Albanian Journal of Mathematics

Për një Shqipëri të shkencës dhe kulturës.

Volume 4, 2010

www.albanian-j-math.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 1, Pages 3–13
ISSN 1930-1235: (2010)

EXPONENTIAL SUMS FOR NONLINEAR RECURRING SEQUENCES IN RESIDUE RINGS

EDWIN EL-MAHASSNI

Abstract. We prove some new bounds on exponential sums for nonlinear recurring sequences over residue rings. In addition, we also show similar novel results when the modulus is almost squarefree, thereby improving the results in El-Mahassni, Shparlinski, and Winterhof [11] and El-Mahassni and Winterhof [13] This is done by using a technique employed by Niederreiter and Winterhof [26] and through the generalisation of a Lemma found in [11] and [13]. Lastly, applications to the distribution of nonlinear congruential pseudorandom numbers are also given.

1. Introduction

For an integer $M \geq 2$, we let $f(X) \in \mathbb{Z}_M[X]$ be a polynomial of degree $d \geq 2$ over the residue ring $\mathbb{Z}_M$ modulo M , defined by a recurrence relation of the form

$$u_{n+1} \equiv f(u_n) \pmod{M}, \quad 0 \leq u_n \leq M-1, \qquad n = 0, 1, \ldots \tag{1}$$

with some initial value $u_0 = v$. It is obvious that the sequence (1) eventually becomes periodic with some period $t \leq M$.

We define the sequence of polynomials $f_k(X)$, by the recurrence relation

$$f_k(X) = f(f_{k-1}(X)), \qquad k = 1, 2, \ldots, \tag{2}$$

where $f_0(X) = X$. It is clear that if $\deg f = d \geq 2$ then $\deg f_k \leq d^k$ and that $u_{n+k} \equiv f_k(u_n) \pmod{M}$.

Throughout this paper we assume that this sequence is *purely periodic*, that is, $u_n = u_{n+t}$ beginning with $n = 0$, otherwise we consider a shift of the original sequence.

We define $\mathbf{e}_M(x) = \exp(2\pi i x/M)$ and consider the incomplete exponential sums

$$S_{\mathbf{a}}(M, N) = \sum_{n=0}^{N-1} \mathbf{e}_M\left(\sum_{j=0}^{s-1} a_j u_{n+j}\right), 1 \leq N \leq t, s \geq 1,$$

where $\mathbf{a} = (a_0, \ldots, a_{s-1}) \not\equiv 0 \pmod{M}$. Now, throughout the rest of the paper we assume that f is of degree at least 2 modulo every prime divisor of M.

Key words and phrases. Pseudorandom numbers; nonlinear congruential method; discrepancy; exponential sums.

The author is very grateful to Igor Shparlinski for helpful comments and suggestions.

2000 Mathematics Subject Classification. Primary: 11K45, 11L07, 65C10.

We now go on to recall some previous bounds which we will improve upon. First, we assume that $G = \gcd(a_0, \dots, a_{s-1}, M) < M/2$. We start by noting that from [13], for an arbitrary modulus M, the bound

$$\max_{\gcd(a_0,\dots,a_{s-1},M)=G} S_{\mathbf{a}}(M,N) = O\left(N^{1/2}\frac{M^{1/2}}{(\log\log(M/G))^{1/2}}\right) \tag{3}$$

holds, where the implied constant depends only on d and s.

Then, in [11], an improvement on this bound was proven when the modulus is almost squarefree. This was defined to be when

$$\omega(M) \le 2\log\log M \quad \text{and} \quad \rho(M) \ge \frac{M}{(\log\log M)^2}, \tag{4}$$

where $\omega(M)$ denotes the number of distinct prime divisors of M and $\rho(M)$ is the largest squarefree divisor of M. In those cases, for any $\varepsilon \ge 0$, the bound

$$\max_{\gcd(a_0,\dots,a_{s-1},M)\le M^{1-\varepsilon}} S_{\mathbf{a}}(M,N) = O\left(N^{1/2}M^{1/2}\frac{(\log\log M)^{1/2}}{(\log M)^{1/2}}\right) \tag{5}$$

holds, where the implied constant depends on d, s and ε.

Further, in [11], it has also been proven that if the constraints of (4) are satisfied, for every sufficiently large integer Q, the bound given by (5) holds for all positive integers $M \le Q$ except $o(Q)$ of them.

The rest of the paper is structured as follows. In Section 2, we list some previously established results which we use to prove our main bound. In Section 3, using a similar technique to that in [26], we modify the methods in [11] and [13] to provide new bounds for $S_{\mathbf{a}}(M,N)$. We will show that we can obtain improvements for the bounds in (3) and (5) when $N \ge M/\log M$ and by placing some restrictions on the size of p_1, the smallest prime divisor of M. In Section 4, we apply the exponential sum bound to analyse the distribution of *nonlinear congruential pseudorandom numbers* $u_n/M, n \ge 0$, in the unit interval in terms of a discrepancy bound. We refer to [22, Chapter 8], [24] and [1] for further background on nonlinear congruential pseudorandom numbers.

2. Preliminaries

We now recall some results which will aid us in proving our main results. For a sequence of N points

$$\Gamma = (\gamma_{1,n}, \dots, \gamma_{s,n})_{n=1}^{N} \tag{6}$$

of the half-open interval $[0,1)^s$, denote by Δ_Γ its *discrepancy*, that is,

$$\Delta_\Gamma = \sup_{B\subseteq[0,1)^s} \left|\frac{T_\Gamma(B)}{N} - |B|\right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the box

$$B = [\alpha_1, \beta_1) \times \dots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes. For an integer vector $\mathbf{a} = (a_0, \dots, a_{s-1}) \in \mathbb{Z}^s$ we put

$$|\mathbf{a}| = \max_{i=0,\dots,s-1} |a_i| \qquad \text{and} \qquad r(\mathbf{a}) = \prod_{i=0}^{s-1} \max\{|a_i|, 1\}. \tag{7}$$

We also need the *Erdös–Turán–Koksma inequality* (see [5, Theorem 1.21]) for the discrepancy of a sequence of points of the s-dimensional unit cube, which we present in the following form.

Lemma 1. *There exists a constant $C_s > 0$ depending only on the dimension s such that, for any integer $L \geq 1$, for the discrepancy of a sequence of points* (6) *the bound*

$$\Delta_\Gamma < C_s \left(\frac{1}{L} + \frac{1}{N} \sum_{0<|\mathbf{a}|\leq L} \frac{1}{r(\mathbf{a})} \left| \sum_{n=1}^{N} \exp\left(2\pi i \sum_{j=0}^{s-1} a_j \gamma_{j,n} \right) \right| \right)$$

holds, where $|\mathbf{a}|$ and $r(\mathbf{a})$ are defined by (7) *and the sum is taken over all integer vectors*

$$\mathbf{a} = (a_0, \dots, a_{s-1}) \in \mathbb{Z}^s$$

with $0 < |\mathbf{a}| \leq L$.

The currently best value of C_s is given in [3].

We also make use of the Hua Loo Keng bound in a form which is a relaxation of the main result of [27] (see also Section 3 of [2]).

Lemma 2. *For any polynomial $F(X) = B_D X^D + \ldots + B_1 X + B_0 \in \mathbb{Z}_M[X]$ of degree $D \geq 1$, there is a constant $c_0 > 0$ so that the bound*

$$\left| \sum_{x=1}^{M} \mathbf{e}_M\left(F(x)\right) \right| < e^{c_0 D} M^{1-1/D} G^{1/D}$$

holds, where $G = \gcd(B_D, \dots, B_1, M)$.

Note that the currently best known constant is $c_0 = 1.74$ see [4].

We now list the following lemmas. The first is listed in a slightly weaker form than found in [11, Lemma 4], whilst the second is an extension of [13, Lemma 3] respectively.

Lemma 3. *Let $F(X) = \sum_{i=0}^{D} B_i X^i \in \mathbb{Z}_M[X]$ be of degree D. Then*

$$\left| \sum_{x=0}^{M-1} \mathbf{e}_M(F(x)) \right| \leq (D-1)^{\omega(M)} M \Delta^{1/2} \rho(M)^{-1/2},$$

where $\Delta = \gcd(B_1, ..., B_D, M)$.

Lemma 4. *Let $f(X) \in \mathbb{Z}_M[X]$ be a polynomial of degree at least 2 modulo every prime divisor of M, with p_1 being the least prime divisor of M, and let*

$$\sum_{j=0}^{s-1} a_j \left(\left(f_{k_1+j}(X) + \ldots + f_{k_r+j}(X)\right) - \left(f_{k_{r+1}+j}(X) + \ldots f_{k_{2r}+j}(X)\right) \right) = B_D X^D + \ldots + B_1 X + B_0.$$

Then, if $\{k_1, \ldots, k_r\} \neq \{k_{r+1}, \ldots, k_{2r}\}$ *as multisets, for any* $p_1 > r \geq 1$*, we have*

$$\gcd(B_D, \ldots, B_1, M) = \gcd(a_0, \ldots, a_{s-1}, M).$$

Proof. We put $A_j = a_j/G$, $j = 0, \ldots, s-1$ and $m = M/G$, where $G = \gcd(a_0, \ldots, a_{s-1}, M)$. In particular,

$$\gcd(A_0, \ldots, A_{s-1}, m) = 1. \tag{8}$$

It is enough to show that the polynomial

$$H(X) = \sum_{j=0}^{s-1} A_j \left(\left(f_{k_1+j}(X) + \ldots + f_{k_r+j}(X)\right) - \left(f_{k_{r+1}+j}(X) + \ldots + f_{k_{2r}+j}(X)\right)\right)$$

is not a constant polynomial modulo p for any prime $p|m$.

We take $f^{(p)}$ to be the reduction of f modulo p. By our assumption, $\deg f^{(p)} = d_p \geq 2$. Denoting by $f_k^{(p)}$ the kth iteration of $f^{(p)}$ defined similarly to (2) and by $H^{(p)}(X)$ as $H(X) \pmod p$. Thus,

$$H^{(p)}(X) = \sum_{t=1}^{r} \sum_{j=0}^{s-1} A_j \left(f_{k_t+j}^{(p)}(X) - f_{k_{r+t}+j}^{(p)}(X)\right) \pmod p.$$

Let h be the largest $j = 1, \ldots, s$ with $\gcd(A_j, p) = 1$ (we see from (8) that such h exists). Then for $\{k_1, \ldots, k_r\} \neq \{k_{r+1}, \ldots, k_{2r}\}$ as multisets, where $r < p_1$, the polynomial $H(X)$ is of degree exactly $d_p^{k+h} \geq 1$ modulo p, where k is the largest k_i which appears in one of the two sets more often than in the other one, such that $k_i \neq k_{i+r}$, for some $1 \leq i \leq t$, which finishes the proof. □

The following statement proceeds immediately from the classical result of Hardy-Ramanujan on the typical order of $\omega(M)$, see [18, Theorem 431], [28, Section 3.4, Theorem 4], and used also in [11, Lemma 6].

Lemma 5. *For every sufficiently large* Q*, the bound* $\omega(M) \leq 2 \log\log M$ *holds for all positive integers* $M \leq Q$ *except* $o(Q)$ *of them.*

Lastly, we also use the next result which was proved in [11, Lemma 7].

Lemma 6. *For any integer* $Y \geq 1$ *the bound* $\rho(M) > M/Y$ *holds for all positive integers* $M \leq Q$ *except* $O(Q/Y^{1/2})$*.*

3. Bounds of Exponential Sums

In this section, through the use of the Hölder inequality as employed in [26], we improve bounds (3) and (5) respectively, by refining the method of bounding exponential sums that were applied in [11] and [13].

Theorem 7. *Let the sequence* (u_n)*, given by* (1) *with a polynomial* $f(X) \in \mathbb{Z}_M[X]$*, of total degree* d*, be purely periodic modulo* M *with period* t*. Assume that for every*

prime divisor p of M, we have $p \ge 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \ge N \ge M/\log\log M$, then the bound

$$\max_{\gcd(a_0,\ldots,a_{s-1},M)=G} |S_{\mathbf{a}}(M,N)| = O\left(N\left(\frac{\log(2M/N)}{\log\log(M/G)}\right)^{1/2}\right)$$

holds, where the implied constant depends only on d and s.

Proof. We first prove that, for any integer $2\log\log\log M > r \ge 1$, and $\gcd(a_0,\ldots,a_{s-1},M) = G$, we have

$$S_{\mathbf{a}}(M,N) = O\Bigg(Nr^{1/2}(M/N)^{1/(2r)} \times \left(\min\left\{\lfloor \log\log(M/G)/3\log d\rfloor, \left\lfloor rc_1 e^{(\log(M/G))^{1/3}/r}\right\rfloor\right\}\right)^{-1/2}\Bigg)$$

for $T \ge N \ge M/\log\log M$ and some positive constant c_1. It is obvious that for any integer $k \ge 0$ we have

$$\left|S_{\mathbf{a}}(M,N) - \sum_{n=0}^{N-1} \mathbf{e}_M\left(\sum_{j=0}^{s-1} a_j u_{n+k+j}\right)\right| \le 2k.$$

Therefore, for any integer $K \ge 1$,

$$K|S_{\mathbf{a}}(M,N)| \le W + K(K-1), \tag{9}$$

where

$$W = \sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1} \mathbf{e}_M\left(\sum_{j=0}^{s-1} a_j u_{n+k+j}\right)\right|.$$

By the Hölder inequality, and using

$$F_k(X) = \sum_{j=0}^{s-1} a_j f_{k+j}(X),$$

we obtain

$$\begin{aligned} W^{2r} &\le N^{2r-1}\sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(u_n)\right)\right|^{2r} \\ &\le N^{2r-1}\sum_{x\in\mathbb{Z}_M}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(x)\right)\right|^{2r} \\ &\le N^{2r-1}\sum_{k_1,\ldots,k_{2r}=0}^{K-1}\left|\sum_{x\in\mathbb{Z}_M}\mathbf{e}_M\left(F_{k_1,\ldots,k_{2r}}(x)\right)\right|, \end{aligned}$$

where $F_{k_1,\ldots,k_{2r}}(X) = F_{k_1}(X) + \ldots + F_{k_r}(X) - F_{k_{r+1}}(X) - \ldots - F_{k_{2r}}(X)$.

If $\{k_1,\ldots,k_r\} = \{k_{r+1},\ldots,k_{2r}\}$ as multisets, then $F_{k_1,\ldots,k_{2r}}(X)$ is constant and the inner sum is trivially equal to M. There are at most $r!K^r \le r^rK^r$ such sums. Otherwise, we can apply Lemma 2 together with Lemma 4, to get the upper bound $e^{c_0 d^{K+s-2}}M^{1-1/d^{K+s-2}}G^{1/d^{K+s-2}}$ for at most K^{2r}. Hence,

$$W^{2r} \le r^rK^rN^{2r-1}M + e^{c_0 d^{K+s-2}}M^{1-1/d^{K+s-2}}G^{1/d^{K+s-2}}K^{2r}N^{2r-1} \tag{10}$$

Choose

$$K = \min\left\{ \left\lfloor \frac{\log\log(M/G)}{3\log d} \right\rfloor, \left\lfloor rc_1 e^{(\log(M/G))^{1/3}/r} \right\rfloor \right\},$$

for some positive constant c_1. Note that we get $\left\lfloor \frac{\log\log(M/G)}{3\log d} \right\rfloor$, when $r = 1$ and using this value for $e^{c_0 d^{K+s-2}}$ we then obtain $\left\lfloor rc_1 e^{(\log(M/G))^{1/3}/r} \right\rfloor$ for arbitrary r.

Then it is easy to see that the first term in the right-hand side of (10) dominates the second one in terms of the order of magnitude in M, and we get the first equation of the proof from (9) and (10) after simple calculations.

Finally, we choose

$$r = \lceil \log(2M/N) \rceil .$$

Note that $1 \le r < 2\log\log\log M$, since $N \ge M/\log\log M$. Thus, for all suitable large M, we have

$$c_1 r e^{(\log(M/G))^{1/3}/r} \ge \log\log(M/G).$$

To see this is true, we note that this is equivalent to proving

$$\log r + \log c_1 + \frac{(\log(M/G))^{1/3}}{r} \ge \log\log\log(M/G).$$

If $\log r \ge \log\log\log(M/G)$ then we are done, else we have $r < \log\log(M/G)$. In this case, we simply need to show that for all large enough M

$$\frac{(\log(M/G))^{1/3}}{(\log\log(M/G))} \ge \log\log(M/G).$$

But, taking logarithms from both sides we can then indeed see that

$$\log\log(M/G) \ge 4\log\log\log(M/G)).$$

If we then note that $r^{1/2}(M/N)^{1/2r} < \log(2M/N)$, the theorem then follows from the first equation of the proof. □

This next bound is an improvement for the exponential sum of nonlinear congruential generators with an "almost squarefree" modulus.

Theorem 8. *Let an integer $M \ge 1$ be such that*

$$\omega(M) \le 2\log\log M \qquad \text{and} \qquad \rho(M) \ge \frac{M}{(\log\log M)^2},$$

where $\omega(M)$ denotes the number of distinct prime divisors of M and $\rho(M)$ is the largest squarefree divisor of M.

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \ge 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \ge N \ge M/\log\log M$, then, for any $\varepsilon > 0$, the bound

$$\max_{\gcd(a_0,\ldots,a_{s-1},M) \le M^{1-\varepsilon}} |S_{\mathbf{a}}(M,N)| = O\left(N \left(\frac{(\log(2M/N)\log\log M)}{\log M} \right)^{1/2} \right)$$

holds, where the implied constant depends on d, s and ε.

Proof. Put $w = \omega(M)$ and $R = \rho(M)$. We first prove that, for any integer $2\log\log\log M > r \geq 1$, and $\gcd(a_0, \ldots, a_{s-1}, M) \leq M^{1-\varepsilon}$, we have

$$S_{\mathbf{a}}(M,N) =$$

$$O\Bigg(Nr^{1/2}(M/N)^{1/(2r)}\left(\min\left\{\left\lfloor \varepsilon \log M/(5\log d\log\log M)\right\rfloor, \left\lfloor r\left(M^{\varepsilon/10}/\left(\log\log M\right)\right)^{1/r}\right\rfloor\right\}\right)^{-1/2}\Bigg),$$

for $M/\log\log M \leq t \leq M$. It is obvious that for any integer $k \geq 0$ we have

$$\left|S_{\mathbf{a}}(M,N) - \sum_{n=0}^{N-1}\mathbf{e}_M\left(\sum_{j=0}^{s-1}a_j u_{n+k+j}\right)\right| \leq 2k.$$

Therefore, for any integer $K \geq 1$,

$$K|S_{\mathbf{a}}(M,N)| \leq W + K(K-1), \tag{11}$$

where

$$W = \sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(\sum_{j=0}^{s-1}a_j u_{n+k+j}\right)\right|.$$

By the Hölder inequality, and using

$$F_k(X) = \sum_{j=0}^{s-1}a_j f_{k+j}(X),$$

we obtain

$$\begin{aligned} W^{2r} &\leq N^{2r-1}\sum_{n=0}^{N-1}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(u_n)\right)\right|^{2r} \\ &\leq N^{2r-1}\sum_{x\in\mathbb{Z}_M}\left|\sum_{k=0}^{K-1}\mathbf{e}_M\left(F_k(x)\right)\right|^{2r} \\ &\leq N^{2r-1}\sum_{k_1,\ldots,k_{2r}=0}^{K-1}\left|\sum_{x\in\mathbb{Z}_M}\mathbf{e}_M\left(F_{k_1,\ldots,k_{2r}}(x)\right)\right|, \end{aligned}$$

where $F_{k_1,\ldots,k_{2r}}(X) = F_{k_1}(X) + \ldots + F_{k_r}(X) - F_{k_{r+1}}(X) - \ldots - F_{k_{2r}}(X)$

If $\{k_1,\ldots,k_r\} = \{k_{r+1},\ldots,k_{2r}\}$ as multisets, then $F_{k_1,\ldots,k_{2r}}(X)$ is constant and the inner sum is trivially equal to M. There are at most $r!K^r \leq r^rK^r$ such sums. Otherwise, we can apply Lemma 3, together with Lemma 4 to the inner sum, to get the upper bound $d^{(K+s-2)w}M^{(3-\varepsilon)/2}R^{-1/2}$ for at most K^{2r}. Hence,

(12)

$$W^{2r} \leq r^rK^rN^{2r-1}M + d^{2(K+s-2)\log\log M}K^{2r}N^{2r-1}M^{1-\varepsilon/2}\log\log M$$

Choose

$$K = \min\left\{\left\lfloor\frac{\varepsilon\log M}{5\log d\log\log M}\right\rfloor, \left\lfloor r\left(M^{\varepsilon/10}/\log\log M\right)^{1/r}\right\rfloor\right\}.$$

Note that we get $\left\lfloor \frac{\varepsilon \log M}{5 \log d \log\log M} \right\rfloor$ when $r = 1$ and using this value for $d^{2(K+s-2)\log\log M}$ we then obtain $\left\lfloor r \left(M^{\varepsilon/10}/\log\log M\right)^{1/r} \right\rfloor$ for arbitrary r.

Then it is easy to see that the first term in the right-hand side of (12) dominates the second one in terms of the order of magnitude in M, and we get the first equation of the proof from (11) and (12) after simple calculations.

Finally, we choose

$$r = \lceil \log(2M/N) \rceil.$$

Note that $r < 2 \log\log\log M$ since $N \geq M/\log\log M$. Clearly, for our choice of r and all large enough M, we have

$$\begin{aligned} r \left(M^{\varepsilon/10}/\log\log M\right)^{1/r} &> \log\left(M^{\varepsilon/10}/\log\log M\right)/2\log\log\log M \\ &> \log M^{\varepsilon}/5 \log d \log\log M, \end{aligned}$$

for any $\varepsilon > 0$. If we then note that $r^{1/2}(M/N)^{1/2r} < \log(2M/N)$, the theorem then follows from the first equation of the proof. □

Recalling Lemmas 5 and 6 we obtain:

Corollary 9. *For every sufficiently large Q, the following statement holds for all positive integers $M \leq Q$ except $o(Q)$ of them:*

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \geq 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \geq N \geq M/\log\log M$, then, for any $\varepsilon > 0$, the bound

$$\max_{\gcd(a_0,\ldots,a_{s-1},M) \leq M^{1-\varepsilon}} |S_{\mathbf{a}}(M,N)| = O\left(N\left(\frac{(\log(2M/N)\log\log M)}{\log M}\right)^{1/2}\right)$$

holds, where the implied constant depends on d, s and ε.

We now present some new discrepancy bounds using our new results for the exponential sums for the nonlinear congruential generator. The first bound applies to arbitrary moduli, whilst the latter is for almost squarefree moduli.

Let $D_s(M,N)$ denote the discrepancy of the points

$$\left(\frac{u_n}{M}, \ldots, \frac{u_{n+s-1}}{M}\right), \qquad n = 0, 1, \ldots, N-1,$$

given by (1) in the s-dimensional unit cube $[0,1)^s$.

Theorem 10. *If the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \geq 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \geq N \geq M/\log\log M$, then, the bound*

$$D_s(M,N) = O\left(\left(\frac{\log(2M/N)}{\log\log M}\right)^{1/2} (\log\log\log M)^s\right)$$

holds, where the implied constant depends only on s and d.

Proof. The statement follows from Lemma 1, taken with

$$L = \left\lceil \left(\frac{\log\log M}{\log(2M/N)} \right)^{1/2} \right\rceil$$

and the bound of Theorem 7, as

$$\gcd(a_0, \dots, a_{s-1}, M) \le L \le 2\left(\log\log M\right)^{1/2} \le (\log M)^{1/2} \le M^{1/2}$$

where for any nonzero vector $\mathbf{a} = (a_1, \dots, a_s) \in \mathbb{Z}^s$ with $|\mathbf{a}| \le L$ and sufficiently large M. □

Theorem 11. *Let an integer $M \ge 1$ be such that*

$$\omega(M) \le 2\log\log M \qquad \text{and} \qquad \rho(M) \ge \frac{M}{(\log\log M)^2}.$$

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \ge 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \ge N \ge M/\log\log M$, then, for any $\varepsilon > 0$, the bound

$$D_s(M, N) = O\left(\left(\frac{(\log(2M/N)}{\log M} \right)^{1/2} (\log\log M)^{s+1/2} \right)$$

holds, where the implied constant depends only on s and d.

Proof. The statement follows from Lemma 1 taken with

$$L = \left\lceil \left(\frac{\log M}{\log(2M/N)\log\log M)} \right)^{1/2} \right\rceil$$

and the bound of Theorem 8, as

$$\gcd(a_0, \dots, a_{s-1}, M) \le L \le 2\left(\log M\right)^{1/2} \le M^{1/2}$$

for any nonzero vector $\mathbf{a} = (a_1, \dots, a_s) \in \mathbb{Z}^s$ with $|\mathbf{a}| \le L$ and sufficiently large M. □

Recalling Lemmas 5 and 6 we obtain:

Corollary 12. *For every sufficiently large Q, the following statement holds for all positive integers $M \le Q$ except $o(Q)$ of them:*

Let the sequence (u_n), given by (1) with a polynomial $f(X) \in \mathbb{Z}_M[X]$, of total degree d, be purely periodic modulo M with period t. Assume that for every prime divisor p of M, we have $p \ge 2\log\log\log M$ and also f of degree at least 2 modulo every prime $p|M$. If $t \ge N \ge M/\log\log M$, then, for any $\varepsilon > 0$, the bound

$$D_s(M, N) = O\left(\left(\frac{(\log(2M/N)}{\log M} \right)^{1/2} (\log\log M)^{s+1/2} \right)$$

holds, where the implied constant depends only on s and d.

4. Discussion

We remark that for Theorems 7 and 8 results covering all possible N would be desirable. We also note that for the counter-dependent generators, the Holdër inequality was also applied to the prime modulus case [12]. However, we believe that through a similar variant of Lemma 4, improvements on the bounds for the arbitrary modulus case [10] and for the higher order cases (both prime and arbitrary modulus [9, 17]) could also be obtained. We finally note that this technique does not improve the bound of permutation polynomials modulo almost a squarefree integer (see [11, Section 4]).

References

[1] S. Blackburn and I. Shparlinski, Character Sums and Nonlinear Recurring Sequences, Discrete Mathematics, 2006, 306, 1126-1131.

[2] T. Cochrane and Z. Y. Zheng, A Survey on Pure and Mixed Exponential Sums Modulo Prime Powers, Proc. Illinois Millennial Conf. on Number Theory, 2002, 1, 271-300.

[3] T. Cochrane, Trigonometric Approximations and Uniform Distribution Modulo 1, Proc. Amer. Math. Soc., 1988, 103, 695—703.

[4] P. Ding and M. G. Qi, Further Estimates of Complete Trigonometric Sums, J. Tsinghua Univ., 1989, 29, 74–85.

[5] M. Drmota and R. Tichy, Sequences, Discrepancies and Applications, Springer-Verlag, Berlin, 1997.

[6] E. El-Mahassni and I. E. Shparlinski, On the Distribution of the Elliptic Curve Power Generator, Proc. 8th. Conf. Finite Fields and Their Appl, Contemp. Math. (2007), 2008, 461, 111–118.

[7] On the Distribution of the Power Generator Modulo a Prime Power for Parts of the Period, Bol. Soc. Mat. Mex., 2008, 13 (1), 1.

[8] E. El-Mahassni, On the Distribution of the Power Generator Over a Residue Ring for Parts of the Period, Rev. Mat. Compl., 2008, 21 (2), 319-325.

[9] E. El-Mahassni and D. Gomez, On the Distribution of the Counter-Dependent Nonlinear Congruential Generator in Residue Rings, Int. J. Num. Th., 2008, 4 (6), 1009–1018.

[10] E. El-Mahassni and D. Gomez, On the Distribution of Nonlinear Congruential Pseudorandom Numbers of Higher Orders in Residue Rings, AAECC, Lecture Notes in Computer Science, 2009, 5527, 195-203.

[11] E. D. El-Mahassni and I. E. Shparlinski and A. Winterhof, Distribution of Nonlinear Congruential Pseudorandom Numbers for Almost Squarefree Integers, Monatsh. Math., 2006, 148, 297–307.

[12] E. D. El-Mahassni and A. Winterhof, On the Distribution and Linear Complexity of Counter-Dependent Nonlinear Congruential Pseudorandom Number Generators, JP Journal of Algebra and Number Theory, 2006, 6(2), 411–423.

[13] E. D. El-Mahassni and A. Winterhof, On the Distribution of Nonlinear Congruential Pseudorandom Numbers in Residue Rings, Intern. J. Number Th., 2006, 2(1), 163–168.

[14] J. B. Friedlander, J. Hansen and I. E. Shparlinski, On Character Sums with Exponential Functions, Mathematika, 2000, 47, 75–85.

[15] J. B. Friedlander and I. E. Shparlinski , On the Distribution of the Power Generator, Math. Comp., 2001, 70, 1575–1589.

[16] Domingo Gomez and Jaime Gutierrez and Igor E. Shparlinski, Exponential sums with Dickson polynomials, Finite Fields and Their Applications, 2006, 12, 16–25.

[17] F. Griffin and H. Niederreiter and I. E. Shparlinski, On the Distribution of Nonlinear Recursive Congruential Pseudorandom Numbers of Higher Orders, AAECC, Lecture Notes in Computer Science , 1999, 1719, 87-93.

[18] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Clarendon Press, 1979.

[19] R. Lidl and H. Niederreiter, Finite Fields and Applications, Cambridge, 1997.

[20] T. Lange and I. E. Shparlinski, Certain Exponential Sums and Random Walks on Elliptic Curves, Canada J. Math, 2005, 57, 338–350.
[21] H. Niederreiter, Design and Analysis of Nonlinear Pseudorandom Number Generators, Monte Carlo Simulation, 2001, A. A. Balkema Publishers, Rotterdam, 3–9.
[22] H. Niederreiter, Random Number Generation and Quasi–Monte Carlo Methods, Siam Press, 1992.
[23] H. Niederreiter and I. E. Shparlinski, On the Distribution and Lattice Structure of Nonlinear Congruential Pseudorandom Numbers, Finite Fields and Their Appl., 1999, 5, 246–253.
[24] H. Niederreiter and I. E. Shparlinski, Recent Advances in the Theory of Nonlinear Pseudorandom Number Generators, Proc. Conf. on Monte Carlo and Quasi Monte Carlo Methods, 2000, 2002, 86–102.
[25] H. Niederreiter and I. E. Shparlinski, Dynamical Systems Generated by Rational Functions, Lect. Notes in Comp. Sci., 2003, 2643,Springer-Verlag, Berlin, 6–17.
[26] H. Niederreiter and A. Winterhof, Exponential Sums for Nonlinear Recurring Sequences, Finite Fields and Their Appl., 2008, 14(1), 59–64.
[27] S. B. Stečkin, An Estimate of a Complete Rational Exponential Sum, Trudy Mat. Inst. Steklov., 1977, 143, 188–207 (in Russian).
[28] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, University Press, 1995, Cambridge, UK.

Department of Computing, Macquarie University, North Ryde, NSW 2109, Australia

E-mail address: edwinelm@ics.mq.edu.au

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 1, Pages 13–17
ISSN 1930-1235: (2010)

SOLVABILITY OF EXTENDED GENERAL MIXED VARIATIONAL INEQUALITIES

MUHAMMAD ASLAM NOOR*

Abstract. In this paper, we consider and study a new class of mixed variational inequality, which is called the extended general mixed variational inequality. We use the auxiliary principle technique to study the existence of a solution of the extended general mixed variational inequality. Several special cases are also discussed.

1. Introduction

Variational inequalities, which were introduced in 1960's, are being used as a powerful tool to study a wide class of problems, which arise in various branches of mathematical, financial, regional and engineering sinces, see[1-27] and the references therein. Using the technique of Noor [16-21] and Noor et al [22], one cam show that the minimum of the sum of differentiable hg-convex function and a nondifferentiable hg-convex functions can be charactrized by a class of variational inequality. Motivated by this result, we introduce a new class of mixed variational inequalities, which is calle *extended general mixed variational inequality* involving four different operators. It is known that it is very difficult to find the projection of the operator except in very special cases. To overcome this drawback, on uses the auxiliary principle technique. This technique is mainly due to Glowinski, Lions and Tremolieres [4]. This technique is more flexible and has been used to develop several numerical methods for solving the variational inequalities and the equilibrium problems. In this paper, we again use the auxiliary principle technique to study the existence of a solution of the extended general mixed variational inequalities. Since the extended general variational inequalities include various classes of variational inequalities and complementarity problems as special cases, results proved in this paper continue to hold for these problems. Results proved in this paper may be viewed as important and significant improvement of the previously known results. It is interesting to explore the applications of these extended general variational inequalities in mathematical and engineering sciences with new and novel aspects. This may lead to new research in this field.

2. Preliminaries

Let H be a real Hilbert space whose inner product and norm are denoted by $\langle \cdot, \cdot \rangle$ and $\|.\|$, respectively. Let K be a nonempty closed and convex set in H. Let $\varphi : H \longrightarrow R \cup \{\infty\}$ be a continuous function.

For given nonlinear operators $T, g, h : H \to H$, consider the problem of finding $u \in H, h(u) \in K$ such that

$$\langle Tu, g(v) - h(u) \rangle + \varphi(g(v)) - \varphi(h(u)) \geq 0, \qquad \forall v \in H : g(v) \in K. \tag{2.1}$$

Received by the editors Received: 20 March 2010.

* Corresponding author.

2000 *Mathematics Subject Classification.* Primary 49J40; Secondary 90C33.

Key words and phrases. Variational inequalities, nonconvex functions, fixed-point problem, convergence, auxiliary principle.

Inequality of type (2.1) is called the *extended general mixed variational inequality involving four operators*.

We now show that the minimum of the sum of differentiable nonconvex function and a class of differentiable nonconvex functions and nondifferentiable nonconvex function on the hg-convex set K in H can be characterized by extended general variational inequality (2.1). For this purpose, we recall the following well known concepts, see [2, 16-20].

Definition 2.1. Let K be any set in H. The set K is said to be hg-convex, if there exist functions $g, h : H \longrightarrow H$ 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[2]. If $g = h$, then the hg-convex set K is called the g-convex set, which was introduced by Youness [26]. See also Cristescu and Lupsa [2] for its various extensions and generalization.

Definition 2.2. The function $F : K \longrightarrow H$ is said to be hg-convex on the hg-convex set K, if there exist two functions h, g such that

$$\begin{aligned} F(h(u) + t(g(v) - h(u))) \quad &\leq \quad (1-t)F(h(u)) + tF(g(v)). \\ &\forall u, v \in H : h(u), g(v) \in K, \quad t \in [0, 1]. \end{aligned}$$

Clearly every convex function is hg-convex, but the converse is not true. For $g = h$, Definition 2.2 is due to Youness [26].

It is known [16-19] that the minimum of a differentiable hg-convex function on a hg-convex set K in H can be characterized by the extended general variational inequality (2.1). One can prove a similar result for the sum of nonconvex functions on the hg-convex set.

Lemma 2.3. *Let $F : K \longrightarrow H$ be a differentiable hg-convex function on the hg-convex set K. Then $u \in H : h(u) \in K$ is the minimum of the functional $I[v]$ defind by (2.) on the hg-convex set K, if and only if, $u \in H : h(u) \in K$ satisfies the inequality*

$$\langle F'(h(u)), g(v) - h(u)\rangle + \varphi(g(v)) - \varphi(h(u)) \geq 0, \quad \forall v \in H : g(v) \in K, \tag{2.2}$$

where $F'(u)$ is the differential of F at $u \in K$.

Lemma 2.3 implies that hg-convex programming problem can be studied via the extended general mixed variational inequality (2.1) with $Tu = F'(h(u))$.

We now list some special cases of the extended general variational inequalities.

I. If $g = h$, then Problem(2.1) is equivalent to finding $u \in H : g(u) \in K$ such that

$$\langle Tu, g(v) - g(u)\rangle + \varphi(g(v)) - \varphi(g(u)) \geq 0, \qquad \forall v \in H : g(v) \in K, \tag{2.3}$$

which is known as general mixed variational inequality, introduced and studied by Noor [8]. 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.

II. For $g \equiv I$, the identity operator, the extended general variational inequality (2.1) collapses to: find $u \in H : h(u) \in K$ such that

$$\langle Tu, v - h(u)\rangle + \varphi(v) - \varphi(g(u)) \geq 0, \quad \forall v \in K, \tag{2.4}$$

which is also called the general mixed variational inequality, see Noor et al [22].

III. For $h = I$, the identity operator, the extended general variational inequality (2.1) is equivalent to finding $u \in KI$ such that

$$\langle Tu, g(v) - u\rangle + \varphi(g(u)) - \varphi(u) \geq 0, \quad \forall v \in H : g(v) \in K, \tag{2.5}$$

which is also called the general mixed variational inequality involving two nonlinear operators which was introduced and studied by Noor [18-20].

We would like to emphasize the fact that general variational inequalities (2.4), (2.5) and (2.6) are quite different from each other and have different applications.

VI. For $g = h = I$, the identity operator, the extended general variational inequality (2.1) is equivalent to finding $u \in K$ such that

$$\langle Tu, v - u\rangle + \varphi(v) - \varphi(u) \geq 0, \qquad \forall v \in K, \tag{2.6}$$

which is known as the classical mixed variational inequality. We would like to remark that, if $\varphi(.) =$, then the extended general variational inequality () and its variant forms are exactly the same as considered by Noor [5-21] and Stampacchia [27]. For the recent applications, numerical methods, sensitivity analysis, dynamical systems and formulations of variational inequalities, see [1-27] and the references therein. From the above discussion, it is clear that the extended general mixed variational inequalities (2.1) 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.

We also need the following concepts and results.

Definition 2.4. For all $u, v \in H$, an operator $T : H \to H$ is said to be:

(i) *strongly monotone*, if there exists a constant $\alpha > 0$ such that

$$\langle Tu - Tv, u - v\rangle \geq \alpha||u - v||^2$$

(ii) *Lipschitz continuous*, if there exists a constant $\beta > 0$ such that

$$||Tu - Tv|| \leq \beta||u - v||.$$

From (i) and (ii), it follows that $\alpha \leq \beta$.

Remark 2.5. It follows from the strongly monotonicity of the operator T, that

$$\alpha\|u - v\|^2 \leq \langle Tu - Tv, u - v\rangle \leq \|Tu - Tv\|\|u - v\|, \quad \forall u, v \in H,$$

which implies that

$$\|Tu - Tv\| \geq \alpha\|u - v\|, \quad \forall u, v \in H.$$

This observation enables us to define the following concept.

Definition 2.6. The operator T is said to firmly expanding if

$$\|Tu - Tv\| \geq \|u - v\|, \quad \forall u, v \in H.$$

3. Main Results

In this Section, we use the auxiliary principle technique of Glowinski, Lions and Tremolieres [4] to study the existence of a solution of the extended general mixed variational inequality (2.1).

Theorem 3.1. *Let T be a strongly monotone with constant $\alpha > 0$ and Lipschitz continuous with constant $\beta > 0$. Let g be a strongly monotone and Lipschitz continuous operator with constants $\sigma > 0$ and $\delta > 0$ respectively. If the operator h is firmly expanding and there exists a constant $\rho > 0$ such that*

$$|\rho - \frac{\alpha}{\beta^2}| < \frac{\sqrt{\alpha^2 - \beta^2 k(2-k)}}{\beta^2}, \quad \alpha > \beta\sqrt{k(2-k)}, \quad k < 1, \tag{3.1}$$

where

$$\theta = k + \sqrt{1 - 2\rho\alpha + \rho^2\beta^2} \tag{3.2}$$

$$k = \sqrt{1 - 2\sigma + \delta^2}. \tag{3.3}$$

then the extended general mixed variational inequality (2.1) has a unique solution.

Proof. We use the auxiliary principle technique to prove the existence of a solution of (2.1). For a given $u \in H : g(u) \in K$ satisfying the extended general mixed variational inequality (2.1), we consider the problem of finding a solution $w \in H : h(w) \in K$ such that

$$\langle \rho Tu + h(w) - g(u), g(v) - h(w)\rangle + \rho\varphi(g(v)) - \rho\varphi(h(u)) \geq 0, \quad \forall v \in H : g(v) \in K, \tag{3.4}$$

where $\rho > 0$ is a constant.

