}$$

*be a multi variable polynomial where $h(i_1, i_2, \ldots, i_p) \in \mathbb{N}$. Then, we define an operator $T$ on multivariable polynomial $H$ as follows:*

$$T(H) = \sum_{(i_1,i_2,\ldots,i_p)} h(i_1, i_2, \ldots, i_p)X_1^{w(i_1)(i_1+1)}X_2^{w(i_2)(i_2+1)}\cdots X_p^{w(i_p)(i_p+1)}.$$

**Example 3.2.** *We consider the burst errors of order $2 \times 2$ in the space of matrices $Mat_{3\times3}(F_2)$. Then,*

$$G(\tilde{X}, \tilde{Y}) = x(1 + X^2)(1 + y)(1 + Y^2) + X^2(y(1 + Y^2)).$$

*and*

$$G(\tilde{X}, \tilde{Y}) = x+xY^2+xy+xyY^2+xX^2+xX^2Y^2+xX^2y+xX^2yY^2+X^2y+X^2yY^2.$$

*There are 10 burst errors of order $2 \times 2$ in the space of matrices $Mat_{2\times2}(F_2)$.*

*There is $s-r = 1$ movement to the right and obtaining 10 more bursts in the space $Mat_{3\times3}(F_2)$. Hence, 20 burst errors in $Mat_{3\times3}(F_2)$. Since, $m-p = 1$, there is one movement down. Thus, obtaining 20 more burst errors in $Mat_{3\times3}(F_2)$. Altogether, there are $(s-r+1)(m-p+1)\times10 = 4\times10 = 40$ matrices in $Mat_{3\times3}(F_2)$. These burst errors are explicitly listed in Example 3.1 in* [6].

$$\begin{aligned} H(X, Y) &= 2X^2Y + 3X^2Y^2 + 2Y^2X + X^2 + YX + X \\ &= (2X + 3X^2)Y^2 + (2X^2 + X)Y + X + X^2. \end{aligned}$$

$$T(H) = 2X^3Y^2 + 3X^3Y^3 + 2Y^3X^2 + X^3 + Y^2X^2 + X^2.$$

$H+T(H) = 2Y^2X+4X^2Y^2+2X^2Y+YX+2Y^3X^2+3Y^3X^3+2Y^2X^3+X+2X^2+X^3$.
*Setting* $X = Y = t$ *in* $H + T(H)$, *we obtain* $3t^6 + 4t^5 + 4t^4 + 5t^3 + 3t^2 + t$. *Thus,*

$$W_{3\times 3}^{2\times 2}(t) = 6t^6 + 8t^5 + 8t^4 + 10t^3 + 6t^2 + 2t.$$

*Hence, the number of burst errors of* $\rho$*-weight* 3 *or less is equal to* $T_{3\times 3}^{2\times 2}(F_2, 3) = 18$.

## 4. Conclusion

The work presented here is an approach for enumerating burst errors. This generator function like approach can be applied to similar problems. Two dimensional burst error concept in array codes is still an interesting problem. Depending on the definition of burst errors in two dimensional arrays, enumeration of them in order to establish bounds on parameters of codes is an important problem.

## References

[1] R.T. Chien and D.T. Tang, *On Definition of a Burst,* IBM Journal Research Development, 9, p.292-293, 1965.
[2] Steven T. Dougherty and Maxim M. Skriganov, *MacWilliams Duality and the Rosenbloom-Tsfasman Metric*, Moscow Mathematical Journal, Vol. 2 Number 1, p. 83-89, 2002.
[3] P. Fire, *A class of Multiple Error Correcting Binary Codes for Non-independent Errors,* Sylvania Reports RSL-E-2, Sylvania Reconnaissance Systems, Mountain View, California, 1959.
[4] Mehmet Ozen, Irfan Siap, *On The Structure And Decoding of Linear Codes with respect to Rosenbloom-Tsfasman Metric*, Selcuk Journal of Applied Mathematics, Vol. 5, No. 2, pp.25-31,2004.
[5] Mehmet Ozen, Irfan Siap, *Linear codes over* $\mathbb{F}_q[u](u^s)$ *with respect to the Rosenbloom-Tsfasman metric*, Designs Codes and Cryptography, Vol.38, p. 17-29, 2006.
[6] Sapna Jain, *CT Bursts- From Classical to Array Coding,* Discrete Mathematics, 308(9), p.1489-1499, 2008.
[7] Sapna Jain, *Bursts in m- Metric Array Codes,* Linear Algebra and Its Applications, Vol. 418, p.130-141, 2006.
[8] Irfan Siap, *The Complete Weight Enumerator for Codes over* $\mathcal{M}_{n\times s}(\mathbb{F}_q)$, Lecture Notes on Computer Sciences 2260, p. 20-26, 2001.
[9] Irfan Siap, *Burst Error Enumeration of m-Array Codes,* submitted, 2007.
[10] M. Yu Rosenbloom and M. A. Tsfasman, *Codes for the m-metric,* Problems of Information Transmission, Vol. 33. No. 1, 45-52, 1997.
[11] M.M. Skriganov, *Coding theory and uniform distributions,* St. Petersburg Math. J. Vol 143, No. 2, 2002.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 179–184
ISSN 1930-1235: (2008)

# ON IDENTIFICATION FOR SOURCES EXTENDED TO MODEL WITH LIES

Zlatko Varbanov

*Department of Mathematics and Informatics*
*Veliko Tarnovo University, 5000 Veliko Tarnovo*
*e-mail:vtgold@yahoo.com*

## 1. Introduction

The classical transmission problem deals with the question how many possible messages can we transmit over a noisy channel? Transmission means there is an answer to the question "What is the actual message?"

In the identification problem we deal with the question how many possible messages the receiver of a noisy channel can identify? Identification means there is an answer to the question "Is the actual message $u$?". Here $u$ can be any member of the set of possible messages.

Allowing randomized encoding the optimal code size grows double exponentially in the block length and somewhat surprisingly the second order capacity equals Shannon's first order transmission capacity (see [5]).

Thus, Shannon's Channel Coding Theorem for Transmission is paralleled by a Channel Coding Theorem for Identification. It seems natural to look for such a parallel for sources, in particular for noiseless coding. This was suggested by Ahlswede in [1].

Let $(\mathcal{U}, P)$ be a source, where $\mathcal{U} = \{1, 2, \ldots, N\}, P = \{P_1, P_2, \ldots, P_N\}$, and let $\mathcal{C} = \{c_1, c_2, \ldots, c_N\}$ be a binary prefix code (PC) for this source with $||c_u||$ as length of $c_u$. Introduce the random variable $U$ with $\text{Prob}(U = u) = p_u$ for $u = 1, 2, \ldots, N$ and the random variable $C$ with $C = c_u = (c_1, c_2, \ldots, c_{u||c_u||})$ if $U = u$.

We use the PC for noiseless identification, that is user $u$ wants to know whether the source output equals $u$, that is, whether $C$ equals $c_u$ or not. The user iteratively checks whether $C$ coincides with $c_u$ in the first, second, etc. letter and stops when the first different letter occurs or when $C = c_u$. The problem is: **What is the expected number $L_{\mathcal{C}}(P, u)$ of checkings?**

In order to calculate this quantity we introduce for the binary tree $T_{\mathcal{C}}$, whose leaves are the codewords $c_1, c_2, \ldots, c_N$, the sets of leaves $\mathcal{C}_{ik} (1 \leq i \leq N; 1 \leq k)$, where $\mathcal{C}_{ik} = \{c \in \mathcal{C} : c$ coincides with $c_i$ exactly until the $k$'th letter of $c_i\}$. If $C$ takes a value in $\mathcal{C}_{uk}, 0 \leq k \leq ||c_u|| - 1$, the answers are $k$ times "Yes" and 1 time "No". For $C = c_u$ we have

$$L_{\mathcal{C}}(P, u) = \sum_{k=0}^{||c_u||-1} P(C \in \mathcal{C}_{uk})(k + 1) + ||c_u|| P_u.$$

Partially supported by RD491-09/2008 project, Veliko Tarnovo University.

For a code $\mathcal{C}$, the number $L_{\mathcal{C}}(P) = \max_{1\geq u\geq N} L_{\mathcal{C}}(P,u)$ is the expected number of checkings in the worst case and $L(P) = \min_{\mathcal{C}} L_{\mathcal{C}}(P)$ is this number for the best code.

## 2. Uniformly distributed sources

2.1. **Construction of a prefix code.** Let $P^N = \{\frac{1}{N},\dots,\frac{1}{N}\}$. We construct a prefix code $\mathcal{C}$ in the following way. In each node (starting at the root) we split the number of remaining codewords in proportion as close as possible to $(\frac{1}{2},\frac{1}{2})$. It is known [3] that for such code $\mathcal{C}$

$$\lim_{N\to\infty} L_{\mathcal{C}}(P^N) = 2 \tag{1}$$

**Example 1.** *Let* $N = 9,\ \mathcal{U} = \{1,2,\dots,9\},\ P_1 = \cdots = P_9 = \frac{1}{9}$. *Then,*

$$\mathcal{C} = \{000, 001, 010, 011, 100, 101, 110, 1110, 1111\}$$

$$L_{\mathcal{C}}(P) = L_{\mathcal{C}}(P,c_8) = \frac{4}{9}.1 + \frac{2}{9}.2 + \frac{1}{9}.3 + \frac{1}{9}.4 + \frac{1}{9}.4 = \frac{19}{9} \approx 2,111$$

$$L_{\mathcal{C}}(P,c_9) = L_{\mathcal{C}}(P,c_8); L_{\mathcal{C}}(P,c_7) = \frac{17}{9}; L_{\mathcal{C}}(P,c_5) = L_{\mathcal{C}}(P,c_6) = \frac{16}{9};$$

$$L_{\mathcal{C}}(P,c_1) = L_{\mathcal{C}}(P,c_2) = L_{\mathcal{C}}(P,c_3) = L_{\mathcal{C}}(P,c_4) = \frac{15}{9}$$

In [2] was stated the problem to estimate an universal constant $A = \sup L(P)$ for general distribution $P = (P_1,\dots,P_N)$. Here, we compute such constant for uniform distribution and this code $\mathcal{C}$.

Using decomposition formula for subtrees, we obtain the following recursion

$$L_{\mathcal{C}_N}(P^N) = \frac{\lceil \frac{N}{2} \rceil}{N} L_{\mathcal{C}_{\lceil \frac{N}{2} \rceil}}(P^{\lceil \frac{N}{2} \rceil}) + 1\ ,\ L_{\mathcal{C}_2}(P^2) = 1 \tag{2}$$

where $\mathcal{C}_t$ is the corresponding code with $t$ codewords.

From (2) follows that the worst case for $L_{\mathcal{C}}(P^N)$ is when $N = 2^k + 1$, for any integer $k$. We compute the exact value for $L_{\mathcal{C}}(P^N)$ in this case.

**Theorem 1.** $\sup_N L_{\mathcal{C}}(P^N) = 2 + \frac{log_2(N-1)-2}{N}$

*Proof.* If $N = 2^k + 1$ then $2^k$ codewords are in level $k$ (the root is level 0) in the binary tree $T_{\mathcal{C}}$ and one codeword is in level $k+1$ (if this codeword is $w$ then $L_{\mathcal{C}}(P^N, w) = L_{\mathcal{C}}(P^N)$). For every node in level $i$ $(0 \leq i \leq k-1)$ we split $2^{k-i-1}$ codewords in the left side and $2^{k-i-1}+1$ codewords in the right side. Therefore, $P(C \in \mathcal{C}_{wi}) = \frac{2^{k-i-1}}{2^k+1},\ i = 0,\dots,k-1$. Then, for $L_{\mathcal{C}}(P^N)$ we obtain

$$\begin{aligned} L_{\mathcal{C}}(P^N) = L_{\mathcal{C}}(P^N, w) &= \sum_{i=0}^{k} P(C \in \mathcal{C}_{wi})(i+1) + ||c_w||P_w \\ &= \sum_{i=0}^{k-1} P(C \in \mathcal{C}_{wi})(i+1) + P(C \in \mathcal{C}_{wk})(k+1) + ||c_w||P_w \\ &= \sum_{i=0}^{k-1} \frac{2^{k-i-1}}{2^k+1}(i+1) + \frac{1}{2^k+1}(k+1) + \frac{k+1}{2^k+1} \\ &= \frac{2^k}{2^k+1} \sum_{i=0}^{k-1} \frac{i+1}{2^{i+1}} + \frac{2(k+1)}{2^k+1} \end{aligned}$$

$$= \frac{2^k}{2^k+1}.\frac{2^{k+1}-k-2}{2^k} + \frac{2k+2}{2^k+1} = \frac{2^{k+1}-k-2}{2^k+1} + \frac{2k+2}{2^k+1}$$
$$= \frac{2^{k+1}+2+k-2}{2^k+1} = 2 + \frac{k-2}{2^k+1}$$

But $N = 2^k+1$ and $k = log_2(N-1)$. Then we obtain $L_{\mathcal{C}}(P^N) = 2+\frac{log_2(N-1)-2}{N}$. □

2.2. **Average identification length.** Also, in our work we consider the case where not only the source outputs but the users occur at random. In addition to the source $(\mathcal{U}, P)$ and random variable $U$, we are given $(\mathcal{V}, Q), \mathcal{V} \equiv \mathcal{U}$ with random variable $V$ independent of $U$ and defined by $\text{Prob}(V = v) = Q_v$ for $v \in V$. The source encoder knows the value $u$ of $U$ but not that of $V$, which chooses the user $v$ with probability $Q_v$. Again let $\mathcal{C} = \{c_1, \ldots, c_N\}$ be a binary prefix code and let $L_{\mathcal{C}}(P, u)$ be the expected number of checkings on code $\mathcal{C}$ for user $u$.

Instead of $L_{\mathcal{C}}(P) = \max_{u\in\mathcal{U}} L_{\mathcal{C}}(P, u)$ we can consider the average number of expected checkings (also called *average identification length*):

$$L_{\mathcal{C}}(P, Q) = \sum_{v\in\mathcal{V}} Q_v L_{\mathcal{C}}(P, v);\ L(P, Q) = \min_{\mathcal{C}} L_{\mathcal{C}}(P, Q)$$

A special case is $Q = P$, where

$$L_{\mathcal{C}}(P, P) = \sum_{u\in\mathcal{U}} P_u L_{\mathcal{C}}(P, u); \quad L(P, P) = \min_{\mathcal{C}} L_{\mathcal{C}}(P, P)$$

and for uniform distribution we have $L_{\mathcal{C}}(P^N, P^N) = \frac{1}{N}\sum_{u\in\mathcal{U}} L_{\mathcal{C}}(P^N, u)$.

2.3. **Results.** We calculate exact values of $L_{\mathcal{C}}(P^N)$ and $L_{\mathcal{C}}(P^N, P^N)$ for some $N$ and summarize them in Table 1. We know [3] that for $N = 2^k, L_{\mathcal{C}}(P^N) = L_{\mathcal{C}}(P^N, P^N) = 2 - \frac{2}{N}$.

TABLE 1 - some exact values for uniform distribution, $2^k < N < 2^{k+1}, k \geq 3$

| **N** | $L_{\mathcal{C}}(P^N)$ | $L_{\mathcal{C}}(P^N, P^N)$ |
|---|---|---|
| $2^k + 1$ | $2 + \frac{log_2(N-1)-2}{N}$ | $2 + \frac{log_2(N-1)-2}{N^2}$ |
| $2^k + 2^{k-1} - 1$ | 2 | $2 - \frac{5(N+1)-3log_2(\frac{2N+2}{3})}{3N^2}$ |
| $2^k + 2^{k-1}$ | $2 - \frac{1}{N}$ | $2 - \frac{5}{3N}$ |
| $2^k + 2^{k-1} + 1$ | $2 + \frac{log_2(\frac{N-1}{12})}{N}$ | $2 - \frac{(5N-2)-3log_2(\frac{N-1}{12})}{3N^2}$ |
| $2^{k+1} - 1$ | $2 - \frac{1}{N}$ | $2 - \frac{2N-log_2(N+1)+1}{N^2}$ |

## 3. Extension to liar models

3.1. **Identification and lies.** Suppose that when user $u$ iteratively checks whether $C$ coincides with $c_u$ in the first, second, etc. letter, for some reasons he obtains wrong information in any position. Then, there is a lie(error) in this position of the codeword. In this model with lies (we follow the idea in [4] but here no different costs of the lies), the user knows only that the general number of lies is at most $e$ and no information for the positions of lies.

Let $L_{\mathcal{C}}(P,u) = L_{\mathcal{C}}(P)$ for any $u \in \mathcal{U}$. In this case, we denote by $L_{\mathcal{C}}(P;e)$ the expected number of checkings if there are at most $e$ lies. Now, main question is: **What is the expected number of checkings if there are at most $e$ lies?**

We can see that the user needs of $e+1$ the same answers ("Yes" or "No") to be sure for the correct answer in any position. If the user has done $2e+1$ questions for any position he gets exact information for the value in this position. Therefore, there exists trivial upper bound

$$L_{\mathcal{C}}(P;e) \leq (2e+1)L_{\mathcal{C}}(P) \tag{3}$$

Clearly, this bound (3) can be improved by decreasing the number of remaining lies. The algorithm described below can be used.

3.2. **An Algorithm.** To decrease the number of remaining lies the following algorithm can be used for any $u \in \mathcal{U}$:

**Step 0**: BEGIN $i := 1, Checkings := 0$, actual message $:= v$;

**Step 1**: If $i > ||c_v||$ then Step 3. Otherwise, check codeword position $i$ until $e+1$ the same answers. Let $t$ be the number of obtained answers "Yes" and $f$ be the number of obtained answers "No";

**Step 2**: $Checkings := Checkings + (t+f)$. If $t > f$, then $e := e - f$, $i := i+1$, Step 1. Otherwise, the actual message $v \neq u$;

**Step 3**: END.

By this algorithm, we obtain the following result.

**Lemma 2.** *Let $v$ be the current checked codeword and let $i$ be the first position in which $c_u$ and $c_v$ differ (if $c_u = c_v$ then $i = ||c_u||$). Then, the number of checkings in the worst case is $e(i+1)+i$.*

*Proof.* We can see that the worst case with respect by $e$ is when all lies(errors) occur in position $i$. In this case

$Checkings = (e+1)(i-1) + (2e+1).1 = e(i+1) + i$.

If there is even one lie in any position $m$ $(1 \leq m \leq i-1)$, for every position $j$ $(m+1 \leq j \leq i)$ the user needs of $e$ the same answers. Then

$Checkings = (m-1)(e+1) + (e+2) + (i-m-1)e + (2e-1) = e(i+1) + m < e(i+1) + i$.

Therefore, this number $e(i+1)+i$ is the maximal number of checkings if this algorithm is used. □

**Example 2.** *Let $N = 9$, $\mathcal{U} = \{1, 2, \ldots, 9\}$, $P_1 = \cdots = P_9 = \frac{1}{9}$, and $e = 3$*

*Then*

$$\mathcal{C} = \{000, 001, 010, 011, 100, 101, 110, 1110, 1111\},$$

*and*

$$\begin{aligned} L_{\mathcal{C}}(P, c_8) &= L_{\mathcal{C}}(P, c_9) = L_{\mathcal{C}}(P) \\ L_{\mathcal{C}}(P; 3) &\le \frac{4}{9}.7 + \frac{2}{9}.(4+7) + \frac{1}{9}.(4+4+7) \\ &\quad + \frac{1}{9}.(4+4+4+7) + \frac{1}{9}.(4+4+4+7) = \frac{103}{9} \end{aligned}$$

3.3. **Results for liar models.** Using Lemma 2, we prove our main result.

**Theorem 3.** $L_{\mathcal{C}}(P; e) \le (e+1)L_{\mathcal{C}}(P) + e$

*Proof.* Let $k = ||c_u||$ and $P_{ui} = P(C \in \mathcal{C}_{ui})$. Then, in the worst case we obtain the following

$$\begin{aligned} L_{\mathcal{C}}(P; e) &\le \sum_{i=0}^{k-1} P_{ui}(e(i+2) + i + 1) + (e(k+1) + k)P_u \\ &= e\sum_{i=0}^{k-1} P_{ui}(i+2) + e(k+1)P_u + \sum_{i=0}^{k-1} P_{ui}(i+1) + kP_u \\ &= e\sum_{i=0}^{k-1}(P_{ui}(i+1) + P_{ui}) + e(k+1)P_u + L_{\mathcal{C}}(P) \\ &= e(\sum_{i=0}^{k-1} P_{ui}(i+1) + kP_u) + e(\sum_{i=0}^{k-1} P_{ui} + P_u) + L_{\mathcal{C}}(P) \\ &= eL_{\mathcal{C}}(P) + e.1 + L_{\mathcal{C}}(P) = \underline{(e+1)L_{\mathcal{C}}(P) + e}. \end{aligned}$$

□

Let $M_{\mathcal{C}}(P; e) = (e+1)L_{\mathcal{C}}(P) + e$. Then we have;

**Corollary 4.** *For uniform distribution* $P^N$

$$\lim_{N\to\infty} M_{\mathcal{C}}(P^N; e) = 3e + 2$$

*Proof.* Follows from (1) and Theorem 3. □

Let consider other distribution $P$ when all individual probabilities are powers of $\frac{1}{2}$, $P_u = \frac{1}{2^{\ell_u}},\ u \in \mathcal{U} = \{1, 2, \ldots, N\}$. Since

$$\sum_{u\in\mathcal{U}} \frac{1}{2^{\ell_u}} = 1$$

by Kraft's theorem there is a prefix code $\mathcal{C}$ with codeword lengths $||c_u|| = \ell_u$.

For such code $\mathcal{C}$ we know [2] that $L_{\mathcal{C}}(P, u) = 2(1-P_u)$. Therefore, $\lim_{N\to\infty} L_{\mathcal{C}}(P) = 2$ and by Theorem 3 we obtain the same result for this distribution $P$.

**Corollary 5.** $\lim_{N\to\infty} M_{\mathcal{C}}(P; e) = 3e + 2$

Also, for general distribution $P = (P_1, P_2, \ldots, P_N)$ we know that $L(P) \le 3$ ([3], Theorem 3). Therefore, for $L(P; e)$ (the expected number of checkings for the best code $\mathcal{C}$ and at most $e$ lies) we have

**Corollary 6.** $L(P; e) \le 4e + 3$

## References

[1] R.Ahlswede, General theory of information transfer: updated (Original version: General theory of information transfer, Preprint 97-118, SFB 343 "Diskrete Strukturen in der Mathematik", Universität Bielefeld), General Theory of Information Transfer and Combinatorics, a Special issue of Discrete Applied Mathematics.

[2] R. Ahlswede, "Identification entropy", General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 595–613, 2006.

[3] R. Ahlswede, B. Balkenhol, and C. Kleinewächter, "Identification for sources", General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, Vol. 4123, Springer Verlag, 51–61, 2006.

[4] R. Ahlswede, F. Cicalese, and C. Deppe, Searching with lies under error transition cost constraints, General Theory of Information Transfer and Combinatorics, Special Issue of Discrete Applied Mathematics, to appear.

[5] R.Ahlswede, G.Dueck, "Identification via channels", IEEE Trans. Inf. Theory, Vol.35, No.1, 15–29, 1989.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 185–198
ISSN 1930-1235: (2008)

# CLIFFORD-WEIL GROUPS FOR FINITE GROUP RINGS, SOME EXAMPLES.

Annika Günther
Lehrstuhl D für Mathematik,
RWTH Aachen University
52056 Aachen, Germany
annika.guenther@math.rwth-aachen.de

Gabriele Nebe
Lehrstuhl D für Mathematik,
RWTH Aachen University
52056 Aachen, Germany
nebe@math.rwth-aachen.de

Abstract. Finite group rings carry a natural involution that defines a form ring structure. We investigate the associated Clifford-Weil groups for the indecomposable representations of the groups of order $2, 3$ and the symmetric group $\mathrm{Sym}_3$ over the fields with 2 and 3 elements as well as suitable symmetrizations. An analogue of Kneser's neighboring method is introduced, to classify all self-dual codes in a given representation.

## 1. Introduction.

Let $G$ be a finite group and $K$ be a finite field. Then the group algebra $KG$ is a finite $K$-algebra with a natural $K$-linear involution

$$^- : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}.$$

This defines a form ring structure $\mathcal{R}^\epsilon(KG)$ on $KG$ where $\epsilon = \pm 1$; see Section 2).

A finite representation $\rho$ of $\mathcal{R}^\epsilon(KG)$ consists of a finite $KG$-module $V$ together with a $G$-invariant non-degenerate $K$-bilinear form $\beta : V \times V \to K$ which is symmetric, if $\epsilon = 1$ and skew-symmetric if $\epsilon = -1$. We do not deal with Hermitian forms here, since in our examples $K$ will be a prime field.

In this language, a self-dual code $C$ of length $N$ for the representation $\rho$ (for short, a code in $\rho$) is a $KG$-submodule of $V^N$ that is self-dual with respect to

$$\beta^N : V^N \times V^N \to K, \beta^N((x_1, \ldots, x_N), (y_1, \ldots, y_N)) = \sum_{i=1}^{N} \beta(x_i, y_i).$$

The complete weight enumerator of a code $C \leq V^N$ is

$$\mathrm{cwe}(C) := \sum_{c \in C} \prod_{i=1}^{N} x_{c_i} \in \mathbb{C}[x_v \mid v \in V]$$

and a homogeneous polynomial of degree $N$ in $|V|$ variables.

In Section 2 we will give explicit generators for a finite complex matrix group, the associated Clifford-Weil group $\mathcal{C}(\rho)$ such that $\mathrm{cwe}(C)$ is invariant under all variable substitutions defined by elements in $\mathcal{C}(\rho)$, hence $\mathrm{cwe}(C) \in \mathrm{Inv}(\mathcal{C}(\rho))$ lies in the invariant ring $\mathrm{Inv}(\mathcal{C}(\rho))$.

In fact the main results of [7] (Corollary 5.7.4 and 5.7.5) show that for a fairly general class of form rings $\mathrm{Inv}(\mathcal{C}(\rho))$ is generated as a vector space over $\mathbb{C}$ by the complete weight enumerators of self-dual codes in $\rho$. We conjecture that this is true for arbitrary finite form rings (cf. [7, Conjecture 5.7.2]) and in particular also for $\mathcal{R}^\epsilon(KG)$, but we do not know how to prove this for arbitrary finite group rings $KG$.

We denote the cyclic group of order $n$ by $Z_n$ and the symmetric group of degree $n$ by $\mathrm{Sym}_n$. Moreover we let $\mathbb{F}_p$ be the field with $p$ elements.

## 2. Rings with involution.

Rings with involution define certain form rings as explained below. We will apply the theory developed in this section to group rings with the natural involution $\bar{}$.

Let $R$ be a ring with 1 and

$$^J : R \to R, x \mapsto x^J$$

an involution, i.e. a ring antiautomorphism of order 1 or 2. So $(ab)^J = b^J a^J$ and $(a^J)^J = a$ for all $a, b \in R$. Moreover let $\epsilon \in Z(R)$ be a central unit of $R$ such that $\epsilon^J \epsilon = 1$. As explained in [7, Lemma 1.4.5] this setting defines a twisted ring $(R, \mathrm{id}, M = R)$ where the twist $\tau$ on $M = R$ is defined by

$$\tau : R \to R, a \mapsto a^J \epsilon.$$

The quadrupel

$$\mathcal{R}(R, J, \epsilon) := (R, \mathrm{id}, M = R, \Phi = R)$$

is a form ring (see [7, Definition 1.7.1]) with mappings

$$\{\!\{ \quad \}\!\} : M \to \Phi, m \mapsto m \text{ and } \lambda : \Phi \to M, \phi \mapsto \phi + \phi^J \epsilon.$$

The $R$-qmodule structure on $\Phi$ is given by

$$\phi[x] = x^J \phi x \text{ for all } \phi \in \Phi, x \in R.$$

A representation of the form ring $\mathcal{R}(R, J, \epsilon)$ is given by a left $R$-module $V$ together with a non-degenerate biadditive form $\beta : V \times V \to A$ into some abelian group $A$ such that

$$\beta(v, rw) = \beta(r^J v, w) \text{ and } \beta(v, w) = \beta(w, \epsilon v) \text{ for all } v, w \in V, r \in R.$$

That $\beta$ is non-degenerate means that it induces an isomorphism

$$\beta^* : V \to \mathrm{Hom}(V, A), v \mapsto (w \mapsto \beta(w, v))$$

which is then an isomorphism of $R$-left-modules, where $\mathrm{Hom}(V, A)$ is an $R$-left-module by

$$(rf)(v) := f(r^J v) \text{ for all } f \in \mathrm{Hom}(V, A), r \in R, v \in V.$$

The corresponding homomorphisms

$$\rho_M : R \to \mathrm{Bil}(V, A), \rho_\Phi : \Phi \to \mathrm{Quad}_0(V, A)$$

are given by

$$\rho_M(m) : (v, w) \mapsto \beta(v, mw),\ \ \rho_\Phi(\phi) : v \mapsto \beta(v, \phi v).$$

2.1. **Symmetric idempotents.** An idempotent $e^2 = e \in R$ is called symmetric, if $eR \cong e^J R$ as right $R$-modules. In this case there are $u_e \in eRe^J$ and $v_e \in e^J Re$ such that $u_e v_e = e$ and $v_e u_e = e^J$. A set of representatives of the $R^*$-conjugacy classes of symmetric idempotents in $R$ will be denoted by $\mathrm{SymId}(R)$.

2.2. **The associated Clifford-Weil group.** In coding theory one is mainly interested in finite alphabets $V$. We now assume that $R$ is a finite dimensional algebra over a finite field $K$ such that the restriction of $^J$ is the identity on $K$. For any representation $\rho = (V, \beta)$ of the form ring $\mathcal{R}(R, J, \epsilon)$ we may take the abelian group $A$ to be the field $K$ and $\beta^* : V \to V^* := \mathrm{Hom}_K(V, K)$. Let $p$ be the characteristic of $K$ and $\mathrm{trace} : K \to \mathbb{F}_p$ denote the trace from $K$ into its prime field $\mathbb{F}_p$. Identifying $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ with $\frac{1}{p}\mathbb{Z}/\mathbb{Z} \leq \mathbb{Q}/\mathbb{Z}$ the form $\beta : V \times V \to K$ defines a biadditive form

$$\tilde{\beta} : V \times V \to \mathbb{Q}/\mathbb{Z}, \tilde{\beta}(v, w) := \frac{1}{p}\mathrm{trace}(\beta(v, w))$$

which is again non-degenerate by the non-degeneracy of the trace form.

To define the associated Clifford-Weil group $\mathcal{C}(\rho)$ we index a basis $(e_v | v \in V)$ of $\mathbb{C}^{|V|}$ by the elements of $V$. Then $\mathcal{C}(\rho) \leq \mathrm{GL}_{|V|}(\mathbb{C})$ is the finite complex matrix group

$$\mathcal{C}(\rho) = \langle m_r, d_\phi, h_{e,u_e,v_e} : r \in R^*, \phi \in R, e = u_e v_e \in \mathrm{SymId}(R) \rangle$$

where

$$m_r : b_v \mapsto b_{rv}, \qquad d_\phi : b_v \mapsto \exp(2\pi i \tilde{\beta}(v, \phi v)) b_v$$

and

$$h_{e,u_e,v_e} : b_v \mapsto \frac{1}{|eV|^{1/2}} \sum_{w \in eV} \exp(2\pi i \tilde{\beta}(w, v_e v)) b_{w+(1-e)v}.$$

2.3. **Symmetrized weight enumerators.** Very often certain elements of $V$ share the same property (for instance they have the same Hamming weight). Then one might be interested in the symmetrized weight enumerators of the codes rather than the complete weight enumerators. One way to obtain the ring spanned by these symmetrized weight enumerators is of course to first calculate generators of the ring of complete weight enumerators and then apply the appropriate symmetrization. Since the ring spanned by the complete weight enumerators might be rather large, it is very helpful to have shortcuts to this procedure. This is only possible, if the action of the associated Clifford-Weil group commutes with the symmetrization.

**Definition 2.1.** *Let $G \leq \mathrm{Sym}(V)$ be a group permuting the elements of $V$ and $X_0, \ldots, X_n$ denote the $G$-orbits on $V$. Then the $G$-*symmetrized weight enumerator *$\mathrm{swe}_G(C)$ of a code $C \leq V^N$ is the homogeneous polynomial in $\mathbb{C}[x_0, \ldots, x_n]$ of degree $N$,*

$$\mathrm{swe}_G(C) := \sum_{c \in C} \prod_{i=0}^{n} x_i^{a_i(c)}$$

*where* $a_i(c) := |\{j \in \{1,\dots,N\} \mid c_j \in X_i\}|$ *for* $0 \le i \le n$. *The* $V$-Hamming weight enumerator *of* $C$ *is*

$$\mathrm{hwe}_V(C) := \sum_{c\in C} x^{N-w_V(c)} y^{w_V(c)} \in \mathbb{C}[x,y]$$

*where the* $V$-weight of $c = (c_1,\dots,c_N) \in V^N$ *is*

$$w_V(c) := |\{i \in \{1,\dots,N\} \mid c_i \neq 0\}|.$$

There are certain symmetrizations that commute with the action of the associated Clifford-Weil group, for instance if one takes $G$ to be a subgroup of the central unitary group of $R$ as defined and proven below. Usually the symmetization yielding the $V$-Hamming weight enumerators does not commute with $\mathcal{C}(\rho)$ and one may not expect that in general the $V$-Hamming weight enumerators of self-dual codes in a given representation generate the invariant ring of a finite group (see the end of Section 7.2 and [7, Section 5.8] for examples).

**Definition 2.2.** *Let* $(R,J)$ *be a ring with involution. Then the* central unitary group

$$\mathrm{ZU}(R,J) := \{g \in Z(R) \mid gg^J = g^J g = 1\}.$$

**Theorem 2.3.** *Let* $\rho := (V,\beta)$ *be a finite representation of the form ring* $\mathcal{R}(R,J)$ *and* $U \le \mathrm{ZU}(R,J)$. *Then*

$$\rho(U) := \langle m_u \mid u \in U\rangle$$

*is in the center of* $\mathcal{C}(\rho)$.

Proof. Clearly $\rho(U) \le \mathcal{C}(\rho)$ commutes with the generators $m_r$ for $r \in R^*$ since $U$ is central in $R^*$. For $\phi \in \Phi$, $u \in U$ and $v \in V$ we have

$$\beta(uv, \phi uv) = \beta(uv, u\phi v) = \beta(u^J uv, \phi v) = \beta(v, \phi v)$$

so $m_u$ commutes with $d_\phi$. To see that $m_u$ commutes with the last type $h_{e,u_e,v_e}$ of generators of $\mathcal{C}(\rho)$ one has to note that $ueV = eV$ since $u$ is a central unit and that $\beta(uw, v_e uv) = \beta(w, v_e v)$ for all $v, w \in V, u \in U$. □

**Remark 2.4.** *The theorem uses that* $\{\!\{\ \ \}\!\}$ *is surjective in our situation. In general one has to replace* $\mathrm{ZU}(R,J)$ *by its subgroup*

$$U_\rho = \{g \in \mathrm{ZU}(R,J) \mid \rho(\phi)(gv) = \rho(\phi(v)) \text{ for all } v \in V, \phi \in \Phi\}$$

*to obtain the same theorem as above.*

**Corollary 2.5.** *Let* $\rho := (V,\beta)$ *be a finite representation of the form ring* $\mathcal{R}(R,J)$ *and* $U \le \mathrm{ZU}(R,J)$. *Then* $U$ *acts as permutations on the set* $V$ *and the corresponding symmetrization commutes with the action of* $\mathcal{C}(\rho)$.

In this setup we can define the $U$-symmetrized Clifford-Weil group,

$$\mathcal{C}^{(U)}(\rho) \le \mathrm{GL}_{n+1}(\mathbb{C}).$$

Generators for $g^{(U)}$ the symmetrized group may be obtained from the generators $g$ of $\mathcal{C}(\rho)$ as follows. If

$$g \sum_{v\in X_i} e_v = \sum_{j=0}^{n} a_{ij} \Big( \sum_{w\in X_j} e_w \Big)$$

then

$$g^{(U)}(x_i) = \sum_{j=0}^{n} a_{ij} \frac{|X_j|}{|X_i|} x_j.$$

Of course $\rho(U)$ is in the kernel of this symmetrization $\mathcal{C}(\rho) \to \mathcal{C}^{(U)}(\rho)$.

**Remark 2.6.** *The invariant ring of $\mathcal{C}^{(U)}(\rho)$ consists of the $U$-symmetrized invariants of $\mathcal{C}(\rho)$. In particular, if the invariant ring of $\mathcal{C}(\rho)$ is spanned by the complete weight enumerators of self-dual codes in $\rho$, then the invariant ring of $\mathcal{C}^{(U)}(\rho)$ is spanned by the $U$-symmetrized weight-enumerators of self-dual codes in $\rho$.*

2.4. **Form group rings.** Let $G$ be a finite group and $K$ be a finite field. Then the group algebra $KG$ is a finite $K$-algebra with a natural $K$-linear involution

$$^- : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}.$$

Since $\epsilon = 1$ and $\epsilon = -1$ are central units in $KG$, the construction of Section 2 defines a natural form ring structure $\mathcal{R}^\epsilon(KG)$ on $KG$ where $\epsilon = \pm 1$.

A representation of the form ring $\mathcal{R}^\epsilon(KG)$ is given by a finite $KG$-module $V$ together with a $G$-invariant non-degenerate $K$-bilinear form $\beta : V \times V \to K$ which is symmetric, if $\epsilon = 1$ and skew-symmetric if $\epsilon = -1$.

## 3. A method to enumerate all self-dual codes.

There is a very nice and efficient method to enumerate all self-dual codes in a given length representation of a form ring. This is based on M. Kneser's ideas [4], described in [6] for codes over finite fields and in [5] for $\mathbb{Z}G$-lattices. We often apply it to find self-dual codes in representations of the finite form ring $\mathcal{R}(KG)$ and therefore we will describe it in a fairly general setting adopted to this situation.

Let $(V, \rho_M, \rho_\Phi, \beta)$ be a finite representation of a form ring $(R, M, \psi, \Phi)$ as defined in [7, Section 1]. In particular $V$ is a finite left-module for the ring $R$ and $\beta : V \times V \to \mathbb{Q}/\mathbb{Z}$ a non-degenerate form on $V$ which induces an $R$-module isomorphism

$$\beta^* : V \to V^* := \mathrm{Hom}(V, \mathbb{Q}/\mathbb{Z}), w \mapsto (v \mapsto \beta(v, w)).$$

A self-dual code $C$ in $\rho$ is a $R$-submodule $C \leq V$ such that

$$C = C^\perp := \{v \in V \mid \beta(c, v) = 0 \text{ for all } c \in C\}.$$

Let

$$\mathcal{M}(V) := \{C \leq V \mid C = C^\perp\}$$

denote the set of all self-dual codes in $V$.

**Lemma 3.1.** *Let $C \in \mathcal{M}(V)$ and*

$$\star \quad \{0\} = V_0 < V_1 < \ldots < V_s = C < V_{s+1} < \ldots < V_t = V$$

*be a composition series of $V$ with simple $R$-left-module $S_i := V_i/V_{i-1}$ $(1 \leq i \leq t)$. Then $t = 2s$ and there is a bijection $\pi : \{1, \ldots, s\} \to \{s+1, \ldots, t\}$ such that $(S_i)^* = S_{\pi(i)}$.*

Proof. The mapping $\beta^* : V \to \mathrm{Hom}(C, \mathbb{Q}/\mathbb{Z})$, $v \mapsto (c \mapsto \beta(v, c))$ is an epimorphism with kernel $C^\perp$. Hence $V/C = V/C^\perp \cong \mathrm{Hom}(C, \mathbb{Q}/\mathbb{Z}) = C^*$. Now the lemma follows since the composition factors of $C^*$ are the dual $S^* = \mathrm{Hom}(S, \mathbb{Q}/\mathbb{Z})$ of the

composition factors $S$ of $C$.
Alternatively one may choose $V_{t-i} = V_i^{\perp}$ in the composition series $\star$. Then

$$V_{t-i}/V_{t-i-1} = V_i^{\perp}/V_{i+1}^{\perp} \cong (V_{i+1}/V_i)^*$$

and the lemma follows from the Jordan-Hölder theorem on the uniqueness of composition factors. □

**Corollary 3.2.** *If $\mathcal{M}(V) \neq \emptyset$ then each simple composition factor $S$ of $V$ that is isomorphic to its dual, $S \cong S^*$, occurs with even multiplicity in every composition series of $V$.*

**Corollary 3.3.** *Any two modules $C, D \in \mathcal{M}(V)$ have the same composition lengths: $\ell(C) = \ell(D) = s = \ell(V)/2$.*

**Definition 3.4.** *Two self-dual codes $C, D \in \mathcal{M}(V)$ are called* neighbors*, if the $R$-module $C/C\cap D$ is simple. The* neighbor-graph *is the graph $\Gamma$ with vertex set $\mathcal{M}(V)$. Two vertices $C, D \in \mathcal{M}(V)$ are connected, if $C$ and $D$ are neighbors.*

**Theorem 3.5.** *The neighbor graph $\Gamma$ is connected.*

Proof. We define a distance on the set $\mathcal{M}(V)$. For $C, D \in \mathcal{M}(V)$ let

$$d(C, D) := \ell(C/(C \cap D))$$

be the number of composition factors of the factor module $C/(C \cap D)$. Then clearly $d(C, D) = 0$ if and only if $C = D$ and $d(C, D) = d(D, C)$ by Corollary 3.3 and Jordan-Hölder. Also the triangle inequality follows easily from the fact that the number of composition factors is well defined. Clearly $d(C, D) \leq \ell(C) = s$ for all $C, D \in \mathcal{M}(V)$
We claim that this distance $d(C, D)$ is the number of edges in any shortest path in $\Gamma$ connecting $C$ and $D$, which shows that the diameter of $\Gamma$ is bounded from above by $s$ and in particular that $\Gamma$ is connected.
To prove this claim we proceed by induction on $n := d(C, D)$. For $n = 0$ and $n = 1$ the claim is true by definition. Now assume that $n \geq 2$. Then we construct a code $C_1 \in \mathcal{M}(V)$ such that

$$d(C, C_1) = 1 \text{ and } d(C_1, D) = n - 1.$$

To this aim let $U := C \cap D$ and choose $D > U_1 > U$ such that $U_1/U \cong S$ is simple. This is possible since the composition length $n = \ell(D/U) \geq 2$. Then $U = U_1 \cap C$ and

$$S \cong U_1/(U_1 \cap C) \cong (U_1 + C)/C.$$

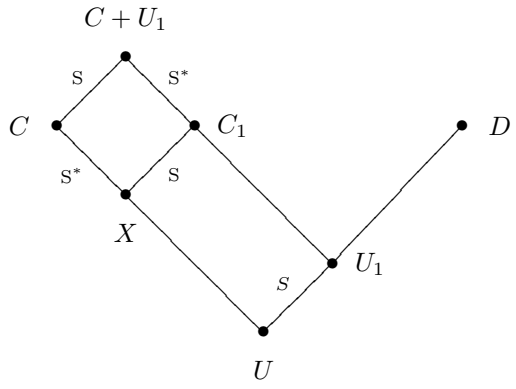
The module $X := (U_1 + C)^{\perp} < C = C^{\perp}$ is a submodule of $C$ with $C/X \cong S^*$. Put

$$C_1 := X + U_1 = (U_1 + C)^{\perp} + U_1.$$

Then

$$C_1^{\perp} = (U_1 + C) \cap (U_1^{\perp}) \supseteq X + U_1 = C_1$$

since $U_1 \subseteq D = D^\perp \subseteq U_1^\perp$. Comparing the composition lengths we get $C_1^\perp = C_1 \in \mathcal{M}(V)$. Clearly $d(C, C_1) = 1$. Moreover $C_1 \cap D = U_1$ and hence $d(C_1, D) = n - 1$.




□

This provides an algorithm to enumerate all elements of $\mathcal{M}(V)$. Start with some self-dual code $C \in \mathcal{M}(V)$. For all composition factors $S$ of $V$ calculate all non-zero $R$-homomorphisms $\varphi : C \to S$. Their kernels $U := \ker(\varphi)$ provide all submodules $U \leq C$ such that $C/U \cong S$. The neighbors $D$ of $C$ such that $D \cap C = U$ can be obtained as full preimages of the self-dual submodules $D/U$ of $U^\perp/U$ (not equal to $C/U$). Continue with all neighbors until all codes in $\mathcal{M}(V)$ have been found. Usually one is only interested in representatives of equivalence classes of codes in $\mathcal{M}(V)$, so there is a certain group $G$ acting on $\mathcal{M}(V)$ that preserves submodules and duality. Then it is enough to work with representatives of the $G$-orbits. More details can be found in [3].

## 4. $\mathbb{F}_2 Z_2$

The Type of singly even self-dual codes over $\mathbb{F}_2 Z_2$ is one of the rare cases for which the invariant ring of the associated Clifford-Weil group is a polynomial ring. The Type of doubly even self-dual codes over $\mathbb{F}_2 Z_2$ is interesting because of the connection to Type IV codes over $\mathbb{Z}_4$. The Gray image of a Type IV code over $\mathbb{Z}_4$ is a doubly even $\mathbb{F}_2 Z_2$-linear self-dual code (see [1], [2]) However not all such codes are Gray images of a Type IV code over $\mathbb{Z}_4$.

Let $Z_2 = \langle a \rangle$. Then $\mathbb{F}_2 Z_2 \cong \mathbb{F}_2[x]/(x^2)$ via $(1 + a) \mapsto x$. In particular the unit group $(\mathbb{F}_2 Z_2)^* = \langle a \rangle \cong Z_2$ and $\mathbb{F}_2 Z_2$ has just two indecomposable modules, the simple module $S = \mathbb{F}_2$ and the projective module $P = \mathbb{F}_2 Z_2$. The representation $\rho_S$ with underlying module $S$ defines $\mathcal{C}(\rho_S) = \mathcal{C}(2_I)$ the Clifford-Weil group associated to the Type of singly even binary self-dual codes which is treated in detail in [7, Section 6.3].

$Z_2$ acts on the module $P \cong \mathbb{F}_2^2$ via

$$a \mapsto \rho_P(a) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and the two non-degenerate $a$-invariant bilinear forms (with Gram matrices $I_2$ and $\rho_P(a)$) are in the same orbit under $(\mathbb{F}_2 Z_2)^*$ and hence define the same notion of duality. We choose $\beta$ to be the standard form with Gram matrix $I_2$. Then with respect to the basis

$$e_{(0,0)}, e_{(1,0)}, e_{(0,1)}, e_{(1,1)}$$

of $\mathbb{C}[P]$ the associated Clifford-Weil group $\mathcal{C}(\mathbb{F}_2 Z_2)$ is generated by

$$m_a := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\ d_\phi := \mathrm{diag}(1,-1,-1,1),\ h_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

($\phi = \{\!\{\beta\}\!\}$) has order 16 and is isomorphic to $D_8 \times Z_2$, the direct product of the dihedral group of order 8 and the cyclic group of order 2. $\mathcal{C}(\mathbb{F}_2 Z_2)$ is a real reflection group and the invariant ring is the polynomial ring

$$\mathrm{Inv}(\mathcal{C}(\mathbb{F}_2 Z_2)) = \mathbb{C}[p_1, p_2, p_3, p_4]$$

with

$$\begin{aligned} p_1 &= x + t, \\ p_2 &= x^2 + y^2 + z^2 + t^2, \\ p_3 &= x^2 + 2yz + t^2, \\ p_4 &= x^4 + y^4 + z^4 + t^4 + 8xyzt + 2x^2t^2 + 2y^2z^2 \end{aligned}$$

where we put $x = x_{(0,0)}, y = x_{(1,0)}, z = x_{(0,1)}, t = x_{(1,1)}$ for simplicity. These polynomials are the complete weight enumerators of the codes $C_i \leq P^N$ with generator matrices

$$[(1,1)],\ \begin{bmatrix} (1,0) & (1,0) \\ (0,1) & (0,1) \end{bmatrix},\ \begin{bmatrix} (1,1) & (1,1) \\ (1,0) & (0,1) \end{bmatrix},$$

and

$$\begin{bmatrix} (1,0) & (0,0) & (0,1) & (1,1) \\ (0,1) & (0,0) & (1,0) & (1,1) \\ (0,0) & (1,0) & (1,1) & (0,1) \\ (0,0) & (0,1) & (1,1) & (1,0) \end{bmatrix}.$$

For the module theoretic structure we get

$$C_1 \cong S, C_2 \cong C_3 \cong P, C_4 \cong P \oplus P$$

(as $\mathbb{F}_2 Z_2$-modules). As binary codes, $C_2$, $C_3$ and $C_1 \perp C_1$ are equivalent, and $C_4$ is equivalent to the extended Hamming code $e_8$ of length 8.

To obtain the type of doubly even binary codes in $P^N$, we may enlarge $\Phi$ and obtain one additional generator $d_\varphi := \mathrm{diag}(1, i, i, -1)$, with $i \in \mathbb{C}, i^2 = -1$. The group

$$\mathcal{C}_{\mathrm{II}}(\mathbb{F}_2 Z_2) = \langle \mathcal{C}(\mathbb{F}_2 Z_2), d_\varphi \rangle$$

has order 192 and Molien series

$$\frac{1 + \lambda^4 + 2\lambda^8}{(\lambda^4 - 1)^3(\lambda^{12} - 1)}.$$

The invariant ring $\mathrm{Inv}(\mathcal{C}_{\mathrm{II}}(\mathbb{F}_2 Z_2))$ is a free module over the polynomial subring $R := \mathbb{C}[p_4, p_5, p_6, p_7]$,

$$\mathrm{Inv}(\mathcal{C}_{\mathrm{II}}(\mathbb{F}_2 Z_2)) = R \oplus Rq_1 \oplus Rq_2 \oplus Rq_3$$

where $p_4$ is as above, $p_5, p_6, q_1$ are complete weight enumerators of further $Z_2$-structures of $e_8$, $q_2 = \mathrm{cwe}(e_8 \otimes P)$, $q_3$ is the complete weight enumerators of a suitable $Z_2$-structure on $d_{16}^+$ and $p_7$ is the weight enumerator of any $Z_2$-structure of the Golay code.

To find the inequivalent doubly even codes in $P^4$ that are equivalent to $e_8$ as binary codes, we consider the automorphism group $G = \mathrm{Aut}(e_8)$. There are 2 conjugacy classes of elements of order 2 in $G$ which are conjugate to $a = (1,2)(3,4)(5,6)(7,8)$ in $\mathrm{Sym}_8$.

The $a$-invariant codes $C_k$ have generator matrices $(I_4, J_k)$ with $k = 1, \ldots, 6$, where $I_4$ is the $4 \times 4$ unit matrix viewed as element of $P^{4\times 2}$ and

$$J_1 = \begin{bmatrix} (0,1) & (1,1) \\ (1,0) & (1,1) \\ (1,1) & (0,1) \\ (1,1) & (1,0) \end{bmatrix},\ J_2 = \begin{bmatrix} (1,0) & (1,1) \\ (0,1) & (1,1) \\ (1,1) & (0,1) \\ (1,1) & (1,0) \end{bmatrix},\ J_3 = \begin{bmatrix} (1,0) & (1,1) \\ (0,1) & (1,1) \\ (1,1) & (1,0) \\ (1,1) & (0,1) \end{bmatrix},$$

$$J_4 = \begin{bmatrix} (1,1) & (1,0) \\ (0,1) & (1,1) \\ (1,1) & (0,1) \\ (1,0) & (1,1) \end{bmatrix},\ J_5 = \begin{bmatrix} (0,1) & (1,1) \\ (1,1) & (1,0) \\ (1,1) & (0,1) \\ (0,1) & (1,1) \end{bmatrix},\ J_6 = \begin{bmatrix} (1,1) & (1,0) \\ (1,0) & (1,1) \\ (1,1) & (0,1) \\ (0,1) & (1,1) \end{bmatrix}.$$

with complete weight enumerators

$$\begin{aligned}
\mathrm{cwe}(C_1) = p_4 = &\quad x^4 + 2x^2t^2 + 8xyzt + y^4 + 2y^2z^2 + z^4 + t^4 \\
\mathrm{cwe}(C_2) = p_5 = &\quad x^4 + 2x^2t^2 + 2xy^2t + 4xyzt + 2xz^2t + 2y^3z + 2yz^3 + t^4 \\
\mathrm{cwe}(C_3) = &\quad x^4 + 2x^2t^2 + 4xy^2t + 4xz^2t + 4y^2z^2 + t^4 \\
\mathrm{cwe}(C_4) = &\quad x^4 + 3xy^2t + 6xyzt + 3xz^2t + y^3z + yz^3 + t^4 \\
\mathrm{cwe}(C_5) = p_6 = &\quad x^4 + 12xyzt + y^4 + z^4 + t^4 \\
\mathrm{cwe}(C_6) = q_1 = &\quad x^4 + 4xy^2t + 4xyzt + 4xz^2t + 2y^2z^2 + t^4
\end{aligned}$$

For the secondary invariants of degree 8 one may take

$$\begin{aligned}
q_2 := \mathrm{cwe}(e_8 \otimes P) = x^8 + y^8 + z^8 + t^8 + 14(x^4y^4 + x^4z^4 + x^4t^4 + y^4z^4 \\
+ y^4t^4 + z^4t^4) + 168x^2y^2z^2t^2
\end{aligned}$$

(where $Z_2$ acts trivially on $e_8$) and the weight enumerator of a $Z_2$-structure of the indecomposable Type II code $d_{16}^+$ of length 16,

$$\begin{aligned}
q_3 = \mathrm{cwe}(d_{16}^+) &= x^8 + 4x^6t^2 + 2x^5y^2t + 8x^5yzt + 2x^5z^2t + 4x^4y^3z \\
&+ 4x^4y^2z^2 + 4x^4yz^3 + 6x^4t^4 + 4x^3y^2t^3 + 32x^3yzt^3 + 4x^3z^2t^3 + 8x^2y^4t^2 \\
&+ 16x^2y^3zt^2 + 24x^2y^2z^2t^2 + 16x^2yz^3t^2 + 8x^2z^4t^2 + 4x^2t^6 + 4xy^5zt \\
&+ 24xy^4z^2t + 8xy^3z^3t + 24xy^2z^4t + 2xy^2t^5 + 4xyz^5t + 8xyzt^5 + 2xz^2t^5 + 2y^7z \\
&+ 6y^5z^3 + 6y^3z^5 + 4y^3zt^4 + 4y^2z^2t^4 + 2yz^7 + 4yz^3t^4 + t^8.
\end{aligned}$$

A corresponding generator matrix is

$$\begin{bmatrix}
(1,0) & (0,0) & (0,1) & (0,0) & (0,0) & (0,1) & (0,0) & (0,1) \\
(0,1) & (0,0) & (1,0) & (0,0) & (0,0) & (0,1) & (0,0) & (0,1) \\
(0,0) & (1,0) & (1,1) & (0,1) & (0,0) & (0,0) & (1,1) & (1,1) \\
(0,0) & (0,1) & (1,1) & (0,1) & (0,0) & (0,1) & (1,1) & (1,0) \\
(0,0) & (0,0) & (0,0) & (1,1) & (0,0) & (0,1) & (0,0) & (0,1) \\
(0,0) & (0,0) & (0,0) & (0,0) & (1,0) & (0,1) & (0,1) & (0,1) \\
(0,0) & (0,0) & (0,0) & (0,0) & (0,1) & (0,1) & (1,0) & (0,1) \\
(0,0) & (0,0) & (0,0) & (0,0) & (0,0) & (1,1) & (0,0) & (1,1)
\end{bmatrix}$$

The automorphism group of the extended binary Golay code $\mathcal{G}_{24}$ has one conjugacy class of elements that are conjugate in $\mathrm{Sym}_{24}$ to

$a = (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18)(19,20)(21,22)(23,24)$

yielding an $\mathbb{F}_2 Z_2$-structure of $\mathcal{G}_{24}$ with generator matrix $(I_{12}, J)$ where

$$J := \begin{bmatrix} (1,0) & (1,1) & (1,0) & (1,1) & (0,0) & (0,1) \\ (0,1) & (1,1) & (0,1) & (1,1) & (0,0) & (1,0) \\ (1,1) & (1,0) & (0,1) & (0,0) & (1,1) & (1,0) \\ (1,1) & (0,1) & (1,0) & (0,0) & (1,1) & (0,1) \\ (0,0) & (1,1) & (1,0) & (1,0) & (1,1) & (1,0) \\ (0,0) & (1,1) & (0,1) & (0,1) & (1,1) & (0,1) \\ (1,0) & (0,1) & (1,1) & (0,1) & (1,0) & (1,0) \\ (0,1) & (1,0) & (1,1) & (1,0) & (0,1) & (0,1) \\ (0,1) & (1,0) & (1,0) & (0,1) & (1,0) & (1,1) \\ (1,0) & (0,1) & (0,1) & (1,0) & (0,1) & (1,1) \\ (1,1) & (0,0) & (0,1) & (1,1) & (1,0) & (0,1) \\ (1,1) & (0,0) & (1,0) & (1,1) & (0,1) & (1,0) \end{bmatrix}$$

whose complete weight enumerator yields the last generator

$$\begin{aligned} p_7 = {} & x^{12} + 15x^8t^4 + 14x^6y^4t^2 + 64x^6y^3zt^2 + 84x^6y^2z^2t^2 + 64x^6yz^3t^2 + 14x^6z^4t^2 \\ & + 32x^6t^6 + 4x^5y^6t + 40x^5y^5zt + 92x^5y^4z^2t + 112x^5y^3z^3t + 92x^5y^2z^4t + 40x^5yz^5t \\ & + 4x^5z^6t + x^4y^8 + 4x^4y^7z + 10x^4y^6z^2 + 28x^4y^5z^3 + 34x^4y^4z^4 + 28x^4y^4t^4 + 28x^4y^3z^5 \\ & + 128x^4y^3zt^4 + 10x^4y^2z^6 + 168x^4y^2z^2t^4 + 4x^4yz^7 + 128x^4yz^3t^4 + x^4z^8 + 28x^4z^4t^4 \\ & + 15x^4t^8 + 24x^3y^6t^3 + 112x^3y^5zt^3 + 296x^3y^4z^2t^3 + 416x^3y^3z^3t^3 + 296x^3y^2z^4t^3 \\ & + 112x^3yz^5t^3 + 24x^3z^6t^3 + 2x^2y^8t^2 + 24x^2y^7zt^2 + 76x^2y^6z^2t^2 + 168x^2y^5z^3t^2 \\ & + 180x^2y^4z^4t^2 + 14x^2y^4t^6 + 168x^2y^3z^5t^2 + 64x^2y^3zt^6 + 76x^2y^2z^6t^2 + 84x^2y^2z^2t^6 \\ & + 24x^2yz^7t^2 + 64x^2yz^3t^6 + 2x^2z^8t^2 + 14x^2z^4t^6 + 4xy^6t^5 + 40xy^5zt^5 + 92xy^4z^2t^5 \\ & + 112xy^3z^3t^5 + 92xy^2z^4t^5 + 40xyz^5t^5 + 4xz^6t^5 + 2y^10z^2 + 16y^8z^4 + y^8t^4 + 4y^7zt^4 \\ & + 28y^6z^6 + 10y^6z^2t^4 + 28y^5z^3t^4 + 16y^4z^8 + 34y^4z^4t^4 + 28y^3z^5t^4 + 2y^2z^10 + 10y^2z^6t^4 \\ & + 4yz^7t^4 + z^8t^4 + t^{12}. \end{aligned}$$

## 5. $\mathbb{F}_2 \operatorname{Sym}_3$

The group ring $\mathbb{F}_2 \operatorname{Sym}_3 = \mathbb{F}_2 Z_2 \oplus \mathbb{F}_2^{2\times 2}$ is the direct product of two blocks that are invariant under the canonical involution. The first block is already dealt with in Section 4. For the second block, we should note that the left modules of the matrix ring $R = \mathbb{F}_2^{2\times 2}$ are of the form $M = \mathbb{F}_2^{2\times 1} \otimes V$ for some $\mathbb{F}_2$-vector space $V$. The self-dual $R$-submodules of $M$ are of the form $\mathbb{F}_2^{2\times 1} \otimes C = C(2)$ for a self-dual binary code $C \leq V$. The associated Clifford-Weil group is the real Clifford group $\mathcal{C}_2(2_I)$ of genus 2 (see [7, Section 6.3]) of which the invariant ring is spanned by the genus 2 complete weight enumerators of the self-dual binary codes.