The inequality of type (3.4) is called the auxiliary extended general mixed variational inequality associated with the problem (2.1). It is clear that the relation (3.4) defines a mapping $u \longrightarrow w$. It is enough to show that the mapping $u \longrightarrow w$ defined by the relation (3.4) has a unique fixed point

belonging to H satisfying the general variational inequality (2.1). Let $w_1 \neq w_2$ be two solutions of (2.13) related to $u_1, u_2 \in H$ respectively. It is sufficient to show that for a well chosen $\rho > 0$,

$$\|w_1 - w_2\| \leq \theta \|u_1 - u_2\|,$$

with $0 < \theta < 1$, where θ is independent of u_1 and u_2. Taking $v = w_2$(respectively w_1) in (3.4) related to u_1 (respectively u_2), adding the resultant, we have

$$\langle h(w_1) - h(w_2), h(w_1) - h(w_2)\rangle \leq \langle g(u_1) - g(u_2) - \rho(Tu_1 - Tu_2), h(w_1) - h(w_2)\rangle,$$

from which we have

$$\begin{aligned} \|h(w_1) - h(w_2)\| &\leq \|g(u_1) - g(u_2) - \rho(Tu_1 - Tu_2)\| \\ &\leq \|u_1 - u_2 - (g(u_1) - g(u_2))| + \|u_1 - u_2 - \rho(Tu_1 - Tu_2)\|. \end{aligned} \tag{3.5}$$

Since T is both strongly monotone and Lipschitz continuous operator with constants $\alpha > 0$ and $\beta > 0$ respectively, it follows that

$$\begin{aligned} \|u_1 - u_2 - \rho(Tu_1 - Tu_2)\|^2 &\leq \|u_2 - u_2\|^2 - 2\rho\langle u_1 - u_2, Tu_1 - Tu_2\rangle + \rho^2\|Tu_1 - Tu_2\|^2 \\ &\leq \left(1 - 2\rho\alpha + \rho^2\beta^2\right)\|u_1 - u_2\|^2. \end{aligned} \tag{3.6}$$

In a similar way, using the strongly monotonicity with constant $\sigma > 0$ and Lipschitz continuity with constant $\delta > 0$, we have

$$\|u_1 - u_2 - (g(u_1) - g(u_2))\| \leq \sqrt{1 - 2\sigma + \delta^2}\|u_1 - u_2\|. \tag{3.7}$$

From (3.5), (5.6), (3.7) and using the fact that the operator h is firmly expanding, we have

$$\begin{aligned} \|w_1 - w_2\| &\leq \left\{k + \sqrt{1 - 2\rho\alpha + \rho^2\beta^2}\right\}\|u_1 - u_2\| \\ &= \theta\|u_1 - u_2\|, \end{aligned}$$

From (3.1) and (3.2), it follows that $\theta < 1$ showing that the mapping defined by (3.4) has a fixed point belonging to K, which is the solution of (2.1), the required result. □ □

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

References

1. C. Baiocchi and A. Capelo, Variational and Quasi Variational Inequalities, J. Wiley and Sons, New York, 1984.
2. G. Cristescu and L. Lupsa, Non-connected Convexities and Applications, Kluwer Academic Publishers, Dordrecht, Holland, 2002.
3. F. Giannessi and A. Maugeri, Variational Inequalities and Network Equilibrium Problems, Plenum Press, New York, 1995.
4. R. Glowinski, J.L. Lions and R. Trémolières, Numerical Analysis of Variational Inequalities, North-Holland, Amsterdam, 1981.
5. M. Aslam Noor, General variational inequalities, Appl. Math. Letters **1**(1988), 119-121.
6. M. Aslam Noor, Quasi variational inequalities, Appl. Math. Letters **1**(1988), 367-370.
7. M. Aslam Noor, Wiener-Hopf equations and variational inequalities, J. Optim. Theory Appl. **79**(1993), 197-206.
8. M. Aslam Noor, Some algorithms for general monotone mixed variational inequalities, Mathl. Computer Modelling **29**(7)(1999), 1-9.
9. M. Aslam Noor, Some recent advances in variational inequalities, Part I, basic concepts, New Zealand J. Math. **26**(1997), 53-80.
10. M. Aslam Noor, Some recent advances in variational inequalities, Part II, other concepts, New Zealand J. Math. **26**(1997), 229-255.
11. M. Aslam Noor, New approximation schemes for general variational inequalities, J. Math. Anal. Appl. , **251**(2000), 217-229.
12. M. Aslam Noor, Some developments in general variational inequalities, Appl. Math. Computation, **152**(2004), 199-277.
13. M. Aslam Noor, Projection-proximal methods for general variational inequalities, J. Math. Anal. Appl., **318**(2006), 53-62.

14. M. Aslam Noor, General variational inequalities and nonexpansive mappings, J. Math. Anal. Appl., **331**(2007), 810-822.
15. M. Aslam Noor, Auxilairy principle technique for extended general variational inequalities, Banach J. Math. Anal. **1**(2(2008), 33-39.
16. M. Aslam Noor, Some iterative methods for extended general variational inequalities, Albanian J. Math. **2**(2008), 265-275.
17. M. Aslam Noor, Extended general variational inequalities, Appl. Math. Letters, **22**(2009), 182-185.
18. M. Aslam Noor, Differentiable nonconvex functions and general variational inequalities, Appl. Math. Comput., **199**(2008), 623-630.
19. M. Aslam Noor, On a class of general variational inequalities, J. Adv.. Math. Studies, **1**(2008), 31-42.
20. M. Aslam Noor, Sensivity analysis for extended general variational inequalities, Appl. Math. E-Notes, **9**(2009), 17-26.
21. M. Aslam Noor, Auxiliary principle technique for solving general mixed variational inequalities, J. Adv. Math. Studies, **3**(2010).
22. M. Aslam Noor, K. Inayat Noor and H. Yaqoob, On general mixed variational inequalities, Acta Appl. Math. **110**(2010), 227-246.
23. M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Some aspects of variational inequalities, J. Comput. Appl. Math., **47**(1993), 285-312.
24. M. Aslam Noor, K. Inayat Noor and Th. M. Rassias, Set-valued resolvent equations and mixed variational inequalities, J. Math. Anal. Appl., **220**(1998), 741-759.
25. M. Patriksson, Nonlinear Programming and Variational Inequality Problems: A Unified Approach, Kluwer Academic Publishers, Dordrecht, 1998.
26. E. A. Youness, E-convex sets, E-convex functions and E-convex programming, J. Optim. Theory Appl. **102**(1999),439-450.
27. G. Stampacchia, Formes bilineaires coercitives sur les ensembles convexes, C. R. Acad. Sci, Paris, **258**(1964), 4413-4416

Department of Mathematics, COMSATS Institute of Information Technology, Islamabad, Pakistan

Mathematics Department, College of Science, King Saud University, Riaydh, Saudi Arabia

E-mail address: noormaslam@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 1, Pages 19–29
ISSN 1930-1235: (2010)

COMMON FIXED POINT THEOREMS OF GENERALIZED CONTRACTION, ZAMFIRESCU PAIR OF MAPS IN CONE METRIC SPACES

G.V.R. BABU*, G.N. ALEMAYEHU†, AND K.N.V.V. VARA PRASAD‡

Abstract. We prove the existence of common fixed points of a generalized contraction / Zamfirescu pair of maps in a complete cone metric space. Our results generalize the results of Huang anf Zhang [L-G. Huang, X. Zhang: Cone metric spaces and fixed point theorems of contractive mappings, J. Math. Anal. Appl. 332 (2007) 1468–1476] and extend the results of Rezapour and Hamlbarani [Sh. Rezapour, R. Hamlbarani: Some notes on the paper "Cone metric spaces and fixed point theorems of contractive mappings", J. Math. Anal. Appl. 345 (2008) 719–724].

1. Introduction

In 2007, Huang and Zhang [2] generalized the concept of a metric space, replacing the set of real numbers by an ordered Banach space by defining the concept of a cone metric space which is more general than that of a metric space, and obtained fixed point theorems for mappings on complete cone metric spaces having normal cone. Later in 2008, Rezapour and Hamlbarani [4] generalized the results of Huang and Zhang [2] by relaxing the normality property of the cones.

Recently, Jungck, Radenović, Radojević and Rakočević [3] have studied common fixed point results for weakly compatible pairs of mappings in cone metric spaces by omitting the assumptions of normality of the cone in their results, which generalize and extend some earlier results ([2], [4], [1],[5]).

Thoughout this paper we use the following notation: $\mathbb{R}$ denotes the set of all reals; and $\mathbb{N}$ denotes the set of all natural numbers.

Let E be a real Banach space and P be a subset of E. P is called a *cone* if the following three conditions hold:

(1) P is closed, nonempty, and $P \neq \{0\}$,
(2) $a, b \in \mathbb{R}$, $a, b \geq 0, x, y \in P \Rightarrow ax + by \in P$, and
(3) $x \in P$ and $-x \in P \Rightarrow x = 0$.

Given a cone $P \subset E$, we define a partial order $\leq$ with respect to P by $x \leq y$ if and only if $y - x \in P$. In this case we call P an order cone. We write $x < y$ if $x \leq y$ and $x \neq y$; we write $x \ll y$ if $y - x \in int\ P$, where $int\ P$ denotes the interior of P.

2000 *Mathematics Subject Classification.* 47H10, 54H25, 55M20.
Key words and phrases. Cone metric spaces; generalized contraction pair; Zamfirescu pair; common fixed points.

.

An order cone P is called *normal* if there is a number $K > 0$ such that for all $x, y \in E$,

$$0 \leq x \leq y \text{ implies } \| x \| \leq K \| y \| .$$

The least positive number satisfying the above inequality is called the normal constant of P.

Rezapour and Hamlbarani [4] observed that there is no normal cone with normal constant $K < 1$. There exists an ordered Banach space E with cone P which is not normal but $\text{int}P \neq \emptyset$.

Definition 1.1. Let X be a nonempty set. If the mapping $d : X \times X \to E$ satisfies

(1) $0 \leq d(x, y)$ for all $x, y \in X$ and $d(x, y) = 0$ if and only if $x = y$,
(2) $d(x, y) = d(y, x)$, for all $x, y \in X$, and
(3) $d(x, y) \leq d(x, z) + d(z, y)$, for all $x, y, z \in X$,

then d is called a *cone metric* on X, and (X, d) is called *a cone metric space.*

Definition 1.2. Let (X, d) be a cone metric space and let $\{x_n\}$ be a sequence in X. We say that $\{x_n\}$ is

(1) a Cauchy sequence in X if for each c in E with $0 \ll c$, there is an N such that for all $m, n > N$, $d(x_m, x_n) \ll c$;
(2) a convergent sequence in X if for each c in E with $0 \ll c$, there is an N such that for all $n > N$, $d(x_n, x) \ll c$ for some x in X. In this case, we say that $\{x_n\}$ converges to x in X and we denote it by $\lim_{n\to\infty} x_n = x$ or $x_n \to x$ as $n \to \infty$.

A cone metric space is said to be *complete* if every Cauchy sequence in X is convergent in X.

Remark 1.3. [3] Let E be an ordered Banach (normed) space with a cone P.

(1) c is an interior point of the cone P if and only if $[-c, c]$ is a neighborhood of 0.
(2) If $a \leq b$ and $b \ll c$, then $a \ll c$.
(3) If $a \ll b$ and $b \ll c$, then $a \ll c$.
(4) If $0 \leq u \ll c$ for each $c \in \text{int}P$, then $u = 0$.
(5) If $c \in \text{int}P$, $0 \leq a_n$ and $a_n \to 0$, then there exists n_0 such that for all $n > n_0$ we have $a_n \ll c$.
(6) Let $0 \ll c$. If $0 \leq d(x_n, x) \leq b_n$ and $b_n \to 0$, then eventually $d(x_n, x) \ll c$, where $\{x_n\}$ is a sequence in X and x is a given point in X.
(7) If $a_n \leq b_n$ and $a_n \to a$, $b_n \to b$, then $a \leq b$ for each cone P.
(8) If E is a real Banach space with cone P and $a \leq \lambda a$ where $a \in P$ and $0 < \lambda < 1$, then $a = 0$.

From Remark 1.3 (4) and (5), we observe that if a sequence $\{x_n\}$ is convergent in a cone metric space with a cone P having nonempty interior, then the limit of $\{x_n\}$ is unique.

Definition 1.4. [3] Let (X, d) be a cone metric space and P a cone with nonempty interior. Suppose that the mappings $f, g : X \to X$ are such that $f(X) \subset g(X)$, and $f(X)$ or $g(X)$ is a complete subspace of X. Then the pair (f, g) is called Abbas and Jungck's pair, or shortly AJ's pair.

Definition 1.5. [3]. Let f and g be selfmaps of a set X. If $w = fx = gx$ for some x in X, then x is called a coincidence point of f and g, and w is called a point of coincidence of f and g. f and g are said to be weakly compatible if they commute at their coincidence point; that is, if $fx = gx$ for some x in X, then $fgx = gfx$.

Recently, Jungck *et. al.* [3] proved the following theorems.

Theorem 1.6. (Jungck *et. al.* [3], Theorem 2.1). *Suppose that (f, g) is AJ's pair, and that for some constant $k \in (0, 1)$ and for every $x, y \in X$, there exists*

$$p(x, y) \in \{d(gx, gy), d(fx, gx), d(fy, gy), \frac{d(fx, gy) + d(fy, gx)}{2}\}, \tag{1.6.1}$$

such that

$$d(fx, fy) \leq k\ p(x, y). \tag{1.6.2}$$

Then f and g have a unique point of coincidence in X. Moreover, if f and g are weakly compatible, then f and g have a unique common fixed point in X.

Theorem 1.7. (Jungck *et. al.* [3], Theorem 2.2). *Suppose that (f, g) is AJ's pair, and that for some constant $k \in (0, 1)$ and for every $x, y \in X$, there exists*

$$p(x, y) \in \{d(gx, gy), \frac{d(fx, gx) + d(fy, gy)}{2}, \frac{d(fx, gy) + d(fy, gx)}{2}\}, \tag{1.7.1}$$

such that

$$d(fx, fy) \leq k\ p(x, y). \tag{1.7.2}$$

Then f and g have a unique point of coincidence in X. Moreover, if f and g are weakly compatible, then f and g have a unique common fixed point in X.

We now introduce a generalized contraction pair of mappings.

Definition 1.8. Let (X, d) be a cone metric space and P a cone with nonempty interior. Let $f, g : X \to X$ be selfmaps. Suppose that there exists a constant $k \in (0, 1)$ and there exists

$$p(x, y) \in \{d(x, y), d(x, fx), d(y, gy), \frac{d(x, gy) + d(y, fx)}{2}\}, \tag{1.8.1}$$

such that

$$d(fx, gy) \leq k\ p(x, y) \text{ for all } x, y \text{ in } X. \tag{1.8.2}$$

Then the pair (f, g) is called a generalized contraction pair on X.

The following examples, Example 1.9 and Example 1.10, show that a pair of maps that satisfies inequality (1.6.2) and a generalized contraction pair are independent.

Example 1.9. Let $X = [0, 1]$, $E = C^1_{\mathbb{R}}[0, 1]$ and $P = \{\varphi \in E : \varphi \geq 0\}$. Then P is a cone with nonempty interior. We observe that P is not normal [4].
We define $d : X \times X \to E$ by $d(x, y) = |x - y|\varphi$, where $\varphi : [0, 1] \to \mathbb{R}$ by $\varphi(t) = e^t$. Then d is a cone metric on X. We define mappings $f, g : X \to X$ by

$$f(x) = \begin{cases} \frac{1}{3}x & \text{if } 0 \leq x < \frac{5}{6} \\ \frac{1}{3} & \text{if } \frac{5}{6} \leq x \leq 1 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 0 & \text{if } 0 \leq x < \frac{5}{6} \\ \frac{1}{3}x & \text{if } \frac{5}{6} \leq x \leq 1. \end{cases}$$

We observe that the pair (f, g) is a generalized contraction pair with $k = \frac{4}{5}$.

We also observe that neither $f(X) \subset g(X)$ nor $g(X) \subset f(X)$. Hence the pair (f, g) is not AJ's pair. Also, f and g do not satisfy the inequality (1.6.2). For we choose $x = 0$ and $y = 1$. Then for all $k \in (0, 1)$ we have

$$\frac{1}{3}\varphi = d(f0, f1) > k\ p(0, 1),$$

where

$$p(0,1) \in \{d(g0,g1), d(f0,g0), d(f1,g1), \frac{d(f0,g1)+d(f1,g0)}{2}\} = \{0, \frac{1}{3}\varphi\};$$

and

$$\frac{1}{3}\varphi = d(g0, g1) > k\ p(0, 1),$$

where

$$p(0,1) \in \{d(f0,f1), d(g0,f0), d(g1,f1), \frac{d(g0,f1)+d(g1,f0)}{2}\} = \{0, \frac{1}{3}\varphi\}.$$

Example 1.10. Let $X = \mathbb{R}$, $E = C^1_{\mathbb{R}}[0, 1]$ and $P = \{\varphi \in E : \varphi \geq 0\}$.
We define $d : X \times X \to E$ by $d(x, y) = |x - y|\varphi$, where $\varphi : [0, 1] \to \mathbb{R}$ by $\varphi(t) = e^t$. Then d is a cone metric on X. We define mappings $f, g : X \to X$ by

$$f(x) = \begin{cases} \frac{1}{3}x - 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} x - 2 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

Then f and g satisfy the inequality (1.6.2) with $k = \frac{1}{2}$. However, the pair (f, g) is not a generalized contraction pair. For, we choose $x = 2$ and $y = -1$. Then, for all $k \in (0, 1)$, we have

$$3\varphi = d(f2, g(-1)) > k\ p(2, -1),$$

where

$$p(2,-1) \in \{d(2,-1), d(2,f2), d(-1,g(-1)), \frac{d(2,g(-1))+d(-1,f2)}{2}\} = \{2\varphi, 3\varphi\}.$$

We now introduce a Zamfirescu pair in a cone metric space.

Definition 1.11. Let (X, d) be a cone metric space and P a cone with nonempty interior. Let $f, g : X \to X$ be selfmaps. Suppose that there exists a constant $k \in (0, 1)$ and there exists

$$p(x, y) \in \{d(x, y), \frac{d(x, fx) + d(y, gy)}{2}, \frac{d(x, gy) + d(y, fx)}{2}\}, \tag{1.11.1}$$

such that

$$d(fx, gy) \leq k\ p(x, y) \text{ for all } x, y \text{ in } X. \tag{1.11.2}$$

Then the pair (f, g) is called a Zamfirescu pair on X.

The following examples, Example 1.12 and Example 1.13, show that a pair of maps that satisfies inequality (1.7.2) and a Zamfirescu pair are independent.

Example 1.12. Let X, E, P, d and φ be as in Example 1.9.

We define mappings $f, g : X \to X$ by

$$f(x) = \begin{cases} \frac{1}{4}x & \text{if } x \neq 1 \\ \frac{1}{5} & \text{if } x = 1 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} \frac{1}{5}x & \text{if } x \neq 1 \\ \frac{1}{4} & \text{if } x = 1. \end{cases}$$

We observe that the pair (f, g) is a Zamfirescu pair with $k = \frac{2}{3}$.

We also observe that neither $f(X) \subset g(X)$ nor $g(X) \subset f(X)$. Hence the pair (f, g) is not AJ's pair. Also, f and g do not satisfy the inequality (1.7.2). For, by choosing $x = 0$ and $y = \frac{1}{2}$, and for all $k \in (0, 1)$ we obtain

$$\frac{1}{8}\varphi = d(f0, f\frac{1}{2}) > k\ p(0, \frac{1}{2}),$$

where

$$p(0, \frac{1}{2}) \in \{d(g0, g\frac{1}{2}), \frac{d(f0, g0) + d(f\frac{1}{2}, g\frac{1}{2})}{2}, \frac{d(f0, g\frac{1}{2}) + d(f\frac{1}{2}, g0)}{2}\} = \{\frac{1}{10}\varphi, \frac{1}{80}\varphi, \frac{9}{80}\varphi\},$$

Now, by taking $x = 0$ and $y = 1$, for all $k \in (0, 1)$ we obtain

$$\frac{1}{4}\varphi = d(g0, g1) > k\ p(0, 1),$$

where

$$p(0, 1) \in \{d(f0, f1), \frac{d(g0, f0) + d(g1, f1)}{2}, \frac{d(g0, f1) + d(g1, f0)}{2}\} = \{\frac{1}{5}\varphi, \frac{1}{40}\varphi, \frac{9}{40}\varphi\}.$$

Example 1.13. Let X, E, P, d, φ, f and g be as in Example 1.10.
Then f and g satisfy the inequality (1.7.2) with $k = \frac{1}{2}$. However, the pair (f, g) is not a Zamfirescu pair. For, we choose $x = 2$ and $y = -1$. Then, for all $k \in (0, 1)$, we have

$$3\varphi = d(f2, g(-1)) > k\ p(2, -1),$$

where

$$\begin{aligned} p(2, -1) &\in \{d(2, -1), \frac{d(2, f2) + d(-1, g(-1))}{2}, \frac{d(2, g(-1)) + d(-1, f2)}{2}\} \\ &= \{2\varphi, \frac{5}{2}\varphi, 3\varphi\}. \end{aligned}$$

The aim of this paper is to prove the existence of common fixed points of a generalized contraction pair in a complete cone metric space. The same is also established for Zamfirescu pair in Section 3. Our results generalize the results of Huang and Zhang [2] and extend the results of Rezapour and Hamlbarani [4].

2. Common fixed point theorems of a generalized contraction pair

Theorem 2.1. *Let (X, d) be a complete cone metric space. Suppose that (f, g) is a generalized contraction pair on X. Then f and g have a unique common fixed point in X.*

Proof. Let $x_0 \in X$. Since $f(X) \subset X$, there exists $x_1 \in X$ such that $x_1 = fx_0$. Since $g(X) \subset X$, there exists $x_2 \in X$ such that $x_2 = gx_1$. By continuing this process, having defined $x_n \in X$, we define $x_{n+1} \in X$ such that

$$x_{n+1} = \begin{cases} fx_n & \text{if } n = 0, 2, 4, \cdots \\ gx_n & \text{if } n = 1, 3, 5, \cdots . \end{cases}$$

We first show that

$$d(x_{n+1}, x_n) \leq k\ d(x_n, x_{n-1}),\ \text{for } n = 1, 2, 3, \cdots . \tag{2.1.1}$$

We consider two cases.

Case (i): n is even. Then,

$$d(x_{n+1}, x_n) = d(fx_n, gx_{n-1}) \leq k\ p(x_n, x_{n-1}),$$

where

$$p(x_n, x_{n-1}) \in \{d(x_n, x_{n-1}), d(x_n, fx_n), d(x_{n-1}, gx_{n-1}), \frac{d(x_n, gx_{n-1}) + d(x_{n-1}, fx_n)}{2}\}$$

$$= \{d(x_n, x_{n-1}), d(x_{n+1}, x_n), \frac{1}{2}d(x_{n+1}, x_{n-1})\}.$$

Now if $p(x_n, x_{n-1}) = d(x_n, x_{n-1})$, then clearly (2.1.1) holds;
if $p(x_n, x_{n-1}) = d(x_{n+1}, x_n)$, then from Remark 1.3 (8), we have $d(x_{n+1}, x_n) = 0$, and hence (2.1.1) holds;
if $p(x_n, x_{n-1}) = \frac{1}{2}d(x_{n+1}, x_{n-1})$, then we have

$$d(x_{n+1}, x_n) \leq \frac{1}{2}d(x_{n+1}, x_n) + \frac{k}{2}d(x_n, x_{n-1}),$$

and hence (2.1.1) holds.
Case (ii): n is odd. Then,

$$d(x_{n+1}, x_n) = d(gx_n, fx_{n-1}) = d(fx_{n-1}, gx_n) \leq k\ p(x_{n-1}, x_n),$$

where

$$p(x_{n-1}, x_n) \in \{d(x_{n-1}, x_n), d(x_{n-1}, fx_{n-1}), d(x_n, gx_n), \frac{d(x_{n-1}, gx_n) + d(x_n, fx_{n-1})}{2}\}$$

$$= \{d(x_n, x_{n-1}), d(x_{n+1}, x_n), \frac{1}{2}d(x_{n+1}, x_{n-1})\}.$$

Now if $p(x_{n-1}, x_n) = d(x_n, x_{n-1})$, then clearly (2.1.1) holds;
if $p(x_{n-1}, x_n) = d(x_{n+1}, x_n)$, then from Remark 1.3 (8), we have $d(x_{n+1}, x_n) = 0$, and hence (2.1.1) holds;
if $p(x_{n-1}, x_n) = \frac{1}{2}d(x_{n+1}, x_{n-1})$, then we have

$$d(x_{n+1}, x_n) \leq \frac{1}{2}d(x_{n+1}, x_n) + \frac{k}{2}d(x_n, x_{n-1}),$$

and hence (2.1.1) holds.

Hence, in both cases the inequality (2.1.1) holds.

By repeated application of (2.1.1), we get

$$d(x_{n+1}, x_n) \leq k^n\ d(x_1, x_0),\ n = 1, 2, \cdots . \tag{2.1.2}$$

We show that $\{x_n\}$ is a Cauchy sequence in X. For $n > m$, we have

$$\begin{aligned} d(x_n, x_m) &\leq d(x_n, x_{n-1}) + d(x_{n-1}, x_{n-2}) + \cdots + d(x_{m+1}, x_m) \\ &\leq (k^{n-1} + k^{n-2} + \cdots + k^m)d(x_1, x_0) \\ &\leq \frac{k^m}{1-k}d(x_1, x_0) \to 0 \text{ as } m \to \infty. \end{aligned} \tag{2.1.3}$$

Let $0 \ll c$. From (2.1.3) and Remark 1.3 (5), there exists an integer N such that $k^m(1-k)^{-1}d(x_1, x_0) \ll c$ for all $m > N$. By Remark 1.3 (2), $d(x_n, x_m) \ll c$. Hence, by Definition 1.2 (1), $\{x_n\}$ is a Cauchy sequence in X. By the completeness of X, there exists z in X such that $x_n \to z$ as $n \to \infty$.

We claim that $fz = z$.

Let $0 \ll c$. Without loss of generality we assume that n is odd. Then,

$$\begin{aligned} d(fz, z) &\leq d(fz, gx_n) + d(gx_n, z) \\ &\leq k\ p(z, x_n) + d(x_{n+1}, z), \end{aligned} \tag{2.1.4}$$

where

$$p(z,x_n) \in \{d(z,x_n), d(z,fz), d(x_n,gx_n), \frac{d(z,gx_n)+d(x_n,fz)}{2}\}$$

$$= \{d(z,x_n), d(z,fz), d(x_n,x_{n+1}), \frac{d(z,x_{n+1})+d(x_n,fz)}{2}\}.$$

Clearly one of the following cases hold for infinitely many n.
If $p(z,x_n) = d(z,x_n)$, then from (2.1.4) we have

$$d(fz,z) \leq k\ d(z,x_n) + d(x_{n+1},z) \ll k\ \frac{c}{2k} + \frac{c}{2} = c;$$

if $p(z,x_n) = d(z,fz)$, then from (2.1.4) we get

$$d(fz,z) \leq \frac{1}{1-k}\ d(z,x_{n+1}) \ll \frac{1}{1-k}\ \frac{c}{\frac{1}{1-k}} = c;$$

if $p(z,x_n) = d(x_n,x_{n+1})$, then from (2.1.4) we get

$$d(fz,z) \leq k\ d(x_n,z) + (1+k)\ d(x_{n+1},z) \ll k\ \frac{c}{2k} + (1+k)\frac{c}{2(1+k)} = c;$$

if $p(z,x_n) = \frac{d(z,x_{n+1})+d(x_n,fz)}{2}$, then from (2.1.4) we get

$$d(fz,z) \leq k\ \frac{d(z,x_{n+1})+d(x_n,fz)}{2} + d(x_{n+1},z)$$

$$\leq (1+\frac{k}{2})\ d(z,x_{n+1}) + \frac{k}{2}\ d(x_n,z) + \frac{1}{2}d(z,fz)$$

so that

$$d(fz,z) \leq (2+k)\ d(z,x_{n+1}) + k\ d(x_n,z) \ll (2+k)\ \frac{c}{2(2+k)} + k\frac{c}{2k} = c.$$

In all cases, we obtain $d(fz,z) \ll c$ for each $c \in \text{int } P$. Using Remark 1.3 (4), it follows that $d(fz,z) = 0$, or $fz = z$.

Next we prove that $gz = z$.
Consider

$$d(z,gz) = d(fz,gz) \leq k\ p(z,z), \tag{2.1.5}$$

where

$$p(z,z) \in \{d(z,z), d(z,fz), d(z,gz), \frac{d(z,fz)+d(z,gz)}{2}\}$$

$$= \{0, d(z,gz), \frac{d(z,gz)}{2}\}.$$

Now, if $p(z,z) = 0$, from (2.1.5) trivially we get $gz = z$. If either $p(z,z) = \frac{d(z,gz)}{2}$ or $p(z,z) = d(z,gz)$, then from (2.1.5) and Remark 1.3 (8), we have $d(z,gz) = 0$; i.e., $z = gz$.

Hence, $fz = gz = z$.

The uniqueness of z follows from the inequality (1.8.2). Hence the theorem follows. □

The following is an example in support of Theorem 2.1.

Example 2.2. Let X, E, P, d, φ, f and g be as in Example 1.9.

The pair (f, g) is a generalized contraction pair with $k = \frac{4}{5}$; and the maps f and g satisfy all the conditions of Theorem 2.1 and 0 is the unique common fixed point of f and g.

3. Common fixed point theorems of Zamfirescu pair

In the following theorem, we prove a common fixed point theorem in cone metric spaces which is an analog of the well-known Zamfirescu result in metric spaces [6].

Theorem 3.1. *Let (X, d) be a complete cone metric space. Suppose that (f, g) is a Zamfirescu pair on X. Then f and g have a unique common fixed point in X.*

Proof. Let $x_0 \in X$. Since $f(X) \subset X$, there exists $x_1 \in X$ such that $x_1 = fx_0$. Since $g(X) \subset X$, there exists $x_2 \in X$ such that $x_2 = gx_1$. By continuing this process, having defined $x_n \in X$, we can define $x_{n+1} \in X$ such that

$$x_{n+1} = \begin{cases} fx_n & if\ n = 0, 2, 4, \cdots \\ gx_n & if\ n = 1, 3, 5, \cdots . \end{cases}$$

We first show that

$$d(x_{n+1}, x_n) \leq k\ d(x_n, x_{n-1}),\ \text{for } n = 1, 2, 3, \cdots . \tag{3.1.1}$$

We consider two cases.
Case (i): n is even. Then,

$$d(x_{n+1}, x_n) = d(fx_n, gx_{n-1}) \leq k\ p(x_n, x_{n-1}),$$

where

$$p(x_n, x_{n-1}) \in \{d(x_n, x_{n-1}), \frac{d(x_n, fx_n) + d(x_{n-1}, gx_{n-1})}{2}, \frac{d(x_n, gx_{n-1}) + d(x_{n-1}, fx_n)}{2}\}$$
$$= \{d(x_n, x_{n-1}), \frac{d(x_{n+1}, x_n) + d(x_n, x_{n-1})}{2}, \frac{1}{2}d(x_{n+1}, x_{n-1})\}.$$

Now if $p(x_n, x_{n-1}) = d(x_n, x_{n-1})$, then clearly (3.1.1) holds;
if $p(x_n, x_{n-1}) = \frac{d(x_{n+1}, x_n) + d(x_n, x_{n-1})}{2}$, then we have

$$d(x_{n+1}, x_n) \leq k\ \frac{d(x_{n+1}, x_n) + d(x_n, x_{n-1})}{2}$$
$$\leq \frac{1}{2}d(x_{n+1}, x_n) + \frac{k}{2}d(x_n, x_{n-1}),$$

and hence (3.1.1) holds;
if $p(x_n, x_{n-1}) = \frac{1}{2}d(x_{n+1}, x_{n-1})$, then we have

$$d(x_{n+1}, x_n) \leq \frac{1}{2}d(x_{n+1}, x_n) + \frac{k}{2}d(x_n, x_{n-1}),$$

and hence (3.1.1) holds.
Case (ii): n is odd. Then,

$$d(x_{n+1}, x_n) = d(gx_n, fx_{n-1}) = d(fx_{n-1}, gx_n) \leq k\ p(x_{n-1}, x_n),$$

where

$$p(x_{n-1}, x_n) \in \{d(x_{n-1}, x_n), \frac{d(x_{n-1}, fx_{n-1}) + d(x_n, gx_n)}{2}, \frac{d(x_{n-1}, gx_n) + d(x_n, fx_{n-1})}{2}\}$$

$$= \{d(x_n, x_{n-1}), \frac{d(x_{n+1}, x_n) + d(x_n, x_{n-1})}{2}, \frac{1}{2}d(x_{n+1}, x_{n-1})\}.$$

Now if $p(x_{n-1}, x_n) = d(x_n, x_{n-1})$, then clearly (3.1.1) holds;
if $p(x_{n-1}, x_n) = \frac{d(x_{n+1},x_n)+d(x_n,x_{n-1})}{2}$, then we have

$$\begin{aligned} d(x_{n+1}, x_n) &\leq k\ \frac{d(x_{n+1}, x_n) + d(x_n, x_{n-1})}{2} \\ &\leq \frac{1}{2}d(x_{n+1}, x_n) + \frac{k}{2}d(x_n, x_{n-1}), \end{aligned}$$

and hence (3.1.1) holds;
if $p(x_{n-1}, x_n) = \frac{1}{2}d(x_{n+1}, x_{n-1})$, then we have

$$d(x_{n+1}, x_n) \leq \frac{1}{2}d(x_{n+1}, x_n) + \frac{k}{2}d(x_n, x_{n-1}),$$

and hence (3.1.1) holds.

Hence, in both cases the inequality (3.1.1) holds.

By repeated application of (3.1.1), we get

$$d(x_{n+1}, x_n) \leq k^n\ d(x_1, x_0),\ n = 1, 2, \cdots . \tag{3.1.2}$$

We show that $\{x_n\}$ is a Cauchy sequence in X. For $n > m$, we have

$$\begin{aligned} d(x_n, x_m) &\leq d(x_n, x_{n-1}) + d(x_{n-1}, x_{n-2}) + \cdots + d(x_{m+1}, x_m) \\ &\leq (k^{n-1} + k^{n-2} + \cdots + k^m)d(x_1, x_0) \\ &\leq \frac{k^m}{1-k}d(x_1, x_0) \to 0 \text{ as } m \to \infty. \end{aligned} \tag{3.1.3}$$

Let $0 \ll c$. From (3.1.3) and Remark 1.3 (5), there exists an integer N such that $k^m(1-k)^{-1}d(x_1, x_0) \ll c$ for all $m > N$. By Remark 1.3 (2), $d(x_n, x_m) \ll c$. Hence, by Definition 1.2 (1), $\{x_n\}$ is a Cauchy sequence in X. By the completeness of X, there exists z in X such that $x_n \to z$ as $n \to \infty$.

We claim that $fz = z$.

Let $0 \ll c$. Without loss of generality we assume that n is odd. Then,

$$\begin{aligned} d(fz, z) &\leq d(fz, gx_n) + d(gx_n, z) \\ &\leq k\ p(z, x_n) + d(x_{n+1}, z), \end{aligned} \tag{3.1.4}$$

where

$$\begin{aligned} p(z, x_n) &\in \{d(z, x_n), \frac{d(z, fz) + d(x_n, gx_n)}{2}, \frac{d(z, gx_n) + d(x_n, fz)}{2}\} \\ &= \{d(z, x_n), \frac{d(z, fz) + d(x_n, x_{n+1})}{2}, \frac{d(z, x_{n+1}) + d(x_n, fz)}{2}\}. \end{aligned}$$

Clearly one of the following cases hold for infinitely many n.
If $p(z, x_n) = d(z, x_n)$, then from (3.1.4) we have

$$d(fz, z) \leq k\ d(z, x_n) + d(x_{n+1}, z) \ll k\ \frac{c}{2k} + \frac{c}{2} = c;$$

if $p(z, x_n) = \frac{d(z,fz)+d(x_n,x_{n+1})}{2}$, then from (3.1.4) we get

$$\begin{aligned} d(fz, z) &\leq k\ \frac{d(z, fz) + d(x_n, x_{n+1})}{2} + d(x_{n+1}, z) \\ &\leq (1 + \frac{k}{2})\ d(z, x_{n+1}) + \frac{k}{2}\ d(x_n, z) + \frac{1}{2}d(z, fz), \end{aligned}$$

so that

$$d(fz,z) \leq (2+k)\ d(z,x_{n+1}) + k\ d(x_n,z) \ll (2+k)\ \frac{c}{2(2+k)} + k\frac{c}{2k} = c.$$

if $p(z,x_n) = \frac{d(z,x_{n+1})+d(x_n,fz)}{2}$, then from (3.1.4) we get

$$\begin{aligned} d(fz,z) &\leq k\ \frac{d(z,x_{n+1}) + d(x_n,fz)}{2} + d(x_{n+1},z) \\ &\leq (1+\frac{k}{2})\ d(z,x_{n+1}) + \frac{k}{2}\ d(x_n,z) + \frac{1}{2}d(z,fz), \end{aligned}$$

so that

$$d(fz,z) \leq (2+k)\ d(z,x_{n+1}) + k\ d(x_n,z) \ll (2+k)\ \frac{c}{2(2+k)} + k\frac{c}{2k} = c.$$

In all cases, we obtain $d(fz,z) \ll c$ for each $c \in \text{int } P$. Using Remark 1.3 (4), it follows that $d(fz,z) = 0$, or $fz = z$.

Next we prove that $gz = z$.
Consider

$$d(z,gz) = d(fz,gz) \leq k\ p(z,z), \tag{3.1.5}$$

where

$$\begin{aligned} p(z,z) &\in \{d(z,z), \frac{d(z,gz)+d(z,fz)}{2}, \frac{d(z,fz)+d(z,gz)}{2}\} \\ &= \{0, \frac{d(z,gz)}{2}\}. \end{aligned}$$

Now if $p(z,z) = 0$, from (3.1.5) trivially we get $gz = z$. If $p(z,z) = \frac{d(z,gz)}{2}$, then from (3.1.5) and Remark 1.3 (8), we have $d(z,gz) = 0$; i.e., $z = gz$.

Hence, $fz = gz = z$.

The uniqueness of z follows from the inequality (1.11.2). Hence the theorem follows. □

The following is an example in support of Theorem 3.1.

Example 3.2. Let X, E, P, d, φ, f and g be as in Example 1.12.
The pair (f,g) is a Zamfirescu pair with $k = \frac{2}{3}$; and the maps f and g satisfy all the conditions of Theorem 3.1 and 0 is the unique common fixed point of f and g.

The following are corollaries which follow from Theorem 3.1.

Corollary 3.3. *Let (X,d) be a complete cone metric space and P a cone with nonempty interior. Let $f,g : X \to X$ be selfmaps. Suppose that for some constant $k \in (0,1)$ and for every $x,y \in X$,*

$$d(fx,gy) \leq k\ d(x,y).$$

Then f and g have a unique common fixed point in X.

Corollary 3.4. *Let (X,d) be a complete cone metric space and P a cone with nonempty interior. Let $f,g : X \to X$ be selfmaps. Suppose that for some constant $k \in (0,\frac{1}{2})$ and for every $x,y \in X$,*

$$d(fx,gy) \leq k\ [d(x,fx) + d(y,gy)].$$

Then f and g have a unique common fixed point in X.

Corollary 3.5. *Let (X, d) be a complete cone metric space and P a cone with nonempty interior. Let $f, g : X \to X$ be selfmaps. Suppose that for some constant $k \in (0, \frac{1}{2})$ and for every $x, y \in X$,*

$$d(fx, gy) \leq k\ [d(x, gy) + d(y, fx)].$$

Then f and g have a unique common fixed point in X.

Remark 3.6. Corollary 3.3, Corollary 3.4 and Corollary 3.5 are extensions of Theorem 2.3, Theorem 2.4 and Theorem 2.5 of Rezapour and Hamlbarani [4] respectively and hence generalize some results of Huang and Zhang [2] since we do not use the assumption 'normality of cone' in our results.

References

[1] M. Abbas, G. Jungck, "Common fixed point results for noncommuting mappings without continuity in cone metric spaces", J. Math. Anal. Appl. 341 (1) (2008), 416–420.

[2] L-G. Huang, X. Zhang, Cone metric spaces and fixed point theorems of contractive mappings, J. Math. Anal. Appl. 332 (2007) 1468–1476.

[3] G. Jungck, S. Radenović, S. Radojević, V. Rakočević," Common fixed point theorems for weakly compatible pairs on cone metric spaces", Fixed point theory and applications, 2009, ID: 643840, 13 pages.

[4] Sh. Rezapour, R. Hamlbarani, "Some notes on the paper "Cone metric spaces and fixed point theorems of contractive mappings"", J. Math. Anal. Appl. 345 (2008) 719–724.

[5] P. Vetro, "Common fixed points in cone metric spaces", Rendiconti del circolo Matematico di Palermo, 56 (3) (2007), 461–468.

[6] T. Zamfirescu, "Fix point theorems in metric spaces", Arch. Math. (Basel), 23 (1972), 292–298.

*Department of Mathematics, Andhra University, Visakhapatnam-530 003, India.
E-mail address: gvr_babu@hotmail.com

†Department of Mathematics, Jimma University, Jimma, P.O.Box 378, Ethiopia.
Current address: Department of Mathematics, Andhra University, Visakhapatnam-530 003, India.
E-mail address: alemg1972@gmail.com

‡Department of Mathematics, Dr. L. B. College, Visakhapatnam-530 013, India.
E-mail address: knvp71@yahoo.co.in

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 2, Pages 31–47
ISSN 1930-1235: (2010)

MAPPINGS AND DECOMPOSITIONS OF PAIRWISE CONTINUITY ON PAIRWISE NEARLY LINDELÖF SPACES

A. KILIÇMAN AND Z. SALLEH

Abstract. The purpose of this paper is to study the effect of mappings, some decompositions of pairwise continuity and some generalized pairwise open mappings on pairwise nearly Lindelöf spaces. The main result indicates that a pairwise δ-continuous image of a pairwise nearly Lindelöf space is pairwise nearly Lindelöf.

1. Introduction

In literature there are several generalizations of the notion of Lindelöf spaces and these are studied separately for different reasons and purposes. In 1982, Balasubramaniam [1] introduced and studied the notion of nearly Lindelöf spaces. Then in 1996, Cammaroto and Santoro [2] studied and gave further new results about these spaces which are considered as one of the main generalizations of Lindelöf spaces. Recently the authors introduced and studied the notion of pairwise Lindelöf spaces [9] and pairwise nearly Lindelöf spaces [18] and pairwise weakly regular-Lindelf spaces [12] as well as pairwise almost Lindelöf spaces in bitopological setting, see [10] and extended some results due to Balasubramaniam [1] and Cammaroto and Santoro [2].