## 6. $\mathbb{F}_3 \operatorname{Sym}_3$

$\mathbb{F}_3 \operatorname{Sym}_3$ has 6 indecomposable modules:

$$S_+, S_-, V_+, V_- = V_+ \otimes S_-, P_+, P_- = P_+ \otimes S_-$$

where $S_+$ and $S_-$ are the two simple modules (with trivial character, respectively the signum character), $P_+$ and $P_-$ the two corresponding projective indecomposable modules, $P_+$ is just the natural permutation module of the symmetric group $\operatorname{Sym}_3$,

and $V_+ = P_+/\operatorname{soc}(P_+)$, $V_- = P_-/\operatorname{soc}(P_-)$ are the two indecomposables with composition length 2. Since $V_- \cong \operatorname{Hom}_{\mathbb{F}_3}(V_+, \mathbb{F}_3)$, both modules $V_+$ and $V_-$ do not carry a $\mathrm{Sym}_3$-invariant non-degenerate bilinear form. $\mathbb{F}_3\,\mathrm{Sym}_3$ acts on the simple modules $S_+$ and $S_-$ just as $\mathbb{F}_3$, so the self-dual codes in $S_+^N$ and $S_-^N$ are the self-dual ternary codes of length $N$. The corresponding Clifford-Weil group is described in [7, Section 7.4.1]. The self-dual codes in $P_+^N$ are the same as the ones in $P_-^N$, so it is enough to consider the representation $\rho_{P_+}$. The projective indecomposable $\mathrm{Sym}_3$-module $P_+$ is uniserial,

$$P_+ > J(P_+) > \operatorname{soc}(P_+) > 0$$

with composition factors $(S_+, S_-, S_+)$. The Clifford-Weil group $\mathcal{C}(P_+) \leq \mathrm{GL}_{27}(\mathbb{C})$ has order $2^8 3^9$. Its invariant ring is far from being a polynomial ring. The Molien series starts with

$$1 + 5\lambda^4 + 40\lambda^8 + 2321\lambda^{12} + 140997\lambda^{16} + \ldots = f(\lambda)/N(\lambda)$$

with

$$N(\lambda) = (1-\lambda^4)^5(1-\lambda^8)^4(1-\lambda^{12})^{12}(1-\lambda^{36})^6$$

and a positive polynomial $f$ of degree 376 with $f(1) > 10^{22}$. So it is hopeless to calculate the full invariant ring here. The 5 invariants of degree 4 are provided by the complete weight enumerators $p_1, \ldots, p_5$ of the codes $C_1, \ldots, C_5$ with generator matrices

$$\begin{bmatrix} (1,1,1) & (0,0,0) & (0,0,0) & (0,0,0) \\ (0,0,0) & (1,1,1) & (0,0,0) & (0,0,0) \\ (0,0,0) & (0,0,0) & (1,1,1) & (0,0,0) \\ (0,0,0) & (0,0,0) & (0,0,0) & (1,1,1) \\ (0,1,2) & (0,0,0) & (0,1,2) & (0,1,2) \\ (0,0,0) & (0,1,2) & (0,1,2) & (0,2,1) \end{bmatrix} \quad \begin{bmatrix} (1,1,1) & (1,1,1) & (1,1,1) & (1,1,1) \\ (1,1,1) & (0,0,0) & (0,0,0) & (2,2,2) \\ (0,0,0) & (1,1,1) & (0,0,0) & (2,2,2) \\ (1,0,0) & (1,0,0) & (0,0,0) & (1,0,0) \\ (0,1,2) & (0,0,0) & (0,1,2) & (0,2,1) \\ (0,0,0) & (0,1,2) & (0,2,1) & (0,2,1) \end{bmatrix}$$

$$\begin{bmatrix} (1,0,0) & (2,0,0) & (0,0,0) & (2,0,0) \\ (0,1,0) & (0,2,0) & (0,0,0) & (0,2,0) \\ (0,0,1) & (0,0,2) & (0,0,0) & (0,0,2) \\ (0,0,0) & (1,0,0) & (2,0,0) & (2,0,0) \\ (0,0,0) & (0,1,0) & (0,2,0) & (0,2,0) \\ (0,0,0) & (0,0,1) & (0,0,2) & (0,0,2) \end{bmatrix} \quad \begin{bmatrix} (1,0,0) & (2,0,0) & (0,0,0) & (2,0,0) \\ (0,1,0) & (0,2,0) & (0,0,0) & (0,2,0) \\ (0,0,1) & (0,0,2) & (0,0,0) & (0,0,2) \\ (0,0,0) & (0,0,0) & (1,1,1) & (0,0,0) \\ (1,2,0) & (0,0,0) & (0,2,1) & (1,2,0) \\ (0,1,2) & (0,0,0) & (0,2,1) & (0,1,2) \end{bmatrix}$$

$$\begin{bmatrix} (1,0,0) & (1,0,0) & (1,1,1) & (1,0,0) \\ (0,1,0) & (0,1,0) & (1,1,1) & (0,1,0) \\ (0,0,1) & (0,0,1) & (1,1,1) & (0,0,1) \\ (1,0,0) & (2,0,0) & (2,0,0) & (1,1,1) \\ (0,1,0) & (0,2,0) & (0,2,0) & (1,1,1) \\ (0,0,1) & (0,0,2) & (0,0,2) & (1,1,1) \end{bmatrix}$$

Imposing the additional condition that the codes contain the all-ones vector $\mathbf{1}$, one gets a Clifford-Weil group of order $2^8 3^{11}$ with Molien series

$$1 + 2\lambda^4 + 10\lambda^8 + 403\lambda^{12} + 16200\lambda^{16} + \ldots = g(\lambda)/N_1(\lambda)$$

with

$$N_1(\lambda) = (1-\lambda^4)^2(1-\lambda^8)^7(1-\lambda^{12})^{12}(1-\lambda^{36})^6$$

and a positive polynomial $g$ of degree 388 with $g(1) > 10^{22}$. The two invariants of degree 4 are $p_1$ and $p_2$.

## 7. $\mathbb{F}_3 Z_3$

$\mathbb{F}_3 Z_3$ has 3 indecomposable modules: the simple module $S \cong \mathbb{F}_3$, the projective module $P \cong \mathbb{F}_3 Z_3$ and $P/\operatorname{soc}(P) = V$ of composition length 2.

7.1. **The 3-dimensional module $P$.** The module $P$ is just the restriction of the $\mathbb{F}_3 \operatorname{Sym}_3$-module $P_+$ to $Z_3$. The associated Clifford-Weil group $\mathcal{C}(P)$ has order $2^5 3^5$ and Molien series starting with

$$1 + 37\lambda^4 + 9294\lambda^8 + \dots.$$

The additional condition that the codes contain the all-ones vector yields a Clifford-Weil group of order $2^5 3^7$ whose Molien series starts with

$$1 + 6\lambda^4 + 911\lambda^8 + 148842\lambda^{12} + \dots.$$

A system of representatives for the $\operatorname{Sym}_4$-equivalence classes of self-dual $\mathbb{F}_3 Z_3$-codes in $P^4$ may be calculated as follows.

An $\mathbb{F}_3 Z_3$-code $C$ in $P^4$ is a self-dual code in $\mathbb{F}_3^{12}$, with the additional property that $a := (1,2,3)(4,5,6)(7,8,9)(10,11,12)$ is contained in the permutation group $P(C)$ of $C$.

Up to monomial equivalence, there exist three self-dual codes in $\mathbb{F}_3^{12}$. Hence for each of these three codes $D$ we have to determine the set $\mathcal{G}_D := \{\pi \in \mathcal{M}on \mid a \in P(D\pi)\}$, where $\mathcal{M}on$ is the group of monomial permutations on twelve points. Since the condition $a \in P(D\pi)$ is equivalent with $\pi a \pi^{-1} \in \operatorname{Aut}(D)$, the set $\mathcal{G}_D$ can be determined with elementary calculations. Now $\mathcal{G}_D$ consists of right cosets of the subgroup

$$< (1,4)(2,5)(3,6), (1,4,7,10)(2,5,8,11)(3,6,9,12) > \cong \operatorname{Sym}_4$$

in $\mathcal{M}on$, hence may be reduced to a set of coset representatives. The union of the reduced sets $\mathcal{G}_D$ then yields a system of representatives for the $\operatorname{Sym}_4$-equivalence classes of self-dual $\mathbb{F}_3 Z_3$-codes in $P^4$, consisting of 48 codes.

Since it is hopeless to calculate generators for the invariant ring here, it is useful to apply the strategy described in Section 2.3 to obtain generators for the ring spanned by the $U$-symmetrized weight enumerators of the codes, where $U \cong Z_6$ is the full central unitary group of $(\mathbb{F}_3 Z_3, {}^-)$. $U$ preserves the composition series

$$P > V > S > 0$$

and has 3 orbits $X_3, X_4, X_5$ of length 6 on $P - V$ (distinguished by their Hamming weight) one orbit $X_2$ of length 6 on $V - S$, one orbit $X_1$ on $S - \{0\}$ and the orbit $X_0 = \{0\}$. The symmetrized Clifford-Weil group $\mathcal{C}^{(U)}(P)$ has order $2^4 3^4$ and Molien series starting with

$$1 + 3\lambda^4 + 9\lambda^8 + 34\lambda^{12} + \ldots = \frac{f}{g}$$

with

$$g(\lambda) = (1 - \lambda^{36})(1 - \lambda^{12})^2 (1 - \lambda^4)^3$$

and

$$f(\lambda) = \lambda^{60} + 5\lambda^{56} + 17\lambda^{52} + 18\lambda^{48} + 25\lambda^{44} + 25\lambda^{40} + 32\lambda^{36} + 26\lambda^{32} + 27\lambda^{28} + 31\lambda^{24} + 21\lambda^{20} + 11\lambda^{16} + 13\lambda^{12} + 3\lambda^8 + 1.$$

The 48 codes of length 4 yield four different symmetrized weight enumerators which generate the 3-dimensional space of invariants of degree 4.

$$x_0^4 + 72x_4x_3x_5(x_0 + x_1) + 24(x_0x_2^3 + x_1(2x_2^3 + x_3^3 + x_4^3 + x_5^3)) +$$
$$144x_2(x_3x_4^2 + x_3^2x_5 + x_4x_5^2) + 8x_0x_1^3,$$
$$x_0^4 + 24x_0(x_4^3 + x_3^3 + x_2^3 + x_5^3) + 144(x_2x_3x_4^2 + x_1x_3x_4x_5$$
$$+ x_2x_4x_5^2 + x_2x_3^2x_5) + 8x_0x_1^3 + 48x_1x_2^3,$$
$$x_0^4 + 8x_0^3x_1 + 24x_0^2x_1^2 + 216x_0x_2^3 + 32x_0x_1^3 + 432x_2^3x_1 + 16x_1^4,$$
$$x_0^4 + 2x_0^3x_1 + 6x_0(x_0x_1^2 + x_4^3 + x_3^3 + x_5^3) + +36(x_0 + 2x_1)(x_3x_4x_5 + 2x_2^3) +$$
$$12x_1(x_3^3 + x_4^3 + x_5^3) + 108x_2(x_3x_4^2 + x_4x_5^2 + x_3^2x_5) + 14x_0x_1^3 + 4x_1^4$$

7.2. **The 2-dimensional module $V$.** The 2-dimensional indecomposable $\mathbb{F}_3Z_3$-module $V$ has an $\mathbb{F}_3$-basis with respect to which $a$ acts as

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$$

and an $A$-invariant bilinear form with Gram matrix

$$F = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

There are no symmetric non-degenerated invariant forms on $V$, so here we need to work with $\mathcal{R}^-(\mathbb{F}_3Z_3)$ and $\epsilon = -1$. The associated Clifford-Weil group is isomorphic to $Z_2 \times Z_3 \times Z_3 \times \mathrm{Sym}_3$ of order 108. The Molien series is

$$d(\lambda)/n(\lambda) = 1 + \lambda + \lambda^2 + 7\lambda^3 + 11\lambda^4 + 11\lambda^5 + 49\lambda^6 + 91\lambda^7 + \dots$$

with denominator

$$n(\lambda) = (1 - \lambda)(1 - \lambda^3)^4(1 - \lambda^6)^4$$

and numerator

$$d(\lambda) = 2\lambda^{25} + 4\lambda^{24} + 18\lambda^{22} + 22\lambda^{21} + 16\lambda^{20} + 43\lambda^{19} + 65\lambda^{18} + 89\lambda^{17} +$$
$$83\lambda^{16} + 91\lambda^{15} + 123\lambda^{14} + 89\lambda^{13} + 78\lambda^{12} + 71\lambda^{11} + 59\lambda^{10} +$$
$$45\lambda^9 + 25\lambda^8 + 26\lambda^7 + 16\lambda^6 + 4\lambda^4 + 2\lambda^3 + 1$$

The invariant of degree 1 is of course the weight enumerator $p$ of the code $C_1 := C = \langle(1,1)\rangle \leq V$. There are 13 self-dual codes in $V^3$, one of which is $C^3$. The other yield 6 different weight enumerators providing in total seven invariants of degree 3, that are linearly independent. Generator matrices $(I_3|J_i)$ of 6 such codes with distinct weight enumerators are as follows:

$$J_1 = \begin{bmatrix} 2) & (0,2) \\ 1) & (2,0) \\ 1) & (2,2) \end{bmatrix}, \quad J_2 = \begin{bmatrix} 1) & (0,1) \\ 2) & (1,0) \\ 1) & (2,2) \end{bmatrix}, \quad J_3 = \begin{bmatrix} 1) & (2,0) \\ 2) & (2,1) \\ 1) & (2,2 \end{bmatrix},$$

$$J_4 = \begin{bmatrix} 2) & (1,2) \\ 1) & (0,2) \\ 1) & (1,1) \end{bmatrix}, \quad J_5 = \begin{bmatrix} 2) & (2,1) \\ 1) & (0,1) \\ 1) & (2,2) \end{bmatrix}, \quad J_6 = \begin{bmatrix} 2) & (1,0) \\ 1) & (1,2) \\ 1) & (2,2) \end{bmatrix}.$$

The submodule structure of $V$ is $V > S > 0$ with $S = \langle(1,1)\rangle$. So $V = X_0 \cup X_1 \cup X_2$ with $X_0 = \{(0,0)\}$, $X_1 = V - S = \{(1,0),(2,0),(0,1),(0,2),(1,2),(2,1)\}$, $X_2 = S - \{(0,0)\} = \{(1,1),(2,2)\}$. This partition of $V$ is the set of orbits of the central unitary group of the group ring and hence the corresponding symmetrization

commutes with the action of the Clifford-Weil group. The resulting symmetrized Clifford-Weil group is generated by

$$d := \mathrm{diag}(1, \zeta_3, 1) \text{ and } h = \begin{pmatrix} 1/3 & 2 & 2/3 \\ 1/3 & 0 & -1/3 \\ 1/3 & -1 & 2/3 \end{pmatrix}$$

has order 18 and is isomorphic to the complex reflection group $G = Z_3 \times \mathrm{Sym}_3$. All 12 codes of length 3 that are $\neq C^3$ have the same symmetrized weight enumerator

$$p_3 := x_0^3 + 6x_0x_2^2 + 18x_1^3 + 2x_2^3.$$

The invariant ring of $G$ is the polynomial ring $\mathbb{C}[p_1, p_3, p_6]$, where $p_1 := x_0 + 2x_2$ is the symmetrized weight enumerator of $C$ and

$$p_6 = x_0^6 + 30x_0^4x_2^2 + 40x_0^3x_2^3 + 90x_0^2x_2^4 + 60x_0x_2^5 + 486x_1^6 + 22x_2^6$$

the symmetrized weight enumerator of a suitable code of length 6, for instance $C_6$ with generator matrix

$$\begin{bmatrix} (1,0) & (0,2) & (0,2) & (0,2) & (0,2) & (1,0) \\ (0,1) & (0,1) & (0,1) & (0,1) & (0,1) & (1,2) \\ (0,0) & (1,1) & (0,0) & (0,0) & (0,0) & (2,2) \\ (0,0) & (0,0) & (1,1) & (0,0) & (0,0) & (2,2) \\ (0,0) & (0,0) & (0,0) & (1,1) & (0,0) & (2,2) \\ (0,0) & (0,0) & (0,0) & (0,0) & (1,1) & (2,2) \end{bmatrix}.$$

Continuing to symmetrize to obtain $V$-Hamming weight enumerators $q_i := p_i(x, y, y) = \mathrm{hwe}_V(C_i)$ we will not obtain an invariant ring of a group. The subgroup of $\mathrm{GL}_2(\mathbb{Q})$ that stabilizes $q_1$ and $q_3$ is of order 2 and its invariant ring is

$$\mathbb{C}[x + 2y, x^2 + 8y^2]$$

which properly contains the ring spanned by $q_1, q_3$ and

$$q_6 = (\frac{1}{3}q_1^9q_3 - \frac{1}{2}q_1^6q_3^2 + q_1^3q_3^3 + \frac{1}{6}q_3^4)/(q_1^3q_3).$$

This shows that the assumption that the symmetrization commutes with the action of the Clifford-Weil group is necessary.

## References


[1] Stefka Bouyuklieva, Some results on Type IV codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory 48 (March 2002) 768-773.

[2] S. Dougherty, P. Gaborit, M. Harada, A. Munemasa, P. Solé, Type IV self-dual codes over rings. IEEE Trans. Inf. Theory 45 (Nov. 1999) 2345-2360.

[3] A. Günther, Self-dual group ring codes, PhD Thesis, RWTH Aachen University (in preparation).

[4] M. Kneser, Klassenzahlen definiter quadratischer Formen, Archiv der Math. 8 (1957) 241–250.

[5] J. Morales, Maximal hermitian forms over $\mathbb{Z}G$. Comment. Math. Helvetici 63 (1988) 209–225.

[6] G. Nebe, Kneser-Hecke-operators in coding theory. Abh. Math. Sem. Univ. Hamburg 76 (2006) 79–90.

[7] G. Nebe, E. Rains, N. Sloane, *Self-dual codes and invariant theory*. Springer (2006)

[8] *The Magma Computational Algebra System for Algebra, Number Theory and Geometry*. available via the magma home page http://www.maths.usyd.edu.au:8000/u/magma/

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 199–213
ISSN 1930-1235: (2008)

# DETERMINING EQUATIONS OF FAMILIES OF CYCLIC CURVES

R. Sanjeewa

*Department of Mathematics and Statistics*
*Oakland University,*
*Rochester, MI, 48309.*
*rsanjeew@oakland.edu*

T. Shaska

*Department of Mathematics*
*University of Vlora,*
*Vlora, Albania*
*shaska@univlora.edu.al*

Abstract. In previous work we determined automorphism groups of cyclic algebraic curves defined over fields of any odd characteristic. In this paper we determine parametric equations of families of curves for each automorphism group for such curves.

## 1. Introduction

Let $\mathcal{X}_g$ be an algebraic curve of genus $g \geq 2$ defined over a algebraically closed field of characteristic $p \neq 2$. If an automorphism group of a algebraic curve has normal cyclic subgroup such that the quotient space has genus zero, then such a curve is called a *cyclic curve*. We have studied automorphism groups of *cyclic curves* in [29], where we have listed all automorphism groups as well as ramification signatures of corresponding covers. In this paper we give a corresponding parametric equation for each family in [29].

In the second section we briefly introduce basic facts on cyclic curves and their automorphism. Let $G = \mathrm{Aut}(\mathcal{X}_g)$ automorphism group of given cyclic curve $\mathcal{X}_g$, the reduced automorphism group is $\bar{G} := \mathrm{Aut}(\mathcal{X}_g)/\langle w \rangle$, where $C_n = \langle w \rangle$ such that $g(\mathcal{X}^{C_n}) = 0$. This group $\bar{G}$ is embedded in $PGL_2(k)$ and therefore is isomorphic to one of $C_m$, $D_m$, $A_4$, $S_4$, $A_5$, *a semi direct product of elementary Abelian group with cyclic group*, $PSL(2,q)$, or $PGL(2,q)$. Then, $\bar{G}$ acts on a genus 0 field $k(x)$. We determine a rational function $\phi(x)$ that generates the fixed field $k(x)^{\bar{G}}$ in all cases cf. Lemma 1.

In section three, we determine the ramification signature $\sigma$ of the cover $\Phi(x) : \mathcal{X}_g \to \mathbb{P}^1$ with monodromy group $G := \mathrm{Aut}(\mathcal{X}_g)$. Moduli spaces of covers $\Phi$ are

2000 *Mathematics Subject Classification.* Primary: 14Hxx, Secondary: 14H37, 14H10,
*Key words and phrases.* algebraic curves, Hurwitz spaces, equations.
Both authors were supported by a NATO grant, ICS. EAP. ASI No 982903.

Hurwitz spaces, which we denoted by $\mathcal{H}_\sigma$. There is a map $\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$, where $\mathcal{M}_g$ is the moduli space of genus $g$ algebraic curves. The image of this map is a subvariety of $\mathcal{M}_g$, which we denoted by $\mathcal{H}(G,\sigma)$. The dimension of $\mathcal{H}(G,\sigma)$ is determined. Hence, we have

$$\mathcal{X}_g \xrightarrow{C_n} \mathbb{P}^1 \xrightarrow{\bar{G}} \mathbb{P}^1$$

We list all possible automorphism groups, their signatures, and dimension of the loci $\mathcal{H}(G,\sigma)$.

In the last section, we determine the equations of families of curves for a given group. Using the rational function $\phi(x)$ we are able to determine parametric equation of each family $\mathcal{H}(G,\sigma)$. Since we know $\phi(x)$, we can find the branch points and then determine the equation of the curve from these branch points. We list corresponding equations of families of curves which we have listed in section three.

Throughout this paper we let $g \geq 2$ be a fixed integer, $\mathcal{X}$ a genus $g$ cyclic curve, $G = \mathrm{Aut}(\mathcal{X})$ and $C_n \triangleleft G$ such that $g(\mathcal{X}^{C_n}) = 0$.

## 2. Preliminaries

Let $\mathcal{X}_g$ be genus $g \geq 2$ cyclic curve defined over an algebraically closed field $k$ of characteristic $p \neq 2$. We take the equation of $\mathcal{X}_g$ to be $y^n = F(x)$, where $deg(F) = 2g+2$. Let $K := k(x,y)$ be the function field of $\mathcal{X}_g$. Then $K$ is a degree $n$ extension field of $k(x)$ ramified exactly at $d = 2g+2$ places $\alpha_1, ..., \alpha_d$ of $k(x)$.

Let $G = Aut(K/k)$. Since $k(x)$ is the only genus 0 subfield of degree $n$ of $K$, then $G$ fixes $k(x)$. Thus $Gal(K/k(x)) = \langle w \rangle$, with $w^n = 1$. Then the group $\bar{G} := G/\langle w \rangle$ is called *reduced automorphism group*. By the theorem of Dickson, $\bar{G}$ is isomorphic to one of the following: $C_m$, $D_m$, $A_4$, $S_4$, $A_5$, $PSL(2,q)$ and $PGL(2,q)$, or a semi direct product of elementary Abelian group with cyclic group, defined as

$$K_m := \langle \{\sigma_a, t | a \in \mathcal{U}_m\} \rangle, \quad \textit{where } \mathcal{U}_m := \{a \in k | (a \prod_{j=0}^{\frac{p^t-1}{m}-1} (a^m - b_j)) = 0\}$$

and $t(x) = \xi^2 x, \quad \sigma_a(x) = x + a$, for each $a \in \mathcal{U}$, $b_j \in k^*$ and $\xi$ is a primitive $2m$-th root of unity; see [10]. $\mathcal{U}_m$ is a subgroup of the additive group of $k$.

The group $\bar{G}$ acts on $k(x)$ via the natural way. The fixed field is a genus 0 field, say $k(z)$. Thus $z$ is a degree $|\bar{G}|$ rational function in $x$, say $z = \phi(x)$. The following lemma determines rational functions for all $\bar{G}$; see [29].

Let $\phi_0 : \mathcal{X}_g \to \mathbb{P}^1$ and $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be covers which correspond to the extensions $K/k(x)$ and $k(x)/k$ respectively. Then, $\psi := \phi \circ \phi_0$ has monodromy group $G := Aut(\mathcal{X}_g)$. By basic covering theory, the group $G$ is embedded in the group $S_l$, where $l = deg(\psi)$. There is an $r$-tuple $\overline{\sigma} := (\sigma_1, ..., \sigma_r)$, where $\sigma_i \in S_l$ such that $\sigma_1, ..., \sigma_r$ generate $G$ and $\sigma_1 ... \sigma_r = 1$. The signature of $\Phi$ is an $r$-tuple of conjugacy classes $\mathcal{C} := (C_1, ..., C_r)$ in $S_l$ such that $C_i$ is the conjugacy class of $\sigma_i$. We can find the signature of $\psi_0 : \mathcal{X}_g \to \mathbb{P}^1$ by using the signature of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ and Riemann-Hurwitz formula.

Moduli spaces of covers $\psi$ are Hurwitz space, which we denoted by $\mathcal{H}_\sigma$. There is a map $\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$, where $\mathcal{M}_g$ is the moduli space of genus $g$ algebraic curves. The image of this map is a subvariety of $\mathcal{M}_g$, which we denoted by $\mathcal{H}(G,\sigma)$. Using the signature of $\psi$ and Riemann-Hurwitz formula, one can find out dimension of $\mathcal{H}(G,\sigma)$, which we denoted by $\delta$.

We summarize all in the following Lemma:

**Lemma 1.** *Let $k$ be an algebraically closed field of characteristic $p$, $H_t$ a subgroup of the additive group of $k$ with $|H_t| = p^t$ and $b_j \in k^*$, and $\bar{G}$ be a finite subgroup of $PGL_2(k)$ acting on the field $k(x)$. Then, $\bar{G}$ is isomorphic to one of the following groups $C_m$, $D_m$, $A_4$, $S_4$, $A_5$, $U = C_p^t$, $K_m$, $PSL_2(q)$ and $PGL_2(q)$, where $q = p^f$ and $(m,p) = 1$. Moreover, the fixed subfield $k(x)^{\bar{G}} = k(z)$ is given by Table 1, where $\alpha = \frac{q(q-1)}{2}$, $\beta = \frac{q+1}{2}$.*

| *Case* | $\bar{G}$ | $z$ | *Ramification* |
|---|---|---|---|
| 1 | $C_m$, $(m,p)=1$ | $x^m$ | $(m,m)$ |
| 2 | $D_{2m}$, $(m,p)=1$ | $x^m + \frac{1}{x^m}$ | $(2,2,m)$ |
| 3 | $A_4$, $p \neq 2,3$ | $\frac{x^{12}-33x^8-33x^4+1}{x^2(x^4-1)^2}$ | $(2,3,3)$ |
| 4 | $S_4$, $p \neq 2,3$ | $\frac{(x^8+14x^4+1)^3}{108(x(x^4-1))^4}$ | $(2,3,4)$ |
| 5 | $A_5$, $p \neq 2,3,5$ | $\frac{(-x^{20}+228x^{15}-494x^{10}-228x^5-1)^3}{(x(x^{10}+11x^5-1))^5}$ | $(2,3,5)$ |
| | $A_5$, $p=3$ | $\frac{(x^{10}-1)^6}{(x(x^{10}+2ix^5+1))^5}$ | $(6,5)$ |
| 6 | $U$ | $\prod_{a\in H_t}(x+a)$ | $(p^t)$ |
| 7 | $K_m$ | $(x\prod_{j=0}^{\frac{p^t-1}{m}-1}(x^m-b_j))^m$ | $(mp^t,m)$ |
| 8 | $PSL(2,q)$, $p\neq 2$ | $\frac{((x^q-x)^{q-1}+1)^{\frac{q+1}{2}}}{(x^q-x)^{\frac{q(q-1)}{2}}}$ | $(\alpha,\beta)$ |
| 9 | $PGL(2,q)$ | $\frac{((x^q-x)^{q-1}+1)^{q+1}}{(x^q-x)^{q(q-1)}}$ | $(2\alpha,2\beta)$ |

TABLE 1. Rational functions correspond to each $\bar{G}$

## 3. Automorphism groups and their signatures of cyclic curves

As above $\bar{G} := G/G_0$, where $G_0 := Gal(k(x,y)/k(x))$. The following theorem determines ramification signatures and dimensions of $\delta$ of $\mathcal{H}(G,\sigma)$ for all $\bar{G}$ when $p > 5$; see [29] for details.

**Theorem 3.1.** *The signature of cover $\Phi(x) : \mathcal{X} \to \mathcal{X}^G$ and dimension $\delta$ is given in Table 2. In Table 2, $m = |PSL_2(q)|$ for cases 38-41 and $m = |PGL_2(q)|$ for cases 42-45.*

| # | $G$ | $\delta(G,C)$ | $\delta, n, g$ | $\mathcal{C} = (C_1, ..., C_r)$ |
|---|---|---|---|---|
| 1 | $(p,m)=1$ | $\frac{2(g+n-1)}{m(n-1)} - 1$ | $n < g+1$ | $(m, m, n, ..., n)$ |
| 2 | $C_m$ | $\frac{2g+n-1}{m(n-1)} - 1$ | | $(m, mn, n, ..., n)$ |
| 3 | | $\frac{2g}{m(n-1)} - 1$ | $n < g$ | $(mn, mn, n, ..., n)$ |
| 4 | $(p,m)=1$ | $\frac{g+n-1}{m(n-1)}$ | | $(2, 2, m, n, ..., n)$ |
| 5 | | $\frac{2g+m+2n-nm-2}{2m(n-1)}$ | | $(2n, 2, m, n, ..., n)$ |
| 6 | $D_{2m}$ | $\frac{g}{m(n-1)}$ | | $(2, 2, mn, n, ..., n)$ |
| 7 | | $\frac{g+m+n-mn-1}{m(n-1)}$ | $n < g+1$ | $(2n, 2n, m, n, ..., n)$ |
| 8 | | $\frac{2g+m-mn}{2m(n-1)}$ | $g \neq 2$ | $(2n, 2, mn, n, ..., n)$ |
| 9 | | $\frac{g+m-mn}{m(n-1)}$ | $n < g$ | $(2n, 2n, mn, n, ..., n)$ |
| 10 | | $\frac{n+g-1}{6(n-1)}$ | | $(2, 3, 3, n, ..., n)$ |
| 11 | $A_4$ | $\frac{g-n+1}{6(n-1)}$ | | $(2, 3n, 3, n, ..., n)$ |
| 12 | | $\frac{g-3n+3}{6(n-1)}$ | | $(2, 3n, 3n, n, ..., n)$ |
| 13 | | $\frac{g-2n+2}{6(n-1)}$ | $\delta \neq 0$ | $(2n, 3, 3, n, ..., n)$ |
| 14 | | $\frac{g-4n+4}{6(n-1)}$ | | $(2n, 3n, 3, n, ..., n)$ |
| 15 | | $\frac{g-6n+6}{6(n-1)}$ | $\delta \neq 0$ | $(2n, 3n, 3n, n, ..., n)$ |
| 16 | | $\frac{g+n-1}{12(n-1)}$ | | $(2, 3, 4, n, ..., n)$ |
| 17 | | $\frac{g-3n+3}{12(n-1)}$ | | $(2, 3n, 4, n, ..., n)$ |
| 18 | | $\frac{g-2n+2}{12(n-1)}$ | | $(2, 3, 4n, n, ..., n)$ |
| 19 | | $\frac{g-6n+6}{12(n-1)}$ | | $(2, 3n, 4n, n, ..., n)$ |
| 20 | $S_4$ | $\frac{g-5n+5}{12(n-1)}$ | | $(2n, 3, 4, n, ..., n)$ |
| 21 | | $\frac{g-9n+9}{12(n-1)}$ | | $(2n, 3n, 4, n, ..., n)$ |
| 22 | | $\frac{g-8n+8}{12(n-1)}$ | | $(2n, 3, 4n, n, ..., n)$ |
| 23 | | $\frac{g-12n+12}{12(n-1)}$ | | $(2n, 3n, 4n, n, ..., n)$ |
| 24 | | $\frac{g+n-1}{30(n-1)}$ | | $(2, 3, 5, n, ..., n)$ |
| 25 | | $\frac{g-5n+5}{30(n-1)}$ | | $(2, 3, 5n, n, ..., n)$ |
| 26 | | $\frac{g-15n+15}{30(n-1)}$ | | $(2, 3n, 5n, n, ..., n)$ |
| 27 | | $\frac{g-9n+9}{30(n-1)}$ | | $(2, 3n, 5, n, ..., n)$ |
| 28 | $A_5$ | $\frac{g-14n+14}{30(n-1)}$ | | $(2n, 3, 5, n, ..., n)$ |
| 29 | | $\frac{g-20n+20}{30(n-1)}$ | | $(2n, 3, 5n, n, ..., n)$ |
| 30 | | $\frac{g-24n+24}{30(n-1)}$ | | $(2n, 3n, 5, n, ..., n)$ |
| 31 | | $\frac{g-30n+30}{30(n-1)}$ | | $(2n, 3n, 5n, n, ..., n)$ |
| 32 | | $\frac{2g+2n-2}{p^t(n-1)} - 2$ | | $(p^t, n, ..., n)$ |
| 33 | $U$ | $\frac{2g+np^t-p^t}{p^t(n-1)} - 2$ | $(n,p)=1, n\|p^t - 1$ | $(np^t, n, ..., n)$ |
| 34 | | $\frac{2(g+n-1)}{mp^t(n-1)} - 1$ | $(m,p)=1, m\|p^t - 1$ | $(mp^t, m, n, ..., n)$ |
| 35 | | $\frac{2g+2n+p^t-np^t-2}{mp^t(n-1)} - 1$ | $(m,p)=1, m\|p^t - 1$ | $(mp^t, nm, n, ..., n)$ |
| 36 | $K_m$ | $\frac{2g+np^t-p^t}{mp^t(n-1)} - 1$ | $(nm,p)=1, nm\|p^t - 1$ | $(nmp^t, m, n, ..., n)$ |
| 37 | | $\frac{2g}{mp^t(n-1)} - 1$ | $(nm,p)=1, nm\|p^t - 1$ | $(nmp^t, nm, n, ..., n)$ |
| 38 | | $\frac{2(g+n-1)}{m(n-1)} - 1$ | $\left(\frac{q-1}{2}, p\right) = 1$ | $(\alpha, \beta, n, ..., n)$ |
| 39 | $PSL_2(q)$ | $\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)} - 1$ | $\left(\frac{q-1}{2}, p\right) = 1$ | $(\alpha, n\beta, n, ..., n)$ |
| 40 | | $\frac{2g+nq(q-1)+q-q^2}{m(n-1)} - 1$ | $\left(\frac{n(q-1)}{2}, p\right) = 1$ | $(n\alpha, \beta, n, ..., n)$ |
| 41 | | $\frac{2g}{m(n-1)} - 1$ | $\left(\frac{n(q-1)}{2}, p\right) = 1$ | $(n\alpha, n\beta, n, ..., n)$ |
| 42 | | $\frac{2(g+n-1)}{m(n-1)} - 1$ | $(q-1,p)=1$ | $(2\alpha, 2\beta, n, ..., n)$ |
| 43 | $PGL_2(q)$ | $\frac{2g+q(q-1)-n(q+1)(q-2)-2}{m(n-1)} - 1$ | $(q-1,p)=1$ | $(2\alpha, 2n\beta, n, ..., n)$ |
| 44 | | $\frac{2g+nq(q-1)+q-q^2}{m(n-1)} - 1$ | $(n(p-1),p)=1$ | $(2n\alpha, 2\beta, n, ..., n)$ |
| 45 | | $\frac{2g}{m(n-1)} - 1$ | $(n(q-1),p)=1$ | $(2n\alpha, 2n\beta, n, ..., n)$ |

TABLE 2. The signature of curves and dimensions $\delta$ for char $> 5$

**Remark 1.** *The above theorem gives signatures and dimensions for $p > 5$. We know that $\bar{G} \cong C_m, D_m, A_4, S_4, U, K_m, PSL(2,q), PGL(2,q)$ when $p = 5$ and $\bar{G} \cong C_m, D_m, A_5, U, K_m, PSL(2,q), PGL(2,q)$ when $p = 3$; see [10]. All cases except $\bar{G} \cong A_5$ have ramification as $p > 5$. Hence signatures and dimensions are the same as $p > 5$. However, $\bar{G} \cong A_5$ has different ramification. Hence, that case has signatures and dimensions as in Table 3.*

| *Case* | $G$ | $\delta(G,C)$ | $\mathcal{C} = (C_1, ..., C_r)$ |
|---|---|---|---|
| $a$ | $A_5$ | $\frac{g+n-1}{30(n-1)} - 1$ | $(6, 5, n, ..., n)$ |
| $b$ | | $\frac{g+5n-5}{30(n-1)} - 1$ | $(6, 5n, n, ..., n)$ |
| $c$ | | $\frac{g+6n-6}{30(n-1)} - 1$ | $(6n, 5, n, ..., n)$ |
| $d$ | | $\frac{g}{30(n-1)} - 1$ | $(6n, 5n, n, ..., n)$ |

TABLE 3. The signature of curve and dimension $\delta$ for $\bar{G} \cong A_5$, $p = 3$

The following theorem determines the list of all automorphism groups of cyclic algebraic curves defined over any algebraically closed field of characteristic $p \neq 2$, details will be provided in [29].

**Theorem 3.2.** *Let $\mathcal{X}_g$ be a genus $g \geq 2$ irreducible cyclic curve defined over an algebraically closed field $k$ of characteristic char $(k) = p$, $G = Aut(\mathcal{X}_g)$, and $\bar{G}$ its reduced automorphism group. If $|G| > 1$ then is $G$ is one of the following:*

(1) *$\bar{G} \cong C_m$: Then, $G \cong C_{mn}$ or $\langle r, s |\, r^n = 1, s^m = 1, srs^{-1} = r^l \rangle$, $(l, n) = 1$ and $l^m \equiv 1$ (mod $n$).*

(2) *If $\bar{G} \cong D_{2m}$ then $G \cong D_{2m} \times C_n$ or*

$G'_4 = \langle r, s, t |\, r^n = 1, s^2 = 1, t^2 = 1, (st)^m = 1, srs^{-1} = r^l, trt^{-1} = r^l \rangle$

$G'_7 = \langle r, s, t |\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^2 = r^{\frac{n}{2}}, (st)^m = 1, srs^{-1} = r^l, trt^{-1} = r^l \rangle$

*where $(l, n) = 1$ and $l^2 \equiv 1$ (mod $n$) or*

$G_4 = \langle r, s, t |\, r^n = 1, s^2 = 1, t^2 = 1, (st)^m = 1, srs^{-1} = r^l, trt^{-1} = r^k \rangle$

$G_5 = \langle r, s, t |\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^2 = 1, (st)^m = 1, srs^{-1} = r^l, trt^{-1} = r^k \rangle$

$G_6 = \langle r, s, t |\, r^n = 1, s^2 = 1, t^2 = 1, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r^k \rangle$

$G_7 = \langle r, s, t |\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^2 = r^{\frac{n}{2}}, (st)^m = 1, srs^{-1} = r^l, trt^{-1} = r^k \rangle$

$G_8 = \langle r, s, t |\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^2 = 1, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r^k \rangle$

$G_9 = \langle r, s, t |\, r^n = 1, s^2 = r^{\frac{n}{2}}, t^2 = r^{\frac{n}{2}}, (st)^m = r^{\frac{n}{2}}, srs^{-1} = r^l, trt^{-1} = r^k \rangle$

*where $(l, n) = 1$ and $l^2 \equiv 1$ (mod $n$), $(k, n) = 1$ and $k^2 \equiv 1$ (mod $n$).*

(3) *If $\bar{G} \cong A_4$ and $p \neq 2, 3$ then $G \cong A_4 \times C_n$ or*

$G'_{10} = \langle r, s, t |\, r^n = 1, s^2 = 1, t^3 = 1, (st)^3 = 1, srs^{-1} = r, trt^{-1} = r^l \rangle$

$G'_{12} = \langle r, s, t |\, r^n = 1, s^2 = 1, t^3 = r^{\frac{n}{3}}, (st)^3 = r^{\frac{n}{3}}, srs^{-1} = r, trt^{-1} = r^l \rangle$

*where $(l, n) = 1$ and $l^3 \equiv 1$ (mod $n$) or*

$$\langle r,s,t|\, r^n=1, s^2=r^{\frac{n}{2}}, t^3=r^{\frac{n}{2}}, (st)^5=r^{\frac{n}{2}}, srs^{-1}=r, trt^{-1}=r\rangle, \text{ or}$$

$$G_{10}=\langle r,s,t|\, r^n=1, s^2=1, t^3=1, (st)^3=1, srs^{-1}=r, trt^{-1}=r^k\rangle$$

$$G_{13}=\langle r,s,t|\, r^n=1, s^2=r^{\frac{n}{2}}, t^3=1, (st)^3=1, srs^{-1}=r, trt^{-1}=r^k\rangle$$

*where* $(k,n)=1$ *and* $k^3\equiv 1$ *(mod n).*

(4) *If* $\bar{G}\cong S_4$ *and* $p\neq 2,3$ *then* $G\cong S_4\times C_n$ *or*

$$G_{16}=\langle r,s,t|\, r^n=1, s^2=1, t^3=1, (st)^4=1, srs^{-1}=r^l, trt^{-1}=r\rangle$$

$$G_{18}=\langle r,s,t|\, r^n=1, s^2=1, t^3=1, (st)^4=r^{\frac{n}{2}}, srs^{-1}=r^l, trt^{-1}=r\rangle$$

$$G_{20}=\langle r,s,t|\, r^n=1, s^2=r^{\frac{n}{2}}, t^3=1, (st)^4=1, srs^{-1}=r^l, trt^{-1}=r\rangle$$

$$G_{22}=\langle r,s,t|\, r^n=1, s^2=r^{\frac{n}{2}}, t^3=1, (st)^4=r^{\frac{n}{2}}, srs^{-1}=r^l, trt^{-1}=r\rangle$$

*where* $(l,n)=1$ *and* $l^2\equiv 1$ *(mod n).*

(5) *If* $\bar{G}\cong A_5$ *and* $p\neq 2,5$ *then* $G\cong A_5\times C_n$ *or*

$$\langle r,s,t|\, r^n=1, s^2=r^{\frac{n}{2}}, t^3=r^{\frac{n}{2}}, (st)^5=r^{\frac{n}{2}}, srs^{-1}=r, trt^{-1}=r\rangle$$

(6) *If* $\bar{G}\cong U$ *then* $G\cong U\times C_n$ *or*

$$\langle r,s_1,s_2,...,s_t|r^n=s_1^p=s_2^p=...=s_t^p=1, s_is_j=s_js_i, s_irs_i^{-1}=r^l, 1\leq i,j\leq t\rangle$$

*where* $(l,n)=1$ *and* $l^p\equiv 1$ *(mod n).*

(7) *If* $\bar{G}\cong K_m$ *then* $G\cong <r,s_1,...,s_t,v|r^n=s_1^p=...=s_t^p=v^m=1, s_is_j=s_js_i, vrv^{-1}=r, s_irs_i^{-1}=r^l, s_ivs_i^{-1}=v^k, 1\leq i,j\leq t>$ *where* $(l,n)=1$ *and* $l^p\equiv 1$ *(mod n),* $(k,m)=1$ *and* $k^p\equiv 1$ *(mod m) or*

$$G_{35}=\langle r,s_1,...,s_t|r^{nm}=s_1^p=...=s_t^p=1, s_is_j=s_js_i, s_irs_i^{-1}=r^l, 1\leq i,j\leq t\rangle$$

*where* $(l,nm)=1$ *and* $l^p\equiv 1(\mod nm)$.

(8) *If* $\bar{G}\cong PSL_2(q)$ *then* $G\cong PSL_2(q)\times C_n$ *or* $SL_2(3)$.

(9) *If* $\bar{G}\cong PGL(2,q)$ *then* $G\cong PGL(2,q)\times C_n$.

*Proof.* See [29]. □

## 4. Equations of curves

The group $\bar{G}$ is the monodromy group of the cover $\phi:\mathbb{P}^1\to\mathbb{P}^1$ with signature $(\sigma_1,\sigma_2,\sigma_3)$ as in section 2. We fix coordinates in $\mathbb{P}^1$ as $x$ and $z$ respectively and from now on we denote the cover $\phi:\mathbb{P}^1_x\to\mathbb{P}^1_z$. Thus, $z$ is a rational function in $x$ of the degree $|\bar{G}|$. We denote by $q_1,q_2,q_3$ corresponding branch points of $\phi$. Let $S$ be the set of branch points of $\Phi:\mathcal{X}_g\to\mathbb{P}^1_z$. Clearly $q_1,q_2,q_3\in S$. Let $y^n=f(x)$ be the equation of $\mathcal{X}_g$ and $W$ be the images in $\mathbb{P}^1_x$ of roots of $f(x)$ and

$$V:=\bigcup_{i=1}^{3}\phi^{-1}(q_i).$$

Let

$$z = \frac{\Psi(x)}{\Upsilon(x)}, \text{ where } \Psi(x), \Upsilon(x) \in k[x].$$

Then we have

$$z - q_i = \frac{\Gamma(x)}{\Upsilon(x)}$$

for each branch point $q_i$, $i = 1, 2, 3$, where $\Gamma(x) \in k[x]$. Hence,

$$\Gamma(x) = \Psi(x) - q_i \cdot \Upsilon(x)$$

is degree $|\bar{G}|$ equation and multiplicity of all roots of $\Gamma(x)$ correspond to the ramification index for each $q_i$. Now we define the following three functions:

$$\begin{aligned} \varphi^r(x) &:= \Psi(x) - q_1 \cdot \Upsilon(x) \\ \chi^s(x) &:= \Psi(x) - q_2 \cdot \Upsilon(x) \\ \psi^t(x) &:= \Psi(x) - q_3 \cdot \Upsilon(x) \end{aligned} \tag{1}$$

where superscript denote the ramification index of $q_i$. Clearly, $\phi^{-1}(S \backslash \{q_1, q_2, q_3\}) \subset W$. Let $\lambda \in \mathrm{S} \setminus \{q_1, q_2, q_2\}$. The points in the fiber $\phi^{-1}(\lambda)$ are the roots of the equation:

$$\Psi(x) - \lambda \cdot \Upsilon(x) = 0 \tag{2}$$

Let

$$G(x) := \prod_{\lambda \in S \backslash \{q_1, q_2, q_2\}} (\Psi(x) - \lambda \cdot \Upsilon(x)) \tag{3}$$

There are following cases and corresponding equations of the curve $y^n = f(x)$ for each fixed $\phi$.

| | Intersection | $f(x)$ |
|---|---|---|
| 1) | $V \cap W = \emptyset$ | $G(x)$ |
| 2) | $V \cap W = \phi^{-1}(q_1)$ | $\varphi(x) \cdot G(x)$ |
| 3) | $V \cap W = \phi^{-1}(q_2)$ | $\chi(x) \cdot G(x)$ |
| 4) | $V \cap W = \phi^{-1}(q_3)$ | $\psi(x) \cdot G(x)$ |
| 5) | $V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_2)$ | $\varphi(x) \cdot \chi(x) \cdot G(x)$ |
| 6) | $V \cap W = \phi^{-1}(q_2) \cup \phi^{-1}(q_3)$ | $\chi(x) \cdot \psi(x) \cdot G(x)$ |
| 7) | $V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_3)$ | $\varphi(x) \cdot \psi(x) \cdot G(x)$ |
| 8) | $V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_2) \cup \phi^{-1}(q_3)$ | $\varphi(x) \cdot \chi(x) \cdot \psi(x) \cdot G(x)$ |

The following theorem gives us equations of families of curves for automorphism groups which are related to Theorem 3.1 and Theorem 3.2.

**Theorem 4.1.** *Let $\mathcal{X}_g$ be a genus $g \geq 2$ cyclic curve with $Aut(\mathcal{X}_g) = G$, where $G$ is related to the cases 1-45 in Table 2. Then $\mathcal{X}_g$ has an equation as cases 1-45 in Table 4.*

**Proof:** We consider all cases one by one for the reduced automorphism group $\bar{G}$.

| # | $G$ | $y^n = f(x)$ |
|---|---|---|
| 1 | $C_m$ | $x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1$ |
| 2 | | $x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1$ |
| 3 | | $x(x^{m\delta} + a_1 x^{m(\delta-1)} + \cdots + a_\delta x^m + 1)$ |
| 4 | $D_{2m}$ | $F(x) := \prod_{i=1}^{\delta}(x^{2m} + \lambda_i x^m + 1)$ |
| 5 | | $(x^m - 1) \cdot F(x)$ |
| 6 | | $x \cdot F(x)$ |
| 7 | | $(x^{2m} - 1) \cdot F(x)$ |
| 8 | | $x(x^m - 1) \cdot F(x)$ |
| 9 | | $x(x^{2m} - 1) \cdot F(x)$ |
| 10 | $A_4$ | $G(x) := \prod_{i=1}^{\delta}(x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1)$ |
| 11 | | $(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$ |
| 12 | | $(x^8 + 14x^4 + 1) \cdot G(x)$ |
| 13 | | $x(x^4 - 1) \cdot G(x)$ |
| 14 | | $x(x^4 - 1)(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$ |
| 15 | | $x(x^4 - 1)(x^8 + 14x^4 + 1) \cdot G(x)$ |
| 16 | $S_4$ | $M(x)$ |
| 17 | | $S(x) \cdot M(x)$ |
| 18 | | $T(x) \cdot M(x)$ |
| 19 | | $S(x) \cdot T(x) \cdot M(x)$ |
| 20 | | $R(x) \cdot M(x)$ |
| 21 | | $R(x) \cdot S(x) \cdot M(x)$ |
| 22 | | $R(x) \cdot T(x) \cdot M(x)$ |
| 23 | | $R(x) \cdot S(x) \cdot T(x).M(x)$ |
| 24 | $A_5$ | $\Lambda(x)$ |
| 25 | | $(x(x^{10} + 11x^5 - 1)) \cdot \Lambda(x)$ |
| 26 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \Lambda(x)$ |
| 27 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \Lambda(x)$ |
| 28 | | $Q(x) \cdot \Lambda(x)$ |
| 29 | | $x(x^{10} + 11x^5 - 1).\psi(x) \cdot \Lambda(x)$ |
| 30 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \psi(x) \cdot \Lambda(x)$ |
| 31 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \psi(x) \cdot \Lambda(x)$ |
| 32 | $U$ | $B(x)$ |
| 33 | | $B(x)$ |
| 34 | $K_m$ | $\Theta(x)$ |
| 35 | | $x \prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j) \cdot \Theta(x)$ |
| 36 | | $\Theta(x)$ |
| 37 | | $x \prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j) \cdot \Theta(x)$ |
| 38 | $PSL_2(q)$ | $\Delta(x)$ |
| 39 | | $((x^q - x)^{q-1} + 1) \cdot \Delta(x)$ |
| 40 | | $(x^q - x) \cdot \Delta(x)$ |
| 41 | | $(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Delta(x)$ |
| 42 | $PGL_2(q)$ | $\Omega(x)$ |
| 43 | | $((x^q - x)^{q-1} + 1) \cdot \Omega(x)$ |
| 44 | | $(x^q - x) \cdot \Omega(x)$ |
| 45 | | $(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Omega(x)$ |

TABLE 4. The equations of the curves related to the cases in Table 2

4.1. $\bar{G} \cong C_m$. Then, $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has signature $(m, m)$. We identify the branch points of $\phi$ are 0 and $\infty$. Let $q_1 = \infty$, $q_2 = 0$. By Lemma 1, we know that $\phi(x) = x^m$. Hence $\varphi(x) = 1$ and $\chi(x) = x$. Let $\lambda_i \in S \setminus \{0, \infty\}$. The points in the fiber $\phi^{-1}(\lambda_i)$ are the roots of the polynomial

$$G_{\lambda_i}(x) := x^m - \lambda_i$$

Now we can compute equations for the cases 1-3 in Table 4. If $W \cap V = \varnothing$ then the equation of the curve is $y^n = G(x)$ where

$$G(x) = \prod_{i=1}^{\delta} G_{\lambda_i}(x)$$

and $\delta$ is as case 1 in Table 2. Let $a_1, ..., a_\delta$ denote the symmetric polynomials in $\lambda_1, ..., \lambda_\delta$. Further we can take $\lambda_1 ... \lambda_\delta = 1$. Hence the equation of the curve is

$$y^n = x^{m\delta} + a_1 x^{m(\delta-1)} + ... + a_\delta x^m + 1$$

If $V \cap W = \phi^{-1}(q_1)$(i.e. case 2 in Table 4) then we know that the equation is $y^n = \varphi(x).G(x)$. Hence the equation is

$$y^n = x^{m\delta} + a_1 x^{m(\delta-1)} + ... + a_\delta x^m + 1$$

where $\delta$ is as case 2 in Table 2. If $V \cap W = \phi^{-1}(q_1) \cup \phi^{-1}(q_2)$ (i.e. case 3 in Table 4) then the equation is $y^n = \varphi(x).\chi(x).G(x)$. Hence

$$y^n = x(x^{m\delta} + a_1 x^{m(\delta-1)} + ... + a_\delta x^m + 1)$$

where $\delta$ is as case 3 in Table 2.