Our purpose in this paper is to study the decompositions of pairwise continuity concepts, openness and closedness functions and its generalizations concepts, and mappings on pairwise nearly Lindelöf spaces in a suitable way of bitopological spaces after the manner of Fawakhreh and Kılıçman [5]. We extend most of their results in topological spaces to bitopological spaces.

The concepts of continuous functions and its generalizations have been introduced and studied in topological spaces. In [11, 13], the authors studied the pairwise Lindelöfness and pairwise continuity, the authors also introduced and studied the pairwise almost regular-Lindelöf bitopological spaces, their subspaces and subsets, and investigated some of their characterizations (see [14]). In this paper we extend the previous types of continuity to bitopological spaces and investigate their relationships. Moreover, the concepts of open and closed functions and its generalizations also have been introduced and studied in topological spaces. We extend these types of openness and closedness functions to bitopological spaces and investigate their relationship. Some examples and counterexamples will be given in order to establish further relationships.

In section 4, we shall study the effect of mappings, some decompositions of pairwise continuity and some generalized pairwise openness functions on pairwise nearly Lindelöf spaces. We also show that some mappings preserve this property. The main result in our study is that the image of a pairwise nearly Lindelöf space under a pairwise δ-continuous functions is pairwise nearly Lindelöf.

2. Preliminaries

Throughout this paper, all spaces (X, τ) and (X, τ_1, τ_2) (or simply X) are always mean topological spaces and bitopological spaces, respectively. If $\mathcal{P}$ is a topological property, then (τ_i, τ_j)-$\mathcal{P}$ denotes an analogue of this property for τ_i has property $\mathcal{P}$ with respect to τ_j, and p-$\mathcal{P}$ denotes the conjunction (τ_1, τ_2)-$\mathcal{P} \wedge (\tau_2, \tau_1)$-$\mathcal{P}$, i.e., p-$\mathcal{P}$ denotes an absolute bitopological analogue of $\mathcal{P}$. The prefix τ_i-$\mathcal{P}$ denotes the (X, τ_1, τ_2) has a property $\mathcal{P}$ with respect to τ_i. Note that (X, τ_i) has a property $\mathcal{P} \Longleftrightarrow (X, \tau_1, \tau_2)$ has a property τ_i-$\mathcal{P}$.

By τ_i-int (A) and τ_i-cl (A), we shall mean the interior and the closure of a subset A of X with respect to topology τ_i, respectively. By τ_i-open cover of X, we mean that the cover of X by τ_i-open sets in X; similar for the (τ_i, τ_j)-regular open cover of X and etc. The prefixes (τ_i, τ_j)- or τ_i- will be replaced by (i, j)- or i- respectively, if there is no chance for confusion. In this paper always $i, j \in \{1, 2\}$ and $i \neq j$.

The concepts of open, regular open, regular closed, preopen and β-open sets are well known in topological spaces. We extend these concepts to bitopological spaces as follows.

Definition 2.1. *A subset S of a bitopological space (X, τ_1, τ_2) is said to be*

(a) *i-open if S is open with respect to τ_i in X, S is called open in X if it is both 1-open and 2-open, or equivalently, $F \in (\tau_1 \cap \tau_2)$ in X;*
(b) *(i, j)-regular open* [8] *if $S = i$-int $(j$-cl $(S))$, S is called pairwise regular open if it is both $(1, 2)$-regular open and $(2, 1)$-regular open;*
(c) *(i, j)-regular closed* [8] *if $S = i$-cl $(j$-int $(S))$, S is called pairwise regular closed if it is both $(1, 2)$-regular closed and $(2, 1)$-regular closed;*
(d) *(i, j)-preopen if $S \subseteq i$-int $(j$-cl $(S))$, S is called pairwise preopen if it is both $(1, 2)$-preopen and $(2, 1)$-preopen;*
(e) *(i, j)-β-open if $S \subseteq j$-cl $(i$-int $(j$-cl $(S)))$, S is called pairwise β-open if it is both $(1, 2)$-β-open and $(2, 1)$-β-open;*

where $i, j \in \{1, 2\}$ and $i \neq j$.

Definition 2.2 (see [6, 9])**.** *A bitopological space (X, τ_1, τ_2) is said to be i-Lindelöf if the topological space (X, τ_i) is Lindelöf. X is called Lindelöf if it is both 1-Lindelöf and 2-Lindelöf. Equivalently, (X, τ_1, τ_2) is Lindelöf if every i-open cover of X has a countable subcover for each $i = 1, 2$.*

Definition 2.3 (see [7, 8])**.** *A bitopological space (X, τ_1, τ_2) is said to be (i, j)-regular if for each point $x \in X$ and for each i-open set V containing x, there exists an i-open set U such that $x \in U \subseteq j$-cl $(U) \subseteq V$. X is called pairwise regular if it is both $(1, 2)$-regular and $(2, 1)$-regular.*

Definition 2.4 (see [20])**.** *A bitopological space X is said to be (i, j)-almost regular if for each $x \in X$ and for each (i, j)-regular open set V of X containing x, there is*

an (i,j)-regular open set U such that $x \in U \subseteq j\text{-cl}(U) \subseteq V$. The space X is called pairwise almost regular if it is both $(1,2)$-almost regular and $(2,1)$-almost regular.

Definition 2.5 (see [8, 20])**.** *A bitopological space X is said to be (i,j)-semiregular if for each $x \in X$ and for each i-open set V of X containing x, there is an i-open set U such that $x \in U \subseteq i\text{-int}(j\text{-cl}(U)) \subseteq V$. Similarly, X is called pairwise semiregular if it is both $(1,2)$-semiregular and $(2,1)$-semiregular.*

3. Decompositions of Pairwise Continuity and Pairwise Openness

The concepts of R-map, almost continuous, precontinuous, β-continuous, almost precontinuous, almost β-continuous, δ-continuous and almost δ-continuous functions have been introduced by many authors in a topological space (see [3, 5, 15]). These concepts are extended to bitopological spaces as follows.

Definition 3.1. *A function $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ is said to be*

(1) *i-continuous if the functions $f : (X, \tau_i) \to (Y, \sigma_i)$ is continuous, f is called continuous if it is i-continuous for each $i = 1, 2$;*
(2) *(i,j)-R-map if $f^{-1}(V)$ is (τ_i, τ_j)-regular open set in X for every (σ_i, σ_j)-regular open set V in Y, f is called pairwise R-map if it is both $(1,2)$-R-map and $(2,1)$-R-map;*
(3) *(i,j)-almost continuous if $f^{-1}(V)$ is τ_i-open set in X for every (σ_i, σ_j)-regular open set V in Y, f is called pairwise almost continuous if it is both $(1,2)$-almost continuous and $(2,1)$-almost continuous;*
(4) *(i,j)-precontinuous (resp. (i,j)-β-continuous) if $f^{-1}(V)$ is (τ_i, τ_j)-preopen (resp. (τ_i, τ_j)-β-open) set in X for every σ_i-open set V in Y, f is called pairwise precontinuous (resp. pairwise β-continuous) if it is both $(1,2)$-precontinuous (resp. $(1,2)$-β-continuous) and $(2,1)$-precontinuous (resp. $(2,1)$-β-continuous);*
(5) *(i,j)-almost precontinuous (resp. (i,j)-almost β-continuous) if for each $x \in X$ and each (σ_i, σ_j)-regular open set V in Y containing $f(x)$, there exists a (τ_i, τ_j)-preopen (resp. (τ_i, τ_j)-β-open) set U in X containing x such that $f(U) \subseteq V$, f is called pairwise almost precontinuous (resp. pairwise almost β-continuous) if it is both $(1,2)$-almost precontinuous (resp. $(1,2)$-almost β-continuous) and $(2,1)$-almost precontinuous (resp. $(2,1)$-almost β-continuous);*
(6) *(i,j)-δ-continuous (resp. (i,j)-almost δ-continuous) if for each $x \in X$ and each (σ_i, σ_j)-regular open subset V of Y containing $f(x)$, there exists a $((\tau_i, \tau_j))$-regular open subset U of X containing x such that $f(U) \subseteq V$ (resp. $f(U) \subseteq \sigma_j\text{-cl}(V)$), f is called pairwise δ-continuous (resp. pairwise almost δ-continuous) if it is both $(1,2)$-δ-continuous (resp. $(1,2)$-almost δ-continuous) and $(2,1)$-δ-continuous (resp. $(2,1)$-almost δ-continuous).*

Lemma 3.1. *Let $\{A_\alpha : \alpha \in \Delta\}$ be a collection of (i,j)-β-open (resp. (i,j)-preopen) sets in a bitopological space X. Then $\bigcup_{\alpha\in\Delta} A_\alpha$ is (i,j)-β-open (resp. (i,j)-preopen) set in X.*

Proof. We need to prove the (i,j)-β-open part of the lemma. The (i,j)-preopen part can be proved by the similar procedure. For each $\alpha \in \Delta$, since A_α is (i,j)-β-open set in X, we have $A_\alpha \subseteq j\text{-}cl\,(i\text{-}int\,(j\text{-}cl\,(A_\alpha)))$. Then

$$\begin{aligned}\bigcup_{\alpha\in\Delta} A_\alpha &\subseteq \bigcup_{\alpha\in\Delta} j\text{-cl}\,(i\text{-}int\,(j\text{-}cl\,(A_\alpha)))\\ &\subseteq j\text{-}cl\left(\bigcup_{\alpha\in\Delta} i\text{-}int\,(j\text{-}cl\,(A_\alpha))\right)\\ &\subseteq j\text{-}cl\left(i\text{-}int\left(\bigcup_{\alpha\in\Delta} j\text{-}cl\,(A_\alpha)\right)\right)\\ &\subseteq j\text{-}cl\left(i\text{-}int\left(j\text{-}cl\left(\bigcup_{\alpha\in\Delta} A_\alpha\right)\right)\right).\end{aligned}$$

Therefore $\bigcup_{\alpha\in\Delta} A_\alpha$ is (i,j)-β-open set in X. □

Theorem 3.1. *The following are equivalent for a function $f:(X,\tau_1,\tau_2)\to(X,\sigma_1,\sigma_2)$:*

(1) *f is (i,j)-almost precontinuous (resp. (i,j)-almost β-continuous);*
(2) *$f^{-1}(V)$ is (τ_i,τ_j)-preopen (resp. (τ_i,τ_j)-β-open) set in X for every (σ_i,σ_j)-regular open set V in Y.*

Proof. (1) $\Longrightarrow$ (2) : Let V be any (σ_i,σ_j)-regular open set in Y and $x\in f^{-1}(V)$. Then $f(x)\in V$, and by (1), there exists a (τ_i,τ_j)-preopen set U_x in X containing x such that $f(U_x)\subseteq V$. Thus $x\in U_x\subseteq f^{-1}(V)$. Therefore, we obtain $f^{-1}(V)=\bigcup_{x\in f^{-1}(V)} U_x$. This shows that $f^{-1}(V)$ is (τ_i,τ_j)-preopen set in X by Lemma 3.1.

(2) $\Longrightarrow$ (1) : Let $x\in X$ and let V be a (σ_i,σ_j)-regular open set in Y containing $f(x)$. Then $x\in f^{-1}(V)$ and by (2), $f^{-1}(V)$ is (τ_i,τ_j)-preopen set in X. So take $U=f^{-1}(V)$, then U is a (τ_i,τ_j)-preopen set in X containing x such that $f(U)=f\left(f^{-1}(V)\right)\subseteq V$. This shows that f is (i,j)-almost continuous.

The proof for the (i,j)-almost β-continuous is similar. □

Corollary 3.1. *The following are equivalent for a function $f:(X,\tau_1,\tau_2)\to(X,\sigma_1,\sigma_2)$:*

(1) *f is pairwise almost precontinuous (resp. pairwise almost β-continuous);*
(2) *$f^{-1}(V)$ is pairwise preopen (resp. pairwise β-open) set in X for every pairwise regular open set V in Y.*

Proposition 3.1. *If $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ is a pairwise almost continuous function, then f is pairwise almost δ-continuous.*

Proof. Let $x\in X$ and let V be a (σ_1,σ_2)-regular open set in Y containing $f(x)$. Then $x\in f^{-1}(V)$ and since f is $(1,2)$-almost continuous, $f^{-1}(V)$ is a τ_1-open set in X containing x. Since $W=\tau_1\text{-}int\left(\tau_2\text{-}cl\left(f^{-1}(V)\right)\right)$ is a (τ_1,τ_2)-regular open set in X containing x,

$$f(W)=f\left(\tau_1\text{-}int\left(\tau_2\text{-}cl\left(f^{-1}(V)\right)\right)\right)\subseteq f\left(\tau_2\text{-}cl\left(f^{-1}(V)\right)\right).$$

Since f is also $(2,1)$-almost continuous and σ_2-$cl(V)$ is a (σ_2,σ_1)-regular closed set in Y, τ_2-$cl\left(f^{-1}(V)\right) \subseteq f^{-1}(\sigma_2\text{-}cl(V))$ because $f^{-1}(\sigma_2\text{-}cl(V))$ is a τ_2-closed set in X containing $f^{-1}(V)$. So

$$f(W) \subseteq f\left(\tau_2\text{-}cl\left(f^{-1}(V)\right)\right) \subseteq f\left(f^{-1}(\sigma_2\text{-}cl(V))\right) \subseteq \sigma_2\text{-}cl(V).$$

This shows that f is $(1,2)$-almost δ-continuous. Similarly, f is also $(2,1)$-almost δ-continuous and completes the proof. □

The converse of Proposition 3.1 is not true as the following example shows.

Example 3.1. *Let $X = \{a,b,c\}$ with topologies*

$$\tau_1 = \{\emptyset,\{b\},\{a,b\},\{b,c\},X\},\ \tau_2 = \{\emptyset,\{c\},X\}$$

and

$$\sigma_1 = \{\emptyset,\{a\},\{b\},\{a,b\},X\},\ \sigma_2 = \{\emptyset,\{a\},X\}.$$

Let $f : (X,\tau_1,\tau_2) \to (X,\sigma_1,\sigma_2)$ be a function defined by $f(a) = b$ and $f(b) = f(c) = c$. Then f is $(1,2)$-almost δ-continuous as well as $(2,1)$-almost δ-continuous so pairwise almost δ-continuous but it is not $(1,2)$-almost continuous since there exists a (σ_1,σ_2)-regular open set $\{b\}$ in (X,σ_1,σ_2) such that $f^{-1}(\{b\}) = \{a\}$ is not τ_1-open set in (X,τ_1,τ_2). Thus f is not pairwise almost continuous. Even f is $(1,2)$-almost δ-continuous but it is not $(1,2)$-δ-continuous since for the (σ_1,σ_2)-regular open set $\{b\}$ in (X,σ_1,σ_2) containing $f(a) = b$, there is no (τ_1,τ_2)-regular open set U in (X,τ_1,τ_2) containing a such that $f(U) \subseteq \{b\}$. It is also not 1-continuous since $f^{-1}(\{b\}) = \{a\}$ is not τ_1-open set in (X,τ_1,τ_2) while $\{b\}$ is σ_1-open set in (X,σ_1,σ_2).

The following we prove that (i,j)-δ-continuity implies (i,j)-almost continuity but the converse is not true as Example 3.2 below shows.

Proposition 3.2. *If $f : (X,\tau_1,\tau_2) \to (Y,\sigma_1,\sigma_2)$ is (i,j)-δ-continuous function, then f is (i,j)-almost continuous.*

Proof. Let V be a (σ_i,σ_j)-regular open set in Y containing $f(x)$. Since f is (i,j)-δ-continuous function, there exists a (τ_i,τ_j)-regular open set U_x in X containing x such that $f(U_x) \subseteq V$. Then $x \in U_x \subseteq f^{-1}(V)$ and $f^{-1}(V) = \bigcup_{x\in f^{-1}(V)} U_x$. Since every (τ_i,τ_j)-regular open set is τ_i-open, then U_x is τ_i-open set for each x. This implies that $f^{-1}(V)$ is τ_i-open set in X. Therefore f is (i,j)-almost continuous. □

Corollary 3.2. *If $f : (X,\tau_1,\tau_2) \to (Y,\sigma_1,\sigma_2)$ is pairwise δ-continuous function, then f is pairwise almost continuous.*

Observe that, every i-continuous function is (i,j)-almost continuous and every (i,j)-R-map is (i,j)-almost continuous too, but the converses are not true in general. In fact, i-continuity and (i,j)-R-map property are independent as Example 3.2 and Example 3.3 below show. Moreover, Example 3.2 and Example 3.3 below also shows that i-continuity and (i,j)-δ-continuity are independent concepts. Every (i,j)-R-map is (i,j)-δ-continuous by Lemma 4.1 below but the converse is not true in general as Example 4.1 below show. Furthermore, i-continuity and (i,j)-almost δ-continuity are independent concepts as Example 3.1 above and Example 3.2 below show.

It is also very clear that (i,j)-δ-continuity implies (i,j)-almost δ-continuity but the converse is not true in general as Example 3.1 above shows. The Example 3.1 above and Example 3.2 below show that (i,j)-almost continuity and (i,j)-almost δ-continuity are independent concepts. Furthermore, (i,j)-almost continuity as well as (i,j)-precontinuity implies (i,j)-almost precontinuity, and (i,j)-almost precontinuity as well as (i,j)-β-continuity implies (i,j)-almost β-continuity but the converses are not true in general as Example 3.4, Example 3.5 and Example 3.6 below show. It is very clear that i-continuity implies (i,j)-precontinuity and (i,j)-precontinuity implies (i,j)-β-continuity but the converses are not true as we will see in Example 3.7 and Example 3.8 below.

Example 3.2. *Let $X = \{a,b,c\}$ with topologies*

$$\tau_1 = \{\emptyset, \{a\}, \{b\}, \{a,b\}, \{b,c\}, X\},\ \tau_2 = \{\emptyset, \{a\}, \{c\}, \{a,c\}, X\}$$

and

$$\sigma_1 = \{\emptyset, \{a\}, \{c\}, \{a,c\}, X\},\ \sigma_2 = \{\emptyset, \{b,c\}, X\}.$$

Then the function $f : (X,\tau_1,\tau_2) \to (X,\sigma_1,\sigma_2)$ defined by $f(a) = a, f(b) = c$ and $f(c) = b$ is 1-continuous so $(1,2)$-almost continuous. But f is not a $(1,2)$-R-map since $f^{-1}(\{a\}) = \{a\}$ is not (τ_1,τ_2)-regular open set in (X,τ_1,τ_2) while $\{a\}$ is (σ_1,σ_2)-regular open set in (X,σ_1,σ_2). Even f is 1-continuous and $(1,2)$-almost continuous, it is not $(1,2)$-almost δ-continuous since $\{a\}$ is (σ_1,σ_2)-regular open set in (X,σ_1,σ_2) containing $f(a) = a$ but there is no (τ_1,τ_2)-regular open set U in (X,τ_1,τ_2) containing a such that $f(U) \subseteq \sigma_2\text{-}cl\{a\} = \{a\}$. Thus f is also not $(1,2)$-δ-continuous.

Example 3.3. *Let $X = \{a,b,c\}$ with topologies*

$$\tau_1 = \{\emptyset, \{c\}, \{a,b\}, X\},\ \tau_2 = \{\emptyset, \{a\}, \{c\}, \{a,c\}, X\}$$

and

$$\sigma_1 = \{\emptyset, \{a\}, X\},\ \sigma_2 = \{\emptyset, \{a,c\}, X\}.$$

Then the identity function $f : (X,\tau_1,\tau_2) \to (X,\sigma_1,\sigma_2)$ is a $(1,2)$-R-map since $\emptyset$ and X are the only (σ_1,σ_2)-regular open set in (X,σ_1,σ_2). So f is $(1,2)$-δ-continuous and also $(1,2)$-almost continuous. However f is not 1-continuous since $f^{-1}(\{a\}) = \{a\}$ is not τ_1-open set in (X,τ_1,τ_2) while $\{a\}$ is σ_1-open set in (X,σ_1,σ_2).

Example 3.4. *Let $X = \{a,b,c,d\}$ and $Y = \{x,y,z\}$. Define on X the topologies $\tau_1 = \{\emptyset, \{c\}, \{d\}, \{a,c\}, \{c,d\}, \{a,c,d\}, X\}$, $\tau_2 = \{\emptyset, \{c\}, \{a,c\}, X\}$ and on Y define the topologies $\sigma_1 = \{\emptyset, \{x\}, \{x,y\}, Y\}$, $\sigma_2 = \{\emptyset, Y\}$. Let $f : (X,\tau_1,\tau_2) \to (Y,\sigma_1,\sigma_2)$ be a function defined by $f(a) = f(d) = x$, $f(b) = y$ and $f(c) = z$. Then f is a $(1,2)$-R-map thus $(1,2)$-almost continuous, $(1,2)$-almost precontinuous and $(1,2)$-almost β-continuous. But f is not $(1,2)$-β-continuous since $f^{-1}(\{x\}) = \{a,d\}$ is not (τ_1,τ_2)-β-open set in (X,τ_1,τ_2) while $\{x\}$ is σ_1-open set in (Y,σ_1,σ_2). Thus f is neither $(1,2)$-precontinuous nor 1-continuous.*

Example 3.5. *Let $X = \{a,b,c,d\}$ with topologies*

$$\tau_1 = \{\emptyset, \{a\}, \{b\}, \{a,b\}, X\},\ \tau_2 = \{\emptyset, \{a,d\}, X\}$$

and

$$\sigma_1 = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}, X\},\ \sigma_2 = \{\emptyset, \{a,c\}, X\}.$$

Let $f : (X,\tau_1,\tau_2) \to (X,\sigma_1,\sigma_2)$ be a function defined by $f(a) = a$, $f(b) = f(c) = b$ and $f(d) = d$. Then f is $(1,2)$-almost β-continuous since the (σ_1,σ_2)-regular open

subsets of (X, σ_1, σ_2) *are* $\emptyset, \{b\}$ *and* X. *But* f *is not* $(1,2)$*-almost precontinuous by Theorem 3.1 since there exists a* (σ_1, σ_2)*-regular open set* $\{b\}$ *in* (X, σ_1, σ_2) *such that* $f^{-1}(\{b\}) = \{b, c\}$ *is not* (τ_1, τ_2)*-preopen set in* (X, τ_1, τ_2) *because* $\{b, c\} \not\subseteq \tau_1$*-int* $(\tau_2$*-cl* $(\{b, c\})) = \tau_1$*-int* $(\{b, c\}) = \{b\}$.

Example 3.6. *Let* $X = \{a, b, c, d\}$ *with topologies*

$$\tau_1 = \{\emptyset, \{c\}, \{d\}, \{a, c\}, \{c, d\}, \{a, c, d\}, X\}, \ \tau_2 = \{\emptyset, \{b\}, X\}$$

and let $Y = \{x, y, z\}$ *with topologies*

$$\sigma_1 = \{\emptyset, \{x\}, \{y\}, \{x, y\}, Y\}, \ \sigma_2 = \{\emptyset, \{x\}, Y\}.$$

Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ *be a function defined by* $f(a) = z$ *and* $f(b) = f(c) = f(d) = y$. *Then* f *is* $(1,2)$*-almost precontinuous since the* (σ_1, σ_2)*-regular open sets in* (Y, σ_1, σ_2) *are* $\emptyset, \{y\}$ *and* Y. *But* f *is not* $(1,2)$*-almost continuous since there exists a* (σ_1, σ_2)*-regular open set* $\{y\}$ *in* (Y, σ_1, σ_2) *such that* $f^{-1}(\{y\}) = \{b, c, d\}$ *is not* τ_1*-open set in* (X, τ_1, τ_2).

Example 3.7. *Let* $X = \{a, b, c\}$ *with topologies*

$$\tau_1 = \{\emptyset, \{c\}, \{a, b\}, X\}, \ \tau_2 = \{\emptyset, \{c\}, X\}$$

and

$$\sigma_1 = \{\emptyset, \{a\}, X\}, \ \sigma_2 = \{\emptyset, \{a, c\}, X\}.$$

Then the identity function $f : (X, \tau_1, \tau_2) \to (X, \sigma_1, \sigma_2)$ *is* $(1,2)$*-precontinuous. However* f *is not* 1*-continuous since* $f^{-1}(\{a\}) = \{a\}$ *is not* τ_1*-open set in* (X, τ_1, τ_2) *while* $\{a\}$ *is* σ_1*-open set in* (X, σ_1, σ_2).

Example 3.8. *Let* $X = \{a, b, c\}$ *with topologies*

$$\tau_1 = \{\emptyset, \{a\}, \{c\}, \{a, c\}, X\}, \ \tau_2 = \{\emptyset, \{c\}, X\}$$

and

$$\sigma_1 = \{\emptyset, \{a\}, \{c\}, \{a, c\}, \{a, b\}, X\}, \ \sigma_2 = \{\emptyset, \{b\}, \{b, c\}, X\}.$$

Then the identity function $f : (X, \tau_1, \tau_2) \to (X, \sigma_1, \sigma_2)$ *is* $(1,2)$*-*β*-continuous but it is not* $(1,2)$*-precontinuous since there exists a* σ_1*-open set* $\{a, b\}$ *in* (X, σ_1, σ_2) *such that* $f^{-1}(\{a, b\}) = \{a, b\}$ *is not* (τ_1, τ_2)*-preopen set in* (X, τ_1, τ_2) *because* $\{a, b\} \not\subseteq \tau_1$*-int* $(\tau_2$*-cl* $(\{a, b\})) = \tau_1$*-int* $(\{a, b\}) = \{a\}$.

From the above discussions, we obtain the following diagram in which none of these implications are reversible.

$$\begin{array}{ccccc}
 & & (i,j)\text{-}R\text{-map} & & \\
 & & \Downarrow & & \\
 & & (i,j)\text{-}\delta\text{-continuous} & \Longrightarrow & (i,j)\text{-almost } \delta\text{-continuous} \\
 & & \Downarrow & & \\
i\text{-continuous} & \Longrightarrow & (i,j)\text{-almost continuous} & & \\
\Downarrow & & \Downarrow & & \\
(i,j)\text{-precontinuous} & \Longrightarrow & (i,j)\text{-almost precontinuous} & & \\
\Downarrow & & \Downarrow & & \\
(i,j)\text{-}\beta\text{-continuous} & \Longrightarrow & (i,j)\text{-almost } \beta\text{-continuous} & &
\end{array}$$

In terms of pairwise properties, we have the following diagram in which none of these implications are reversible. We shall use p- to denote pairwise.

$$p\text{-}R\text{-map}$$

$$
\begin{array}{ccccc}
 & & \Downarrow & & \\
 & & p\text{-}\delta\text{-continuous} & & \\
 & & \Downarrow & & \\
\text{continuous} & \Longrightarrow & p\text{-almost continuous} & \Longrightarrow & p\text{-almost } \delta\text{-continuous} \\
\Downarrow & & \Downarrow & & \\
p\text{-precontinuous} & \Longrightarrow & p\text{-almost precontinuous} & & \\
\Downarrow & & \Downarrow & & \\
p\text{-}\beta\text{-continuous} & \Longrightarrow & p\text{-almost } \beta\text{-continuous} & &
\end{array}
$$

Many types of open of functions between topological spaces are studied such as almost open, almost α-open, weakly open and M-preopen functions (see [5, 16, 17]). We extend these types of open functions to bitopological setting as follows.

Definition 3.2. *A function $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ is said to be*

(1) *i-open if the function $f : (X, \tau_i) \to (Y, \sigma_i)$ is open, f is called open if it is both 1-open and 2-open;*
(2) *(i, j)-almost open if $f(U)$ is σ_i-open set in Y for every (τ_i, τ_j)-regular open set U in X, f is called pairwise almost open if it is both $(1, 2)$-almost open and $(2, 1)$-almost open;*
(3) *(i, j)-almost α-open if $f(U) \subseteq \sigma_i\text{-}int(\sigma_j\text{-}cl(\sigma_i\text{-}int(f(U))))$ for every (τ_i, τ_j)-regular open set U in X, f is called pairwise almost α-open if it is both $(1, 2)$-almost α-open and $(2, 1)$-almost α-open;*
(4) *(i, j)-weakly open if $f(U) \subseteq \sigma_i\text{-}int(f(\tau_j\text{-}cl(U)))$ for every τ_i-open subset U of X, f is called pairwise weakly open if it is both $(1, 2)$-weakly open and $(2, 1)$-weakly open;*
(5) *(i, j)-M-preopen if $f(U)$ is (σ_i, σ_j)-preopen set in Y for every (τ_i, τ_j)-preopen set U in X, f is called pairwise M-preopen if it is both $(1, 2)$-M-preopen and $(2, 1)$-M-preopen.*

The following proposition shows that (i, j)-almost open function implies (i, j)-weakly open.

Proposition 3.3. *If $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ is (i, j)-almost open function, then f is (i, j)-weakly open.*

Proof. Let U be a τ_i-open subset of X. Then $\tau_i\text{-}int(\tau_j\text{-}cl(U))$ is a (τ_i, τ_j)-regular open subset of X. Since f is (i, j)-almost open, then $f(\tau_i\text{-}int(\tau_j\text{-}cl(U)))$ is a σ_i-open set in Y. Hence $f(\tau_i\text{-}int(\tau_j\text{-}cl(U))) = \sigma_i\text{-}int(f(\tau_i\text{-}int(\tau_j\text{-}cl(U)))) \subseteq \sigma_i\text{-}int(f(\tau_j\text{-}cl(U)))$. Since $U \subseteq \tau_i\text{-}int(\tau_j\text{-}cl(U))$, it implies that

$$f(U) \subseteq f(\tau_i\text{-}int(\tau_j\text{-}cl(U)))$$

and thus $f(U) \subseteq \sigma_i\text{-}int(f(\tau_j\text{-}cl(U)))$. This shows that f is (i, j)-weakly open. □

Corollary 3.3. *If $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ is pairwise almost open function, then f is pairwise weakly open.*

Observe that every i-open function is (i, j)-almost open but the converse is not true as Example 3.9 below shows. Every (i, j)-almost open function is (i, j)-almost α-open but the converse is not true as Example 3.10 below shows. Although i-openness implies (i, j)-weakly openness but the converse is not true as Example 3.13

below shows. Proposition 3.3 above shows that (i,j)-almost openness implies (i,j)-weakly openness but the converse is not true as Example 3.13 below shows. Moreover, (i,j)-weakly openness and (i,j)-almost α-openness are independent concepts as Example 3.10 and Example 3.13 below show. Furthermore, i-openness and (i,j)-M-preopenness are independent, (i,j)-almost openness and (i,j)-M-preopenness are independent, (i,j)-almost α-openness and (i,j)-M-preopenness are independent, and (i,j)-weakly openness and (i,j)-M-preopenness are also independent concepts by the Example 3.11 and Example 3.12 below show.

Example 3.9. *Let $X=\{a,b,c\}$ with topologies*

$$\tau_1=\{\emptyset,\{a\},\{a,b\},X\},\ \tau_2=\{\emptyset,X\}$$

and

$$\sigma_1=\{\emptyset,\{a\},X\},\ \sigma_2=\{\emptyset,\{b\},\{b,c\},X\}.$$

Then the identity function $f:(X,\tau_1,\tau_2)\to(X,\sigma_1,\sigma_2)$ is $(1,2)$-almost open since the only (τ_1,τ_2)-regular open set in (X,τ_1,τ_2) are $\emptyset$ and X. However f is not 1-open since $f(\{a,b\})=\{a,b\}$ is not σ_1-open set in (X,σ_1,σ_2) for $\{a,b\}$ is τ_1-open set in (X,τ_1,τ_2).

Example 3.10. *Let $X=\{a,b,c,d\}$ with topologies*

$$\begin{aligned}\tau_1 &= \{\emptyset,\{c\},\{d\},\{a,c\},\{c,d\},\{a,c,d\},X\},\\ \tau_2 &= \{\emptyset,\{d\},\{a,d\},\{b,d\},\{a,b,d\},X\}\end{aligned}$$

and let $Y=\{x,y,z\}$ with topologies

$$\sigma_1=\{\emptyset,\{z\},\{x,y\},Y\},\ \sigma_2=\{\emptyset,Y\}.$$

Then a function $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ defined as $f(a)=f(d)=x$, $f(b)=y$ and $f(c)=z$ is $(1,2)$-almost α-open since the (τ_1,τ_2)-regular open sets in (X,τ_1,τ_2) are $\emptyset,\{c\},\{a,c\}$ and X. However f is not $(1,2)$-almost open since there exists a (τ_1,τ_2)-regular open set $\{a,c\}$ in (X,τ_1,τ_2) such that $f(\{a,c\})=\{x,z\}$ is not σ_1-open set in (Y,σ_1,σ_2). Even f is $(1,2)$-almost α-open but it is not $(1,2)$-weakly open since there exists a τ_1-open set $\{a,c\}$ in (X,τ_1,τ_2) such that $f(\{a,c\})=\{x,z\}\not\subseteq \sigma_1\text{-}int(f(\tau_2\text{-}cl(\{a,c\})))=\sigma_1\text{-}int(f(\{a,c\}))=\sigma_1\text{-}int(\{x,z\})=\{z\}$.

Example 3.11. *Let $X=\{a,b,c\}$ with topologies*

$$\tau_1=\{\emptyset,\{a\},\{a,b\},X\},\ \tau_2=\{\emptyset,X\}$$

and

$$\sigma_1=\{\emptyset,\{a\},\{b\},\{a,b\},X\},\ \sigma_2=\{\emptyset,\{b\},X\}.$$

Then the identity function $f:(X,\tau_1,\tau_2)\to(X,\sigma_1,\sigma_2)$ is 1-open, thus $(1,2)$-almost open, $(1,2)$-almost α-open and $(1,2)$-weakly open. However f is not $(1,2)$-M-preopen since $\{a,c\}$ is a (τ_1,τ_2)-preopen set in (X,τ_1,τ_2) but $f(\{a,c\})=\{a,c\}$ is not (σ_1,σ_2)-preopen set in (X,σ_1,σ_2) because $f(\{a,c\})=\{a,c\}\not\subseteq\sigma_1\text{-}int(\sigma_2\text{-}cl(f(\{a,c\})))=\{a\}$.

Example 3.12. *Let $X=\{a,b,c\}$ with topologies*

$$\tau_1=\{\emptyset,\{a\},\{b\},\{a,b\},X\},\ \tau_2=\{\emptyset,\{b,c\},X\}$$

and

$$\sigma_1=\{\emptyset,\{b\},X\},\ \sigma_2=\{\emptyset,X\}.$$

Then the identity function $f : (X, \tau_1, \tau_2) \to (X, \sigma_1, \sigma_2)$ *is* $(1,2)$*-M-preopen since the* $(1,2)$*-preopen sets in* (X, σ_1, σ_2) *are all subsets of* X*. However* f *is neither* $(1,2)$*-weakly open nor* $(1,2)$*-almost* α*-open. For this purpose we take a* τ_1*-open set* $\{a\}$ *in* (X, τ_1, τ_2) *but*

$$f(\{a\}) = \{a\} \not\subseteq \sigma_1\text{-}int(f(\tau_2\text{-}cl(\{a\}))) = \sigma_1\text{-}int(f(\{a\})) = \sigma_1\text{-}int(\{a\}) = \emptyset$$

and a (τ_1, τ_2)*-regular open set* $\{a\}$*in* (X, τ_1, τ_2) *but*

$$f(\{a\}) = \{a\} \not\subseteq \sigma_1\text{-}int(\sigma_2\text{-}cl(\sigma_1\text{-}int(f(\{a\})))) = \sigma_1\text{-}int(\sigma_2\text{-}cl(\emptyset)) = \emptyset$$

in (X, σ_1, σ_2)*. Thus* f *is also neither* $(1,2)$*-almost open nor* 1*-open by direct implications.*

Example 3.13. *Let* $X = \{a, b, c\}$ *with* $\tau_1 = \{\emptyset, \{a\}, \{c\}, \{a, c\}, X\}$, $\tau_2 = \{\emptyset, \{c\}, X\}$ *and let* $Y = \{x, y\}$ *with* $\sigma_1 = \{\emptyset, Y\}$, $\sigma_2 = \{\emptyset, \{x\}, Y\}$*. Let* $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ *be a function defined by* $f(a) = f(c) = x$ *and* $f(b) = y$*. Then* f *is* $(1,2)$*-weakly open but it is not* $(1,2)$*-almost* α*-open since there exists a* (τ_1, τ_2)*-regular open set* $\{a\}$ *in* (X, τ_1, τ_2) *such that*

$$f(\{a\}) = \{x\} \not\subseteq \sigma_1\text{-}int(\sigma_2\text{-}cl(\sigma_1\text{-}int(f(\{a\})))) = \sigma_1\text{-}int(\sigma_2\text{-}cl(\emptyset)) = \emptyset$$

in (Y, σ_1, σ_2)*. Thus* f *is neither* $(1,2)$*-almost open nor* 1*-open by direct implication or by* $f(\{a\}) = \{x\}$ *is not* σ_1*-open set in* (Y, σ_1, σ_2) *for* $\{a\}$ *is a* (τ_1, τ_2)*-regular open set or a* τ_1*-open set in* (X, τ_1, τ_2)*.*

Therefore, we obtain the following diagram in which none of these implications are reversible.

$$\begin{array}{ccccc} i\text{-open} & \Longrightarrow & (i,j)\text{-almost open} & \Longrightarrow & (i,j)\text{-almost } \alpha\text{-open} \\ & & \Downarrow & & \\ & & (i,j)\text{-weakly open} & & \end{array}$$

In terms of pairwise properties, we have the following diagram in which none of these implications are reversible.

$$\begin{array}{ccccc} p\text{-open} & \Longrightarrow & p\text{-almost open} & \Longrightarrow & p\text{-almost } \alpha\text{-open} \\ & & \Downarrow & & \\ & & p\text{-weakly open} & & \end{array}$$

4. Mapping on Pairwise Nearly Lindelöf Spaces

Definition 4.1 (see [18])**.** *A bitopological space* (X, τ_1, τ_2) *is said to be* (τ_i, τ_j)*-nearly Lindelöf if for every* τ_i*-open cover* $\{U_\alpha : \alpha \in \Delta\}$ *of* X*, there exists a countable subset* $\{\alpha_n : n \in \mathbb{N}\}$ *of* Δ *such that* $X = \bigcup_{n \in \mathbb{N}} \tau_i\text{-}int(\tau_j\text{-}cl(U_{\alpha_n}))$*, or as is easily seen to be equivalent, if every* (τ_i, τ_j)*-regular open cover of* X *has a countable subcover.* X *is called pairwise nearly Lindelöf if it is both* (τ_1, τ_2)*-nearly Lindelöf and* (τ_2, τ_1)*-nearly Lindelöf.*

It is also equivalent to say that, a bitopological space X is (i,j)-nearly Lindelöf if and only if every (i,j)-regular open cover of X has a countable subcover (see[18]).

It is well known that in a topological space and a bitopological space, the continuous image of a Lindelöf space is Lindelöf. While Fawakhreh and Kılıçman [5]

stated that the δ-continuous image of a nearly Lindelöf space is nearly Lindelöf. For the (τ_i, τ_j)-nearly Lindelöf spaces we give the following theorem.

Theorem 4.1. *Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a surjective and (i, j)-δ-continuous function. If X is (τ_i, τ_j)-nearly Lindelöf, then Y is (σ_i, σ_j)-nearly Lindelöf.*

Proof. Let $\{V_\alpha : \alpha \in \Delta\}$ be a (σ_i, σ_j)-regular open cover of Y. Let $x \in X$ and let $\alpha_x \in \Delta$ such that $f(x) \in V_{\alpha_x}$. Since f is (i, j)-δ-continuous, there exists a (τ_i, τ_j)-regular open set U_{α_x} of X containing x such that $f(U_{\alpha_x}) \subseteq V_{\alpha_x}$. So $\{U_{\alpha_x} : x \in X\}$ forms a (τ_i, τ_j)-regular open cover of X. Since X is (τ_i, τ_j)-nearly Lindelöf, there exists a countable subset $\{x_n : n \in \mathbb{N}\}$ of X such that $X = \bigcup_{n\in\mathbb{N}} U_{\alpha_{x_n}}$. Since f is surjective, we have $Y = f(X) = f\left(\bigcup_{n\in\mathbb{N}} U_{\alpha_{x_n}}\right) = \bigcup_{n\in\mathbb{N}} f\left(U_{\alpha_{x_n}}\right) \subseteq \bigcup_{n\in\mathbb{N}} V_{\alpha_{x_n}}$ which implies $Y = \bigcup_{n\in\mathbb{N}} V_{\alpha_{x_n}}$. This shows that Y is (σ_i, σ_j)-nearly Lindelöf and completes the proof. □

Corollary 4.1. *Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a surjective and pairwise δ-continuous function. If X is pairwise nearly Lindelöf, then so is Y.*

Lemma 4.1. *If $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ is an (i, j)-R-map, then f is (i, j)-δ-continuous.*

Proof. Let $x \in X$ and let V be a (σ_i, σ_j)-regular open subset of Y containing $f(x)$. Then $x \in f^{-1}(V)$. Since f is an (i, j)-R-map, $f^{-1}(V)$ is a (τ_i, τ_j)-regular open set in X. So if $U = f^{-1}(V)$, then U is a (τ_i, τ_j)-regular open subset of X containing x such that $f(U) = f\left(f^{-1}(V)\right) \subseteq V$. This shows that f is (i, j)-δ-continuous. □

Corollary 4.2. *If $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ is a pairwise R-map, then f is pairwise δ-continuous.*

The converse of Lemma 4.1 is not true as the following example shows.