4.2. $\bar{G} \cong D_{2m}$. Then, $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has signature $(2, 2, m)$. The branch points of $\phi(x)$ are $\infty$ and $\pm 2$. Let $q_1 = \infty$, $q_2 = 2$ and $q_3 = -2$. By Lemma 1, we know that

$$\phi(x) = x^m + \frac{1}{x^m}.$$

Since $\phi(x) - 2 = \frac{(x^m-1)^2}{x^m}$ and $\phi(x) + 2 = \frac{(x^m+1)^2}{x^m}$, $\varphi(x) = x$, $\chi(x) = x^m - 1$ and $\psi = x^m + 1$. In this case we have $G(x)$ as below.

$$G(x) = \prod_{i=1}^{\delta} (x^{2m} - \lambda_i x^m + 1)$$

where $\lambda_i \in S \setminus \{0, \pm 2\}$ and $\delta$ is as corresponding case in Table 2. Then each family is parameterized as cases 4-9 in Table 4.

4.3. $\bar{G} \cong A_4$. Then, $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has signature $(2, 3, 3)$. We choose branch points $q_1 = \infty$, $q_2 = 6i\sqrt{3}$, and $q_3 = -6i\sqrt{3}$, where $i^2 = -1$. We know that

$$\phi(x) = \frac{x^{12} - 33x^8 - 33x^4 + 1}{x^2(x^4 - 1)^2}.$$

Thus the points in the fiber of $q_1, q_2, q_3$ are the roots of the polynomials:

$$\varphi(x) = x(x^4 - 1)$$
$$\chi(x) = x^4 - 2i\sqrt{3}x^2 + 1$$
$$\psi(x) = x^4 + 2i\sqrt{3}x^2 + 1$$

Let $\lambda_i \in \mathrm{S} \setminus \{\infty, \pm 6i\sqrt{3}\}$ then points of $\phi^{-1}(\lambda_i)$ are roots of the polynomial

$$G_{\lambda_i}(x) = x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1$$

There are $\delta$ points in $\mathrm{S} \setminus \{\infty, \pm 6i\sqrt{3}\}$. Hence, we have

$$G(x) = \prod_{i=1}^{\delta}(x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1)$$

Then, each family is parameterized as cases 10-15 in Table 4, where $\delta$ is as corresponding case in Table 2.

4.4. $\bar{G} \cong S_4$. Then, $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has signature $(2, 3, 4)$. The branch points of $\phi(x)$ are $\{0, 1, \infty\}$. Let $q_1 = 1$, $q_2 = 0$ and $q_3 = \infty$. Then

$$\begin{aligned}\varphi(x) &= x^{12} - 33x^8 - 33x^4 + 1\\ \chi(x) &= x^8 + 14x^4 + 1\\ \psi(x) &= x(x^4 - 1)\end{aligned}$$

For $\lambda_i \in \mathrm{S} \setminus \{0, 1, \infty\}$, the points in $\phi^{-1}(\lambda_i)$ are roots of the polynomial

$$\begin{aligned}G_{\lambda_i}(x) =& x^{24} + \lambda_i x^{20} + (759 - 4\lambda_i)x^{16} + 2(3\lambda_i + 1228)x^{12}\\ &+ (759 - 4\lambda_i)x^8 + \lambda_i x^4 + 1\end{aligned}$$

There are $\delta$ points in $S\setminus\{0, 1, \infty\}$, where $\delta$ is given as in Table 2. We denote

$$M(x) := \prod_{i=1}^{\delta} G_{\lambda_i}(x)$$

Then, each family is parameterized as cases 16-23, where $R(x), S(x), T(x)$ are $\varphi(x), \chi(x), \psi(x)$ respectively.

4.5. $\bar{G} \cong A_5$. The branch points of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ are 0, 1728 and $\infty$. Let $q_1 = 0$, $q_2 = \infty$ and $q_3 = 1728$. At the place $q_3 = 1728$ the function has the following ramification

$$\phi(x) - 1728 = -\frac{(x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1)^2}{x^5(x^{10} + 11x^5 - 1)^5}$$

Then,

$$\begin{aligned}\varphi(x) &= x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1\\ \chi(x) &= x(x^{10} + 11x^5 - 1)\\ \psi(x) &= x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1\end{aligned}$$

For each $\lambda_i \in \mathrm{S} \setminus \{0, 1728, \infty\}$ the places in $\phi^{-1}(\lambda_i)$ are the roots of the following polynomial

$$\begin{aligned}G_{\lambda_i}(x) =& - x^{60} + (684 - \lambda_i)x^{55} - (55\lambda_i + 157434)x^{50} - (1205\lambda_i - 12527460)x^{45}\\ &- (13090\lambda_i + 77460495)x^{40} + (130689144 - 69585\lambda_i)x^{35}\\ &+ (33211924 - 134761\lambda_i)x^{30} + (69585\lambda_i - 130689144)x^{25}\\ &- (13090\lambda_i + 77460495)x^{20} - (12527460 - 1205\lambda_i)x^{15}\\ &- (157434 + 55\lambda_i)x^{10} + (\lambda_i - 684)x^5 - 1\end{aligned}$$

Then,

$$\Lambda(x) = \prod_{i=1}^{\delta} G_{\lambda_i}(x)$$

Then equations of the curves are as in cases 24-31 in Table 4, where $Q(x) = \psi(x)$.

4.6. $\bar{G} \cong U$. The branch point of the curve $\phi$ is $\{\infty\}$. Let $q_1 = \infty$. Then $\varphi(x) = 1$. For each $\lambda_i \in S\backslash\{\infty\}$ we have

$$G_{\lambda_i}(x) = \prod_{a \in H_t} (x + a) - \lambda_i$$

There are $\delta$ points in $S\backslash\{\infty\}$. Where $\delta$ is as in Table 2. We denote

$$B(x) = \prod_{i=1}^{\delta} G_{\lambda_i}(x)$$

Then, each family is parameterized as cases 32-33.

4.7. $\bar{G} \cong K_m$. The branch points of the curve $\phi$ are $\{0, \infty\}$. Let $q_1 = 0$, $q_2 = \infty$. Then the polynomial over the branch point is

$$\varphi(x) = x \prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j)$$
$$\chi(x) = 1$$

For $\lambda_i \in S\backslash\{0, \infty\}$ we have

$$G_{\lambda_i}(x) = ((x \prod_{j=1}^{\frac{p^t-1}{m}} (x^m - b_j))^m - \lambda_i)$$

There are $\delta$ points in $S\backslash\{0, \infty\}$. Where $\delta$ is as in Table 2. We denote

$$\Theta(x) = \prod_{i=1}^{\delta} G_{\lambda_i}(x)$$

Then, each family is parameterized as cases 34-37.

4.8. $\bar{G} \cong PSL_2(q)$. The branch points of $\phi(x)$ are $\{0, \infty\}$. Let $q_1 = 0$, $q_2 = \infty$. Then

$$\varphi(x) = (x^q - x)^{q-1} + 1$$
$$\chi(x) = x^q - x$$

For $\lambda_i \in S\backslash\{0, \infty\}$, points in $\phi^{-1}(\lambda_i)$ are roots of the polynomials,

$$G_{\lambda_i}(x) = (((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}} - \lambda_i (x^q - x)^{\frac{q(q-1)}{2}})$$

There are $\delta$ points in $S\backslash\{0, \infty\}$. Where $\delta$ is as in Table 2. We denote

$$\Delta(x) = \prod_{i=1}^{\delta} (((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}} - \lambda_i (x^q - x)^{\frac{q(q-1)}{2}})$$

Then, each family is parameterized as cases 38-41.

4.9. $\bar{G} \cong PGL_2(q)$**.** The branch points of $\phi(x)$ are $\{0, \infty\}$. Let $q_1 = 0$, $q_2 = \infty$. Then

$$\varphi(x) = (x^q - x)^{q-1} + 1$$
$$\chi(x) = x^q - x$$

For $\lambda_i \in S \backslash \{0, \infty\}$, points in $\phi^{-1}(\lambda_i)$ are roots of the polynomials,

$$G_{\lambda_i}(x) = (((x^q - x)^{q-1} + 1)^{q+1} - \lambda_i (x^q - x)^{q(q-1)})$$

Then we let,

$$\Omega(x) = \prod_{i=1}^{\delta} (((x^q - x)^{q-1} + 1)^{q+1} - \lambda_i (x^q - x)^{q(q-1)})$$

where $\delta$ is gives as Table 2. Then, each family is parameterized as cases 42-45. This completes the proof.

□

**Remark 2.** *By Remark 1, we know that $A_5$ has different ramification when $p = 3$. In this case $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has signature $(6, 5)$. The branch points of $\phi(x)$ are $\infty$ and $0$. Let $q_1 = \infty$ and $q_2 = 0$. By Lemma 1, we know that*

$$\phi(x) = \frac{(x^{10} - 1)^6}{(x(x^{10} + 2ix^5 + 1))^5}.$$

*Then,*

$$\varphi(x) = x(x^{10} + 2ix^5 + 1)$$
$$\chi(x) = x^{10} - 1$$

*For $\lambda_j \in S \setminus \{0, \infty\}$, the points in $\phi^{-1}(\lambda_j)$ are roots of the polynomial*

$$\begin{aligned} G_{\lambda_j}(x) = {} & x^{60} + \lambda_j x^{55} - (6 + 10i\lambda_j)x^{50} + 35\lambda_j x^{45} + (15 + 40i\lambda_j)x^{40} + 30\lambda_j x^{35} \\ & - (20 - 68i\lambda_j)x^{30} + 30\lambda_j x^{25} + (15 + 40i\lambda_j)x^{20} + 35\lambda_j x^{15} \\ & - (6 + 10i\lambda_j)x^{10} - \lambda_j x^5 + 1 \end{aligned}$$

*There are $\delta$ points in $S \setminus \{0, \infty\}$, where $\delta$ is given as in Table 3. We denote*

$$P(x) := \prod_{j=1}^{\delta} G_{\lambda_j}(x)$$

*Then, each family is parameterized as in Table 5.*

| *Case* | $y^n =$ |
|---|---|
| $a$ | $P(x)$ |
| $b$ | $x(x^{10} + 2ix^5 + 1) \cdot P(x)$ |
| $c$ | $(x^{10} - 1) \cdot P(x)$ |
| $d$ | $x(x^{10} + 2ix^5 + 1)(x^{10} - 1) \cdot P(x)$ |

TABLE 5. Equation of curve when $\bar{G} \cong A_5$, $p = 3$

**Lemma 2.** *Let $\mathcal{X}_g$ be a cyclic curve defined over an algebraically closed field $k$ of characteristic $p = 3$ such that $\bar{G}$ for $\mathcal{X}_g$ is isomorphic to $A_5$. Then, the equation of $\mathcal{X}_g$ is as in one of the cases in Table 5.*

We summarize all the cases in the following Theorem.

**Theorem 4.2.** *Let $\mathcal{X}_g$ be e genus $g \geq 2$ algebraic curve defined over an algebraically closed field $k$, $G$ its automorphism group over $k$, and $H$ cyclic normal subgroup of $G$ of order $n$ such that $g(X_g^H) = 0$. Then, the equation of $\mathcal{X}_g$ can be written as in one of the following cases:*

| # | $\bar{G}$ | $y^n = f(x)$ |
|---|---|---|
| 1 | $C_m$ | $x^{m\delta} + a_1 x^{m(\delta-1)} + \ldots + a_\delta x^m + 1$ |
| 2 | | $x^{m\delta} + a_1 x^{m(\delta-1)} + \ldots + a_\delta x^m + 1$ |
| 3 | | $x(x^{m\delta} + a_1 x^{m(\delta-1)} + \ldots + a_\delta x^m + 1)$ |
| 4 | $D_{2m}$ | $F(x) := \prod_{i=1}^{\delta}(x^{2m} + \lambda_i x^m + 1)$ |
| 5 | | $(x^m - 1) \cdot F(x)$ |
| 6 | | $x \cdot F(x)$ |
| 7 | | $(x^{2m} - 1) \cdot F(x)$ |
| 8 | | $x(x^m - 1) \cdot F(x)$ |
| 9 | | $x(x^{2m} - 1) \cdot F(x)$ |
| 10 | $A_4$ | $G(x) := \prod_{i=1}^{\delta}(x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1)$ |
| 11 | | $(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$ |
| 12 | | $(x^8 + 14x^4 + 1) \cdot G(x)$ |
| 13 | | $x(x^4 - 1) \cdot G(x)$ |
| 14 | | $x(x^4 - 1)(x^4 + 2i\sqrt{3}x^2 + 1) \cdot G(x)$ |
| 15 | | $x(x^4 - 1)(x^8 + 14x^4 + 1) \cdot G(x)$ |
| 16 | $S_4$ | $M(x)$ |
| 17 | | $\left(x^8 + 14x^4 + 1\right) \cdot M(x)$ |
| 18 | | $x(x^4 - 1) \cdot M(x)$ |
| 19 | | $\left(x^8 + 14x^4 + 1\right) \cdot x(x^4 - 1) \cdot M(x)$ |
| 20 | | $\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot M(x)$ |
| 21 | | $\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot \left(x^8 + 14x^4 + 1\right) \cdot M(x)$ |
| 22 | | $\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot x(x^4 - 1) \cdot M(x)$ |
| 23 | | $\left(x^{12} - 33x^8 - 33x^4 + 1\right) \cdot \left(x^8 + 14x^4 + 1\right) \cdot x(x^4 - 1)M(x)$ |
| 24 | $A_5$ | $\Lambda(x)$ |
| 25 | | $(x(x^{10} + 11x^5 - 1)) \cdot \Lambda(x)$ |
| 26 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \Lambda(x)$ |
| 27 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \Lambda(x)$ |
| 28 | | $Q(x) \cdot \Lambda(x)$ |
| 29 | | $x(x^{10} + 11x^5 - 1).\psi(x) \cdot \Lambda(x)$ |
| 30 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \psi(x) \cdot \Lambda(x)$ |
| 31 | | $(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \psi(x) \cdot \Lambda(x)$ |
| 32 | $U$ | $B(x)$ |
| 33 | | $B(x)$ |
| 34 | $K_m$ | $\Theta(x)$ |
| 35 | | $x\prod_{j=1}^{\frac{p^t-1}{m}}(x^m - b_j) \cdot \Theta(x)$ |
| 36 | | $\Theta(x)$ |
| 37 | | $x\prod_{j=1}^{\frac{p^t-1}{m}}(x^m - b_j) \cdot \Theta(x)$ |
| 38 | $PSL_2(q)$ | $\Delta(x)$ |
| 39 | | $((x^q - x)^{q-1} + 1) \cdot \Delta(x)$ |
| 40 | | $(x^q - x) \cdot \Delta(x)$ |
| 41 | | $(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Delta(x)$ |
| 42 | $PGL_2(q)$ | $\Omega(x)$ |
| 43 | | $((x^q - x)^{q-1} + 1) \cdot \Omega(x)$ |
| 44 | | $(x^q - x) \cdot \Omega(x)$ |
| 45 | | $(x^q - x)((x^q - x)^{q-1} + 1) \cdot \Omega(x)$ |

TABLE 6. The equations of the curves related to the cases in Table 2

*where $\delta$ is given as in Table 2 and $M, \Lambda, Q, B, \Delta$, and $\Omega$ are as follows:*

$$
\begin{aligned}
M =& \prod_{i=1}^{\delta} \big(x^{24} + \lambda_i x^{20} + (759 - 4\lambda_i)x^{16} + 2(3\lambda_i + 1228)x^{12} \\
&+ (759 - 4\lambda_i)x^8 + \lambda_i x^4 + 1\big) \\
\Lambda =& \prod_{i=1}^{\delta} \big(-x^{60} + (684 - \lambda_i)x^{55} - (55\lambda_i + 157434)x^{50} - (1205\lambda_i - 12527460)x^{45} \\
&- (13090\lambda_i + 77460495)x^{40} + (130689144 - 69585\lambda_i)x^{35} \\
&+ (33211924 - 134761\lambda_i)x^{30} + (69585\lambda_i - 130689144)x^{25} \\
&- (13090\lambda_i + 77460495)x^{20} - (12527460 - 1205\lambda_i)x^{15} \\
&-(157434 + 55\lambda_i)x^{10} + (\lambda_i - 684)x^5 - 1\big) \\
Q =& x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1 \\
B =& \prod_{i=1}^{\delta} \prod_{a \in H_t} ((x + a) - \lambda_i) \\
\Delta =& \prod_{i=1}^{\delta} (((x^q - x)^{q-1} + 1)^{\frac{q+1}{2}} - \lambda_i (x^q - x)^{\frac{q(q-1)}{2}}) \\
\Omega =& \prod_{i=1}^{\delta} (((x^q - x)^{q-1} + 1)^{q+1} - \lambda_i (x^q - x)^{q(q-1)})
\end{aligned}
$$

## References


[1] R. Brandt and H. Stichtenoth, Die Automorphismengruppen hyperelliptischer Kurven, Man. Math 55 (1986), 83–92.

[2] E. Bujulance, J. Gamboa, and G. Gromadzki, The full automorphism groups of hyperelliptic Riemann surfaces, Manuscripta Math. 79 (1993), no. 3-4, 267–282.

[3] W. Baily, On the automorphism group of a generic curve of genus $> 2$. J. Math. Kyoto Univ. 1 1961/1962 101–108; correction, 325.

[4] Y. Demirbas, Automorphism groups of hyperelliptic curves of genus 3 in characteristic 2, Computational aspects of algebraic curves, T. Shaska (Edt), Lect. Notes in Comp., World Scientific, 2005.

[5] Magaard, K.; Shaska, T.; Shpectorov, S.; Völklein, H.; The locus of curves with prescribed automorphism group. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). Sürikaisekikenkyüsho Kökyüroku No. 1267 (2002), 112–141.

[6] Miller, G. A.; Blichfeldt, H. F.; Dickson, L. E.; Theory and applications of finite groups. (English) 2. ed. XVII + 390 p. New York, Stechert. Published: 1938

[7] P. G. Henn, Die Automorphismengruppen der algebraischen Funktionenkörper vom Geschlecht 3, PhD thesis, University of Heidelberg, (1976).

[8] P. Roquette, Abschtzung der Automorphismenanzahl von Funktionenkrpern bei Primzahlcharakteristik. Math. Z. 117 1970 157–163.

[9] A. Kontogeorgis, The Group of Automorphisms of Cyclic Extensions of Rational Function Fields, J. Algebra 216(2) (1999), 665-706.

[10] C. R. Valentini and L. M. Madan, A Hauptsatz of L. E. Dickson and Artin-Scheier extension, J. Reine Angew. Math. 318 (1980), 156-177.

[11] T. Shaska, Subvarieties of the Hyperelliptic Moduli Determined by Group Actions, Serdica Math. J. 32 (2006), 355-374.

[12] T. Shaska, Some special families of hyperelliptic curves. J. Algebra Appl. 3, 1 (2004), 75-89.

[13] T. Shaska, Determining the automorphism groups of hyperelliptic curves. Proceeding of the 2003 International Symposium on Symbolic Algebraic Computation, ACM Press, 2003, 248-254.

[14] T. Shaska and J. Thompson, On the generic curve of genus 3. Affine algebraic geometry, 233–243, Contemp. Math., 369, Amer. Math. Soc., Providence, RI, 2005.

[15] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus 2 function fields. Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 703–723, Springer, Berlin, 2004.

[16] E. Previato, T. Shaska, and S. Wijesiri, Thetanulls of cyclic curves of small genus, *Albanian J. Math.*, Special issue on computational algebraic geometry, **vol. 1**, Nr. 4, 2007, pg. 265-282.

[17] T. Shaska, Some open problems in computational algebraic geometry, *Albanian J. Math.*, Special issue on computational algebraic geometry, **vol 1**, Nr. 4, 2007, 309-321.

[18] T. Shaska and C. Shor, Codes over $F_{p^2}$ and $F_p \times F_p$, lattices, and theta functions, *Advances in Coding Theory and Cryptology*, vol 3. (2007), pg. 70-80.

[19] T. Shaska and Q. Wang, On the automorphism groups of some AG-codes based on $C_{ab}$ curves, Serdica Journal of Computing, 2007, vol. 1. pg. 193-206.

[20] T. Shaska and D. Sevilla, Hyperelliptic curves with reduced automorphism group $A_5$, *Appl. Algebra Engrg. Comm. Comput.*, (2007), vol. 1, pg. 3-20.

[21] J. Gutierrez and T. Shaska, Hyperelliptic curves with extra involutions, *LMS J. of Comput. Math.*, 8 (2005), 102-115.

[22] T. Shaska and S. Zheng, A Maple package for hyperelliptic curves, Ed. I. Kotsieras, Maple conference, 2005, pg. 161-175.

[23] J. Gutierrez, D. Sevilla and T. Shaska, Hyperelliptic curves of genus 3 with prescribed automorphism group, *Lect. Notes in Computing*, vol 13. (2005), pg. 201-225.

[24] T. Shaska, Genus 2 curves covering elliptic curves, a computational approach, *Lect. Notes in Computing*, vol 13. (2005), pg. 151-195.

[25] T. Shaska, Genus 2 fields with degree 3 elliptic subfields, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.

[26] T. Shaska, Computational algebra and algebraic curves, ACM, *SIGSAM Bulletin*, *Comm. Comp. Alg.*, Vol. **37**, No. 4, 117-124, 2003.

[27] T. Shaska, Computational aspects of hyperelliptic curves, Computer mathematics. Proceedings of the sixth Asian symposium (ASCM 2003), Beijing, China, April 17-19, 2003. River Edge, NJ: World Scientific. *Lect. Notes Ser. Comput.* 10, 248-257 (2003).

[28] T. Shaska, Determining the automorphism group of a hyperelliptic curve, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ACM Press, pg. 248 - 254, 2003.

[29] R. Sanjeewa and T. Shaska, Automorphism groups of cyclic curves, (preprint)

[30] H. Stichtenoth, ber die Automorphismengruppe eines algebraischen Funktionenkrpers von Primzahlcharakteristik. I. Eine Abschtzung der Ordnung der Automorphismengruppe. Arch. Math. (Basel) 24 (1973) 527–544.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 215–220
ISSN 1930-1235: (2008)

# A NEW ENCRYPTION AND SIGNING ALGORITHM.

Urszula Romaczuk

*John Paul II Catholic University of Lublin,*
*Lublin, Poland*
*urszula_romanczuk@o2.pl*

Abstract. In this paper we describe a new method of encryption that originates from the public key cryptography and number theory. Our algorithm was inspired by the RSA algorithm and Diffie-Hellman key exchange protocol. It is based on a computationally difficult problem - the discrete logarithm problem in multiplicative group.

## 1. Basic idea

Let $\mathbb{A}$ and $\mathbb{B}$ be users that communicate in a secure channel based on public key cryptography. $\mathbb{A}$ is a sender and $\mathbb{B}$ is a receiver of a message. Hence, each of them have a pair of keys - public and private. $\mathbb{A}$ has pair $(k_{\mathbb{A}},\ l_{\mathbb{A}})$ , $\mathbb{B}$ has $(k_{\mathbb{B}},\ l_{\mathbb{B}})$ ($k_{\mathbb{A}},\ k_{\mathbb{B}}$ are private keys and $l_{\mathbb{A}},\ l_{\mathbb{B}}$ are public keys). Assume that $\mathbb{A}$ wants to send $c$ (that is encrypted message $m$) to $\mathbb{B}$.

Let $f$ denote the encryption function and let $f^{-1}$ denote the corresponding decryption function. In asymmetrical cryptography arguments of the function $f$ are: receiver's public key $l_{\mathbb{B}}$ and plain text $m$, that is

$$c = f(m, l_{\mathbb{B}}),$$

where $c$ is ciphertext. The decryption function's $f^{-1}$ arguments are: the receiver's private key $k_{\mathbb{B}}$ and ciphertext $c$. In our case:

$$f^{-1}(c, k_{\mathbb{B}}) = m.$$

In this paper a different approach is presented. Namely, arguments of the encryption function are: plaintext $m$, the receiver's public key $l_{\mathbb{B}}$ and the sender's private key $k_{\mathbb{A}}$. Hence

$$c = f(m, l_{\mathbb{B}}, k_{\mathbb{A}}).$$

Similarly, arguments of decryption function $f^{-1}$ are three parameters, that is: ciphertext $c$, receiver's private key $k_{\mathbb{B}}$ and sender's public key $l_{\mathbb{A}}$. We have

$$f^{-1}(c, k_{\mathbb{B}}, l_{\mathbb{A}}) = m.$$

This cross-keyed approach in both encryption and decryption functions aims not only at encrypting and decrypting, but also at signing, simultaneously. That makes receiver $\mathbb{A}$ ensured that $\mathbb{B}$ is an authentic sender of a message. Then, the sender cannot deny his authorship of a message, that is the authentication of the sender and typical digital signature take place at the same time. Hence, that signature

identifies the author of the message and checks that the message was not changed during transmission.

From a mathematical point of view I find this cryptosystem very interesting. It may be used e.g. to protect transmission in LAN networks.

## 2. Description of encryption and digital signature algorithm.

In this paper I assume that the reader has basic knowledge in abstract algebra and number theory.

Let $\mathbb{Z}_n$ denote the additive group of integers residues modulo $n$ and let $\mathbb{Z}_n^*$ denote the multiplicative group of integers residues modulo $n$, where $n$ is a natural integer. Let $\varphi$ be Euler's function, that is, if $m$ is a natural integer then $\varphi(m)$ denotes the number of integers that are less than $m$ and relatively prime to $m$.

Lets assume $\mathbb{A}$ and $\mathbb{B}$ are going to communicate. First, each of them has to generate a pair of keys: public and private. Now they are ready to send each other a secret message.

Let $(k_{\mathbb{A}},l_{\mathbb{A}})$ be the pair of keys that belong to user $\mathbb{A}$. Similarly, let the pair $(k_{\mathbb{B}},l_{\mathbb{B}})$ belong to user $\mathbb{B}$.

**1.: Keys generation.**

**1.1.:** Both users set:

**-** two positive integers $q$ and $n$, where $q$ is prime. It is important to choose such integers that the discrete logarithm problem in $\mathbb{Z}^*_{\varphi(q^n)}$ is computationally difficult,

**-** integer $g \in \mathbb{Z}^*_{\varphi(q^n)}$ has such a property that it generates the biggest subgroup of multiplicative group $\mathbb{Z}^*_{\varphi(q^n)}$. It would be best if $g$ generates the entire group $\mathbb{Z}^*_{\varphi(q^n)}$, so that the group would be cyclic. Of course:

$$\gcd(g, \varphi(q^n)) = 1 \quad \text{and} \quad g \neq 1.$$

Function $\gcd(n, m)$ denotes the greatest common divisor of integers $n$ and $m$.

**1.2.:** Next, user $\mathbb{A}$ chooses randomly $x \in \mathbb{Z}^*_{\varphi(\varphi(q^n))}$, user $\mathbb{B}$ chooses $y \in \mathbb{Z}^*_{\varphi(\varphi(q^n))}$ and they compute $g^x,\ g^y$ modulo $\varphi(q^n)$. If

$$g^x \equiv 1 \,(\text{mod } \varphi(q^n)), \quad \text{or} \quad g^y \equiv 1 \,(\text{mod } \varphi(q^n)),$$

then $x$ or $y$ must be chosen randomly again. Clearly, $\varphi(q^n) = q^{n-1}(q-1)$.

**1.3.:** Both users agree on a hash function $h$ which is used to generate a digital signature.

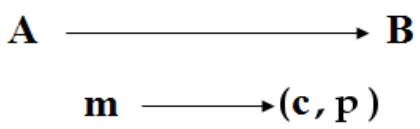
Then, for user $\mathbb{A}$:

**-** private key is $k_{\mathbb{A}} = x$,

**-** public key $l_{\mathbb{A}} = (\ g^x,\ q,\ n,\ h\ )$.

(User B: $k_{\mathbb{B}} = y$, $l_{\mathbb{B}} = (\ g^y,\ q,\ n,\ h\ )$).

Let $m \in \mathbb{Z}^*_{q^n}$. Lets assume that user $\mathbb{A}$ is going to send message $m$ to user $\mathbb{B}$. Moreover, $m$ is both encrypted and signed, so $\mathbb{B}$ receives $(c, p)$, where $c$ denotes ciphertext and $p$ denotes the signature of that ciphertext.




**Communication schema between users $\mathbb{A}$ and $\mathbb{B}$.**

**2.:** **Encryption and signature.** (User $\mathbb{A}$).

**2.1.:** Gets public key of user $\mathbb{B}$, $l_{\mathbb{B}} = (\, g^y, q, n, h\,)$ and computes:

$$k \equiv (g^y)^x \equiv g^{xy} \,(\mathrm{mod}\ \varphi\,(q^n))\,.$$

**2.2.:** Next, he encrypts message $m$:

$$m^k \equiv c \,(\mathrm{mod}\ q^n)\,.$$

**2.3.:** Generation of signature $p$ is as follows. Firstly:

$$r \equiv c^k \,(\mathrm{mod}\ q^n)\,.$$

Secondly, using hash function $h$, he computes signature $p = h\,(r)$.

**2.4.:** Ciphertext $c$ and signature $p$ is sent to user $\mathbb{B}$.

**3.:** **Decryption and verification.** (User $\mathbb{B}$).

**3.1.:** After receiving ciphertext $c\,'$ and signature $p\,'$ from user $\mathbb{A}$, he gets the public key of user $\mathbb{A}$ $l_{\mathbb{A}} = (\, g^x, q, n, h\,)$. Next he computes $k$ and $k^{-1}$:

$$k \equiv (g^x)^y \equiv (g^{xy}) \,(\mathrm{mod}\ \varphi\,(q^n))\,,$$

$$k^{-1} \equiv (g^{xy})^{-1} \,(\mathrm{mod}\ \varphi\,(q^n))\,.$$

**3.2.:** In the next step $\mathbb{B}$ computes :

$$r\,' \equiv (c\,')^k \,(\mathrm{mod}\ q^n)\,.$$

**3.3.:** By using hash function $h$ he gets $p'$, so $p' = h\,(r\,')$. Next he checks that no enemy pretends to be the valid sender, that is, the following equation must occur:

$$p\,' = p\,''.$$

If so, that means nobody faked the ciphertext $c'$, hence $c = c'$. Additionally, authentication of user $\mathbb{A}$ takes place at this moment, because the only persons that can compute $k$ are $\mathbb{A}$ and $\mathbb{B}$. Now $\mathbb{B}$ is ready to process decryption of ciphertext $c$.

3.4.: Decryption of ciphertext $c$ is as follows:

$$c^{k^{-1}} \equiv m \,(\mathrm{mod}\ q^n)\,.$$

and that is all.

Notice that the existence of the of inverse of the element $g^{xy}$ in group $\mathbb{Z}^*_{\varphi(q^n)}$ is a sufficient condition of verification. Let us assume that such an $(g^{xy})^{-1}$ exists in that group. Then we have

$$c^{k^{-1}} \equiv \left[m^{g^{xy}}\right]^{(g^{xy})^{-1}} \equiv m^{g^{xy} g^{-xy}} \equiv m \,(\mathrm{mod}\ q^n)\,.$$

In fact, now it is sufficient to prove that the element $(g^{xy})^{-1}$ exists in group $\mathbb{Z}^*_{\varphi(q^n)}$.

By assumption $g \in \mathbb{Z}^*_{q^{n-1}}$. Moreover it is the generator of that group. Hence $g \in \left(1, g^{n-1}\right)$ and $\gcd(g, \varphi(q^n)) = 1$, so element $g$ belongs to the multiplicative group $\mathbb{Z}^*_{\varphi(q^n)}$ and has its inverse. We have

$$1 \equiv g \cdot g^{-1} \equiv \left(g \cdot g^{-1}\right)^{xy} \equiv g^{xy} \cdot g^{-xy} \pmod{\varphi(q^n)}.$$

We proved that an inverse to the element $g^{xy}$ exists in group $\mathbb{Z}^*_{\varphi(q^n)}$ Hence decryption is correct.

The strength of the described algorithm lies in the fact that having public keys of the sender and the receiver there is no possibility that an enemy gets the private key of neither sender nor receiver.

Indeed, we know public keys of users $\mathbb{A}$ and $\mathbb{B}$ because they publish their keys in public: $l_{\mathbb{A}} = (g^x, q, n, h)$ and $l_{\mathbb{B}} = (g^y, q, n, h)$. An enemy has no possibility of computing the private key of $\mathbb{A}$: $k_{\mathbb{A}} = x$. The element $g^x \in \mathbb{Z}^*_{\varphi(q^n)}$, $\varphi(q^n) = q^{n-1} \cdot (q-1)$ (as it's easy to prove). However, even if a generator $g$ of a subgroup of the group $\mathbb{Z}^*_{\varphi(q^n)}$ was published publicly, the expression $x$ would be based on a computationally hard problem, that is on discrete logarithm problem. Of course, we have to carefully choose a prime $q$ and a natural integer $n$. Hence, an enemy not only has to compute private keys of sender and receiver, but additionally he has to guess the generator $g$ that was used in encryption.

Notice that if an enemy catches both ciphertext and signature $(c, p)$, which was sent by user $\mathbb{A}$ to $\mathbb{B}$, then he also knows public keys : $l_{\mathbb{A}} = (g^x, q, n, h)$ and $l_{\mathbb{B}} = (g^y, q, n, h)$. However, he does not know the generator $g$ of a subgroup of the group $\mathbb{Z}^*_{\varphi(q^n)}$ and private keys of $\mathbb{A}$ and $\mathbb{B}$, recpectively $k_{\mathbb{A}} = x$ and $k_{\mathbb{B}} = y$. It is clear that $x, y \in \mathbb{Z}^*_{\varphi(\varphi(q^n))}$, $\varphi(\varphi(q^n)) = q^{n-2} \cdot (q-1) \cdot \varphi(q-1)$. Of course, having this information, somebody can try brute force attack and check in turn every element of $\mathbb{Z}^*_{\varphi(\varphi(q^n))}$, but, as we know, if we choose a group of big enough order, then finding $x$ to compute $k$, that is.

$$k \equiv (g^x)^y \equiv (g^{xy}) \pmod{\varphi(q^n)},$$

takes a large amount of time, up to a dozen or so years. Additionally $k^{-1}$ must also be found to decrypt the ciphertext $c$.

## 3. Conclusion.

In choosing an adequate multiplicative group $\mathbb{Z}^*_{q^n}$, where $q$ is prime and $n$ is natural integer, it is important for the group $\mathbb{Z}^*_{\varphi(q^n)}$ to be cyclic. This guarantees that the ciphertext set extends to the maximum and the number of constant elements is minimal and equal 2 (that is elements where $f(m) = m$, where $f$ is an encryption function and $m \in \mathbb{Z}^*_{q^n}$, these elements are $m = 1$ and $m = q^n - 1$, because $2 | \#\mathbb{Z}^*_{q^n}$, where $\#\mathbb{Z}^*_{q^n} = (q-1)\, q^{n-1}$ is rank of a group $\mathbb{Z}^*_{q^n}$ ). This is indeed so, because the Abelian group $\mathbb{G}$ of rank $n$ is a cyclic group, if and only if for any divisor $d$ of $n$, there are exactly $d$ elements fulfilling the condition $x^d = e$, where $e$ is a natural element of the group.(See: [1])

After conducting research on multiplicative groups $\mathbb{Z}^*_{q^n}$ of residues modulo $q^n$, where $q$ is prime and $n$ is natural integer such as $n > 1$, I came to the conclusion that the most effective multiplicative group in the described method of encryption is $\mathbb{Z}^*_{3^n}$, that is, when $q = 3$. This is so, because group $\mathbb{Z}^*_{\varphi(3^n)} = \mathbb{Z}^*_{2 \cdot 3^{n-1}}$ is cyclic, that is, a generator $g$ exists, which generates the entire group $\mathbb{Z}^*_{\varphi(3^n)}$ and not only

its subgroup and, as well, group $\mathbb{Z}^*_{\varphi(\varphi(3^n))} = \mathbb{Z}^*_{2\cdot 3^{n-2}}$ is cyclic, that is, a generator $g'$ exists, which generates the entire group $\mathbb{Z}^*_{\varphi(\varphi(3^n))}$ and not only its subgroup. This means that the set of possible private and public keys extends to maximum size, that is $x, y \in \mathbb{Z}^*_{\varphi(\varphi(3^n))}$ and $g^x, g^y \in \mathbb{Z}^*_{\varphi(3^n)}$.

Indeed this is so because the following fact occurs: if $p$ is an odd prime, for any natural integer $n$, the multiplicative groups $\mathbb{Z}^*_{p^n}$ and $\mathbb{Z}^*_{2p^n}$ are cyclic groups.(See: [2], [3])

After my research on groups of the form $\mathbb{Z}^*_{q^n}$, $n > 1$, I noticed that if we take a prime $q \neq 3$ and we apply it to the encryption algorithm, then there exist many fixed points. That means that there exists message $m \in \mathbb{Z}^*_{q^n}$, which stays unchanged after encryption, that is $c = m$. For $\mathbb{Z}^*_{3^n}$ we don't have that problem, because then every message $m \neq 1$ and $m \neq (3^n - 1)$ after encryption is different from ciphertext $c$. It is indeed so, because, in my opinion, the following hypothesis, which stems from my research, is true: the group $\mathbb{Z}^*_{\varphi(q^n)}$ , $n > 1$ and for odd prime $q$ is cyclic if and only if is odd prime $q = 3$. It was Professor Thomas Bier who reassured me that the above mentioned hypothesis is correct by proving this fact.

So far, I haven't come across any evidence in literature, which could prove that in the group $\mathbb{Z}^*_{3^n}$ or $\mathbb{Z}^*_{2\cdot 3^{n-1}}$ , the discrete logarithm problem is computationally simple. Thus, it would be an interesting open problem to find such an algorithm, which would solve the problem of the discrete logarithm in the groups $\mathbb{Z}^*_{3^n}$ and $\mathbb{Z}^*_{2\cdot 3^n}$ for large values of $n$, given that such a discovery is possible today.

According to one theory, the discrete logarithm in the group $\mathbb{Z}^*_n$ when $n$ has small prime factors is not a computationally difficult problem and is easy to solve. Regardless, there is no know algorithm for breaking the discrete logarithm in the proposed group $\mathbb{Z}^*_{3^n}$ or $\mathbb{Z}^*_{2\cdot 3^{n-1}}$ for sufficiently large $n$, though in the above mentioned group we have small prime factors.

When $n = 1$, we have a multiplicative group $\mathbb{Z}^*_q$ of residues modulo $q$. As we know, the multiplicative group $\mathbb{Z}^*_{\varphi(q)}$ is not cyclic for every prime number. However, when e.g. the prime number $q$ is in the form $q = 2p + 1$ where $p$ is a large Sophie Germain prime, then $\mathbb{Z}^*_{\varphi(q)} = \mathbb{Z}^*_{2p}$ is cyclic. Keep in mind that: a prime $p$ is a *Sophie Germain prime* if both $p$ and $2p + 1$ are prime. We do not yet know if an infinite number of Sophie Germain primes exist.(See: [5] )

Continuing with this argumentation, if the prime number is in the form $q = 2p^m + 1$ where $m$ is a natural integer and $p$ is an odd prime number, then it becomes obvious that, in this case, $\mathbb{Z}^*_{\varphi(q)} = \mathbb{Z}^*_{2p^m}$ is cyclic (numbers in the form $q = 2p^n + 1$ where $p$ is an odd prime and $m$ is a natural integer do indeed exist, for example $163 = 2 \cdot 3^4 + 1$, $251 = 2 \cdot 5^3 + 1$, $487 = 2 \cdot 3^5 + 1$, $2663 = 2 \cdot 11^3 + 1$). I do not know how many such numbers $q = 2p^n + 1$ exist nor could I find any forms of such numbers in published literature. As far as I know $q = 2p^n + 1$ is not a prime number for every prime $p$ and natural integer $m$. Let us say that a prime power $p^e$ is called a *Sophie Germain prime power* iff $p$ is odd and $q = 2p^e + 1$ is also a prime number, or if $p = 2$ and $e = 0, 1$.

Hence, the as yet unanswered question arises: for which other prime numbers $q$ will the group $\mathbb{Z}^*_{\varphi(q)}$ be cyclic. I would be very interested in getting familiar with other suggestions regarding this open problem and the method of encryption proposed.

Attaching a signature is necessary to detect if somebody else pretends to be the sender of the message. Notice that determination of $k$ which is used in encryption and decryption, can be done easily and independently only by sender and receiver.

If somebody wants to fabricate ciphertext and signature, he must know $k$ and this leads to knowledge of the private key of the sender or the receiver. In such a situation the discrete logarithm problem must be solved, which is a computationally difficult problem.

The algorithm is based on the RSA encryption algorithm, the Diffie-Hellman key exchange protocol.

**Acknowledgments:** I would like to express my deepest gratitude to Professor Vasyl Ustymenko and Professor Thomas Bier for their guidance and kindness, as well as their helpful advice and valuable suggestions. In would like to particularly thank Professor Jerzy Urbanowicz for inspiration and encouragement, without which this cryptosystem wouldn't have come into existence.

## References

1. Bagiski Czesaw ,,Introdution to group theory", SCRIPT, Warsaw 2002
2. Ireland Kenneth, Rosen Michael, ,,A Classical Introduction to Modern Number Theory", Springer, New York 1988
3. Leveque William Judson ,,Fundamentals of Number Theory", Addison-Wesley Publishing Company, 1977
4. Schneier Bruce ,,Applied Cryptography", WNT, Warsaw 1995.
5. Ribenboim Paulo ,,The Little Book of Big Primes", Springer-Verlag, New York Berlin Heidelberg 1991
6. Urbanowicz Jerzy Eugeniusz ,,Asymmetrical cryptography" - undergraduate lecture for IV/V - year students of mathematics at KUL in 2005/2006.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 221–227
ISSN 1930-1235: (2008)

# CONSTRUCTION OF LINEAR CODES HAVING PRESCRIBED PRIMAL-DUAL MINIMUM DISTANCE WITH APPLICATIONS IN CRYPTOGRAPHY

Axel Kohnert

*Mathematical Department,*
*University of Bayreuth,*
*D-95440 Bayreuth, Germany*

Abstract. A method is given for the construction of linear codes with prescribed minimum distance and also prescribed minimum distance of the dual code. This works for codes over arbitrary finite fields. In the case of binary codes Matsumoto et al. showed how such codes can be used to construct cryptographic Boolean functions. This new method allows to compute new bounds on the size of such codes, extending the table of Matsumoto et al..

## 1. Introduction

A linear $[n,k]_q-$code $C$ is a $k-$dimensional subspace of the vectorspace $GF(q)^n$, where $GF(q)$ denotes the finite field with $q$ elements. To use such a code $C$ we work with a *generator matrix* $\Gamma_C$ of $C$, which is a $k\times n$ matrix over $GF(q)$ whose rows are a basis of $C$. In coding theory we are interested in the minimum distance of the code $C$. For this we define the *Hamming distance* between two codewords (i.e. elements from $C$) $u=(u_1,\ldots,u_n)$ and $v=(v_1,\ldots,v_n)$ as the number of coordinates which are different (i.e. $u_i\neq v_i$). Then we define the *minimum distance* of $C$ as the minimum of the Hamming distance between all pairs of codewords from $C$. The interest in this number comes from the fact that is possible to correct $\lfloor (d-1)/2\rfloor$ errors if we use a code $C$ with minimum distance $d$. Such a code is called an $[n,k,d]_q-$code. In this paper $d$ will also be called primal distance.

One of the fundamental problems in coding theory [10] is the following:

**Problem 1.1.** For a fixed *length* $n$, dimension $k$ and field $GF(q)$ find a code $C$ with minimum distance $d$ as large as possible.

This original problem was modified in [16] to study cryptographic problems. We denote by $C^\perp$ the dual code (i.e. the space of all words from $GF(q)^n$ which are

*Key words and phrases.* coding theory, minimum distance, dual minimum distance, Boolean function .

The author wants to thank the NATO for providing a grant to cover travel costs.

orthogonal to all words from $C$) and by $d^\perp$ the minimum distance of the dual code. Now the problem in [16] can be stated as follows:

**Problem 1.2.** For fixed parameters $n, k, q$ and given *primal distance* $d$ and given *dual distance* $d^\perp$ find a code $C$ with these properties.

Such a code is called an $[n, k, d, d^\perp]_q-$code. The interest in this questions comes from the fact that the generator matrix of such a code in the binary case (i.e. $q = 2$) can be used for the construction of cryptographic Boolean functions satisfying special propagation properties [14].

## 2. Geometric Description

It is known that the above problem 1.1 of finding a $[n, k]_q-$code of high minimum distance can be restated in a geometrical setting. Denote by $PG(k-1, q)$ the *finite projective geometry* of dimension $k-1$ over the finite field $GF(q)$. For our purpose we identify $PG(k-1, q)$ with the *linear lattice* of subspaces of $GF(q)^k$. The points of $PG(k-1, q)$ are the one-dimensional subspaces, the hyperplanes are the $(k-1)-$dimensional subspaces. In general an $m-$flat is the a $(m+1)-$dimensional subspace of $GF(q)^k$. The correspondence between $k-$dimensional codes over $GF(q)$ is via the columns of a generator matrix. Each column generates a one-dimensional subspace of $GF(q)^k$. This defines a correspondence $\phi$ between an $n-$element set of points in $PG(k-1, q)$ and an $[n, k']_q-$code where $k'$ may be less than $k$. To use $\phi$ for our purposes we have to restrict on one side to *non-degenerate* codes (i.e. without an all-zero column in a generator matrix) and we have to allow a multiset of points in $PG(k-1, q)$ on the other side to handle the case of columns in the generator matrix, which are equal or differ only by the multiplication of a nonzero element in $GF(q)$. Then there is the well-known

**Theorem 2.1.** [2, 4] *There exists a non-degenerate $[n, k]_q-$ code with minimum distance at least $d$, if and only if there is a multiset $X$ of size $n$ of points in $PG(k-1, q)$ with the property:*

*Each hyperplane in $PG(k-1, q)$ contains at most $n-d$ points of $X$.*

To handle the dual distance we have to use the following

**Theorem 2.2.** [2, 4]

*Let $C$ be a $[n, k]_q-$code $C$ with a check matrix $\Gamma^\perp$. $C$ has minimum distance greater or equal $d$, if and only if there are no $d-1$ columns in $\Gamma^\perp$ which are linearly dependent.*

Then the solution of the extended problem 1.2 can be formulated using above geometric description.

**Corollary 2.3.**

*There exists a non-degenerate $[n, k]_q-$ code with minimum distance at least $d$ and dual distance at least $d^\perp$, if and only if there is a multiset $X$ of size $n$ of points in $PG(k-1, q)$ with the following properties:*

- *each hyperplane in $PG(k-1, q)$ contains at most $n-d$ points of $X$.*
- *each $m-$flat contains at most $m+1$ points of $X$. (for all $m$ from $0, \ldots, d^\perp - 3$)*

The second condition is always true if we ask for dual distance 2. In this case we can get a solution which is a real multiset. In all other cases with $d^\perp$ greater than two, $X$ will not be a multiset, as the second condition says for $m = 0$ that there are no multiple points. In the following we will try to construct an $[n, k, d, d^\perp]-$code using this geometric description.

## 3. Diophantine System of Equations

To use above characterization for the construction of codes satisfying the conditions of corollary 2.3 we restate this using a Diophantine system of equations. This was already done in [5, 6] for the case where we only prescribed the minimum distance and not also the dual distance. Denote by $M^m$ the $(m-$flat$)-$point incidence matrix of $PG(k-1, q)$. The rows are labeled by the $m-$flats the columns are labeled by the points of $PG(k-1, q)$. We have

$$M^m_{i,j} = \begin{cases} 1 & \text{point } j \text{ is in flat } i \\ 0 & \text{else} \end{cases}.$$

We denote the number of rows of $M^m$ by $r_m$. The number of columns is $r_0$. Now we can solve both problems from the introduction in Section 1 by solving a Diophantine system of equations.

**Theorem 3.1.** [5, 6]
*There exists a non-degenerate $[n, k]_q-$ code with minimum distance at least $d$, if and only if there is a integral non-negative solution $x = (x_1, \ldots, x_{r_0})$ of the following Diophantine system:*

- $x_1 + \ldots + x_{r_0} = n$.
- $M^{k-2}x^T \leq \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix}$.

*where the inequality in the second part is to be read componentwise.*

This Diophantine system is now enlarged by the conditions prescribing the dual distance:

**Theorem 3.2.**
*There exists a non-degenerate $[n, k]_q-$ code with primal distance at least $d$ and dual distance at least $d^\perp$, if and only if there is a integral non-negative solution $x = (x_1, \ldots, x_{r_0})$ of the following Diophantine system:*

- $x_1 + \ldots + x_{r_0} = n$.
- $M^{k-2}x^T \leq \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix}$.
- $M^0 x^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$.
- $M^1 x^T \leq \begin{pmatrix} 2 \\ \vdots \\ 2 \end{pmatrix}$.

- $\vdots$
- $M^{d^{\perp}-3}x^T \leq \begin{pmatrix} d^{\perp}-2 \\ \vdots \\ d^{\perp}-2 \end{pmatrix}$.

## 4. Prescribing Automorphisms

The size of these Diophantine systems are given by the size of the corresponding projective geometry. They become too large for increasing parameters $k$ and $q$ to be solved directly. Like in the papers describing the solution of problem 1.1 we reduce the size of problem by prescribing automorphisms. Let $G$ be a subgroup of $GL(k,q)$ acting on the subspaces of $GF(q)^k$. The induced action of $G$ on the $m-$flats of $PG(k-1,q)$ gives a partition of the $r_m$ $m-$flats into $r_{G,m}$ orbits denoted by $\omega_{G,m,1}, \omega_{G,m,2}, \ldots$. By $V_{G,m,i}$ we denote an representative of the orbit $\omega_{G,m,i}$. Then we define a condensed matrix $M^{G,m}$ by setting:

$$M^{G,m}_{i,j} := \left|\{x \in \omega_{G,0,j} : x \in V_{G,m,j}\}\right|.$$

This is a matrix with $r_{G,m}$ rows and $r_{G,0}$ columns. This matrix is well-defined as the definition is independent of the choice of the representative $V_{G,m,i}$. We get the same matrix if we add up the columns of $M^m$ corresponding to the points in the orbit of $G$. The action of $G$ is compatible with the incidence relation. This means for points $p$ and $m-$flats $V$ and $\phi \in G$ we have:

$$p \in V \iff \phi(p) \in \phi(V).$$

Therefore after the addition of columns the rows corresponding to $m-$flats in an orbit are equal. If we take only one copy for each orbit we get again the matrix $M^{G,m}$. This action of $G$ on the points (= columns of a generator matrix) is used for the following definition: A linear code $C$ has $G$ as a group of symmetries if there is a generator matrix $\Gamma$ of $C$ whose columns correspond to full orbits of $G$ on the 1-subspaces of $GF(q)^k$. We get a new version of theorem 3.2 using the condensed matrix:

**Theorem 4.1.**

*There exists a non-degenerate $[n,k]_q-$ code with primal distance at least $d$ and dual distance at least $d^{\perp}$ and a group of symmetries which contains $G$ as a subgroup if and only if there is a integral non-negative solution $x = (x_1, \ldots, x_{r_{G,0}})$ of the following Diophantine system:*

- $\left|\omega_{G,0,1}\right| x_1 + \ldots + \left|\omega_{G,0,r_{G,0}}\right| x_{r_{G,0}} = n$.
- $M^{G,k-2}x^T \leq \begin{pmatrix} n-d \\ \vdots \\ n-d \end{pmatrix}$.
- $M^{G,0}x^T \leq \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$.
- $M^{G,1}x^T \leq \begin{pmatrix} 2 \\ \vdots \\ 2 \end{pmatrix}$.

- $\vdots$
- $M^{G,d^\perp-3}x^T \leq \begin{pmatrix} d^\perp-2 \\ \vdots \\ d^\perp-2 \end{pmatrix}$.

## 5. Results

For the binary case, which is the interesting for cryptographic applications, the authors

defined in [16] the number $N(d, d^\perp)$ as the minimal length of a linear binary code with minimum distance $d$ and dual distance $d^\perp$. They gave lower and upper bounds and computed the exact values for some combinations of the two parameters. This was done by exhaustive search. Their result was the following table:

| $d\backslash d^\perp$ | 3 | 4 | 5 | 6 |
|---|---|---|---|---|
| 3 | 6 | – | | |
| 4 | 7 | 8 | | |
| 5 | 11 | 13 | 16 | |
| 6 | 12 | 14 | 17 | 18 |
| 7 | 14 | 15 | | |
| 8 | 15 | 16 | | |

To extend their results we first make use of the classification of small binary linear codes done by Anton Betten in [2]. Two binary codes are isomorphic if they differ only by a permutation of the coordinates. The work of Betten allows us to specify the minimum distance $d$ and the length $n$, and we get (in the smaller cases) the number of different (=non-isomorphic) codes together with a generator matrix. Given such a generator matrix we compute the weight-enumerator together with the dual weight-enumerator, which we get using MacWilliams theorem. This allows us to extend the table:

| $d\backslash d^\perp$ | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|
| 3 | 6 | – | | | | |
| 4 | 7 | 8 | | | | |
| 5 | 11 | 13 | 16 | | | |
| 6 | 12 | 14 | 17 | 18 | | |
| 7 | 14 | 15 | $19-20$ | $20-21$ | 22 | |
| 8 | 15 | 16 | $20-21$ | $21-22$ | 23 | 24 |

Using the program of Ryutaroh Matsumoto for the computation of the lower bound for $N(d, d^\perp)$ given by their version of the linear programming bound in [16] we are able to show that some of the newly found codes are as short as possible. The code $C$ found for $N(7, 7)$ is a formally self-dual code. The weight-enumerator of $C$ and $C^\perp$ are equal. The code found for $N(8, 8)$ is a self-dual code. For larger numbers no classification results are available. But we can apply the methods described in the previous section.

Using the methods described in Section 4 we were able to construct for fixed $q, n, k$ linear codes with prescribed distances $d$ and $d^\perp$ for arbitrary finite fields. As an example for the non-binary case we give a table for $q = 3$ and $k = 5$ which lists

for fixed $d^\perp = 4$ and all lengths $n$ the maximum possible minimum distance $d$ for which we were able to construct a code using our method. From the theory of caps in $PG(4,3)$ [12] it is known, that the maximum length of code with $d^\perp = 4$ is 20.

| $n$ | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|
| $d$ | 2 | 2 | 3 | 4 | 5 | 6 | 6 | 6 |
| $n$ | 14 | 15 | 16 | 17 | 18 | 19 | 20 | |
| $d$ | 7 | 8 | 8 | 9 | 10 | 11 | 12 | |

Only in the case $n = 16$ this number $d$ may not be the best possible value. There may be an other codes having primal distance 9 which we didn't found using our method. In all other cases it is known that the found minimum distance is at an upper limit, in most cases given by the Griesmer bound.

This method works for arbitrary finite fields, so we define $N_q(d, d^\perp)$ as the minimal length of a linear code over the alphabet $GF(q)$ with minimum distance $d$ and dual distance $d^\perp$. From the constructed codes we can give upper bounds for $N_q(d, d^\perp)$. From the above table for $q = 3$ and $k = 5$ we get for example $N_3(4, 4) \leq 9$.

## 6. Related Work

There are several papers, which study caps [1, 4, 11, 12] in the finite projective geometry $PG(k-1, q)$. These are set of points with the additional property that on each line are at most 2 points. Now one question is which is the maximal possible size of such a point-set. If we translate the caps property into the language of the dual distance, we ask for dual distance = 4 but without any restrictions on the primal distance.

The reduction of the ($m-$flat)–point incidence matrix $M^m$ using automorphisms is a general approach that works for many incidence structures for example designs [3, 15], $q$-analogs of designs [8], parallelisms in projective geometries [7]. The first application was in the work of Kramer and Mesner [13].

After the initial definition of the cryptographic applications it was already in the work of Carlet that he looked at the Kerdock and Preparata codes [9]. These are linear codes over the ring $\mathbb{Z}_4$. It would be interesting to apply the above method for the construction of codes with prescribed dual distance also in the case of $\mathbb{Z}_4$ and other rings.

## 7. Acknowledgment

The author thanks Ryutaroh Matsumoto for his helpful comments and for providing a copy of his program for the calculation of the linear programming bound from [16] which we used in section 5.

## References

[1] J. Barát, Y. Edel, R. Hill, and L. Storme. On complete caps in the projective geometries over $\mathbb{F}_3$. II: New improvements. *J. Comb. Math. Comb. Comput.*, 49:9–31, 2004.

[2] Anton Betten, Michael Braun, Harald Fripertinger, Adalbert Kerber, Axel Kohnert, and Alfred Wassermann. *Error-correcting linear codes. Classification by isometry and applications. With CD-ROM.* Algorithms and Computation in Mathematics 18. Berlin: Springer. xxix, 798 p. , 2006.

[3] Anton Betten, Adalbert Kerber, Axel Kohnert, Reinhard Laue, and Alfred Wassermann. The discovery of simple 7-designs with automorphism group PΓL(2, 32). Cohen, Gérard (ed.) et al., Applied algebra, algebraic algorithms and error-correcting codes. 11th international symposium, AAECC-11, Paris, France, July 17-22, 1995. Proceedings. Berlin: Springer-Verlag. Lect. Notes Comput. Sci. 948, 131-145 (1995)., 1995.

[4] Juergen Bierbrauer. *Introduction to coding theory.* Discrete Mathematics and its Applications. Boca Raton, FL: Chapman & Hall/CRC. xxiii, 390 p., 2005.

[5] M. Braun. Construction of linear codes with large minimum distance. *IEEE Transactions on Information Theory*, 50(8):1687–1691, 2004.

[6] M. Braun, A. Kohnert, and A. Wassermann. Optimal linear codes from matrix groups. *IEEE Transactions on Information Theory*, 12:4247–4251, 2005.

[7] Michael Braun. Construction of a point-cyclic resolution in PG(9,2). *Innov. Incidence Geom.*, 3:33–50, 2006.

[8] Michael Braun, Adalbert Kerber, and Reinhard Laue. Systematic construction of $q$-analogs of $t$-$(v, k, \lambda)$-designs. *Des. Codes Cryptography*, 34(1):55–70, 2005.

[9] Claude Carlet. On cryptographic propagation criteria for Boolean functions. *Inf. Comput.*, 151(1-2):32–56, 1999.

[10] Ray Hill and Emil Kolev. A survey of recent results on optimal linear codes. In *Holroyd, Fred C. (ed.) et al., Combinatorial designs and their applications. Proceedings of the one-day conference, Milton Keynes, UK, 19 March 1997. London: Chapman & Hall/CRC. Chapman & Hall/CRC Res. Notes Math. 403, 127-152* . 1999.

[11] J.W.P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces: Update 2001. Blokhuis, A. (ed.) et al., Finite geometries. Proceedings of the fourth Isle of Thorns conference, Brighton, UK, April 2000. Dordrecht: Kluwer Academic Publishers. Dev. Math. 3, 201-246 (2001)., 2001.

[12] J.W.P. Hirschfeld and J.A. Thas. *General Galois geometries.* Oxford Mathematical Monographs. Oxford: Clarendon Press. xii, 407 p. , 1991.

[13] Earl S. Kramer and Dale M. Mesner. t-designs on hypergraphs. *Discrete Math.*, 15:263–296, 1976.

[14] Kaoru Kurosawa and Takashi Satoh. Design of SAC/PC($l$) of order $k$ Boolean functions and three other cryptographic criteria. *Lecture Notes in Computer Science*, 1233:434–449, 1997.

[15] Reinhard Laue, Anton Betten, and Evi Haberberger. A new smallest simple 6-design with automorphism group $A_4$. *Congr. Numerantium*, 150:145–153, 2001.

[16] R. Matsumoto, K. Kurosawa, T. Itoh, T. Konno, and T. Uyematsu. Primal-dual distance bounds of linear codes with application to cryptography. *IEEE Transactions on Information Theory*, 52(9):4251–4256, 2006.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 229–234
ISSN 1930-1235: (2008)

# ON SOME PROPERTIES OF GRAPH BASED PUBLIC KEYS

ANETA WROBLEWSKA

*Maria Curie-Skłodowska University*
*Lublin, Poland.*
*e-mail: wroblewska-aneta@wp.pl*

Abstract. In this paper we will evaluate degrees of nonlinear polynomial encryption transformation in $F_q^n$, which was defined in [11] in terms of the walk on the graph with vertex set $F_q^n \cup F_g^n$. Independently from the length of the walk, this transformation has degree 3. It means that public user can do the encryption process in polynomial time.

## 1. Introduction

We will study some properties of graph base public key algorithm, which was proposed in [11]. Some generalization of this method the reader can find in [13], [14]. First (Section 2) we introduce some definitions needed to describe our algorithm. Like in the well known example of polynomial encryption used by Imai and Matsumoto or Patarin in his "small dragon" ([6], [7]) in Section 3 we combine "graphical encryption" $P$ with two affine transformations $T_1$ and $T_2$ and work with the public map $Q = T_1PT_2$. After such transformation we get a system of polynomial map and in Section 4 we will investigate its degrees in order to find out a heuristic complexity of this cryptosystem.

Let us use traditional characters in Cryptography: Alice is the holder of the key, Bob — the public user and the cryptoanalyst — Catherine ([5], [6]). The speed of the software implementation of symmetric encryption algorithm for Alice is evaluated in [14]. Evaluation of the degree of the transformation demonstrated the feasibility of the algorithm for Bob.

## 2. Graph based encryption algorithm

We define graph as an irreflexive and symmetric binary relation $\phi \subset V \times V$, where V is the set of vertices. Missing graph theoretical definition can be find in [1], [2]. In this subsection we will consider the *parallelotopic graphs* and linguistic graph with alphabet $M = GF(q)$. Here, our messages (plaintexts or ciphertexts) and enryption tools (passwords) are tuples over $GF(q)$. What is important the idea can be expand to arbitrary chosen commutative ring $K$, which leads to a very fast cryptoalgorithm (operation in $K = Z_{p^n}$ are much faster than in case of $F_{p^n}$ for large $n$).

We say that $\Gamma = (\Gamma, M, \pi)$ is a *parallelotopic graph* over a finite set $M$ if we have a surjective function $\pi : V(\Gamma) \to M$ such that for every pair $(v, m)$, $v \in V(\Gamma)$,

*Key words and phrases.* Public Key Cryptography, polynomial encryption.

$m \in M$, there is a unique neighbour $u$ of $v$ satisfying $\pi(u) = m$. For given vertex $v$, and any colour $m$, there exists exactly one neighbour $u$ of $v$ of colour $m$. Then the neighborhood of each vertex looks like rainbow ie. consist of $|M|$ vertices of different colours. This is obvious that the graph is $k$-regular with $k = |M|$.

Let $\Gamma$ be a parallelotopic graph. We shall treat its vertices as plaintexts. So the set of vertices $V(\Gamma)$ is the plainspace and cipherspace. Let $N(t, v)$ be the operator taking the neighbour $u$ of a vertex $v$ with colour $t$. Then the password be the string of colours $(t_1, t_2, \ldots, t_n)$, $t_i \in M$ such that $t_i \neq t_{i+2}$ and encryption process is the composition $N_{t_1} \times N_{t_2} \times \cdots N_{t_n}$ of bijective maps $N_{t_i} : V(\Gamma) \to V(\Gamma)$. If the plaintext $v \in V(\Gamma)$ is given, then the encryption procedure corresponds to the followin chain in the graph: $v \to v_1 = N(t_1, v) \to v_2 = N(t_2, v_1) \to \cdots \to v_n = N(t_n, v_{n-1})$. It is clear that $(t_{n-1}, \cdots, t_1, c(v))$ is the "decoding tuple", because it corresponds to the decoding arc.

We use the term linguistic graph over $GF(q)$ when we have a linguistic graph with alphabet $M = GF(q)$ and the set of neighbors of any vertex $v$ is an algebraic manifold over $GF(q)$, i.e. is the totality of solutions of a certain system of polynomial equations.

Let $P$ and $L$ be two $n$-dimensional vector spaces over $GF(q)$. Elements of $P$ will be called *points* and those of $L$ *lines*. To distinguish points from lines we use parentheses and brackets: If $x \in V$, then $(x) \in P$ and $[x] \in L$. It will also be advantageous to chose two fixed bases and write:

$$(p) = (p_1, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, p_{3,2}, p_{3,3}, p'_{3,3}, \ldots)$$

$$[l] = [l_1, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, l_{3,2}, l_{3,3}, l'_{3,3}, \ldots]$$

We now define an incidence structure $(P, L, I)$ as follows. We say the point $(p)$ is incident with the line $[l]$, and we write $(p)I[l]$, if the following relations between their coordinates hold:

$$l_{1,1} - p_{1,1} = l_1 p_1$$

$$l_{1,2} - p_{1,2} = l_{1,1} p_1$$

$$l_{2,1} - p_{2,1} = l_1 p_{1,1}$$

$$l_{i,i} - p_{i,i} = l_1 p_{i-1,i}$$

$$l'_{i,i} - p'_{i,i} = l_{i,i-1} p_1$$

$$l_{i,i+1} - p_{i,i+1} = l_{i,i} p_1$$

$$l_{i+1,i} - p_{i+1,i} = l_1 p'_{i,i}.$$

To decrypt the data we use a key or password of length $m$, $\rho = (\alpha_1, \ldots, \alpha_m)$, where $\alpha_i$'s are password characters such as $\alpha_i$ is different from $\alpha_{i+2}$. Each arc of the graph represents one possible character. For the plaintext $(p_1, \ldots, p_n)$, in each number of walk $j$, $l_1$ or $p_1$ will be $p_1 + \alpha_1 \cdots + \alpha_j$.

## 3. Linguistic graphs system hidden by the affine transformation.

Let $F_q$, $q > 2$ be the finite field, where $q$ is a prime power. Alice shall be using the hidden graph scheme based on the family of linguistic graphs $L_n(q)$ with the operators $N_c(v)$ to take the neighbour $u$ of vertex $v$ such that $c$ is the colour of $u$. As in previous section the plaintext and the ciphertext are $n$-tuples over $F_q$, $q > 2$ and we identify them with points (or lines) of the graph $L_n(q)$. Alice shall choose to keep her graph secret.

In transforming plaintext into ciphertext Alice shall work with two intermediate vectors denoted $\mathrm{u} = (u_1, \ldots, u_n) \in {F_q}^n$ and $\mathrm{v} = (v_1, \ldots, v_n) \in {F_q}^n$. First, Alice choose the constant password $\alpha = \alpha_1\alpha_2 \ldots \alpha_n$. In addition, Alice chooses two secret affine transformations, i.e. two invertible matrices $A = (a_{ij}), 1 \leq i, j \leq n$ and $B = (b_{i,j}), 1 \leq i, j \leq n$ with entries in $F_q$ and the constant vectors $\mathrm{c} = (c_1, \ldots, c_n)$ and $\mathrm{d} = (d_1, \ldots, d_n)$. We use the two affine transformations in order to hide the graph and to hide the walk on the hidden graph. Then, she sets $\mathrm{u} = A \times \mathrm{x} + \mathrm{c}$. Next, she would like to have $\mathrm{v} \in {F_q}^n$ simply equal to the $\mathrm{v} = N(\mathrm{u})$, received from graph based algorithm. Finally, Alice sets $\mathrm{y} = B^{-1}(\mathrm{v} - \mathrm{d})$ (that is $\mathrm{v} = B\mathrm{y} + \mathrm{d}$). After, Alice will combine $T$ with two affine transformations and get a formula: $\mathrm{y} = (F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n)$, where $F_i(x_1, \ldots, x_n)$ are polynomials in $n$ variables written in expanded form, i.e. as the sums of monomials of kind ${x_1}^{i_1} \ldots {x_n}^{i_n}$ with the coeficients from $F_q$. Alice makes polynomial equations $y_i = F_i(x_1, \ldots, x_n)$ public.

Again, like in Imai-Matsumoto scheme, if Bob wants to send her a plaintext message x, he just substitutes $x_i$ in the public equations and finds $y_i$. On the other hand Catherine, who knows only the ciphertext and the public key must solve a nonlinear system for the unknowns $x_i$.

When Alice receives the ciphertext y, she uses her knowledge of $A, B, \mathrm{c}, \mathrm{d}$, graph $L_n(q)$ and the password. Namely, she shall compute $\mathrm{v} = B\mathrm{y} + \mathrm{d}$. Then Alice using iterative process of decryption based on the graph can compute $\mathrm{u} = N^{-1}(\mathrm{v})$. Finally, she computes the plaintext $\mathrm{x} = A^{-1} \times (\mathrm{u} - \mathrm{c})$.

## 4. Degrees of polynomials in ciphertext

Before applying affine transformation we want to find out a degree of polynomial map $T : u \to v$. We take the password $\alpha = \alpha_1\alpha_2 \ldots \alpha_n$ which is used by adding element $\alpha_j$ to the first character of the encrypted data in each walk number $j$. Therefore we are getting transformation $T_{\alpha_1}T_{\alpha_2} \ldots T_{\alpha_n}$. If we treat the elements of the plain data before encryption as variables, in each transformation $T_{\alpha_1}$, $T_{\alpha_1}T_{\alpha_2}$, $T_{\alpha_1}T_{\alpha_2} \ldots T_{\alpha_n}$ we get a polynomials of these variables. We would like to find out a degree of the polynomials.

4.1. **Transformation $T_{\alpha_1}$.** Our research we start with studying transformation $T_{\alpha_1}$. Hence we have:

$$l_1 = p_1 + \alpha_1 \qquad \deg l_1 = 1$$

$$l_{1,1} = p_{1,1} + l_1p_1 = p_{1,1} + \alpha_1p_1 + p_1^2$$

$$l_{1,2} = p_{1,2} + p_1l_{1,1} = p_{1,2} + p_1p_{1,1} + \alpha_1p_1^2 + p_1^3$$

$$l_{i,i} = p_{i,i} + l_1p_{i-1,i} = p_{i,i} + \alpha_1p_{i-1,i} + p_1p_{i-1,i}$$

$$l_{i,i+1} = p_{i,i+1} + p_1l_{i,i} = p_{i,i+1} + \alpha_1p_1p_{i-1,i} + p_1p_{i,i} + p_1^2p_{i-1,i}.$$

Similarly we are receiving:

$$l_{i+1,i} = p_{i+1,i} + l_1 p_{i,i}^{'} = p_{i+1,i} + \alpha_1 p_{i,i}^{'} + p_1 p_{i,i}^{'}$$

$$l_{i,i}' = p_{i,i}' + p_1 l_{i,i-1} = p_{i,i}' + \alpha_1 p_1 p_{i-1,i-1}' + p_1 p_{i,i-1} + p_1^2 p_{i-1,i-1}.$$

So if we take the plane data $(p)$ as $(p_1, p_2, \ldots, p_n)$ after this transformation we get the line vertex $f_1(p_1), f_2(p_1, p_2), \ldots, f_n(p_1, p_2, \ldots, p_n)$,

$$\deg f_n(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 2, & n = 2, \\ 2, & n = 4k, 4k+1, \\ 3, & n = 4k+2, 4k-1 \quad \text{where} \quad k = 1, 2, 3 \ldots \end{cases}$$

4.2. **Transformation $T_{\alpha_1} T_{\alpha_2}$.** Using the previous part of the calculation (transformation $T_{\alpha_1}$) we can calculate elements of the encrypted data after transformation $T_{\alpha_2}$.

$$p_1^{(2)} = p_1 + \alpha_1 + \alpha_2$$

$$p_{1,1} = l_{1,1} - l_1 p_1^{(2)} = -(\alpha_1 + \alpha_2)(\alpha_1 + p_1)$$

$$p_{1,2}^{(2)} = l_{1,2} - p_1^{(2)} l_{1,1} = p_{1,2} - (\alpha_1 + \alpha_2) p_{1,1} - \alpha_1(\alpha_1 + \alpha_2) p_1 - (\alpha_1 + \alpha_2) p_1^2$$

$$p_{i,i+1}^{(2)} = l_{i,i+1} - p_1^{(2)} l_{i,i} = p_{i,i+1} - (\alpha_1 + \alpha_2)(p_{i,i} + \alpha_1 p_{i-1,i} + p_1 p_{i-1,i})$$

$$p_{i,i}^{(2)} = l_{i,i} - l_1 p_{i-1,i}^{(2)} = p_{i,i} + (\alpha_1 + p_1)(\alpha_1 + \alpha_2)(p_{i-1,i-1} + \alpha_1 p_{i-2,i-1} + p_1 p_{i-2,i-1})$$

Similarly we are receiving:

$$p_{i,i}^{\prime(2)} = l_{i,i}' - p_1^{(2)} l_{i,i-1} = p_{i,i}^{'} - (\alpha_1 + \alpha_2)(p_{i,i-1} + \alpha_1 p_{i-1,i-1} + p_1 p_{i-1,i-1}')$$

$$p_{i+1,i}^{(2)} = l_{i+1,i} - l_1 p_{i,i}^{\prime(2)} = p_{i+1,i} + (\alpha_1 + p_1)(\alpha_1 + \alpha_2)(p_{i-1,i-1} + \alpha_1 p_{i-1,i-1}' + p_1 p_{i-1,i-1}')$$

Hence we got vertex point $(p) = (g_1(p_1), g_2(p_1, p_2), \ldots, g_n(p_1, p_2, \ldots, p_n))$ and degrees of each component are following:

$$\deg g_n(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 1, & n = 2, \\ 2, & n = 4k-1, 4k+2, \\ 3, & n = 4k, 4k+1 \quad \text{where} \quad k = 1, 2, 3 \ldots \end{cases}$$

4.3. **Transformation $T_{\alpha_1} T_{\alpha_2} \ldots T_{\alpha_m}$.** Degrees of elements of vertex point and vertex line after transformation $T_{\alpha_1} T_{\alpha_2} \ldots T_{\alpha_{m-1}}$ and $T_{\alpha_1} T_{\alpha_2} \ldots T_{\alpha_m}$ respectively, we will calculate using induction, imposing $m$-even.

Assume transformation $T_{\alpha_1} T_{\alpha_2} \ldots T_{\alpha_{m-3}}$ gave us vertex point:

$$(p)^{(m-3)} = (g_1^{(m-3)}(p_1), g_2^{(m-3)}(p_1, p_2), \ldots, g_n^{(m-3)}(p_1, p_2, \ldots, p_n))$$

with degree

$$\deg g_n^{(m-3)}(p_1, p_2, \ldots, p_n) = \begin{cases} 1, & n = 1, \\ 1, & n = 2, \\ 2, & n = 4k-1, 4k+2, \\ 3, & n = 4k, 4k+1 \quad \text{where} \quad k = 1, 2, 3, \ldots \end{cases}$$

and vertex line after transformation $T_{\alpha_1} T_{\alpha_2} \ldots T_{\alpha_{m-2}}$:

$$[l]^{(m-2)} = (f_1^{(m-2)}(p_1), f_2^{(m-2)}(p_1, p_2), \ldots, f_n^{(m-2)}(p_1, p_2, \ldots, p_n))$$

with degree

$$\deg f_n^{(m-2)}(p_1,p_2,\ldots,p_n)=\begin{cases}1, & n=1,\\ 2, & n=2,\\ 2, & n=4k,4k+1,\\ 3, & n=4k+2,4k-1 \quad \text{where} \quad k=1,2,3,\ldots\end{cases}$$

Now we have to check the degree of polynomial $g_n^{(m-1)}$.

$$\begin{aligned}p_1^{(m-1)} &= p_1+\alpha_1+\alpha_2+\ldots+\alpha_{m-3}+\alpha_{m-2}+\alpha_{m-1}\\ &= p_1^{(m-3)}+\alpha_{m-2}+\alpha_{m-1}\\ p_{i,i+1}^{(m-1)} &= l_{i,i+1}^{(m-2)}-p_1^{(m-1)}l_{i,i}^{(m-2)}\\ &= p_{i,i+1}^{(m-3)}+p_1^{(m-3)}l_{i,i}^{(m-2)}-p_1^{(m-3)}l_{i,i}^{(m-2)}-(\alpha_{m-2}+\alpha_{m-1})l_{i,i}^{(m-2)}\\ &= p_{i,i+1}^{(m-3)}-(\alpha_{m-2}+\alpha_{m-1})l_{i,i}^{(m-2)}\end{aligned}$$

Since $p_{i,i+1}^{(m-3)}$ is independent from $\alpha_{m-2}$ and $\alpha_{m-1}$ and both $p_{i,i+1}^{(m-3)}$ and $l_{i,i}^{(m-2)}$ have degree equal 2, we get that $p_{i,i+1}^{(m-1)}$ has degree 2.

By similar reasoning we obtain that $p_{i,i}^{(m-1)}$ has degree 3, $p_{i,i}^{'(m-1)}$ degree 2, $p_{i+1,i}^{(m-1)}$ degree 3.

Hence by means of transformation $T_{\alpha_1}T_{\alpha_2}\ldots T_{\alpha_{n-1}}$ we encoded plain text $(p_1,p_2,\ldots,p_n)$ on ciphertext

$$(p)^{(m-1)}=(g_1^{(m-1)}(p_1),g_2^{(m-1)}(p_1,p_2),\ldots,g_n^{(m-1)}(p_1,p_2,\ldots,p_n))$$

with degree

$$\deg g_n^{(m-1)}(p_1,p_2,\ldots,p_n)=\begin{cases}1, & n=1,\\ 1, & n=2,\\ 2, & n=4k-1,4k+2,\\ 3, & n=4k,4k+1 \quad \text{where} \quad k=1,2,3,\ldots\end{cases}$$

In the same way using second part of inductive assumption we get the ciphertext $[l]^{(m)}=(f_1^{(m)}(p_1),f_2^{(m)}(p_1,p_2),\ldots,f_n^{(m)}(p_1,p_2,\ldots,p_n))$ after transformation $T_{\alpha_1}T_{\alpha_2}\ldots T_{\alpha_m}$ with

$$\deg f_n^{(m)}(p_1,p_2,\ldots,p_n)=\begin{cases}1, & n=1,\\ 2, & n=2,\\ 2, & n=4k,4k+1,\\ 3, & n=4k+2,4k-1 \quad \text{where} \quad k=1,2,3,\ldots\end{cases}$$

## 5. Remarks on the complexity of public rules

Using previous subsections, combining graph transformation $T$ with two affine transformation, Bob get a formula:

$$y=(F_1(x_1,\ldots,x_n),\ldots,F_n(x_1,\ldots,x_n)),$$

where $F_i(x_1,\ldots,x_n)$ are polynomials of $n$ variables written as the sums of monomials of kind $x_{i_1}\ldots x_{i_3}$, where $i_1,i_2,i_3\in 1,2,\ldots,n$ with the coefficients from $F_q$. Hence the polynomial equations $y_i=F_i(x_1,x_2,\ldots,x_n)$, which are made public, have degree 3. Hence the process of straightforward encryption can be done in

polynomial time $O(n^4)$ (to compute one $y_i,\ i = 1, 2 \ldots, n$ we need not more than $3n^3 + n^3$ additions and multiplications). But the cryptanalyst Catherine, having a only a formula for $y$, has very hard task to solve the system of $n$ equations in $n$ variables of degree 3. We know that the variety of solution has the dimension 0. So general algorithm for such mass problem has exponential time $3^{O(n)}$ (different versions the reader can find in [3], [4], [9], [10]).

But of course for our specific system faster algorithm may exist. We encourage cryptanalysts to make an effort to break the cryptosystem.

## References


[1] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73–80.

[2] B. Bollobás, *Extremal Graph Theory*, Academic Press,

[3] B. Buchberger, *Grobner Bases: An Algorithmic Method in Polynomial Ideal Theory* , Recent Trends in Multidimentional Systems Theory, N.K.Bose ed., D.Reidel Publishing comp., 1983, 184232.

[4] J. Canny *Generalized characteristic polynomials*, J. Symbolic Computation, 1990, No. 9, 241-250.

[5] Neal Coblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer, 1994, 237 p.

[6] Neal Coblitz, *Algebraic Aspects of Cryptography*, Springer, 1998, 198 p.

[7] Imai, Matsumoto,*Public quadratic polynomial tuples for efficient signature verification and message encryption*, Advances in Cryptology, Eurocrypt '88, Springer Verlag, 419-453.

[8] F. Lazebnik F. and V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.

[9] B. Mourrain, *Bezoutian ande quotient ring structure* J. of Symbolic Computations, 39 (2005), 397-415.

[10] T. R. Seifullin, *Determination of the basis of the space of all root functionals of a system of polynomial equations and the basis of its ideal by the operation of extension of bounded root functionals* (Russian) Dopov. Nats. Akad. Nauk Ukr., Mat. Prirodozn. Tekh. Nauki 2003, No.8, 29-36 (2003)

[11] V. A. Ustimenko, *Maximality of affine group, and hidden graph cryptosystems*, J. Algebra and Discrete Math., 10 (October 2004), 51-65.

[12] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, v. 2227, 278-287.

[13] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications* In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

[14] V. Ustimenko, *On the graph based cryptography and symbolic computations*, Serdica Journal of Computing, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 235–239
ISSN 1930-1235: (2008)

# SIERPIŃSKI GASKET-BASED GRAPHS IN CODING THEORY

MONIKA KOTOROWICZ

## 1. Introduction

In this paper we build a family of hierarchical graphs based on the triangle (Sierpiński gasket-based graphs) and calculate their important characteristics, such as average degree, average shortest path length, small-world graph family characteristics. Then we present stream ciphers defined on a finite automaton corresponding to this family.

## 2. Basic network characteristics

Our family of graphs $\{\Lambda_k\}_{k\in\mathbb{N}}$ is generated in an hierarchical way (see [1]). Here $k = 1, 2, 3, \ldots$ denotes the level of the hierarchy understood as the step of the construction. The initial graph $\Lambda_1$ is the complete graph of order 3. At each step of the construction we join 3 graphs of level $k-1$ (called units) in a way shown in Figure 1.

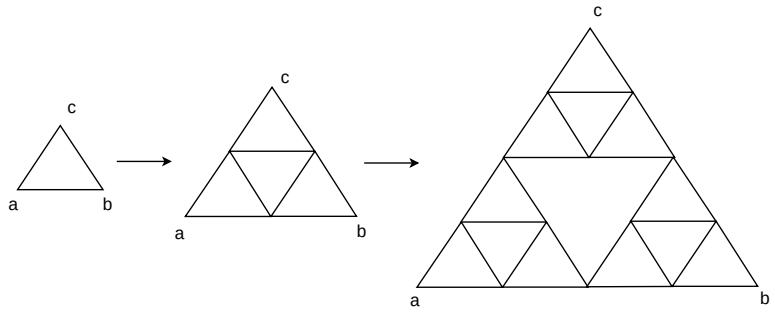



Figure 1. Construction of the graph $\Lambda_3$

Each graph has 3 external vertices of special meaning. Units of the same level are attached to them to form the unit of a higher level. In the figures we denote them by $a, b, c$. The rest of vertices are called internal.

The result is a family of Sierpiński gasket-based graphs $\{\Lambda_k\}_{k\in\mathbb{N}}$ with no loops and no multiple edges. By $V_k$ and $E_k$ we denote the sets of vertices and edges of $\Lambda_k$, respectively. One can find the *order* $|V_k|$ and the *size* $|E_k|$ of $\Lambda_k$:

$$|V_k| = \frac{3}{2}(3^{k-1}+1), \quad |E_k| = 3^k.$$

2.1. **Average degree.** Let $n_k(v)$ stand for the number of edges ending at a vertex $v \in V_k$. Clearly, $n_k(v) = 2$ for each external vertex and $n_k(v) = 4$ for each internal one. So

$$\langle n_k \rangle \stackrel{\text{def}}{=} \frac{1}{|V_k|} \sum_{v \in V_k} n_k(v) = \frac{3 \cdot 3 + 4 \cdot (|V_k| - 3)}{|V_k|}$$

which tends to 4 when $k \to \infty$.

2.2. **Average shortest-path length.** As Figure 2 suggests, it is convenient to introduce the following notations. The graph of level $k$, $k > 1$, consists of 3 subgraphs of level $k-1$

$$\Lambda_k = \Lambda^a_{k-1} \cup \Lambda^b_{k-1} \cup \Lambda^c_{k-1}.$$

Every vertex $v \in V_k$ has a label determining its place in the graph

$$v = \{\alpha_1 \alpha_2 \dots \alpha_k\}, \alpha_i \in \{a, b, c\}.$$

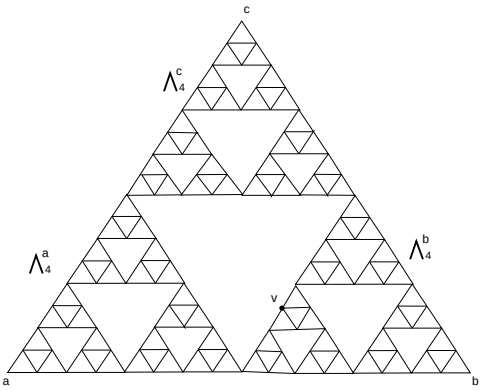



FIGURE 2. The graph of level 5

Each symbol corresponds to the choice of the triangle of the previous level. Notice that every vertex, besides the external ones, has two labels. For example the vertex $v$ in Figure 2 can be labelled by $\{bacca\}$ or $\{bacac\}$. The distance $\rho_k(v, \gamma)$ between $v$ and $\gamma \in \{a_k, b_k, c_k\}$, measured in terms of the number of edges along the path in $\Lambda_k$, is

$$\rho_k(v, \gamma) = (1 - \delta_{\alpha_k \gamma}) + \sum_{j=1}^{k-1} 2^{j-1}(1 - \delta_{\alpha_{k-j} \gamma}), \quad \delta_{\alpha_i \gamma} = \begin{cases} 1 & \alpha_i = \gamma, \\ 0 & \alpha_i \neq \gamma. \end{cases}$$

Let $v \in \Lambda^a_{k-1}$ and $w \in \Lambda^b_{k-1}$. Then the distance between $v$ and $w$ is

$$\rho_k(v, w) \leq \rho_{k-1}(v, b) + \rho_{k-1}(w, a).$$

Thus, the average shortest-path length $\rho_k$ is

$$\rho_k = \frac{\sum_{v,w \in V_k} \rho_k(v, w)}{\frac{1}{2}|V_k|(|V_k| - 1)} = \Theta(2^k).$$

2.3. **Small world graph family.** In the last years, small-world networks have been studied intensively, see [2, 3]. The family of graphs $\{\Lambda_k\}$ is a small world graph family if the diameter of $\Lambda_k$ (i. e. the maximal distance between the two vertices in $\Lambda_k$) scales logarithmically or slower with the graph size, that is,

$$\exists C > 0 \quad \mathrm{diam}\Lambda_k \leq C \log_{\langle n_k \rangle} |V_k|.$$

In our model, one has $\mathrm{diam}\Lambda_k = 2^{k-1}$ so it is not the small world graph family. We need this important information to our application in cryptography.

## 3. Cryptographical application on Sierpiński gasket-based graphs

To adapt our model described in previous section to our cryptographical application ([4, 5]) we need to make some changes. For every pair of distinct vertices connected with a simple edge we replace this edge with a pair of directed edges with opposite directions. Moreover, for every pair of distinct external vertices we add two directed edges with opposite directions (Figure 3). So every vertex $v \in V_k$ has the same number of input and output edges (equal to 4). Our graph is 4-regular.

From now on, $\Lambda_k$ and other notation stand for the changed model. Notice that the order of $\Lambda_k$ has not changed but the size of $\Lambda_k$ has ($|E_k| = 2(3^k + 3)$). Of course, the average shortest-path length and the diameter of $\Lambda_k$ has changed too. But they are still the powers of 2. So new $\{\Lambda_k\}$ is not a small world graphs family.

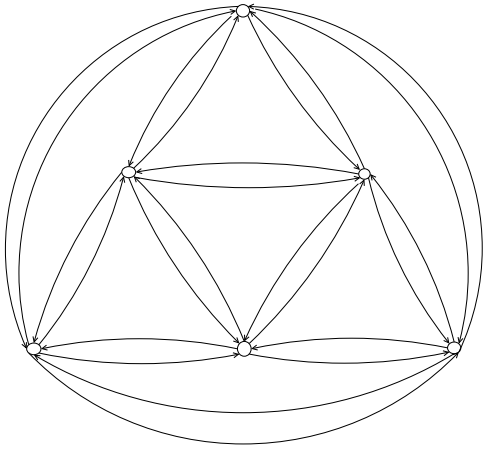


Figure 3. The graph of level 2

In this paper we use the conventional cryptographical notation. The ordinary information (called plaintext) will be transformed into an encrypted, unintelligible information (a ciphertext) by the cryptographical algorithm with a password (a key).

The vertices and the edges represent the states and the transition between these states in an automaton, respectively.

3.1. **Encryption scheme.** Let $\mathbb{F}_3^k$ be a vector space over a finite field $\mathbb{F}_3 = \{a, b, c\}$. Every vector $v = [\alpha_1\alpha_2 \ldots \alpha_k], \alpha_i \in \mathbb{F}_3$ is considered to be a vertex label in $\Lambda_k$. We identify every label $v \in \mathbb{F}_3^k$ with a plaintext or a ciphertext of length $k$. Notice that

every label points to exactly one vertex but every vertex (besides external ones) has two labels.

An encryption scheme on our graph model relies on special colouring of edges. We need to attribute a colour to each edge $e \in E_k$ in such a way that no two adjacent edges of the same direction (starting at the same vertex or ending in it) share the same colour.

**Lemma 1.** *Let $\{\Lambda_k\}_{k\in\mathbb{N}}$ be a graphs family presented above. For every $k = 1, 2, \ldots$ there exists a 4-colouring of edges such that for every vertex $v \in V_k$ any pair of edges starting (or ending) at $v$ has not the same colour. And there is a representative of each colour in the set of edges starting (or ending) at each vertex $v$.*

For example Figure 4 presents edges colouring in $\Lambda_2$. We identify a set of colours with elements of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. A path in $\Lambda_k$ between $v, w \in V_k$ is represented by a finite sequence of colours $[c_0, c_1, \ldots, c_m], c_i \in \mathbb{Z}_4$.

Let $c$ be a colour of edge from a vertex $v$ to a vertex $w$. By $c^{-1}$ we denote the colour of edge from $w$ to $v$.

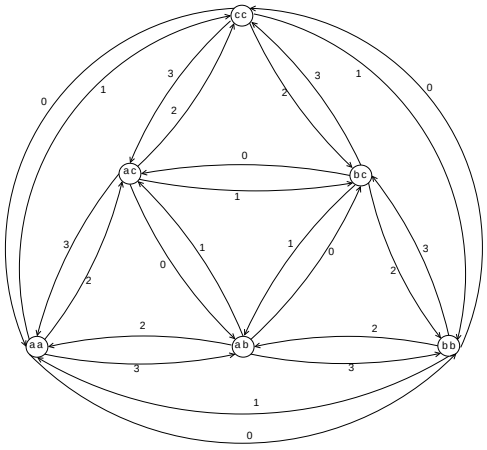



FIGURE 4. The vertex labeling and edges colouring in $\Lambda_2$

Let $p$ be a plaintext we encrypt to a ciphertext $c$. Let $v_p$ and $v_c$ be a vertices representing the plaintext and the ciphertext, respectively. The key $k = [c_0, c_1, \ldots, c_m, \eta], c_i \in \mathbb{Z}_4$, $i = 0, 1, \ldots, m$, $c_{i+1} \neq c_i^{-1}$, $\eta \in \{0, 1\}$ in an encryption procedure consisting of two parts. The first one $[c_0, c_1, \ldots, c_m]$ is the path between $v_p$ and $v_c$. The second part $\eta$ defines which one of two possible labels at $v_p$ concerns a plaintext. The space $\mathbb{F}_3^k$ is totally ordered, so we put $\eta = 0$ for the first label and $\eta = 1$ for the second one. This information is necessary to a decryption procedure.

Notice that $v_p$ is a starting state in an automaton. Every password leads us to some $v_c$ and all states (vertices) of such automaton are accepting ones.

The encryption scheme is to start in a vertex $v_p$ and pass on the graph along the path defined by a password $k$ (Figure 5). In each step of the algorithm the transition

function $f : V_k \times \mathbb{Z}_4 \to V_k$ appoints a next vertex according to the following scheme

$$\begin{array}{rcl} f(v_p, c_0) & = & v_1 \\ f(v_1, c_1) & = & v_2 \\ & \dots & \\ f(v_m, c_m) & = & v_c. \end{array} \tag{1}$$

At the end of this procedure we will reach the vertex $v_c$.

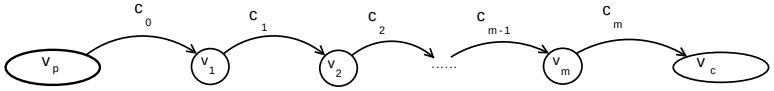



FIGURE 5. The encryption algorithm

As was mentioned above, the family $\{\Lambda_k\}_{k\in\mathbb{N}}$ is not a small world graphs family. It means that short paths between every pair of distinct vertices cannot exist. So if we choose a sufficiency long password we will be sure that ciphertext cannot be decrypted by other passwords of small length.

Each graph $\Lambda_k$ is connected and the average shortest-path length is a power of 2. Hence our algorithm is a stream cipher. Each step depends only on the state of the system after the previous step.

3.2. **Decryption procedure.** A decryption procedure bases on the inverse function $f^{-1} : V_k \times \mathbb{Z}_4 \to V_k$. The function $f^{-1}$ for $v_i \in V_k$ and $c \in \mathbb{Z}_4$ returns a vertex $v_j \in V_k$ such that $f(v_j, c) = v_i$ (one of predecessors of $v_i$ indicated by an edge of colour $c$). Knowing the ciphertext $v_c$ and the key $k = [c_0, c_1, \dots, c_m, \eta], c_i \in \mathbb{Z}_4, \eta \in \{0, 1\}$ one can obtain the vertex $v_p$ in the following decryption scheme

$$\begin{array}{rcl} f^{-1}(v_c, c_m) & = & v_m \\ f^{-1}(v_m, c_{m-1}) & = & v_{m-1} \\ & \dots & \\ f^{-1}(v_1, c_0) & = & v_p. \end{array} \tag{2}$$

Every internal vertex $v_p$ has two labels, so we have to choose the proper one using the information $\eta$ of the key $k$.

## REFERENCES

[1] Clauset A., Moore C., Newman M., *Structural Inference of Hierarchies in Networks*, In: Proceedings of the 23rd International Conference on Machine Learning, Workshop on "Statistical Network Analysis", Springer Lecture Notes in Computer Science (Pittsburgh, June 2006), also arXiv:physics/0610051v1 [physics.soc-ph] 9 Oct 2006

[2] Newman M.E.J., SIAM Review, 2003, **45**, 167 – 256

[3] Barrat A., Weigh M., Eur. Phys. J. B, 2000, **13**, 547–560

[4] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, v. 2227, 278-287.

[5] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications* In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 241–248
ISSN 1930-1235: (2008)

# DEGREE EVEN COVERINGS OF ELLIPTIC CURVES BY GENUS 2 CURVES

N. Pjero, M. Ramasaço

*Dep. of Mathematics,*
*University of Vlora, Albania*
*npjero@univlora.edu.al, ramosaco@univlora.edu.al*

T. Shaska

*Dep. of Computer Science and Electrical Engineering*
*University of Vlora, Albania*

Abstract. In this survey we study the genus 2 curves with $(n, n)$-split Jacobian for even $n$.

## 1. Introduction

Let $C$ be a genus 2 curve defined over an algebraically closed field $k$, of characteristic zero. Let $\psi : C \to E$ be a degree $n$ maximal covering (i.e. does not factor through an isogeny) to an elliptic curve $E$ defined over $k$. We say that $C$ has a *degree n elliptic subcover*. Degree $n$ elliptic subcovers occur in pairs. Let $(E, E')$ be such a pair. It is well known that there is an isogeny of degree $n^2$ between the Jacobian $J_C$ of $C$ and the product $E \times E'$. The locus of such $C$, denoted by $\mathcal{L}_n$, is a 2-dimensional algebraic subvariety of the moduli space $\mathcal{M}_2$ of genus two curves and has been the focus of many papers in the last decade; see [5, 7, 8, 9, 10, 1, 2].

The space $\mathcal{L}_2$ was studied in Shaska/Völklein [9]. The space $\mathcal{L}_3$ was studied in [5] were an algebraic description was given as sublocus of $\mathcal{M}_2$. Lately the space $\mathcal{L}_5$ has been studied in detail in [10]. The case of even degree has been less studied even though there have been some attempts lately to compute some of the cases for $n = 4$; see [4]. In this survey we study the genus 2 curves with $(n, n)$-split Jacobian for small $n$. While such curves have been studied by many authors, our approach is simply computational.

## 2. Curves of genus 2 with split Jacobians

Most of the results of this section can be found in [11]. Let $C$ and $E$ be curves of genus 2 and 1, respectively. Both are smooth, projective curves defined over $k$, $char(k) = 0$. Let $\psi : C \longrightarrow E$ be a covering of degree $n$. From the Riemann-Hurwitz formula, $\sum_{P \in C} (e_\psi (P) - 1) = 2$ where $e_\psi(P)$ is the ramification index of points $P \in C$, under $\psi$. Thus, we have two points of ramification index 2 or one point of ramification index 3. The two points of ramification index 2 can be in the same fiber or in different fibers. Therefore, we have the following cases of the covering $\psi$:

**Case I:** There are $P_1$, $P_2 \in C$, such that $e_\psi(P_1) = e_\psi(P_2) = 2$, $\psi(P_1) \neq \psi(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_\psi(P) = 1$.

**Case II:** There are $P_1$, $P_2 \in C$, such that $e_\psi(P_1) = e_\psi(P_2) = 2$, $\psi(P_1) = \psi(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_\psi(P) = 1$.

**Case III:** There is $P_1 \in C$ such that $e_\psi(P_1) = 3$, and $\forall P \in C \setminus \{P_1\}$, $e_\psi(P) = 1$.

In case I (resp. II, III) the cover $\psi$ has 2 (resp. 1) branch points in E.

Denote the hyperelliptic involution of $C$ by $w$. We choose $\mathcal{O}$ in E such that $w$ restricted to $E$ is the hyperelliptic involution on $E$. We denote the restriction of $w$ on $E$ by $v$, $v(P) = -P$. Thus, $\psi \circ w = v \circ \psi$. E[2] denotes the group of 2-torsion points of the elliptic curve E, which are the points fixed by $v$. The proof of the following two lemmas is straightforward and will be omitted.

**Lemma 1.** *a) If $Q \in E$, then $\forall P \in \psi^{-1}(Q)$, $w(P) \in \psi^{-1}(-Q)$.*
*b) For all $P \in C$, $e_\psi(P) = e_\psi(w(P))$.*

Let $W$ be the set of points in C fixed by $w$. Every curve of genus 2 is given, up to isomorphism, by a binary sextic, so there are 6 points fixed by the hyperelliptic involution $w$, namely the Weierstrass points of $C$. The following lemma determines the distribution of the Weierstrass points in fibers of 2-torsion points.

**Lemma 2.** *The following hold:*

(1) $\psi(W) \subset E[2]$
(2) *If $n$ is an odd number then*
   *i)* $\psi(W) = E[2]$
   *ii) If $Q \in E[2]$ then* $\#(\psi^{-1}(Q) \cap W) = 1 \mod (2)$
(3) *If $n$ is an even number then for all $Q \in E[2]$,* $\#(\psi^{-1}(Q) \cap W) = 0 \mod (2)$

Let $\pi_C : C \longrightarrow \mathbb{P}^1$ and $\pi_E : E \longrightarrow \mathbb{P}^1$ be the natural degree 2 projections. The hyperelliptic involution permutes the points in the fibers of $\pi_C$ and $\pi_E$. The ramified points of $\pi_C$, $\pi_E$ are respectively points in $W$ and $E[2]$ and their ramification index is 2. There is $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ such that the diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & \mathbb{P}^1 \\ \psi \downarrow & & \downarrow \phi \\ E & \xrightarrow{\pi_E} & \mathbb{P}^1 \end{array} \tag{1}$$

Next, we will determine the ramification of induced coverings $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. First we fix some notation. For a given branch point we will denote the ramification of points in its fiber as follows. Any point $P$ of ramification index $m$ is denoted by $(m)$. If there are $k$ such points then we write $(m)^k$. We omit writing symbols for unramified points, in other words $(1)^k$ will not be written. Ramification data between two branch points will be separated by commas. We denote by $\pi_E(E[2]) = \{q_1, \ldots, q_4\}$ and $\pi_C(W) = \{w_1, \ldots, w_6\}$.

2.0.1. *The Case When $n$ is Even.* Let us assume now that $deg(\psi) = n$ is an even number. The following theorem classifies the induced coverings in this case.

**Theorem 1.** *If $n$ is an even number then the generic case for $\psi : C \longrightarrow E$ induce the following three cases for $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$:*

**I:** $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

**II:** $\left((2)^{\frac{n-4}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(2)\right)$
**III:** $\left((2)^{\frac{n-6}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(2)\right)$

*Each of the above cases has the following degenerations (two of the branch points collapse to one)*

**I:** (1) $\left((2)^{\frac{n}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n}{2}}\right)$
(2) $\left((2)^{\frac{n-2}{2}},(2)^{\frac{n-2}{2}},(4)(2)^{\frac{n-6}{2}},(2)^{\frac{n}{2}}\right)$
(3) $\left((2)^{\frac{n-2}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n-2}{2}},(4)(2)^{\frac{n-4}{2}}\right)$
(4) $\left((3)(2)^{\frac{n-4}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n}{2}}\right)$
**II:** (1) $\left((2)^{\frac{n-2}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$
(2) $\left((2)^{\frac{n-4}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$
(3) $\left((4)(2)^{\frac{n-8}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$
(4) $\left((2)^{\frac{n-4}{2}},(4)(2)^{\frac{n-6}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$
(5) $\left((2)^{\frac{n-4}{2}},(2)^{\frac{n-2}{2}},(2)^{\frac{n-4}{2}},(2)^{\frac{n}{2}}\right)$
(6) $\left((3)(2)^{\frac{n-6}{2}},(2)^{\frac{n-2}{2}},(4)(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$
(7) $\left((2)^{\frac{n-4}{2}},(3)(2)^{\frac{n-4}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$
**III:** (1) $\left((2)^{\frac{n-4}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(4)(2)^{\frac{n}{2}}\right)$
(2) $\left((2)^{\frac{n-6}{2}},(4)(2)^{\frac{n-4}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$
(3) $\left((2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(4)(2)^{\frac{n-10}{2}}\right)$
(4) $\left((3)(2)^{\frac{n-8}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}},(2)^{\frac{n}{2}}\right)$

*Proof.* We skip the details of the proof. □

**Remark 1.** *The case $n = 8$ is the first true generic case when all the subcases occur.*

2.1. **Maximal coverings $\psi : C \longrightarrow E$.** Let $\psi_1 : C \longrightarrow E_1$ be a covering of degree $n$ from a curve of genus 2 to an elliptic curve. The covering $\psi_1 : C \longrightarrow E_1$ is called a **maximal covering** if it does not factor through a nontrivial isogeny. A map of algebraic curves $f : X \to Y$ induces maps between their Jacobians $f^* : J_Y \to J_X$ and $f_* : J_X \to J_Y$. When $f$ is maximal then $f^*$ is injective and $ker(f_*)$ is connected, see [8] for details.

Let $\psi_1 : C \longrightarrow E_1$ be a covering as above which is maximal. Then ${\psi^*}_1 : E_1 \to J_C$ is injective and the kernel of $\psi_{1,*} : J_C \to E_1$ is an elliptic curve which we denote by $E_2$; see [2]. For a fixed Weierstrass point $P \in C$, we can embed $C$ to its Jacobian via

$$\begin{aligned} i_P : C &\longrightarrow J_C \\ x &\to [(x) - (P)] \end{aligned} \tag{2}$$

Let $g : E_2 \to J_C$ be the natural embedding of $E_2$ in $J_C$, then there exists $g_* : J_C \to E_2$. Define $\psi_2 = g_* \circ i_P : C \to E_2$. So we have the following exact sequence

$$0 \to E_2 \xrightarrow{g} J_C \xrightarrow{\psi_{1,*}} E_1 \to 0$$

The dual sequence is also exact

$$0 \to E_1 \xrightarrow{\psi_1^*} J_C \xrightarrow{g_*} E_2 \to 0$$

If $deg(\psi_1)$ is an odd number then the maximal covering $\psi_2 : C \to E_2$ is unique up to isomorphism of elliptic curves. If the cover $\psi_1 : C \longrightarrow E_1$ is given, and therefore $\phi_1$, we want to determine $\psi_2 : C \longrightarrow E_2$ and $\phi_2$. The study of the relation between the ramification structures of $\phi_1$ and $\phi_2$ provides information in this direction. The following lemma (see [2, pg. 160]) answers this question for the set of Weierstrass points $W = \{P_1, \ldots, P_6\}$ of C when the degree of the cover is odd.

**Lemma 3.** *Let $\psi_1 : C \longrightarrow E_1$, be maximal of degree $n$. Then, the map $\psi_2 : C \to E_2$ is a maximal covering of degree $n$. Moreover,*

i) *if $n$ is odd and $\mathcal{O}_i \in E_i[2]$, $i = 1, 2$ are the places such that $\#(\psi_i^{-1}(\mathcal{O}_i) \cap W) = 3$, then $\psi_1^{-1}(\mathcal{O}_1) \cap W$ and $\psi_2^{-1}(\mathcal{O}_2) \cap W$ form a disjoint union of $W$.*
ii) *if $n$ is even and $Q \in E[2]$, then $\#\left(\psi^{-1}(Q)\right) \cap W = 0$ or 2.*

The above lemma says that if $\psi$ is maximal of even degree then the corresponding induced covering can have only type **I** ramification, see Theorem 1.

**Example 1.** Let $\psi : C \to E$ be a degree $n = 8$ maximal covering of the elliptic curve $E$ by a genus 2 curve $C$. Then, we have Type I covering as in previous theorem. Hence, the ramification is

$$\left((2)^3, (2)^3, (2)^3, (2)^4, (2)\right)$$

This case is the first case which has all its subcases with ramifications as follows:

**i)** $\left((2)^4, (2)^3, (2)^3, (2)^4\right)$

**ii)** $\left((2)^3, (2)^3, (4)(2), (2)^4\right)$

**iii)** $\left((2)^3, (2)^3, (2)^3, (4)(2)^2\right)$

**iv)** $\left((3)(2)^2, (2)^3, (2)^3, (2)^4\right)$

The locus of genus 2 curves in the generic case is a 2-dimensional subvariety of the moduli space $\mathcal{M}_2$. It would be interesting to explicitly compute such subvariety since it is the first case which could give some clues to what happens in the general case for even degree.

## 3. The locus of genus two curves with $(n, n)$ split Jacobians

In this section we will discuss the Hurwitz spaces of coverings with ramification as in the previous section and the Humbert spaces of discriminant $n^2$.

3.1. **Hurwitz spaces of covers $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.** Two covers $f : X \to \mathbb{P}^1$ and $f' : X' \to \mathbb{P}^1$ are called **weakly equivalent** if there is a homeomorphism $h : X \to X'$ and an analytic automorphism $g$ of $\mathbb{P}^1$ (i.e., a Moebius transformation) such that $g \circ f = f' \circ h$. The covers $f$ and $f'$ are called **equivalent** if the above holds with $g = 1$.

Consider a cover $f : X \to \mathbb{P}^1$ of degree $n$, with branch points $p_1, ..., p_r \in \mathbb{P}^1$. Pick $p \in \mathbb{P}^1 \setminus \{p_1, ..., p_r\}$, and choose loops $\gamma_i$ around $p_i$ such that $\gamma_1, ..., \gamma_r$ is a

standard generating system of the fundamental group $\Gamma := \pi_1(\mathbb{P}^1 \setminus \{p_1, ..., p_r\}, p)$, in particular, we have $\gamma_1 \cdots \gamma_r = 1$. Such a system $\gamma_1, ..., \gamma_r$ is called a homotopy basis of $\mathbb{P}^1 \setminus \{p_1, ..., p_r\}$. The group $\Gamma$ acts on the fiber $f^{-1}(p)$ by path lifting, inducing a transitive subgroup $G$ of the symmetric group $S_n$ (determined by $f$ up to conjugacy in $S_n$). It is called the **monodromy group** of $f$. The images of $\gamma_1, ..., \gamma_r$ in $S_n$ form a tuple of permutations $\sigma = (\sigma_1, ..., \sigma_r)$ called a tuple of **branch cycles** of $f$.

We say a cover $f : X \to \mathbb{P}^1$ of degree $n$ is of type $\sigma$ if it has $\sigma$ as tuple of branch cycles relative to some homotopy basis of $\mathbb{P}^1$ minus the branch points of $f$. Let $\mathcal{H}_\sigma$ be the set of weak equivalence classes of covers of type $\sigma$. The **Hurwitz space** $\mathcal{H}_\sigma$ carries a natural structure of an quasiprojective variety.

We have $\mathcal{H}_\sigma = \mathcal{H}_\tau$ if and only if the tuples $\sigma$, $\tau$ are in the same **braid orbit** $\mathcal{O}_\tau = \mathcal{O}_\sigma$. In the case of the covers $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ from above, the corresponding braid orbit consists of all tuples in $S_n$ whose cycle type matches the ramification structure of $\phi$.

This and the genus of $\mathcal{H}_\sigma$ in the degenerate cases (see the following table) has been computed in GAP by the BRAID PACKAGE written by K. Magaard.

| deg | Case | cycle type of $\sigma$ | $\#(\mathcal{O}_\sigma)$ | $G$ | $\dim \mathcal{H}_\sigma$ | genus of $\mathcal{H}_\sigma$ |
|---|---|---|---|---|---|---|
| 8 | | $(2^3, 2^3, 2^3, 2^4, 2)$ | 224 | $S_8$ | 2 | – |
| | 1 | $(2^4, 2^3, 2^3, 2^4)$ | 4 | 16 | 1 | 0 |
| | 2 | $(2^3, 2^3, (4)(2), 2^4)$ | 48 | $S_8$ | 1 | 4 |
| | 3 | $(2^3, 2^3, 2^3, (4)(2)^2)$ | 96 | $S_8$ | 1 | 16 |
| | 4 | $((3)2^2, 2^3, 2^3, 2^4)$ | 36 | $S_8$ | 1 | 4 |

TABLE 1. The length of braid orbits, the order of the group, and the genus of 1-dimensional subspaces for even degree maximal coverings.

As the reader can imagine even such computations are not easy for higher $n$. It is unclear what are the monodromy groups that appear in all the subcases and the formulas for the lengths of the braid orbits.

3.2. **Humbert surfaces.** Let $\mathcal{A}_2$ denote the moduli space of principally polarized abelian surfaces. It is well known that $\mathcal{A}_2$ is the quotient of the Siegel upper half space $\mathfrak{H}_2$ of symmetric complex $2 \times 2$ matrices with positive definite imaginary part by the action of the symplectic group $Sp_4(\mathbb{Z})$.

Let $\Delta$ be a fixed positive integer and $N_\Delta$ be the set of matrices $\tau = \begin{pmatrix} z_1 & z_2 \\ z_2 & z_3 \end{pmatrix} \in \mathfrak{H}_2$ such that there exist nonzero integers $a, b, c, d, e$ with the following properties:

$$\begin{aligned} & az_1 + bz_2 + cz_3 + d(z_2^2 - z_1 z_3) + e = 0 \\ & \Delta = b^2 - 4ac - 4de \end{aligned} \tag{3}$$

The *Humbert surface* $\mathcal{H}_\Delta$ of discriminant $\Delta$ is called the image of $N_\Delta$ under the canonical map

$$\mathfrak{H}_2 \to \mathcal{A}_2 := Sp_4(\mathbb{Z}) \setminus \mathfrak{H}_2.$$

It is known that $\mathcal{H}_\Delta \neq \emptyset$ if and only if $\Delta > 0$ and $\Delta \equiv 0$ *or* $1 \mod 4$. Humbert (1900) studied the zero loci in Eq. (3) and discovered certain relations between points in these spaces and certain plane configurations of six lines.