Example 4.1. *Let $X = \{a, b, c, d\}$ with topologies*

$$\begin{aligned} \tau_1 &= \{\emptyset, \{b\}, \{c\}, \{d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, c, d\}, \{b, c, d\}, X\}, \\ \tau_2 &= \{\emptyset, \{b\}, \{c\}, \{d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{b, c, d\}, X\} \end{aligned}$$

and $Y = \{x, y, z\}$ with topologies

$$\sigma_1 = \{\emptyset, \{x\}, \{y\}, \{x, y\}, Y\}, \ \sigma_2 = \{\emptyset, \{x, z\}, Y\}.$$

Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a function defined by $f(a) = z$, $f(b) = f(c) = f(d) = y$. Then f is $(1, 2)$-δ-continuous but it is not $(1, 2)$-R-map since there exists a (σ_1, σ_2)-regular open set $\{y\}$ in (Y, σ_1, σ_2) such that $f^{-1}(\{y\}) = \{b, c, d\}$ is not (τ_1, τ_2)-regular open set in (X, τ_1, τ_2).

By using Lemma 4.1 and Theorem 4.1 above, we have the following corollary.

Corollary 4.3. *Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a surjective and (i, j)-R-map. If X is (τ_i, τ_j)-nearly Lindelöf, then Y is (σ_i, σ_j)-nearly Lindelöf.*

Corollary 4.4. *Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a surjective and pairwise R-map. If X is pairwise nearly Lindelöf, then Y is pairwise nearly Lindelöf.*

Lemma 4.2. *Every pairwise almost continuous and (i,j)-almost α-open function is an (i,j)-R-map.*

Proof. Let $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ be a pairwise almost continuous and (i,j)-almost α-open function. Let V be a (σ_i,σ_j)-regular open set in Y. Since f is (i,j)-almost continuous, $f^{-1}(V)$ is a τ_i-open set in X. So $f^{-1}(V)\subseteq \tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$. Next we have to show the opposite inclusion. Since f is (i,j)-almost α-open and $\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$ is a (τ_i,τ_j)-regular open set in X, we have

$$\begin{aligned} & f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right) \\ \subseteq\ & \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(\sigma_i\text{-}int\left(f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right)\right)\right) \\ \subseteq\ & \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(\sigma_i\text{-}int\left(f\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right)\right). \end{aligned}$$

Since f is (j,i)-almost continuous and $\sigma_j\text{-}cl(V)$ is a $\sigma_j\sigma_i$-regular closed set in Y, $\tau_j\text{-}cl\left(f^{-1}(V)\right)\subseteq f^{-1}(\sigma_j\text{-}cl(V))$ because $f^{-1}(\sigma_j\text{-}cl(V))$ is a τ_j-closed set in X containing $f^{-1}(V)$. So

$$\begin{aligned} f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right) &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(\sigma_i\text{-}int\left(f\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(\sigma_i\text{-}int\left(f\left(f^{-1}(\sigma_j\text{-}cl(V))\right)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(\sigma_i\text{-}int\left(\sigma_j\text{-}cl(V)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl(V)\right)=V. \end{aligned}$$

Thus

$$\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\subseteq f^{-1}\left(f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right)\subseteq f^{-1}(V).$$

Hence $f^{-1}(V)=\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$ which implies that $f^{-1}(V)$ is a (τ_i,τ_j)-regular open set in X. This shows that f is an (i,j)-R-map and completes the proof. □

Corollary 4.5. *Every pairwise almost continuous and pairwise almost α-open function is a pairwise R-map.*

Corollary 4.6. *Let $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ be a surjective, pairwise almost continuous and (i,j)-almost α-open function. If X is (τ_i,τ_j)-nearly Lindelöf, then Y is (σ_i,σ_j)-nearly Lindelöf.*

Proof. It is a direct consequence of Lemma 4.2 and Corollary 4.3 above. □

Corollary 4.7. *Let $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ be a surjective, pairwise almost continuous and pairwise almost α-open function. If X is pairwise nearly Lindelöf, then so is Y.*

Since (i,j)-almost open function is (i,j)-almost α-open, by using Lemma 4.2 we obtain the following lemma.

Lemma 4.3. *Every pairwise almost continuous and (i,j)-almost open function is an (i,j)-R-map.*

Corollary 4.8. *Every pairwise almost continuous and pairwise almost open function is a pairwise R-map.*

Corollary 4.9. *Let $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ be a surjective, pairwise almost continuous and (i,j)-almost open function. If X is (τ_i,τ_j)-nearly Lindelöf, then Y is (σ_i,σ_j)-nearly Lindelöf.*

Proof. It is a direct consequence of Lemma 4.3 and Corollary 4.3 above. It is also a direct consequence of Corollary 4.6 above. □

Corollary 4.10. *Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a surjective, pairwise almost continuous and pairwise almost open function. If X is pairwise nearly Lindelöf, then so is Y.*

Lemma 4.4. *Every pairwise almost continuous and (i, j)-weakly open function is an (i, j)-R-map.*

Proof. Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a pairwise almost continuous and (i, j)-weakly open function. Let V be a (σ_i, σ_j)-regular open set in Y. Since f is (i, j)-almost continuous, $f^{-1}(V)$ is a τ_i-open set in X. So $f^{-1}(V) \subseteq \tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$. Next we have to show the opposite inclusion. Since f is (i, j)-weakly open and τ_i-$int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$ is also τ_i-open set in X, we have

$$\begin{aligned} f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right) &\subseteq \sigma_i\text{-}int\left(f\left(\tau_j\text{-}cl\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(f\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right). \end{aligned}$$

Since f is (j, i)-almost continuous, $\tau_j\text{-}cl\left(f^{-1}(V)\right) \subseteq f^{-1}(\sigma_j\text{-}cl(V))$. So

$$\begin{aligned} f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right) &\subseteq \sigma_i\text{-}int\left(f\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(f\left(f^{-1}\left(\sigma_j\text{-}cl(V)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl(V)\right) = V. \end{aligned}$$

Thus

$$\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right) \subseteq f^{-1}\left(f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right) \subseteq f^{-1}(V).$$

Hence $f^{-1}(V) = \tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$ which implies that $f^{-1}(V)$ is a (τ_i, τ_j)-regular open set in X. This shows that f is an (i, j)-R-map and completes the proof. □

Corollary 4.11. *Every pairwise almost continuous and pairwise weakly open function is a pairwise R-map.*

By using Lemma 4.4 and Corollary 4.3 above, we conclude the following corollary.

Corollary 4.12. *Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a surjective, pairwise almost continuous and (i, j)-weakly open function. If X is (τ_i, τ_j)-nearly Lindelöf, then Y is (σ_i, σ_j)-nearly Lindelöf.*

Corollary 4.13. *Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a surjective, pairwise almost continuous and pairwise weakly open function. If X is pairwise nearly Lindelöf, then so is Y.*

Lemma 4.5. *Every pairwise almost continuous and (i, j)-M-preopen function is an (i, j)-R-map.*

Proof. Let $f : (X, \tau_1, \tau_2) \to (Y, \sigma_1, \sigma_2)$ be a pairwise almost continuous and (i, j)-M-preopen function. Let V be a (σ_i, σ_j)-regular open set in Y. Since f is (i, j)-almost continuous, $f^{-1}(V)$ is a τ_i-open set in X. So $f^{-1}(V) \subseteq \tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$. Next we have to show the opposite inclusion. Since f is (i, j)-M-preopen and

$$\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right) \subseteq \tau_i\text{-}int\left(\tau_j\text{-}cl\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right),$$

i.e., τ_i-$int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$ is a (τ_i,τ_j)-preopen set in X,

$$f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)$$

is a (σ_i,σ_j)-preopen set in Y, i.e.,

$$\begin{aligned} f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right) &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(f\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right). \end{aligned}$$

Since f is (j,i)-almost continuous, τ_j-$cl\left(f^{-1}(V)\right) \subseteq f^{-1}\left(\sigma_j\text{-}cl(V)\right)$. So

$$\begin{aligned} f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right) &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(f\left(f^{-1}\left(\sigma_j\text{-}cl(V)\right)\right)\right)\right) \\ &\subseteq \sigma_i\text{-}int\left(\sigma_j\text{-}cl\left(\sigma_j\text{-}cl(V)\right)\right) \\ &= \sigma_i\text{-}int\left(\sigma_j\text{-}cl(V)\right) = V. \end{aligned}$$

Thus

$$\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right) \subseteq f^{-1}\left(f\left(\tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)\right)\right) \subseteq f^{-1}(V).$$

Hence $f^{-1}(V) = \tau_i\text{-}int\left(\tau_j\text{-}cl\left(f^{-1}(V)\right)\right)$ which implies that $f^{-1}(V)$ is a (τ_i,τ_j)-regular open set in X. This shows that f is an (i,j)-R-map and completes the proof. □

Corollary 4.14. *Every pairwise almost continuous and pairwise M-preopen function is a pairwise R-map.*

By using Lemma 4.5 and Corollary 4.3, we have the following corollary.

Corollary 4.15. *Let $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ be a surjective, pairwise almost continuous and (i,j)-M-preopen function. If X is (τ_i,τ_j)-nearly Lindelöf, then Y is (σ_i,σ_j)-nearly Lindelöf.*

Corollary 4.16. *Let $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ be a surjective, pairwise almost continuous and pairwise M-preopen function. If X is pairwise nearly Lindelöf, then so is Y.*

Let X be a topological space. A cover $\mathcal{V}=\{V_\lambda:\lambda\in\Lambda\}$ of X is a refinement [2, 4] of another cover $\mathcal{U}=\{U_\alpha:\alpha\in\Delta\}$ if for each $\lambda\in\Lambda$, there exists an $\alpha(\lambda)\in\Delta$ such that $V_\lambda\subseteq U_{\alpha(\lambda)}$, i.e., each $V\in\mathcal{V}$ is contained in some $U\in\mathcal{U}$. If the elements of $\mathcal{V}$ are open sets, we will call $\mathcal{V}$ an open refinement of $\mathcal{U}$; if they are closed sets, we call $\mathcal{V}$ a closed refinement. A family $\mathcal{U}=\{U_\alpha:\alpha\in\Delta\}$ of subsets of a topological space X is locally finite [2, 4] if for every point $x\in X$, there exists a neighbourhood U_x of x such that the set $\{\alpha\in\Delta:U_x\cap U_\alpha\neq\emptyset\}$ is finite, i.e., each $x\in X$ has a neighbourhood U_x meeting only finitely many $U\in\mathcal{U}$.

If bitopological space (X,τ_1,τ_2) considered, i-locally finite concept appear as follows.

Definition 4.2. *A family $\mathcal{U}=\{U_\alpha:\alpha\in\Delta\}$ of subsets of a space (X,τ_1,τ_2) is i-locally finite if for every point $x\in X$, there exists an i-neighbourhood U_x of x such that the set $\{\alpha\in\Delta:U_x\cap U_\alpha\neq\emptyset\}$ is finite, i.e., each $x\in X$ has an i-neighbourhood U_x meeting only finitely many $U\in\mathcal{U}$.*

In 1969, Singal and Arya [19] introduced the notion of nearly paracompact spaces in topological spaces. Now we extend this notion to bitopological setting as follows.

Definition 4.3. *A bitopological space X is said to be (i,j)-nearly paracompact if every cover of X by (i,j)-regular open sets admits an i-locally finite refinement (not necessarily 1-open or 2-open). X is called pairwise nearly paracompact if it is both $(1,2)$-nearly paracompact and $(2,1)$-nearly paracompact.*

Cammaroto and Santoro [2] proved that an almost regular and nearly Lindelöf space is nearly paracompact. We extend this result to bitopological setting as follows.

Lemma 4.6. *Let (X,τ_1,τ_2) be an (i,j)-almost regular and (i,j)-nearly Lindelöf space. Then X is (i,j)-nearly paracompact.*

Proof. Let $\mathcal{V} = \{V_\alpha : \alpha \in \Delta\}$ be an (i,j)-regular open cover of X. For each $x \in X$, there exists $\alpha_x \in \Delta$ such that $x \in V_{\alpha_x}$. Since X is (i,j)-almost regular, there exists an (i,j)-regular open neighbourhood U_{α_x} of x such that $x \in U_{\alpha_x} \subseteq j\text{-}cl\,(U_{\alpha_x}) \subseteq V_{\alpha_x}$. So $\{U_{\alpha_x} : x \in X\}$ is an (i,j)-regular open cover of X. Since X is (i,j)-nearly Lindelöf, there exists a countable subset of points $x_1, x_2, \ldots, x_n, \ldots$ of X such that $X = \bigcup_{n\in\mathbb{N}} U_{\alpha_{x_n}}$. For each $n \in \mathbb{N}$, put $G_n = V_{\alpha_{x_n}} \setminus \left(\bigcup_{k=1}^{n-1} j\text{-}cl\left(U_{\alpha_{x_k}}\right)\right)$. By construction $\{G_n : n \in \mathbb{N}\}$ is an i-locally finite family. In fact, if $x \in X$ then there exist $U_{\alpha_{x_p}}$ (since $\left\{U_{\alpha_{x_n}} : n \in \mathbb{N}\right\}$ is a cover of X) and $V_{\alpha_{x_p}}$ such that $x \in U_{\alpha_{x_p}} \subseteq V_{\alpha_{x_p}}$. We will prove that $U_{\alpha_{x_p}}$ intersects at most finitely many members of the family $\{G_n : n \in \mathbb{N}\}$. Since $G_1 = V_{\alpha_{x_1}}, G_2 = V_{\alpha_{x_2}} \setminus j\text{-}cl\left(U_{\alpha_{x_1}}\right), \ldots, G_p = V_{\alpha_{x_p}} \setminus \left(j\text{-}cl\left(U_{\alpha_{x_1}}\right) \cup \cdots \cup j\text{-}cl\left(U_{\alpha_{x_{p-1}}}\right)\right), G_{p+1} = V_{\alpha_{x_{p+1}}} \setminus \left(j\text{-}cl\left(U_{\alpha_{x_1}}\right) \cup \cdots \cup j\text{-}cl\left(U_{\alpha_{x_p}}\right)\right)$, $U_{\alpha_{x_p}} \cap G_r = \emptyset$ for each $r \geq p+1$. Therefore $U_{\alpha_{x_p}}$ intersects at most a finite number of sets in the family $\{G_n : n \in \mathbb{N}\}$. Next we assert that $\{G_n : n \in \mathbb{N}\}$ is the required refinement of $\mathcal{V}$. Let x be any point of X. We wish to prove that x lies in an element of $\{G_n : n \in \mathbb{N}\}$. Consider the cover $\left\{V_{\alpha_{x_n}} : n \in \mathbb{N}\right\}$ of X; let N be the smallest integer such that x lies in $V_{\alpha_{x_N}}$. Observe that the point x is not lies in G_k for $k < N$ but x lies in G_N since it is not lies in $\bigcup_{k=1}^{N-1} j\text{-}cl\left(U_{\alpha_{x_k}}\right)$. Therefore $x \in \bigcup_{n\in\mathbb{N}} G_n$ which implies that $\{G_n : n \in \mathbb{N}\}$ covers X. This shows that X is (i,j)-nearly paracompact. □

Corollary 4.17. *Let (X,τ_1,τ_2) be a pairwise almost regular and pairwise nearly Lindelöf space. Then X is pairwise nearly paracompact.*

Note that, if (X,τ_1,τ_2) is (i,j)-semiregular and (i,j)-nearly Lindelöf then it is i-Lindelöf (see [14]). Thus by this fact and Lemma 4.6, we conclude the following corollaries.

Corollary 4.18. *Let $f : (X,\tau_1,\tau_2) \to (Y,\sigma_1,\sigma_2)$ be a surjective function satisfying one of the following conditions*:

(1) *(i,j)-δ-continuous,*
(2) *(i,j)-R-map,*
(3) *pairwise almost continuous and (i,j)-almost α-open,*
(4) *pairwise almost continuous and (i,j)-almost open,*
(5) *pairwise almost continuous and (i,j)-weakly open,*

(6) *pairwise almost continuous and* (i,j)*-M-preopen.*

If X *is* (τ_i,τ_j)*-nearly Lindelöf and* Y *is a* (σ_i,σ_j)*-semiregular* (*resp.* (σ_i,σ_j) *-almost regular*) *space, then* Y *is* σ_i*-Lindelöf* (*resp.* (σ_i,σ_j) *-nearly paracompact*).

Corollary 4.19. *Let* $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ *be a surjective function satisfying one of the following conditions*:

(1) *pairwise* δ*-continuous,*
(2) *pairwise R-map,*
(3) *pairwise almost continuous and pairwise almost* α*-open,*
(4) *pairwise almost continuous and pairwise almost open,*
(5) *pairwise almost continuous and pairwise weakly open,*
(6) *pairwise almost continuous and pairwise M-preopen.*

If X *is pairwise nearly Lindelöf and* Y *is a pairwise semiregular* (*resp. pairwise almost regular*) *space, then* Y *is Lindelöf* (*resp. pairwise nearly paracompact*).

Since an (i,j)-regular space is (i,j)-semiregular and (i,j)-almost regular (see [14]), we have the following corollary.

Corollary 4.20. *Let* $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ *be a surjective function satisfying one of the conditions* $(1)-(6)$ *of Corollary 4.18. If* X *is* (τ_i,τ_j)*-nearly Lindelöf and* Y *is a* (σ_i,σ_j)*-regular space, then* Y *is* σ_i*-Lindelöf and* (σ_i,σ_j)*-nearly paracompact.*

Corollary 4.21. *Let* $f:(X,\tau_1,\tau_2)\to(Y,\sigma_1,\sigma_2)$ *be a surjective function satisfying one of the conditions* $(1)-(6)$ *of Corollary 4.19. If* X *is pairwise nearly Lindelöf and* Y *is a pairwise regular space, then* Y *is Lindelöf and pairwise nearly paracompact.*

Acknowledgement: The authors gratefully acknowledge that this research was partially supported by the Ministry of Science, Technology and Innovations(MOSTI), Malaysia under the e-Science Grant 06-01-04-SF0115. The authors also wish to thank the referees for their constructive comments and suggestions.

References

[1] G. Balasubramaniam, On some generalizations of compact spaces, *Glasnik Mat.*, **17**(37)(1982), pp.367–380.
[2] F. Cammaroto and G. Santoro, Some counterexamples and properties on generalizations of Lindelöf spaces, *Int. J. Math & Math. Sci.*, **19**(4)(1996), pp. 737–746.
[3] D. Carnahan, Some Properties Related to Topological Spaces, PhD Thesis, Univ. of Arkansas (1973).
[4] R. Engelking, General Topology, PWN-Pol. Scien. Publ., Warszawa, 1977.
[5] A. J. Fawakhreh and A. Kılıçman, Mappings and some decompositions of continuity on nearly Lindelöf spaces, *Acta Math. Hungar.* **97**(3)(2002), pp. 199–206.
[6] Ali A. Fora and Hasan Z. Hdeib, On pairwise Lindelöf spaces, *Rev. Colombiana Mat.*, **17**(2)(1983), pp. 37–57.
[7] J. C. Kelly, Bitopological spaces, *Proc. London Math. Soc.*, **13**(3)(1963), pp. 71–89.
[8] F. H. Khedr and A. M. Alshibani, On pairwise super continuous mappings in bitopological spaces, *Int. J. Math & Math. Sci.*, **14**(4)(1991), pp. 715–722.
[9] A. Kılıçman and Z. Salleh, On pairwise Lindelöf bitopological spaces. *Topology Appl.* **154**(8)(2007), pp. 1600–1607.
[10] A. Kılıçman and Z. Salleh, Pairwise almost Lindelöf bitopological spaces,*Journal of Malaysian Mathematical Sciences*, **1**(2)(2007), pp.227-238.
[11] A. Kılıçman and Z. Salleh, Mappings and pairwise continuity on pairwise Lindelöf bitopological spaces, *Albanian J. Math.*, **1**(2)(2007), pp. 115–120.
[12] A. Kılıçman; Z. Salleh, Pairwise weakly regular-Lindelf spaces. *Abstr. Appl. Anal.* 2008, Art. ID 184243, 13 pp.

[13] A. Kılıçman and Z. Salleh, A note on pairwise continuous mappings and bitopological spaces, *European Journal of Pure and Applied Mathematics*, **2**(3)(2009), pp. 325–337.
[14] A. Kılıçman and Z. Salleh, On pairwise almost regular-Lindelöf spaces, *Scientiae Mathematicae Japonicae*, **70**(3)(2009), pp. 285–298.
[15] A. A. Nasef and T. Noiri, Some weak forms of almost continuity, *Acta Math. Hungar.,* **74**(3)(1997), pp. 211–219.
[16] T. Noiri, Almost αg-closed functions and separation axioms, *Acta Math. Hungar.* **82**(3)(1999), pp. 193–205.
[17] D. A. Rose, Weak openness and almost openness, *Int. J. Math & Math. Sci.*, **7** (1) (1984), pp. 35–40.
[18] Z. Salleh and A. Kılıçman, Pairwise nearly Lindelöf spaces, *Proc. of the* 5^{th} *Asian Mathematical Conference, Malaysia*, Vol. I, 2009, pp. 190–197.
[19] M. K. Singal and S. P. Arya, On nearly paracompact spaces, Mat. Vesnik, **6**(21) (1969), pp. 3–16.
[20] A. R. Singal and S. P. Arya, On pairwise almost regular spaces, *Glasnik Math.*, 26 (6) (1971), pp. 335–343.
[21] M. K. Singal and A. R. Singal, Some more separation axioms in bitopological spaces, *Ann. Son. Sci. Bruxelles.*, **84**(1970), pp. 207–230.

Adem Kiliçman, Department of Mathematics and Institute for Mathematical Research, University Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia
E-mail address: akilicman@putra.upm.edu.my

Zabidin Salleh, Department of Mathematics, Faculty of Science and Technology, University Malaysia Terengganu 21030 Kuala Terengganu, Terengganu, Malaysia
E-mail address: zabidin@umt.edu.my

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 2, Pages 49–56
ISSN 1930-1235: (2010)

ON REGULAR SEMI GENERALIZED CLOSED SETS

T.NOIRI AND M.KHAN

Abstract. In this paper we introduce the concept of rsg-closed sets and investigate some of its properties in topological spaces. We also define an rsg-regular space and give some of its fundamental properties.

1. Introduction

In 1970, Levine [12] introduced the notion of generalized closed sets in topological spaces. In 1987, Battacharyya and Lahiri [2] used semi-open sets [11] to define the notion of semi-generalized closed sets. In 1990, Arya and Nour [1] introduced the concept of generalized semi-closed sets. The notion of s*g-closed sets was introduced by Rao and Joseph [16]. In this paper, we investigate many properties of rsg-closed sets which are situated between s*g-closed sets and rg-closed sets. We also show that arbitrary intersection of rsg-closed sets in a locally indiscrete space is rsg-closed. Moreover rsg-regular space is defind and some of its basic properties are investigated.

2. Preliminary

Throughout this paper, (X, τ) (or simply X) will always represent a topological space on which no separation axioms are assumed, unless otherwise mentioned. When A is a subset of X, cl(A) and Int(A) denote the closure and interior of a set A, respectively. A subset A of a space X is said to be semi-open [11] if there exists an open set U such that $U \subset A \subset cl(U)$. The complement of a semi-open set is said to be semi-closed. A subset A of a topological space X is said to be semi-regular [6] if it is both semi-open and semi-closed. In [6], it is pointed out that a set is semi-regular if and only if there exists a regular open set U such that $U \subset A \subset cl(U)$. Cameron [4] called semi regular sets regular semi-open.

Definition 2.1. *A subset A of a space X is said to be*

- **(1):** *generalized closed* [12] *(briefly, g-closed) if* $cl(A) \subset U$ *whenever* $A \subset U$ *and U is open in X. The complement of a g-closed set is said to be g-open;*
- **(2):** *s*g-closed* [16] *if* $cl(A) \subset G$ *whenever* $A \subset G$ *and G is semi-open in X. The complement of an s*g-closed set is said to be s*g-open;*
- **(3):** *regular generalized closed* [15] *(briefly, rg-closed) if* $cl(A) \subset U$ *whenever* $A \subset U$ *and U is regular-open in X. The complement of an rg-closed set is said to be rg-open;*
- **(4):** *semi-generalized closed* [3] *(briefly, sg-closed) if* $scl(A) \subset U$ *whenever* $A \subset U$ *and U is semi-open in X.*

3. rsg-closed sets

Definition 3.1. *A subset A of a space X is said to be*

(1): *regular semi generalized closed (briefly, rsg-closed) if $cl(A) \subset G$ whenever $G \subset A$ for every semi-regular set G in X;*

(2): *regular semi generalized open (briefly, rsg-open) if $X - A$ is rsg-closed.*

Theorem 3.2. *A subset A of a space (X, τ) is rsg-open if and only if $G \subset Int(A)$ whenever $G \subset A$ for every semi-regular set G in X.*

Proof. Let A be an rsg- open set and G a semi-regular set such that $G \subset A$. Then $X - A$ is rsg -closed and $X - A \subset X - G$. Since $X - G$ is semi-regular in X, $cl(X - A) \subset X - G$ and hence $X - Int(A) \subset X - G$. Therefore, $G \subset Int(A)$.

Conversely, let $G \subset Int(A)$ whenever $G \subset A$ and G is semi-regular in X. This implies that $X - Int(A) = cl(X - A) \subset X - G$ whenever $X - A \subset X - G$ and X-G is semi-regular in X. This proves that X-A is rsg -closed in X and hence A is rsg-open in X.

Remark 3.3. **(1):** *Every closed set is rsg-closed;*

(2): *Every open set is rsg-open;*

(3): *Semi open sets and rsg- open sets are independent of each other.*

Example 3.4. *Let $X = \{a, b, c, d\}$ and let*

(1): *$\tau = \{\phi, \{a\}, \{c\}, \{d\}, \{a, c\}, \{a, d\}, \{c, d\}, \{a, c, d\}, X\}$. Then $\{a, b, c\}$ is semi open but not rsg-open, similarly let*

(2): *$\tau = \{\phi, \{a\}, \{c, d\}, \{a, c, d\}, \{b, c, d\}, X\}$. Then $\{b\}$ is rsg-open but not semi open.*

Example 3.5. *The union of two rsg-open sets is generally not rsg-open. To see this in Example 3.4(1), $\{a\}$ and $\{b\}$ are rsg-open sets in X but $\{a, b\}$ is not rsg-open. Therefore, the intersection of two rsg-closed sets is generally not rsg-closed.*

Theorem 3.6. *If A and B are rsg-open, then $A \cap B$ is rsg-open.*

Proof. If $G \subset A \cap B$ and G is semi-regular, then $G \subset Int(A)$ and $G \subset Int(B)$ and hence $G \subset Int(A) \cap Int(B) = Int(A \cap B)$. By Theorem 3.2, $A \cap B$ is rsg-open.

Theorem 3.7. *The union of two rsg-closed sets is rsg-closed.*

Proof. This is an immediate consequence of Theorem 3.6.

Diagram

$$\begin{array}{ccccc} \text{closed} & \longrightarrow & \text{s*g-closed} & \longrightarrow & \text{g-closed} \\ & & \searrow & & \searrow \\ & & \text{rsg-closed} & \longrightarrow & \text{rg-closed} \end{array}$$

Remark 3.8. *In Example 3.4(1), $\{a, c, d\}$ is rsg- closed but it is neither g-closed nor sg-closed. $\{c, d\}$ is sg-closed but not rsg-closed. Let $X = \{a, b, c, d\}$ and let $\tau = \{\phi, \{a\}, \{b\}, \{a, b\}, X\}$, then $\{c\}$ is g-closed but not rsg-closed.*

Remark 3.9. *By Remark 3.8, we have*

(1): *rsg-closedness and g-closedness are independent of each other.*

(2): *rsg-closedness and sg-closedness are also independent of each other.*

Theorem 3.10. *If a set A is rsg-closed, then $cl(A) - A$ contains no non empty semi-regular set.*

Proof. Let F be a semi-regular subset of $cl(A)-A$. Then $A \subset X-F$ and since A is rsg-closed and $X-F$ is semi-regular, we have $cl(A) \subset X-F$ or $F \subset X-cl(A)$. Thus $F \subset cl(A) \cap (X-cl(A)) = \phi$. Therefore F is empty.

Theorem 3.11. *If A is an rsg-closed subset of X, then $cl(A)-A$ is rsg-open.*

Proof. Let A be an rsg-closed subset of X and G be a semi-regular subset of X such that $G \subset cl(A)-A$. By Theorem 3.10, $G = \phi$ and thus $G \subset Int[cl(A)-A]$. By Theorem 3.2, $cl(A)-A$ is an rsg-open set.

Definition 3.12. *A subset A of a space X is said to be preopen* [14] *if $A \subset Int(cl(A))$.*

Lemma 3.13. *(Dorsett* [8]*). Let A be a preopen set in a space (X,τ), then $SR(A,\tau_A) = SR(X,\tau) \cap A$, where $SR(X,\tau)$ denotes the family of all semi-regular sets of (X,τ).*

Definition 3.14. *A subset B of a space X is said to be rsg-closed relative to A if $cl_A(B) \subset G$ whenever $B \subset G$ for every semi-regular set G in A.*

Theorem 3.15. *Let $B \subset A \subset X$ and X be a space. If B is an rsg-closed set relative to A and A is open and s*g-closed in X, then B is rsg-closed relative to X.*

*Proof. Let $B \subset G$ and suppose that G is semi-regular in X. Then $B \subset A \cap G$. Therefore $cl_A(B) \subset A \cap G$ since by Lemma 3.13, $A \cap G$ is semi-regular in A. It follows that $A \cap cl_X(B) \subset A \cap G$ or $A \subset G \cup (X - cl_X(B))$. Since A is s*g-closed, $cl_X(A) \subset G \cup (X - cl_X(B))$ or $cl_X(B) \subset G$. This proves that B is rsg-closed relative to X.*

Corollary 3.16. *Let A be an open and s*g-closed subset of the space X and F be a closed subset of X. Then $A \cap F$ is an rsg-closed set.*

Proof. $A \cap F$ is closed in A and hence rsg-closed in A. By Theorem 3.15, $A \cap F$ is rsg-closed relative to X.

Theorem 3.17. *Let $B \subset A \subset X$ and suppose that B is rsg-closed in X and A is pre-open in X. Then B is rsg-closed relative to A.*

Proof. Let $B \subset A \cap G$ and suppose that G is semi-regular in X then by Lemma 3.13, $A \cap G$ is semi-regular in A. Now $B \subset G$ implies that $cl_A(B) \subset G$. It follows that $A \cap cl_X(B) \subset A \cap G$. This gives $cl_A(B) \subset A \cap G$. This proves that B is rsg-closed relative to A.

Corollary 3.18. *Let $B \subset A \subset X$ where A is open and s*g-closed. Then B is rsg-closed relative to A if and only if B is rsg-closed in X.*

Proof. This is an immediate consequence of Theorems 3.15 and 3.17.

Theorem 3.19. *If B is a subset of a space X such that $A \subset B \subset cl(A)$ and A is an rsg-closed set in X, then B is also rsg-closed in X.*

Proof. Let G be a semi-regular set containing B, then $A \subset G$. Since A is rsg-closed, therefore $cl(A) \subset G$. This gives $cl(B) \subset G$. Hence B is rsg-closed in X.

Corollary 3.20. *If B is a subset of a space X such that $Int(A) \subset B \subset A$, where A is an rsg-open set in the space X, then B is also rsg-open in X.*

Proof. Let F be any semi-regular set contained in B. Then $F \subset A$. Since A is rsg-open, therefore $F \subset Int(A)$. This gives $F \subset Int(B)$. Hence B is rsg-open.

Definition 3.21. *A space X is said to be locally indiscrete* [7] *if every open set in it is closed.*

Theorem 3.22. *In a locally indiscrete space X, a subset A is rsg-open in X if and only if $G = X$ whenever G is semi-regular and $Int(A) \cup (X - A) \subset G$.*

Proof. Necessity. Suppose that G is semi-regular and that $Int(A) \cup (X - A) \subset G$. Now $(X - G) \subset cl(X - A) \cap A = cl(X - A) - (X - A)$. Since $(X - G)$ is semi-regular and $(X - A)$ is rsg-closed, by Theorem 3.10 it follows that $(X - G) = \phi$ or $X = G$.

Sufficiency. Suppose that F is a semi-regular set and $F \subset A$. It suffices to show that $F \subset Int(A)$. Now $Int(A) \cup (X - A) \subset Int(A) \cup (X - F)$ and hence $Int(A) \cup (X - F) = X$. It follows that $F \subset Int(A)$.

Theorem 3.23. *If $A \subset Y \subset X$ where A is rsg-open relative to Y and Y is open in X, then A is rsg-open relative to X.*

Proof. Let F be any semi-regular subset of X contained in A. Since Y is open, therefore by Lemma 3.13, F is semi-regular in Y. Since A is rsg-open relative to Y, therefore $F \subset Int_Y(A)$. Since Y is open in X, $F \subset Int_Y(A) = Int_X(A)$. This proves that A is rsg-open in X.

Theorem 3.24. *For each $x \in X$, either $\{x\}$ is semi-regular or $X - \{x\}$ is rsg-closed.*

Proof. If $\{x\}$ is not semi-regular, then the only semi-regular superset of $X - \{x\}$ is X itself. Hence the closure of $X - \{x\}$ is contained in each of its semi-regular neighbourhoods and $X - \{x\}$ is rsg-closed.

Theorem 3.25. *Let A and B be subsets of spaces X and Y, respectively, then A and B are rsg-closed in X and Y, respectively, if $A \times B$ is rsg-closed in $X \times Y$.*

Proof. Let G and H be semi-regular subsets of X and Y, respectively, such that $A \subset G$ and $B \subset H$. This implies $A \times B \subset G \times H$ where $G \times H$ is semi-regular in $X \times Y$. Since $A \times B$ is rsg-closed in $X \times Y$, therefore $cl(A \times B) = cl(A) \times cl(B) \subset G \times H$ or $cl(A) \subset G$ and $cl(B) \subset H$. This proves that A and B are rsg-closed in X and Y, respectively.

Theorem 3.26. *Let X and Y be two spaces and A be a subset of a space X,*

(1): *If $A \times Y$ is rsg-open in $X \times Y$, then A is rsg-open in X;*
(2): *If $A \times Y$ is rsg-closed in $X \times Y$, then A is rsg-closed in X.*

Proof. (1) Let G be a semi-regular set in X such that $G \subset A$. Since $G \times Y$ is a semi-regular set in $X \times Y$, then by definition $G \times Y \subset Int(A \times Y) = Int(A) \times Int(Y) = Int(A) \times Y$. This gives that $G \subset Int(A)$. This proves that A is rsg-open in X.

(2) Let G be a semi-regular set in X such that $A \subset G$. Since $G \times Y$ is semi-regular in $X \times Y$ and $A \times Y \subset G \times Y$. By definition $cl(A) \times Y = cl(A) \times cl(Y) = cl(A \times Y) \subset G \times Y$. This gives that $cl(A) \subset G$. This proves that A is rsg-closed in X.

Theorem 3.27. *Let A be an open and rsg-closed set, then $cl(A)$ is clopen in X.*

Proof. Since A is open, $Int(A) = A \subset Int(cl(A))$. Since $Int(cl(A))$ is semi-regular and A is rsg-closed, we obtain $cl(A) \subset Int(cl(A))$. This proves that $cl(A)$ is clopen.

Theorem 3.28. *A regular open and rsg-closed set is clopen.*

Proof. Let A be regular open then A is semi-regular. This gives that $cl(A) \subset A$. But $A \subset cl(A)$. Therefore A is closed.

Theorem 3.29. *In a locally indiscrete space X, every semi-closed set is rsg-closed.*

Proof. Let A be semi-closed. Then $X-A \in SO(X)$. *Since X is locally indiscrete,* $SO(X) = RO(X)$ *(*[9]*, Theorem 3.3). This shows that* $X - A$ *is regular open in X or A is regular-closed in X. Therefore A is rsg-closed.*

Definition 3.30. *The intersection of all semi-regular subsets of a space X containing a set A is called the semi-regular kernel of A and is denoted by* $srker(A)$.

Lemma 3.31. *A subset A of a space X is rsg-closed if and only if* $cl(A) \subset srker(A)$.

Proof. Assume that A is an rsg-closed set in X. Then $cl(A) \subset G$ *whenever* $A \subset G$ *and G is semi-regular in X. This implies* $cl(A) \subset \cap\{G : A \subset G$ *and* $G \in SR(X)\} = srker(A)$

Conversely. Assume that $cl(A) \subset srker(A)$. *This implies* $cl(A) \subset \cap\{G : A \subset G$ *and* $G \in SR(X)\}$. *This shows that* $cl(A) \subset G$ *for any semi-regular set G containing A. This proves that A is rsg-closed.*

Lemma 3.32. *(Jankovic and Reilly* [10]*). Let x be a point of a space X. Then* $\{x\}$ *is either nowhere dense or preopen.*

Theorem 3.33. *Arbitrary intersection of rsg-closed sets in a locally indiscrete space X is rsg-closed.*

Proof. Let $\{A_\alpha : \alpha \in I\}$ *be an arbitrary collection of rsg-closed sets in a space X and let* $A = \cap_{\alpha \in I} A_\alpha$. *Let* $x \in cl(A)$. *In view of Lemma 3.32, we consider the following two cases.*

Case I. Let $\{x\}$ *be nowhere dense. If* $x \notin A$, *then for some* $j \in I$, *we have* $x \notin A_j$. *Since nowhere dense subsets are semi-closed and X is locally indiscrete, therefore* $X - \{x\}$ *is a regular open set containing* A_j. *Hence* $x \notin srker(A_j)$. *On the other hand, by Lemma 3.31, since* A_j *is rsg-closed,* $x \in cl(A) \subset cl(A_j) \subset srker(A_j)$. *By contradiction,* $x \in A$ *and hence* $x \in srker(A)$.

Case II. Let $\{x\}$ *be preopen. Set* $F = Int(cl(\{x\}))$. *Assume that* $x \notin rsker(A)$. *Then there exists a semi-regular set C containing x such that* $C \cap A = \phi$. *Now by (*[5]*, Theorem 1.2)* $x \in F = Int(cl(\{x\})) \subset Int(cl(C)) \subset C$. *Since F is an open set containing x and* $x \in cl(A)$, *therefore* $F \cap A \neq \phi$. *Since* $F \subset C$, $C \cap A \neq \phi$. *By contradiction* $x \in srker(A)$. *Thus in both cases* $x \in srker(A)$. *By Lemma 3.31, A is rsg-closed.*

Corollary 3.34. *For a locally indiscrete space X, the family of all rsg-open sets of X is a topology for X.*

Proof. This is an immediate consequence of Theorems 3.6 and 3.33.

4. rsg-Regular Spaces

In this section, we define an rsg-regular space and investigate some of its fundamental properties.

Definition 4.1. *A space* (X, τ) *is said to be s-regular* [13] *if for each closed set F and any point* $x \in X - F$, *there exist disjoint semi-open sets U and V in X such that* $x \in U$ *and* $F \subset V$.

Definition 4.2. *A space* (X, τ) *is said to be rsg-regular if for every rsg-closed set F and* $x \in X - F$ *there exist disjoint open sets U and V in X such that* $x \in U$ *and* $F \subset V$.

Remark 4.3. *Every rsg-regular space is regular as well as s-regular but the converse is not true in general.*

Example 4.4. *Let $X = Y \cup Z$ where $Y \cap Z = \phi$ and Y, Z are infinite sets. Let $\tau = \{\phi, Y, Z, X\}$ then (X, τ) is a regular space. If $\phi \neq A \subset Y$ and $x \in Y - A$, then A is an rsg-closed set but A and x can not be separated by disjoint open sets. Hence (X, τ) fails to be an rsg-regular space.*

Theorem 4.5. *The following are equivalent for a space (X, τ):*

(1): *(X, τ) is rsg-regular.*

(2): *For every rsg-open set U containing $x \in X$, there exists an open set G in X such that $x \in G \subset cl(G) \subset U$.*

Proof. (1) $\Rightarrow$ (2) *Let U be any rsg-open set containing $x \in X$. Then $x \notin X - U$, where $X - U$ is rsg-closed in X. Hence there exist disjoint open sets G and H such that $x \in G$ and $X - U \subset H$ or $x \in G \subset cl(G) \subset X - H \subset U$. This proves (2).*

(2) $\Rightarrow$ (1) *Let F be an rsg-closed set and $x \in X - F$. By hypothesis, there exists an open set G in X such that $x \in G \subset cl(G) \subset X - F$ or $x \in G$ and $F \subset X - cl(G)$where $G \cap (X - cl(G)) = \phi$. This proves that X is rsg-regular.*

Definition 4.6. *A space (X, τ) is said to be rsg-regular at a point $x \in X$ if every rsg-open neighbourhood of x contains a closed neighbourhood of x.*

Theorem 4.7. *A space (X, τ) is rsg-regular if and only if it is rsg-regular at each of its points.*

Proof. Suppose X is rsg-regular and $x \in X$. Let U be any rsg-open neighbourhood of $x \in X$. Then $X - U$ is rsg-closed and $x \notin X - U$. Since X is rsg-regular, there exist disjoint open sets G and H such that $x \in G$ and $X - U \subset H$. Now $G \cap H = \phi$ implies $x \in G \subset X - H \subset U$. This proves that X is rsg-regular at each of its points.

Conversely, let X be rsg-regular at each of its points. Let F be an rsg-closed set and $x \in X - F$, where $X - F$ is an rsg-open neighbourhood of x. By hypothesis there exists an open set V of X such that $x \in V \subset cl(V) \subset X - F$. By Theorem 4.5, X is rsg-regular.