For a genus 2 curve $C$ defined over $\mathbb{C}$, $[C]$ belongs too $\mathcal{L}_n$ if and only if the isomorphism class $[J_C] \in \mathcal{A}_2$ of its (principally polarized) Jacobian $J_C$ belongs to the Humbert surface $\mathcal{H}_{n^2}$, viewed as a subset of the moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces. There is a one to one correspondence between the points in $\mathcal{L}_n$ and points in $\mathcal{H}_{n^2}$. Thus, we have the map:

$$\begin{array}{c} \mathcal{H}_\sigma \longrightarrow \mathcal{L}_n \longrightarrow \mathcal{H}_{n^2} \\ ([f], (p_1, \ldots, p_r) \to [\mathcal{X}] \to [J_{\mathcal{X}}] \end{array} \tag{4}$$

In particular, every point in $\mathcal{H}_{n^2}$ can be represented by an element of $\mathfrak{H}_2$ of the form

$$\tau = \begin{pmatrix} z_1 & \frac{1}{n} \\ \frac{1}{n} & z_2 \end{pmatrix}, \qquad z_1,\, z_2 \in \mathfrak{H}.$$

There have been many attempts to explicitly describe these Humbert surfaces. For some small discriminant this has been done by several authors; see [9], [5]. Geometric characterizations of such spaces for $\Delta = 4, 8, 9$, and 12 were given by Humbert (1900) in [3] and for $\Delta = 13, 16, 17, 20,$ 21 by Birkenhake/Wilhelm (2003).

## 4. Computing the locus $\mathcal{L}_n$ in $\mathcal{M}_2$

We take the most general case for maximal coverings of even degree, namely $n$, Type I. The ramification structure of $\phi : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is

$$\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)\right)$$

We denote the branch points respectively $q_1, \ldots, q_5$. Let $q_1 = 0, q_2 = 1, q_3 = \infty$. The red places in $\mathbb{P}^1_x$ denote the unramified places and the black places all have ramification index 2. We pick the coordinate $x$ such that it is $x = 0, x = 1, x = \infty$ in the unramified places of $\mathbb{P}^1_z$ and respectively in the fibers of $0, 1, \infty$ as in the picture.

There are exactly $d = \frac{n-2}{2}$ places of index 2 in $\phi^{-1}(0)$. Let $P(x)$ denote the polynomial whose roots are exactly these places. Similarly denote by $R(x), Q(x)$ such polynomials for fibers of 1 and $\infty$. The other unramified places in the fibers of 0,1, $\infty$ we denote by $w_4, w_5, w_6$ respectively.

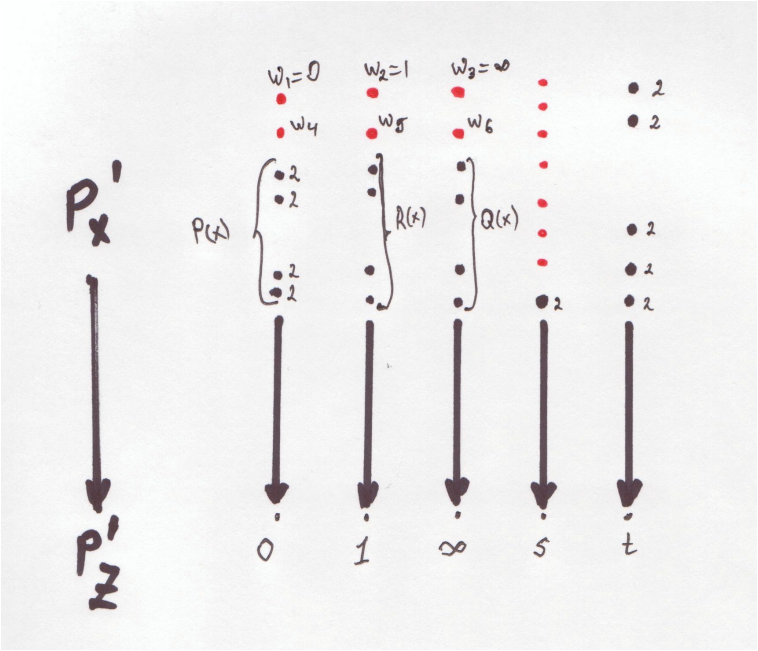
Then, we have

$$z = \lambda \cdot x \frac{x - w_4}{x - w_6} \cdot \frac{P^2(x)}{Q^2(x)}$$

for some $\lambda \cdot \in \mathbb{C}$, $\lambda \neq 0$. Furthermore,

$$z - 1 = \lambda \cdot (x - 1) \cdot \frac{x - w_5}{x - w_6} \cdot \frac{R^2(x)}{Q^2(x)}$$

where $P(x), Q(x), R(x)$ are monic polynomials of degree $d = \frac{n-2}{2}$ with no multiple roots and no common roots.




Substituting for $z$ we get a degree $n$ equation

$$\lambda x(x-w_4)P^2(x) - (x-w_6)Q^2(x) - \lambda \cdot (x-1)(x-w_5)R^2(x) = 0$$

By equaling coefficients of this polynomial with zero we get a nonlinear system of $n+1$ equations. In the same way we get the corresponding equations from the fibers of the other two branch points $s$ and $t$. Solving such system would determine also $w_4, w_5, w_6$. The equation of the genus 2 curve $C$ is given by

$$y^2 = x(x-1)(x-w_4)(x-w_5)(x-w_6)$$

4.1. **Degree 4 covers.** In this section we focus on the case $\deg(\phi) = 4$ (not necessarily maximal). The goal is to determine all ramifications $\sigma$ and explicitly compute $\mathcal{L}_4(\sigma)$. There is one generic case and one degenerate case in which the ramification of $\deg(\phi) = 4$ applies, as given by the above possible ramification structures.

i) $(2, 2, 2, 2^2, 2)$ (generic)
ii) $(2, 2, 2, 4)$ (degenerate)

4.2. **Degenerate Case.** In this case one of the Weierstrass points has ramification index 3, so the cover is totally ramified at this point.

Let the branch points be 0, 1, $\lambda$, and $\infty$, where $\infty$ corresponds to the element of index 4. Then, above the fibers of 0, 1, $\lambda$ lie two Weierstrass points. The two Weierstrass points above 0 can be written as the roots of a quadratic polynomial $x^2 + ax + b$; above 1, they are the roots of $x^2 + px + q$; and above $\lambda$, they are the roots of $x^2 + sx + t$. This gives us an equation for the genus 2 curve $C$:

$$C : y^2 = (x^2 + ax + b)(x^2 + px + q)(x^2 + sx + t).$$

The four branch points of the cover $\phi$ are the 2-torsion points $E[2]$ of the elliptic curve $E$, allowing us to write the elliptic subcover as

$$E : y^2 = x(x-1)(x-\lambda).$$

We have the following theorem:

**Theorem 2.** *Let $C$ be a genus 2 curve with a degree 4 degenerate elliptic subcover. Then $C$ is isomorphic to the curve given by*

$$\begin{aligned} C : y^2 &= \left(\frac{1-b}{3} + \frac{2}{3}(1-b)x + x^2\right)\left(\frac{1}{12}(b-4)b + \frac{1}{3}(b-4)x + x^2\right) \\ &\quad \left(b - \frac{2}{3}(b+2)x + x^2\right) \\ E : v^2 &= u(u-1)\left(u - \frac{b^3(4-b)}{16(b-1)}\right) \end{aligned} \tag{5}$$

*where the corresponding discriminants of the right sides must be non-zero. Hence,*

$$\Delta_C := b(b-4)(b-2)(b-1)(2+b) \neq 0 \tag{6}$$

$$\Delta_E := \frac{(b-4)^2(b-2)^6 b^6 (b+2)^2}{65536(b-1)^4} \neq 0. \tag{7}$$

*and its invariants satisfy*

$$\begin{aligned} &154106152812576000\, {J_2}^2 {J_4}^2 - 22835312232360960000\, J_2\, J_4\, J_6 + 5009676947631\, {J_2}^6 \\ &- 8782271900467200000\, {J_6}^2 + 1176812184652746480\, {J_2}^4 J_4 + 12448207102988800000\, {J_4}^3 \\ &- 3715799948429529600\, {J_2}^3 J_6 = 0 \\ &186626560000\, {J_2}^2 {J_4}^4 + 13896214476734335874457600000\, {J_{10}}^2 + \frac{282429536481}{10^4}\, {J_2}^{10} \\ &+ 619923800736\, {J_2}^6 {J_4}^2 - 25600000000\, {J_4}^5 - \frac{28249152375924}{100}\, {J_2}^8 J_4 \\ &+ 266576269949878792320\, {J_2}^5 J_{10} - 510202022400\, {J_2}^4 {J_4}^3 \\ &+ 693067624145203200000\, J_2\, {J_4}^2 J_{10} + 1763516708182388736000\, {J_2}^3 J_4\, J_{10} = 0. \end{aligned} \tag{8}$$

*Proof.* See [4]. □

## References


[1] G. Frey, On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2. *Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993)*, 79-98, Ser. Number Theory, I, *Internat. Press, Cambridge, MA*, 1995.

[2] G. Frey and E. Kani, Curves of genus 2 covering elliptic curves and an arithmetic application. *Arithmetic algebraic geometry (Texel, 1989)*, 153-176, *Progr. Math.*, 89, Birkhäuser Boston, MA, 1991.

[3] G. Humbert Sur les fonctionnes abéliennes singulières. I, II, III. J. Math. Pures Appl. serie 5, t. V, 233–350 (1899); t. VI, 279–386 (1900); t. VII, 97–123 (1901).

[4] T. Shaska, S. Wijesiri, S. Wolf, L. Woodland, Degree four coverings of elliptic curves by genus two curves. Albanian J. Math, vol. 2, Nr. 4, 2008.

[5] T. Shaska, Genus 2 curves with degree 3 elliptic subcovers, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.

[6] T. Shaska, Computational algebra and algebraic curves, ACM, *SIGSAM Bulletin*, *Comm. Comp. Alg.*, Vol. **37**, No. 4, 117-124, 2003.

[7] T. Shaska, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, Algorithmic Number Theory (Sydney, 2002), **6**, 205-218, *Lect. Not. in Comp. Sci.*, 2369, Springer, Berlin, 2002.

[8] T. Shaska, Curves of genus 2 with $(n, n)$-decomposable Jacobians, *J. Symbolic Comput.* 31 (2001), no. 5, 603–617.

[9] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications*, pg. 687 - 707, Springer (2004).

[10] K. Magaard, T. Shaska, H. Völklein, Genus 2 curves with degree 5 elliptic subcovers, Forum Math..

[11] T. Shaska, Genus 2 curves covering elliptic curves, a computational approach, Lect. Notes in Comp, vol 13. (2005), 151-195.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 249–255
ISSN 1930-1235: (2008)

# ON SOME APPLICATIONS OF GRAPHS TO CRYPTOGRAPHY AND TURBOCODING

Tanush Shaska

*Department of Mathematics*
*Oakland University*
*shaska@oakland.edu*

V. Ustimenko

*University of Maria Curie-Sklodowska ( Poland)*
and *Institute of telecommunications and global information space (Ukraine)*
*vasyl@golem.umcs.lublin.pl*

Abstract. Families of simple graphs of high girth had been used for the development of algorithms in Cryptography and Turbocoding. Recent results in that directions show the interest of applied researchers to "families of directed graphs of high girth", but the concept of the girth for the directed graphs is not well established. We discuss one of the possible definition. It agrees well with the classical definition in the case of simple graph and allows to create the analog of Extremal graph theory for simple graphs without small cycles for the class of balanced graphs i.e. directed graphs without multiple arrows such that each vertex has same number of inputs and outputs. Finally we discussed some explicit construction of simple and directed graphs which can be applicable to Turbocoding and Cryptography.

## 1. Introduction

Various applications of graph theory to Coding Theory are hard to observe. We just mention that the code is just subset in finite metric space defined via distance regular graph (see [8], [7], [1]) and xpanding graphs (superconcentrators, magnifyers) had been used for the design of important codes (see [14], [26], [20], [19]).

Similar situation is in Cryptography: each computation can be defined in terms of finite automaton, roughly directed graph with labels on arrows, various applications of automata theory to cryptography are very hrd to observe. We just mention [38]( see also further references in this survey).

In this note we mentioned just some traditional applications of families of simple graphs of large girth to construction of LDPS and Turbo Codes (see [25], last chapter of [15], [29], [23], [12], [13]) and Cryptography (see surveys [33], [35], [37]).

Low-density parity-check (LDPC) codes were originally introduced in his doctoral thesis by Gallager in 1961 [11]. Since the discovery of Turbo codes in 1993

by Berrou, Glavieux, and Thitimajshima [5], and the rediscovery of LDPC codes by Mackay and Neal in 1995 [22], there has been renewed interest in Turbo codes and LDPC codes, because their error rate performance approaches asymptotically the Shannon limit. Much research is devoted to characterizing the performance of LDPC codes and designing codes that have good performance. Commonly, a graph, the Tanner graph ( see [29],[25] and further references), is associated with the code and an important parameter affecting the performance of the code is the girth of its Tanner graph. In [23], [12], [13] authors consider the design of structured regular LDPC codes based on Tanner graphs of large girth. The regularity and structure of LDPC codes utilize memory more efficiently and simplify the implementation of LDPC coders. The Tanner graph is a special type of graph, a bipartite graph, where the nodes divide into two disjoint classes with edges only between nodes in the two different classes.

Large girth speeds the convergence of iterative decoding and improves the performance of LDPC codes, at least in the high SNR range, by slowing down the onsetting of the error floor. Large size of such graphs implies fast convergence.

On the web page of Professor Moura (see also [23]) one can find the following text: "Commonly, a graph, the Tanner graph, is associated with the code and an important parameter affecting the performance of the code is the girth of its Tanner graph. In our work, we consider the design of structured regular LDPC codes whose Tanner graphs have large girth. The regularity and structure of LDPC codes utilize memory more efficiently and simplify the implementation of LDPC coders. The Tanner graph is a special type of graph, a bipartite graph, where the nodes divide into two disjoint classes with edges only between nodes in the two different classes. The problem we have been considering is a generic problem in graph theory, namely, that of designing bipartite graphs with large girth. We actually have studied a more special class of this generic problem, in particular, the design of undirected regular bipartite graphs with large girth".

So here we can see clearly two ideas:

(i) new families of bipartite simple graphs of large girth can be used as families of Tanner's graphs

(ii) for the constructions of LDPS codes and turbo codes we can use directed graphs which are analogs of bipartite graphs of large girth.

In the cryptography shift to directed graphs of large girth is very natural because of the finite automaton is directed graphs. Last results demonstrated that choice of appropriate directed graphs lead to very fast graph based encryption algorithms (see [35], [16]). The new algorithms are much faster than encryption schemes [30], [31], [32] corresponding to simple graphs.

## 2. On the classical extremal graph theory for graphs without prescribed cycles and its modification

According to Bourbaki the graph (or directed graph) is the pair $V$ (vertex set) and subset $\Phi$ in the Cartesian product $V \times V$ (see [24] for more general definitions). We refer to element $v \in V$ as vertex (state in automata theory).

We use term arc (or arrow as in automata theory) for the element $(a, b) \in \Phi$. We refer to $(a, b) \in \Phi$ as arc (arrow) from $a$ to $b$, Element $a$ and $b$ are starting and ending vertex of the arc $(a, b)$. We say that $(a, b)$ is output of vertex $a$ and $b$ is input of $b$. As it follows from above definition graph has no multiple arcs.

The cardinalities of $V$ and $\Phi$ are the order and size of the graph, respectively.

Graph is simple if $\Phi$ is symmetric and anti-reflexive relation. The information about simple graph can be given by edge i. e. set of kind $\{a, b\}$, where $(a, b)$ is an arc. Graphically simple graph has no loops and multiple edges. In case of simple graph term size is used for the number of edges within the graph.

The classical extremal graph theory studies extremal properties of simple graphs. Let $F$ be family of graphs none of which is isomorphic to a subgraph of the graph $\Gamma$. In this case we say that $\Gamma$ is $F$-free. Let $P$ be certain graph theoretical property. By $\mathrm{ex}_P(v, F)$ we denote the greatest number of edges of $F$-free graph on $v$-vertices, which satisfies property $P$. If $P$ is just a property to be simple graph we omit index $P$ and write $\mathrm{ex}(v, F)$. The missing definitions in extremal graph theory the reader can find in [4].

This theory contains several important results on $\mathrm{ex}(v, F)$, where $F$ is a finite collection of cycles of different length [4], [28]. The following statement had been formulated by P. Erdös'.

Let $C_n$ denote the cycle of length $n$. Then

$$\mathrm{ex}(v, C_{2k}) \leq Cv^{1+1/k} \tag{1.1}$$

where $C$ is independent positive constant.

For the proof of this result and its generalizations see [6], [10].

In [9] the upper bound

$$\mathrm{ex}(v, C_3, C_4, \ldots, C_{2k}, C_{2k+1}) \leq (1/2)^{1+1/k} v^{1+1/k} + O(v) \tag{1.2}$$

was established for all integers $k \geq 1$.

Both bounds are known to be sharp for $k = 2, 3, 5$ in other cases the question on the sharpness is open (see [4], [2] and further references).

The girth of the simple graph is the minimal length of its cycle. So the above bound is the restriction on the size of the graph on $v$ vertices of girth $\geq n$. Graphs of high girth, i.e. graphs which size is close to the above upper bounds can be used in Networking and Operation Research (see [4]) and Cryptography.

The generalizations (or analogs) of classical extremal graph theory on directed graphs require certain restrictions on inputs or outputs of the graph. Really, the graph $DK_v$ of binary relation $\phi$: $P \cup L = V$, $P \cap L = \emptyset$, $|P| = |L|$, $|V| = v$, $\phi = P \times L$ of order $O(v^2)$ has no directed cycles or commutative diagrams.

In [33], [37] the above results on maximal size of the graphs generalized on the case of balanced graphs, when for each vertex $a \in V$ cardinalities of $\mathrm{id}(v) = \{x \in V | (a, x) \in \phi\}$ and $\mathrm{od}(v) = \{x \in V | (x, a) \in \phi\}$ are same. We refer to numbers $\mathrm{id}(v)$ and $\mathrm{od}(v)$ as input degree and output degree of vertex $v$ in the graph, respectively.

Let $\Gamma$ be directed graph. The *pass* between vertices $a$ and $b$ is the sequence $a = x_0 \to x_1 \to \ldots x_s = b$ of length $s$, where $x_i$, $i = 0, 1, \ldots, s$ are distinct vertices. We refer to the minimal $s$ among all passes between $a$ and $b$ as output distance $\mathrm{odist}(a, b)$. we assume $\mathrm{odist}(a, b) = \infty$ in case of absence of passes from $a$ to $b$.

We say that the pair of passes $a = x_0 \to x_1 \to \cdots \to x_s = b$, $s \geq 1$ and $a = y_0 \to y_1 \to \cdots \to y_t = b$, $t \geq 1$ form an $(s, t)$- commutative diagram $O_{s,t}$ if $x_i \neq y_j$ for $0 < i < s$, $0 < j < t$. Without loss of generality we assume that $s \geq t$ and refer to the number $s$ as the rank of $O_{s,t}$. The directed cycle with $s$ arrows we denote as $O_{s,0}$. We will count directed cycles as commutative diagram.

The minimal parameter $s = \max(s,t)$ of the commutative diagram $O_{s,t}$ with $s+t \geq 3$ in the binary relation graph $\Gamma$ we call the *girth indicator* of the $\Gamma$ and denote it as $\mathrm{gi}(\Gamma)$. It can be infinity as in case of $DK_v$.

Notice that directed graph does not contain diagrams $O_{1,1}$, because there are no multiple edges.

We assume that the *girth* $g(\Gamma)$ of directed graph $\Gamma$ with the girth indicator $d+1$ is $2d+1$ if it contains commutative diagram $O_{d+1,d}$. If there are no such diagrams we assume that $g(\Gamma)$ is $2d+2$.

In the case of symmetric irreflexive relations it agrees with the standard definition of the girth of simple graph i.e the length of its minimal cycle.

Let $F$ be a list of directed graphs and $P$ be some graph-theoretical property. By $\mathrm{Ex}_P(v,F)$ we denote the greatest number of arrows of $F$-free directed graph on $v$ vertices satisfying to property $P$ (graph without subgraphs isomorphic to graph from $F$).

Let $\mathrm{E}_P = \mathrm{E}_P(d,v) = \mathrm{Ex}_P(v, O_{s,t}, s+t \geq 3 | 2 \leq s \leq d)$ be the maximal size (number of arrows) of the balanced binary relation graphs with the girth indicator $> d$.

The main result of [37] is the following statement. If $B$ is the property to be the balanced directed graph, then

$$v^{1+1/d} - O(v) \leq \mathrm{E}_B(d,v) \leq v^{1+1/d} + O(v) \tag{1.3}$$

Notice, that the size of symmetric irreflexive relation is the double of the size of corresponding simple graph. because undirected edge of the simple graph corresponds to two arrows (arcs) of $O_{2,0}$.

If $P$ is the property to be a graph of symmetric irreflexive relation then $\mathrm{Ex}_P(v, O_{s,t}, s+t \geq 3 | 2 \leq s \leq d) = 2\mathrm{ex}(v, C_3, \ldots, C_{2d-1}, C_{2d})$ because undirected edge of the simple graph corresponds to two arrows of $O_{2,0}$. So equality (1, 3) implies the following inequality

$$\mathrm{ex}(v, C_3, C_4, \ldots, C_{2k}) \leq (1/2)v^{1+1/k} + O(V) \tag{1.4}$$

we evaluate the maximal size of the directed graph of order $v$ with the girth indicator $> d$ which does not contain commutative diagrams $O_{d+1,d}$, as well. The inequality (1.2) is the corollary from such evaluation.

We can see that studies of extremal properties of balanced graphs with the high girth indicator and studies of $ex(v, C_3, \ldots, C_n)$ are far from being equivalent. Really, the sharpness of the Erdös' bound (1.1) and bounds (1.2) and (1.4) up to magnitude for $k = 8$ and $k \geq 12$ are old open problems (see [2], [4]) .

The regularity $R$ of graph $(V, \Phi)$ means that either for each vertex $a \in V$ sets $\{x | (v,x) \in \Phi\}$ are same or for each $a \in V$ set $\{x | (x,v) \in \Phi\}$ are same.

The family of directed graphs $G_i$, $i = 1, \ldots$ with average output degree $k_i$ and order $v_i$ is the family of graphs of large girth if the girth indicator of $G_i$ is $\geq c \times \log_{k_i}(v_i)$. It agrees well with the standard definition for the simple graphs. In case of balanced or regular graphs of large girth their size is close to the upper bounds (1. 3) and (1. 5).

## 3. Explicit constructions of Tanner graphs

3.1. **Some suggestions in case of simple graphs.** The induced biregular bipartite subraphs of graphs $D(n,q)$ (see [17] and further references) of order $2q^n$, degree $q$ and girth $\geq n+4$ or their connected components $CD(d,q)$had been used

by Guinnand and Lodge for the construction of turbocodes. The description of the class of biregular subgraphs of the above graphas the reader can find in [18]. The parameters of related codes are very close to the Shannon bound.

We notice that the family of graphs $D(n,q)$ depending on two parameters $n$ and $q=p^m$, where $p$ is prime, is not the unique known family of graphs of unbounded degree and arbitrarily large girth. For "sufficiently large $p$" the exact girth is computed in [27].

The first explicit examples of families of simple graphs with large girth of arbitrary large degree were given by Margulis. The constructions were Cayley graphs $X^{p,q}$ of group $SL_2(Z_q)$ with respect to special sets of $q+1$ generators, $p$ and q are primes congruent to 1 mod4. The family of $X^{p,q}$ is not a family of algebraic graphs because the neighborhood of each vertex is not an algebraic variety over $F_q$. For each $p$, graphs $X^{p,q}$, where $q$ is running via appropriate primes, form a family of small world graph of unbounded diameter (see [21],[19]).

Of course Cayley graph corresponding to finite group $G$ and symmetrical set of generators $S$ ( $s\in S$ leads to $s^{-1}\in S$ is not a bipartite graph. But we can take it bipartite analog - the graph of incidence structure $I=I(G,S)$for which the point set $P$ and line set $L$ are two distinct copies of $G$ and $p\in P$ is incident to $l\in L$ if and only if $ps=l$ in group $G$ for some generator $s\in S$.

Let $R$ be arbitrary subset of $S$ containing at least 3 elements, $G_R$ be the group generated by $R\cup R^{-1}$ and $G_R<H<G$.

We can consider the bipartite graph $I'=I(H,R)$ with the partition sets $P'=P\ capH$ and $L'=L\cap H$ such that $p\in P'$ and $l\in L'$ are incident ($pI'l$ or $lI'p$) if and only if $ps=l$ for some $s\in R$. Notice, that last condition is equivalent to $ls=p$ for some $s\in R^{-1}$.

We set the Cayley graph corresponding to $G,S$ is $X^{p,q}$. then $g(I(H,R)$ is larger than the girth of $X^{p,q}$. So $I(H,R)$ can be used as Tanner graph.

Some other regular graphs of high girth the reader can find in [34].

3.2. **Examples of directed bipartite graphs with large girth indicators.** Let $M_k$, $m\geq k+2$ as the totality of tuples $(x_1,x_2,\dots x_k)\in M^k$, such that $x_i\neq x_j$ for each pair $(i,j)\in M^2$. Let us consider the binary relation $\phi=\phi_k(m)$ on $M_k$ consisting of all pairs of tuples $((x_1,\dots,x_m)\ ,(y_1,\dots,y_m))$, such that $y_i=x_{i+1}$ for $i=1,\dots,k-1$ and $y_m\neq x_i$ for each $i\in\{1,\dots,k\}$. The corresponding directed graph $\Gamma=\Gamma_i(m)$ has order $m(m-1)\dots(m-k+1)$, each vertex has $m-k$ input and output arrows.

**Proposition 1.** *The girth indicator and diameter of the graph $\Gamma_k(m)$ is $k+1$ and $2k$, respectively. The girth of the graph is $2d+1$.*

The reader can find the proof in [36].

Let us consider the bipartite version $\Gamma'=\Gamma'_k(m)$ of the graph $\Gamma=\Gamma_k(m)$. Let $M$ be a finite set, $m=|M|\geq 2$. Let $P$ (point set) and $L$ (line set) are two copies of the vertex set $M_k$, $m\geq k+2$ of the graph $\Gamma$. We will use the brackets and parenthesis for the tuples from $P$ and $L$, respectively.

Let$\Gamma'=\Gamma'_k(m)$ be the graph of binary relation on $P\cup L$ consisting of all pairs of tuples $((x_1,\dots,x_m),[y_1,\dots,y_m)$ or $(x_1,\dots,x_m,(y_1,\dots,y_m))$, such that $y_i=x_{i+1}$ for $i=1,\dots,k-1$ and $y_m\neq x_i$ for each $i\in\{1,\dots,k\}$. The corresponding directed graph $\Gamma'=\Gamma'_k(m)$ has order $2m(m-1)\dots(m-k+1)$, each vertex has $m-k$ input and output arrows.

**Proposition 2.** *The girth indicator and diameter of the graph* ${\Gamma'}_k(m)$ *is* $k+1$ *and* $2k+1$*, respectively. The graph does not contain commutative diagram* $O_{k+1,k}$*. The girth of the graph is* $2d+2$*.*

So one can use these directed bipartite regular graphs as directed Tanner graphs.

## References


[1] E. Bannai, T. Ito, *Algebraic Combinatorics 1: Association Schemes*, Benjumin-Cummings Lecture Notes, Ser. 58, London, 1984.

[2] C.T. Benson, *Minimal regular graphs of girth eight and twelve*, Canadien Journal of Mathematics, (18):1091- 1094, 1966.

[3] N. Biggs, *Algebraic Graph Theory* (2nd ed), Cambridge, University Press, 1993.

[4] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.

[5] C. Berrou, A. Glavieux and P. Thitimajshima, *Near Shannon limit errorcorrecting coding and decoding: turbocodes*, ICC 1993, Geneva, Switzerland, pp. 10641070, May 1993.

[6] J.A. Bondy and M.Simonovits, *Cycles of even length in graphs*, J. Combin.Theory, Ser. B, 16 (1974) 87-105.

[7] A. Brower, A. Cohen, A. Nuemaier, *Distance regular graphs*, Springer, Berlin, 1989.

[8] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Phillips Research Reports Suppl., 10 (1973).

[9] P. Erdös', M. Simonovits, *Compactness results in extremal graph theory*, Combinatorica 2 (3), 1982, 275-288.

[10] W. Faudree, M. Simonovits, *On a class of degenerate extremal graph problems*, Combinatorica 3 (1), 1983, 83-93.

[11] R. G. Gallager, *Lowdensity paritycheck codes*, IRE Transactions on Information Theory, vol. IT8, pp. 2128, Jan. 1962.

[12] P. Guinand and J. Lodge, "Tanner Type Codes Arising from Large Girth Graphs", Proceedings of the 1997 Canadian Workshop on Information Theory (CWIT '97), Toronto, Ontario, Canada, pp. 5-7, June 3-6, 1997.

[13] P. Guinand and J. Lodge, *Graph Theoretic Construction of Generalized Product Codes*, Proceedings of the 1997 IEEE International Symposium on Information Theory (ISIT '97), Ulm, Germany, p. 111, June 29-July 4, 1997.

[14] S. Hoory, N. linial and A. Widgerson, *Expander graphs and their applications* Bulletin (New series) od the American Mathematical Society, volume 43, N4,2006, 439-561.

[15] W. C. Huffman and V. Pless, Fundamentals of Error Correcting Codes, Cambridge University Press, 2003, 646 pp.

[16] J. Kotorowicz, V. A. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condenced Matters Physics, Special Issue: Proceedings of the international conferences "Infinite particle systems, Complex systems theory and its application", Kazimerz Dolny, Poland, 2006, 11 (no. 2(54)) (2008) 347–360.

[17] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.

[18] F. Lazebnik, V. A. Ustimenko and A. Woldar,*New upper bound on the order of cages*, Electronic Journal of Combinatorics, Volume 4 (1997), No. 2, Paper R13.

[19] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

[20] A Lubotsky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Progres in Math., Birkhauser, 1994.

[21] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.

[22] D. J. C. MacKay and R. N. Neal, *Good Codes based on very sparse matrices*, In "Cryptography and Coding", 5th IMA Conference, Lecture Notes in Computer Science, v. 1025, 1995, pp. 110-111.

[23] Jose M. F. Moura, Jin Lu, and Haotian Zhang, *Structured LDPC Codes with Large Girth*, IEEE Signal Processing Magazine, vol. 21:1, pp.42-55, January 2004. Included in Special Issue on Iterative Signal Processing for Communications.

[24] R. Ore, *Graph Theory*, Wiley, London, 1971.

[25] T. Richardson, R. Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008, 592 pp.
[26] P. Sarnak, *What is an expander?*, Notices of AMS, 2004, 762-763. Linear Algebra and its Applications Article in Press, Corrected
[27] T. Shaska, V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra and its Applications Article in Press, 2008 (in press, available on line).
[28] M. Simonovits *Extremal Graph Theory*, Selected Topics in Graph Theory 2 (L.W. Beineke and R.J. Wilson, eds), Academic Press, London, 1983, 161-200.
[29] R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, 27(5):533-547, Sept.1984.
[30] V. A. Ustimenko, *Coordinatisation of regular tree and its quotients*, in "Voronoi's impact on modern science, eds P. Engel and H. Syta, book 2, National Acad. of Sci, Institute of Matematics, 1998, 228p.
[31] V. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.
[32] V. Ustimenko, *CRYPTIM: Graphs as tools for symmetric encryption*, In Lecture Notes in Comput. Sci., 2227, Springer, New York, 2001.
[33] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications*, In: T. Shaska, W. C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding Theory and Cryptology, vol. 3, 181-200 (2007).
[34] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol. 140, N3 (2007), pp 412-434.
[35] V. Ustimenko *On the graph based cryptography and symbolic computations*, Serdica journal of computing, N1, 2007, 131-156.
[36] V. A. Ustimenko, *On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography*, Albanian. J. of Mathematics, Special Issue "Algebra and Computational Algebraic Geometry", vol. 1, N4, 387-400, 2007.
[37] V. Ustimenko, *On the cryptographical properties of extremal algebraic graphs*, In Publisher: IOS Press Title: Mathematics and Communications Editors: T. Shaska, E. Hasimaj, IOS Press, 2008 (to appear).
[38] S. Wolfram, *Cryptography with cellular automata* , Lecture notes in computer sciences, 218 (1985) (Advances in cryptology-CRYPTO 85, Santa Barbara, California), 429 - 432.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 3, Pages 259–265
ISSN 1930-1235: (2008)

# QUANTUM CHANNELS WITH CONTINUOUS INPUT ALPHABET

Georges Parfionov

*Dept. of Mathematics,*
*SPb EF University,*
*Griboyedova 30–32, 191023, St.Petersburg, Russia*

Romàn R. Zapatrin

*Dept. Informatics,*
*The State Russian Museum,*
*Inénernaya, 4, 191186, St.Petersburg, Russia*
*e-mail: Roman.Zapatrin@gmail.com*

Abstract. Any communication assumes a preliminary agreement between the parties involved. In our paper we address the question: what can we get when there is no agreement between the parties in the framework of classical communication quantum channels. We admit the concept of mixed coding and starting from it derive an idealized communication scheme based on continuous coding.

## 1. Classical communication through quantum channel

For the sake of self-consistency, we start from the conventional scheme of classical communication through quantum channel. Its basic ingredients are:

- **Coding.** It contains
  - A set of input states associated with the symbols of input alphabet
  - For each input state its a priori probability $\pi_j$ is given
- **Transmission.** It is described by a superoperator: an affine mapping from the state space of the input of the channel ti that of the output.
- **Receiving a signal.** It is described by applying appropriate measurement on the set of output states, so that:
  - A measurement is a resolution of unit
  - When a signal is received, we judge which was the input state
  - For each input state $j$ we calculate the probabilities $p_M(k \mid j)$ of taking the decision that the observed symbol was $k$ (for every $k$)
  - The task in *conventional framework* is to find an optimal procedure to decide which was the input state

When the input coding and the output measurements are fixed, the probability to take the right decision then reads:

$$P_M = \sum_j \pi_j p_M(j \mid j) \tag{1}$$

This kinds of tasks are typical for communication theory and mathematical statistics. Finding the maximum of $P_M$ is called identification of signals based on the criterion of maximal likelihood. Given an input coding, the task is, varying the output measurement $M$, to find such one that the probability $P_M$ defined in (1) becomes maximal.

In standard framework we are given an input ensemble, that is, a collection of input states $\psi_j$ with given probabilities $\pi_j$. For the input ensemble, its average density matrix $\rho$ is calculated:

$$\rho = \sum_j \pi_j \psi_j \tag{2}$$

What is crucial in this scheme is that the efficiency of the channel (1) primarily depends on the input ensemble rather than on its average density matrix (see, e.g. optimal coding schemes by Schumacher and Westmoreland [1])
What is peculiar for our framework. In our framework we suppose that *only the average* density matrix (2) of the input ensemble is known, while the ensemble itself is not given for us. For quantum mechanical systems there are (infinitely) many ensembles having the same average density.

In other words, we only know the channel as a physical system. Any communication assumes a preliminary agreement between the parties dealing with input and output of the channel. In our paper we address the question: what can we get when there is *no agreement* between the parties.

That means, we are given the state space of the input but we *do not know* the a priori probabilities of input states and the result of measurements reduces to specifying the average output density matrix.

The problems of this kind have a long history lasting from Laplace to Boltzmann; their are solved on the basis of the principle of maximal entropy.

## 2. From Laplace principle to maximal entropy

It was Laplace who introduced the *principle of insufficient reason*: if there is no reason to prefer one outcome w.r.t. another one, all outcomes are treated equally probable (provided they are mutually exclusive and collectively exhaustive). Its direct consequence was the formula of classical probability [2]:

$$p = \frac{\text{Favorables}}{\text{Possibles}} \tag{3}$$

According to Laplace, if we are given an unknown distribution and we *need* to estimate it, we assume it to be uniform.

But what should we do if we have an additional information about the distribution? Can we still use the Laplace principle?

Let us illustrate it on a classical example. Suppose we play with die whose properties are not known. If we are asked what is the probability of a face to appear, we intuitively (but in fact according to Laplace) answer 1/6.

Let $N$ identical dice are rolled and the mean value $M$ of the number of points appeared is known. First suppose it turned out to be 3.5. This is an additional information about the dice, and how it affects our estimation? In this particular case we see that result is compatible with the initial hypothesis:

$$M = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = 3.5$$

Now take another kind of 'biased' dice such that the appropriate average value turns out to be, say, 4. In this case the hypothesis of the equality of all *faces* is no longer compatible with initial hypothesis and the Laplace principle is not applicable, at least in its direct form.

Among this we have $n_1$ times face 1,..., $n_6$ times face 6. The values $n_1, \dots, n_6$ satisfy the equations

$$n_1 + \cdots + n_6 = N$$

and

$$1 \cdot n_1 + \cdots + 6 \cdot n_6 = M \cdot N$$

When we try to solve this system with respect to $n_1, \dots n_6$, we get many solutions. Although, each particular solution occurs with its frequency:

$$W(n_1, \dots, n_6) = \frac{N!}{n_1! \cdots n_6!}$$

We are finding the solution $n_1, \dots, n_6$, which has greatest probability to occur, therefore we maximize the value of the frequency $W(n_1, \dots n_6)$. As it is known (see, e.g. [3]):

$$\log W \sim N \cdot \left( -\frac{n_1}{N} \log \frac{n_1}{N} - \cdots - \frac{n_6}{N} \log \frac{n_6}{N} \right) \tag{4}$$

And the maximum is attained at

$$n_k \sim N \cdot \frac{e^{-\beta k}}{Z} \tag{5}$$

where the normalizing factor $Z$ is

$$Z = \sum_k e^{-\beta k} \tag{6}$$

Although the knowledge of the mean value is an additional information, the Laplace principle still works and this particular mean value gives no preference to any state, therefore the null hypothesis (the uniform distribution $p_j = \frac{1}{6}$) should not be rejected.

Biased die. Now let us consider what happens when the average is 4. In this case the Laplace principle should be developed: namely, the distribution should have maximal entropy $H = -\sum p_j \log p_j$. In our particular case this gives the following answer:

$$p_j = \frac{e^{-\beta j}}{Z} \tag{7}$$

where $Z = \sum_j e^{-\beta j}$ and $\beta$ is calculated from the given average value (in our case, 4)

$$\sum_j j \cdot p_j = 4$$

This principle extends the Laplace principle to the notion of maximal entropy [4].

Why the idea to maximize the entropy $H$ is a development of Laplace idea of symmetry and non-preference? For any given average value we consider all possible distributions which yield this average value. Then the take such distributions which are typical, that is, which mostly occur in all possible configurations. The preference is given to what occur with maximal number of combinations. The statistical weight

$$W = \frac{N!}{\prod_j n_j}$$

where $N$ is the total number of trials and $n_j$ is number of occurrence of $j$-th face.

The main message of this section is the following. We provide a completely classical example where we have *no knowledge* about the input state (distribution) but we *need* to tell something about it. A principle is suggested to choose a concrete distribution on the basis of a given small amount of knowledge.

In the case of quantum systems these distributions will be of a particular kind — continuous ensembles.

## 3. Continuous ensembles

The set of all self-adjoint operators in $\mathcal{H} = \mathbb{C}^n$ has a natural structure of a real space $\mathbb{R}^{2n}$, in which the set of all density matrices is a hypersurface, which is the zero surface $T = 0$ of the affine functional $T = \mathrm{TrX} - 1$.

Let $\mathcal{H} = \mathbb{C}^n$ be an $n$-dimensional Hermitian space, let $\rho$ be a density matrix in $\mathcal{H}$. We would like to represent the state whose density operator is $\rho$ by an ensemble of pure states. We would like this ensemble to be continuous with the probability density expressed by a function $\mu(\phi)$ where $\phi$ ranges over all unit vectors in $\mathcal{H}$.
Technical remark. Pure states form a projective space rather than the unit sphere in $\mathcal{H}$. On the other hand, one may integrate over any probabilistic space. Usually distributions of pure states over the spectrum of observables are studied, sometimes probability distributions on the projective spaces are considered [5]. In this paper for technical reasons I prefer to represent ensembles of pure states by measures on unit vectors in $\mathcal{H}$. We use the Umegaki measure on $\mathbb{C}B_n$— the uniform measure with respect to the action of $U(n)$ normalized so that $\int_{\mathbb{C}B_n} \mathrm{d}\psi = 1$.
Effective definition. The density operator of a continuous ensemble associated with the measure $\mu(\phi)$ on the set $\mathbb{C}B_n$ of unit vectors in $\mathcal{H}$ is calculated as the following (matrix) integral

$$\rho = \int\limits_{\phi \in \mathbb{C}B_n} \mu(\phi)\ |\phi\rangle\langle\phi|\ \mathrm{d}\psi \tag{8}$$

where $|\phi\rangle\langle\phi|$ is the projector onto the vector $\langle\phi|$ and $\mathrm{d}\psi$ is the above mentioned normalized measure on $\mathbb{C}B_n$:

$$\int\limits_{\phi\in\mathbb{C}B_n} \mathrm{d}\psi \;=\; 1 \tag{9}$$

Effectively, the operator integral $\rho$ in (8) can be calculated by its matrix elements. In any fixed basis $\{|\mathbf{e}_i\rangle\}$ in $\mathcal{H}$, each its matrix element $\rho_{ij} = \langle \mathbf{e}_i| \rho |\mathbf{e}_j\rangle$ is the following numerical integral:

$$\rho_{ij} \;=\; \langle \mathbf{e}_i| \rho |\mathbf{e}_j\rangle \;=\; \int\limits_{\phi\in\mathbb{C}B_n} \mu(\phi)\, \langle \mathbf{e}_i|\, \phi\rangle \langle\phi|\, \mathbf{e}_j\rangle \;\mathrm{d}\psi \tag{10}$$

The task of likelihood-based recognition of the initial input coding is solved by introducing a special sort of continuous ensembles: so-called Lazy ensembles [6].

## 4. Lazy ensembles

Potentially we consider all possible input states, and the result we will find in terms of a distribution on the set of all input states. Our task is to guess (to mostly possible extent) what was the distribution of input states.

Definition of Kullback–Leibler distance. We quantify the state preparation efforts by the difference between the entropy of uniform distribution (that is, our null hypothesis) and the entropy of the ensemble[1] in question. The only obstacle may occur is to define this entropy, let us dwell on it in more detail.

The entropy of a finite distribution $\{p_i\}$ is given by Shannon formula

$$S(\{p_i\}) = -\sum p_i \ln p_i$$

This expression diverges for any continuous distribution: we approximate a continuous distribution $\mu(x)$ by a discrete one $\{p_i\}$, calculate its Shannon entropy, but it tends to infinity as we refine the partition. However, we are always interested in the *difference* between the entropy of the uniform distribution and the distribution $\mu(x)$ rather then the entropy itself. At each approximation step we calculate this difference, and the appropriate limit always exists. To show it (see, e.g. [8] for details), make a partition of the probability space by $N$ sets $\Delta_i$ having equal uniform measure. Then the difference $E_N$ between the entropies read:

$$E_N \;=\; \ln N \;-\; \Big(-\sum p_i \ln p_i\Big)$$

where $p_i = \int_{\Delta_i} p(x)dx$. The limit expression $\lim_{N\to\infty} E_N$ is the differential entropy

$$S(\mu) \;=\; \int \mu(x) \ln \mu(x) \mathrm{dx} \tag{11}$$

Remarkably, this is equal to Kullback-Leibler distance [3]

$$S(\mu\|\mu_0) \;=\; \int \mu(x) \ln \frac{\mu(x)}{\mu_0(x)} \mathrm{dx}$$

between the distribution $\mu(x)$ and the uniform distribution $\mu_0(x)$ with constant density, normalize the counting measure dx on the probability space so that $\mu_0 = 1$.

[1]We are speaking here of *mixing entropy* [7] of the ensemble rather than about von Neumann entropy of its density matrix.

This distance is the average likelihood ratio, on which the choice of statistical hypothesis is based. Then, in order to minimize the Type I error we have to choose a hypothesis with the smallest average likelihood ratio.
Maximizing the entropy. The problem reduces to the following. For given density matrix $\rho$ find a continuous ensemble $\mu$ having minimal differential entropy (11):

$$S(\mu) \;\to\; \min, \qquad \int |\psi\rangle\langle\psi| \;\mu(\psi)\,\mathrm{d}\psi \;=\; \rho \tag{12}$$

where $\mathrm{d}\psi$ is the unitary invariant measure on pure states normalized to integrate to unity. When there is no constraints in (12), the answer is straightforward—the minimum (equal to zero) is attained on uniform distribution. To solve the problem with constraints, we use the Lagrange multiples method. The appropriate Lagrange function reads:

$$\mathcal{L}(\mu) \;=\; S(\mu) \;-\; \mathrm{Tr}\,\Lambda \left( \int |\psi\rangle\langle\psi| \;\mu(\psi)\,\mathrm{d}\psi \;-\; \rho \right)$$

where the Lagrange multiple $\Lambda$ is a matrix since the constraints in (12) are of matrix character. Substituting the expression (11) for $S(\mu)$ and making the derivative of $\mathcal{L}$ over $\mu$ zero, we get

$$\mu(\psi) \;=\; \frac{\mathrm{e}^{-\,\mathrm{TrB}|\psi\rangle\langle\psi|}}{Z\,(B)} \tag{13}$$

where $B$ is the optimal value of the Lagrange multiple $\Lambda$ which we derive from the constraint (12) and the normalizing multiple

$$Z(B) \;=\; \int \mathrm{e}^{-\,\mathrm{TrB}|\psi\rangle\langle\psi|}\,\mathrm{d}\psi \tag{14}$$

is the partition function for (13). Substituting he resulting density (13) to the expression (11) for differential entropy we get

$$S \;=\; \mathrm{TrB}\rho \;-\; \ln \mathrm{Z} \tag{15}$$

## 5. Conclusions

It follows directly from the Holevo bound formula that the classical communication capacity of a quantum channel increases when pure states are used for input coding. In the meantime the idea to represent the input ensemble by minimal number of input states, that is, to make them orthogonal, does not in general increase the efficiency of the channel, some coding schemes are essentially based on non-orthogonal states [1]. The usage in statistics of non-orthogonal, overfilled bases of pure states, that is, using the randomization, may sometimes bring some gain in *identifying* the state of the system. This is an essentially quantum phenomenon as in the classical case randomization only produce problems in state identification.

In this contribution we are dealing with the extreme case of overfilled systems of pure states, namely, in a finite-dimensional space we consider bases of infinitely many, continuously many pure states. The research along this lines was first carried out in [9], where the so-called 'Scrooge' ensembles were introduced as bringing minimal amount of information about the preparation procedure. These ensembles

turn out to be continuous. The closest analogy to them in quantum coding are mixed sources [10]

The relevance of continuous ensembles is also justified when we take into account the fact that even we use discrete ensembles of pure states, in reality, when we are preparing them, we can not completely avoid noises produced by the measurement apparata, that is, the distribution of really prepared pure states again turns out to be continuous. We use continuous ensembles for the purpose of building statistical inferences according to the standard schemes of re-estimation of hypotheses, which looks as follows. We have a null hypothesis, then we acquire some information about the system, and then we pass to a new, concurring hypothesis choosing it in such a way that it should be closest to the null hypothesis. This new hypothesis is put forward according to the concept of maximal likelihood.

The concept of maximal likelihood technically reduces to maximization of the logarithm of the probability of the distribution. The appropriate opposite value is a well-known L.J.Savage entropy, or Kullback-Leibler distance between distributions.

In other words, we use the acquired information about the system with a maximal precaution in order to minimize the Type II error.

In our case the null hypothesis is that all pure states are equiprobable. In this case Kullback-Leibler distance between the new ensemble and the null hypothesis is equal to the differential entropy of the new ensemble. The source of additional information is the average density matrix of the input ensemble.

Optimal ensembles that we obtain are exponential distributions of pure staes, which average to a density matrix $\rho$. These distribution have a striking similarity with the Gibbs ensembles, which form the basis of statistical physics.

The matrix parameter $B$ here plays a rôle similar to that of the temperature in thermodynamics. Under appropriate normalization the value

$$\mathrm{TrB}\rho$$

Will be equal to the differential entropy of the ensemble. So, we may treat this parameter as the differential entropy of the density matrix.

## References


[1] Schumacher B, Westmoreland M, *Relative entropy in quantum information theory*, Quantum Computation and Quantum Information: A Millenium Volume , S.Lomonaco, editor (American Mathematical Society Contemporary Mathematics series, 2001); arXiv:quant-ph/0004045

[2] Edwin Thompson Jaynes, *Probability Theory: The Logic of Science*, Cambridge University Press (2003)

[3] Kullback S, *Information theory and statistics*, New York, Dover (1968)

[4] N. Hadjisavvas, The Maximum Entropy Principle as a consequence of the principle of Laplace, *J. Stat. Phys.* **26**, 807–815 (1981)

[5] E. Lehrer, E. Shmaya, *A Subjective Approach to Quantum Probability*; eprint quant-ph/0503066

[6] George Parfionov, Roman Zapatrin, 'Lazy' quantum ensembles, *Journal of Physics A: Mathematical and General*, **39** 10891–10900 (2006), arxiv:quant-ph/0603019

[7] Wehrl A, *General properties of entropy*, Reviews of Modern Physics, **50**, 221–260 (1978)

[8] Stratonovich R L, *Information theory* (in Russian), Moscow, Nauka (1975)

[9] R.Jozsa, D.Robb and W.K.Wootters, A Lower Bound for Accessible Information in Quantum Mechanics, *Physical Review* **A49**, 668-699 (1994)

[10] Garry Bowen, Nilanjana Datta, Quantum oding Theorems for Arbitrary Sources, Channels and Entanglement Resources, arXiv:quant-ph/0610003v1

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 4, Pages 265–275
ISSN 1930-1235: (2008)

# SOME ITERATIVE ALGORITHMS FOR EXTENDED GENERAL VARIATIONAL INEQUALITIES

Muhammad Aslam Noor

*COMSATS Institute of Information Technology*
*Mathematics Department*
*Islamabad, Pakistan*
*noormaslamgmail.com, noormaslamhotmail.com*

Abstract. In this paper, we suggest and analyze a new class of three-step projection iterative methods for solving the extended general variational inequalities, which are obtained using the updating technique of the solution in conjunction with projection technique. We also consider the convergence criteria of these new iterative methods under some mild conditions. Since the extended general variational inequalities include the general variational inequalities and other related optimization problems as special cases, results obtained in this paper continue to hold for these problems. Results obtained in this paper may be viewed as a refinement and improvement of the known results.

## 1. Introduction

Extended general variational inequality, which was introduced and studied by Noor[20-23,26], is an important and useful generalization of variational inequalities. It has been shown that the extended general variational inequalities provide us with a unified, simple and natural framework to study a wide class of problems including unilateral, moving, obstacle, free, equilibrium and economics arising in various areas of pure and applied sciences. Noor [20,21,26] has shown that the minimum of a differentiable nonconvex functions on the nonconvex sets can be characterized by the extended general variational inequalities. It has been shown in [21,22, 26 ] that the extended general variational inequalities are equivalent to the fixed point problems. This equivalent alternative equivalent has been used to discuss the uniqueness of the solution as well as to suggest some iterative methods for solving the extended general variational inequalities, see Noor [20-23,26] and the references therein.

Noor[13,15] has suggested and analyzed some three steps forward-backward splitting algorithms for solving variational inequalities by using the updating techniques of the solution and auxiliary principle. These forward-backward splitting algorithms

Received by the editors October 20, 2008 and, in revised form, October 25, 2008.
2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 90C33.
*Key words and phrases.* Variational inequalities; nonconvex functions; fixed-point problem, convergence.

are similar to that of the $\theta$-scheme of Glowinski and Le Tellec[6], which they suggested by using the Lagrangian technique. It is known that three step schemes are versatile and efficient, see [3, 6]. These three-step schemes are natural generalization of the splitting methods for solving partial differential equations. We would like to point out that the iterative methods serve to solve a variety of problems which are either of the feasibility or the optimization type. This class of algorithms has witnessed great progress in recent years. Apart from theoretical interest, the main advantage of these iterative methods, which make them use of in real world problems, is computational. These methods have the ability to handle large-size problems of dimensions beyond which other methods cease to be efficient. In short, the field if the iterative type methods is vast, see [1-35] and the references therein.

Inspired and motivated by the usefulness and applications of the splitting type methods, we suggest and analyze a new class of three step approximation schemes for solving the extended general variational inequalities and related problems. These new methods include the Mann and Ishikawa iterative schemes and modified forward-backward splitting methods of Noor[13,15] as special cases. We also study the convergence criteria of these new methods under some mild conditions. Our results represent an improvement and refinement of the previously known results in these fields. We hope that the interested reader may be able to explore the novel and innovative applications of these extended general variational inequalities in other branches of pure and applied sciences. This is may open other window of future research in this growing and dynamic field.

## 2. Preliminaries

Let $H$ be a real Hilbert space whose inner product and norm are denoted by $< \cdot, \cdot >$ and $\|.\|$ respectively. Let $K$ be a nonempty closed convex set in $H$.

For given nonlinear operators $T, g, h : H \to H$, consider the problem of finding $u \in H, h(u) \in K$ such that

$$\langle Tu, g(v) - h(u)\rangle \geq 0, \qquad \forall v \in H : g(v) \in K. \tag{1}$$

Inequality of type (1) is called the *extended general variational inequality involving three opertors.* Noor [20-23,26] has shown that the minimum of a class of differentiable nonconvex functions on $hg$-convex set $K$ in $H$ can be characterized by extended general variational inequality (1).

For this purpose, we recall the following well known concepts, see [3].

**Definition 2.1[3,21].** Let $K$ be any set in $H$. The set $K$ is said to be $hg$-convex, if there exist a function $g, h : H \longrightarrow H$ such that

$$h(u) + t(g(v) - h(u)) \in K, \quad \forall u, v \in H : h(u), g(v) \in K, \quad t \in [0, 1].$$

Note that every convex set is $hg$-convex, but the converse is not true, see[22]. If $g = h$, then the $hg$-convex set $K$ is called the $g$-convex set, which was introduced by Youness [34].

From now onward, we assume that $K$ is a $hg$-convex set, unless otherwise specified.

**Definition 2.2[22,26].** The function $F : K \longrightarrow H$ is said to be $hg$-convex, iff, there exists two functions $h, g$ such that

$$F(h(u) + t(g(v) - h(u))) \leq (1 - t)F(h(u)) + tF(g(v))$$

for all $u, v \in H : h(u), g(v) \in K, \quad t \in [0,1]$. Clearly every convex function is $hg$-convex, but the converse is not true. For $g = h$, definition 2.2 is due to Youness [34].

We now show that the minimum of a differentiable $hg$-convex function on the $hg$-convex set $K$ in $H$ can be characterized by the extended general variational inequality (1). This result is due to Noor [21,22,26]. We include all the details for the sake of completeness and to convey the main idea.

**Lemma 2.1[22,26].** Let $F : K \longrightarrow H$ be a differentiable $hg$-convex function. Then $u \in H : h(u) \in K$ is the minimum of $hg$-convex function $F$ on $K$ if and only if $u \in H : h(u) \in K$ satisfies the inequality

$$\langle F'(h(u)), g(v) - h(u)\rangle \geq 0, \quad \forall v \in H : g(v) \in K, \tag{2}$$

where $F'(u)$ is the differential of $F$ at $h(u) \in K$.

**Proof.** Let $u \in H : h(u) \in K$ be a minimum of $hg$-convex function $F$ on $K$. Then

$$F(h(u)) \leq F(g(v)), \quad \forall v \in H : g(v) \in K. \tag{3}$$

Since $K$ is a $hg$-convex set, so, for all $u, v \in H : h(u), g(v) \in K, t \in [0,1], g(v_t) = h(u) + t(g(v) - h(u)) \in K$. Setting $g(v) = g(v_t)$ in (3), we have

$$F(h(u)) \leq F(h(u) + t(g(v) - h(u)).$$

Dividing the above inequality by $t$ and taking $t \longrightarrow 0$, we have

$$\langle F'(h(u)), g(v) - h(u)\rangle \geq 0, \quad \forall v \in H : g(v) \in K,$$

which is the required result(2).

Conversely, let $u \in H : h(u) \in K$ satisfy the inequality (2). Since $F$ is a $hg$-convex function, $\quad \forall u, v \in H : h(u), g(v) \in K, \quad t \in [0,1], \quad h(u) + t(g(v) - h(u)) \in K$ and

$$F(h(u) + t(g(v) - h(u))) \leq (1-t)F(h(u)) + tF(g(v)),$$

which implies that

$$F(g(v)) - F(h(u)) \geq \frac{F(h(u) + t(g(v) - g(u))) - F(h(u))}{t}.$$

Letting $t \longrightarrow 0$, we have

$$F(g(v)) - F(h(u)) \geq \langle F'(h(u)), g(v) - h(u)\rangle \geq 0, \quad \text{using (2)},$$

which implies that

$$F(h(u)) \leq F(g(v)), \quad \forall v \in H : g(v) \in K$$

showing that $u \in K$ is the minimum of $F$ on $K$ in $H$. □

Lemma 2.1 implies that $hg$-convex programming problem can be studied via the extended general variational inequality (1) with $Tu = F'(h(u))$. In a similar way, one can show that the extended general variational inequality is the Fritz-John condition of the inequality constrained optimization problem.

We would like to emphasize that problem (1) is equivalent to finding $u \in H : h(u) \in K$ such that

$$\langle \rho Tu + h(u) - g(u), g(v) - h(u)\rangle \geq 0, \quad \forall v \in H : g(v) \in K. \tag{4}$$

This equivalent formulation is also useful from the applications point of view.

We now list some special cases of the extended general variational inequalities.

**I.** I f $g = h$, then Problem (1) is equivalent to finding $u \in H : g(u) \in K$ such that

$$\langle Tu, g(v) - g(u)\rangle \geq 0, \qquad \forall v \in H : g(v) \in K, \tag{5}$$

which is known as general variational inequality, introduced and studied by Noor [7] in 1988. It turned out that odd order and nonsymmetric obstacle, free, moving, unilateral and equilibrium problems arising in various branches of pure and applied sciences can be studied via general variational inequalities, see [8-10,13-15, 18-23] and the references therein.

**II.** For $h = I$, the identity operator, then problem (1) ie equivalent to finding $u \in K$ such that

$$\langle Tu, g(v) - u\rangle \geq 0, \quad \forall v \in H : g(v) \in K, \tag{6}$$

which is also called the general variational inequalities, introduced and studied by Noor [24].

**III.** For $g \equiv I$, the identity operator, the extended general variational inequality (1) collapses to: find $u \in H : h(u) \in K$ such that

$$\langle Tu, v - h(u)\rangle \geq 0, \quad \forall v \in K, \tag{7}$$

which is also called the general variational inequality, see Noor [8].

**IV.** For $g = h = I$, the identity operator, the extended general variational inequality (2.1) is equivalent to finding $u \in K$ such that

$$\langle Tu, v - u\rangle \geq 0, \qquad \forall v \in K, \tag{8}$$

which is known as the classical variational inequality and was introduced in 1964 by Stampacchia [33]. For the recent applications, numerical methods, sensitivity analysis, dynamical systems and formulations of variational inequalities, see [1-35] and the references therein.

**V.** If $K^* = \{u \in H; \langle u, v\rangle \geq 0, \quad \forall v \in K\}$ is a polar(dual) convex cone of a closed convex cone $K$ in $H$, then problem (1) is equivalent to finding $u \in H$ such that

$$g(u) \in K, \quad Tu \in K^*, \quad \langle g(u), Tu\rangle = 0, \tag{9}$$

which is known as the general complementarity problem, see[15]. If $g = I$, the identity operator, then problem (9) is called the generalized complementarity problem. For $g(u) = u - m(u)$, where $m$ is a point-to-point mapping, then problem (9) is called the quasi(implicit) complementarity problem, see [15,30] and the references therein.

From the above discussion, it is clear that the extended general variational inequalities (1) is most general and includes several previously known classes of variational inequalities and related optimization problems as special cases. These variational inequalities have important applications in mathematical programming and engineering sciences, see the references.

We also need the following concepts and results.

**Lemma 2.2.** Let $K$ be a closed convex set in $H$. Then, for a given $z \in H$, $u \in K$ satisfies the inequality

$$\langle u - z, v - u\rangle \geq 0, \quad \forall v \in K,$$

if and only if

$$u = P_K z,$$

where $P_K$ is the projection of $H$ onto the closed convex set $K$ in $H$.

It is well known that the projection operator $P_K$ is a nonexpansive operator, that is,

$$\|P_K u - P_K v\| \leq \|u - v\|, \quad \forall u, v \in H.$$

**Definition 2.3.** An operator $T : H \to H$ is said to be:

**(i)** *strongly monotone*, if there exists a constant $\alpha > 0$ such that

$$\langle Tu - Tv, u - v\rangle \geq \alpha||u - v||^2, \quad \forall u, v \in H.$$

**(ii)** *Lipschitz continuous*, if there exists a constant $\beta > 0$ such that

$$||Tu - Tv|| \leq \beta||u - v||, \quad \forall u, v \in H..$$

From (i) and (ii), it follows that $\alpha \leq \beta$.

**Definition 2.4** A mapping $T : H \to H$ is called relaxed cocoercive, if there exists a constant $\gamma > 0$ such that

$$\langle Tx - Ty, x - y\rangle \geq -\gamma||Tx - Ty||^2, \quad \forall x, y \in H.$$

**Definition 2.5.** A mapping $T : H \to H$ is called relaxed co-coercive strongly monotone, if there exist constants $\gamma > 0, \alpha > 0$ such that

$$\langle Tx - Ty, x - y\rangle \geq -\gamma||Tx - Ty||^2 + \alpha||x - y||^2 \quad \forall x, y \in H.$$

It is clear that, if $T$ is Lipschitz continuous, then the relaxed co-coercive strongly monotone operator is strongly monotone with a constant $(\alpha - \gamma\beta^2)$. However, the converse is not true. Thus it is obvious that class of relaxed cocoercive strongly monotone operator is more general than the class of strongly monotone operators.

## 3. Main Results

In this section, we suggest and analyze some new approximation schemes for solving the extended general variational inequality (4). One can prove that the extended general variational inequality (4) is equivalent to the fixed point problem by invoking Lemma 2.2.

**Lemma 3.1[22].** The function $u \in H : h(u) \in K$ is a solution of the extended general variational inequality (4) if and only if $u \in H : h(u) \in K$ satisfies the relation

$$h(u) = P_K[g(u) - \rho Tu], \tag{10}$$

where $P_K$ is the projection operator and $\rho > 0$ is a constant.

Lemma 3.1 implies that the extended general variational inequality (4) is equivalent to the fixed point problem (10). This alternative equivalent formulation is very useful from the numerical and theoretical points of view. Zhao and Sun [35] used the concept of the exceptional family to study the existence of a solution of the nonlinear projection equations (10).

We rewrite the the relation (10) in the following form

$$F(u) = u - h(u) + P_K[g(u) - \rho Tu], \tag{11}$$

which is used to study the existence of a solution of the extended general variational inequalities (4).

We now study those conditions under which the extended general variational inequality (4) has a unique solution and this is the main motivation of our next result.

**Theorem 3.1.** Let the operators $T, g, h : H \longrightarrow H$ be relaxed co-coercive strongly monotone with constants $(\gamma > 0, \alpha > 0)$, $(\gamma_1 > 0, \sigma > 0)$, $(\gamma_2 > 0, \mu > 0)$ and Lipschitz continuous with constants with $\beta > 0$, $\delta > 0$, $\eta > 0$ respectively. If

$$|\rho - \frac{(\alpha - \gamma\beta^2)}{\beta^2}| < \frac{\sqrt{(\alpha - \gamma\beta^2)^2 - \beta^2 k(2-k)}}{\beta^2}, \quad \alpha > \gamma\beta^2 + \beta\sqrt{k(2-k)}, \quad k < 1, \tag{12}$$

where

$$k = \sqrt{1 - 2(\sigma - \gamma_1\delta^2) + \delta^2} + \sqrt{1 - 2(\mu - \gamma_2\eta^2) + \eta^2}, \tag{13}$$

then, there exists a unique solution $u \in H : h(u) \in K$ of the extended general variational inequality (4).

**Proof.** From Lemma 3.1, it follows that problems (10) and (4) are equivalent. Thus it is enough to show that the map $F(u)$, defined by (11), has a fixed point. For all $u \neq v \in H$,

$$\begin{aligned} ||F(u) - F(v)|| &= ||u - v - (h(u) - h(v)) + P_K[g(u) - \rho Tu] - P_K[g(v) - \rho Tv]|| \\ &\leq ||u - v - (h(u) - h(v))|| + ||P_K[g(u) - \rho Tu] - P_K[g(v) - \rho Tv]|| \\ &\leq ||u - v - (g(u) - g(v))|| + ||u - v - (h(u) - h(v))|| \\ &\quad + ||u - v - \rho(Tu - Tv)||, \end{aligned} \tag{14}$$

where we have used the fact that the operator $P_K$ is nonexpansive.

Since the operator $T$ is relaxed co-coercive strongly monotone with constants $\gamma > 0, \alpha > 0$ and Lipschitz continuous with constant $\beta > 0$, it follows that

$$\begin{aligned} ||u - v - \rho(Tu - Tv)||^2 &\leq ||u - v||^2 - 2\rho\langle Tu - Tv, u - v\rangle + \rho^2||Tu - Tv||^2 \\ &\leq (1 - 2\rho(\alpha - \gamma\beta^2) + \rho^2\beta^2)||u - v||^2. \end{aligned} \tag{15}$$

In a similar way, we have

$$||u - v - (g(u) - g(v))||^2 \leq (1 - 2(\sigma - \gamma_1\delta^2) + \delta^2)||u - v||^2, \tag{16}$$

$$||u - v - (h(u) - h(v))||^2 \leq (1 - 2(\mu - \gamma_2\eta^2) + \eta^2)||u - v||^2, \tag{17}$$

where $\gamma_1 > 0, \sigma > 0$, $\gamma_2 > 0, \mu > 0$ and $\delta > 0$, $\eta > 0$ are the relaxed co-coercive strongly monotonicity and Lipschitz continuity constants of the operator $g$ and $h$ respectively.

From (13), (14), (15),(16) and (17), we have

$$\begin{aligned} ||F(u) - F(v)|| &\leq (\sqrt{1 - 2(\sigma - \gamma_1\delta^2) + \delta^2} + \sqrt{1 - 2(\mu - \gamma_2\eta^2) + \eta^2} \\ &\quad + \sqrt{1 - 2\rho(\alpha - \gamma\beta^2) + \beta^2\rho^2})||u - v|| \\ &= (k + t(\rho))||u - v||, \\ &= \theta||u - v||, \end{aligned}$$

where

$$t(\rho) = \sqrt{1 - 2\rho(\alpha - \gamma\beta^2) + \rho^2\beta^2}. \tag{18}$$

and

$$\theta = k + t(\rho). \tag{19}$$

From (12), it follows that $\theta < 1$, which implies that the map $F(u)$ defined by has a fixed point, which is a unique solution of (4). □

Using the fixed point formulation (10), Noor [22] has suggested and analyzed the following iterative method for solving the extended general variational inequalities (4).

**Algorithm 3.1.** For a given $u_0 \in H$, find the approximate solution $u_{n+1}$ by the iterative schemes

$$u_{n+1} = (1-\alpha_n)u_n + \alpha_n\{u_n - h(u_n) + P_K[g(u_n) - \rho T u_n]\}, \quad n = 0, 1, \ldots$$

which is known as the Mann iteration process for solving the extended general variational inequalities (4).

Note that if $h = g$, then Algorithm 3.1 reduces to the following iterative method for solving the general variational inequalities (5).

**Algorithm 3.2.** For a given $u_0 \in H$, find the approximate solution $u_{n+1}$ by the iterative schemes

$$u_{n+1} = (1-\alpha_n)u_n + \alpha_n\{u_n - g(u_n) + P_K[g(u_n) - \rho T u_n]\}, \quad n = 0, 1, \ldots$$

which is due to Noor [21]. For the convergence analysis of Algorithm 3.2 and Algorithm 3.2, see Noor [13,15].

Using the technique of updating the solution, we now suggest and analyze some iterative three-step iterative schemes for solving the extended general variational inequalities (2.4) and this is the main motivation of this paper.

**Algorithm 3.3.** For a given $u_0 \in H$, compute the approximate solutions $\{u_n\}$, $\{w_n\}$ and $\{y_n\}$ by the iterative schemes

$$\begin{aligned} h(y_n) &= P_K[g(u_n) - \rho T u_n] \\ h(w_n) &= P_K[g(y_n) - \rho T y_n] \\ h(u_{n+1}) &= P_K[g(w_n) - \rho T w_n], \quad n = 0, 1, 2, \ldots \ldots \end{aligned}$$

Using Lemma 2.2, Algorithm 3.3 can be written as

**Algorithm 3.4.** For a given $u_0 \in H$, compute the approximate solution $\{u_n\}$ by the iterative schemes

$$\begin{aligned} &\langle \rho T u_n + h(y_n) - g(u_n), g(v) - h(y_n) \rangle \geq 0, \quad \forall g(v) \in K \\ &\langle \rho T y_n + h(w_n) - g(y_n), g(v) - h(w_n) \rangle \geq 0, \quad \forall g(v) \in K \\ &\langle \rho T w_n + h(u_{n+1}) - g(w_n), g(v) - h(u_{n+1}) \rangle \geq 0, \quad \forall g(v) \in K \end{aligned}$$

Invoking Algorithm 3.3, we now suggested another three step scheme for solving the extended general variational inequality (4).

**Algorithm 3.5.** For a given $u_0 \in H$, compute the approximate solution $\{u_n\}$ by the iterative schemes

$$y_n = (1-\gamma_n)u_n + \gamma_n\{u_n - h(u_n) + P_K[g(u_n) - \rho T u_n]\} \tag{20}$$

$$w_n = (1-\beta_n)u_n + \beta_n\{y_n - h(y_n) + P_K[g(y_n) - \rho T y_n]\} \tag{21}$$

$$u_{n+1} = (1-\alpha_n)u_n + \alpha_n\{w_n - h(w_n) + P_K[g(w_n) - \rho T w_n]\}. \tag{22}$$

For $\gamma_n = 0$, Algorithm 3.5 reduces to:

**Algorithm 3.6.** For a given $u_0 \in H$, compute $\{u_n\}$ by the iterative schemes

$$\begin{aligned} w_n &= (1-\beta_n)u_n + \beta_n\{u_n - h(u_n) + P_K[g(u_n) - \rho T u_n]\} \\ u_{n+1} &= (1-\alpha_n)u_n + \alpha_n\{w_n - h(w_n) + P_K[g(w_n) - \rho T w_n]\}, \quad n = 0, 1, 2, \ldots \ldots \end{aligned}$$

which is known as the Ishikawa iterative scheme for the extended general variational inequality (4). Note that for $\gamma_n = 0$ and $\beta_n = 0$, Algorithm 3.5 is called the Mann iterative method.

For $g = h = I$, the identity operator, Algorithm 3.5 collapses to the following algorithm for variational inequality (8), which are mainly due to Noor [13,15].

**Algorithm 3.7.** For a given $u_0 \in K$, compute $\{u_n\}$ by the iterative schemes

$$\begin{aligned} y_n &= (1-\gamma_n)u_n + \gamma_n P_K[u_n - \rho T u_n] \\ w_n &= (1-\beta_n)u_n + \beta_n P_K[y_n - \rho T y_n] \\ u_{n+1} &= (1-\alpha_n)u_n + \alpha_n P_K[w_n - \rho T w_n], \quad n = 0, 1, 2, \ldots\ldots \end{aligned}$$

Now we suggest a perturbed iterative scheme for solving the extended general variational inequality (4).

**Algorithm 3.8.** For a given $u_o \in H$, compute the approximate solution $\{u_n\}$ by the iterative schemes

$$\begin{aligned} y_n &= (1-\gamma_n)u_n + \gamma_n\{u_n - h(u_n) + P_{K_n}[g(u_n) - \rho T u_n]\} + \gamma_n h_n \\ w_n &= (1-\beta_n)u_n + \beta_n\{y_n - h(y_n) + P_{K_n}[g(y_n) - \rho T y_n]\} + \beta_n f_n \\ u_{n+1} &= (1-\alpha_n)u_n + \alpha_n\{w_n - h(w_n) + P_{K_n}[g(w_n) - \rho T w_n]\} + \alpha_n e_n, \end{aligned}$$

where $\{e_n\}$, $\{f_n\}$, and $\{h_n\}$ are the sequences of the elements of $H$ introduced to take into account possible inexact computations and $P_{K_n}$ is the corresponding perturbed projection operator; and the sequences $\{\alpha_n\}$, $\{\beta_n\}$ and $\{\gamma_n\}$ satisfy $0 \leq \alpha_n, \beta_n, \gamma_n \leq 1$; for all $n \geq 0$ and $\sum_{n=0}^{\infty} \alpha_n = \infty$.

For $\gamma_n = 0$, we obtain the perturbed Ishikawa iterative method and for $\gamma_n = 0$ and $\beta_n = 0$, we obtain the perturbed Mann iterative schemes for solving the extended general variational inequality (4). If $g = h$, , we obtain the perturbed iterative method for solving the general variational inequalities (5), which is mainly due to Noor [13,15].

If $g = h = I$, and $K = H$, then Algorithm 3.8 is equivalent to the following three-step scheme for the nonlinear equations $Tu = 0$, which is known as Noor three-step iterative method, see [13,15] and the references therein.

**Algorithm 3.9.** For a given $u_0 \in H$, find the approximate solution $\{u_n\}$ by the iterative schemes

$$\begin{aligned} y_n &= (1-\gamma_n)u_n + \gamma_n T u_n + \gamma_n h_n \\ w_n &= (1-\beta_n)u_n + \beta_n T y_n + \beta_n f_n \\ u_{n+1} &= (1-\alpha_n)u_n + \alpha_n T w_n + \alpha_n e_n, \quad n = 0, 1, 2, \ldots \end{aligned}$$

where $\{e_n\}$, $\{f_n\}$ and $\{h_n\}$ are sequences of the elements of $H$ introduced to take into account possible inexact computations and the sequences $\{\alpha_n\}$, $\{\beta_n\}$ and $\{\gamma_n\}$ satisfy $0 \leq \alpha_n, \beta_n, \gamma_n \leq 1$; for all $n \geq 0$ and $\sum_{n=0}^{\infty} \alpha_n = \infty$.

In brief, for suitable and appropriate choice of the operators $T, g$ and the space $H$, one can obtain a number of new and previously known iterative schemes for solving variational inequalities and related problems. This clearly shows that Algorithm 3.5 and Algorithm 3.9 are quite general and unifying ones.

We now study the convergence criteria of Algorithms 3.5. In a similar way, one can analyze the convergence criteria of other algorithms.

**Theorem 3.2.** Let the operators $T, g, h$ satisfy all the assumptions of Theorem 3.1. If the condition (12) holds, then the approximate solution $\{u_n\}$ obtained from

Algorithm 3.5 converges to an exact solution $u$ of the extended general variational inequality (4) strongly in $H$.

**Proof.** From Theorem 3.1, we see that there exists a unique solution $u \in H$ of the extended general variational inequality (4). Let $u \in H$ be a unique solution of (4). Then, using Lemma 3.1, we have

$$u = (1-\alpha_n)u + \alpha_n\{u - h(u) + P_K[g(u) - \rho Tu]\} \tag{23}$$

$$= (1-\beta_n)u + \beta_n\{u - h(u) + P_K[g(u) - \rho Tu]\} \tag{24}$$

$$= (1-\gamma_n)u + \gamma_n\{u - h(u) + P_K[g(u) - \rho Tu]\}. \tag{25}$$

From (20),(23),(15), (16) and (17), we have

$$\begin{aligned} ||u_{n+1} - u|| &= ||(1-\alpha_n)(u_n - u) + \alpha_n(w_n - u - (h(w_n) - h(u))) \\ &+ \alpha_n\{P_K[g(w_n) - \rho Tw_n] - P_K[g(u) - \rho Tu]\}|| \\ &\leq (1-\alpha_n)||u_n - u|| + \alpha_n||w_n - u - (g(w_n) - g(u))|| \\ &\quad + + \alpha_n||w_n - u - (h(w_n) - h(u))|| \\ &+ \alpha_n||w_n - u - \rho(Tw_n - Tu)|| \\ &\leq (1-\alpha_n)||u_n - u|| + \alpha_n(k + t(\rho))||w_n - u||, \\ &= (1-\alpha_n)||u_n - u|| + \alpha_n\theta||w_n - u||, \end{aligned} \tag{26}$$

In a similar way, from (21),(24) and using (13), (15), and (16), we have

$$\begin{aligned} ||w_n - u|| &\leq (1-\beta_n)||u_n - u|| + 2\beta_n\theta||y_n - u - (g(y_n) - g(u))|| \\ &+ \beta_n||y_n - u - \rho(Ty_n - Tu)|| \\ &\leq (1-\beta_n)||u_n - u|| + \beta_n(k + t(\rho))||y_n - u||, \\ &\leq (1-\beta_n)||u_n - u|| + \beta_n\theta||y_n - u||, \end{aligned} \tag{27}$$

and from (16), (25) and (17), we obtain

$$\begin{aligned} ||y_n - u|| &\leq (1-\gamma_n)||u_n - u|| + \gamma_n\theta||u_n - u||, \\ &\leq (1-(1-\theta)\gamma_n)||u_n - u|| \\ &\leq ||u_n - u||. \end{aligned} \tag{28}$$

From (27) and (28), we obtain

$$\begin{aligned} ||w_n - u|| &\leq (1-\beta_n)||u_n - u|| + \beta_n\theta||u_n - u|| \\ &= (1-(1-\theta)\beta_n)||u_n - u|| \\ &\leq ||u_n - u||. \end{aligned} \tag{29}$$

Combining (26) and (29), we have

$$\begin{aligned} ||u_{n+1} - u|| &\leq (1-\alpha_n)||u_n - u|| + \alpha_n\theta||u_n - u|| \\ &= [1-(1-\theta)\alpha_n]||u_n - u|| \\ &\leq \prod_{i=0}^{n}[1-(1-\theta)\alpha_i]||u_0 - u||. \end{aligned}$$

Since $\sum_{n=0}^{\infty}\alpha_n$ diverges and $1-\theta > 0$, we have $\lim_{n\longrightarrow\infty}\prod_{i=0}^{n}[1-(1-\theta)\alpha_i] = 0$. Consequently the sequence $\{u_n\}$ convergences strongly to $u$. From (28), and (29), it follows that the sequences $\{y_n\}$ and $\{w_n\}$ also converge to u strongly in $H$. This completes the proof. □

**Acknowledgement.** The author would like to express his deepest gratitude to Dr. S. M. Junaid Zaidi, Rector, CIIT, Islamabad, for the excellent research facilities and support in his research endeavors.

## References

[1] C. Baiocchi and A. Capelo, Variational and Quasi Variational Inequalities, J. Wiley and Sons, New York, 1984.
[2] A. Bnouhachem and M. Aslam Noor, Numerical methods for general mixed variational inequalities, Appl. Math. Comput. **204**(2008), 27-36.
[3] G. Cristescu and L. Lupsa, Non-connected Convexities and Applications, Kluwer Academic Publishers, Dordrecht, Holland, 2002.
[4] F. Giannessi and A. Maugeri, Variational Inequalities and Network Equilibrium Problems, Plenum Press, New York, 1995.
[5] R. Glowinski, J.L. Lions and R. Trémolières, Numerical Analysis of Variational Inequalities, North-Holland, Amsterdam, 1981.
[6] R. Glowinski and P. Le Tellec, Augmented Lagrangian and Operator Splitting Methods in Nonlinear Mechanics, SIAM, Philadelphia,, Pennsylvania, 1989.
[7] M. Aslam Noor, General variational inequalities, Appl. Math. Letters **1**(1988), 119-121.
[8] M. Aslam Noor, Quasi variational inequalities, Appl. Math. Letters, **1**(1988), 367-370.
[9] M. Aslam Noor, Wiener-Hopf equations and variational inequalities, J. Optim. Theory Appl. **79**(1993), 197-206.
[10] M. Aslam Noor, Some algorithms for general monotone mixed variational inequalities, Mathl. Computer Modelling **29**(7)(1999), 1-9.
[11] M. Aslam Noor, Some recent advances in variational inequalities, Part I, basic concepts, New Zealand J. Math. **26**(1997), 53-80.
[12] M. Aslam Noor, Some recent advances in variational inequalities, Part II, other concepts, New Zealand J. Math. **26**(1997), 229-255.
[13] M. Aslam Noor, New approximation schemes for general variational inequalities, J. Math. Anal. Appl. , **251**(2000), 217-229.
[14] M. Aslam Noor, Mixed quasi variational inequalities, Appl. Math. Computation, **146**(2003), 553-578.
[15] M. Aslam Noor, Some developments in general variational inequalities, Appl. Math. Computation, **152**(2004), 199-277.
[16] M. Aslam Noor, Fundamentals of mixed quasi variational inequalities, Inter. J. Pure Appl. Math. **15**(2004), 137-258,
[17] M. Aslam Noor, Fundamentals of equilibrium problems, Math. Inequal. Appl. **9**(2006), 529-566.
[18] M. Aslam Noor, Merit functions for general variational inequalities, J. Math. Anal. Appl. **316**(2006), 736-752.
[19] M. Aslam Noor, Projection-proximal methods for general variational inequalities, J. Math. Anal. Appl. **318**(2006), 53-62.
[20] M. Aslam Noor, Auxiliary principle technique for extended general variational inequalities, Banach J. Math. Anal. **2**(2008), 33-39.
[21] M. Aslam Noor, Projection iterative methods for extended general variational inequalities, J. Appl. Math. Comput. (2009).
[22] M. Aslam Noor, Extended general variational inequalities, Appl. Math. Letters, (2008).
[23] M. Aslam Noor, Sensitivity analysis of extended general variational inequalities, Appl. Math. E-Notes, (2009).
[24] M. Aslam Noor, Differentiable nonconvex functions and general variational inequalities, Appl. Math. Comput. **199**(2008), 623-630.
[25] M. Aslam Noor, Implicit Wiener-Hopf equations and quasi variational inequalities, Albanian J. Math. **2**(2008), 15-25.
[26] M. Aslam Noor, Variational Inequalities and Applications, Lecture Notes, Mathematics department, COMSATS Institute of Information Technology, Islamabad, Pakistan, 2007.

[27] M. Aslam Noor and K. Inayat Noor, On sensitivity analysis of general variational inequalities, Math. Comm. **13**(2008), 75-83.
[28] M. Aslam Noor and K. Inayat Noor, Projection Iterative Methods for General Variational Inequalities, Inter. J. Appl. Math. Engng. Sci. **2**(2008).
[29] M. Aslam Noor and K. Inayat Noor, Projection algorithms for solving a system of general variational inequalities, Nonl. Anal. (2009).
[30] M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Some aspects of variational inequalities, J. Comput. Appl. Math. **47**(1993), 285-312.
[31] M. Aslam Noor, Y. Yao and Y. C. Liou, Extragradient method for equilibrium problems and variational inequalities, Albanian J. Math. **2**(2008), 125-138.
[32] M. Patriksson, Nonlinear Programming and Variational Inequalities: A Unified Approach, Kluwer Academic Publishers, Dordrecht, 1998.
[33] G. Stampacchia, Formes bilineaires coercivities sur les ensembles convexes, C. R. Acad. Sci. Paris, **258** (1964), 4413-4416.
[34] E. A. Youness, $E$-convex sets, $E$-convex functions and $E$-convex programming, J. Optim. Theory Appl. **102**(1999),439-450.
[35] Y Zhao and D. Sun, Alternative theorems for nonlinear projection equations and applications to generalized complementarity problems, Nonl. Anal. **46**(2001), 853-868.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 4, Pages 277–282
ISSN 1930-1235: (2008)

# COMMON FIXED POINT THEOREM IN INTUITIONISTIC FUZZY METRIC SPACES

R. Saadati

*Department of Mathematics and Computer Science,*
*Amirkabir University of Technology,*
*No. 424, Hafez Ave., Tehran, Iran*
*rsaadati@eml.cc*

S.M. Vaezpour

*Department of Mathematics and Computer Science,*
*Amirkabir University of Technology,*
*No. 424, Hafez Ave., Tehran, Iran*

J. Vahidi

*Department of Mathematics,*
*University of Mazandaran,*
*Babolsar, Iran*

Abstract. In this paper, a common fixed point theorem for $R$-weakly commuting maps in intuitionistic fuzzy metric spaces is proved.

## 1. Introduction and Preliminaries

In this section, using the idea of intuitionistic fuzzy metric spaces introduced by Park [5] we define the new notion of intuitionistic fuzzy metric spaces with the help of the notion of continuous $t$–representable.

**Definition 1.1.** A complete lattice is a partially ordered set in which every nonempty subset admits supremum and infimum.

2000 *Mathematics Subject Classification.* 54E40; 54E35; 54H25.

*Key words and phrases.* Intuitionistic Fuzzy contractive mapping; Complete intuitionistic fuzzy metric space; Common fixed point theorem; $R$-weakly commuting maps.

This research is partially supported by Research Center in Algebraic Hyperstructures and Fuzzy Mathematics, University of Mazandaran, Babolsar, Iran.

**Lemma 1.2.** ([2]) *Consider the set $L^*$ and operation $\leq_{L^*}$ defined by:*

$$L^* = \{(x_1, x_2) : (x_1, x_2) \in [0,1]^2 \text{ and } x_1 + x_2 \leq 1\},$$

*$(x_1, x_2) \leq_{L^*} (y_1, y_2) \iff x_1 \leq y_1$ and $x_2 \geq y_2$, for every $(x_1, x_2), (y_1, y_2) \in L^*$. Then $(L^*, \leq_{L^*})$ is a complete lattice .*

**Definition 1.3.** ([1]) An intuitionistic fuzzy set $\mathcal{A}_{\zeta,\eta}$ in a universe $U$ is an object $\mathcal{A}_{\zeta,\eta} = \{(\zeta_{\mathcal{A}}(u), \eta_{\mathcal{A}}(u)) | u \in U\}$, where, for all $u \in U$, $\zeta_{\mathcal{A}}(u) \in [0,1]$ and $\eta_{\mathcal{A}}(u) \in [0,1]$ are called the membership degree and the non-membership degree, respectively, of $u$ in $\mathcal{A}_{\zeta,\eta}$, and furthermore they satisfy $\zeta_{\mathcal{A}}(u) + \eta_{\mathcal{A}}(u) \leq 1$.

We denote its units by $0_{L^*} = (0,1)$ and $1_{L^*} = (1,0)$. Classically, a triangular norm $* = T$ on $[0,1]$ is defined as an increasing, commutative, associative mapping $T : [0,1]^2 \longrightarrow [0,1]$ satisfying $T(1,x) = 1 * x = x$, for all $x \in [0,1]$. A triangular conorm $S = \diamond$ is defined as an increasing, commutative, associative mapping $S : [0,1]^2 \longrightarrow [0,1]$ satisfying $S(0,x) = 0 \diamond x = x$, for all $x \in [0,1]$. Using the lattice $(L^*, \leq_{L^*})$ these definitions can be straightforwardly extended.

**Definition 1.4.** ([2]) A triangular norm ($t$–norm) on $L^*$ is a mapping $\mathcal{T} : (L^*)^2 \longrightarrow L^*$ satisfying the following conditions:

$(\forall x \in L^*)(\mathcal{T}(x, 1_{L^*}) = x)$, (boundary condition)

$(\forall (x,y) \in (L^*)^2)(\mathcal{T}(x,y) = \mathcal{T}(y,x))$, (commutativity)

$(\forall (x,y,z) \in (L^*)^3)(\mathcal{T}(x, \mathcal{T}(y,z)) = \mathcal{T}(\mathcal{T}(x,y), z))$, (associativity)

$(\forall (x,x',y,y') \in (L^*)^4)(x \leq_{L^*} x' \text{ and } y \leq_{L^*} y' \implies \mathcal{T}(x,y) \leq_{L^*} \mathcal{T}(x',y'))$. (monotonicity)

If $(L^*, \leq_{L^*}, \mathcal{T})$ is an Abelian topological monoid with unit $1_{L^*}$ then $\mathcal{T}$ is said to be a *continuous* $t$–norm.

**Definition 1.5.** ([2]) A continuous $t$–norm $\mathcal{T}$ on $L^*$ is called continuous $t$–*representable* if and only if there exist a continuous $t$–norm $*$ and a continuous $t$–conorm $\diamond$ on $[0,1]$ such that, for all $x = (x_1, x_2), y = (y_1, y_2) \in L^*$,

$$\mathcal{T}(x,y) = (x_1 * y_1, x_2 \diamond y_2).$$

For example $\mathcal{T}(a,b) = (a_1 b_1, \min(a_2 + b_2, 1))$ for all $a = (a_1, a_2)$ and $b = (b_1, b_2)$ in $L^*$ is a continuous $t$–representable.

**Definition 1.6.** A negator on $L^*$ is any decreasing mapping $\mathcal{N} : L^* \longrightarrow L^*$ satisfying $\mathcal{N}(0_{L^*}) = 1_{L^*}$ and $\mathcal{N}(1_{L^*}) = 0_{L^*}$ . If $\mathcal{N}(\mathcal{N}(x)) = x$, for all $x \in L^*$, then $\mathcal{N}$ is called an involutive negator. A negator on $[0,1]$ is a decreasing mapping $N : [0,1] \longrightarrow [0,1]$ satisfying $N(0) = 1$ and $N(1) = 0$. $N_s$ denotes the standard negator on $[0,1]$ defined as, for all $x \in [0,1]$, $N_s(x) = 1 - x$. We define $(N_s(\lambda), \lambda) = \mathcal{N}_s(\lambda)$.

**Definition 1.7.** Let $M, N$ are fuzzy sets from $X^2 \times (0, +\infty)$ to $[0,1]$ such that $M(x,y,t) + N(x,y,t) \leq 1$ for all $x, y \in X$ and $t > 0$, in which, $M$ is membership degree and $N$ is non-membership degree of an intuitionistic fuzzy set. The triple $(X, \mathcal{M}_{M,N}, \mathcal{T})$ is said to be an *intuitionistic fuzzy metric space* if $X$ is an arbitrary (non-empty) set, $\mathcal{T}$ is a continuous $t$–representable and $\mathcal{M}_{M,N}$ is a mapping $X^2 \times (0, +\infty) \to L^*$ (an intuitionistic fuzzy set, see Definition 2.4) satisfying the following conditions for every $x, y, z \in X$ and $t, s > 0$:

(a) $\mathcal{M}_{M,N}(x,y,t) >_{L^*} 0_{L^*}$;

(b) $\mathcal{M}_{M,N}(x,y,t) = 1_{L^*}$ if and only if $x = y$;

(c) $\mathcal{M}_{M,N}(x,y,t) = \mathcal{M}_{M,N}(y,x,t)$;
(d) $\mathcal{M}_{M,N}(x,y,t+s) \geq_{L^*} \mathcal{T}(\mathcal{M}_{M,N}(x,z,t), \mathcal{M}_{M,N}(z,y,s))$;
(e) $\mathcal{M}_{M,N}(x,y,\cdot) : (0,\infty) \longrightarrow L^*$ is continuous.

In this case $\mathcal{M}_{M,N}$ is called an *intuitionistic fuzzy metric*. Here,

$$\mathcal{M}_{M,N}(x,y,t) = (M(x,y,t), N(x,y,t)).$$

Let $(X, \mathcal{M}_{M,N}, \mathcal{T})$ be an intuitionistic fuzzy metric space. For $t > 0$, define the *open ball* $B(x,r,t)$ with center $x \in X$ and radius $0 < r < 1$, as

$$B(x,r,t) = \{y \in X : \mathcal{M}_{M,N}(x,y,t) >_{L^*} (N_s(r), r) = \mathcal{N}_s(r)\}.$$

A subset $A \subseteq X$ is called *open* if for each $x \in A$, there exist $t > 0$ and $0 < r < 1$ such that $B(x,r,t) \subseteq A$. Let $\tau_{\mathcal{M}_{M,N}}$ denote the family of all open subset of $X$. $\tau_{\mathcal{M}_{M,N}}$ is called the *topology induced by intuitionistic fuzzy metric*. A sequence $\{x_n\}$ in an intuitionistic fuzzy metric space $(X, \mathcal{M}_{M,N}, \mathcal{T})$ is called a *Cauchy sequence* if for each $\varepsilon > 0$ and $t > 0$, there exists $n_0 \in \mathbf{N}$ such that

$$\mathcal{M}_{M,N}(x_n, x_m, t) >_{L^*} \mathcal{N}_s(\varepsilon),$$

and for each $n, m \geq n_0$. The sequence $\{x_n\}$ is said to be *convergent* to $x \in V$ in the intuitionistic fuzzy metric space $(X, \mathcal{M}_{M,N}, \mathcal{T})$ and denoted by $x_n \overset{\mathcal{M}_{M,N}}{\longrightarrow} x$ if $\mathcal{M}_{M,N}(x_n, x, t) \longrightarrow 1_{L^*}$ whenever $n \longrightarrow \infty$ for every $t > 0$. An intuitionistic fuzzy metric space is said to be *complete* if and only if every Cauchy sequence is convergent (see [3, 5]).

**Lemma 1.8.** ([3]) *Let $(X, \mathcal{M}_{M,N}, \mathcal{T})$ be an intuitionistic fuzzy metric space. Then, $\mathcal{M}_{M,N}(x,y,t)$ is nondecreasing with respect to $t$, for all $x, y$ in $X$.*

**Example 1.9.** ([7]) Let $(X,d)$ be a metric space. Denote $\mathcal{T}(a,b) = (a_1 b_1, \min(a_2 + b_2, 1))$ for all $a = (a_1, a_2)$ and $b = (b_1, b_2)$ in $L^*$ and let $M$ and $N$ be fuzzy sets on $X^2 \times (0,\infty)$ defined as follows:

$$\mathcal{M}_{M,N}(x,y,t) = (M(x,y,t), N(x,y,t)) = \left(\frac{t}{t + md(x,y)}, \frac{d(x,y)}{t + d(x,y)}\right),$$

in which $m > 1$. Then $(X, \mathcal{M}_{M,N}, \mathcal{T})$ is an intuitionistic fuzzy metric space.

Let $\mathcal{T}$ be a continuous $t$–norm on $L^*$ in which, for every $\mu \in (0,1)$, there exists $\lambda \in (0,1)$ such that

$$\mathcal{T}^{n-1}(\mathcal{N}_s(\lambda), ..., \mathcal{N}_s(\lambda)) >_{L^*} \mathcal{N}_s(\mu), \tag{1.1}$$

where $\mathcal{N}_s$ is an standard negation. For more information see [6].

**Definition 1.10.** Let $(X, \mathcal{M}_{M,N}, \mathcal{T})$ be an intuitionistic fuzzy metric space. $\mathcal{M}_{M,N}$ is said to be continuous on $X \times X \times (0,\infty)$ if

$$\lim_{n\to\infty} \mathcal{M}_{M,N}(x_n, y_n, t_n) = \mathcal{M}_{M,N}(x,y,t)$$

whenever a sequence $\{(x_n, y_n, t_n)\}$ in $X \times X \times (0,\infty)$ converges to a point $(x,y,t) \in X \times X \times (0,\infty)$ i.e., $\lim_n \mathcal{M}_{M,N}(x_n, x, t) = \lim_n \mathcal{M}_{M,N}(y_n, y, t) = 1_{L^*}$ and

$$\lim_n \mathcal{M}_{M,N}(x,y,t_n) = \mathcal{M}_{M,N}(x,y,t).$$

**Lemma 1.11.** *Let $(X, \mathcal{M}_{M,N}, \mathcal{T})$ be an intuitionistic fuzzy metric space. Then $\mathcal{M}_{M,N}$ is continuous function on $X \times X \times (0,\infty)$.*

*Proof.* The proof is same as fuzzy metric spaces (see Proposition 1 of [4]). □

## 2. The Main Results

**Definition 2.1.** Let $f$ and $g$ be maps from an intuitionistic fuzzy metric space $(X, \mathcal{M}_{M,N}, \mathcal{T})$ into itself. The maps $f$ and $g$ are said to be weakly commuting if

$$\mathcal{M}_{M,N}((fog)(x), (gof)(x), t) \geq_{L^*} \mathcal{M}_{M,N}(f(x), g(x), t)$$

for each $x$ in $X$ and $t > 0$.

**Definition 2.2.** Let $f$ and $g$ be maps from an intuitionistic fuzzy metric space $(X, \mathcal{M}_{M,N}, \mathcal{T})$ into itself. The maps $f$ and $g$ are said to be $R$-weakly commuting if there exists some positive real number $R$ such that

$$\mathcal{M}_{M,N}((fog)(x), (gof)(x), t) \geq_{L^*} \mathcal{M}_{M,N}(f(x), g(x), t/R)$$

for each $x$ in $X$ and $t > 0$.

Weak commutativity implies $R$-weak commutativity in intuitionistic fuzzy metric space. However, $R$-weak commutativity implies weak commutativity only when $R \leq 1$.

**Example 2.3.** Let $X = \mathbf{R}$. Let $\mathcal{T}(a, b) = (a_1 b_1, \min(a_2 + b_2, 1))$ for all $a = (a_1, a_2), b = (b_1, b_2) \in L^*$ and let $\mathcal{M}_{M,N}$ be the intuitionistic fuzzy set on $X \times X \times ]0, +\infty[$ defined as follows:

$$\mathcal{M}_{M,N}(x, y, t) = \left( (\exp(\frac{|x-y|}{t}))^{-1}, \frac{\exp(\frac{|x-y|}{t}) - 1}{\exp(\frac{|x-y|}{t})} \right),$$

for all $t \in \mathbf{R}^+$. Then $(X, \mathcal{M}_{M,N}, \mathcal{T})$ is an intuitionistic fuzzy metric space. Define $f(x) = 2x - 1$ and $g(x) = x^2$. Then,

$$\mathcal{M}_{M,N}((fog)(x), (gof)(x), t) - \left( (\exp(2\frac{|x-1|^2}{t}))^{-1}, \frac{\exp(2\frac{|x-1|^2}{t}) - 1}{\exp(2\frac{|x-1|^2}{t})} \right)$$

$$\left( (\exp(\frac{|x-1|^2}{t/2}))^{-1}, \frac{\exp(\frac{|x-1|^2}{t/2}) - 1}{\exp(\frac{|x-1|^2}{t/2})} \right) = \mathcal{M}_{M,N}(f(x), g(x), t/2)$$

$$<_{L^*} \left( (\exp(\frac{|x-1|^2}{t}))^{-1}, \frac{\exp(\frac{|x-1|^2}{t}) - 1}{\exp(\frac{|x-1|^2}{t})} \right) = \mathcal{M}_{M,N}(f(x), g(x), t)$$

Therefore, for $R = 2$, $f$ and $g$ are $R$-weakly commuting. But $f$ and $g$ are not weakly commuting since exponential function is strictly increasing.

**Theorem 2.4.** *Let $(X, \mathcal{M}_{M,N}, \mathcal{T})$ be a complete intuitionistic fuzzy metric space and let $f$ and $g$ be $R$-weakly commuting self-mappings of $X$ satisfying the following conditions:*

(a) $f(X) \subseteq g(X)$;

(b) *$f$ or $g$ is continuous;*

(c) $\mathcal{M}_{M,N}(f(x), f(y), t) \geq_{L^*} \mathcal{C}(\mathcal{M}_{M,N}(g(x), g(y), t))$, *where $\mathcal{C} : L^* \longrightarrow L^*$ is a continuous function such that $\mathcal{C}(a) >_{L^*} a$ for each $a \in L^* \setminus \{0_{L^*}, 1_{L^*}\}$.*

*Then $f$ and $g$ have a unique common fixed point.*

*Proof.* Let $x_0$ be an arbitrary point in $X$. By (a), choose a point $x_1$ in $X$ such that $f(x_0) = g(x_1)$. In general choose $x_{n+1}$ such that $f(x_n) = g(x_{n+1})$. Then for $t > 0$

$$\begin{aligned}\mathcal{M}_{M,N}(f(x_n), f(x_{n+1}), t) &\geq_{L^*} \mathcal{C}(\mathcal{M}_{M,N}(g(x_n), g(x_{n+1}), t)) \\ &= \mathcal{C}(\mathcal{M}_{M,N}(f(x_{n-1}), f(x_n), t)) \\ &>_{L^*} \mathcal{M}_{M,N}(f(x_{n-1}), f(x_n), t)\end{aligned}$$

Thus $\{\mathcal{M}_{M,N}(f(x_n), f(x_{n+1}), t); n \geq 0\}$ is increasing sequence in $L^*$. Therefore, tends to a limit $a \leq_{L^*} 1_{L^*}$. We claim that $a = 1_{L^*}$. For if $a <_{L^*} 1_{L^*}$ on making $n \longrightarrow \infty$ in the above inequality we get $a \geq_{L^*} \mathcal{C}(a) >_{L^*} a$, a contradiction. Hence $a = 1_{L^*}$, i.e.,

$$\lim_n \mathcal{M}_{M,N}(f(x_n), f(x_{n+1}), t) = 1_{L^*}.$$

If we define

$$c_n(t) = \mathcal{M}_{M,N}(f(x_n), f(x_{n+1}), t) \tag{2.1}$$

then $\lim_{n\to\infty} c_n(t) = 1_{L^*}$. Now, we prove that $\{f(x_n)\}$ is a Cauchy sequence in $f(X)$. Suppose that $\{f(x_n)\}$ is not a Cauchy sequence in $f(X)$. For convenience, let $y_n = fx_n$ for $n = 1, 2, 3, \cdots$. Then there is an $\epsilon \in L^* \setminus \{0_{L^*}, 1_{L^*}\}$ such that for each integer $k$, there exist integers $m(k)$ and $n(k)$ with $m(k) > n(k) \geq k$ such that

$$d_k(t) = \mathcal{M}_{M,N}(y_{n(k)}, y_{m(k)}, t) \leq_{L^*} \mathcal{N}_s(\epsilon) \quad \text{for} \quad k = 1, 2, \cdots . \tag{2.2}$$

We may assume that

$$\mathcal{M}_{M,N}(y_{n(k)}, y_{m(k)-1}, t) >_{L^*} \mathcal{N}_s(\epsilon), \tag{2.3}$$

by choosing $m(k)$ be the smallest number exceeding $n(k)$ for which (2.2) holds. Using (2.1), we have

$$\begin{aligned}\mathcal{N}_s(\epsilon) &\geq_{L^*} d_k(t) \\ &\geq_{L^*} \mathcal{T}(\mathcal{M}_{M,N}(y_{n(k)}, y_{m(k)-1}, t/2), \mathcal{M}_{M,N}(y_{m(k)-1}, y_{m(k)}, t/2)) \\ &\geq_{L^*} \mathcal{T}(c_k(t/2), \mathcal{N}_s(\epsilon))\end{aligned}$$

Hence, $d_k(t) \longrightarrow \mathcal{N}_s(\epsilon)$ for every $t > 0$ as $k \longrightarrow \infty$.

$$\begin{aligned}&d_k(t) = \mathcal{M}_{M,N}(y_{n(k)}, y_{m(k)}, t) \\ &\geq_{L^*} \mathcal{T}^2(\mathcal{M}_{M,N}(y_{n(k)}, y_{n(k)+1}, t/3), \mathcal{M}_{M,N}(y_{n(k)+1}, y_{m(k)+1}, t/3), \mathcal{M}_{M,N}(y_{m(k)+1}, y_{m(k)}, t/3) \\ &\geq_{L^*} \mathcal{T}^2(c_k(t/3), \mathcal{C}(\mathcal{M}_{M,N}(y_{n(k)}, y_{m(k)}, t/3)), c_k(t/3)) \\ &\mathcal{T}^2(c_k(t/3), \mathcal{C}(d_k(t/3)), c_k(t/3)).\end{aligned}$$

Thus, as $k \longrightarrow \infty$ in the above inequality we have

$$\mathcal{N}_s(\epsilon) \geq_{L^*} \mathcal{C}(\mathcal{N}_s(\epsilon)) >_{L^*} \mathcal{N}_s(\epsilon)$$

which is a contradiction. Thus, $\{f(x_n)\}_n$ is Cauchy and by the completeness of $X$, $\{f(x_n)\}_n$ converges to $z$ in $X$. Also $\{g(x_n)\}_n$ converges to $z$ in $X$. Let us suppose that the mapping $f$ is continuous. Then $\lim_n (fof)(x_n) = f(z)$ and $\lim_n (fog)(x_n) = f(z)$. Further we have since $f$ and $g$ are $R$-weakly commuting

$$\mathcal{M}_{M,N}((fog)(x_n), (gof)(x_n), t) \geq_{L^*} \mathcal{M}_{M,N}(f(x_n), g(x_n), t/R).$$

On letting $n \to \infty$ in the above inequality we get $\lim_n (gof)(x_n) = f(z)$, by Lemma 1.11. We now prove that $z = f(z)$. Suppose $z \neq f(z)$ then $\mathcal{M}_{M,N}(z, f(z), t) <_{L^*} 1_{L^*}$. By (c)

$$\mathcal{M}_{M,N}(f(x_n), (fof)(x_n), t) \geq_{L^*} \mathcal{C}(\mathcal{M}_{M,N}(g(x_n), (gof)(x_n), t)).$$

On making $n \to \infty$ in the above inequality we get

$$\mathcal{M}_{M,N}(z, f(z), t) \geq_{L^*} \mathcal{C}(\mathcal{M}_{M,N}(z, f(z), t)) >_{L^*} \mathcal{M}(z, f(z), t),$$

a contradiction. Therefore, $z = f(z)$. Since $f(X) \subseteq g(X)$ we can find $z_1$ in $X$ such that $z = f(z) = g(z_1)$. Now,

$$\mathcal{M}((fof)(x_n), f(z_1), t) \geq_{L^*} \mathcal{C}(\mathcal{M}_{M,N}((gof)(x_n), g(z_1), t)).$$

Taking limit as $n \to \infty$ we get

$$\mathcal{M}_{M,N}(f(z), f(z_1), t) \geq_{L^*} \mathcal{C}(\mathcal{M}_{M,N}(f(z), g(z_1), t)) = 1_{L^*}$$

since $\mathcal{C}(1_{L^*}) = 1_{L^*}$, which implies that $f(z) = f(z_1)$, i.e., $z = f(z) = f(z_1) = g(z_1)$. Also for any $t > 0$,

$$\mathcal{M}_{M,N}(f(z), g(z), t) = \mathcal{M}((fog)(z_1), (gof)(z_1), t) \geq_{L^*} \mathcal{M}_{M,N}(f(z_1), g(z_1), t/R) = 1_{L^*}$$

which again implies that $f(z) = g(z)$. Thus $z$ is a common fixed point of $f$ and $g$.

Now to prove uniqueness let if possible $z' \neq z$ be another common fixed point of $f$ and $g$. Then there exists $t > 0$ such that $\mathcal{M}(z, z', t) <_L 1_{\mathcal{L}}$, and

$$\begin{aligned}\mathcal{M}_{M,N}(z, z', t) &= \mathcal{M}_{M,N}(f(z), f(z'), t) \\ &\geq_{L^*} \mathcal{C}(\mathcal{M}_{M,N}(g(z), g(z'), t)) = \mathcal{C}(\mathcal{M}_{M,N}(z, z', t)) \\ &>_{L^*} \mathcal{M}_{M,N}(z, z', t)\end{aligned}$$

which is contradiction. Therefore, $z = z'$, i.e., $z$ is a unique common fixed point of $f$ and $g$. □

## Acknowledgments

The authors would like to thank referee for giving useful comments and suggestions for the improvement of this paper.

## References

[1] K. T. Atanassov, Intuitionistic fuzzy sets, Fuzzy Sets and Systems, 20 (1986), 87–96.
[2] G. Deschrijver and E. E. Kerre. On the relationship between some extensions of fuzzy set theory, Fuzzy Sets and Syst 23 (2003), 227–235.
[3] S. B. Hosseini, D. ORegan, R. Saadati, Some results on intuitionistic fuzzy spaces, Iranian J. Fuzzy Syst, 4 (2007) 53–64.
[4] J. Rodríguez López and S. Ramaguera, The Hausdorff fuzzy metric on compact sets, Fuzzy Sets Syst, 147 (2004) 273–283.
[5] J.H. Park, Intuitionistic fuzzy metric spaces, Chaos, Solitons and Fractals, 22 (2004), 1039–1046.
[6] R. Saadati, A. Razani, and H. Adibi, A Common fixed point theorem in $\mathcal{L}$-fuzzy metric spaces Chaos, Solitons and Fractals,33 (2007) 358–363.
[7] R. Saadati and J.H. Park, Intuitionistic fuzzy Euclidean normed spaces, Commun. Math. Anal., 1 (2006), 86–90.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 4, Pages 283–291
ISSN 1930-1235: (2008)

# DECOMPOSABILITY OF EXTENSION RINGS

V. K. Bhat

*School of Applied Physics and Mathematics,*
*SMVD University,*
*P/o Kakryal, Katra, J and K, India- 182301*
*vijaykumarbhat2000@yahoo.com*

Abstract. Skew polynomial rings have invited attention of mathematicians and various properties of these rings have been discussed. The nature of ideals (in particular prime ideals, minimal prime ideals, associated prime ideals), primary decomposition and Krull dimension have been investigated in certain cases.

This article concerns transparent (decomposable) rings. Recall that a ring R is said to be a *Transparent ring* if in R there exist irreducible ideals $I_j$, $1 \leq j \leq n$ such that $\cap_{j=1}^{n} I_j = 0$ and each $R/I_j$ has a right Artinian quotient ring.

Now let R be a ring, which is an order in an Artinian ring S. Let $\sigma$ and $\tau$ be automorphisms of R and $\delta$ be a $(\sigma, \tau)$-derivation of R; i.e. $\delta : R \to R$ is an additive mapping satisfying $\delta(ab) = \sigma(a)\delta(b) + \delta(a)\tau(b)$ for all a, $b \in R$. We define an extension of R, namely $R[x, \sigma, \tau, \delta] = \{f = \sum_{i=0}^{n} x^i a_i, a_i \in R\}$, subject to the relation $ax = x\sigma(\tau(a)) + \delta(a)$ for all $a \in R$.

We show that if R is a commutative Noetherian $\mathbb{Q}$-algebra, $\sigma$ and $\tau$ as usual, then there exists an integer $m \geq 1$ such that the extension ring $R[x, \alpha, \beta, \vartheta]$ is a *Transparent ring*, where $\alpha = \sigma^m$, $\beta = \tau^m$ and $\vartheta$ is an $(\alpha, \beta)$-derivation of R with $\alpha(\vartheta(a)) = \vartheta(\alpha(a))$, and $\beta(\vartheta(a)) = \vartheta(\beta(a))$, for all $a \in R$.

## 1. Introduction

Throughout this article R is an associative ring with identity and any R-module is unitary. Spec(R) denotes the set of prime ideals of R. Min.Spec(R) denotes the set of minimal prime ideals of R. The set of associated prime ideals of R (viewed as a module over itself) is denoted by Ass(R). For a subset U of an R-module M, the annihilator of U is denoted by Ann(U). Now let R be a Noetherian ring. For any uniform R-module K, the unique associated prime of K (known as assassinator of K) is denoted by Assas(K). C(0) denotes the set of regular elements of R. C(I) denotes the set of elements of R regular modulo I, where I is an ideal of R. N(R) denotes the prime radical of R. $\mid M \mid_{\mathrm{r}}$ denotes the right Krull dimension of a right R-module M. For further details on Krull dimension, the reader is referred to [10]. Let I and J be any two ideals of a ring R. Then $I \subset$ J means that I is strictly

1991 *Mathematics Subject Classification.* Primary 16-XX; Secondary 16N40, 16P40, 16W20, 16W25.

*Key words and phrases.* Automorphism, $\alpha$-derivation, Ore extension, associated prime, decomposable ring.

contained in J. The field of rational numbers, the ring of integers and the set of positive integers are denoted by $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$ respectively, unless otherwise stated.