Theorem 4.8. *Every open and s*g-closed subspace of an rsg-regular space is rsg-regular.*

*Proof. Suppose X is an rsg-regular space and Y is an open and s*g-closed subspace of X. Let A be an rsg-closed set in Y. By Theorem 3.15, A is an rsg-closed in X. Let $x \in Y - A$, then $x \in X - A$ implies that there exist open sets U and V in X such that $x \in U$, $A \subset V$ and $U \cap V = \phi$; hence $x \in U \cap Y$, $A \subset V \cap Y$, where $U \cap Y$ and $V \cap Y$ are disjoint open sets in Y. This proves that Y is an rsg-regular space.*

Lemma 4.9. *In an rsg-regular space every rsg-open set is the union of open sets.*

Proof. Let U be an rsg-open subset of an rsg-regular space X such that $x \in U$. If $A = X - U$, then A is an rsg-closed set and $x \in X - A$. By hypothesis there exist disjoint open sets W_x and W of X such that $x \in W_x$ and $A \subset W$. It follows that $x \in W_x \subset U$. This completes the proof.

Corollary 4.10. *In an rsg-regular space every rsg-closed set is the intersection of closed sets.*

Definition 4.11. *A space (X, τ) is called a $T_r -$ space if every rsg-closed subset of X is closed.*

Lemma 4.12. *A space (X, τ) is rsg-regular if and only if (X, τ) is a regular and $T_r -$ space.*

Proof. Let X be an rsg-regular space, then X is a regular space. Let A be an rsg-closed subset of X. Let $x \in cl(A)$. If $x \notin A$, then by hypothesis, there exist disjoint open sets U and V containing x and A, respectively. This contradicts that $x \in cl(A)$. Therefore $x \in A$ and hence A is closed.

Conversely, let (X, τ) be a regular and $T_r -$ space. Let A be an rsg-closed subset of X and $x \in X - A$. By definition 4.11, A is closed and by regularity of X, there exist disjoint open sets U and V containing x and A, respectively. This proves that X is an rsg-regular space.

Theorem 4.13. *For a space (X, τ), the following are equivalent:*

(1): *(X, τ) is a $T_r -$ space.*

(2): *Every singleton subset of X is either open or semi-regular.*

Proof. (1) $\Rightarrow$ (2) *Let $x \in X$. Suppose $\{x\}$ is not a semi-regular subset of X. This gives $X - \{x\}$ is not semi-regular and therefore X is the only semi-regular super set of $X - \{x\}$. Trivially $X - \{x\}$ is rsg-closed. By hypothesis, $X - \{x\}$ is closed or $\{x\}$ is open.*

(2) $\Rightarrow$ (1) *Let A be an rsg-closed subset of X. Let $x \in cl(A)$. By hypothesis $\{x\}$ is either open or semi-regular. If $\{x\}$is open, then $\{x\} \cap A \neq \phi$ implies $x \in A$. If $\{x\}$ is semi-regular and $x \notin A$, then $x \in cl(A) - A$. This implies that $cl(A) - A$ contains a nonempty semi-regular set. This contradicts Theorem 3.10. Hence $x \in A$. This proves (1).*

Remark 4.14. *In $T_r -$ space, closed sets, s*g-closed sets and rsg-closed sets coincide.*

References

[1] S. P. Arya and T. M. Nour, Characterizations of s-normal spaces, *Indian J.Pure Appl. Math.,* **21** (1990), 717 - 719.

[2] P. Bhattacharyya and B.K. Lahiri, Semi-generalized closed sets in topology, *Indian J. Math.,* **29** (1987), 375 - 382.

[3] P. Bhattacharya and B. K. Lahiri, Semi-generalized continuous maps in topological spaces, *Portug. Math.,* **52(4)** (1995), 399 - 407.

[4] D.E. Cameron, Properties of S-closed spaces, *Proc. Amer. Math. Soc.,* **72** (1978), 581 - 586.

[5] S. G. Crossley and S. K. Hildebrand, Semi-topological properties, *Fund. Math.,* **74** (1972), 233 - 254.

[6] G. Di Maio and T. Noiri, On s-closed spaces, *Indian J. Pure Appl. Math.,* **18(3)** (1987), 226 - 233.

[7] K. Dlaska, N. Ergun and M. Ganster, On the topology generalized by semi regular sets, *Indian J. Pure Appl. Math.,* **25(11)** (1995), 1163 - 1170.

[8] C. Dorsett, Pre-open sets and feeble separation axioms, *Ann. Univ. Timisoara Ser. St. Mat.,* **25** (1987), 39 - 48.

[9] D. S. Jankovic , On locally irreducible spaces, *Ann. Soc. Sci. Bruxelles,* **97** (1983), 59 - 72.

[10] D. S. Jankovic and I.L. Railly, On semi-separation properties, *Indian J. Pure Appl. Math.,* **16(9)** (1985), 957 - 964.

[11] N. Levine, Semi-open sets and semi-continuity in topological spaces, *Amer. Math. Monthly,* **70(1)** (1963), 36 - 41.

[12] N. Levine, Generalized closed sets in topological spaces, *Rend. Circ. Mat. Palermo,* **19(2)** (1970), 89 - 96.

[13] S.N. Maheshwari and R. Prasad, On s-regular spaces, *Glasnik Mat.,* **10(30)** (1975), 347 - 350.
[14] A. S. Mashhour, M. E. Abd El-Monsef and S. N. El-Deep, On precontinuous and weak precontinuous mappings, *Proc. Math. Phys. Soc. Egypt.,* **53** (1982), 47 - 53.
[15] N. Palaniappan and K.C. Rao, Regular generalized closed sets, *Kyungpook Math. J.,* **33** (1993), 211 - 219.
[16] K.C. Rao and K. Joseph, Semi star generalized closed sets, *Bull. Pure Appl. Sci.,* **19(E)(2)** (2002), 281 - 290.

T.Noiri, 2949-1 Shiokita-cho, Hinagu, Yatsushiro-shi, Kumamoto-ken, 869-5142 JAPAN

M.Khan, Department of Mathematics, COMSATS Institute of Information Technology, Park Road, Islamabad, PAKISTAN

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 2, Pages 57–65
ISSN 1930-1235: (2010)

ON τ-$\oplus$-SUPPLEMENTED MODULES

Y. TALEBI, T. AMOOZEGAR, AND A. R. MONIRI HAMZEKOLAEI

Abstract. Let τ be any preradical and M any module. In [2], Al-Takhman, Lomp and Wisbauer defined τ-supplemented module. In this paper we introduce the (completely) τ-$\oplus$-supplemented modules. It is shown that (1) Any finite direct sum of τ-$\oplus$-supplemented modules is τ-$\oplus$-supplemented. (2) If M is τ-$\oplus$-supplemented module and (D_3) then M is completely τ-$\oplus$-supplemented.

1. Introduction

Throughout this paper R will denote an arbitrary associative ring with identity and all modules will be unitary right R-modules. A functor τ from the category of the right R-modules to itself is called a *preradical* if it satisfies the following properties:

(1) $\tau(M)$ is a submodule of an R-module M,

(2) If $f : M' \to M$ is an R-module homomorphism, then $f(\tau(M')) \subseteq \tau(M)$ and $\tau(f)$ is the restriction of f to $\tau(M')$.

A preradical τ is called a *right exact preradical* if for any submodule K of M, $\tau(K) = \tau(M) \cap K$. But it is well known if K is a direct summand of M, then $\tau(K) = \tau(M) \cap K$ for a preradical.

Let M be an R-module and τ denote a preradical. Like in [2], a submodule $K \leq M$ is called τ-supplement (weak τ-supplement) provided there exists some $U \leq M$ such that $M = U + K$ and $U \cap K \subseteq \tau(K)$ $(U \cap K \subseteq \tau(M))$.

M is called *τ-supplemented* (*weakly τ-supplemented*) if each of its submodules has a τ-supplement (weak τ-supplement) in M. M is called *amply τ-supplemented*, if for all submodules K and L of M with $K + L = M$, K contains a τ-supplement of L in M. Kosan and Harmanci [9] studied supplemented modules relative to torsion theories. Motivated by their work, we study $\oplus$-supplemented modules with respesct to a preradical. Also another work has been done on C_1 modules (see [12]).

A module M is called *τ-lifting* if for every submodule K of M, there is a decomposition $K = A \oplus B$, such that A is a direct summand of M and $B \subseteq \tau(M)$.

In this paper we introduce the (completely) τ-$\oplus$-supplemented modules and investigate some properties of them.

Our paper is organized as follows.

In Section 2, we define the concept of τ-$\oplus$-supplemented module. We call a module M *τ-$\oplus$-supplemented* if every submodule of M has a τ-supplement that is a direct summand of M. Then we show any finite direct sum of τ-$\oplus$-supplemented modules is τ-$\oplus$-supplemented. We also investigate when a direct summand of a τ-$\oplus$-supplemented module is τ-$\oplus$-supplemented.

In Section 3, we call a module M *completely τ-$\oplus$-supplemented* if every direct summand of M is τ-$\oplus$-supplemented and prove if M is τ-$\oplus$-supplemented module and (D_3), then M is completely τ-$\oplus$-supplemented.

The notation $N \leq_d M$ denotes that N is a direct summand of M.

Definition 1.1. For any preradical τ, we call a module M, *τ-$\oplus$-supplemented* if every submodule of M has a τ-supplement that is a direct summand of M.

Theorem 1.2. *For any preradical τ, any finite direct sum of τ-$\oplus$-supplemented modules is τ-$\oplus$-supplemented.*

Proof. Let $M = M_1 \oplus M_2$ where M_1 and M_2 are two τ-$\oplus$-supplemented modules. Let P be any submodule of M. We have $P + M_2 = M_2 \oplus [(P + M_2) \cap M_1]$ and $(P + M_2) \cap M_1$ is a submodule of M_1. Since M_1 is τ-$\oplus$-supplemented, there exists a direct summand K_1 of M_1 such that $[(P + M_2) \cap M_1] + K_1 = M_1$ and $(P + M_2) \cap K_1 \subseteq \tau(K_1)$. We have $(P + K_1) \cap M_2$ is a submodule of M_2, so there exists a direct summand K_2 of M_2 such that $[(P + K_1) \cap M_2] + K_2 = M_2$ and $(P+K_1)\cap K_2 \subseteq \tau(K_2)$. Let $K = K_1 \oplus K_2$, K is a direct summand of M. Moreover $M_1 \leq P + M_2 + K_1$ and $M_2 \leq P + K_1 + K_2$. Hence $M = P + K_1 + K_2 = P + K$. Since $P\cap(K_1+K_2) \leq [(P+K_1)\cap K_2]+[(P+K_2)\cap K_1]$, thus $P\cap(K_1+K_2) \leq [(P+K_1)\cap K_2]+[(P+N_2)\cap K_1]$. As $(P+M_2)\cap K_1 \subseteq \tau(K_1)$ and $(P+K_1)\cap K_2 \subseteq \tau(K_2)$, we have $(P \cap K) \subseteq \tau(K)$. Thus M is τ-$\oplus$-supplemented. □

A nonzero module M is called *completely torsion* if for every proper submodule K of M, $K \subseteq \tau(M)$.

Corollary 1.3. *For any preradical τ, any finite direct sum of completely torsion modules is τ-$\oplus$-supplemented.*

Theorem 1.4. *Let M_i $(1 \leq i \leq n)$ be any finite collection of relatively projective modules. Then for any preradical τ, the module $M = \bigoplus_{i=1}^{n} M_i$ is τ-$\oplus$-supplemented if and only if M_i is τ-$\oplus$-supplemented for each $1 \leq i \leq n$.*

Proof. The sufficiency is proved in Theorem 1.2. Conversely, we only prove M_1 to be τ-$\oplus$-supplemented. Let $A \leq M_1$. Then there exists $B \leq M$ such that $M = A + B$, B is a direct summand of M and $A\cap B \subseteq \tau(B)$. Since $M = A+B = M_1+B$, by [10, Lemma 4.47], there exists $B_1 \leq B$ such that $M = M_1\oplus B_1$. Thus $B = B_1\oplus(M_1\cap B)$. Note that $M_1 = A + (M_1 \cap B)$ and $M_1 \cap B$ is a direct summand of M_1. Therefore $A \cap B = A \cap (M_1 \cap B) \subseteq \tau(B) \cap (M_1 \cap B) = \tau(M_1 \cap B)$. Hence M_1 is τ-$\oplus$-supplemented. □

A factor module of a τ-$\oplus$-supplemented module need not be τ-$\oplus$-supplemented for $\tau = Rad$ (see [6, Examples 2.2 and 2.3]).

Theorem 1.5. *Let M be a τ-$\oplus$-supplemented module for any preradical τ and $X \leq M$. If for every direct summand K of M, $(X + K)/X$ is a direct summand of M/X, then M/X is τ-$\oplus$-supplemented.*

Proof. Let $N/X \leq M/X$. Since M is τ-$\oplus$-supplemented, there exists a direct summand K of M such that $N + K = M$ and $N \cap K \subseteq \tau(K)$. Then $N/X + (K + X)/X = M/X$. By assumption, $(K + X)/X$ is a direct summand of M/X. It is easy to check that $(N/X) \cap ((K + X)/X) \subseteq \tau((K + X)/X)$. □

Let M be a module. Then M is called *distributive* if its lattice of submodules is a distributive lattice, equivalently for submodules K, L, N of M, $N + (K \cap L) = (N + K) \cap (N + L)$ or $N \cap (K + L) = (N \cap K) + (N \cap L)$.
Let M be a module. A submodule X of M is called *fully invariant*, if for every $f \in End(M)$, $f(X) \subseteq X$. The module M is called *duo module*, if every submodule of M is fully invariant. The submodule A of M is called *projection invariant* in M if $f(A) \subseteq A$, for any idempotent $f \in End(M)$.

Corollary 1.6. *Let M be a τ-$\oplus$-supplemented module for any preradical τ.*
(1) Let $N \leq M$ such that for each decomposition $M = M_1 \oplus M_2$ we have $N = (N \cap M_1) \oplus (N \cap M_2)$. Then M/N is τ-$\oplus$-supplemented. (In particular, this is true for any distributive module). If moreover $N \leq_d M$, then N is τ-$\oplus$-supplemented.
(2) Let X be a projection invariant submodule of M. Then M/X is τ-$\oplus$-supplemented. In particular, for every fully invariant submodule A of M, M/A is τ-$\oplus$-supplemented.

Proof. (1) Let $L/N \leq M/N$. Since M is τ-$\oplus$-supplemented, there exists a direct summand D of M such that $M = L + D$ and $L \cap D \subseteq \tau(D)$. Then $M/N = L/N + (D + N)/N$ and $L/N \cap (D + N)/N = (L \cap (D + N))/N \subseteq \tau((D + N)/N)$. Let $M = D \oplus D'$. By assumption, $N = (N \cap D) \oplus (N \cap D') = (D + N) \cap (D' + N)$. So, $(D + N)/N \oplus (D' + N)/N = M/N$. It follows that M/N is τ-$\oplus$-supplemented.
Now let $N \leq_d M$ and $V \leq N$. Then there exist submodules K and K' of such that $M = K \oplus K' = V + K$ and $V \cap K \subseteq \tau(K)$. Thus $N = V + N \cap K$. By assumption $N \cap K \leq_d N$. Moreover, $V \cap (N \cap K) \subseteq \tau(K)$. Then $V \cap (N \cap K) \subseteq \tau(N \cap K)$. Therefore, N is τ-$\oplus$-supplemented.
(2) Clear by (1). □

Let M be an R-module. By $P_\tau(M)$ we denote the sum of all submodules N of M with $\tau(N) = N$. Since $P_\tau(M)$ is a sum of some submodules of M, itself is a submodule of M.

Corollary 1.7. *Let M be a τ-$\oplus$-supplemented module for any preradical τ. Then $M/P_\tau(M)$ is τ-$\oplus$-supplemented. If moreover $P_\tau(M) \leq_d M$, then $P_\tau(M)$ is τ-$\oplus$-supplemented.*

Proof. By Corollary 1.6(1), it suffices to prove that $P_\tau(M)$ is a fully invariant submodule of M. Let $N \leq M$ such that $N = \tau(N)$ and $f \in End(M)$ and g its restriction to N. But $\tau(N) = N$ and $f(N) = g(N)$, hence $f(N) \subseteq \tau(f(N))$. Thus, $\tau(f(N)) = f(N)$. This implies that $f(N) \subseteq P_\tau(M)$. This completes the proof. □

We recall that a module M is called *semi-Artinian* if every nonzero quotient module of M has nonzero socle. For a module M, we define $Sa(M) = \sum\{U \leq M \mid U semi-Artinian\}$.

Corollary 1.8. *Let M be a τ-$\oplus$-supplemented module for any preradical τ. Then $M/Sa(M)$ is τ-$\oplus$-supplemented. If, moreover, $Sa(M)$ is a direct summand of M, then $Sa(M)$ is also τ-$\oplus$-supplemented.*

Proof. Let $f \in End(M)$ and U a semi-Artinian submodule. Let g be restriction of f to U. Thus $U/Ker(g) \cong g(U)$. Hence $f(U) \cong U/Ker(g)$. But it is easy to check that $U/Ker(g)$ is a semi-Artinian module. Therefore, $f(U)$ is semi-Artinian. This implies that $f(Sa(M)) \subseteq Sa(M)$. Thus $Sa(M)$ is a fully invariant submodule of M. The result follows from Corollary 1.6(1). □

Remark 1.9. If M is a τ-$\oplus$-supplemented module for any preradical τ, then $M/\tau(M)$ is semisimple and hence τ-$\oplus$-supplemented.

Example 1.10. Let M be the Z-module $Z/2Z \oplus Z/8Z$. By [8, Example 10], M is not lifting and it is not τ-lifting. By [5, Theorem 1.4], M is $\oplus$-supplemented and hence τ-$\oplus$-supplemented for $\tau = Rad$.

A τ-lifting module is τ-$\oplus$-supplemented. But the converse does not hold. The following proposition shows that under some assumption it can be true.

Proposition 1.11. *Assume M is τ-$\oplus$-supplemented for any preradical τ such that whenever $M = M_1 \oplus M_2$ then M_1 and M_2 are relatively projective. Then M is τ-lifting.*

Proof. Let $N \leq M$. Since M is τ-$\oplus$-supplemented, there exists a decomposition $M = M_1 \oplus M_2$ such that $M = N + M_2$ and $N \cap M_2 \subseteq \tau(M_2)$ for submodules M_1, M_2 of M. By hypothesis, M_1 is M_2-projective. By [10, Lemma 4.47], we obtain $M = A \oplus M_2$ for some submodule A of M such that $A \leq N$. Then $N = A \oplus (M_2 \cap N)$. So M is τ-lifting by [2, 2.8]. □

Corollary 1.12. *Let M be a τ-$\oplus$-supplemented module for any prerardical τ. If M is projective then M is τ-lifting.*

Now we give a characterization of τ-$\oplus$-supplemented rings.

Theorem 1.13. *Let τ be any preradical. Then the following are equivalent:*
(1) *R is τ-$\oplus$-supplemented;*
(2) *Every finitely generated free R-module is τ-$\oplus$-supplemented;*
(3) *If F is a finitely generated free R-module and N a fully invariant submodule, then F/N is τ-$\oplus$-supplemented.*

Proof. (1) $\Rightarrow$ (2) Let M be a finitely generated free R-module. Then $M \cong \bigoplus_{i=1}^{n} R$. Since any finite direct sum of τ-$\oplus$-supplemented modules is τ-$\oplus$-supplemented, the result follows.

(2) $\Rightarrow$ (3) By (2), F is τ-$\oplus$-supplemented. The result follows from Corollary 1.6(2).

(3) $\Rightarrow$ (1) is clear. □

Lemma 1.14. *Let $M = M_1 \oplus M_2$. Then for any preradical τ, M_2 is τ-$\oplus$-supplemented if and only if for every submodule N/M_1 of M/M_1, there exists a direct summand K of M such that $K \leq M_2$, $M = K + N$ and $N \cap K \subseteq \tau(M)$.*

Proof. Suppose that M_2 is τ-$\oplus$-supplemented. Let $N/M_1 \leq M/M_1$. As M_2 is τ-$\oplus$-supplemented, there exists a decomposition $M_2 = K \oplus K'$ such that $M_2 = (N \cap M_2) + K$ and $N \cap K \subseteq \tau(K)$. Note that $M = (N \cap M_2) + K + M_1$ gives $M = N + K$.

Conversely, suppose that M/M_1 has the stated property. Let H be a submodule of M_2. Consider the submodule $(H \oplus M_1)/M_1 \leq M/M_1$. By hypothesis, there exists a direct summand L of M such that $L \leq M_2$, $M = (L + H) + M_1$ and $L \cap (H + M_1) \subseteq \tau(M)$. By modularity, $M_2 = L + H$. Then $L \cap H \subseteq \tau(L)$. Thus, L is a τ-supplement of H in M_2 and it is a direct summand of M_2. Therefore, M_2 is τ-$\oplus$-supplemented. □

Theorem 1.15. *Let τ be any preradical and M_2 a direct summand of a τ-$\oplus$-supplemented module M such that for every direct summand K of M with $M = K + M_2$, $K \cap M_2$ is a direct summand of M. Then M_2 is τ-$\oplus$-supplemented.*

Proof. Suppose that $M = M_1 \oplus M_2$ and let $N/M_1 \leq M/M_1$. Consider the submodule $N \cap M_2$ of M. Since M is τ-$\oplus$-supplemented, there exists a direct summand K of M such that $M = (N \cap M_2) + K$ and $N \cap M_2 \cap K \subseteq \tau(K)$. Note that $M = N + M_2$. By [7, Lemma 1.2], $M = (K \cap M_2) + N$. Since $M = K + M_2$, $K \cap M_2$ is a direct summand of M by hypothesis. By Lemma 1.14, M_2 is τ-$\oplus$-supplemented. □

Corollary 1.16. *Let M be a τ-$\oplus$-supplemented module for any preradical τ and K a direct summand of M such that M/K is K-projective. Then K is τ-$\oplus$-supplemented.*

Proof. Let L be a direct summand of M with $M = L + K$. Since K is a direct summand of M, $M = K \oplus K_0$ for some submodule K_0 of M. Therefore, K_0 is K-projective. Then by [16, 41.14], there exists a submodule L_0 of L such that $M = L_0 \oplus K$. Now $L = L' \oplus (L \cap K)$ implies that $L \cap K$ is a direct summand of M. By Theorem 1.15, K is τ-$\oplus$-supplemented. □

Corollary 1.17. *Let M be a τ-$\oplus$-supplemented module for any preradical τ and $N \leq_d M$ such that M/N is projective. Then N is τ-$\oplus$-supplemented.*

A submodule N of M is called *small* in M (notation $N \ll M$) if $\forall L \lneq M, L+N \neq M$. A module M is called *hollow* if every proper submodule of M is small in M.

Let M be a module and S denote the class of all small modules. Talebi and Vanaja [13] defined $\overline{Z}(M)$ as follows:

$\overline{Z}(M) = \bigcap\{kerg \mid g \in Hom(M, L), L \in S\}$. The module M is called *cosingular (non-cosingular)* if $\overline{Z}(M) = 0$ ($\overline{Z}(M) = M$). Clearly every non-cosingular module is $\overline{Z}$-$\oplus$-supplemented. Also if R is a non-cosingular ring, then every R-module is $\overline{Z}$-$\oplus$-supplemented by [13, Proposition 2.4].

In [11] for any preradical τ, the authors call a module M, τ-semiperfect if it is satisfies one of the following conditions (see [11, Proposition 2.1]):

(1) For every submodule K of M there exists a decomposition $K = A \oplus B$ such that A is a projective direct summand of M and $B \subseteq \tau(M)$;

(2) For every submodule K of N, there exists a decomposition $M = A \oplus B$ such that A is a projective direct summand of M, $A \leq K$ and $K \cap B \subseteq \tau(M)$.

By this definition every τ-semiperfect module is τ-lifting and hence τ-$\oplus$-supplemented. Also if M is projective we have the following:

τ-semiperfect $\Leftrightarrow$ τ-lifting $\Leftrightarrow$ τ-$\oplus$-supplemented.

A τ-$\oplus$-supplemented module need not be $\oplus$-supplemented and the converse also hold.

Example 1.18. Let K be a field and let $R = \prod_{n\geq 1} K_n$ with $K_n = K$. By [14, Example 4.1(1)] R is not semiperfect. Since R is projective, R is not $\oplus$-supplemented by [5, Lemma 1.2]. Again by [14, Example 4.1(1)], the module R is $\overline{Z}$-semiperfect and so it is $\overline{Z}$-$\oplus$-supplemented.

If R is a DVR (Discrete Valuation Ring) , then by [14, Example 4.1(1)] the R-module R_R is semiperfect and hence $\oplus$-supplemented but it is not $\overline{Z}$-semiperfect and so it is not $\overline{Z}$-$\oplus$-supplemented.

Now we give an equivalent condition for a module to be $\overline{Z}$-$\oplus$-supplemented under some assumptions.

Proposition 1.19. *Let R be a commutative ring and P a projective module with $Rad(P) \ll P$ and P has finite hollow dimension. Then the following are equivalent:*
(1) *P is $\overline{Z}$-$\oplus$-supplemented;*
(2) *$P = P_1 \oplus P_2 \oplus P_3$ with P_1 is $\oplus$-supplemented and $Rad(P_1) = \overline{Z}(P_1)$, P_2 is semisimple and $\overline{Z}(P_3) = P_3$.*

Proof. (1) $\Rightarrow$ (2) By the proof of [14, Corollary 4.3] and since every semiperfect is $\oplus$-supplemented .
(2) $\Rightarrow$ (1) By [14, Corollary 4.3] all P_1, P_2 and P_3 are $\overline{Z}$-semiperfect and hence $\overline{Z}$-$\oplus$-supplemented. Since any finite direct sum of $\overline{Z}$-$\oplus$-supplemented modules is $\overline{Z}$-$\oplus$-supplemented, P is $\overline{Z}$-$\oplus$-supplemented. □

Let $e = e^2 \in R$. Then e is called a *left (right) semicentral idempotent* if $xe = exe$ ($ex = exe$), for all $x \in R$. The set of all left (right) semicentral idempotents is denoted by $S_l(R)$ ($S_r(R)$). A ring R is called *Abelian* if every idempotent is central.

Let M be a module. We consider the following condition.

(D_3) If M_1 and M_2 are direct summands of M with $M = M_1 + M_2$, then $M_1 \cap M_2$ is also a direct summand of M.

By [10, Lemma 4.6 and Proposition 4.38], every quasi-projective module is (D_3).

Proposition 1.20. *Let M be an R-module such that $End(M)$ is Abelian and $X \leq M$ implies $X = \sum_{i\in I} h_i(M)$ where $h_i \in End(M)$. Then for any preradical τ, M is τ-$\oplus$-supplemented if and only if M is τ-lifting and has (D_3)-condition.*

Proof. The sufficiency is obvious. Conversely, let $X \leq M$, $X = \sum_{i\in I} h_i(M)$ with $h_i(M) \in End(M)$. Since M is τ-$\oplus$-supplemented, there exists a direct summand eM such that $X + eM = M$ and $(X \cap eM) \subseteq \tau(eM)$ for some $e^2 = e \in End(M)$. Since $End(M)$ is Abelian, $(1-e)X = (1-e)M = (1-e)\sum_{i\in I} h_i(M) = \sum_{i\in I} h_i(1-e)(M) \subseteq X$. Therefore $X = (1-e)M \oplus (X \cap eM)$. Hence M is τ-lifting. If $eM + fM = M$ for $e^2 = e$, $f^2 = f \in End(M)$, then $eM \cap fM = efM$ with $(ef)^2 = ef$. So M has (D_3)-condition.

□

Recall that an R-module M is said to be a *multiplication module* if for each $X \leq M$ there exists $A_R \leq R_R$ such that $X = MA$.

Corollary 1.21. *If M satisfies one of the following conditions, then M is τ-lifting if and only if M is τ-$\oplus$-supplemented for any preradical τ.*
(1) *M is cyclic and R is commutative.*
(2) *M is a multiplication module and R is commutative.*

Proof. (1) Assume that M is cyclic and R is commutative. There exists $B_R \leq R_R$ such that $M \cong R/B$. Let $Y/B \leq R/B$, $Y/B = \sum_{i\in I}(y_iR + B) = (\sum_{i\in I} y_i + B)R$ where each $y_i \in Y$. Define $h_i : R/B \to R/B$ by $h_i(r + B) = y_ir + B$, $i \in I$. Then it is easy to check that $h_i \in End_R(R/B)$. Hence $Y/B = \sum_{i\in I} h_i(R/B)$. Since R is commutative, $End_R(R/B)$ is also commutative. By Proposition 1.20, M is τ-lifting.
(2) Assume M is a multiplication module. Let $X \leq M$. Then $X = MA$ for some $A_R \leq R_R$. For each $a \in A$, define $h_\alpha : M \to M$ by $h_\alpha(m) = ma$ for all $m \in M$. Then h_α is an R-homomorphism and $X = MA = \sum_{\alpha\in A} h_\alpha(M)$. Since every multiplication module is a duo module, thus if $e^2 = e \in S = End(M)$, then e,

$1-e \in S_l(S)$. Therefore e is central. So $End(M)$ is Abelian. Again by Proposition 1.20, M is τ-lifting.

□

2. Completely τ-$\oplus$-Supplemented Modules

Definition 2.1. For any preradical τ, we call a module M *completely τ-$\oplus$-supplemented* for any preradical τ if every direct summand of M is a τ-$\oplus$-supplemented.

Theorem 2.2. *Let M be a module with (D_3) and τ a preradical. Then M is τ-$\oplus$-supplemented if and only if M is completely τ-$\oplus$-supplemented.*

Proof. Sufficiency is clear. Conversely, assume that M is τ-$\oplus$-supplemented and K a direct summand of M and A a submodule of K. We show A has a τ-supplement in K that is a direct summand of K. Since M is τ-$\oplus$-supplemented, there exists a direct summand B of M such that $M = A + B$ and $A \cap B \subseteq \tau(B)$. Then $K = A + (K \cap B)$. Furthermore $K \cap B$ is a direct summand of M because M has (D_3). Then $A \cap (K \cap B) = (A \cap B) \cap (K \cap B) \subseteq \tau(B) \cap (K \cap B) = \tau(K \cap B)$. □

A submodule K of M is called *essential* in M (notation $K \leq_e M$) if $K \cap A \neq 0$ for any nonzero submodule A of M.

Proposition 2.3. *Let M be a τ-supplemented module for any preradical τ. Then $M = M_1 \oplus M_2$, where M_1 is semisimple module and M_2 is a module with $\tau(M_2)$ essential in M_2.*

Proof. See [2, 2.2]. □

Recall that a module M has the *Summand Sum Property* (SSP) if the sum of any two direct summand of M is again a direct summand.

Theorem 2.4. (1) *Every τ-lifting module is completely τ-$\oplus$-supplemented for any preradical τ.*

(2) *Let M be a τ-$\oplus$-supplemented module for any preradical τ. If M has the (SSP), then M is completely τ-$\oplus$-supplemented.*

Proof. (1) By [2, 2.10] every direct summand of a τ-lifting module is τ-lifting. The rest is clear.

(2) Assume that M is τ-$\oplus$-supplemented and M has the (SSP). Let N be a direct summand of M. We will show that N is τ-$\oplus$-supplemented. Let $M = N \oplus N'$ for some submodule N' of M. Suppose that A is a direct summand of M. Since M has the (SSP), $A + N'$ is a direct summand of M. Let $M = (A + N') \oplus B$ for some $B \leq M$. Then $M/N' = (A+N')/N' \oplus (B+N')/N'$. Hence by Theorem 1.5, M/N' is τ-$\oplus$-supplemented and so N is τ-$\oplus$-supplemented. □

We give a decomposition of any τ-$\oplus$-supplemented (D_3)-module by the second singular submodule $Z_2(M)$ of M. We will show that if M is τ-$\oplus$-supplemented and $N \leq M$ with M/N projective, then N is τ-$\oplus$-supplemented.

Recall that the *singular submodule* $Z(M)$ of a module M is defined by $Z(M) = \{m \in M \mid mE = 0, E \leq_e R\}$.

The *Goldie torsion submodule (or second singular submodule)* $Z_2(M)$ of M is a submodule of M containing $Z(M)$ such that $Z_2(M)/Z(M)$ is the singular submodule of $M/Z(M)$.

Proposition 2.5. *Let M be a module with (D_3). Suppose that $Z_2(M)$ is τ-coclosed in M. Then for any preradical τ, M is τ-$\oplus$-supplemented if and only if $M = Z_2(M) \oplus K$ for some submodule K of M and, $Z_2(M)$ and K are τ-$\oplus$-supplemented.*

Proof. Sufficiency is clear by Theorem 1.2. Conversely, assume that M is τ-$\oplus$-supplemented. There exist submodules K and K' of M such that $M = K \oplus K' = Z_2(M) + K$ and $Z_2(M) \cap K \subseteq \tau(K)$. Now $Z_2(M) = Z_2(K) \oplus Z_2(K')$. Thus, $M = K \oplus Z_2(K')$ and hence $Z_2(K') = K'$. Note that $Z_2(M) \cap K = Z_2(K) \subseteq \tau(K)$. So, we can obtain that $Z_2(M)/K' \subseteq \tau(M/K')$. Therefore, $Z_2(M) = K'$ because $Z_2(M)$ is τ-coclosed in M. So, $M = K \oplus Z_2(M)$. Clearly K and $Z_2(M)$ are τ-$\oplus$-supplemented. □

Proposition 2.6. *Let M be a τ-supplemented module for any preradical τ. Then $M = M_1 \oplus M_2$, where M_1 is semisimple module and M_2 is a module with $\tau(M_2)$ essential in M_2.*

Proof. See [2, 2.2]. □

Corollary 2.7. *Let M be a τ-$\oplus$-supplemented module for any preradical τ. Then $M = M_1 \oplus M_2$ where M_1 is a semisimple module and M_2 is a module with $\tau(M_2)$ essential in M_2.*

Proof. Since each τ-$\oplus$-supplemented module is τ-supplemented the result follows from Proposition 2.6. □

Proposition 2.8. *Let M be a τ-$\oplus$-supplemented module for a left exact preradical τ. Then $M = M_1 \oplus M_2$ such that $\tau(M_2) = M_2$.*

Proof. Suppose that M is a τ-$\oplus$-supplemented module. There exists a direct summand M_1 of M such that $M = M_1 + \tau(M)$ and $M_1 \cap \tau(M) = \tau(M_1)$ since τ is a left exact preradical and $M = M_1 \oplus M_2$ for some submodule M_2 of M. Then $M = \tau(M_2) \oplus M_1$. Thus $M_2 = \tau(M_2)$. □

Theorem 2.9. *For module M with (D_3) and a left exact preradical τ the following statements are equivalent:*

(1) *M is completely τ-$\oplus$-supplemented;*

(2) *M is τ-$\oplus$-supplemented;*

(3) *$M = M_1 \oplus M_2$, where M_1 is semisimple module and M_2 is a τ-$\oplus$-supplemented module with $\tau(M_2)$ essential in M_2;*

(4) *$M = M_1 \oplus M_2$ such that M_1 is a τ-$\oplus$-supplemented module and M_2 is a τ-$\oplus$-supplemented module with $\tau(M_2) = M_2$.*

Proof. (1) $\Rightarrow$ (2) Clear from definition.

(2) $\Rightarrow$ (1) It follows from Theorem 2.2.

(1) $\Rightarrow$ (3) By Proposition 2.6, $M = M_1 \oplus M_2$, where M_1 is semisimple module and M_2 is module with $\tau(M_2)$ essential in M_2. By (1), M_2 is τ-$\oplus$-supplemented.

(1) $\Rightarrow$ (4) By Proposition 2.8, $M = M_1 \oplus M_2$ such that $\tau(M_2) = M_2$ and M_1, M_2 are τ-$\oplus$-supplemented by (1).

(3) $\Rightarrow$ (2), (4) $\Rightarrow$ (2) follows by Theorem 1.2. □

Lemma 2.10. *Let M be an indecomposable module. Then for any preradical τ, M is completely torsion if and only if M is completely τ-$\oplus$-supplemented.*

Proof. Clear. □

Proposition 2.11. *Let $M = M_1 \oplus M_2$ such that M_1 and M_2 have local endomorphism rings. Then for any preradical τ, M is completely τ-$\oplus$-supplemented if and only if M_1 and M_2 are completely torsion modules.*

Proof. The necessity is clear from Lemma 2.10. Conversely, let K be a direct summand of M. If $K = M$ then by Corollary 1.3, K is τ-$\oplus$-supplemented. Assume $K \neq M$. Then either $K \cong M_1$ or $K \cong M_2$ by [3, Corollary 12.7]. In either case K is τ-$\oplus$-supplemented. Thus M is completely τ-$\oplus$-supplemented. □

References

[1] M. Alkan, On τ-lifting and τ-semiperfect modules, *Turkish J. Math.* **33** (2009), 117–130.
[2] K. Al-Takhman, C. Lomp and R. Wisbaure, τ-complemented and τ-supplemented modules, *Algebra and Discrete Mathematics*, **3** (2006), 1–15.
[3] F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*, Springer-Verlog, New York, 1992.
[4] K. R. Goodearl, *Ring Theory, Nonsingular Rings and Modules*, Marcel Dekker New York - Basel, 1976.
[5] A. Harmanci, D.Keskin and P. F. Smith, On $\oplus$-supplemented modules, *Acta Math. Hungar.* **83** (1999), 161–169.
[6] A. Idelhadj and R. Tribak, On some properties of $\oplus$-supplemented modules, *International Journal of Mathemathics and Mathematical Sciences*, **69** (2003), 4373–4378.
[7] D. Keskin, On lifting modules, *Comm. Alg.* **28**(7) (2000), 3427–3440.
[8] D. Keskin, Finite direct sum of (D_1)-modules, *Turkish J. Math.* **22**(1) (1998), 85–91.
[9] M. T. Kosan and A. Harmanci, Modules supplemented relative to a torsion theory, *Turkish J. Math.* **28** (2004), 177–184.
[10] S. M. Mohamed and B. J. Müller, *Continuous and Discrete Modules*, London Math. Soc. Lecture Notes Series 147, Cambridge, University Press, 1990.
[11] A. Ç. Özcan and M. Alkan, Semiperfect modules with respect to a preradical, *Commun. Alg.* **34** (2006), 841–856.
[12] T. Ozen, C_1 modules with respect to a hereditary torsion theory, *Turkish J. Math.* **33** (2009), 321–329.
[13] Y. Talebi and N. Vanaja, The torsion theory cogenerated by M-small modules, *Comm. Alg.* **30**(3) (2002), 1449-1460.
[14] R. Tribak and D. Keskin, On $\overline{Z}_M$-semiperfect modules, *East-West J. of Mathematicas*, **8**(2) (2006), 193–203.
[15] K. Varadarajan, Dual Goldie dimension, *Comm. Alg.* **21** (1993), 1809–1847.
[16] R. Wisbauer, *Foundations of module and ring theory*, Gordon and Breach, Reading, 1991.

Y. Talebi, Department of Mathematics, Faculty of Mathematical Sciences, University of Mazandaran, Babolsar, Iran
E-mail address: talebi@umz.ac.ir

T. Amoozegar, Department of Mathematics, Faculty of Mathematical Sciences, University of Mazandaran, Babolsar, Iran
E-mail address: t.amoozegar@umz.ac.ir

A. R. Moniri Hamzekolaei, Department of Mathematics, Faculty of Mathematical Sciences, University of Mazandaran, Babolsar, Iran
E-mail address: a.monirih@umz.ac.ir

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 3, Pages 67–77
ISSN 1930-1235: (2010)

COMMON FIXED POINT THEOREMS IN FUZZY METRIC SPACES VIA PROPERTIES

ABDELKRIM ALIOUCHE

Abstract. We prove common fixed point theorems for weakly compatible mappings via an implicit relation in fuzzy metric spaces using property (E.A) and a common property (E.A). Our theorems extend theorems of [1, 3, 4, 6, 15, 16] and a corollary of [2].

1. Introduction and Preliminaries

The concept of fuzzy sets was introduced initially by Zadeh [29] in 1965. To use this concept in topology and analysis, many authors have expansively developed the theory of fuzzy sets and applications. George and Veeramani [12] modified the concept of fuzzy metric space introduced by Kramosil and Michalek [19] and defined the Hausdorff topology of fuzzy metric spaces which have very important applications in quantum particle physics particularly in connections with both string and $E-$infinity theory which were given and studied by El Naschie and Tanaka [8, 9, 10, 11, 28]. They showed also that every metric induces a fuzzy metric. The authors [13, 14, 21] proved fixed point theorems in fuzzy (probabilistic) metric spaces and the authors [2, 4, 5, 7, 23, 27, 30] proved fixed and common fixed point theorems using contractive conditions of integral type and generalized contractive conditions.

Motivated by a work due to Popa [22], we have observed that proving fixed point theorems using an implicit relation is a good idea since it covers several contractive conditions rather than one contractive condition.

It is our purpose in this paper to prove common fixed point theorems in fuzzy metric spaces via an implicit relation for weakly compatible mappings satisfying the property (E.A) introduced by [1] and a common property (E.A) introduced by Liu et al [20]. Our Theorems generalize Theorems of [1, 3, 4, 6, 15, 16] and a corollary of [2].

Definition 1.1 ([24])**.** A binary operation $* : [0,1]^2 \longrightarrow [0,1]$ is called a continuous t-norm if $([0,1], *)$ is an abelian topological monoid; i.e.,

(1) $*$ is associative and commutative,
(2) $*$ is continuous,
(3) $a * 1 = a$ for all $a \in [0,1]$,
(4) $a * b \leq c * d$ whenever $a \leq c$ and $b \leq d$, for each $a, b, c, d \in [0,1]$.

2000 *Mathematics Subject Classification.* 54H25; 47H10.
Key words and phrases. Fuzzy metric space, weakly compatible mappings, common fixed point, property (E.A), common property (E.A)..