Let $\sigma$ and $\tau$ be automorphisms of a ring R and $\delta$ be a $(\sigma, \tau)$-derivation of R; i.e. $\delta : R \to R$ is an additive mapping satisfying $\delta(ab) = \sigma(a)\delta(b) + \delta(a)\tau(b)$.
For example let $\sigma$ and $\tau$ be automorphism of a ring R and $\delta : R \to R$ any map.
Let $\phi : R \to M_2(R)$ be defined by

$$\phi(r) = \begin{pmatrix} \tau(r) & 0 \\ \delta(r) & \sigma(r) \end{pmatrix}, \text{ for all } r \in R.$$

Then $\delta$ is a right $(\sigma, \tau)$-derivation of R.

We define an extension of R, namely $R[x, \sigma, \tau, \delta] = \{f = \sum_{i=0}^{n} x^i a_i, a_i \in R\}$, subject to the relation $ax = x\sigma(\tau(a)) + \delta(a)$ for all $a \in R$. Denote $R[x, \sigma, \tau, \delta]$ by $E(R)$. In case $\tau$ is the identity map, we denote $R[x, \sigma, \delta]$ by $O(R)$. In case $\tau$ is the identity map and $\delta$ is the zero map, we denote $R[x, \sigma]$ by $S(R)$. In case $\sigma$ and $\tau$ are the identity maps, we denote $R[x, \delta]$ by $D(R)$. Note that $\delta$ in this case is just a derivation. We denote the skew Laurent polynomial ring $R[x, x^{-1}, \sigma]$ by L(R).

For more details on Ore extensions (skew polynomial rings), we refer the reader to Chapter (1) of [8]. Notion of the quotient rings and contractions and extensions of ideals appear in Chapter (9) of [8].

The classical study of any commutative Noetherian ring is done by studying its primary decomposition. Further there are other structural properties of rings, for example the existence of quotient rings or more particularly the existence of Artinian quotient rings etc. which can be nicely tied to primary decomposition of a Noetherian ring.

The first important result in the theory of non commutative Noetherian rings was proved in 1958 (Goldie's Theorem) which gives an analog of field of fractions for factor rings R/P, where R is a Noetherian ring and P is a prime ideal of R. In 1959 the one sided version was proved by Goldie, Lesieur-Croisot (Theorem (5.12) of [8])and in 1960 Goldie generalized the result for semiprime rings (Theorem (5.10) of [8]).

In [5] it is shown that if R has characteristic zero and it is embeddable in a right Artinian ring, then the differential operator ring $R[x, \delta]$ embeds in a right Artinian ring, where $\delta$ is a derivation of R. It is also shown in [5] that if R is a commutative Noetherian ring and $\sigma$ is an automorphism of R, then the skew-polynomial ring $R[x, \sigma]$ embeds in an Artinian ring.

In this paper the above mentioned properties have been studied with emphasis on primary decomposition of the Ore extension E(R), where R is a commutative Noetherian $\mathbb{Q}$-algebra, where $\sigma$ and $\tau$ are automorphisms of R and $\delta$ is a $(\sigma, \tau)$-derivation of R.

A non commutative analogue of associated prime ideals of a Noetherian ring has also been also discussed. We would like to note that a considerable work has been done in the investigation of prime ideals (in particular minimal prime ideals and associated prime ideals) of skew polynomial rings (K. R. Goodearl and E. S. Letzter [9], C. Faith [6], S. Annin [1], Leroy and Matczuk [12], Nordstrom [14] and Bhat [4]).

In section (4) of [9] Goodearl and Letzter have proved that if R is a Noetherian ring, then for each prime ideal P of O(R), the prime ideals of R minimal over $P \cap R$ are contained within a single $\sigma$-orbit of Spec(R).

The author has proved in Theorem (2.4) of [4] that if $\sigma$ is an automorphism of a Noetherian ring R and K(R) is any of S(R) or L(R), then $P \in Ass(K(R))$ if and only if there exists $U \in Ass(R)$ such that $K(P \cap R) = P$ and $P \cap R = \cap_{i=0}^{m} \sigma^i(U)$, where $m \geq 1$ is an integer such that $\sigma^m(V) = V$ for all $V \in Ass(R)$. (Same result has been proved for minimal prime ideal case).

Carl Faith has proved in [6] that if R is a commutative ring, then the associated prime ideals of the usual polynomial ring R[x] (viewed as a module over itself) are precisely the ideals of the form P[x], where P is an associated prime ideal of R.

S. Annin has proved in Theorem (2.2) of [1] that if R is a ring and M be a right R-module. If $\sigma$ is an endomorphism of R and $S = R[x, \sigma]$ and $M_R$ is $\sigma$-compatible, then $Ass(M[x]_S) = \{P[x] \text{ such that } P \in Ass(M_R)\}$.

In [12], Leroy and Matczuk have investigated the relationship between the associated prime ideals of an R-module $M_R$ and that of the induced S - module $M_S$, where $S = R[x, \sigma]$ ($\sigma$ an automorphism of a ring R). They have proved the following:

**Theorem (5.7) of** [12]: Suppose $M_R$ contains enough prime submodules and let $Q \in Ass(M_S)$. If for every $P \in Ass(M_R)$, $\sigma(P) = P$, then Q = PS for some $P \in Ass(M_R)$.

In Theorem (1.2) of [14] Nordstrom has proved that if R is a ring with identity and $\sigma$ is a surjective endomorphism of R, then for any right R-module M, $Ass(M[x, \sigma]) = \{I[x, \sigma],\ I \in \sigma - Ass(M)\}$. In Corollary (1.5) of [14] it has been proved that if R is Noetherian and $\sigma$ is an automorphism of R, then $Ass(M[x, \sigma]_S) = \{P_\sigma[x, \sigma],\ P \in Ass(M)\}$, where $P_\sigma = \cap_{i \in N} \sigma^{-i}(P)$ and $S = R[x, \sigma]$.

The above discussion leads to a stronger type of primary decomposition of a Noetherian ring. We call a Noetherian ring with such a decomposition a *Transparent ring*.

Before we give the definition of a *Transparent ring*, we need the following:

**Definition 1.1.** A ring R is said to be an irreducible ring if the intersection of any two non-zero ideals of R is non-zero. An ideal I of R is called irreducible if $I = J \cap K$ implies that either $J = I$ or $K = I$. Note that if I is an irreducible ideal of R, then $R/I$ is an irreducible ring.

**Proposition 1.2.** *Let R be a Noetherian ring. Then there exist irreducible ideals* $I_j$, $1 \leq j \leq n$ *of R such that* $\cap_{j=1}^{n} I_j = 0$.

*Proof.* The proof is obvious and we leave the details to the reader. □

**Definition (A):** A Noetherian ring R is said to be a *Transparent ring* if there exist irreducible ideals $I_j$, $1 \leq j \leq n$ such that $\cap_{j=1}^{n} I_j = 0$ and each $R/I_j$ has a right Artinian quotient ring.

It can be easily seen that an integral domain is a *Transparent ring*, a commutative Noetherian ring is a *Transparent ring* and so is a Noetherian ring having an Artinian quotient ring. A fully bounded Noetherian ring is also a *Transparent ring*.

This type of decomposition was actually introduced by the author in [2]. Such a ring was called a *decomposable ring*, but in order to distinguish between one more definition of a *decomposable ring* given below and pointed out by the referee of one of the papers of the author, we now call such a ring a *Transparent ring*.

**Decomposable ring (Hazewinkel and Krichenko**[11]**)** Let R be a ring. An R-module M is said to be decomposable if $M \simeq M_1 \oplus M_2$ of non zero R-modules $M_1$ and $M_2$. A ring R is called a *decomposable ring* if it is a direct sum of two rings.

Now there arises a natural question: If R is a *Transparent ring*; $\sigma$, $\tau$ and $\delta$ are as usual. Is E(R) a *Transparent ring*? We have not been able to answer this question in general, however, in commutative case we have the following:
If R is a commutative Noetherian $\mathbb{Q}$-algebra; $\sigma$ and $\tau$ are automorphisms of R, then there exists an integer $m \geq 1$ such that the extension ring $R[x, \alpha, \beta, \vartheta]$ is decomposable, where $\alpha = \sigma^m$, $\beta = \tau^m$ and $\vartheta$ is an $(\alpha, \beta)$-derivation of R with $\alpha(\vartheta(a)) = \vartheta(\alpha(a))$, and $\beta(\vartheta(a)) = \vartheta(\beta(a))$, for all $a \in R$. This is proved in Theorem (3.12).

Before proving the main result, we recall that if R is a ring, which is an order in an Artinian ring S. If $\sigma$ and $\tau$ are automorphisms of R and $\delta$ is a $(\sigma, \tau)$-derivation of R, then $\sigma$ and $\tau$ can be extended to automorphisms $\alpha$ and $\beta$ (say) of S and $\delta$ can be extended to an $(\alpha, \beta)$-derivation (say) $\rho$ of S. This has been proved in Proposition (2.1) of [3]. In Theorem (2.11) of [3] it has been proved that that E(R) is an order in $E(S)_L$, where $E(S) = S[x, \alpha, \beta, \rho]$ and L is the set of monic polynomials of E(S).

## 2. Preliminaries

Recall that the skew power series ring $R[[t, \sigma, \tau]]$ is as a set the power series ring $R[[t]]$ in which multiplication is subject to the relation $ax = x\sigma(\tau(a))$, for all $a \in R$. Denote $R[[t, \sigma, \tau]]$ by T.

**Definition 2.1.** Let R be a ring. Let $\sigma$ and $\tau$ be automorphisms of R and $\delta$ be a $(\sigma, \tau)$-derivation of R. Then $R[x, \sigma, \tau, \delta] = \{f = \sum_{i=0}^{n} x^i a_i, a_i \in R\}$, subject to the relation $ax = x\sigma(\tau(a)) + \delta(a)$ for all $a \in R$.

*Remark* 2.2. If $\sigma(\delta(a)) = \delta(\sigma(a))$ and $\tau(\delta(a)) = \delta(\tau(a))$, for all $a \in R$, then $\sigma$ and $\tau$ can be extended to an automorphisms of E(R) such that $\sigma(x) = x$ and $\tau(x) = x$ and $\delta$ can be extended to a $(\sigma, \tau)$-derivation of E(R) such that $\delta(x) = 0$, that is $\sigma(xa) = x\sigma(a)$, $\tau(xa) = x\tau(a)$ and $\delta(xa) = x\delta(a)$.

**Lemma 2.3.** *Let R be a Noetherian $\mathbb{Q}$-algebra; $\sigma$ and $\tau$ automorphisms of R and $\delta$ a $(\sigma, \tau)$-derivation of R such that $\sigma(\delta(a)) = \delta(\sigma(a))$, and $\tau(\delta(a)) = \delta(\tau(a))$ for all $a \in R$. Then $e^{t\delta} = 1 + t\delta + (t^2/2!)\delta^2 + ...$is an automorphism of T.*

*Proof.* The proof is on the same lines as in [16] and in non-commutative case, it is similar to the sketch of the proof provided in [5]. □

*Remark* 2.4. Let R be a Noetherian ring; $\sigma$, $\tau$ and $\delta$ as usual. Let I be an ideal of R such that $\sigma(I) = I$ and $\tau(I) = I$. Then $IT = \{b_0 + tb_1 + t^2b_2 + ..., b_i \in I\}$. We denote it by $I[[t, \sigma, \tau]]$.

**Lemma 2.5.** *Let R be a Noetherian $\mathbb{Q}$-algebra; $\sigma$, $\tau$ and $\delta$ as usual such that $\sigma(\delta(a)) = \delta(\sigma(a))$ and $\tau(\delta(a)) = \delta(\tau(a))$, for $a \in R$. Then an ideal I of R is $\delta$-invariant if and only if IT is $e^{t\delta}$-invariant.*

*Proof.* Let IT be $e^{t\delta}$-invariant. Let $a \in I$. Then $a \in IT$. So $e^{t\delta}(a) \in IT$; i.e. $a + t\delta(a) + (t^2/2!)\delta^2(a) + ... \in IT$, which implies that $\delta(a) \in I$.
Conversely suppose that $\delta(I) \subseteq I$ and let $f = \sum_{j=0}^{\infty} t^j a_j \in IT$. Then $e^{t\delta}(f) =$

$f + t\delta(f) + (t^2\delta^2/2!)(f) + ... = \sum_{j=0}^{\infty} t^j a_j + t(\sum_{j=0}^{\infty} t^j \delta(a_j) + ... \in IT$, as $\delta(a_i) \in I$. Therefore $e^{t\delta}(IT) \subseteq IT$. Replacing $e^{t\delta}$ by $e^{-t\delta}$, we get that $e^{t\delta}(IT) = IT$. □

**Lemma 2.6.** *Let $R$ be a Noetherian ring; $\sigma$, $\tau$ and $\delta$ as usual such that $\sigma(\delta(a)) = \delta(\sigma(a))$ and $\tau(\delta(a)) = \delta(\tau(a))$, for $a \in R$ and $T$ be as usual. Then:*

(1) *$A \in Ass(R)$ implies that $AT \in Ass(T)$.*
(2) *$P \in Ass(T)$ implies that $P \cap R \in Ass(R)$ and $P = (P \cap R)T$.*

*Proof.* **(1)** Let A = Ann(cR) = Assas(cR), $c \in R$. Then it can be seen that $AT \in Spec(T)$ and AT = Ann(cT) = Assas(cT). Therefore $AT \in Ass(T)$

**(2)** Let $f = a_0 + ta_1 + t^2a_2 + ... \in T$ be such that P = Ann(fT) = Assas(fT). Now $a_iR(P \cap R) = 0$ for all i. Choose $a_n \neq 0$ from coefficients of f. Let $U = Ann(a_nR)$. Now $U = Ann(a_nrR) = Assas(a_nrR)$, $r \in R$ such that $a_nr \neq 0$. Now it is easy to see that $UT = Ann(a_nrRT) = Assas(a^nrRT)$. Now it can be seen that $U = P \cap R$. Therefore $P \cap R \in Ass(R)$ and $P = (P \cap R)T$. □

**Lemma 2.7.** *Let $R$ be a ring; $\sigma$, $\tau$ and $\delta$ as usual such that $\sigma(\delta(a)) = \delta(\sigma(a))$ and $\tau(\delta(a)) = \delta(\tau(a))$, for $a \in R$ and $T$ be as usual. Then:*

(1) *$A \in Min.Spec(R)$ implies that $AT \in Min.Spec(T)$*
(2) *$P \in Min.Spec(T)$ implies that $P \cap R \in Min.Spec(R)$ and $P = (P \cap R)T$.*

*Proof.* The proof follows on the same lines as in Proposition (2.5) of [4]. □

In Lemma (3.4) of [7], Gabriel proved that if R is a Noetherian $\mathbb{Q}$-algebra and $\delta$ is a derivation of R, then $\delta(P) \subseteq P$ for all $P \in Min.Spec(R)$. In Theorem (1) of [16], Seidenberg proved that if R is a commutative Noetherian $\mathbb{Q}$-algebra and $\delta$ is a derivation of R, then $\delta(P) \subseteq P$ for all $P \in Ass(R)$. We generalize these results and prove them in one go. Towards this we have the following:

**Lemma 2.8.** *Let $R$ be a Noetherian $\mathbb{Q}$-algebra; $\sigma$, $\tau$ and $\delta$ as usual such that $\sigma(\delta(a)) = \delta(\sigma(a))$ and $\tau(\delta(a)) = \delta(\tau(a))$, for $a \in R$. Then $P \in Ass(R) \cup Min.Spec(R)$ such that $\sigma(P) = P$ and $\tau(P) = P$ implies that $\delta(P) \subseteq P$.*

*Proof.* Let T be as usual. Now by Lemma (2.3) $e^{t\delta}$ is an automorphism of T. Let $P \in Ass(R) \cup MinS.pec(R)$. Then by Lemma (2.6) and Lemma (2.7) $PT \in Ass(T) \cup Min.Spec(T)$. So there exists an integer $n \geq 1$ such that $(e^{t\delta})^n(PT) = PT$; i.e. $e^{nt\delta}(PT) = PT$. But R is a $\mathbb{Q}$-algebra, therefore $e^{t\delta}(PT) = PT$, and so Lemma 2.5 implies that $\delta(P) \subseteq P$. □

**Definition 2.9.** A ring R is said to be an irreducible ring if the intersection of any two non-zero ideals of R is non-zero. An ideal I of R is called irreducible if $I = J \cap K$ implies that either J = I or K = I. Note that if I is an irreducible ideal of R, then R/I is an irreducible ring.

**Lemma 2.10.** *Let $R$ be a Noetherian ring. Then there exist irreducible ideals $I_j$, $1 \leq j \leq n$ of $R$ such that $\cap_{j=1}^{n} I_j = 0$.*

*Proof.* Suppose such ideals do not exist. Consider K = {Ideals J of R such that J is not intersection of irreducible ideals of R}. Now $K \neq \phi$ as $\{0\} \in K$. Now by Noetherian condition K has a maximal element (say T), and T is reducible. Let T = $U \cap V$, $T \subset U$ and $T \subset V$. Therefore U and V both are intersection of irreducible ideals of R by the maximality of T, which implies that T is an intersection of irreducible ideals of R, a contradiction. □

**Lemma 2.11.** *Let $R$ be a Noetherian ring having a right Artinian quotient ring. Then $R$ is a Transparent ring.*

*Proof.* Let $Q(R)$ be the right quotient ring of $R$ . Now for any ideal $J$ of $Q(R)$, the contraction $J^c$ of $J$ is an ideal of $R$ and the extension of $J^c$ is $J$; i.e. $J^{ce} = J$. For this see Proposition (9.19) of [8]. Let $I_j$, $1 \leq j \leq n$ be the ideals of $Q(R)$ such that $0 = \cap_{j=1}^{n} I_j$ where each $Q(R)/I_j$ is an irreducible ring. Also each $Q(R)/I_j$ is an Artinian ring. Let $I_j^c = K_j$. Then $R/K_j$ has right Artinian quotient ring $Q(R)/I_j$ and each $R/K_j$ is irreducible. Moreover $\cap_{j=1}^{n} K_j = 0$. Hence $R$ is a *Transparent ring.* □

**Definition 2.12.** Let P be a prime ideal of a commutative ring R. Then the symbolic power of P for a positive integer n is denoted by $P^{(n)}$ and is defined as $P^{(n)} = \{a \in R$ such that there exists some $d \in R$, $d \notin P$ such that $da \in P^n\}$. Also if I is an ideal of R, define as usual $\sqrt{I} = \{a \in R$ such that $a^n \in I$ for some $n \in \mathbb{Z}$ with $n \geq 1\}$.

**Lemma 2.13.** *Let $R$ be a commutative Noetherian ring, and $\sigma$ an automorphism of $R$. If $P$ is a prime ideal of $R$ such that $\sigma(P) = P$, then $\sigma(P^{(n)}) = P^{(n)}$ for all integers $n \geq 1$.*

*Proof.* We have $\sigma(P) = P$. Let $a \in P^{(n)}$. Then there exists some $d \in R$, $d \notin P$ such that $da \in P^n$. Therefore $\sigma(da) \in \sigma(P^n)$; i.e. $\sigma(d)\sigma(a) \in (\sigma(P))^n = P^n$. Now $\sigma(d) \notin P$ implies that $\sigma(a) \in P^{(n)}$. Therefore $\sigma(P^{(n)}) \subseteq P^{(n)}$. Hence $\sigma(P^{(n)}) = P^{(n)}$. □

**Lemma 2.14.** *Let $R$ be a commutative Noetherian ring; $\sigma$, $\tau$ and $\delta$ as usual. Let $P$ be a prime ideal of $R$ such that $\sigma(P) = P$, $\tau(P) = P$ and $\delta(P) \subseteq P$. Then $\delta(P^{(k)}) \subseteq P^{(k)}$.*

*Proof.* Let $a \in P^{(k)}$. Then there exists $d \notin P$ such that $da \in P^k$.
Let $da = p_1.p_2...p_t$, $p_i \in P$.

Now

$$\begin{aligned} \delta(da) = \sigma(p_1p_2...p_{t-1})\delta(p_t) + \sigma(p_1p_2...p_{t-2})\delta(p_{t-1})\tau(p_t)+ \\ ... + \sigma(p_1)\delta(p_2)\tau(p_3...p_t) + \delta(p_1)\tau(p_2...p_t) \in P^k \end{aligned} \tag{2.1}$$

as $\sigma(P) = P$, $\tau(P) = P$ and $\delta(P) \subseteq P$; i.e. $\sigma(d)\delta(a) + \delta(d)\tau(a) \in P^k$. Now $\tau(a) \in P^{(k)}$ by 2.13, and therefore $\sigma(d)\delta(a) \in P^{(k)}$, which implies that there exists $d_1 \notin P$ such that $d_1\sigma(d)\delta(a) \in P^k$ and since $d_1\sigma(d) \notin P$, we have $\delta(a) \in P^{(k)}$. □

## 3. Main Result

In this section we prove the main result in the form of Theorem 3.12. We begin with the following Lemma:

**Lemma 3.1.** *Let $R$ be a ring which is an order in an Artinian ring $S$; $\sigma$, $\tau$ and $\delta$ as usual. Then $\sigma$ can be extended to an automorphism (say) $\alpha$ of $S$, $\tau$ can be extended to an automorphism (say) $\beta$ of $S$ and $\delta$ can be extended to an $(\alpha, \beta)$-derivation (say) $\rho$ of $S$.*

*Proof.* Proposition (2.1) of [3]. □

We now state some definitions, Lemmas and analog of some results of [5], which lead us to the main result. The corresponding results and other details can be seen in [5].

**Definition 3.2.** Let R be a ring and U be a right Ore set in R. Let M be a right R-module. The set $T_U(M) = \{m \in M$ such that mu = 0 for some $u \in U\}$ is called the U-torsion submodule of M. M is said to be U-torsion if and only if $T_U(M) = M$ and is said to be torsion free if $T_U(M) = 0$.

**Definition 3.3.** Let R be a ring; $\sigma$, $\tau$ and $\delta$ as usual. Let $B = \{f \in E(R)$ such that f is monic$\}$.

**Lemma 3.4.** *Let R be a right Noetherian ring. Let $\sigma$, $\tau$ and $\delta$ be as usual. Let B be the set of monic polynomials of E(R). Then B is a right denominator set in E(R).*

*Proof.* On the same lines as in Proposition (7.9.3) of [13]. □

**Lemma 3.5.** *Let R be a ring. A right E(R)-module W is B-torsion if and only if every finitely generated E(R)-submodule of W is finitely generated as an R-module.*

*Proof.* Lemma (2.4) of [3]. □

**Theorem 3.6.** *Let R be a right Noetherian ring and B as usual. Then $| E(R)_B |r = | R |r$, where $E(R)_B$ denotes the usual localization of E(R) at B.*

*Proof.* On the same lines as in Theorem (7.9.4) of [13]. □

We now state the following Lemma, the proof is left to the reader.

**Lemma 3.7.** *Let R be a ring which is an order in a right Artinian ring S; $\sigma$, $\tau$ and $\delta$ as usual. Then:*

1. *Every regular element of R is regular in E(R).*
2. *Set of regular elements of R satisfies the right Ore-condition in E(R).*
3. *Any element of E(S) has the form $f(x).c^{-1}$ for some $f(x) \in E(R)$ and some c regular in R.*
4. *If $g(x) = f(x).c^{-1}$ is regular in E(S), then f(x) is regular in E(R).*
5. *Let K be the set of monic polynomials of E(S). Then every regular element of E(R) is right regular as an element of $E(S)_K$.*

**Definition 3.8.** Let R be a ring which has a right(respectively left) quotient ring Q(R). A multiplicative closed subset I of regular elements of R is said to be exhaustive if any $q \in Q(R)$ is such that $q = ra^{-1}$ (respectively $q = a^{-1}r$) for some $r \in R$ and some $a \in I$.

**Definition 3.9.** Let R be a ring. Define $M(E(R)) = \{f \in E(R)$ such that leading coefficient of f is regular in R$\}$

**Lemma 3.10.** *Let R be a semiprime Noetherian ring. Then M(E(R)) is an exhaustive set.*

*Proof.* The proof is obvious. □

**Theorem 3.11.** *Let R be a ring which is an order in a right Artinian ring S. Then E(R) is an order in a right Artinian ring and E(R) has an exhaustive set of elements which have leading coefficients regular in R.*

*Proof.* Theorem (2.11) of [3] □

We are now in a position to state and prove the main result in the form of the following Theorem:

**Theorem 3.12.** *Let $R$ be a commutative Noetherian $\mathbb{Q}$-algebra, $\sigma$ and $\tau$ be automorphisms of $R$. Then there exists an integer $m \geq 1$ such that the extension ring $R[x, \alpha, \beta, \delta]$ is a Transparent ring, where $\sigma^m = \alpha$, $\tau^m = \beta$ and $\delta$ is an $(\alpha, \beta)$-derivation of $R$ such that $\alpha(\delta(a)) = \delta(\alpha(a))$ and $\beta(\delta(a)) = \delta(\beta(a))$, for all $a \in R$.*

*Proof.* $R[x, \alpha, \beta, \delta]$ is Noetherian by Hilbert Basis Theorem, namely Theorem (1.12) of [8]. Now R is a commutative Noetherian $\mathbb{Q}$-algebra, therefore, the ideal (0) has a reduced primary decomposition. Let $I_j$, $1 \leq j \leq n$ be irreducible ideals of $R$ such that $(0) = \cap_{j=1}^{n} I_j$. For this see Theorem (4) of [17]. Let $\sqrt{I_j} = P_j$, where $P_j$ is a prime ideal belonging to $I_j$. Now by Theorem (23) of [17] there exists a positive integer k such that $P_j^{(k)} \subseteq I_j$, $1 \leq j \leq n$. Therefore we have $\cap_{j=1}^{n} P_j^{(k)} = 0$. Now $P_j \in Ass(R)$, $1 \leq j \leq n$ by first uniqueness Theorem. Since Ass(R) is finite, and $\psi^i(P) \in Ass(R)$ for any automorphism $\psi$ of R, for all $i \geq 1$, there exists an integer $m \geq 1$ such that $\sigma^m(P_j) = P_j$ and $\tau^m(P_j) = P_j$. Denote $\sigma^m$ by $\alpha$ and $\tau^m$ by $\beta$. Now $\alpha(P_j) = P_j$ and $\beta(P_j) = P_j$. Therefore $\alpha(P_j^{(k)}) = P_j^{(k)}$ and $\beta(P_j^{(k)}) = P_j^{(k)}$ by Lemma (2.13). Also $\delta(P_j) \subseteq P_j$ by Lemma 2.8 and therefore $\delta(P_j^{(k)}) \subseteq P_j^{(k)}$ by Lemma (2.14). Thus $P_j^{(k)}[x, \alpha, \beta, \delta]$ is an ideal of $R[x, \alpha, \beta, \delta]$. Now $R/P_j^{(k)}$ has no embedded primes, therefore $R/P_j^{(k)}$ has an Artinian quotient ring by Theorem (2.11) of ([15]). Now by Theorem (3.11) $R[x, \alpha, \beta, \delta]/P_j^{(k)}[x, \alpha, \beta, \delta]$ has an Artinian quotient ring. Moreover $\cap_{j=1}^{n} P_j^{(k)}[x, \alpha, \beta, \delta] = 0$, therefore Lemma (2.11) implies that $R[x, \alpha, \beta, \delta]$ is a *Transparent ring.* □

*Remark* 3.13.
(1) Let R be a Noetherian ring having an Artinian quotient ring. Let $\sigma$ be an automorphism of R and $\delta$ be a $\sigma$-derivation of R. Then $R[x, \sigma, \delta]$ is a *Transparent ring.*
(2) Let R be a commutative Noetherian ring and $\sigma$ be an automorphism of R. Then the skew polynomial ring $R[x, \sigma]$ is a *Transparent ring.*
(3) Let R be a commutative Noetherian ring and $\sigma$ be an automorphism of R. Then the skew Laurent polynomial ring $R[x, x^{-1}, \sigma]$ is a *Transparent ring.*
(4) Let R be a commutative Noetherian $\mathbb{Q}$-algebra and $\delta$ be a derivation of R. Then the differential operator ring D(R) = $R[x, \delta]$ is a *Transparent ring.*

**Question**: If R is a commutative Noetherian $\mathbb{Q}$-algebra, $\sigma$ is an automorphism of R and $\delta$ is a $\sigma$-derivation of R. Is $R[x, \sigma, \tau, \delta]$ a *Transparent ring* even if $\sigma(\delta(a)) = \delta(\sigma(a))$ and $\tau(\delta(a)) = \delta(\tau(a))$, for all $a \in R$? The main hurdle is that in such a situation $\delta(P) \subseteq P$ need not imply $\delta(P^{(k)}) \subseteq P^{(k)}$.

## References

[1] S. Annin, Associated primes over skew polynomial rings, Comm. Algebra, 30 (2002), 2511-2528.
[2] V. K. Bhat, Decomposability of iterated extensions, Int. J. Math. Game Theory and Algebra, 15(1) (2006), 45-48.
[3] V. K. Bhat, Ring extensions and their quotient rings, East-West J. Math., Vol. 9(1) (2007), 25-30.

[4] V. K. Bhat, Associated prime ideals of skew polynomial rings, Beitrge Algebra Geom., Vol. 49(1) (2008), 277-283.
[5] W. D. Blair, L. W. Small, Embedding differential and skew polynomial rings into artinian rings, Proc. Amer. Math. Soc., 109(4) (1990), 881-886.
[6] C. Faith, Associated primes in commutative polynomial rings, Comm. Algebra, 28 (2000), 3983-3986.
[7] P. Gabriel, Representations des algebres de Lie resolubles (d apres J.Dixmier) In Seminaire Bourbaki, pp 1-22, Springer Verlag 1968-69.
[8] K. R. Goodearl, R. B. Warfield, An introduction to Non-commutative Noetherian rings. Camb. Uni. Press, 1989.
[9] K. R. Goodearl and E. S. Letzter, Prime ideals in skew and q-skew polynomial rings, Memoirs of the Amer. Math. Soc., No. 521 (1994).
[10] R. Gordon and J. C. Robson, Krull dimension, Memoirs of the Amer. Math. Soc., No. 133, 1973.
[11] M. Hazewinkel and V. V. Krichenko, Algebras, rings and modules; Vol. 1, Mathematics and its applications, Kluwer Academic Press, 2004.
[12] A. Leroy and J. Matczuk, On induced modules over Ore extensions, Comm. Algebra, 32(7) (2004), 2743-2766.
[13] J. C. McConnell and J. C. Robson, Noncommutative Noetherian Rings, Wiley (1987); revised edition: American Math. Society (2001).
[14] H. E. Nordstorm, Associated primes over Ore extensions, J. Algebra, 286(1) (2005), 69-75.
[15] J. C. Robson, Artinian quotient rings, Proc. London Math. Soc., 3(17) (1967), 600-616.
[16] A. Seidenberg, Differential ideals in rings of finitely generated type, Amer. J. Math., 89 (1967), 22-42.
[17] O. Zariski and P. Samuel, Commutative Algebra, Vol. I, D. Van Nostrand Company, Inc. 1967.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 4, Pages 293–305
ISSN 1930-1235: (2008)

# OTHER REPRESENTATIONS OF THE RIEMANN ZETA FUNCTION AND AN ADDITIONAL REFORMULATION OF THE RIEMANN HYPOTHESIS

STEFANO BELTRAMINELLI AND DANILO MERLINI

Abstract. New expansions for some functions related to the Zeta function in terms of the Pochhammer polynomials are given (coefficients $b_k$, $d_k$ and $\hat{d}_k$). In some formal limit our expansion $b_k$ obtained via the alternating series gives the regularized expansion of Maslanka for the Zeta function. The real and the imaginary part of the function on the critical line is obtained with a good accuracy up to $\Im(s) = t < 35$.

Then, we give the expansion (coefficient $\hat{d}_k$) for the derivative of $\ln[(s-1)\zeta(s)]$. The critical function of the derivative, whose bounded values for $\Re(s) > \frac{1}{2}$ at large values of $k$ should ensure the truth of the Riemann Hypothesis (RH), is obtained either by means of the primes or by means of the zeros (trivial and non-trivial) of the Zeta function. In a numerical experiment performed up to high values of $k$ i.e. up to $k = 10^{14}$ we obtain a very good agreement between the two functions, with the emergence of fourteen oscillations with stable amplitude.

## 1. Introduction

Lately there has been new interest in the study of the expansion of the Zeta function via the Pochhammer polynomials. This is related to the original idea of Riesz [17] and of Hardy-Littlewood [13] at the beginning of the last century. In pioneering works, Maslanka obtained a regularized expansion for the Zeta function (with coefficients $A_k$) [14] and Baez-Duarte an expansion for the reciprocal of the Zeta function (with coefficients $c_k$) for the Riesz case [2, 4]. Other cases of interest have also recently been studied [1, 8, 9, 10, 15, 18]. As pointed out in [4], the discrete version by means of the Pochhammer polynomials $P_k(s)$, where $s = \sigma + it$ is the complex variable and $k$ is an integer, has advantages especially in the context of numerical experiments in connection with some "kind of verification" that supports the RH may be true.

In this work we first derive a new expansion for the Zeta function in terms of the Pochhammer polynomials via the alternating series (with new coefficients $b_k$). In some formal limit, a connection with the expansion of Maslanka is also obtained in Section 2. Our expansion is then studied numerically on the critical line where a good agreement with the real function is obtained up to $\Im(s) = t < 35$, with the

Received by the editors 10 November 2008.
1991 *Mathematics Subject Classification.* 11M26.
*Key words and phrases.* Riemann's Zeta function, Riemann Hypothesis, Criteria of Riesz, Hardy-Littlewood and Baez-Duarte, Pochhammer's polynomials.

emergence of the first few low zeros. After this value of $t$, a divergence possibly of numerical nature set on.

In Section 3 we then obtain the expansion for the function $\ln\left[(1-2^{1-s})\zeta(s)\right]$ (with new coefficients $d_k$) as well as for the derivative of $\ln\left[(s-1)\zeta(s)\right]$ (with new coefficients $\hat{d_k}$) in terms of the two parameters $\alpha$ and $\beta$, already introduced in our previous works [5, 6, 7]. The critical function for the derivative (whose boundedness at large $k$ would "ensure" the truth of the RH) is then obtained either with the primes or with the trivial and non-trivial zeros of the Zeta function.

In the numerical experiment for the special case $\alpha = \frac{9}{2}$ and $\beta = 4$ up to high values of $k$, i.e. $k = 10^{14}$, the results for the two functions are in very good agreement, both with the emergence of the same fourteen oscillations of stable amplitude of about 0.01 (Section 4).

## 2. Zeta function representation via the alternating series

In this section we derive a formula for $(1-2^{1-s})\zeta(s)$ similar to the one of Maslanka for $(s-1)\zeta(s)$ [14] and of Baez-Duarte for $[\zeta(s)]^{-1}$ [2, 4].

Here the starting series is convergent for $\Re(s) = \sigma > 0$ and the formula is obtained still in terms of the so called Pochhammer polynomials of degree $k$, in the complex variable $s = \sigma + it$.

$$P_k(s) = \prod_{r=1}^{k}\left(1-\frac{s}{r}\right) \qquad \forall k \in \mathbb{N}^* \quad \text{and} \quad P_0(s) = 1 \tag{2.1}$$

We will also use a family of functions with two parameters ($\alpha$ and $\beta$) as considered already in our recent works [5, 6, 7]. Since the alternating series is given by:

$$\left(1-2^{1-s}\right)\zeta(s) = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s} \qquad \forall \Re(s) = \sigma > 0 \tag{2.2}$$

we have using the trick as in [2] that:

$$\begin{aligned}\left(1-2^{1-s}\right)\zeta(s) &= \sum_{n=1}^{\infty}\tfrac{(-1)^{n-1}}{n^\alpha}\left(1-\left(1-\tfrac{1}{n^\beta}\right)\right)^{\frac{s-\alpha}{\beta}} \\ &= \sum_{n=1}^{\infty}\tfrac{(-1)^{n-1}}{n^\alpha}\sum_{k=0}^{\infty}(-1)^k\left(1-\tfrac{1}{n^\beta}\right)^k\binom{\frac{s-\alpha}{\beta}}{k}\end{aligned}$$

Since

$$\begin{aligned}(-1)^k\binom{\frac{s-\alpha}{\beta}}{k} &= \tfrac{(-1)^k}{k!}\left(\tfrac{s-\alpha}{\beta}+1-1\right)\cdots\left(\tfrac{s-\alpha}{\beta}+1-k\right) \\ &= \prod_{r=1}^{k}\left(1-\tfrac{\frac{s-\alpha}{\beta}+1}{r}\right) = P_k(\tfrac{s-\alpha}{\beta}+1)\end{aligned}$$

we obtain:

$$\begin{aligned}\left(1-2^{1-s}\right)\zeta(s) &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{n=1}^{\infty}\tfrac{(-1)^{n-1}}{n^\alpha}\left(1-\tfrac{1}{n^\beta}\right)^k \\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\binom{k}{j}\sum_{n=1}^{\infty}\tfrac{(-1)^{n-1}}{n^{\alpha+\beta j}}\end{aligned} \tag{2.3}$$

Since from (2.2)

$$\left(1-2^{1-(\alpha+\beta j)}\right)\zeta(\alpha+\beta j) = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^{\alpha+\beta j}}$$

substitution in (2.3) gives:

(2.4)

$$\left(1-2^{1-s}\right)\zeta(s)=\sum_{k=0}^{\infty}P_k\Big(\frac{s-\alpha}{\beta}+1\Big)\sum_{j=0}^{k}(-1)^j\binom{k}{j}\left(1-2^{1-(\alpha+\beta j)}\right)\zeta(\alpha+\beta j)$$

With the definition

$$b_k:=\sum_{j=0}^{k}(-1)^j\binom{k}{j}\left(1-2^{1-(\alpha+\beta j)}\right)\zeta(\alpha+\beta j) \tag{2.5}$$

(2.4) becomes:

$$\left(1-2^{1-s}\right)\zeta(s)=\sum_{k=0}^{\infty}b_kP_k\Big(\frac{s-\alpha}{\beta}+1\Big) \tag{2.6}$$

where $P_0(\frac{s-\alpha}{\beta}+1)=1$ and $b_0=(1-2^{1-\alpha})\zeta(\alpha)$.

The series above, is expected to represent $(1-2^{1-s})\zeta(s)$ for $s$ in some compact subset of the plane as for the Maslanka case [14]. In that case, the central point has been investigated and elucidated by Baez-Duarte [3]. Here many choices of $\alpha$ and $\beta$ are possible. For $\alpha=\beta=2$ we have the Riesz case [17] and it is the analogon to the regularized version of Maslanka but the representation of the Zeta function is not the same. For $\alpha=1+\delta$ $(\delta\downarrow 0)$ and $\beta=2$ we obtain the Hardy-Littlewood case [13] which was also discussed numerically in a different way using other polynomials [12].

In fact, from Lemma 2.3 of Baez-Duarte [4] which states that at large $k$:

$$|P_k(s)|\leq Ck^{-\Re(s)} \tag{2.7}$$

where C is a constant depending on |s|, we obtain here that:

$$\left|P_k\Big(\frac{s-\alpha}{\beta}+1\Big)\right|\leq Ck^{-\left(\frac{\Re(s)-\alpha}{\beta}+1\right)}$$

We thus suspect and expect that the above series represents $(1-2^{1-s})\zeta(s)$ for all $\Re(s)>\frac{1}{2}+\delta,\delta>0$ if we assume $|b_k|\leq Dk^{-\gamma}$ with $\gamma\geq\frac{\alpha-1/2-\delta}{\beta}$ at large values of $k$ and for some constant $D$. In fact with this assumption we have that:

$$\begin{aligned}\left|\left(1-2^{1-s}\right)\zeta(s)\right| &\leq\sum_{k=0}^{\infty}\left|b_kP_k(\tfrac{s-\alpha}{\beta}+1)\right|\leq\text{const.}\sum_{k=0}^{\infty}k^{-\frac{\alpha-1/2-\delta}{\beta}}k^{-\left(\frac{\Re(s)-\alpha}{\beta}+1\right)}\\ &\leq\text{const.}\sum_{k=0}^{\infty}k^{-\left(1+\frac{\Re(s)-1/2-\delta}{\beta}\right)}<\infty\end{aligned}$$

if $\Re(s)>\frac{1}{2}+\delta$.

For $\alpha=\beta=2$ (case of Riesz) we should have $|b_k|\leq Dk^{-\frac{3}{4}+\epsilon}$. For the case $\alpha=1$ and $\beta=2$ (case of Hardy-Littlewood) we should have $|b_k|\leq Dk^{-\frac{1}{4}+\epsilon}$. Another case of interest is the one where $\alpha=\frac{3}{2}$ and $\beta=1$. In this case one should have $|b_k|\leq Dk^{-1+\epsilon}$.

Of interest also, is the limiting case of large values of $\beta$, where barely $b_k$ should behave as $|b_k|\leq D$.

For a strong argument (a Theorem) in favour of the validity of the Maslanka representation of $(s-1)\zeta(s)$ in some regions of the complex plane (compact subsets), the reader should consult the work of Baez-Duarte [3] already mentioned and it is expected that using the same methods, the proof of (2.6) may be obtained for

all $\Re(s) > \frac{1}{2}$. Here, for our series we limit ourselves to a numerical analysis just illustrating the kind of accuracy of some representations.

*Remark* 2.1. Let us consider the Riesz case $\alpha = \beta = 2$. We can write:

$$\left(1 - e^{(1-s)\ln 2}\right)\zeta(s) = \sum_{k=0}^{\infty} P_k\left(\frac{s}{2}\right) \sum_{j=0}^{k} (-1)^j \binom{k}{j} \left(1 - e^{-(1+2j)\ln 2}\right)\zeta(2+2j)$$

and using Taylor's expansion of $e^x$, we obtain:

$$(s-1)\,\zeta(s) = \sum_{k=0}^{\infty} A_k P_k\Big(\frac{s}{2}\Big) \tag{2.8}$$

where

$$A_k = \sum_{j=0}^{k} (-1)^j \binom{k}{j} (2j+1)\,\zeta(2j+2) \tag{2.9}$$

i.e. the representation obtained originally by a different method by Maslanka in a pioneering work [14]. We remark that (2.8) and (2.9) should not be considered as an approximation of our formulas (2.5) and (2.6) and vice versa. (2.5), (2.6) and (2.8), (2.9) are simply two different representations of functions related to the Riemann Zeta function, the first one given by $(s-1)\zeta(s)$, the second one by $(1-2^{1-s})\zeta(s)$.

As an example, for $s = \sigma$ with $\sigma$ in $[0, 1]$, both representations give a good description of the real function $\zeta(\sigma)$ as may easily be computationally checked. We omit here the details.

We now proceed to obtain a representation of $\zeta(s)$ possibly correct on the critical line $s = \frac{1}{2} + it$, with the help of (2.5) and (2.6), in which we are free to set $\alpha = \frac{1}{2}$ and $\beta = i$. Then:

$$\left(1 - 2^{\frac{1}{2}-it}\right)\zeta\Big(\frac{1}{2} + it\Big) = \sum_{k=0}^{\infty} b_k P_k(t+1) \tag{2.10}$$

where now

$$b_k = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \left(1 - 2^{\frac{1}{2}-ij}\right)\zeta\Big(\frac{1}{2} + ij\Big) \tag{2.11}$$

We now check the series in (2.10) restricting $k$ up to 20 for $t \leq 18$ and up to 50 for $t > 18$. We compare the result with the exact functions $\Re\left((1-2^{\overline{s}})\zeta(s)\right)$ and $\Im\left((1-2^{\overline{s}})\zeta(s)\right)$, for $s = \frac{1}{2} + it$ with $t$ up to 40. The plots are given below. The numerical results are satisfactory until $t \cong 35$. We obtain a good qualitative approximation with the emergence of the first five non-trivial zeros ($t_i$). In Table 1 we obtained the calculated $t_i$ by means of the function "FindRoot" in the software package *Mathematica*.

*Remark* 2.2. If instead of the value $\beta = i$ we set $\beta = \frac{i}{m}$ ($m$ integer), then it may be verified that (2.6) gives for $t < k$ and $t = \frac{n}{m}$ ($n$ integer) the same values as the true function $\zeta(\frac{1}{2} + it)$. For these cases more analytical as well as numerical studies are needed. Moreover as $k$ is increasing, we note the emergence of strange oscillations propagating from $t = 0$ away. We argue that numerical complexity set on at this point and we have at the moment no answer to this problem. Researchers are invited to give more elucidations and results in this direction.

TABLE 1. The first five non-trivial zeros $t_i$ calculated by means of the real part of $\sum_{k=0}^{20(50)} b_k P_k(t+1)$

| | $t_i$, see Odlyzko [16] | calculated $t_i$ |
|---|---|---|
| $t_1$ | 14.13472514173469 | 14.05988000296 |
| $t_2$ | 21.02203963877155 | 21.02212625771 |
| $t_3$ | 25.01085758014569 | 25.01083570045 |
| $t_4$ | 30.42487612585951 | 30.39283277445 |
| $t_5$ | 32.93506158773919 | 32.99863566475 |

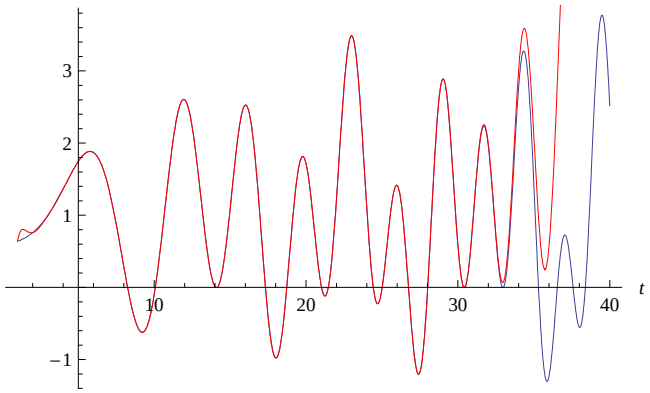



FIGURE 1. The plot of the real part of $\sum_{k=0}^{20(50)} b_k P_k(t+1)$ [red] vs. $\Re\left((1-2^{\overline{s}})\zeta(s)\right)$ [blue]

*Remark* 2.3. The right hand side of (2.10) is a polynomial in the variable $t$ with complex coefficients. It can be seen as a "characteristic polynomial" associated with some matrix whose coefficients depend on the $b(k)$ i.e. on the values of the Zeta function at integer height $j$ on the critical line. The eigenvalues of the matrix should contain a subset given by the non-trivial zeros of the Zeta function. This may be seen on Figure 1 and on Figure 2 for the first few low zeros where $t \leq 33$.

This concludes the first part of our work. Below, in the second part we develop two new representations of the functions $\ln\left[(1-2^{1-s})\zeta(s)\right]$ and $\frac{d}{ds}\ln\left[(s-1)\zeta(s)\right]$ which may possibly constitute a satisfactory approximation to the exact functions.

## 3. A representation for the logarithm of the Zeta Function and an additional criterion for the truth of the RH

We will start as before but instead of writing $\zeta(s)$ as a sum, i.e. $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, we will use the Euler product formula to derive a new representation for $\ln\left[(1-2^{1-s})\zeta(s)\right]$, which of course should be carefully investigated by means of

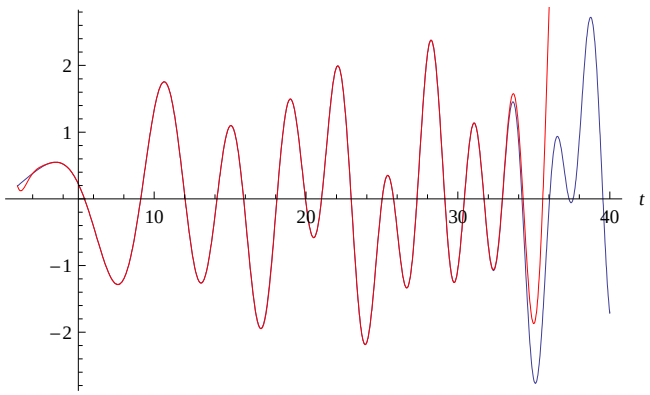



FIGURE 2. The plot of the imaginary part of $\sum_{k=0}^{20(50)} b_k P_k(t+1)$ [red] vs. $\mathfrak{I}\left((1-2^{\overline{s}})\zeta(s)\right)$ [blue]

some numerical experiments. Thus:

$$\ln\left[\left(1-2^{1-s}\right)\zeta(s)\right] = \ln\left[\left(1-2^{1-s}\right)\prod_{p\,\text{prime}}\frac{1}{1-p^{-s}}\right] \qquad \forall \Re(s)>1 \tag{3.1}$$

For any prime $p$, we have:

$$\ln\left(1-p^{-s}\right) = -\sum_{n=1}^{\infty}\frac{p^{-ns}}{n}$$

so that introducing the parameters $\alpha$ and $\beta$ as before we have that:

$$\begin{aligned}\sum_{n=1}^{\infty}\tfrac{p^{-\alpha n}}{n}\left(1-\left(1-p^{-\beta n}\right)\right)^{\frac{s-\alpha}{\beta}} &= \sum_{n=1}^{\infty}\tfrac{p^{-\alpha n}}{n}\sum_{k=0}^{\infty}(-1)^k\left(1-p^{-\beta n}\right)^k\binom{\frac{s-\alpha}{\beta}}{k}\\ &= \sum_{k=0}^{\infty}P_k\left(\tfrac{s-\alpha}{\beta}+1\right)\sum_{n=1}^{\infty}\tfrac{1}{n}\sum_{j=0}^{k}(-1)^j\binom{k}{j}p^{-(\alpha+\beta j)n}\\ &= \sum_{k=0}^{\infty}P_k\left(\tfrac{s-\alpha}{\beta}+1\right)\sum_{j=0}^{k}(-1)^j\binom{k}{j}\ln\left(1-p^{-(\alpha+\beta j)}\right)\end{aligned}$$

The same treatment for the function $\ln\left(1-2^{1-s}\right)$, gives:

$$\ln\left(1-2^{1-s}\right) = \sum_{k=0}^{\infty}P_k\left(\frac{s-\alpha}{\beta}+1\right)\sum_{j=0}^{k}(-1)^j\binom{k}{j}\ln\left(1-2^{1-(\alpha+\beta j)}\right)$$

where $P_k$ are still the Pochhammer polynomials.

Finally, the representation of $\ln\left[\left(1-2^{1-s}\right)\zeta(s)\right]$, we propose is given by:

$$\ln\left[\left(1-2^{1-s}\right)\zeta(s)\right] = \sum_{k=0}^{\infty}d_k P_k\left(\frac{s-\alpha}{\beta}+1\right) \tag{3.2}$$

where now:

$$d_k := \sum_{j=0}^{k}(-1)^j\binom{k}{j}\ln\left[\left(1-2^{1-(\alpha+\beta j)}\right)\zeta(\alpha+\beta j)\right] \tag{3.3}$$

*Remark* 3.1. Another formal derivation of the above equations is the following:

$$\ln\left[\left(1-2^{1-s}\right)\zeta(s)\right]=\ln\left[\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s}\right]$$

Supposing now that the right hand side may be given as an unknown series $\sum_{r=1}^{\infty}\frac{a_r}{r^s}$ we then have:

$$\begin{aligned}\sum_{r=1}^{\infty}\tfrac{a_r}{r^{\alpha}}\left(1-\left(1-\tfrac{1}{r^{\beta}}\right)\right)^{\frac{s-\alpha}{\beta}} &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{r=1}^{\infty}\tfrac{a_r}{r^{\alpha}}\left(1-\tfrac{1}{r^{\beta}}\right)^k\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\sum_{r=1}^{\infty}\tfrac{a_r}{r^{\alpha+\beta j}}\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\ln\Big(\sum_{n=1}^{\infty}\tfrac{(-1)^{n-1}}{n^{\alpha+\beta j}}\Big)\end{aligned}$$

which coincide with (3.2) and (3.3), obtained with the Euler product formula for $\Re(s)>1$. (3.2) with (3.3), is the new formula possibly representing the logarithm of the Zeta function in terms of the two parameters Pochhammer polynomials. To the best of our knowledge the above representation is new and it is our aim to carry out some numerical investigations in the sequel in order to support its validity also in some compact subset of the critical strip.