Two typical examples of a continuous $t-$norm are $a*b = ab$ and $a*b = \min\{a, b\}$.

Definition 1.2 ([12])**.** The 3-tuple $(X, M, *)$ is called a fuzzy metric space if X is an arbitrary non-empty set, $*$ is a continuous t-norm, and M is a fuzzy set on $X^2 \times (0, \infty)$, satisfying the following conditions for each $x, y, z \in X$ and $t, s > 0$,

(FM-1) $M(x, y, t) > 0$,
(FM-2) $M(x, y, t) = 1$ if and only if $x = y$,
(FM-3) $M(x, y, t) = M(y, x, t)$,
(FM-4) $M(x, y, t) * M(y, z, s) \leq M(x, z, t + s)$,
(FM-5) $M(x, y, .) : (0, \infty) \longrightarrow [0, 1]$ is continuous.

Let $(X, M, *)$ be a fuzzy metric space. For $t > 0$, the open ball $B(x, r, t)$ with center $x \in X$ and radius $0 < r < 1$ is defined by

$$B(x, r, t) = \{y \in X : M(x, y, t) > 1 - r\}.$$

A subset $A \subset X$ is called open if for each $x \in A$, there exist $t > 0$ and $0 < r < 1$ such that $B(x, r, t) \subset A$. Let τ denote the family of all open subsets of X. Then τ is called the topology on X induced by the fuzzy metric M. This topology is Hausdorff and first countable.

Example 1.3. Let $X = \mathbb{R}$. Denote $a * b = a.b$ for all $a, b \in [0, 1]$. For each $t \in (0, \infty)$, define

$$M(x, y, t) = \frac{t}{t + |x - y|}$$

for all $x, y \in X$.

Definition 1.4 ([12])**.** Let $(X, M, *)$ be a fuzzy metric space.

1) A sequence $\{x_n\}$ in X converges to x if and only if for any $0 < \epsilon < 1$ and $t > 0$, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, $M(x_n, x, t) > 1 - \epsilon$; i.e., $M(x_n, x, t) \to 1$ as $n \to \infty$ for all $t > 0$.

2) A sequence $\{x_n\}$ in X is called a Cauchy sequence if and only if for any $0 < \epsilon < 1$ and $t > 0$, there exists $n_0 \in \mathbb{N}$ such that for all $n, m \geq n_0$, $M(x_n, x_m, t) > 1-\epsilon$; i.e., $M(x_n, x_m, t) \to 1$ as $n, m \to \infty$ for all $t > 0$.

3) A fuzzy metric space (X, M, t) in which every Cauchy sequence is convergent is said to be complete.

Lemma 1.5 ([13])**.** *For all $x, y \in X$, $M(x, y, .)$ is a non-decreasing function.*

Definition 1.6. Let $(X, M, *)$ be a fuzzy metric space. M is said to be continuous on $X^2 \times (0, \infty)$ if

$$\lim_{n\to\infty} M(x_n, y_n, t_n) = M(x, y, t)$$

whenever $\{(x_n, y_n, t_n)\}$ is a sequence in $X^2 \times (0, \infty)$ which converges to a point $(x, y, t) \in X^2 \times (0, \infty)$; i.e.,

$$\lim_{n\to\infty} M(x_n, x, t) = \lim_{n\to\infty} M(y_n, y, t) = 1 \text{ and } \lim_{n\to\infty} M(x, y, t_n) = M(x, y, t).$$

Lemma 1.7 ([13])**.** *M is continuous function on $X^2 \times (0, \infty)$.*

Let A and S be mappings from a fuzzy metric space $(X, M, *)$ into itself.

Definition 1.8. A and S are said to be

1) compatible [17, 25] if

$$\lim_{n\to\infty} M(ASx_n, SAx_n, t) = 1 \text{ for all } t > 0$$

whenever $\{x_n\}$ is a sequence in X such that

$$\lim_{n\to\infty} Ax_n = \lim_{n\to\infty} Sx_n = x \in X.$$

2) A and S are said to be weakly compatible [18] if they commute at their coincidence points; i.e., $Ax = Sx$ for some $x \in X$ implies that $ASx = SAx$.

Remark 1.9. If A and S of are compatible, then they are weakly compatible and the converse is not true in general, see [26]

Definition 1.10. The pair (A, S) satisfies the property (E.A) if there exists a sequence $\{x_n\}$ in X such that

$$\lim_{n\to\infty} M(Ax_n, u, t) = \lim_{n\to\infty} M(Sx_n, u, t) = 1$$

for some $u \in X$ and all $t > 0$.

Clearly, a pair of noncompatible mappings satisfies the property (E.A).

Example 1.11. Let $X = \mathbb{R}$ and $M(x, y, t) = \dfrac{t}{t + |x - y|}$ for every $x, y \in X$ and $t > 0$. Define A and S by

$$Ax = 2x + 1, \quad Sx = x + 2.$$

Define the sequence $\{x_n\}$ by $x_n = 1 + \dfrac{1}{n},\ n = 1, 2, \ldots$. We have

$$\lim_{n\to\infty} M(Ax_n, 3, t) = \lim_{n\to\infty} M(Sx_n, 3, t) = 1$$

for every $t > 0$. Then, the pair (A, S) satisfies the property (E.A). However, A and S are not weakly compatible.

The following example shows that there are some pairs of mappings which do not satisfy the property (E.A).

Example 1.12. Let $X = \mathbb{R}$ and $M(x, y, t) = \dfrac{t}{t + |x - y|}$ for every $x, y \in X$ and $t > 0$. Define A and S by $Ax = x + 1$ and $Sx = x + 2$. Assume that there exists a sequence $\{x_n\}$ in X such that

$$\lim_{n\to\infty} M(Ax_n, u, t) = \lim_{n\to\infty} M(Sx_n, u, t) = 1$$

for some $u \in X$ and all $t > 0$. Therefore

$$\lim_{n\to\infty} M(x_n + 1, u, t) = \lim_{n\to\infty} M(x_n + 2, u, t) = 1.$$

We conclude that $x_n \to u - 1$ and $x_n \to u - 2$ which is a contradiction. Hence, the pair (A, S) do not satisfy the property (E.A).

Definition 1.13. The pairs (A, S) and (B, T) of a fuzzy metric space $(X, M, *)$ satisfy a common property (E.A) if there exists two sequences $\{x_n\}$ and $\{y_n\}$ such that for some $u \in X$ and for all $t > 0$

(1.1)

$$\lim_{n\to\infty} M(Ax_n, u, t) = \lim_{n\to\infty} M(Sx_n, u, t) = \lim_{n\to\infty} M(By_n, u, t) = \lim_{n\to\infty} M(Ty_n, u, t) = 1.$$

If $B = A$ and $T = S$ in (1.1), we obtain the definition of the property (E.A).

Example 1.14. Let $X = [1, \infty)$ and $M(x, y, t) = \dfrac{t}{t + |x - y|}$ for every $x, y \in X$ and $t > 0$. Define A, B, S, T by

$$Ax = 2 + \frac{x}{3}, Bx = 2 + \frac{x}{2}, Sx = 1 + \frac{2}{3}x, Tx = 1 + x.$$

Define sequences $\{x_n\}$ and $\{y_n\}$ by $x_n = 3 + \dfrac{1}{n}$, $y_n = 2 + \dfrac{1}{n}$, $n = 1, 2, ...$ Since for all $t > 0$

$$\lim_{n\to\infty} M(Ax_n, 3, t) = \lim_{n\to\infty} M(By_n, 3, t) = \lim_{n\to\infty} M(Sx_n, 3, t) = \lim_{n\to\infty} M(Ty_n, 3, t) = 1$$

Therefore, the pairs (A, S) and (B, T) satisfy a common property (E.A)

Let Φ be the set of all continuous functions $\phi : [0, \infty[\longrightarrow [0, \infty[$ such that $\phi(t) < t$ for all $t > 0$.

2. Implicit relations

Let F_6 be the set of all continuous functions $F(t_1, t_2, t_3, t_4, t_5, t_6) : [0, 1]^6 \to \mathbb{R}$ satisfying the following conditions:

$(F_1) : F(u, 1, u, 1, 1, u) < 0$ for all $u \in (0, 1)$.
$(F_2) : F(u, 1, 1, u, u, 1) < 0$ for all $u \in (0, 1)$.
$(F_3) : F(u, u, 1, 1, u, u) < 0$ for all $u \in (0, 1)$.

The aim of this section is to give several examples of the function F.

Example 2.1. $F(t_1, t_2, t_3, t_4, t_5, t_6) = t_1 - \phi(\min\{t_2, t_3, t_4, t_5, t_6\})$, where $\phi : [0, 1] \longrightarrow [0, 1]$ is increasing and continuous function such that $\phi(t) > t$ for all $t \in (0, 1)$.

$(F_1) : F(u, 1, u, 1, 1, u) = u - \phi(u) < 0$ for all $u \in (0, 1)$.
(F_2) : Similarly, $F(u, 1, 1, u, u, 1) < 0$ for all $u \in (0, 1)$.
$(F_3) : F(u, u, 1, 1, u, u) = u - \phi(u) < 0$ for all $u \in (0, 1)$.

Example 2.2. $F(t_1, t_2, t_3, t_4, t_5, t_6) = t_1^2 - c_1 \min\{t_2^2, t_3^2, t_4^2\} - c_2 \min\{t_3 t_6, t_4 t_5\} - c_3 t_5 t_6$

$c_1, c_2, c_3 > 0$, $c_1 + c_2 \geq 1, c_1 + c_3 \geq 1$.
$(F_1) : F(u, 1, u, 1, 1, u) = u^2(1 - c_1 - c_2) - c_3 u < 0$ for all $u \in (0, 1)$.
(F_2) : Similarly, $F(u, 1, 1, u, u, 1) < 0$ for all $u \in (0, 1)$.
$(F_3) : F(u, u, 1, 1, u, u) = u^2(1 - c_1 - c_3) - c_2 u < 0$ for all $u \in (0, 1)$.

Example 2.3. $F(t_1, t_2, t_3, t_4, t_5, t_6) = t_1^3 - a \min\{t_1^2 t_2, t_1 t_3 t_4, t_5^2 t_6, t_5 t_6^2\}$, $a > 1$.
$(F_1) : F(u, 1, u, 1, 1, u) = u^3 - a \min\{u^2, u\} < 0$ for all $u \in (0, 1)$.
(F_2) : Similarly, $F(u, 1, 1, u, u, 1) < 0$ for all $u \in (0, 1)$.
$(F_3) : F(u, u, 1, 1, u, u) = u^3 - a \min\{u^3, u, u^3\} < 0$ for all $u \in (0, 1)$.

Example 2.4. $F(t_1, t_2, t_3, t_4, t_5, t_6) = t_1^3 - a\dfrac{t_3^2 t_4^2 + t_5^2 t_6^2}{t_2 + t_3 + t_4}$, $a \geq 2$.

$(F_1) : F(u, 1, u, 1, 1, u) = u^3 - \dfrac{2au^2}{u + 2} < 0$ for all $u \in (0, 1)$.
(F_2) : Similarly, $F(u, 1, 1, u, u, 1) < 0$ for all $u \in (0, 1)$.
$(F_3) : F(u, u, 1, 1, u, u) = u^3 - a\dfrac{u^4 + 1}{u + 2} < 0$ for all $u \in (0, 1)$.

Example 2.5. $F(t_1, t_2, t_3, t_4, t_5, t_6) = (1 + pt_2)t_1 - p \min\{t_3 t_4, t_5 t_6\} - \phi(\min\{t_2, t_3, t_4, t_5, t_6\})$,
where $p \geq 0$ and $\phi : [0, 1] \longrightarrow [0, 1]$ is increasing and continuous function such that $\phi(t) > t$ for all $t \in (0, 1)$.

$(F_1), (F_2)$ and (F_3) as in Example 2.1.

Example 2.6. $F(t_1,t_2,t_3,t_4,t_5,t_6)=t_1^2-a\dfrac{t_2^2+t_3^2+t_4^2}{t_5+t_6}$, $a\geq 1$.

(F_1) : $F(u,1,u,1,1,u)=u^2-a\dfrac{u^2+2}{u+1}=\dfrac{u^3+(1-a)u^2-2a}{u+1}<0$ for all $u\in(0,1)$.

(F_2) Similarly, $F(u,1,1,u,u,1)<0$ for all $u\in(0,1)$.

(F_3) : $F(u,u,1,1,u,u)=u^2-a\dfrac{u^2+2}{2u}<0$ for all $u\in(0,1)$.

Example 2.7. $F(t_1,t_2,t_3,t_4,t_5,t_6)=t_1^3-a\dfrac{t_3^2t_4^2}{t_2+t_5+t_6}$, $a>3$.

(F_1) : $F(u,1,u,1,1,u)=u^3-a\dfrac{u^2}{u+2}<0$ for all $u\in(0,1)$.

(F_2) Similarly, $F(u,1,1,u,u,1)<0$ for all $u\in(0,1)$.

(F_3) : $F(u,u,1,1,u,u)=u^3-\dfrac{a}{3u}<0$ for all $u\in(0,1)$.

Example 2.8. $F(t_1,t_2,t_3,t_4,t_5,t_6)=t_1^2-a\min\{t_2^2,t_3^2,t_4^2\}-b\dfrac{t_5}{t_5+t_6}$, $a\geq 1$ and $b>0$.

(F_1) : $F(u,1,u,1,1,u)=(1-a)u^2-b\dfrac{u}{u+1}<0$ for all $u\in(0,1)$.

(F_2) Similarly, $F(u,1,1,u,u,1)<0$ for all $u\in(0,1)$.

(F_3) : $F(u,u,1,1,u,u)=(1-a)u^2-\dfrac{b}{2}<0$ for all $u\in(0,1)$.

Example 2.9. $F(t_1,t_2,t_3,t_4,t_5,t_6)=t_1^2-a\min\{t_2^2,t_5^2,t_6^2\}-b\dfrac{t_3}{t_3+t_4}$, $a>1$ and $b>0$.

(F_1), (F_2) and (F_3) as in Example 2.8.

Example 2.10. $F(t_1,t_2,t_3,t_4,t_5,t_6)=t_1-a_1t_2-a_2t_3-a_3t_4-a_4t_5-a_5t_6$, $a_1,a_2,a_3,a_4,a_5>0$, $a_2+a_5\geq 1$, $a_3+a_4\geq 1$ and $a_1+a_4+a_5\geq 1$.

(F_1) : $F(u,1,u,1,1,u)=u-a_1-a_2u-a_3-a_4-a_5u<0$ for all $u\in(0,1)$.

(F_2) Similarly, $F(u,1,1,u,u,1)<0$ for all $u\in(0,1)$.

(F_3) : $F(u,u,1,1,u,u)=u-a_1u-a_2-a_3-a_4u-a_5u<0$ for all $u\in(0,1)$.

Example 2.11. $F(t_1,t_2,t_3,t_4,t_5,t_6)=\int_0^{t_1}\varphi(t)dt-\phi(\int_0^{\min\{t_2,t_3,t_4,t_5,t_6\}}\varphi(t)dt)$, where $\phi:[0,1]\longrightarrow[0,1]$ is increasing and continuous function such that $\phi(t)>t$ for all $t\in(0,1)$ and $\varphi:\mathbb{R}_+\to\mathbb{R}_+$ is a Lebesgue-integrable mapping which is summable and satisfies

$$0<\int_0^{\epsilon}\varphi(s)ds<1 \text{ for all } 0<\epsilon<1 \text{ and } \int_0^{1}\varphi(s)ds=1. \tag{2.1}$$

(F_1) : $F(u,1,u,1,1,u)=\int_0^{u}\varphi(t)dt-\phi(\int_0^{u}\varphi(t)dt)<0$ for all $u\in(0,1)$.

(F_2) : Similarly, $F(u,1,1,u,u,1)<0$ for all $u\in(0,1)$.

(F_3) : $F(u,u,1,1,u,u)=\int_0^{u}\varphi(t)dt-\phi(\int_0^{u}\varphi(t)dt)<0$ for all $u\in(0,1)$.

Example 2.12. $F(t_1,t_2,t_3,t_4,t_5,t_6)=(\int_0^{t_1}\varphi(s)ds)^p-a(\int_0^{t_2}\varphi(s)ds)^p-$

$$b\min\{\int_0^{t_3}\varphi(s)ds, \int_0^{t_4}\varphi(s)ds, (\int_0^{t_3}\varphi(s)ds)^{\frac{1}{2}}\cdot(\int_0^{t_5}\varphi(s)ds)^{\frac{1}{2}}, (\int_0^{t_5}\varphi(s)ds)^{\frac{1}{2}}(\int_0^{t_6}\varphi(s)ds)^{\frac{1}{2}}\}^p,$$

where $a > 0$, $0 < b \leq 1$, $a + b > 1$, $p > 0$, $\phi : [0,1] \longrightarrow [0,1]$ is increasing and continuous function such that $\phi(t) > t$ for all $t \in (0,1)$ and $\varphi : \mathbb{R}_+ \to \mathbb{R}_+$ is a Lebesgue-integrable mapping which is summable and satisfies 2.1.

$(F_1) : F(u,1,u,1,1,u) = (\int_0^u \varphi(s)ds)^p - a(\int_0^1 \varphi(s)ds)^p$
$- b\min\{\int_0^u \varphi(s)ds, \int_0^1 \varphi(s)ds, (\int_0^u \varphi(s)ds)^{\frac{1}{2}}\cdot(\int_0^1 \varphi(s)ds)^{\frac{1}{2}}, (\int_0^1 \varphi(s)ds)^{\frac{1}{2}}(\int_0^u \varphi(s)ds)^{\frac{1}{2}}\}^p$
$= (\int_0^u \varphi(s)ds)^p - a - b(\int_0^u \varphi(s)ds)^p < 0$ for all $u \in (0,1)$.

(F_2) : Similarly, $F(u,1,1,u,u,1) < 0$ for all $u \in (0,1)$.

$(F_3) : F(u,u,1,1,u,u) = (1-a-b)\phi(\int_0^u \varphi(t)dt) < 0$ for all $u \in (0,1)$.

Define $G : R_A^+ \to \mathbb{R}$ satisfying:

Example 2.13. (i) $G(0) = 0$ and $G(t) > 0$ for each $t \in (0,A)$, $A \in (0,\infty]$, $R_A^+ = [0,A)$,
(ii) G is increasing on R_A^+,
(iii) G is continuous.

Example 2.14. $F(t_1,t_2,t_3,t_4,t_5,t_6) = G(t_1) - \phi(G(\min\{t_2,t_3,t_4,t_5,t_6\})$, where $\phi : [0,1] \longrightarrow [0,1]$ is increasing and continuous function such that $\phi(t) > t$ for all $t \in (0,1)$
$(F_1) : F(u,1,u,1,1,u) = G(u) - \phi(G(u)) < 0$ for all $u \in (0,1)$.
(F_2) : Similarly, $F(u,1,1,u,u,1) < 0$ for all $u \in (0,1)$.
$(F_3) : F(u,u,1,1,u,u) = G(u) - \phi(G(u)) < 0$ for all $u \in (0,1)$.

Example 2.15. $F(t_1,t_2,t_3,t_4,t_5,t_6) = (G(t_1))^p - \phi[a(G(t_2))^p +$
$b\min\{G(t_3), G(t_4), (G(t_3))^{\frac{1}{2}}\cdot(G(t_5))^{\frac{1}{2}}, (G(t_5))^{\frac{1}{2}}\cdot(G(t_6))^{\frac{1}{2}}\}^p]$,
where $a > 0$, $0 < b \leq 1$, $a + b > 1$, $p > 0$ and $\phi : [0,1] \longrightarrow [0,1]$ is increasing and continuous function such that $\phi(t) > t$ for all $t \in (0,1)$.

Define $\Phi[0,A) = \{G : G$ satisfies (i)–(iii)$\}$.
The following examples were given by [30].
1) Let $G(t) = t$, then $G \in \Phi[0,A)$ for each $A \in (0,+\infty]$.
2) Suppose that φ is nonnegative, Lebesgue integrable on $[0,A)$ and satisfies

$$\int_0^{\epsilon}\varphi(t)dt > 0 \text{ for each } \epsilon \in (0,A).$$

Let $G(t) = \int_0^t \varphi(s)ds$, then $G \in \Phi[0,A)$.

3) Suppose that ψ is nonnegative, Lebesgue integrable on $[0, A)$ and satisfies

$$\int_0^{\epsilon} \psi(t)dt > 0 \text{ for each } \epsilon \in (0, A)$$

and φ is nonnegative, Lebesgue integrable on $[0, \int_0^A \psi(s)ds)$ and satisfies

$$\int_0^{\epsilon} \varphi(t)dt > 0 \text{ for each } \epsilon \in (0, \int_0^A \psi(s)ds).$$

Let $G(t) = \int_0^{\int_0^t \psi(s)ds} \varphi(u)du$, then $G \in \Phi[0, A)$.

4) If $H \in \Phi[0, A)$ and $G \in \Phi[0, H(A-0))$, then a composition mapping $G \circ H \in \Phi[0, A)$. For instance, let $L(t) = \int_0^{G(t)} \varphi(s)ds$, then $L \in \Phi[0, A)$ whenever $G \in \Phi[0, A)$ and φ is nonnegative, Lebesgue integrable on $\Phi[0, G(A-0))$ and satisfies

$$\int_0^{\epsilon} \varphi(t)dt > 0 \text{ for each } \epsilon \in (0, G(A-0)).$$

Lemma 2.16 ([30]). *Let $A \in (0, +\infty]$ and $G \in \Phi[0, A)$. If $\lim_{n\to\infty} G(\epsilon_n) = 0$ for $\epsilon_n \in R_A^+$, then $\lim_{n\to\infty} \epsilon_n = 0$.*

3. Main Results

The purpose of this section is to give our main results Theorem 3.1 and Theorem 3.3..

Theorem 3.1. *Let A, B, S and T be self-mappings of a fuzzy metric space $(X, M, *)$ satisfying the following conditions*

$$A(X) \subset T(X) \text{ and } B(X) \subset S(X), \tag{3.1}$$

$$\begin{aligned} & F(M(Ax, By, t), M(Sx, Ty, t), M(Ax, Sx, t), \\ & M(By, Ty, t), M(Sx, By, t), M(Ax, Ty, t)) \\ \geq\ & 0 \end{aligned} \tag{3.2}$$

for all x, y in X and $F \in F_6$. Suppose that the pair (A, S) or (B, T) satisfies the property (E.A) and (A, S) and (B, T) are weakly compatible. If the range of one A, B, S and T is a closed subset of X, then A, B, S and T have a unique common fixed point in X.

Proof. Suppose that the pair (B, T) satisfies the property (E.A). Then, there exists a sequence $\{x_n\}$ in X such that $\lim_{n\to\infty} Bx_n = \lim_{n\to\infty} Tx_n = z$ for some $z \in X$. Therefore, we have $\lim_{n\to\infty} M(Bx_n, Tx_n, t) = 1$. Since $B(X) \subset S(X)$, there exists a sequence $\{y_n\}$ in X such that $Bx_n = Sy_n$.

Hence, $\lim_{n\to\infty} Sy_n = z$. Let us show that $\lim_{n\to\infty} Ay_n = z$. Using (3.2) we have

$$\begin{aligned} & F(M(Ay_n, Bx_n, t), M(Sy_n, Tx_n, t), M(Ay_n, Sy_n, t), \\ & M(Bx_n, Tx_n, t), M(Sy_n, Bx_n, t), M(Ay_n, Tx_n, t)) \\ = \; & F(M(Ay_n, Bx_n, t), M(Bx_n, Tx_n, t), M(Ay_n, Bx_n, t), \\ & M(Bx_n, Tx_n, t), 1, M(Ay_n, Tx_n, t)) \\ \geq \; & 0. \end{aligned}$$

Assume that $\limsup_{n\to\infty} M(Ay_n, Bx_n, t) = l < 1$. Taking the limit as $n \to \infty$ we get

$$F(l, 1, l, 1, 1, l) \geq 0$$

which is a contradiction of (F_1) and so $l = 1$; i.e., $\lim_{n\to\infty} Ay_n = z$.

Suppose that $S(X)$ is a closed subspace of X. Then, $z = Su$ for some $u \in X$.

If $z \neq Au$, applying (3.2) we obtain

$$\begin{aligned} & F(M(Au, Bx_n, t), M(Su, Tx_n, t), M(Au, Su, t), \\ & F(M(Au, Bx_n, t), M(Su, Tx_n, t), M(Au, Su, t)) \\ \geq \; & 0 \end{aligned}$$

Letting $n \to \infty$ we have

$$F(M(Au, z, t), 1, M(Au, z, t), 1, 1, M(Au, z, t)) \geq 0$$

which is a contradiction of (F_1). Hence, $z = Au = Su$.

Since $A(X) \subset T(X)$, there exists $v \in X$ such that $z = Au = Tv$.

If $z \neq Bv$, using (3.2) we have

$$\begin{aligned} & F(M(Au, Bv, t), M(Su, Tv, t), M(Au, Su, t), \\ & M(Bv, Tv, t), M(Su, Bv, t), M(Au, Tv, t)) \\ = \; & F(M(z, Bv, t), 1, 1, M(z, Bv, t), M(z, Bv, t), 1) \geq 0 \end{aligned}$$

which is a contradiction of (F_2) and therefore $Au = Su = z = Bv = Tv$.

Since the pairs (A, S) and (B, T) are weakly compatible, we have $ASu = SAu$ and $BTv = TBv$; i.e., $Az = Sz$ and $Bz = Tz$. If $Az \neq z$, using (3.2) we get

$$\begin{aligned} & F(M(Az, Bv, t), M(Sz, Tv, t), M(Az, Sz, t), \\ & M(Bv, Tv, t), M(Sz, Bv, t), M(Az, Tv, t)) \\ = \; & F(M(Az, z, t), M(Az, z, t), 1, 1, \\ & M(Az, z, t), M(Az, z, t)) \\ \geq \; & 0 \end{aligned}$$

which is a contradiction of (F_3). Then, $Az = Sz = z$.

Similarly, we can prove that $Bz = Tz = z$. Hence, $z = Bz = Tz = Az = Sz$ and z is a common fixed point of A, B, S and T. The uniqueness of z follows from (3.2) and (F_3). □

If $B = A$ and $T = S$ in Theorem 3.1, we get the following Corollary.

Corollary 3.2. *Let A and S be self-mappings of a fuzzy metric space $(X, M, *)$ satisfying*

$$A(X) \subset S(X),$$

$$\begin{aligned} & F(M(Ax,Ay,t),M(Sx,Sy,t),M(Ax,Sx,t),\\ & M(Ay,Sy,t),M(Sx,Ay,t),M(Ax,Sy,t))\\ \geq\ & 0. \end{aligned}$$

Suppose that the pair (A,S) satisfies the property (E.A) and (A,S) is weakly compatible. If the range of one A and S is a closed subset of X, then A and S have a unique common fixed point in X.

Theorem 3.3. *Let A,B,S and T be self-mappings of a fuzzy metric space $(X,M,*)$ satisfying* (3.2)*. Suppose that the pairs (A,S) and (B,T) satisfy a common property (E.A) and (A,S) and (B,T) are weakly compatible. If $S(X)$ and $T(X)$ are closed subsets of X, then A,B,S and T have a unique common fixed point in X.*

Proof. Suppose that the pairs (A,S) and (B,T) satisfy a common property (E.A). Then, there exist two sequences $\{x_n\}$ and $\{y_n\}$ such that

$$\lim_{n\to\infty} Ax_n = \lim_{n\to\infty} Sx_n = \lim_{n\to\infty} By_n = \lim_{n\to\infty} Ty_n = z \in X.$$

Since $S(X)$ and $T(X)$ are closed subsets of X, we obtain $z = Su = Tv$ for some $u, v \in X$.

If $z \neq Au$, using (3.2) we obtain

$$\begin{aligned} & F(M(Au,By_n,t),M(Su,Ty_n,t),M(Au,Su,t),\\ & M(By_n,Ty_n,t),M(Su,By_n,t),M(Au,Ty_n,t))\\ \geq\ & 0. \end{aligned}$$

Letting $n \to \infty$ we have

$$F(M(Au,z,t),1,M(Au,z,t),1,1,M(Au,z,t)) \geq 0$$

which is a contradiction of (F_1) and so $z = Au = Su = Tv$. The rest of the proof follows as in Theorem 3.1. □

If we take examples 2.1, 2.11 and 2.14, we get Corollaries which generalize Theorems of [1, 4, 6, 7] and a corollary of [2]

If we take examples 2.2-2.10, we get several Corollaries.

Theorems 3.1 and 3.3 extend theorems of [3, 15, 16].

Example 3.4. Let $(X,M,*)$ be a fuzzy metric space, where $X = [0,2)$ with a t-norm defined by $a * b = \min\{a,b\}$ for all $a,b \in [0,2)$ and $M(x,y,t) = \dfrac{t}{t+|x-y|}$ for all $x,y \in X$ and $t > 0$. Define A,B,S and T by:

$$\begin{aligned} Ax &= Bx = 1,\\ Sx &= \begin{cases} 1 & \text{if } x \text{ is rational,}\\ \frac{2}{3} & \text{if } x \text{ is irrational} \end{cases}, Tx = \begin{cases} 1 & \text{if } x \text{ is rational,}\\ \frac{1}{3} & \text{if } x \text{ is irrational} \end{cases}, \end{aligned}$$

$F(t_1,t_2,t_3,t_4,t_5,t_6) = t_1 - \phi(\min\{t_2,t_3,t_4,t_5,t_6\})$, $\phi(s) = \sqrt{s}$ for all $s \in [0,1]$.

It is easy to see that for all $x,y \in X$ and $t > 0$

$$\begin{aligned} M(Ax,By,t) \geq\ & \phi(\min\{M(Sx,Ty,t),M(Ax,Sx,t),\\ & M(By,Ty,t),M(Sx,By,t),M(Ax,Ty,t)\}) \end{aligned}$$

and the other conditions of Theorem 3.1 are satisfied, consequently, 1 is the unique common fixed point of A,B,S and T.

Example 3.5. Let $(X, M, *)$ and F as in example 3.4. Define A, B, S and T by:

$$Ax = \begin{cases} 1 & \text{if } x \text{ is rational,} \\ \frac{3}{4} & \text{if } x \text{ is irrational} \end{cases}, Bx = \begin{cases} 1 & \text{if } x \text{ is rational,} \\ \frac{1}{2} & \text{if } x \text{ is irrational} \end{cases},$$

$$Sx = \begin{cases} 1 & \text{if } x \text{ is rational,} \\ \frac{2}{3} & \text{if } x \text{ is irrational} \end{cases}, Tx = \begin{cases} 1 & \text{if } x \text{ is rational,} \\ \frac{1}{3} & \text{if } x \text{ is irrational} \end{cases},$$

It is easy to see that for all $x, y \in X$ and $t > 0$

$$\begin{aligned} M(Ax, By, t) \geq\ & \phi(\min\{M(Sx, Ty, t), M(Ax, Sx, t), \\ & M(By, Ty, t), M(Sx, By, t), M(Ax, Ty, t)\}) \end{aligned}$$

and the other conditions of Theorem 3.3 are satisfied, consequently, 1 is the unique common fixed point of A, B, S and T.

Note that Theorem 3.1 is not applicable in example 3.5 since (3.1) is not verified.

Example 3.6. Let $(X, M, *)$, A, B, S and T as in example 3.4,

$F(t_1, t_2, t_3, t_4, t_5, t_6) = G(t_1) - \phi(G(\min\{t_2, t_3, t_4, t_5, t_6\}))$, $\phi(s) = \sqrt{s}$ for all $s \in [0, 1]$ and $G(s) = s^{\frac{1}{s}}$ for $s > 0$, $G(0) = 0$.

It is easy to see that $D = diam(X) = 2$, $G \in \digamma[0, A)$, where $A = e > D = 2$ and for all $x, y \in X$ and $t > 0$

$$G(M(Ax, By, t)) \geq \phi(G(L(x, y, t))),$$

where

$$\begin{aligned} L(x, y, t) =\ & \min\{M(Sx, Ty, t), M(Ax, Sx, t), \\ & M(By, Ty, t), M(Sx, By, t), M(Ax, Ty, t)\}. \end{aligned}$$

and the other conditions of Theorem 3.1 are satisfied, consequently, 1 is the unique common fixed point of A, B, S and T.

Example 3.7. Let $(X, M, *)$, A, B, S and T as in example 3.5 and F as in example 3.6.

It is easy to see that for all $x, y \in X$ and $t > 0$

$$G(M(Ax, By, t)) \geq \phi(G(L(x, y, t))),$$

where

$$\begin{aligned} L(x, y, t) =\ & \min\{M(Sx, Ty, t), M(Ax, Sx, t), \\ & M(By, Ty, t), M(Sx, By, t), M(Ax, Ty, t)\}. \end{aligned}$$

and the other conditions of Theorem 3.3 are satisfied, consequently, 1 is the unique common fixed point of A, B, S and T.

Note that Theorem 3.1 is not applicable in example 3.7 since (3.1) is not verified.

References

[1] M. Aamri and D. El Moutawakil, Some new common fixed point theorems under strict contractive conditions, J. Math. Anal. Appl., 270 (2002), 181-188.

[2] A. Aliouche, A common fixed point theorem for weakly compatible mappings in symmetric spaces satisfying a contractive condition of integral type, J. Math. Anal. Appl., 322 (2) (2006), 796-802.

[3] A. Aliouche, Common fixed point theorems via an implicit relation and new properties, Soochow J. Math, 33 (4) (2007), 593-601.

[4] A. Aliouche, Common fixed point theorems of Gregus type for weakly compatible mappings satisfying generalized contractive conditions, J. Math Anal. Appl., 341 (2008), 707–719.

[5] A. Branciari, A fixed point theorem for mappings satisfying a general contractive condition of integral type, Int. J. Math. Sci., 29 (9) (2002), 531-536.
[6] A. Djoudi and L. Nisse, Gregus type fixed points for weakly compatible mappings, Bull. Belg. Math. Soc., 10 (2003), 369-378.
[7] A. Djoudi and A. Aliouche, Common fixed point theorems of Gregus type for weakly compatible mappings satisfying contractive conditions of integral type, J. Math Anal. Appl., 329 (1) (2007), 31-45.
[8] M. S. El Naschie, On the uncertainty of Cantorian geometry and two-slit experiment. Chaos, Solitons and Fractals., 9 (1998), 517–29.
[9] M. S. El Naschie, A review of E-infinity theory and the mass spectrum of high energy particle physics. Chaos, Solitons and Fractals., 19 (2004), 209–36.
[10] M. S. El Naschie, On a fuzzy Kahler-like Manifold which is consistent with two-slit experiment. Int. J of Nonlinear Science and Numerical Simulation., 6 (2005), 95–98.
[11] M. S. El Naschie, The idealized quantum two-slit gedanken experiment revisited—-Criticism and reinterpretation. Chaos, Solitons and Fractals., 27 (2006), 9–13.
[12] A. George and P. Veeramani, On some result in fuzzy metric space. Fuzzy Sets and Systems., 64 (1994), 395–399.
[13] M. Grabiec, Fixed points in fuzzy metric spaces, Fuzzy Sets and System., 27 (1988), 385-389.
[14] V. Gregori and A. Sapena, On fixed-point theorem in fuzzy metric spaces. Fuzzy Sets and Systems., 125 (2002), 245–252.
[15] M. Imdad and J. Ali, A general fixed point theorem in fuzzy metric spaces via an implicit function, J. Appl. Math. & Informatics, 26 (3 - 4) (2008), 591-603.
[16] J. Ali and M. Imdad, An implicit function implies several contraction conditions, Sarajevo J. Math., 4 (2) (2008), 269-285.
[17] G. Jungck, Compatible mappings and common fixed points, Internat. J. Math. & Math. Sci., 9 (4) (1986), 771-779.
[18] G. Jungck, Common fixed points for non-continuous non-self maps on non metric spaces, Far East J. Math. Sci., 4 (2) (1996), 199-215.
[19] I. Kramosil and J. Michalek, Fuzzy metric and statistical metric spaces. Kybernetica., 11 (1975), 326–334.
[20] Y. Liu, J. Wu and Z. Li, Common fixed points of single-valued and multi-valued maps, Internat J. Math. Math. Sci., 19 (2005), 3045-3055.
[21] D. Mihet, Banach contraction theorem in fuzzy metric spaces, Fuzzy Sets Systems., 144 (2004), 431–439.
[22] V. Popa, Some fixed point theorems for compatible mappings satisfying an implicit relation, Demonstratio Math., 32 (1999),157-163.
[23] B. E. Rhoades, Two fixed-Point Theorems for mappings satisfying a general contractive condition of integral type. Inter. J. Math and Math. Sci., 63 (2003), 4007-4013.
[24] B. Schweizer and A. Sklar, Statistical metric spaces. Pacific J. Math., 10 (1960), 313-334.
[25] B. Singh and M. S. Chauhan, Common fixed point of compatible maps in fuzzy metric space, Fuzzy Sets and System 115 (2000), 471-475.
[26] B. Singh and S. Jain, Semi-compatibility, compatibility and fixed point Theorems in fuzzy metric space, J. Chungcheong Math. Soc., 18 (1) (2005), 1-23.
[27] P. Vijayaraju, B. E. Rhoades and R. Mohanraj, A fixed point theorem for a pair of maps satisfying a general contractive condition of integral type, Internat J. Math. Math. Sci., 15 (2005), 2359-2364.
[28] Tanaka. Y, Mizno Y, Kado T. Chaotic dynamics in Friedmann equation. Chaos, Solitons and Fractals., 24 (2005), 407–422.
[29] L. A. Zadeh, Fuzzy sets. Inform and Control., 8 (1965), 338–353.
[30] X. Zhang, Common fixed point theorems for some new generalized contractive type mappings, J. Math. Anal. Appl., 333 (2) (2007), 780-786.

Abdelkrim Aliouche, Department of Mathematics, University of Larbi Ben M'Hidi, Oum-El-Bouaghi, 04000, Algeria.
E-mail address: alioumath@yahoo.fr.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 3, Pages 79–88
ISSN 1930-1235: (2010)

PRINCIPALLY SUPPLEMENTED MODULES

UMMAHAN ACAR AND ABDULLAH HARMANCI

Abstract. In this paper, principally supplemented modules are defined as generalizations of lifting, principally lifting and supplemented modules. Several properties of these modules are proved. New characterizations of principally semiperfect rings are obtained using principally supplemented modules.

1. Introduction

Throughout this paper R denotes a ring with unity. Modules are unital right $R-$modules. Let M be a module and N, K be submodules of M. We call K *a supplement* of N in M if $M = K + N$ and $K \cap N$ is small in K. A module M is called *supplemented* if every submodule of M has a supplement in M. A module M is called *lifting* if, for all $N \leq M$, there exists a decomposition $M = A \oplus B$ such that $A \leq N$ and $N \cap B$ is small in M. Supplemented and lifting modules have been discussed by several authors(see [7], [8], [9], [13]) and these modules are useful in characterizing semiperfect rings(see [1]).

In this paper, principally supplemented modules are discovered as analogous of lifting and supplemented modules, and used to characterize principally semiperfect rings introduced in chapter 3 and discussed in [6].

Let M be a module and N a submodule module M. N is called a *small(or superfluous) submodule* if whenever $M =$N $+ X$, we have $M = X$. A projective module P is called *a projective cover* of a module M if there exists an epimorphism $f : P \longrightarrow M$ with Ker(f) small in P, and a ring is called *semiperfect* if every simple R-module has a projective cover. For more detailed discussion on small submodules, semiperfect rings, we refer to [1].

In this paper, a module M is defined to be *principally supplemented* if for all cyclic submodule N of M, there exists a submodule X of M such that $M = N + X$ with $N \cap X$ is small X, and a module M is called *principally lifting* if, for all cyclic submodule N of M, there exists a decomposition $M = A \oplus B$ such that $A \leq N$ and $N \cap B$ is small in M. Principally lifting modules are considered as generalizations of lifting modules in [9].

In section 2, various properties of principally supplemented modules are obtained and in section 3 we study some applications our results. One of our main results can be stated as follows:
Let M be a projective module. Then M is principally semiperfect if and only if M is principally supplemented. Also we prove for a projective module M with

2000 *Mathematics Subject Classification.* 16L30; 16E50.
Key words and phrases. principally lifting module, principally supplemented module.

Rad(M) small in M, M is principally supplemented if and only if $M/\text{Rad}(M)$ is principally semisimple.

In what follows, by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_n$ and $\mathbb{Z}/\mathbb{Z}n$ we denote, respectively, integers, rational numbers, the ring of integers modulo n and the $\mathbb{Z}$-module of integers modulo n. For unexplained concepts and notations, we refer the reader to [1, 11].

2. Small Submodules and Supplements

Let M be module. A submodule N of M is called a *small(or superfluous) submodule* if, whenever $M = N + X$, we have $M = X$. Small submodule is named *superfluous submodule* in [1]. We begin by stating the next lemma which is contained in context[1, 11].