We now investigate the representation of the derivative of $\ln\left[(s-1)\zeta(s)\right]$:

$$\frac{d}{ds}\ln\left[(s-1)\,\zeta(s)\right]=\frac{1}{s-1}+\frac{\zeta'(s)}{\zeta(s)} \tag{3.4}$$

Then with $\zeta(s)=\prod_{p\,\text{prime}}\frac{1}{1-p^{-s}}$ we obtain ($\Re(s)>1$):

$$\begin{aligned}\tfrac{\zeta'(s)}{\zeta(s)} &= -\sum_p\tfrac{d}{ds}\ln\left(1-p^{-s}\right)=-\sum_p\tfrac{1}{1-p^{-s}}\tfrac{d}{ds}\left(1-e^{-s\ln p}\right)\\ &= -\sum_p\tfrac{p^{-s}}{1-p^{-s}}\ln p=-\sum_p\ln p\sum_{q=1}^{\infty}\tfrac{1}{p^{sq}}\end{aligned}$$

Introducing as above the Pochhammer polynomials we obtain further:

$$\begin{aligned}\tfrac{\zeta'(s)}{\zeta(s)} &= -\sum_p\ln p\sum_{q=1}^{\infty}\tfrac{1}{p^{q\alpha}}\left(1-\left(1-\tfrac{1}{p^{q\beta}}\right)\right)^{\frac{s-\alpha}{\beta}}\\ &= -\sum_p\ln p\sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\sum_{q=1}^{\infty}\tfrac{1}{p^{q(\alpha+\beta j)}}\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\sum_{q=1}^{\infty}\Big(-\sum_p\tfrac{1}{p^{q(\alpha+\beta j)}}\ln p\Big)\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\tfrac{\partial}{\partial\alpha}\Big(\sum_{q=1}^{\infty}\tfrac{1}{q}\sum_p\tfrac{1}{p^{q(\alpha+\beta j)}}\Big)\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\tfrac{\partial}{\partial\alpha}\Big(-\sum_p\ln\Big(1-\tfrac{1}{p^{\alpha+\beta j}}\Big)\Big)\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\tfrac{\partial}{\partial\alpha}\ln\Big(\prod_p\tfrac{1}{1-p^{-(\alpha+\beta j)}}\Big)\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\tfrac{\partial}{\partial\alpha}\ln\left(\zeta(\alpha+\beta j)\right)\end{aligned}$$

For $\frac{1}{s-1}$, using $\frac{1}{s-1}=\int_0^\infty e^{-\lambda(s-1)}d\lambda$ we have similarly:

$$\begin{aligned}\tfrac{1}{s-1} &= \int_0^\infty e^{\lambda}\tfrac{1}{e^{\lambda s}}d\lambda = \int_0^\infty \tfrac{e^{\lambda}}{e^{\lambda\alpha}}\big(1-\big(1-\tfrac{1}{e^{\lambda\beta}}\big)\big)^{\frac{s-\alpha}{\beta}}d\lambda\\ &= \int_0^\infty e^{\lambda}\sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\tfrac{1}{e^{\lambda(\alpha+\beta j)}}d\lambda\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\int_0^\infty e^{-\lambda(\alpha+\beta j-1)}d\lambda\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\tfrac{1}{\alpha+\beta j-1}\\ &= \sum_{k=0}^{\infty}P_k(\tfrac{s-\alpha}{\beta}+1)\sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\tfrac{\partial}{\partial\alpha}\ln(\alpha+\beta j-1)\end{aligned}$$

Thus, along these lines we obtain:

$$\frac{d}{ds}\ln\left[(s-1)\,\zeta(s)\right]=\sum_{k=0}^{\infty}\hat{d}_k P_k\Big(\frac{s-\alpha}{\beta}+1\Big) \tag{3.5}$$

where:

$$\hat{d}_k=\sum_{j=0}^{k}(-1)^j\binom{k}{j}\frac{\partial}{\partial\alpha}\ln\left[(\alpha+\beta j-1)\,\zeta(\alpha+\beta j)\right] \tag{3.6}$$

From the formula (7) in [11], where $\rho$ represents a non-trivial zero of the Zeta function, i.e.:

$$\begin{aligned}\tfrac{1}{s-1}+\tfrac{\zeta'(s)}{\zeta(s)} &= \tfrac{1}{s-1}-\tfrac{s}{s-1}+\sum_\rho\tfrac{1}{\rho}+\sum_\rho\tfrac{1}{s-\rho}-\sum_{n=1}^{\infty}\tfrac{1}{2n}+\sum_{n=1}^{\infty}\tfrac{1}{s+2n}+\tfrac{\zeta'(0)}{\zeta(0)}\\ &= \tfrac{\zeta'(0)}{\zeta(0)}-1+\sum_\rho\tfrac{1}{\rho}-\sum_{n=1}^{\infty}\tfrac{1}{2n}+\sum_\rho\tfrac{1}{s-\rho}+\sum_{n=1}^{\infty}\tfrac{1}{s+2n}\end{aligned}$$

Setting $C=\frac{\zeta'(0)}{\zeta(0)}-1$, this equation applied to $s=\alpha+\beta j$ in (3.6) gives:

$$\begin{aligned}\hat{d}_k &= \sum_{j=0}^{k}(-1)^j\tbinom{k}{j}\Big(C+\int_0^\infty\Big(\sum_\rho e^{-\lambda(\alpha+\beta j-\rho)}+e^{-\lambda\rho}\\ &\quad+\sum_{n=1}^{\infty}e^{-\lambda(\alpha+\beta j+2n)}-e^{-\lambda 2n}\Big)d\lambda\Big)\\ &= \int_0^\infty\sum_\rho\Big(e^{-\lambda(\alpha-\rho)}\big(1-\tfrac{1}{e^{\lambda\beta}}\big)^k+e^{-\lambda\rho}\big(1-\tfrac{1}{e^{\lambda\beta}}\big)^k\delta_{k,0}\Big)\,d\lambda\\ &\quad+\int_0^\infty\Big(\sum_{n=1}^{\infty}e^{-\lambda(\alpha+2n)}\big(1-\tfrac{1}{e^{\lambda\beta}}\big)^k-e^{-\lambda 2n}\big(1-\tfrac{1}{e^{\lambda\beta}}\big)^k\delta_{k,0}\Big)d\lambda\end{aligned}$$

We consider only $k>0$. Now we make the variable change $e^{-\lambda\beta}=x$ and finally we obtain:

$$\begin{aligned}\hat{d}_k &= \tfrac{1}{\beta}\Big(\int_0^1(1-x)^{k+1-1}\sum_\rho x^{\frac{\alpha-\rho}{\beta}-1}dx+\int_0^1(1-x)^{k+1-1}\sum_{n=1}^{\infty}x^{\frac{\alpha+2n}{\beta}-1}dx\Big)\\ &= \tfrac{1}{\beta}\Big(\sum_\rho B(\tfrac{\alpha-\rho}{\beta},k+1)+\sum_{n=1}^{\infty}B(\tfrac{\alpha+2n}{\beta},k+1)\Big)\end{aligned}$$

where $B(x,y)=\frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$ is the Beta function. Thus for large $k$ we can write:

$$\hat{d}_k=\frac{1}{\beta}\sum_\rho\Gamma\Big(\frac{\alpha-\rho}{\beta}\Big)k^{-\frac{\alpha-\rho}{\beta}}+\frac{1}{\beta}\sum_{n=1}^{\infty}\Gamma\Big(\frac{\alpha+2n}{\beta}\Big)k^{-\frac{\alpha+2n}{\beta}} \tag{3.7}$$

For the critical function (see the definition in [7] corresponding to $\Re(s)=\sigma$ we have an analogous expression to the Baez-Duarte formula for the $c_k$ appearing in the expansion of $\zeta(s)^{-1}$ [2, 4]:

$$k^{\frac{\alpha-\sigma}{\beta}}\hat{d}_k=\frac{1}{\beta}\sum_{\rho}\Gamma\Big(\frac{\alpha-\rho}{\beta}\Big)k^{\frac{\rho-\sigma}{\beta}}+\frac{1}{\beta}\sum_{n=1}^{\infty}\Gamma\Big(\frac{\alpha+2n}{\beta}\Big)k^{-\frac{2n+\sigma}{\beta}}=:\psi_1(k) \tag{3.8}$$

On the other hand we can express $\hat{d}_k$ and then the critical function with a second formula:

$$\hat{d}_k=\frac{1}{\beta}\Gamma\Big(\frac{\alpha-1}{\beta}\Big)k^{-\frac{\alpha-1}{\beta}}-\sum_{p\,\text{prime}}\ln p\sum_{q=1}^{\infty}\frac{1}{p^{\alpha q}}\Big(1-\frac{1}{p^{\beta q}}\Big)^k \tag{3.9}$$

$$k^{\frac{\alpha-\sigma}{\beta}}\hat{d}_k=\frac{1}{\beta}\Gamma\Big(\frac{\alpha-1}{\beta}\Big)k^{\frac{1-\sigma}{\beta}}-k^{\frac{\alpha-\sigma}{\beta}}\sum_{p\,\text{prime}}\ln p\sum_{q=1}^{\infty}\frac{1}{p^{\alpha q}}\Big(1-\frac{1}{p^{\beta q}}\Big)^k=:\psi_2(k) \tag{3.10}$$

In fact (see above) the Pochhammer expansion for $\frac{1}{s-1}$ is:

$$\frac{1}{s-1}=\sum_{k=0}^{\infty}s_kP_k\Big(\frac{s-\alpha}{\beta}+1\Big)$$

where

$$s_k=\int_0^{\infty}e^{-\lambda(\alpha-1)}\big(1-e^{-\lambda\beta}\big)^k d\lambda$$

which for large $k$ behaves as $\frac{1}{\beta}\Gamma(\frac{\alpha-1}{\beta})k^{-\frac{\alpha-1}{\beta}}$. Indeed with the substitution $e^{-\lambda\beta}=x$ we obtain:

$$s_k=\frac{1}{\beta}\int_0^1 x^{\frac{\alpha-1}{\beta}-1}(1-x)^k dx=\frac{1}{\beta}\int_0^1 x^{\frac{\alpha-1}{\beta}-1}(1-x)^{k+1-1}dx=\frac{1}{\beta}B\Big(\frac{\alpha-1}{\beta},k+1\Big)$$

It is interesting to note that one can express the critical function in terms of the zeros of the Zeta function (3.8) or in terms of the primes (3.10). We will investigate numerically these two functions for the case $\alpha=\frac{9}{2}$, $\beta=4$, $\sigma=\frac{1}{2}$, although we derived (3.8) only for $\sigma>1$.

## 4. Numerical experiments

As a test of the goodness of (3.2) we draw in Figure 3 the plots of the function $\ln\big[(1-2^{1-\sigma})\zeta(\sigma)\big]$ and of its polynomial representation in the interval $\sigma\in[-1,1[$. Figure 3 shows a good match between them also in the "critical real interval" $[0,1]$. We set $\alpha=2,\beta=2$ and $k=50$.

In the next two figures we present the results of the numerical experiment performed on our representation (3.5) for the case $\alpha=\frac{9}{2}$ and $\beta=4$. Using formulae (3.8) and (3.10), we calculated the critical functions $\psi_1$ and $\psi_2$ for $\Re(z)=\sigma=\frac{1}{2}$. In our calculations we considered only the first 10 non-trivial zeros of the Zeta function, the first 20 trivial ones and the first 5'000 primes. For comparison's purpose we also did the calculations with 2'000 primes. Furthermore using the usual

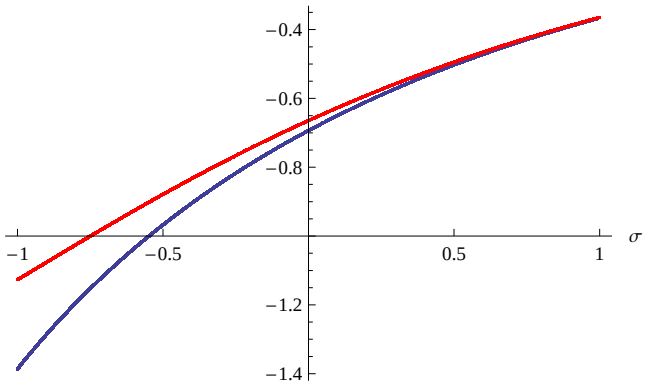



FIGURE 3. The function $\ln\left[(1-2^{1-\sigma})\zeta(\sigma)\right]$ [blue] and its polynomial representation [red]

substitution $x = \log k$, $\psi_1$ and $\psi_2$ become:

$$\psi_1(x) = \frac{\sum_{j=1}^{10} \Gamma\left(1-\frac{it_j}{4}\right)e^{\frac{xit_j}{4}} + \sum_{j=1}^{10} \Gamma\left(1+\frac{it_j}{4}\right)e^{-\frac{xit_j}{4}} + \sum_{n=1}^{20} \Gamma\left(\frac{1}{2}n+\frac{9}{8}\right)e^{-x\left(\frac{1}{2}n+\frac{1}{8}\right)}}{4}$$

$$\psi_2(x) = \frac{1}{4}\Gamma\left(\frac{7}{8}\right)e^{\frac{x}{8}} - e^x \sum_{\substack{5000 \\ \text{primes}}} \ln p \sum_{q=1}^{50} p^{-\frac{9}{2}q} e^{-\frac{e^x}{p^{4q}}}$$

where $t_j$ is the imaginary part of the *j-th* non-trivial zero.

We argue $\psi_2$ should approach $\psi_1$. The convergence is surprising. The computations presented in Figure 4 and Figure 5 indicate that the qualitative and quantitative agreement between the two functions is very good in the range $2.5 \leq x \leq 33$ ($15 \leq k \leq 2.14644 \times 10^{14}$).

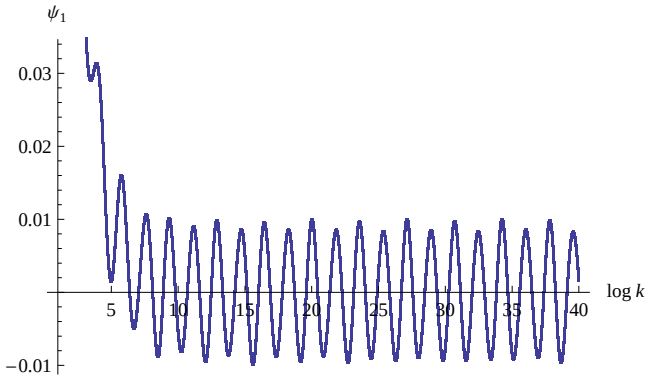



FIGURE 4. The critical function calculated with the zeros of the Zeta function ($\psi_1$), using the first 10 non-trivial zeros and the first 20 trivial ones

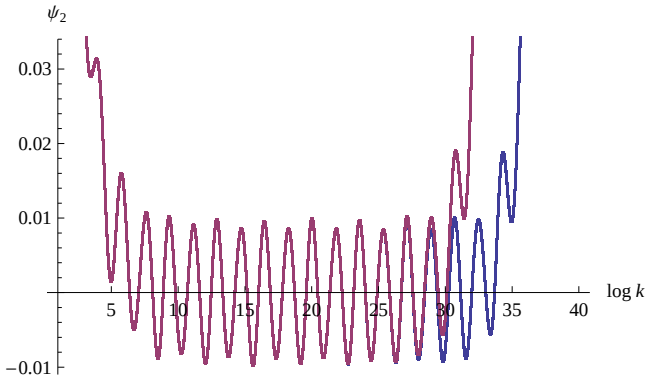



FIGURE 5. The critical function calculated with the primes ($\psi_2$): 2000 primes [red] and 5000 primes [blue]

*Remark* 4.1. We observe that as the number of primes increases from 2'000 to 5'000 $\psi_2$ becomes identical to $\psi_1$ for greater values of $k$. So we suspect that as the number of primes increases, $\psi_1$ and $\psi_2$ would coincide for larger and larger values of $k$. So there is some evidence that the two functions represent the same mathematical object. This fact, which to the best of our knowledge is new, should deserve further studies.

It is interesting to study the single contribution of a prime to the critical function $\psi_2$. In Figure 6 we computed the contributions of the 10th prime ($p = 29$), of the 50th prime ($p = 229$) and of the 100th prime ($p = 541$), all the calculations were performed until $q = 100$. The computations indicate that not only the contributions decrease with increasing $p$ but also that large primes give in fact a contribution only at large values of $k$.

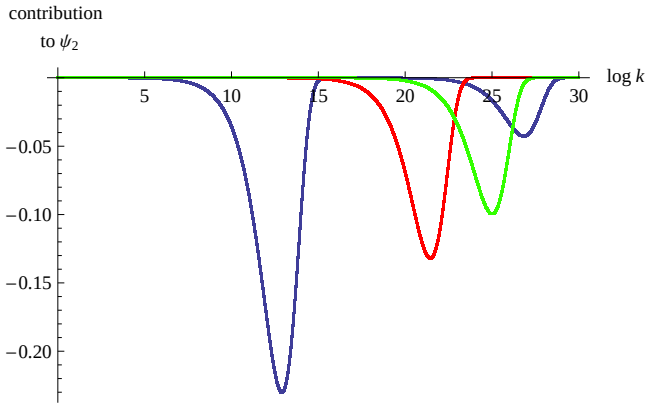



FIGURE 6. The contribution to the critical function $\psi_2$ of the primes $p = 29$ [blue], $p = 229$ [red] and $p = 541$ [green]

*Remark* 4.2. A "verification" for the truth of the RH using the representation of the function (3.4) by means of the Pochhammer polynomials may be given as follows.

Assume that $\hat{d}_k$ (either with the primes or with the zeros of the Zeta function) decays as $\hat{d}_k < \frac{D}{k^\gamma}$ with $\gamma = \frac{\alpha-1/2}{\beta}$ and some constant $D$; in fact this assumption is equivalent to the RH (see [4] and [6]). Then we have:

$$\left|\frac{d}{ds}\ln\left[(s-1)\,\zeta(s)\right]\right| < \left|\sum_{k=1}^{\infty} C\frac{1}{k^{\frac{\sigma-\alpha}{\beta}+1}}\frac{1}{k^{\frac{\alpha-1/2}{\beta}}}\right| < C\zeta\Big(1+\frac{\sigma-1/2}{\beta}\Big) \tag{4.1}$$

So the function would be bounded for $\sigma > \frac{1}{2}$ and there would be no zero with real part greater then $\frac{1}{2}$. In the same way the critical function $\psi$ should behaves like:

$$\psi(\sigma) = k^{\frac{\alpha-\sigma}{\beta}}\,d_k < \frac{D}{k^{\frac{\sigma-1/2}{\beta}}}$$

For $\sigma = \frac{1}{2}$ we have no criteria but it seems (Figure 4) that the critical function $\psi(\frac{1}{2})$ is also bounded. We verified numerically the bound given by (4.1) at $\sigma = 0.6, 0.55, 0.525$ where we found that $D$ is about 9.5.

*Remark* 4.3. Now, suppose that $\psi(\sigma')$ is bounded for some $\sigma' > \frac{1}{2}$, then since

$$\psi(\sigma) = \psi(\sigma')k^{\frac{\sigma'-\sigma}{\beta}}$$

this would indicate that if there is no zero at $\sigma'$ then there is also no zero at $\sigma$. Thus it would be important to study $\psi$ for example in the region $\sigma > 1$ where it is known that there are no zeros and where the primes ($\psi_2$) as well as the zeros ($\psi_1$) can be used.

## 5. Conclusions

In this work we have found some new representations of functions related to the Riemann Zeta function in terms of the Pochhammer polynomials, i.e. for the Zeta function via the alternating series, for $(1-2^{1-s})\zeta(s)$, for $\ln\left[(1-2^{1-s})\zeta(s)\right]$ and for the derivative of $\ln\left[(s-1)\zeta(s)\right]$.

(1) A numerical experiment for the first function give satisfactory results both for the real part as well for the imaginary part even on the critical line $\Re(s) = \frac{1}{2}$ (we have used the values $\alpha = \frac{1}{2}$, $\beta = i$ and $t$ up to $t = \Im(s) < 35$).
(2) In a formal limit of our representation (2.6) for the special case $\alpha = \beta = 2$ we obtain Maslanka's representation of $(s-1)\zeta(s)$.
(3) For the expansion of the derivative of the function $\ln\left[(s-1)\zeta(s)\right]$ in terms of the Pochhammer polynomials $P_k(s)$ we have found two expressions ($\psi_1$ and $\psi_2$) for the so called critical function: $\psi_1$ in terms of the trivial as well as the non-trivial zeros and $\psi_2$ in terms of the primes. We have then carried out a numerical experiment which gives a very satisfactory agreements between the two functions, which up to very high values of $k$ remain bounded. The existence of absolute upper bounds for the critical functions at $k$-infinity may be considered as being equivalent to the truth of the RH.
(4) The "equality" of $\psi_1$ and $\psi_2$ in the numerical context is intriguing because we have found a mathematical object related to the Zeta function and representable by means of the infinity of the zeros of Zeta as well as the infinity of the primes.

## References


[1] S. Albeverio and C. Cebulla, Müntz formula and zero free regions for the Riemann Zeta function, Bull. Sci. Math. **131** (2007), 12–38.

[2] L. Baez-Duarte (2003). A new necessary and sufficient condition for the Riemann Hypothesis. arXiv:math.NT/0307215

[3] L. Baez-Duarte (2003). On Maslanka's representation for the Riemann zeta function. arXiv:math.NT/0307214v1

[4] L. Baez-Duarte, A sequential Riesz-like criterion for the Riemann Hypothesis, International Journal of Mathematical Sciences **2005** (2005), 3527–3537.

[5] S. Beltraminelli and D. Merlini (2006). A special case of the Riesz and Hardy-Littlewood wave and a numerical treatment of the Baez-Duarte coefficients up to some billions in the k-variable. arXiv:math.NT/0609480v1

[6] S. Beltraminelli and D. Merlini, The criteria of Riesz, Hardy-Littlewood et al. for the Riemann Hypothesis revisited using similar functions, Alb. Jour. Math. **1** (2007), 17–30.

[7] S. Beltraminelli and D. Merlini, A numerical treatment of the Riesz and Hardy-Littlewood wave, Alb. Jour. Math. **2** (2008), 61–79.

[8] J. Cislo and M. Wolf (2006). Equivalence of Riesz and Baez-Duarte criterion for the Riemann Hypothesis. arXiv:math.NT/0607782

[9] J. Cislo and M. Wolf (2008). On the Riesz and Baez-Duarte criteria for the Riemann Hypothesis. arXiv:math.NT/0807.2971v1

[10] M. Coffey (2006). On the coefficients of the Baez-Duarte criterion for the Riemann Hypothesis and their extensions. arXiv:math-ph/0608050

[11] M. H. Edwards, *Riemann's zeta function*, Dover Publications, 2001.

[12] M. D'Errico, Talk presented at the International Workshop on Complex Systems (Cerfim-Issi) held in Locarno (Switzerland), 16-18 September 2004 (unpublished)

[13] H. G. Hardy and E. J. Littlewood, Contributions to the theory of the Riemann zeta-function and the theory of the distribution of primes, Acta Math. **41** (1918), 119–196.

[14] K. Maslanka (1997). Hypergeometric-like representation of the Zeta-function of Riemann. arXiv:math-ph/0105007v1

[15] K. Maslanka (2006). Baez-Duarte criterion for the Riemann Hypothesis and Rice's integrals. arXiv:math.NT/0603713

[16] A. Odlyzko, Tables of zeros of the Riemann zeta function, available at http://www.dtc.umn.edu/~odlyzko/zeta_tables/

[17] M. Riesz, Sur l'hypothèse de Riemann, Acta Math. **40** (1916), 185–190.

[18] M. Wolf (2006). Evidence in favor of the Baez-Duarte criterion for the Riemann Hypothesis. arXiv:math.NT/0605485



S. Beltraminelli, CERFIM, Research Center for Mathematics and Physics, PO Box 1132, 6600 Locarno, Switzerland

*E-mail address*: stefano.beltraminelli@ti.ch

D. Merlini, CERFIM, Research Center for Mathematics and Physics, PO Box 1132, 6600 Locarno, Switzerland

*E-mail address*: merlini@cerfim.ch

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 2, Number 4, Pages 307–318
ISSN 1930-1235: (2008)

# DEGREE 4 COVERINGS OF ELLIPTIC CURVES BY GENUS 2 CURVES

T. Shaska, G.S. Wijesiri

*Department of Mathematics*
*Oakland University*
*Rochester, MI, 48309-4485.*

S. Wolf

*Department of Mathematics*
*Cornell University*
*Ithaca, NY 14853-4201.*

L. Woodland

*Department of Mathematics & Computer Science*
*Westminster College*
*501 Westminster Avenue*
*Fulton MO 65251-1299.*

Abstract. Genus two curves covering elliptic curves have been the object of study of many articles. For a fixed degree $n$ the subloci of the moduli space $\mathcal{M}_2$ of curves having a degree $n$ elliptic subcover has been computed for $n = 3, 5$ and discussed in detail for $n$ odd; see [17, 22, 3, 4]. When the degree of the cover is even the case in general has been treated in [16]. In this paper we compute the sublocus of $\mathcal{M}_2$ of curves having a degree 4 elliptic subcover.

## 1. Introduction

Let $\psi : C \to E$ be a degree $n$ covering of an elliptic curve $E$ by a genus two curve $C$. Let $\pi_C : C \longrightarrow \mathbb{P}^1$ and $\pi_E : E \longrightarrow \mathbb{P}^1$ be the natural degree 2 projections. There is $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ such that the diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & \mathbb{P}^1 \\ \psi \downarrow & & \downarrow \phi \\ E & \xrightarrow{\pi_E} & \mathbb{P}^1 \end{array} \tag{1}$$

The ramification of induced coverings $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ can be determined in detail; see [16] for details. Let $\sigma$ denote the fixed ramification of $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. The Hurwitz space of such covers is denoted by $\mathcal{H}(\sigma)$. For each covering $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ (up to equivalence) there is a unique genus two curve $C$ (up to isomorphism). Hence, we

have a map

$$\begin{aligned} \Phi :\ \mathcal{H}(\sigma) &\to \mathcal{M}_2 \\ [\phi] &\to [C]. \end{aligned} \tag{2}$$

We denote by $\mathcal{L}_n(\sigma)$ the image of $\mathcal{H}(\sigma)$ under this map. The main goal of this paper is to study $\mathcal{L}_4(\sigma)$.

## 2. Preliminaries

Most of the material of this section can be found in [23]. Let $C$ and $E$ be curves of genus 2 and 1, respectively. Both are smooth, projective curves defined over $k$, $char(k) = 0$. Let $\psi : C \longrightarrow E$ be a covering of degree $n$. From the Riemann-Hurwitz formula, $\sum_{P\in C} (e_\psi (P) - 1) = 2$ where $e_\psi(P)$ is the ramification index of points $P \in C$, under $\psi$. Thus, we have two points of ramification index 2 or one point of ramification index 3. The two points of ramification index 2 can be in the same fiber or in different fibers. Therefore, we have the following cases of the covering $\psi$:

**Case I:** There are $P_1$, $P_2 \in C$, such that $e_\psi(P_1) = e_\psi(P_2) = 2$, $\psi(P_1) \neq \psi(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_\psi(P) = 1$.
**Case II:** There are $P_1$, $P_2 \in C$, such that $e_\psi(P_1) = e_\psi(P_2) = 2$, $\psi(P_1) = \psi(P_2)$, and $\forall P \in C \setminus \{P_1, P_2\}$, $e_\psi(P) = 1$.
**Case III:** There is $P_1 \in C$ such that $e_\psi(P_1) = 3$, and $\forall P \in C \setminus \{P_1\}$, $e_\psi(P) = 1$.

In case I (resp. II, III) the cover $\psi$ has 2 (resp. 1) branch points in E.

Denote the hyperelliptic involution of $C$ by $w$. We choose $\mathcal{O}$ in E such that $w$ restricted to$E$ is the hyperelliptic involution on $E$. We denote the restriction of $w$ on $E$ by $v$, $v(P) = -P$. Thus, $\psi \circ w = v \circ \psi$. E[2] denotes the group of 2-torsion points of the elliptic curve E, which are the points fixed by $v$. The proof of the following two lemmas is straightforward and will be omitted.

**Lemma 1.** *a) If $Q \in E$, then $\forall P \in \psi^{-1}(Q)$, $w(P) \in \psi^{-1}(-Q)$.*
*b) For all $P \in C$, $e_\psi(P) = e_\psi(w(P))$.*

Let $W$ be the set of points in C fixed by $w$. Every curve of genus 2 is given, up to isomorphism, by a binary sextic, so there are 6 points fixed by the hyperelliptic involution $w$, namely the Weierstrass points of $C$. The following lemma determines the distribution of the Weierstrass points in fibers of 2-torsion points.

**Lemma 2.** *The following hold:*

1. *$\psi(W) \subset E[2]$*
2. *If $n$ is an even number then for all $Q \in E[2]$, $\#(\psi^{-1}(Q) \cap W) = 0 \mod (2)$*

Let $\pi_C : C \longrightarrow \mathbb{P}^1$ and $\pi_E : E \longrightarrow \mathbb{P}^1$ be the natural degree 2 projections. The hyperelliptic involution permutes the points in the fibers of $\pi_C$ and $\pi_E$. The ramified points of $\pi_C$, $\pi_E$ are respectively points in $W$ and $E[2]$ and their ramification index is 2. There is $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ such that the diagram commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi_C} & \mathbb{P}^1 \\ \psi \downarrow & & \downarrow \phi \\ E & \xrightarrow{\pi_E} & \mathbb{P}^1 \end{array} \tag{3}$$

Next, we will determine the ramification of induced coverings $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. First we fix some notation. For a given branch point we will denote the ramification of points in its fiber as follows. Any point $P$ of ramification index $m$ is denoted by $(m)$. If there are $k$ such points then we write $(m)^k$. We omit writing symbols for unramified points, in other words $(1)^k$ will not be written. Ramification data between two branch points will be separated by commas. We denote by $\pi_E(E[2]) = \{q_1, \ldots, q_4\}$ and $\pi_C(W) = \{w_1, \ldots, w_6\}$.

Let us assume now that $deg(\psi) = n$ is an even number. Then the generic case for $\psi : C \longrightarrow E$ induce the following three cases for $\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$:

**I:** $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

**II:** $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

**III:** $\left((2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)\right)$

Each of the above cases has the following degenerations (two of the branch points collapse to one)

**I:** (1) $\left((2)^{\frac{n}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\right)$

(2) $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}\right)$

(3) $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n-4}{2}}\right)$

(4) $\left((3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}\right)$

**II:** (1) $\left((2)^{\frac{n-2}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(2) $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(3) $\left((4)(2)^{\frac{n-8}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(4) $\left((2)^{\frac{n-4}{2}}, (4)(2)^{\frac{n-6}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(5) $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n-2}{2}}, (2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}\right)$

(6) $\left((3)(2)^{\frac{n-6}{2}}, (2)^{\frac{n-2}{2}}, (4)(2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(7) $\left((2)^{\frac{n-4}{2}}, (3)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

**III:** (1) $\left((2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n}{2}}\right)$

(2) $\left((2)^{\frac{n-6}{2}}, (4)(2)^{\frac{n-4}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

(3) $\left((2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (4)(2)^{\frac{n-10}{2}}\right)$

(4) $\left((3)(2)^{\frac{n-8}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}, (2)^{\frac{n}{2}}\right)$

For details see [16].

## 3. Degree 4 case

In this section we focus on the case $\deg(\phi) = 4$. The goal is to determine all ramifications $\sigma$ and explicitly compute $\mathcal{L}_4(\sigma)$.

There is one generic case and one degenerate case in which the ramification of $\deg(\phi) = 4$ applies, as given by the above possible ramification structures:

i) $(2,2,2,2^2,2)$ (generic)
ii) $(2,2,2,4)$ (degenerate)

## 4. Computing the locus $\mathcal{L}_4$ in $\mathcal{M}_2$

4.1. **Non-degenerate case.** Let $\psi : C \longrightarrow E$ be a covering of degree 4, where $C$ is a genus 2 curve and $E$ is an elliptic curve. Let $\phi$ be the Frey-Kani covering with $deg(\phi) = 4$ such that $\phi(1) = 0$, $\phi(\infty) = \infty$, $\phi(p) = \infty$ and the roots of $f(x) = x^2 + ax + b$ be in the fiber of 0. In the following figure, bullets (resp., circles) represent places of ramification index 2 (resp., 1).

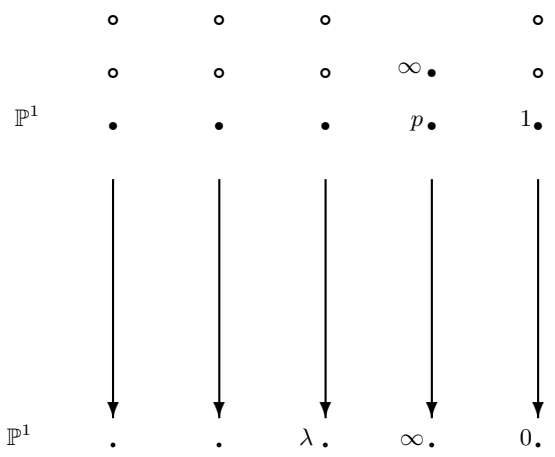



Figure 1. Degree 4 covering for generic case

Then the cover can be given by

$$\phi(x) = \frac{k(x-1)^2(x^2+b)}{(x-p)^2}.$$

Let $\lambda$ be a 2-torsion point of $E$. To find $\lambda$, we solve

$$\phi(x) - \lambda = 0. \tag{4}$$

According to this ramification we should have 3 solutions for $\lambda$, say $\lambda_1, \lambda_2, \lambda_3$. The discriminant of the Eq. (4) gives branch points for the points with ramification index 2. So we have the following relation for $\lambda$, with $p \neq 1$.

$$\begin{aligned}&\left(-b-p^2\right)\lambda^3 + \left(2\,kp^2 - 18\,kbp + 16\,kp^4 - 16\,kp^3 + 3\,kb^2 + 3\,kb + 20\,kbp^2\right)\lambda^2 \\ &+ (-3\,k^2b + 21\,k^2b^2 - 36\,k^2b^2p - 3\,k^2b^3 - 20\,k^2bp^2 + 8\,k^2b^2p^2 + 18\,k^2bp \\ &- k^2p^2)\lambda + k^3b + k^3b^4 + 3\,k^3b^2 + 3\,k^3b^3 = 0.\end{aligned} \tag{5}$$

Using Eq.(4) and Eq.(5) we find the degree 12 equation with 2 factors. One of them with degree 6 corresponds to the equation of genus 2 curve and the other corresponds to the double roots in the fiber of $\lambda_1$, $\lambda_2$ and $\lambda_3$.

The equation of genus 2 curve can be written as follows:

$$C : y^2 = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

where

$$\begin{aligned}
a_6 &= p^2 + b \\
a_5 &= 4\,p^3 - 6\,p^2 + 4\,pb - 6\,b \\
a_4 &= -4\,p^4 - 10\,p^3 + (-5\,b + 13)\,p^2 - 8\,pb + 12\,b \\
a_3 &= 12\,p^4 + (4 + 6\,b)\,p^3 + (-12 + 12\,b)\,p^2 + \left(8\,b^2 - 6\,b\right)p - 8\,b - 8\,b^2 \\
a_2 &= (-11 - 4\,b)\,p^4 + (-20\,b + 6)\,p^3 + \left(4 + 13\,b - 12\,b^2\right)p^2 + 10\,pb + 12\,b^2 \\
a_1 &= (14\,b + 2)\,p^4 + \left(6\,b^2 - 4 + 4\,b\right)p^3 + \left(-24\,b + 6\,b^2\right)p^2 + \left(-6\,b^2 + 4\,b\right)p - 6\,b^2 \\
a_0 &= \left(-b^2 + 1 - 11\,b\right)p^4 + \left(14\,b - 2\,b^2\right)p^3 - 2\,bp^2 + 2\,b^2p + b^2.
\end{aligned}$$

Notice that we write the equation of genus 2 curve in terms of only 2 unknowns. We denote the Igusa invariants of $C$ by $J_2, J_4, J_6$, and $J_{10}$. The absolute invariants of $C$ are given in terms of these classical invariants:

$$i_1 = 144\frac{J_4}{J_2^2}, \quad i_2 = -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \quad i_3 = 486\frac{J_{10}}{J_2^5}.$$

Two genus 2 curves with $J_2 \neq 0$ are isomorphic if and only if they have the same absolute invariants. Notice that these invariants of our genus 2 curve are polynomials in $p$ and $b$. By using a computational symbolic package (as Maple) we eliminate $p$ and $b$ to determine the equation for the non-degenerate locus $\mathcal{L}_4$. The result is very long. We don't display it here.

## 5. Degenerate Case

Notice that only one degenerate case can occur when $n = 4 : (2, 2, 2, 4)$. In this case one of the Weierstrass points has ramification index 3, so the cover is totally ramified at this point.

Let the branch points be 0, 1, $\lambda$, and $\infty$, where $\infty$ corresponds to the element of index 4. Then, above the fibers of 0, 1, $\lambda$ lie two Weierstrass points. The two Weierstrass points above 0 can be written as the roots of a quadratic polynomial $x^2 + ax + b$; above 1, they are the roots of $x^2 + px + q$; and above $\lambda$, they are the roots of $x^2 + sx + t$. This gives us an equation for the genus 2 curve $C$:

$$C : y^2 = (x^2 + ax + b)(x^2 + px + q)(x^2 + sx + t).$$

The four branch points of the cover $\phi$ are the 2-torsion points $E[2]$ of the elliptic curve $E$, allowing us to write the elliptic subcover as

$$E : y^2 = x(x - 1)(x - \lambda).$$

The cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is Frey-Kani covering and is given by

$$\phi(x) = cx^2(x^2 + ax + b).$$

Using $\phi(1) = 1$, we get $c = \frac{1}{1+a+b}$. Then,

$$\phi(x) - 1 = c(x - 1)^2(x^2 + px + q).$$

This implies that $\phi'(1) = 0$, so we get $c(4 + 3a + 2b) = 0$. Since $c$ cannot be 0, we must have $4 + 3a + 2b = 0$, which implies $a = \frac{-2(b+2)}{3}$. Combining this with our equation for $c$, we get $c = \frac{3}{b-1}$.

Now, since $\phi(x) - 1 - c(x-1)^2(x^2 + px + q) = 0$, we want all of the coefficients of this polynomial to be identically 0; thus

$$p = \frac{2(1-b)}{3}, q = \frac{1-b}{3}.$$

Finally, we consider the fiber above $\lambda$. We write

$$\phi(x) - \lambda = c(x-r)^2(x^2 + sx + t).$$

Similar to above, we set the coefficients of the polynomial to 0 to get:

$$\lambda = \frac{b^3(4-b)}{16(b-1)}, \quad r = \frac{b}{2}, \quad s = \frac{b-4}{3}, \quad t = \frac{b(b-4)}{12}.$$

Hence we have $C$ and $E$ with equations:

$$\begin{aligned} C: \quad y^2 &= \left(\frac{1-b}{3} + \frac{2}{3}(1-b)x + x^2\right)\left(\frac{1}{12}(b-4)b + \frac{1}{3}(b-4)x + x^2\right) \\ &\quad \left(b - \frac{2}{3}(b+2)x + x^2\right) \\ E: \quad v^2 &= u(u-1)\left(u - \frac{b^3(4-b)}{16(b-1)}\right) \end{aligned} \tag{6}$$

where the corresponding discriminants of the right sides must be non-zero. Hence,

$$\Delta_C := b(b-4)(b-2)(b-1)(2+b) \neq 0 \tag{7}$$

$$\Delta_E := \frac{(b-4)^2(b-2)^6b^6(b+2)^2}{65536(b-1)^4} \neq 0. \tag{8}$$

From here on, we consider the additional restriction on $b$ that it does not solve $J_2 = 0$, that is,

$$J_2 = -\frac{5}{486}(256 - 384b - 4908b^2 + 5068b^3 - 1227b^4 - 24b^5 + 4b^6) \neq 0. \tag{9}$$

The case when $J_2 = 0$ is considered separately. We can eliminate $b$ from this system of equations by taking the numerators of $i_j - i_j(b)$ and setting them equal to 0, where $i_j$ are absolute invariants of genus 2 curve.

Thus, we have 3 polynomials in $b, i_1, i_2, i_3$. We eliminate $b$ using the method of resultants and get the following:

$$\begin{aligned} &3652054494822999 - 312800728170302145i_1 - 247728254774362875i_1^2 \\ &+3039113062253125i_1^3 - 522534367747902600i_2 - 28017734537115000i_1i_2 \\ &-238234372300000i_2^2 = 0 \end{aligned} \tag{10}$$

and the other equation

$$\begin{aligned} &1158391804615233525i_1 - 17653298856896250i_1^2 + 100894442906250i_1^3 \\ &-256292578125i_1^4 + 244140625i_1^5 - 32389016798910273266880000i_3 \\ &-14879672225288904960000000i_1i_3 - 406094311022580000000000i_1^2i_3 \\ &-16677181699666569 + 3474053619183583968614400000000000i_3^2 = 0 \end{aligned} \tag{11}$$

These equations determine the degenerate locus $\mathcal{L}_4'$ when $J_2 \neq 0$.

When $J_2 = 0$, we must resort to the $a$-invariants of the genus 2 curve. These invariants are defined as

$$a_1 = \frac{J_4 J_6}{J_{10}}, \qquad a_2 = \frac{J_{10} J_6}{J_4^4}.$$

Two genus 2 curves with $J_2 = 0$ are isomorphic iff their $a$-invariants are equal. For our genus 2 curve,

$$J_4 = \frac{1}{5184}\left(65536 - 196608b - 307200b^2 + 1218560b^3 - 834288b^4 - 294432b^5 \right.$$
$$\left. +456600b^6 - 73608b^7 - 52143b^8 + 19040b^9 - 1200b^{10} - 192b^{11} + 16b^{12}\right)$$

It can be guarantee that $J_4$ and $J_2$ are not simultaneously 0 because the resultant of these two polynomials in $b$ is

$$\frac{11784978051522395707646672896000000000000}{42391158275216203514294433201},$$

so there are no more subcases. We want to eliminate $b$ from the set of equations:

$$\begin{aligned} J_2 &= 0 \\ a_1 - a_1(b) &= 0 \\ a_2 - a_2(b) &= 0. \end{aligned}$$

Similar to what we did above with the $i$-invariants, we take resultants of combinations of these and set them equal to 0. Doing so tells us

$$20a_1 - 55476394831 = 0$$
$$1022825924657928a_2 - 522665 = 0.$$

So in other words, if $C$ is a genus 2 curve with a degree 4 elliptic subcover with $J_2 = 0$, then

$$a_1 = \frac{55476394831}{20}, \quad a_2 = \frac{522665}{1022825924657928}.$$

So up to isomorphism, this is the only genus 2 curve with degree 4 elliptic subcover with $J_2 = 0$. In this case the equation of the genus 2 curve is given by Eq.(6), where $b$ is given by the following:

$$b = \frac{2\alpha + \sqrt{429\alpha^2 + 60123\alpha + \beta}}{2\alpha} \tag{12}$$

with $\alpha = \sqrt[3]{2837051 + 9408\, i\sqrt{5}}$ and $\beta = 8511153 + 28224\, i\sqrt{5}$. We summarize the above results in the following theorem.

**Theorem 1.** *Let $C$ be a genus 2 curve with a degree 4 degenerate elliptic subcover. Then $C$ is isomorphic to the curve given by Eq.*(6) *where $b$ satisfies Eq.*(12) *or its absolute invariants satisfy Eq.* (10) *and Eq.* (11).

**Remark 1.** *The genus 2 curve, when $J_2 = 0$, is not defined over the rational.*

**Remark 2.** *When the genus 2 curve has non zero $J_2$ invariant the $j$ invariant of the elliptic curve satisfies the following equation:*

$$\begin{aligned}0 =&(2621440000000000\,{J_4}^4 - 14332985344000000\,{J_2}^2{J_4}^3 - 15871355368243200\,{J_2}^6J_4\\ &+ 1586874322944\,{J_2}^8 + 26122821304320000\,{J_2}^4{J_4}^2)j^2 + (-2535107603331605760\,{J_2}^8\\ &+ 25102192337335536076800\,{J_2}^6J_4 - 16478102426419200000000\,{J_4}^4\\ &+ 9067580952949868544000 0\,{J_2}^4{J_4}^2 - 36316352208339763200000 0\,{J_2}^2{J_4}^3)j\\ &+ 258949145865976645040640000000 0\,{J_4}^4 - 20348236104246820967040000000 0\,{J_2}^2{J_4}^3\\ &+ 39862710766802552045625\,{J_2}^8 - 19433806326190741141800000\,{J_2}^6J_4\\ &+ 32595430043627469074160000 00\,{J_2}^4{J_4}^2.\end{aligned}$$

5.1. **Genus 2 curves with degree 4 elliptic subcovers and extra automorphisms in the degenerate locus of $\mathcal{L}_4$.** In any characteristic different from 2, the automorphism group Aut(C) is isomorphic to one of the groups : $C_2$, $C_{10}$, $V_4$, $D_8$, $D_{12}$, $C_3 \rtimes D_8$, $GF_2(3)$, or $2^+S_5$; See [21] for the description of each group. We have the following lemma.

**Lemma 3.** (a) *The locus $\mathcal{L}_2$ of genus 2 curves $C$ which have a degree 2 elliptic subcover is a closed subvariety of $\mathcal{M}_2$. The equation of $\mathcal{L}_2$ is given by*

(13)
$$\begin{aligned}0 =\ & 8748J_{10}J_2^4J_6^2 - 507384000J_{10}^2J_4^2J_2 - 19245600J_{10}^2J_4J_2^3 - 592272J_{10}J_4^4J_2^2\\ &+ 77436J_{10}J_4^3J_2^4 - 3499200J_{10}J_2J_6^3 + 4743360J_{10}J_4^3J_2J_6 - 870912J_{10}J_4^2J_2^3J_6\\ &+ 3090960J_{10}J_4J_2^2J_6^2 - 78J_2^5J_4^5 - 125971200000J_{10}^3 - 81J_2^3J_6^4 + 1332J_2^4J_4^4J_6\\ &+ 384J_4^6J_6 + 41472J_{10}J_4^5 + 159J_4^6J_2^3 - 236196J_{10}^2J_2^5 - 80J_4^7J_2 - 47952J_2J_4J_6^4\\ &+ 104976000J_{10}^2J_2^2J_6 - 1728J_4^5J_2^2J_6 + 6048J_4^4J_2J_6^2 - 9331200J_{10}J_4^2J_6^2 - J_2^7J_4^4\\ &+ 12J_2^6J_4^3J_6 + 29376J_2^2J_4^2J_6^3 - 8910J_2^3J_4^3J_6^2 - 2099520000J_{10}^2J_4J_6 + 31104J_6^5\\ &- 6912J_4^3J_6^34 - 5832J_{10}J_2^5J_4J_6 - 54J_2^5J_4^2J_6^2 + 108J_2^4J_4J_6^3 + 972J_{10}J_2^6J_4^2.\end{aligned}$$

(b) *The locus $\mathcal{M}_2(D_8)$ of genus 2 curves $C$ with $Aut(C) \equiv D_8$ is given by the equation of $\mathcal{L}_2$ and*

$$0 = 1706J_4^2J_2^2 + 2560J_4^3 + 27J_4J_2^4 - 81J_2^3J_6 - 14880J_2J_4J_6 + 28800J_6^2. \tag{14}$$

(c) *The locus $\mathcal{M}_2(D_{12})$ of genus 2 curves $C$ with $Aut(C) \equiv D_{12}$ is*

$$0 = -J_4J_2^4 + 12J_2^3J_6 - 52J_4^2J_2^2 + 80J_4^3 + 960J_2J_4J_6 - 3600J_6^2 \tag{15}$$

$$\begin{aligned}0 =\ & -864J_{10}J_2^5 + 3456000J_{10}J_4^2J_2 - 43200J_{10}J_4J_2^3 - 2332800000J_{10}^2\\ &- J_4^2J_2^6 - 768J_4^4J_2^2 + 48J_4^3J_2^4 + 4096J_4^5.\end{aligned} \tag{16}$$

We will refer to the locus of genus 2 curves C with $\mathrm{Aut}(C) \equiv D_{12}$ (resp., $\mathrm{Aut}(C) \equiv D_8$) as the $D_{12}$-locus (resp., $D_8$-locus).

Equations (10), (11), and (13) determine a system of 3 equations in the 3 $i$-invariants. The set of possible solutions to this system contains 20 rational points and 8 irrational or complex points (there may be more possible solutions, but finding them involves the difficult task of solving a degree 15 or higher polynomial).

Among the 20 rational solutions, there are four rational points which actually solve the system.

$$(i_1,i_2,i_3)=\left(\frac{102789}{12005},\frac{-73594737}{2941225},\frac{531441}{28247524900000}\right)$$
$$(i_1,i_2,i_3)=\left(\frac{66357}{9245},\frac{-892323}{46225},\frac{7776}{459401384375}\right)$$
$$(i_1,i_2,i_3)=\left(\frac{235629}{1156805},\frac{-28488591}{214008925},\frac{53747712}{80459143207503125}\right)$$
$$(i_1,i_2,i_3)=\left(\frac{1078818669}{383775605},\frac{-77466710644803}{16811290377025},\frac{1356226634181762}{161294078381836186878125}\right).$$

Of these four points, only the first one lies on the $D_{12}$-locus, and none lie on the $D_8$-locus, so the other three curves have automorphism groups isomorphic to $V_4$ (See Remark 3 for their equations). We have the following proposition.

**Proposition 1.** *There is exactly one genus 2 curve $C$ defined over $\mathbb{Q}$ (up to $\mathcal{C}$-isomorphism) with a degree 4 elliptic subcover which has an automorphism group $D_{12}$ namely the curve*

$$C=100X^6+100X^3+27$$

*and no such curves with automorphism group $D_8$.*

*Proof.* From above discussion there is exactly one rational point which lies on the $D_{12}$-locus and three rational points which lies on the $V_4$-locus. Furthermore we have the fact that $\mathrm{Aut}(C)\equiv D_{12}$ if and only if $C$ is isomorphic to the curve given by $Y^2=X^6+X^3+t$ for some $t\in k$; see [19] for more details.

Suppose the equation of the $D_{12}$ case is $Y^2=X^6+X^3+t$. We want to find $t$. We can calculate the $i$-invariants in terms of $t$ accordingly, so we get a system of equations, $i_j-i_j(t)=0$ for $j\in\{1,2,3\}$. Those equations simplify to the following:

$$\begin{aligned}0&=1600i_1t^2-80i_1t+i_1-6480t^2-1296t\\0&=64000i_2t^3-4800i_2t^2+120i_2t-i_2+233280t^3+303264t^2-11664t\\0&=1638400000i_3t^5-204800000i_3t^4+10240000i_3t^3-256000i_3t^2\\&\quad+3200i_3t-16i_3+729t^2+34992t^2-46656t^5-8748t^3.\end{aligned}$$

Replacing our i-invariants into the above system of equations we get:

$$\begin{aligned}0&=86670000\,t^2-23781600\,t+102789\\0&=-4023934200000\,t^3+1245222396000\,t^2-43137816840\,t+73594737\\0&=-82315363050000000\,t^5+61770534511500000\,t^4-15443994116835000\,t^3\\&\quad+1287019350200250\,t^2+106288200\,t-531441.\end{aligned}$$

There is only root those three polynomials share: $t=\frac{27}{100}$. Thus, there is exactly one genus 2 curve $C$ defined over $Q$ (up to $Q$-isomorphism) with a degree 4 elliptic subcover which has an automorphism group $D_{12}$

$$C:\quad y^2=100X^6+100X^3+27$$

Similarly, we show that there are no such curves with automorphism group $D_8$. □

**Remark 3.** *There are at least three genus 2 curves defined over $\mathbb{Q}$ with automorphism group $V_4$. The equations of these curves are given by the followings:*

***Case 1:*** $(i_1, i_2, i_3) = \left(\frac{66357}{9245}, \frac{-892323}{46225}, \frac{7776}{459401384375}\right)$

$$\begin{aligned} C: y^2 = {} & 1432139730944\,x^6 + 34271993769359360\,x^5 + 267643983706245216000\,x^4 \\ & + 12679191724268623131200000\,x^3 + 2394555897022488621383535000\,x^2 \\ & + 27433066616264915379359938047500 0\,x + 10256232919112043807558005130100156 25. \end{aligned}$$

***Case 2:*** $(i_1, i_2, i_3) = \left(\frac{235629}{1156805}, \frac{-28488591}{214008925}, \frac{53747712}{80459143207503125}\right)$

$$\begin{aligned} C: y^2 = {} & 418714415651589643734373217 6707502315929 6\,x^6 \\ & + 1560003589148720089080171770049158184960 00\,x^5 \\ & + 899442975326825232869917531312226304000 0000\,x^4 \\ & + 178575374038215615794800535745331200000000 00\,x^3 \\ & + 775018151562516781352226536816640000000000 0000\,x^2 \\ & + 115824938236869101167923689937600000000000 0000\,x \\ & + 267875276794685142731756552009598888458251953125. \end{aligned}$$

***Case 3:*** $(i_1, i_2, i_3) = \left(\frac{1078818669}{383775605}, \frac{-77466710644803}{16811290377025}, \frac{1356226634181762}{161294078381836186878125}\right)$

$$\begin{aligned} C: y^2 = {} & 92244081240381493089933792170848846613756532277207 04\,x^6 \\ & + 37307587676689848777251296048881523220353648264819200 00\,x^5 \\ & + 11385232838034399124038619442819980922553459130175400000 00\,x^4 \\ & + 18942504904778178462326189523859065867484120488345750000000 0\,x^3 \\ & + 76212520567614919095032412154382218443932939483817128906250000\,x^2 \\ & + 16717294192073070547056921515101088692898208834624180908203125000\,x \\ & + 27668889890454487360674443168609429569542961615592108116149902343 75. \end{aligned}$$

We summarize by the following:

**Theorem 2.** *Let $\psi : C \to E$ be a degree 4 covering of an elliptic curve by a genus 2 curve. Then the following hold:*

*i) In the generic case the equation of $C$ can be written as follows:*

$$C : y^2 = a_6x^6 + a_5x^5 + \cdots + a_1x + a_0$$

*where*

$$\begin{aligned} a_6 &= p^2 + b \\ a_5 &= 4\,p^3 - 6\,p^2 + 4\,pb - 6\,b \\ a_4 &= -4\,p^4 - 10\,p^3 + (-5\,b + 13)\,p^2 - 8\,pb + 12\,b \\ a_3 &= 12\,p^4 + (4 + 6\,b)\,p^3 + (-12 + 12\,b)\,p^2 + \left(8\,b^2 - 6\,b\right)p - 8\,b - 8\,b^2 \\ a_2 &= (-11 - 4\,b)\,p^4 + (-20\,b + 6)\,p^3 + \left(4 + 13\,b - 12\,b^2\right)p^2 + 10\,pb + 12\,b^2 \\ a_1 &= (14\,b + 2)\,p^4 + \left(6\,b^2 - 4 + 4\,b\right)p^3 + \left(-24\,b + 6\,b^2\right)p^2 + \left(-6\,b^2 + 4\,b\right)p - 6\,b^2 \\ a_0 &= \left(-b^2 + 1 - 11\,b\right)p^4 + \left(14\,b - 2\,b^2\right)p^3 - 2\,bp^2 + 2\,b^2p + b^2. \end{aligned}$$

*ii) In the degenerate case the equation of $\mathcal{L}'_4$ is given by*

$$\begin{aligned}
&1541086152812576000\,{J_2}^2{J_4}^2 - 22835312232360960000\,J_2\,J_4\,J_6 + 5009676947631\,{J_2}^6\\
&-8782271900467200000\,{J_6}^2 + 1176812184652746480\,{J_2}^4J_4 + 12448207102988800000\,{J_4}^3\\
&-3715799948429529600\,{J_2}^3J_6 = 0\\
&1866265600000000\,{J_2}^2{J_4}^4 + 13896214476734335874457600000000000\,{J_{10}}^2 + 282429536481\,{J_2}^{10}\\
&+6199238007360000\,{J_2}^6{J_4}^2 - 256000000000000\,{J_4}^5 - 2824915237592400\,{J_2}^8J_4\\
&+2665762699498787923200000\,{J_2}^5J_{10} - 5102020224000000\,{J_2}^4{J_4}^3\\
&+6930676241452032000000000\,J_2\,{J_4}^2J_{10} + 17635167081823887360000000\,{J_2}^3J_4\,J_{10} = 0
\end{aligned}$$

*iii) The intersection $\mathcal{L}'_4 \cap \mathcal{M}_2(D_8) = \emptyset$ and the intersection $\mathcal{L}'_4 \cap \mathcal{M}_2(D_{12})$ contains a single point, namely the curve*

$$C: \quad y^2 = 100X^6 + 100X^3 + 27$$

## References


[1] A. Clebsch, Theorie der Binären Algebraischen Formen, Verlag von B.G. Teubner, Leipzig, 1872.

[2] I. Duursma and N. Kiyavash, The Vector Decomposition Problem for Elliptic and Hyperelliptic Curves, (preprint)

[3] G. Frey, On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2. *Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993)*, 79-98, Ser. Number Theory, I, *Internat. Press, Cambridge, MA*, 1995.

[4] G. Frey and E. Kani, Curves of genus 2 covering elliptic curves and an arithmetic application. *Arithmetic algebraic geometry (Texel, 1989)*, 153-176, *Progr. Math.*, 89, Birkhäuser Boston, MA, 1991.

[5] P. Gaudry and E. Schost, Invariants des quotients de la Jacobienne d'une courbe de genre 2, (in press)

[6] G. van der Geer, Hilbert modular surfaces, Springer, Berlin, 1987.

[7] J. Gutierrez and T. Shaska, Hyperelliptic curves with extra involutions, *LMS J. of Comput. Math.*, 8 (2005), 102-115.

[8] G. Humbert Sur les fonctionnes abliennes singulires. I, II, III. J. Math. Pures Appl. serie 5, t. V, 233–350 (1899); t. VI, 279–386 (1900); t. VII, 97–123 (1901).

[9] J. Igusa, Arithmetic Variety Moduli for genus 2. *Ann. of Math.* (2), 72, 612-649, 1960.

[10] C. Jacobi, Review of Legendre, Théorie des fonctions elliptiques. Troiseme supplém ent. 1832. J. reine angew. Math. 8, 413-417.

[11] A. Krazer, Lehrbuch der Thetafunctionen, Chelsea, New York, 1970.

[12] V. Krishnamorthy, T. Shaska, H. Völklein, Invariants of binary forms , *Developments in Mathematics*, Vol. 12, Springer 2005, pg. 101-122.

[13] M. R. Kuhn, Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc* **307**, 41-49, 1988.

[14] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, The locus of curves with prescribed automorphism group. *Communications in arithmetic fundamental groups* (Kyoto, 1999/2001). Sūrikaisekikenkyūsho Kōkyūroku No. 1267 (2002), 112–141.

[15] N. Murabayashi, The moduli space of curves of genus two covering elliptic curves. Manuscripta Math. 84 (1994), no. 2, 125–133.

[16] N. Pjero, M. Ramosao, T. Shaska, Genus two curves covering elliptic curves of even degree, *Albanian J. Math.* Vol. @, Nr. 3, 241-248.

[17] T. Shaska, Genus 2 curves with degree 3 elliptic subcovers, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.

[18] T. Shaska, Computational algebra and algebraic curves, ACM, *SIGSAM Bulletin*, *Comm. Comp. Alg.*, Vol. **37**, No. 4, 117-124, 2003.

[19] T. Shaska, Genus 2 curves with (3,3)-split Jacobian and large automorphism group, Algorithmic Number Theory (Sydney, 2002), **6**, 205-218, *Lect. Not. in Comp. Sci.*, 2369, Springer, Berlin, 2002.

[20] T. Shaska, Curves of genus 2 with $(n, n)$-decomposable Jacobians, *J. Symbolic Comput.* 31 (2001), no. 5, 603–617.
[21] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus two fields, *Algebra, Arithmetic and Geometry with Applications*, pg. 687 - 707, Springer (2004).
[22] K. Magaard, T. Shaska, H. Völklein, Genus 2 curves with degree 5 elliptic subcovers, Forum Math. (to appear).
[23] T. Shaska, Genus two curves covering elliptic curves: a computational approach. Computational aspects of algebraic curves, 206–231, Lecture Notes Ser. Comput., 13, World Sci. Publ., Hackensack, NJ, 2005.

Albanian Journal of Mathematics (ISSN: 1930-1235) was founded by T. Shaska in 2007 with the idea to support Albanian mathematicians in Albania and abroad.


The journal is not associated with any government institutions in Albania or any public or private universities in Albania or abroad. The journal does not charge any fees to the authors and has always been an open access journal. The journal supports itself with private donations and voluntary work from its staff. Its main office is in Vlora, Albania.