Lemma 1. *Let M be a module. Then we have the following.*

(1). *If K is small in M and $f : M \to N$ is a homomorphism, then $f(K)$ is small in N. In particular, if K is small in $M \subseteq N$, then K is small in N.*
(2). *Let $K_1 \subseteq M_1 \subseteq M$, $K_2 \subseteq M_2 \subseteq M$ and $M = M_1 \oplus M_2$. Then $K_1 \oplus K_2$ is small in $M_1 \oplus M_2$ if and only if K_1 is small in M_1 and $K_2$is small in M_2.*
(3). *Let N, K be submodules of M with K is small in M and $N \leq K$. Then N is also small in M.*

Lemma 2. *Let N and L be submodules of M. Then the following are equivalent:*
(1). *$M = N + L$ and $N \cap L$ is small in L.*
(2). *$M = N + L$ and for any proper submodule K of L, $M \neq N + K$.*

Proof. (1) $\Rightarrow$ (2) Let N and K be submodules of M with $M = N + K$. Then $L = (L \cap N) + K$. Since $L \cap N$ is small in L, $L = K$.
(2) $\Rightarrow$ (1) If $L = (N \cap L) + K$ where $K \leq L$, then $M = N + L = N + K$. By (2), $K = L$. So $N \cap L$ is small in L. □

Lemma 3. *If $M \xrightarrow{f} M'$ is a homomorphism and N is a supplement in M with $Ker(f) \leq N$, then $f(N)$ is a supplement in $f(M)$.*

Proof. Let $M = N + K$ with $N \cap K$ small in K. Then $f(M) = f(N + K) = f(N) + f(K)$. Since $\text{Ker}(f) \leq N$, we have $f(N) \cap f(K) = f(N \cap K)$. By Lemma 1 and being $f(N \cap K)$ small in $f(M)$, $f(N)$ is a supplement of $f(K)$ in $f(M)$. □

Lemma 4. *Let M be an R-module and K; L; N be submodules of M. Then;*
(1) *If K is a supplement of N in M and T is small in M then K is a supplement of $N + T$ in M.*
(2) *If $M \xrightarrow{f} M'$ is an epimorphism with small kernel and L is a supplement of K in M, then the submodule $f(L)$ of M' is a supplement of $f(K)$ in M'.*

Proof. (1) Let K be a supplement of N in M. Then $M = N + K$ and $N \cap K$ is small in K. Then $M = N + K + T$. Let $K = K \cap (N + T) + L$ for some $L \leq K$. Then $M = N + L + T = N + L$ since T is small in M. Then $K = K \cap N + L$. It implies $K = L$ sine $K \cap N$ is small in K.
(2) Let L be a supplement of K in M. Then L is a supplement of $K + Ker(f)$ by (1). By Lemma 3, f(L) = f(L + Kerf) is also a supplement of $f(K)$ in M'. □

Note that the converse statement of Lemma 4 (2) need not be true in general. For if $\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z}$ denotes the canonical epimorphism, then the zero submodule $(\overline{0})$ of $\mathbb{Z}/2\mathbb{Z}$ is small in $\mathbb{Z}/2\mathbb{Z}$ but $\pi^{-1}(\overline{0}) = 2\mathbb{Z}$ is not small in $\mathbb{Z}$.

A module M is *distributive* if for all submodules K, L, and N, $N \cap (K + L) = N \cap K + N \cap L$ or $N + (K \cap L) = (N + K) \cap (N + L)$. Lemma 5 may be very well known and obvious but we prove it for the sake of easy reference.

Lemma 5. *Let $M = M_1 \oplus M_2 = K + N$ and $K \leq M_1$. If M is distributive and $K \cap N$ is small in N, then $K \cap N$ is small in $M_1 \cap N$.*

Proof. Let $M_1 \cap N = (K \cap N) + L$. Since M is distributive, $N = M_1 \cap N \oplus M_2 \cap N$. We have $M = K + N = K + M_1 \cap N + M_2 \cap N = K + L + (M_2 \cap N)$ and $N = K \cap N + L + (M_2 \cap N)$. Since $K \cap N$ is small in N, $N = L \oplus (M_2 \cap N)$. This and $N = (N \cap M_1) \oplus (N \cap M_2)$ and $L \leq M_1 \cap N$ imply $L = M_1 \cap N$. Hence $K \cap N$ is small in $M_1 \cap N$. □

3. Principally Supplemented Modules

In a semiregular module M, every cyclic submodule mR has a direct summand P such that $M = P \oplus K$, P is projective module and $(mR) \cap K$ is small in K[12, Theorem B.51]. In this note we introduce principally supplemented modules which generalizing semiregular modules, principally lifting modules, also supplemented modules.

Definition 6. Let N be a cyclic submodule of M. A submodule L is called *a principally supplement* of N in M if N and L satisfy the conditions in Lemma 2 and the module M is called *principally supplemented* if every cyclic submodule of M has a principally supplement in M.

Clearly, every supplemented module and every lifting module, therefore every principally lifting module is principally supplemented. There are principally supplemented modules but neither supplemented nor principally lifting.

Examples 7. (1). The $\mathbb{Z}$-module $\mathbb{Q}$ of rational numbers has no maximal submodules. Every cyclic submodule of $\mathbb{Q}$ is small, therefore $\mathbb{Q}$ is principally supplemented $\mathbb{Z}$-module. But $\mathbb{Q}$ is not supplemented.
(2). Consider the $\mathbb{Z}$-module $M = \mathbb{Q} \oplus (Z/\mathbb{Z}2)$. We prove M is principally supplemented module but not supplemented. Let $(u, \overline{v}) \in M$. We first prove that $(u, \overline{v})\mathbb{Z}$ has a supplement in M. We divide the proof in some cases :
Case (i) $u = 1$ and $\overline{v} = \overline{1}$. It is rutin to show that $M = (1, \overline{1})\mathbb{Z} + (\mathbb{Q} \oplus (\overline{0}))$ and $(1, \overline{1})\mathbb{Z} \cap (\mathbb{Q} \oplus (\overline{0})) = (1, \overline{0})\mathbb{Z}$ is small in $(\mathbb{Q} \oplus (\overline{0}))$.
Case (ii) $u = 1$ and $\overline{v} = \overline{0}$. Then $(u, \overline{v})\mathbb{Z} = (1, \overline{0})\mathbb{Z}$ is small in $\mathbb{Q} \oplus (\overline{0}))$.
Case (iii) $u = 0$ and $\overline{v} = \overline{1}$. Then $(u, \overline{v})\mathbb{Z} = (1, \overline{0})\mathbb{Z}$ is direct summand of M.
Case (iv) $u \neq 1, 0$ and $\overline{v} = \overline{1}$. Let $(x, \overline{y}) \in M$. We prove $(x, \overline{y}) \in (u, \overline{1})\mathbb{Z} + (\mathbb{Q} \oplus (\overline{0}))$. For if $\overline{y} = \overline{1}$, then $(x, \overline{y}) = (x, \overline{1}) = (u, \overline{1}) + (x - u, \overline{0}) \in (u, \overline{1})\mathbb{Z} + (\mathbb{Q} \oplus (\overline{0}))$. Assume that $\overline{y} = \overline{0}$. Then $(x, \overline{y}) = (x, \overline{0}) = (u, \overline{1})0 + (x, \overline{0}) \in (u, \overline{1})\mathbb{Z} + (\mathbb{Q} \oplus (\overline{0}))$. Hence $(x, \overline{y}) \in (u, \overline{1})\mathbb{Z} + (\mathbb{Q} \oplus (\overline{0}))$ and so $M = (u, \overline{1})\mathbb{Z} + (\mathbb{Q} \oplus (\overline{0}))$. Since $((u, \overline{1})\mathbb{Z}) \cap (\mathbb{Q} \oplus (\overline{0})) = (2u, \overline{0})\mathbb{Z}$ and $(2u, \overline{0})\mathbb{Z}$ is small in $\mathbb{Q} \oplus (\overline{0})$. It follows that, in either cases, $(u, \overline{v})\mathbb{Z}$ has a supplement in M and M is principally supplemented $\mathbb{Z}$-module.
If M were supplemented $\mathbb{Z}$-module, its direct summand $\mathbb{Q}$ would be a supplemented $\mathbb{Z}$-module. A contradiction. So M is not supplemented.
(3). Consider the $\mathbb{Z}$-modules $M_1 = \mathbb{Z}/\mathbb{Z}2$ and $M_2 = \mathbb{Z}/\mathbb{Z}8$. It is clear that M_1 and M_2 are principally supplemented. Let $M = M_1 \oplus M_2$. Then M is a principally supplemented module $\mathbb{Z}$-module but not principally lifting. Let $N_1 = (\overline{1}, \overline{2})\mathbb{Z}$, $N_2 = (\overline{1}, \overline{1})\mathbb{Z}$, $N_3 = (\overline{0}, \overline{2})\mathbb{Z}$, $N_4 = (\overline{0}, \overline{4})\mathbb{Z}$, $N_5 = (\overline{1}, \overline{4})\mathbb{Z}$, M_1 and M_2 are proper

cyclic submodules of M. $M = M_1 \oplus M_2 = N_2 \oplus N_5$ and N_3, N_4 are small submodules of M. $M = N_1 + N_2$ and $N_1 \cap N_2 = N_4$ small in N_2. Hence M is principally supplemented module. Since $M = N_1 + N_2$, N_1 is not small in M and it is not a direct summand of M and does not contain any nonzero direct summand of M. Hence M is not principally lifting.

Let M be a module. A submodule N is called *fully invariant* if for each endomorphism f of M, $f(N) \leq N$. Let $S = End(M_R)$, the ring of R-endomorphisms of M. Then M is a left S-, right R-bimodule and a principal submodule N of the right R-module M is fully invariant if and only if N is a sub-bimodule of M. Clearly 0 and M are fully invariant submodules of M. The right R-module M is called a *duo module* provided every submodule of M is fully invariant. For the readers' convenience we state and prove Lemma 8 which is proved in [14].

Lemma 8. *Let a module $M = \bigoplus_{i\in I} M_i$ be a direct sum of submodules M_i $(i \in I)$ and let N be a fully invariant submodule of M. Then $N = \bigoplus_{i\in I}(N \cap M_i)$.*

Proof. For each $j \in I$, let $p_j : M \to M_j$ denote the canonical projection and let $i_j : M_j \to M$ denote inclusion. Then $i_j p_j$ is an endomorphism of M and hence $i_j p_j(N) \subseteq N$ for each $j \in I$. It follows that $N \subseteq \bigoplus_{j\in I}\ i_j p_j(N) \subseteq \bigoplus_{j\in I}(N \cap M_j) \subseteq N$, so that $N = \bigoplus_{j\in I}(N \cap M_j)$. □

It is easily proved that finite direct sum of supplemented modules is again supplemented. But this is not the case for principally supplemented modules. But it is the case for some classes of modules.

Theorem 9. *Let $M = M_1 \oplus M_2$ be a decomposition of M with M_1 and M_2 principally supplemented modules. If M is a duo module, then M is principally supplemented.*

Proof. Let $M = M_1 \oplus M_2$ be a duo module and mR be a submodule of M. By Lemma 8, $mR = ((mR) \cap M_1) \oplus ((mR) \cap M_2)$. Let $m = m_1 + m_2$ where $m_1 \in M_1$, $m_2 \in M_2$. Then $m_1R = (mR) \cap M_1$ and $m_2R = (mR) \cap M_2$. Since $(mR) \cap M_1$ and $(mR) \cap M_2$ are principal submodules of M_1 and M_2 respectively, there exist $A_1 \leq M_1$ such that $M_1 = m_1R + A_1$, $(m_1R) \cap A_1$ is small in A_1 and $A_2 \leq M_2$ such that $M_2 = (m_2R) + A_2$ and $(m_2R) \cap A_2$ is small A_2. Then $M = (m_1R) + (m_2R) + A_1 + A_2 = (mR) + A_1 + A_2$. We prove $(mR) \cap (A_1 + A_2)$ is small in $A_1 + A_2$.

$$\begin{aligned}(mR) \cap (A_1 + A_2) &= ((mR) \cap M_1 + (mR) \cap M_2) \cap (A_1 + A_2)\\ &\leq (A_1 \cap (((mR) \cap M_1) + M_2)) + (A_2 \cap (((mR) \cap M_2) + M_1))\\ &\leq ((mR) \cap M_1) \cap (A_1 + M_2) + ((mR) \cap M_2) \cap (A_2 + M_1).\end{aligned}$$

On the other hand
$((mR) \cap M_1) \cap (A_1 + M_2) = (m_1R) \cap (A_1 + M_2) \leq A_1 \cap ((m_1R) + M_2) \leq (m_1R) \cap (A_1 + M_2)$ implies $(m_1R) \cap (A_1 + M_2) = A_1 \cap ((m_1R) + M_2) = (m_1R) \cap A_1$.
Similarly $(m_2R) \cap (A_2 + M_1) = A_2 \cap ((m_2R) + M_1) = (m_2R) \cap A_2$. Since $(m_1R) \cap A_1$ and $(m_2R) \cap A_2$ are small in A_1 and A_2 respectively, by Lemma 1 (2) $(m_1R) \cap A_1 + (m_2R) \cap A_2$ is small in $A_1 + A_2$. Again by Lemma 1 (3) $(mR) \cap (A_1 + A_2)$ is small in $A_1 + A_2$. □

Theorem 10. *Let M be a principally supplemented duo module. Then every direct summand of M is a principally supplemented module.*

Proof. Let $M = M_1 \oplus M_2$ and $m \in M_1$. There exists A a submodule such that $M = mR + A$ and $(mR) \cap A$ is small A. Then $M_1 = mR + (M_1 \cap A)$. By Lemma 8, $A = (A \cap M_1) \oplus (A \cap M_2)$. We prove that $(mR) \cap (A \cap M_1)$ is small in $A \cap M_1$. Let T be a submodule of $A \cap M_1$ with $A \cap M_1 = (mR) \cap (A \cap M_1) + T$. Then $A = (mR) \cap (A \cap M_1) + T + (A \cap M_2) = ((mR) \cap A) + T + (A \cap M_2)$. Since $(mR) \cap A$ is small in A, $A = T \oplus (A \cap M_2)$. It follows that $T = A \cap M_1$ that is what we have to prove. □

Theorem 11. *Let M be a principally supplemented distributive module. Then every direct summand of M is a principally supplemented module.*

Proof. Let $M = M_1 \oplus M_2$ and $m \in M_1$. There exists a submodule A of M such that $M = mR + A$ and $(mR) \cap A$ is small in A. Then $M_1 = (mR) + (M_1 \cap A)$. By Lemma 5, $(mR) \cap A$ is small in $M_1 \cap A$. □

For a module M, let $\mathrm{Rad}(M)$ denote the radical of M. A module M is said to be *a principally semisimple* if every cyclic submodule is a direct summand of M. Every semisimple module is principally semisimple. Every principally semisimple module is principally supplemented.

Lemma 12. *Let M be a principally supplemented distributive module. Then $M/\mathrm{Rad}(M)$ is a principally semisimple module.*

Proof. Let $m \in M$. There exists a submodule M_1 such that $M = mR + M_1$ and $(mR) \cap M_1$ is small in M_1. Then $M/\mathrm{Rad}(M) = [(mR + \mathrm{Rad}(M))/\mathrm{Rad}(M)] + [(M_1 + \mathrm{Rad}(M))/\mathrm{Rad}(M)]$. Now we prove that $(mR + \mathrm{Rad}(M)) \cap (M_1 + \mathrm{Rad}(M)) = \mathrm{Rad}(M)$. The distributivity of M implies $(mR + \mathrm{Rad}(M)) \cap (M_1 + \mathrm{Rad}(M)) = (mR) \cap M_1 + \mathrm{Rad}M$. Since $(mR) \cap M_1$ is small in M_1, therefore small in M, $(mR) \cap M_1 \leq \mathrm{RadM}$. Hence $M/\mathrm{Rad}(M) = [(mR + \mathrm{Rad}(M))/\mathrm{Rad}(M)] \oplus [(M_1 + \mathrm{Rad}(M))/\mathrm{Rad}(M)]$ and so every principal submodule of $M/\mathrm{Rad}(M)$ is a direct summand. □

Theorem 13 may be proved easily by making use of Lemma 12 for distributive modules. But we prove it in another way in general.

Theorem 13. *Let M be a principally supplemented module. Then $M = M_1 \oplus M_2$, where M_1 is semisimple module and M_2 is a module with $\mathrm{Rad}(M_2)$ small in M_2.*

Proof. By Zorn's Lemma we may find a submodule M_1 of M such that $Rad(M) \oplus M_1$ is small in M. We prove M_1 is semisimple. Let $m \in M_1$. Since M is principally supplemented, there exists a submodule A of M such that $M = mR + A$ and $(mR) \cap A$ is small in A. Then $(mR) \cap A = 0$. Let K be a maximal submodule of mR. If K is unique maximal submodule in mR, then it is small, therefore small in mR and so in M. This is not possible since $(mR) \cap Rad(M) = 0$. Hence there exists $x \in mR$ such that $mR = K + xR$. We claim that $K \cap (xR) = 0$. Otherwise let $0 \neq x_1 \in K \cap (xR)$. By hypothesis there exists C_1 such that $M = x_1R + C_1$ with $(x_1R) \cap C_1$ is small in M. So $M = x_1R \oplus C_1$ since $(x_1R) \cap C_1 \leq K \cap Rad(M) = 0$. Hence $mR = x_1R \oplus ((mR) \cap C_1)$ and $K = x_1R \oplus (K \cap C_1)$. If $K \cap C_1$ is nonzero, let $0 \neq x_2 \in K \cap C_1$. By hypothesis there exists C_2 such that $M = x_2R + C_2$ with $(x_2R) \cap C_2$ is small in M. So $M = x_2R \oplus C_2$ since $(x_2R) \cap C_2 \leq K \cap Rad(M) = 0$. Then $K \cap C_1 = (x_2R) \oplus (K \cap C_1 \cap C_2)$. Hence $mR = x_1R \oplus x_2R \oplus ((mR) \cap C_1 \cap C_2)$ and $K = x_1R \oplus x_2R \oplus (K \cap C_1 \cap C_2)$. If $K \cap C_1 \cap C_2$ is nonzero, similarly there exists $0 \neq x_3 \in K \cap C_1 \cap C_2$ and $C_3 \leq M$ such that $M = x_3R \oplus C_3$. Then $mR = x_1R \oplus x_2R \oplus x_3R \oplus ((mR) \cap C_1 \cap C_2 \cap C_3)$ and $K = x_1R \oplus x_2R \oplus x_3R \oplus$

$(K \cap C_1 \cap C_2 \cap C_3)$. This process must terminate at a finite step, say t. At this step $mR = x_1R \oplus x_2R \oplus x_3R \oplus ... \oplus x_tR$ and so $mR = K$ since at t^{th} step we must have $K \cap C_1 \cap C_2 \cap ... \cap C_t \leq (mR) \cap C_1 \cap C_2 \cap ... \cap C_t = 0$. This is a contradiction. There exists $x \in mR$ such that $mR = K \oplus (xR)$. Then xR is simple module. Hence every cyclic submodule of M_1 contains a simple submodule. As in the proof of [1, Lemma 9.2], we may prove M_1 is semisimple. □

Principally lifting modules and principally hollow modules are defined and investigated in [9]. A module M is called *principally lifting* if for all $m \in M$, M has a decomposition $M = N \oplus S$ with $N \leq mR$ and $(mR) \cap S$ is small in S, while M is said to be *principally hollow* if every proper cyclic submodule of M is small in M.

Lemma 14. *Let M be an indecomposable module. Consider following conditions :*

(1) *M is a principally lifting module.*
(2) *M is a principally hollow module.*
(3) *M is a principally supplemented module.*

Then (1)⇔(2) and (2)⇒ (3).

Proof. (1)⇒(2) Let $m \in M$. By (1) there exists a submodule A of mR such that $M = A \oplus B$ and $(mR) \cap B$ is small in B. By hypothesis $A = 0$ or $A = M$. If $A = 0$ then mR is small in M. Otherwise $mR = M$. Let K be a maximal submodule of M. Let $k \in K$. Then kR is small in M; for there exists a submodule C of kR such that $M = C \oplus D$ and $(kR) \cap D$ is small in D. By hypothesis C must be zero since K is maximal. Every cyclic submodule of K is small. Let $x \in M \setminus K$. Then $M = K + xR$. Let X be a direct summand of M with $X \leq xR$ with $M = X \oplus Y$ for some $Y \leq M$ and $(xR) \cap Y$ small in Y. Again by hypothesis X is zero or $X = M$. If X is zero then xR is small in M and so $K = M$. A contradiction. Assume $X = M$ then $xR = M$ and so K is small in M. Thus every cyclic submodule of M is small in M.

(2)⇔(1) Let $m \in M$. Then mR is small in M. In this case we take $A = 0$ and $B = M$ to show that $M = A \oplus B$, $A \leq mR$ and $(mR) \cap B$ is small in B.

(2)⇔(3) Let $m \in M$. By (2) each cyclic submodule is hollow. Then $M = (mR) + M$ and $(mR) \cap M$ is small in M. So M is a principally supplemented. □

Note that Lemma 14 (3)⇒ (2) does not hold in general. There exists an indecomposable principally supplemented module but not principally hollow.

Example 15. Let F be a field and x and y commuting indeterminates over F. Consider the polynomial ring $R = F[x, y]$, the ideals $I_1 = (x^2)$ and $I_2 = (y^2)$ of R, and the ring $S = R/(x^2, y^2)$. Let $M = \overline{x}S + \overline{y}S$. Then M is an indecomposable S-module, principally supplemented but not principally hollow.

A module M is called *refinable* if for any submodule U, V of M with $M = U + V$ there is a direct summand U' of M such that $U' \subseteq U$ and $M = U' + V$(See namely [**?**]).

Let M be a module. M is called *a weakly principally supplemented module* if for each $m \in M$ there exists a submodule A such that $M = mR + A$ and $(mR) \cap A$ is small in M. Every weakly supplemented module is weakly principally supplemented. The module M is called *a $\oplus$-principally supplemented* if for each $m \in M$ there exists a direct summand A of M such that $M = mR + A$ and $(mR) \cap A$ is small in A. $\oplus$-supplemented modules are studied in[4]. Every $\oplus$-supplemented

module is $\oplus$-principally supplemented and it is evident that every $\oplus$-principally supplemented is weakly principally supplemented. In a subsequent paper the authors investigates the interconnections between principally supplemented modules, weakly principally supplemented modules and $\oplus$-principally supplemented modules in detail. Recall that a module M is said to have the summand sum property if the sum of any two direct summands of M is again a direct summand of M. The summand sum property was studied by J. L. Garcia [2], who characterized modules with the summand sum property.

Theorem 16. *Let M be a refinable module. Consider following conditions*
(1) *M is principally lifting.*
(2) *M is principally $\oplus$-supplemented.*
(3) *M is principally supplemented.*
(4) *M is principally weak supplemented.*
Then (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (2).
If M has the summand sum property then (4) $\Rightarrow$ (1).

Proof. By definitions (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) always hold.

(4) $\Rightarrow$ (2) Let M be a principally weak supplemented module and $m \in M$. By (4) there exists a submodule A of M such that $M = mR + A$ and $(mR) \cap A$ is small in M. By hypothesis there exists a direct summand U of M with $U \leq A$ and $M = mR + U = U' \oplus U$ for some submodule U' of M. We claim that $(mR) \cap U$ is small in U. For if $(mR) \cap U + L = U$ for some submodule L of U, then $M = U' + ((mR) \cap U) + L = U' \oplus L$ as $(mR) \cap U$ is small in M. Hence $L = U$. Hence M is principally $\oplus$-supplemented.

(4) $\Rightarrow$ (1) Assume that M has the summand sum property and let $m \in M$. By (4) there exists a submodule A such that $M = mR + A$ and $(mR) \cap A$ is small in M. By hypothesis there exists a direct summand U_1 of M such that U_1 is contained in A and $M = mR + U_1 = U_1' \oplus U_1$. Since U_1 is direct summand and $(mR) \cap A$ is small in M, $(mR) \cap U_1$ is small in U_1. Again by hypothesis there exists a direct summand U_2 of M such that U_2 is contained in mR and $M = U_2 + U_1 = U_2 \oplus U_2'$. By the summand sum property $U_2 \cap U_1$ is a direct summand of M, $M = (U_2 \cap U_1) \oplus K$ for some submodule K of M. Then $U_1 = (U_2 \cap U_1) \oplus (K \cap U_1)$ and $M = U_2 \oplus (K \cap U_1)$. It is evident that $(mR) \cap (K \cap U_1)$ is small in $K \cap U_1$ since $(mR) \cap (K \cap U_1) \leq (mR) \cap U_1 \leq U_1$ and $(mR) \cap U_1$ is small in U_1, $(mR) \cap (K \cap U_1)$ is small in U_1 and so small in $K \cap U_1$ as $K \cap U_1$ is direct summand of M. □

4. Applications

In this section, we introduce and study some properties of principally semiperfect modules. A projective module P is called *a projective cover* of a module M if there exists an epimorphism $f : P \longrightarrow M$ with $Kerf$ is small in P, and a ring is called *perfect* (or *semiperfect*) if every R-module (or every simple R-module) has a projective cover. For more detailed discussion on small submodules, perfect and semiperfect rings. A module M is called *principally semiperfect* if every factor module of M by a cyclic submodule has a projective cover. A ring R is called *principally semiperfect* in case the right R-module R is principally semiperfect. Every semiperfect module is principally semiperfect.

Theorem 17. *Let M be a projective module. Then following conditions are equivalent.*

(1) *M is principally semiperfect.*
(2) *M is principally supplemented.*

Proof. (1)⇒ (2) Let $m \in M$. By (1) M/mR has a projective cover $P \xrightarrow{f} M/mR$. There exists $P \xrightarrow{g} M$ such that $f = \pi g$, where $M \xrightarrow{\pi} M/mR$ is the natural epimorphism. Let $m \in M$. There exists $x \in P$ such that $\pi(m) = f(x)$ since f is epimorphism. So $\pi(m) = f(x) = \pi(g(x))$ and then $m - g(x) \in Ker(\pi) = mR$. Hence $M = g(P) + mR$. We prove $g(P) \cap (mR)$ is small in $g(P)$. It suffices to show that $g(P) \cap (mR) = g(Ker(f)$ since $Ker(f)$ is small in P and any homomorphic image of small modules is small under epimorphic maps. Let $x \in Ker(f)$. Then $\pi g(x) = f(x) = 0$. So $g(x) \in Ker(\pi) = mR$. Hence $g(Ker(f) \leq g(P) \cap (mR)$. Let $mr \in g(P) \cap (mR)$ and $g(x) = mr$ for some $x \in P$. Then $f(x) = \pi(g(x)) = \pi(mr) = 0$. Hence $x \in Ker(f)$ and so $g(P) \cap (mR) \leq g(Ker(f)$. It follows that $g(P) \cap (mR) = g(Ker(f)$ and $g(P)$ is a complement of mR.

(2)⇒ (1) Let $m \in M$. By (2) there exists a submodule A such that $M = mR + A$ such that $(mR) \cap A$ is small in A. Let $M \xrightarrow{f} M/(mR)$ defined by $f(y) = a$ where $y = mr + a$ with $mr \in mR$, $a \in A$, and $M \xrightarrow{\pi} M/(mR)$ the natural epimorphism. There exists $M \xrightarrow{g} M$ such that $fg = \pi$. Then $M = g(M) + (mR) \cap A$. Hence $M = g(M) \cong M/\mathrm{Ker}(g)$. Since M is projective $M = \mathrm{Ker}(f) \oplus B$ and B is projective. Let $(fg)_B$ denote the restriction of fg on B. Then $\mathrm{Ker}(fg)_B = (mR) \cap A$ and so $B \xrightarrow{(fg)_B} M/(mR)$ is a projective cover of M. □

Let R be a module. R is called *semiregular ring* if every cyclicly presented R-module has a projective cover. We give a complete proof to Theorem 18 for the convenience of the reader.

Theorem 18. *Let R be a ring. The following conditions are equivalent :*

(1) *R is principally semiperfect.*
(2) *R is principally lifting.*
(3) *R is semiregular.*
(4) *R is principally supplemented.*

Proof. (1) ⇒ (2) Let $x \in R$. By (1) R/xR has a projective cover $P \xrightarrow{f} R/xR$ so that $\mathrm{Ker}(f)$ is small in P. Let $R \xrightarrow{\pi} R/xR$ be the natural epimorphism. Then there exists a map g such that $f = \pi g$. Then $R = g(P) + xR$ and $g(P) \cap (xR) = g(\mathrm{Ker}(f))$ is small in $g(P)$ since homomorphic images of small submodules are small.

(2) ⇒ (3) Assume that R is principally lifting. Let $x \in R$. Then there exists a direct summand right ideal A of R such that $R = A \oplus B$ and $(xR) \cap B$ is small in B. Then $xR = A \oplus (xR) \cap B$ and $(xR) \cap B$ is δ-small in M. By [**?**, Theorem 3.5] R is semiregular.

(3) ⇒ (4) Assume that R is semiregular. Let $x \in R$ and $\pi : R \to R/xR$ natural epimorphism. By hypothesis R/xR has a projective cover $f : P \to R/xR$. There exists $g : P \to R$ such that $f = \pi g$. Then $R = g(P) + xR)$ and $g(P) \cap (xR)$ is small in $g(P)$ since $g(P) \cap (xR) = g(\mathrm{Ker}(f)$ and $\mathrm{Ker}(f)$ is small in P. Hence R is principally supplemented.

(4) ⇒ (1) Clear from Theorem 17. □

Example 19. Let $R = \left\{ \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \mid x, y, z \in \mathbb{Z}_4 \right\}$ denote the ring of upper triangular matrices over integers. It is easy to check that principal right ideals of R are either small in R or direct summands of R. Hence R is principally supplemented right R-module. Let e_{12} denote the matrix unit having 1 at $(1,2)$ and zero elsewhere. Let $I = e_{12}R$. Then I is small right ideal and Jacobson radical $J(R)$ of R is equal to I. Hence $R/J(R)$ is not semisimple. Therefore R is not semiperfect ring.

Theorem 20. *Let M be a projective module with $\mathrm{Rad}(M)$ is small in M. Consider following conditions :*

(1) *M is principally supplemented.*
(2) *$M/\mathrm{Rad}(M)$ is principally semisimple.*

Then (1)⇒ (2). *If M is refinable module then* (2)⇒ (1).

Proof. (1)⇒ (2) Since P is a principally supplemented module, $P/\mathrm{Rad}(P)$ is principally semisimple by Lemma 12. (2)⇒ (1) Let mR be any cyclic submodule of P. By (2) There exists a submodule U of P such that

$$P/\ \mathrm{Rad}(P) = [((mR)+\mathrm{Rad}(P))/\mathrm{Rad}(P)] \oplus [U/\ \mathrm{Rad}(P)].$$

Then $P = (mR) + U$ and $((mR)+\mathrm{Rad}(P)) \cap U = (mR) \cap U + \mathrm{Rad}(P)] = \mathrm{Rad}(P)$. Since $P = (mR) + U$, being M refinable there exists a direct summand A of M such that $A \leq U$ and $M = (mR) + U = (mR) + A = B \oplus A$. $(mR) \cap U$ is small in M so it is small in U since U is direct summand. this completes the proof. □

References

[1] Anderson F.W. and Fuller K.R.,1974, *Rings and Categories of Modules*, Springer-Verlag, New York.
[2] Garcia J. L., 1989, *Properties of direct summand of modules*, Comm. Algebra 17, 7392.
[3] Goodearl K.R.,1976, Ring Theory : Nonsingular Rings and Modules, Dekker, New York
[4] Harmanci A., Keskin D. and Smith P.F., 1999, *On $\oplus$-Supplemented Modules*, Acta Math. Hungar.,83(1/2): 161-169.
[5] Kamal M. A. and Yousef A., *On Principally Lifting Modules*, Int. Electron. J. Algebra, 2 (2007) 127-137.
[6] Inankil H., Halicioglu S. and Harmanci A., *Principally δ-lifting modules*, Accepted for publication in Vietnam J. Mathematics.
[7] Keskin D.,1998, *Finite Direct Sums Of $(D1)$-Modules*, Turkish J. Math. 22 , no. 1, 85–91.
[8] Keskin D.,2000, *On Lifting Modules*, Comm. Algebra 28, no. 7, 3427–3440.
[9] Kamal M. A. and Yousef A., 2(2007), *On Principally Lifting Modules* Int. Electron. J. Algebra, 127-137.
[10] Lomp C., *Regular and Biregular Module Algebras*, Arab. J. Sci. and Eng., 33(2008), 351-363.
[11] Mohamed S.H and Müller B.J., 1990, *Continuous and Discrete Modules*, London Math. Soc. LNS 147 Cambridge Univ. Press, Cambridge.
[12] Nicholson W. K. and Yousif M. F., Quasi-Frobenius Rings, Cambridge Tracts in Mathematics 158, Cambridge University Press, 2003.
[13] Oshiro K., 1984, *Lifting Modules, Extending Modules and Their Applications To Generalized Uniserial Rings*, Hokkaido Math. J., 13, 339-346.
[14] Ozcan A. C., Harmanci A. and Smith P. F., *Duo Modules*, Glasgow Math. J., 48(3)(2006), 533-545.

Ummahan Acar, Mugla University, Faculty of Science, Department of Mathematics, Mugla, Turkey
E-mail address: uacar@mu.edu.tr

Abdullah Harmanci, Hacettepe University, Department of Mathematics, Ankara - Turkey
E-mail address: harmanci@hacettepe.edu.tr

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 3, Pages 89–96
ISSN 1930-1235: (2010)

THREE-STEP PROJECTION METHODS FOR NONCONVEX VARIATIONAL INEQUALITIES

MUHAMMAD ASLAM NOOR

Abstract. It is well-known that the nonconvex variational inequalities are equivalent to the fixed point problems. We use this equivalent formulation to suggest and analyze some three-step iterative methods for solving the nonconvex variational inequalities. We prove the convergence of the three-step iterative methods under suitable weaker conditions. Several special cases are also discussed. Our method of proof is very simple.

1. Introduction

Variational inequalities theory, which was introduced by Stampacchia [1], provides us with a simple, general and unified framework to study a wide class of problems arising in pure and applied sciences. For the applications, physical formulation, numerical methods and other aspects of variational inequalities, see [1-15] and the references therein. It is worth mentioning that all the research work carried our in this direction assumed that the underlying set is a convex set. In many practical problems, a choice set may not be a convex so that the existing results may not be applicable. In this direction, Noor [8] has introduced and considered a new class of variational inequalities, called nonconvex variational inequalities on the uniformly prox-regular sets. It is well-known that the uniformly prox-regular sets are nonconvex and include the convex sets as a special case, see [3,12]. Using the projection operator, Noor [8] has established the equivalence between the nonconvex variational inequalities and the fixed point problem. This equivalent formation has been used to consider the existence theory as well as to develop some numerical methods for nonconvex variational inequalities. We would like to point that the convergence analysis for the Mann and Ishkawa iterative methods requires that the operator must be strongly monotone and Lipschitz continuous. These conditions are very strict and rule out many applications. To overcome these drawbacks, several modifications of the projection iterative methods have been analyzed in recent years, see [6,9,13,15] and the references therein. Inspired and motivated by the research going on in this interesting and fascinating field, we suggest and analyze three-step iterative methods for solving the nonconvex variational inequalities. Using the technique of Noor [6,13,15], we also consider the convergence criteria of

2000 *Mathematics Subject Classification.* 49J40, 90C33.
Key words and phrases. variational inequalities; nonconvex sets; iterative methods; projection.
Submitted September 22, 2010. Published x x, .

three-step iterative method for the partially relaxed strongly monotone operator. It is well known that the partially relaxed strongly monotonicity implies monotonicity, but the converse is not true. This shows that the partially relaxed strongly monotonicity is a weaker condition than monotonicity. We remark that our proof of the convergence analysis is independent of the projection. Consequently, our results represent a refinement of the previously known results. Several special cases are also considered.

2. Basic Concepts

Let H be a real Hilbert space whose inner product and norm are denoted by $\langle \cdot, \cdot \rangle$ and $\|.\|$ respectively. Let K be a nonempty closed convex set in H. The basic concepts and definitions used in this paper are exactly the same as in Noor [8].

Definition 2.1. The proximal normal cone of K at $u \in H$ is given by

$$N_K^P(u) := \{\xi \in H : u \in P_K[u + \xi]\}.$$

where

$$P_K[u] = \{u^* \in K : d_K(u) = \|u - u^*\| = \inf_{v \in K} \|v - u\|\}.$$

The proximal normal cone $N_K^P(u)$ has the following characterization.

Lemma 2.1. Let K be a nonempty, closed and convex subset in H. Then $\zeta \in N_K^P(u)$ if and only if there exists a constant $\alpha > 0$ such that

$$\langle \zeta, v - u \rangle \leq \alpha \|v - u\|^2, \quad \forall v \in K.$$

Poliquin et al. [14] and Clarke et al [3] have introduced and studied a new class of nonconvex sets, which are called uniformly prox-regular sets. This class of uniformly prox-regular sets has played an important part in many nonconvex applications such as optimization, dynamic systems and differential inclusions.

Definition 2.2. For a given $r \in (0, \infty]$, a subset K_r is said to be normalized uniformly r-prox-regular if and only if every nonzero proximal normal to K_r can be realized by an r-ball, that is,$\forall u \in K_r$ and $0 \neq \xi \in N_{K_r}^P(u)$, one has

$$\langle (\xi)/\|\xi\|, v - u \rangle \leq (1/2r)\|v - u\|^2, \quad \forall v \in K_r.$$

It is clear that the class of normalized uniformly prox-regular sets is sufficiently large to include the class of convex sets, p-convex sets, $C^{1,1}$submanifolds (possibly with boundary) of H, the images under a $C^{1,1}$ diffeomorphism of convex sets and many other nonconvex sets; see [2,3,12]. Obviously, for $r = \infty$, the uniformly prox-regularity of K_r is equivalent to the convexity of K. This class of uniformly prox-regular sets have played an important part in many nonconvex applications such as optimization, dynamic systems and differential inclusions. It is known that if K_r is a uniformly prox-regular set, then the proximal normal cone $N_{K_r}^P(u)$ is closed as a set-valued mapping.

We now recall the well known proposition which summarizes some important properties of the uniformly prox-regular sets K_r.

Lemma 2.2. Let K be a nonempty closed subset of H, $r \in (0, \infty]$ and set $K_r = \{u \in H : d_K(u) < r\}$. If K_r is uniformly prox-regular, then
(i) $\forall u \in K_r, P_{K_r}(u) \neq \emptyset$.
(ii) $\forall r' \in (0, r)$, P_{K_r} is Lipschitz continuous with constant $\frac{r}{r-r'}$ on $K_{r'}$.

For a given nonlinear operator T, we consider the problem of finding $u \in K_r$ such that

$$\langle Tu, v - u\rangle \geq 0, \quad \forall v \in K_r, \tag{1}$$

which is called the *nonconvex variational inequality,* introduced and studied by Noor [8].

We now give some examples of prox-regular sets to give an idea and applications of the nonconvex variational inequalities (1). These examples are mainly due to Noor [10].

Example 2.1. Let $u = (x, y)$ and $v = (t, z)$ belong to the real Euclidean plane and consider $Tu = (2x, 2(y-1))$. Let $K = \{t^2 + (z-2)^2 \geq 4, \quad -2 \leq t \leq 2, \quad z \geq -2\}$ be a subset of the Euclidean plane. Then one can easily show that the set K is a prox-regular set K_r. It is clear that nonconvex variational inequality (1) has no solution.

Example 2.2. Let $u = (x, y) \in R^2$, $v = (t, z) \in R^2$ and let $Tu = (-x, 1 - y)$. Let the set K be the union of 2 disjoint squares, say A and B having respectively, the vertices in the points $(0,1), (2,1), (2,3), (0,3)$ and in the points $(4,1), (5,2), (4,3), (3,2)$.
The fact that K can be written in the form:

$$\big\{(t, z) \in R^2 : \max\{|t-1|, |z-2|\} \leq 1\} \cup \{|t-4| + |z-2| \leq 1\}\big\}$$

shows that it is a prox-regular set in R^2 and the nonconvex variational inequality (1) has a solution on the square B. We note that the operator T is the gradient of a strictly concave function. This shows that the square A is redundant.

We note that, if $K_r \equiv K$, the convex set in H, then problem (1) is equivalent to finding $u \in K$ such that

$$\langle Tu, v - u\rangle \geq 0, \qquad \forall v \in K. \tag{2}$$

Inequality of type (2) is called the *variational inequality*, which was introduced and studied by Stampacchia [1] in 1964. It turned out that a number of unrelated obstacle, free, moving, unilateral and equilibrium problems arising in various branches of pure and applied sciences can be studied via variational inequalities, see [1-13] and the references therein.

If K_r is a nonconvex (uniformly prox-regular) set, then problem (1) is equivalent to finding $u \in K_r$ such that

$$0 \in Tu + N^P_{K_r}(u) \tag{3}$$

where $N^P_{K_r}(u)$ denotes the normal cone of K_r at u in the sense of nonconvex analysis. Problem (3) is called the nonconvex variational inclusion problem associated with nonconvex variational inequality (1). This equivalent formulation plays a crucial

and basic part in this paper. We would like to point out this equivalent formulation allows us to use the projection operator technique for solving the nonconvex variational inequalities of the type (1).

Definition 2.3. An operator $T : H \to H$ is said to be *partially relaxed strongly monotone,* iff, there exists a constant $\alpha > 0$ such that

$$\langle Tu - Tv, z - v\rangle \geq -\alpha\|u - z\|^2, \quad \forall u, v, z \in H.$$

Note that for $z = u$, partially relaxed strongly monotonicity reduces to monotoncity. It is well known that the cocoercivity implies partially relaxed strongly monotonicity, but, the converse is not true, see Noor [6,13].

3. Main Results

It is known [8] that the nonconvex variational inequalities (1) are equivalent to the fixed point problem. We recall this result.

Lemma 3.1[8]. $u \in K_r$ is a solution of the nonconvex variational inequality (1) if and only if $u \in K_r$ satisfies the relation

$$u = P_{K_r}[u - \rho Tu], \tag{4}$$

where $\rho > 0$ is a constant and P_{K_r} is the projection of H onto the uniformly prox-regular set K_r.

Lemma 2.1 implies that (1) is equivalent to the fixed point problem (4). This alternative equivalent formulation is very useful from the numerical and theoretical points of view. Noor [7,8] has used this equivalent formulation to discuss the existence of a solution of the nonconvex variational inequality (1). Using the fixed point formulation (4), we suggest and analyze some iterative methods for solving the nonconvex variational inequality (1).

Algorithm 3.1. For a given $u_0 \in H$, find the approximate solution u_{n+1} by the iterative schemes

$$u_{n+1} = P_{K_r}[u_n - \rho Tu_n], \quad n = 0, 1, \ldots,$$

where $\rho > 0$ is a constant. For the convergence analysis of Algorithm 3.1, see Noor [8].

On can also suggest the following implicit method for solving the nonconvex variational inequality (1) as:

Algorithm 3.2. For a given $u_0 \in H$, find the approximate solution u_{n+1} by the iterative schemes

$$u_{n+1} = P_{K_r}[u_n - \rho Tu_{n+1}], \quad n = 0, 1, \ldots,$$

Noor[7] has studied the convergence analysis of Algorithm 3.2 for the pseudomonotone operator. We remark that Algorithm 3.2 is equivalent to the following iterative method

Algorithm 3.3. For a given $u_0 \in H$, find the approximate solution u_{n+1} by the iterative schemes

$$\begin{aligned} u_{n+1} &= P_{K_r}[u_n - \rho T w_n] \\ w_n &= P_{K_r}[u_n - \rho T u_n], \quad n = 0, 1, \ldots, \end{aligned}$$

which is known as the extragradient method, see Noor [10].

We now use the technique of updating the solution to rewrite the fixed-point formulation as:

$$\begin{aligned} w &= P_{K_r}[u - \rho T u] \\ y &= P_{K_r}[w - \rho T w] \\ u &= P_{K_r}[y - \rho T y], \end{aligned}$$

where $\rho > 0$ is a constant.

This is another different fixed point formulation of the nonconvex variational inequality (1). This alternative fixed-point formulation enables us to suggest the following iterative methods for solving the nonconvex variational inequality (1).

Algorithm 3.4. For a given $u_0 \in H$, find the approximate solution u_{n+1} by the iterative schemes

$$\begin{aligned} w_n &= P_{K_r}[u_n - \rho T u_n] \\ y_n &= P_{K_r}[w_n - \rho T w_n] \\ u_{n+1} &= P_{K_r}[y_n - \rho T y_n], \quad n = 0, 1, 2, ..., \end{aligned}$$

Algorithm 3.4 is called the three-step iterative method and can also be considered as an predictor-corrector methods for solving (1). We rewrite Algorithm 3.4 in the following equivalent form which plays a key role in the analysis of the convergence of Algorithm 3.4.

Algorithm 3.5 For a given $u_0 \in H$, find the approximate solution u_{n+1} by the iterative schemes

$$\langle \rho T u_n + w_n - u_n, v - w_n \rangle \geq 0, \quad \forall v \in K_r \tag{5}$$

$$\langle \rho T w_n + y_n - w_n, v - y_n \rangle \geq 0, \quad \forall v \in K_r \tag{6}$$

$$\langle \rho T y_n + u_{n+1} - y_n, v - u_{n+1} \rangle \geq 0, \quad \forall v \in K_r \tag{7}$$

We now consider the convergence analysis of Algorithm 3.4 and this is the main motivation of our next result.

Theorem 3.1. Let $u \in K_r$ be a solution of (1) and let u_{n+1} be the approximate solution obtained from Algorithm 3.4. If the operator T is partially relaxed strongly monotone with constant $\alpha > 0$, then

$$\|u_{n+1} - u\|^2 \leq \|y_n - u\|^2 - (1 - 2\alpha\rho)\|u_{n+1} - y_n\|^2 \tag{8}$$

$$\|y_n - u\|^2 \leq \|w_n - u\|^2 - (1 - 2\alpha\rho)\|w_n - y_n\|^2 \tag{9}$$

$$\|w_n - u\|^2 \leq \|u_n - u\|^2 - (1 - 2\alpha\rho)\|w_n - u_n\|^2. \tag{10}$$

Proof. Let $u \in K_r$ be solution of (1). Then

$$\langle Tu, v - u \rangle \geq 0, \quad \forall v \in K_r. \tag{11}$$

Take $v = w_n$ in (11), we have

$$\langle Tu, w_n - u\rangle \geq 0. \tag{12}$$

Taking $v = u$ in (5) and using (12), we have

$$\langle w_n - u_n, u - w_n\rangle \geq \rho\langle Tu_n - Tu, w_n - u\rangle \geq -\alpha\rho\|u_n - w_n\|^2, \tag{13}$$

since T is partially relaxed strongly monotone with constant $\alpha > 0$.

From (13), we have

$$\|w_n - u\|^2 \leq \|u_n - u\|^2 - (1 - 2\alpha\rho)\|w_n - u_n\|^2,$$

the required result (10).

Now taking $v = u_{n+1}$ in (11), we have

$$\langle Tu, u_{n+1} - u\rangle \geq 0. \tag{14}$$

Taking $v = u$ in (7), we have

$$\langle \rho Ty_n + u_{n+1} - y_n, u - u_{n+1}\rangle \geq 0. \tag{15}$$

From (15), (14) and using the partially relaxed strongly monotonicity T with constant $\alpha > 0$, we have

$$\|u_{n+1} - u\|^2 \leq \|y_n - u\|^2 - (1 - 2\alpha\rho)\|u_{n+1} - y_n\|^2,$$

the required result (8).

Taking $v = y_n$ in (11), we have

$$\langle Tu, y_n - u\rangle \geq 0. \tag{16}$$

Setting $v = u$ in (6), we have

$$\langle \rho Tw_n + y_n - w_n, u - y_n\rangle \geq 0. \tag{17}$$

From (17), (16) and using the partially relaxed strongly monotonicity of T, we have

$$\|y_n - u\|^2 \leq \|w_n - u\|^2 - (1 - \alpha\rho)\|y_n - w_n\|^2,$$

which is the required (9). □

Theorem 3.2. Let $u \in K_r$ be a solution of (1) and let u_{n+1} be the approximate solution obtained from Algorithm 3.4. If H is a finite dimensional space and $0 < \rho < \frac{1}{2\alpha}$, then $\lim_{n\to\infty} u_n = u$.

Proof. Let $\bar{u} \in K_r$ be a solution of (1). Then, the sequences $\{\|u_n - \bar{u}\|\}$ is nonincreasing and bounded and

$$\begin{aligned}
\sum_{n=0}^{\infty}(1 - 2\alpha\rho)\|u_{n+1} - w_n\|^2 &\leq \|y_0 - u\|^2 \\
\sum_{n=0}^{\infty}(1 - 2\alpha\rho)\|w_n - y_n\|^2 &\leq \|w_0 - u\|^2 \\
\sum_{n=0}^{\infty}(1 - 2\alpha\rho)\|w_n - u_n\|^2 &\leq \|u_0 - u\|^2,
\end{aligned}$$

which implies

$$\lim_{n\to\infty}\|u_{n+1} - w_n\| = 0 \quad \lim_{n\to\infty}\|w_n - y_n\| = 0. \quad \lim_{n\to\infty}\|y_n - u_n\| = 0.$$

Thus

$$\lim_{n\to\infty}\|u_{n+1}-u_n\| = |\lim_{n\to\infty}\|u_{n+1}-w_n\| + \lim_{n\to\infty}\|w_n-y_n\| + \lim_{n\to\infty}\|y_n-u_n\| = 0. \quad (18)$$

Let $\hat{u}$ be a cluster point of $\{u_n\}$; there exists a subsequence $\{u_{n_i}\}$ such that $\{u_{n_i}\}$ converges to $\hat{u}$. Replacing u_{n+1} by u_{n_i} in (7), w_n by u_{n_i} in (6), y_n by y_{n_i} in (5) and taking the limits and using (18), we have

$$\langle T\hat{u}, v-\hat{u}\rangle \geq 0, \quad \forall v \in K_r.$$

This shows that $\hat{u} \in K_r$ solves the nonconvex variational inequality (1) and

$$\|u_{n+1}-\hat{u})\|^2 \leq \|u_n-\hat{u}\|^2,$$

which implies that the sequence $\{u_n\}$ has a unique cluster point and $\lim_{n\to\infty} u_n = \hat{u}$, is a solution of (1), the required result. □.

Acknowledgement. The author would like to express his gratitude to Dr. M. Junaid Zaidi, Rector, CIIT, for providing excellent research facilities.

References

[1] Stampacchia, G.: Formes bilineaires coercitives sur les ensembles convexes, C. R. Acad. Sci, Paris, **258**,4413-4416(1964)
[2] Bounkhel, M., Tadji, L., Hamdi, A.: Iterative schemes to solve nonconvex variational problems, J. Inequal. Pure Appl. Math.,**4**, 1-14(2003)
[3] Clarke, F. H., Ledyaev, Y. S., Wolenski, P. R.: Nonsmooth Analysis and Control Theory, Springer-Verlag, Berlin, 1998.
[4] Kinderlehrer, D., Stampacchia, G.: An Introduction to Variational Inequalities and Their Applications, SIAM, Philadelphia, 2000.
[5] Moudafi, A.: Projection methods for s system of nonconvex variational inequalities, **71**, 517-520 (2009)
[6] Noor, M. A.: Some developments in general variational inequalities, Appl. Math. Computation, **152**,199-277 (2004).
[7] Noor, M. A.: Implicit iterative methods for nonconvex variational inequalities, J. Optim. Theory Appl. **143**, 619-624(2009).
[8] Noor, M. A.: Projection methods for nonconvex variational inequalities, Optim Lett. **3**, 411-418(2009).
[9] Noor, M. A. :An extragradient algorithm for solving general noncovex variational inequalities, Appl. Math. Letters, **23**, 917-921, (2010).
[10] Noor, M. A. : On an implicit method for nonconvex variational inequalities, J. Optim. Theory. Appl. **147**(2010).
[11] Noor, M. A., Noor, K. I., Rassias, T. M.: Some aspects of variational inequalities, J. Comput. Appl. Math. **47**, 285-312(1993).
[12] Poliquin, R. A., Rockafellar, R. T., Thibault, L.: Local differentiability of distance functions, Trans. Amer. Math. Soc., **352**, 5231-5249(2000).
[13] Noor, M. A.: New approximation schemes for general variational inequalities, J. Math. Anal. Appl. **251**, 217-229 (2000).
[14] Noor, M. A.: General variational inequalities, Appl. Math. Letters, **1**, 119-121 (1988).
[15] Noor, M. A. : Principles of Variational Inequalities, Lap-Lambert Academic Publishing, Germany, 2009.

Mathematics Department, COMSATS Institute of Information Technology, Islamabad, Pakistan

Mathematics Department, College of Science, King Saud University, Riyadh, Saudi Arabia

E-mail address: noormaslam@hotmail.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 105–122
ISSN 1930-1235: (2010)

CREATING VARIATIONAL INTEGRATORS WITH A COMPUTER ALGEBRA SYSTEM

CHRISTIAN HELLSTRÖM

Abstract. A library to create (new) variational integrators to arbitrary order by means of a computer algebra system is presented. The library provides an interface to design as well as analyse variational integrators for dynamical systems, either with non-conservative forces or without.

1. Introduction

Simulations of generic dynamical systems can rarely be carried out analytically, for the class of integrable dynamical systems has zero measure in the space of all dynamical systems, hence the need for numerical integration algorithms. There is an abundance of numerical integration algorithms, available either in the public domain or embedded in proprietary software. Probably the most common algorithms implemented and used are the classical one-step methods, including the classical Runge–Kutta algorithm, multi-step methods, such as the Adams–Bashforth–Moulton algorithm, and adaptive methods, to which the Runge–Kutta–Fehlberg and Bulirsch–Stoer algorithms belong. Nowadays, Taylor's method backed by either symbolic or automatic (numerical) differentiation techniques (see e.g. [11]) is increasingly being used for highly accurate computations, although we shall not dwell on these alternative integration techniques in the sequel.

For simulations over relatively short time spans as compared to the intrinsic time scales standard (non-geometric) integrators are often advantageous, as they can be both accurate and fast. Extended computations require a different, 'geometric' approach, as non-geometric methods tend to generate or dissipate energy artificially due to the fact that they do not respect the fundamental geometry of the phase flow, which means that at some point the errors dominate.

For dynamical systems that can be formulated as Hamiltonian systems there exist so-called geometric numerical integrators. These integrators respect the fundamental (differential) geometric structure, which underlies the dynamical evolution of the system. It has been common to design such geometric numerical integrators based on either previous knowledge of classical numerical integration algorithms, such as the (partitioned) Runge–Kutta methods, or (approximate) solutions to the Hamilton–Jacobi equation for transformations near the identity.

2000 *Mathematics Subject Classification.* 65P30 and 65P10 and 65L05 and 37M15.

Key words and phrases. variational integrators and geometric numerical integrators and numerical integration and computer algebra system.

Funded by the European Commission through the Astrodynamics Network under Marie Curie contract number MRTN-CT-2006-035151.

There is, however, a different approach that bypasses many of the difficulties inherent in the design of higher-order versions of these geometric numerical integrators. It relies on the discretization of the action, from which the numerical algorithms can be derived in a straightforward manner [24]. These variational integrators, as they are known throughout the literature, conserve the Poisson structure. Any continuous symmetries present in the original system translate directly to the discretized version, and thus all (equivariant) momentum maps are preserved infinitesimally. For non-integrable systems either the Poisson structure or the total energy can be conserved exactly in numerical simulations [10], so that variational integrators do not generally preserve the energy. It can be shown, though, that these variational integrators remain close to the original dynamical systems [13, 20], so that in practice the energy error is bounded.

An approach to design variational integrators systematically based on higher-order approximations to the discrete action by means of a computer algebra system is covered here, in particular a freely available package named VarInt for the computer algebra system Maple is presented, with which variational integrators of arbitrary order and based on any derivative-free quadrature rule can be created and analysed.

The fundamental concepts from discrete mechanics are reviewed briefly in section 2, after which the various built-in quadrature rules are discussed in section 3. In section 4, the details of the package VarInt are discussed, and numerous examples are given on how to obtain (new) variational integrators for both generic and specific dynamical systems.

2. Variational Integrators

Consider an autonomous Lagrangian $L\colon \mathbf{T}\mathbb{Q} \to \mathbb{R}$, where $\mathbf{T}\mathbb{Q}$ is the tangent bundle of the configuration space $\mathbb{Q}$, on which the generalized coordinates q form a chart. A chart for the tangent bundle is given by $(q, \dot{q})$, where $\dot{q} = \mathrm{d}q/\mathrm{d}t$ with t the time. Here and henceforth it is assumed that the generalized coordinates are at least $\mathcal{C}^2([a,b],\mathbb{R})$, where $t \in [a,b]$. The corresponding action functional reads

$$S[L] = \int_a^b L(q(t), \dot{q}(t))\, \mathrm{d}t, \tag{1}$$

from which the famous Euler–Lagrange equations are retrieved upon requiring stationarity of the action functional for fixed endpoints, that is $\delta S[L] = 0$ with $\delta q(a) = \delta q(b) = 0$.

Instead of deriving the Euler–Lagrange equations from the action and then discretizing the equations of motion, a different approach is used in the case of variational integrators. Here we discretize the action first by choosing an appropriate quadrature formula, and then we can derive the discrete version of the Euler–Lagrange equations, which are commonly known as the discrete Euler–Lagrange (dEL) equations. The resulting integration algorithms preserve the differential geometric structure of these dynamical systems *automatically* [24]. Moreover, the order of the quadrature formula determines the order of the variational integrator.

2.1. **Quadrature.**

To obtain a one-step numerical integration algorithm, introduce a sequence of times $t_k = hk$ with $k = 0, \ldots, N$, at which the Lagrangian is to be evaluated. Here h is a sufficiently small time step. Furthermore, let $q_k \approx q(t_k)$ and $\dot{q}_k \approx \dot{q}(t_k)$ for $k = 0, \ldots, N$, and consider the action between two consecutive

points in time, say t_k and t_{k+1}. Since for a generic dynamical system with a certain Lagrangian we do not know the functional form of the solutions in advance, we may choose an interpolating function, usually a polynomial, in accordance with the quadrature rule on the interval $[t_k, t_{k+1}]$. For a quadrature rule of arbitrary order, we evaluate the Lagrangian at $(s+1) \geq 2$ distinct nodes, so that each time step is subdivided into s substeps t_k^i for $i = 0, \ldots, s\}$. Define $t_k^0 = t_k$ and $t_k^s = t_{k+1}$, and let $t_k^i - t_k^{i-1} = \gamma_i h > 0$ for $i = 1, \ldots, s$, so that $\sum_{i=1}^{s} \gamma_i = 1$. The action becomes a sum of the multipoint discrete Lagrangian L_d, which depends on the time step h:

$$\begin{aligned} S[L] &= \sum_{k=0}^{N-1} \int_{t_k}^{t_{k+1}} L\left(q(t), \dot{q}(t)\right) \mathrm{d}t \\ &\approx \sum_{k=0}^{N-1} L_\mathrm{d}\left(q_k^0, q_k^1, \ldots, q_k^s\right) \\ &= \sum_{k=0}^{N-1} \sum_{i=1}^{s} L_\mathrm{d}^i\left(q_k^{i-1}, q_k^i\right), \end{aligned} \tag{2}$$

where $L_\mathrm{d}^i \colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$; it relates the multipoint discrete Lagrangian to its basic components defined on each segment of 'length' $\gamma_i h$. Notice that the discrete state space $\mathbb{Q} \times \mathbb{Q}$ contains the same amount of information as the tangent bundle of the configuration manifold, for locally $\mathbf{T}\mathbb{Q} \cong \mathbb{Q} \times \mathbb{Q}$.

Let $L_\mathrm{d}^{[k]}$ be shorthand for $L_\mathrm{d}\left(q_k^0, q_k^1, \ldots, q_k^s\right)$, and let D_i denote the derivative with respect to the argument carrying the substep label i, that is $D_i L_\mathrm{d}^{[k]} = \partial L_\mathrm{d}^{[k]} / \partial q_k^i$. Stationarity of the discrete action, that is $S[L_\mathrm{d}] = 0$, for arbitrary variations δq_k^i yields the discrete Euler–Lagrange (dEL) equations:

$$D_0 L_\mathrm{d}\left(q_{k+1}^0, q_{k+1}^1, \ldots, q_{k+1}^s\right) + D_s L_\mathrm{d}\left(q_k^0, q_k^1, \ldots, q_k^s\right) = 0, \tag{3a}$$

$$D_i L_\mathrm{d}\left(q_k^0, q_k^1, \ldots, q_k^s\right) = 0, \qquad i = 1, \ldots, s-1. \tag{3b}$$

These equations determine the one-step (flow) map $\left(q(t_k), \dot{q}(t_k)\right) \mapsto \left(q(t_{k+1}), \dot{q}(t_{k+1})\right)$ of the variational integrator. These equations can also be written as

$$D_i L_\mathrm{d}^i\left(q_k^{i-1}, q_k^i\right) + D_i L_\mathrm{d}^{i+1}\left(q_k^i, q_k^{i+1}\right) = 0$$

for each of the components $i = 1, \ldots, s$. Please notice that for $i = s$, the last term on the left-hand side is $D_0 L_\mathrm{d}^1\left(q_{k+1}^0, q_{k+1}^1\right) = D_0 L_\mathrm{d}^{[k+1]}$ by virtue of the identity $q_k^{i+s} = q_{k+1}^i$.

It is common to write the one-step map in terms of the canonical coordinates and momenta on the cotangent bundle. To do that, we need to find a discrete analogue of the Legendre transformation, or fibre derivative $\mathbb{F}L \colon \mathbf{T}\mathbb{Q} \to \mathbf{T}^\star\mathbb{Q}$, which reads in generalized coordinates

$$\mathbb{F}L \colon (q, \dot{q}) \mapsto \left(q, \frac{\partial L}{\partial \dot{q}}(q, \dot{q})\right). \tag{4}$$

The discretized form of the Legendre transformation involves the endpoints of each time segment, $\mathbb{F}^\pm L_\mathrm{d}^i \colon \mathbb{Q} \times \mathbb{Q} \to \mathbf{T}^\star\mathbb{Q}$:

$$\begin{aligned} \mathbb{F}^+ L_\mathrm{d}^i &\colon \left(q_k^{i-1}, q_k^i\right) \mapsto \left(q_k^i, p_k^i\right) = \left(q_k^i, D_i L_\mathrm{d}^i\left(q_k^{i-1}, q_k^i\right)\right), \\ \mathbb{F}^- L_\mathrm{d}^i &\colon \left(q_k^{i-1}, q_k^i\right) \mapsto \left(q_k^{i-1}, p_k^{i-1}\right) = \left(q_k^{i-1}, -D_{i-1} L_\mathrm{d}^i\left(q_k^{i-1}, q_k^i\right)\right). \end{aligned}$$

In fact, the discrete Euler–Lagrange equations (3) can be written as

$$\mathbb{F}^+ L_{\mathrm{d}}^i \left(q_k^{i-1}, q_k^i\right) = \mathbb{F}^- L_{\mathrm{d}}^{i+1} \left(q_k^i, q_k^{i+1}\right),$$

which implies that the canonical momenta are unique along any solution. Now, the one-step map, written in canonical coordinates and momenta, is

$$p_k^{i-1} = -D_{i-1} L_{\mathrm{d}}^i \left(q_k^{i-1}, q_k^i\right),$$
$$p_k^i = D_i L_{\mathrm{d}}^i \left(q_k^{i-1}, q_k^i\right),$$

for $i = 1, \ldots, s$, or equivalently,

$$p_k = -D_0 L_{\mathrm{d}} \left(q_k^0, q_k^1, \ldots, q_k^s\right), \tag{7a}$$
$$p_{k+1} = D_s L_{\mathrm{d}} \left(q_k^0, q_k^1, \ldots, q_k^s\right), \tag{7b}$$
$$D_i L_{\mathrm{d}} \left(q_k^0, q_k^1, \ldots, q_k^s\right) = 0, \qquad i = 1, \ldots, s-1, \tag{7c}$$

where the last set of $(s-1)$ equations seems 'unaffected' by the Legendre transformation, and remains as in equation (3b). The reason for that is quite intuitive yet profound: on each time interval an interpolatory function approximates the Lagrangian function, so that the discrete Lagrangian becomes a piecewise smooth function. The momentum p_k^i computed with the discrete Legendre transformation $\mathbb{F}^- L_{\mathrm{d}}^{i+1}$ requires the interpolation function on the time segment $\left[t_k^i, t_k^{i+1}\right]$, or data 'from the right' of t_k^i, whereas the same momentum calculated from the transformation $\mathbb{F}^+ L_{\mathrm{d}}^i$ uses the interpolation function on $\left[t_k^{i-1}, t_k^i\right]$, or values 'from the left' of t_k^i. Obviously, the intermediate momenta ($i = 1, \ldots, s-1$) are identical, because the interpolating function used is the same, so that its derivatives from the left and right coincide. In principle, the momenta at the endpoints of each time interval need not be related at all, for the interpolating function merely has to be equal in value in order to have a piecewise smooth discrete Lagrangian. However, the principle of stationary action relates the approximate (discrete) Lagrangian function to the (approximated) integral curves of the dynamical system, which in turn relates these momenta by means of the discrete Euler–Lagrange equations. Therefore, the momenta are unique along any trajectory, and equations (3b) and (7c) are identical in both representations.

All integrators obtained in this way are structure-preserving, that is to say they preserve the Poisson structure of the flow. The (discrete) Lagrangian flow conserves the (discrete) symplectic form as well as any momentum maps associated with (infinitesimal) invariances of the (discrete) action under symmetry operations, as shown by Marsden and West [24]. Obviously for this statement to hold we have to choose the time step h sufficiently small, which depends on the particulars of the problem under consideration. Please observe that the right-hand sides of the discrete Euler–Lagrange equations (3) and their Hamiltonian equivalents (7) depend on the time step h.

2.2. **Non-Conservative Forces.** The variational formalism arises naturally throughout mathematical physics, and can of course be extended (see e.g. [17, 19, 21, 22, 24] for a few possibilities). The main advantage and actual utility of the variational construction of numerical integration algorithms lies in the fact that non-conservative forces can easily be included in a consistent way. N-body simulations in atomic and molecular physics, astrophysics, and chemistry are excellent candidates for these non-conservative variational integrators, as these simulations often become

unstable under time reversal, so that higher-order geometric numerical integrators based on the symmetric composition of lower-order ones are not viable alternatives.

A force is a fibre-preserving map over the identity $F\colon \mathbf{T}\mathbb{Q} \to \mathbf{T}^\star\mathbb{Q}$, which reads $F\colon (q,\dot{q}) \mapsto (q, F(q,\dot{q}))$ in coordinates. In order to include these non-conservative forces in the variational framework, we merely have to replace Hamilton's principle $\delta S[L] = 0$ by the so-called Lagrange–d'Alembert principle:

$$\sum_{k=0}^{N-1} \left[\delta \int_{t_k}^{t_{k+1}} L(q(t), \dot{q}(t))\, \mathrm{d}t + \int_{t_k}^{t_{k+1}} F(q(t), \dot{q}(t)) \cdot \delta q(t)\, \mathrm{d}t \right] = 0. \tag{8}$$

As before, all integrals are approximated by a quadrature rule from $t \in [t_k, t_{k+1}]$, so that the Lagrange–d'Alembert principle becomes

$$\sum_{k=0}^{N-1} \left[\delta \underbrace{\sum_{i=0}^{s} L\left(q_{\mathrm{int}}\left(t_k^i\right), \dot{q}_{\mathrm{int}}\left(t_k^i\right)\right)}_{L_{\mathrm{d}}\left(q_k^0, q_k^1, \ldots, q_k^s\right)} + \sum_{i=0}^{s} \underbrace{F\left(q_{\mathrm{int}}\left(t_k^i\right), \dot{q}_{\mathrm{int}}\left(t_k^i\right)\right) \cdot \delta q_{\mathrm{int}}\left(t_k^i\right)}_{f_k^i \cdot \delta q_k^i = f_k^i\left(q_k^0, q_k^1, \ldots, q_k^s\right) \cdot \delta q_k^i} \right] = 0, \tag{9}$$

where we have written the discrete Lagrangian in terms of $q_{\mathrm{int}}\left(t_k^i\right) = q_{\mathrm{int}}\left(q_k^0, \ldots, q_k^s; t_k^i\right)$, the interpolatory approximation of $q(t)$ for $t \in [t_k, t_{k+1}]$. It is worth mentioning that

$$\delta q_{\mathrm{int}}\left(t_k^i\right) = \sum_{j=0}^{s} \frac{\partial q_{\mathrm{int}}\left(t_k^i\right)}{\partial q_k^j} \delta q_k^j,$$

and that generally $q_{\mathrm{int}}\left(q_k^0, \ldots, q_k^s; t_k^i\right) \neq q_k^i$. Therefore,

$$f_k^i\left(q_k^0, q_k^1, \ldots, q_k^s\right) = \sum_{j=0}^{s} F\left(q_{\mathrm{int}}\left(t_k^j\right), \dot{q}_{\mathrm{int}}\left(t_k^j\right)\right) \cdot \frac{\partial q_{\mathrm{int}}\left(t_k^j\right)}{\partial q_k^i}.$$

In a manner similar to the derivation of the discrete Euler–Lagrange equations (3), the *forced* discrete Euler–Lagrange equations can be shown to be

$$D_0 L_{\mathrm{d}}^{[k+1]} + f_{k+1}^0 + D_s L_{\mathrm{d}}^{[k]} + f_k^s = 0, \tag{10a}$$

$$D_i L_{\mathrm{d}}^{[k]} + f_k^i = 0, \qquad i = 1, \ldots, s-1. \tag{10b}$$

Again, it is possible to write the forced discrete Euler–Lagrange equations in terms of the canonical coordinates and momenta instead. To that end, define the left and right discrete forces $f_{\mathrm{d}}^{i\,\pm}\colon \mathbb{Q}\times\mathbb{Q} \to \mathbb{R}$, $f_{\mathrm{d}}^{i\,-}\left(q_k^{i-1}, q_k^i\right)$ and $f_{\mathrm{d}}^{i\,+}\left(q_k^{i-1}, q_k^i\right)$, respectively, such that $f_k^0 = f_{\mathrm{d}}^{1\,-}\left(q_k^0, q_k^1\right)$, $f_k^s = f_{\mathrm{d}}^{s\,+}\left(q_k^{s-1}, q_k^s\right)$, and $f_k^i = f_{\mathrm{d}}^{i\,+}\left(q_k^{i-1}, q_k^i\right) + f_{\mathrm{d}}^{i+1\,-}\left(q_k^i, q_k^{i+1}\right)$ for $i = 1, \ldots, s-1$. These, in turn, imply that

$$\int_{t_k}^{t_{k+1}} F(q(t), \dot{q}(t)) \cdot \delta q(t)\, \mathrm{d}t \approx \sum_{i=1}^{s} \left[f_{\mathrm{d}}^{i\,-}\left(q_k^{i-1}, q_k^i\right) \delta q_k^{i-1} + f_{\mathrm{d}}^{i\,+}\left(q_k^{i-1}, q_k^i\right) \delta q_k^i \right].$$

Consequently, one finds the that equations (10) can be written as

$$D_i L_{\mathrm{d}}^i\left(q_k^{i-1}, q_k^i\right) + f_{\mathrm{d}}^{i\,+}\left(q_k^{i-1}, q_k^i\right) + D_i L_{\mathrm{d}}^{i+1}\left(q_k^i, q_k^{i+1}\right) + f_{\mathrm{d}}^{i+1\,-}\left(q_k^i, q_k^{i+1}\right) = 0,$$

for $i = 1, \ldots, s$.

The appropriate discrete Legendre transformations for forced dynamical systems are

$$\mathbb{F}^{f+}L_{\mathrm{d}}^{i}\colon\ \left(q_k^{i-1},q_k^{i}\right)\mapsto\left(q_k^{i},p_k^{i}\right)=\left(q_k^{i},D_iL_{\mathrm{d}}^{i}\left(q_k^{i-1},q_k^{i}\right)+f_{\mathrm{d}}^{i+}\right),$$
$$\mathbb{F}^{f-}L_{\mathrm{d}}^{i}\colon\ \left(q_k^{i-1},q_k^{i}\right)\mapsto\left(q_k^{i-1},p_k^{i-1}\right)=\left(q_k^{i-1},-D_{i-1}L_{\mathrm{d}}^{i}\left(q_k^{i-1},q_k^{i}\right)-f_{\mathrm{d}}^{i-}\right),$$

so that $\mathbb{F}^{f+}L_{\mathrm{d}}^{i}\left(q_k^{i-1},q_k^{i}\right)=\mathbb{F}^{f-}L_{\mathrm{d}}^{i+1}\left(q_k^{i},q_k^{i+1}\right)$ with $i=1,\dots,s$ as before. Now, it is without any effort that we can derive the forced discrete Euler–Lagrange equations on the cotangent bundle:

$$p_k=-D_0L_{\mathrm{d}}\left(q_k^0,q_k^1,\dots,q_k^s\right)-f_k^0, \tag{12a}$$
$$p_{k+1}=D_sL_{\mathrm{d}}\left(q_k^0,q_k^1,\dots,q_k^s\right)+f_k^s, \tag{12b}$$
$$D_iL_{\mathrm{d}}\left(q_k^0,q_k^1,\dots,q_k^s\right)+f_k^i=0,\qquad i=1,\dots,s-1. \tag{12c}$$

The functions f_k^i can be computed with the Maple procedures described below, so that we can easily generate higher-order variational integrators that include non-conservative forces in a 'variational' manner, that is in a way that respects the fundamental differential geometric properties of any dynamical system.

3. Quadrature Rules

In principle any integration formula can be used to approximate the discrete action, and thus generate a variational integrator, although some cautionary remarks are in order. First, autonomous dynamical systems, which are the ones considered in this article, are time-reversible, so in order to create variational integrators that respect this discrete symmetry, it is necessary to consider quadrature formulas that are 'symmetric', which means that the placement of the (interpolation) nodes must be symmetrical with respect to the midpoint of each time interval. This eliminates the use of open Newton–Cotes and Radau integration formulas, for instance. Second, it is difficult to imagine how quadrature rules based on non-polynomial interpolation should be implemented for generic dynamical systems. Numerical integration based on rational functions (see e.g. [8]) either require the location of the poles in advance, or the integration weights cannot be computed explicitly for generic integrands. In the discrete formalism described so far, the former requires the knowledge of contingent singularities of the (discrete) Lagrangian as functions of time, whereas the latter implies that these quadrature rules would have only limited applicability, if at all. Third, numerical integration methods that involve the derivatives of the integrand with respect to the independent variable, that is Turán (see e.g. [9], pp. 42–43) and Birkhoff quadrature formulas (see e.g. [23], Chapter 10), can be used as well, but they call for the time derivatives of the Lagrangian along the (numerical) solutions; it is essentially possible to compute these using either finite differences or automatic differentiation techniques, although that may be difficult and problem-dependent in practice. Furthermore, quadrature rules with arbitrarily high derivatives lead to derivatives of the resultant force, which are usually considered 'unphysical', and thus discarded as options in numerical integration algorithms.

Here we only consider time-independent Lagrangians. Time-dependent dynamical systems can be analysed similarly in the extended phase space formalism [29]. The fully documented library VarInt for Maple 11 and above can be obtained from the author.

Before going into the specifics of each quadrature formula and the herewith associated MAPLE codes, we wish to mention some notational issues. Because only autonomous dynamical systems are considered, it suffices to define the one-step discrete action on the interval $[0, h]$, where $h > 0$ is the time step. Hence, to make the notation somewhat more manageable in MAPLE, we have removed the 'time step' index $k = 0, \ldots, N$ from all variables, as in actual implementations of these variational algorithms the step index is redundant, in the sense that it is translated to a function that returns the updated values of all variables. However, all variables still carry one index, namely the 'time substep' index $i = 0, \ldots, s$. Henceforth we have written the number of nodes $n = s + 1$.

In order to transform any basic quadrature rule to an approximation of the action functional, it is important to notice that the independent variable is time, and that the coordinates and their derivatives with respect to time are approximated by polynomials of order $(n - 1)$. It is possible to design variational integrators based on non-polynomially fitted quadrature rules with the auxiliary module `CreateVarInt`. An example is given at the end of section 4. Nevertheless, the order of *any* variational integrator is determined entirely by the order of the approximation of the discrete action.

3.1. **Newton–Cotes Quadrature.** The closed Newton–Cotes quadrature formulas approximate definite integrals by approximating the integrand $f : \mathbb{R} \to \mathbb{R}$ with an interpolating polynomial evaluated at the node points $x_k = a + kh$, where $k = 0, \ldots, s$, and the stepsize $h = \frac{b-a}{n-1}$:

$$\begin{aligned}\int_a^b f(x)\,\mathrm{d}x &\approx \int_a^b \{\sum_{k=0}^{s} f(x_k)\,\pi_k(x)\}\,\mathrm{d}x \\ &= \sum_{k=0}^{s} f(x_k) \underbrace{\int_a^b \pi_k(x)\,\mathrm{d}x}_{w_k}.\end{aligned}$$

Here, $\{\pi_k(x)\}$ is a polynomial basis, and w_k are known as the weights; these weights are usually calculated by integration of Lagrange polynomials, although one is in principle free to select any polynomial basis for the interpolation.

3.2. **Romberg Quadrature.** Another family of classical integration formulas with equidistant nodes is the one due to Romberg. Romberg quadrature distinguishes itself from Newton–Cotes quadrature in that it always uses the same basic two-point approximation, the composite trapezium rule, yet recursively by inserting nodes at the centres of all (sub)intervals. The essence of Romberg quadrature is that a Richardson extrapolation procedure is applied to the composite trapezium rule to obtain higher-order approximations to the integral under evaluation.

It is important to note that the composite trapezium rule leads to a continuous approximation of the integrand, yet its derivative with respect to the independent variable is discontinuous at each node. Hence, the naive implementation of Romberg quadrature seems impossible to generate variational integrators, as we require that $q \in \mathcal{C}^1([t_k, t_{k+1}], \mathbb{R})$ for $k = 0, \ldots, N - 1$. Nevertheless, we can still use a 'modified' trapezium rule and Richardson extrapolation in conjunction with a sufficiently smooth interpolating function, at the cost of losing the adaptivity of the algorithm. Again, the composite trapezium rule is used as a basic approximation,

though now the interpolating function is not piecewise linear but rather it is chosen such that both q and $\dot{q}$ are well-defined at each node.

3.3. **Gaussian Quadrature.** A class of n-point quadrature rules that integrate up to $(2n-1)$st-degree polynomials exactly are the Gaussian ones by evaluating a weighted sum of function values. The integrand is assumed to be sufficiently smooth, specifically it is a $\mathcal{C}^{2n}([-1,1],\mathbb{R})$ function.

$$\int_a^b f(x)\,\omega(x)\,\mathrm{d}x = \sum_{k=1}^{n} w_k f(x_k) + R_n, \tag{13}$$

where the 'optimal' values for the weights w_k depend on the placement of the nodes x_k along the interval $[a,b]$. R_n denotes the remainder for a Gaussian integration formula with n nodes,

$$R_n = \frac{f^{(2n)}(\xi)}{(2n)!}\int_a^b \omega(x)\,\phi_n^2(x)\,\mathrm{d}x,$$

where $a<\xi<b$, and $\phi_n(x)$ is the related nth degree orthogonal polynomial (see [28], pp. 180–181). As usual, $\omega(x)$ denotes a positive weight function appearing in the integrand. In the case of interest for variational integrators, the nodes are placed symmetrically over a finite interval, for which $[-1,1]$ is commonly used. For an integral over a arbitrary but finite interval $[a,b]$ the linear transformation $x \mapsto \frac{1}{2}(b-a)\,x + \frac{1}{2}(a+b)$ can then be used. An overview of the various quadrature formulas of the Gauss family can be found in the chapter on numerical analysis in the book by Abramowitz and Stegun [1], for example. Here, we shall discuss the quadrature rules based on the Legendre, Chebyshev and Lobatto nodes. The nodes for the Gauss–Radau quadrature formulas are not distributed symmetrically across the interval of integration, so that they cannot be used for the design of variational integrators for autonomous dynamical systems.

3.3.1. *Gauss–Legendre Quadrature.* In Gauss–Legendre quadrature formulas the weight function $\omega(x)=1$, which is known as the Legendre weight function. The nodes x_k with $k=1,\ldots,n$ for the n-point Gauss–Legendre quadrature formulas are the zeros of the Legendre polynomials $P_n(x)$. The corresponding weights are given by

$$w_k = \frac{2}{1-x_k^2}\frac{1}{\left[P_n'(x_k)\right]^2}, \tag{14}$$

where the prime indicates the derivative with respect to the argument. It is important to note that the zeros of the Legendre polynomials come in pairs, so that the quadrature rule is symmetric about the origin. Furthermore, the zeros lie in the interval $(-1,1)$, that is, they do not include the endpoints.

The fact that the endpoints of the integration interval do not appear explicitly in the quadrature formula means that it is necessary to 'include' the endpoints by means of extrapolation; the values of the coordinates and their derivatives are indeed specified at one such a point for initial-value problems. The idea is to interpolate the coordinates with an $(n-1)$st degree polynomial through the interior points $(i=1,\ldots,s-1)$, as before, and extrapolate to the endpoints of the integration interval ($i=0$ and $i=s$). It is then possible to express the first ($i=1$) and last ($i=s-1$) of the interior points in terms of the remaining interior points and the endpoints. In that way, the endpoints can be included in accordance with the

quadrature nodes. Although polynomial extrapolation is notorious for being very inaccurate outside the interval of the interpolation, we shall assume that the time step h is sufficiently small to overcome the issues associated herewith.

3.3.2. *Gauss–Chebyshev Quadrature.* The n-point Gauss–Chebyshev integration formulas come in two slightly different flavours. The first type of Gauss–Chebyshev quadrature rule has nodes at the roots of the Chebyshev polynomials of the first kind, $T_n(x)$. These are

$$x_k^{(1)} = \cos\theta_k^{(1)}, \qquad \theta_k^{(1)} = \frac{2k-1}{n}\frac{\pi}{2}, \tag{15}$$

and the corresponding weights are

$$w_k^{(1)} = \frac{\pi}{n}. \tag{16}$$

The related quadrature formula reads

$$\int_{-1}^{-1} f(x)\,\mathrm{d}x \approx \sum_{k=1}^{n} w_k^{(1)} f\left(x_k^{(1)}\right)\sqrt{1-\left(x_k^{(1)}\right)^2}, \tag{17}$$

where the square-root is the weight function, now appearing on the right-hand side. Similarly, the integration formula for second type of Gauss–Chebyshev integration formulas is

$$\int_{-1}^{-1} f(x)\,\mathrm{d}x \approx \sum_{k=1}^{n} w_k^{(2)} \frac{f\left(x_k^{(2)}\right)}{\sqrt{1-\left(x_k^{(2)}\right)^2}}, \tag{18}$$

where now the nodes are given by

$$x_k^{(2)} = \cos\theta_k^{(2)}, \qquad \theta_k^{(2)} = \frac{k}{n+1}\pi, \tag{19}$$

which are the zero loci of the Chebyshev polynomials of the second kind, $U_n(x)$. The matching weights are

$$w_k^{(2)} = \frac{\pi}{n+1}\sin^2\theta_k^{(2)}. \tag{20}$$

The Gauss–Chebyshev quadrature formulas are especially suited for integrands with factors of $\sqrt{1-x^2}$ either in their numerators or denominators.

Please observe that the extrapolation to the endpoints of the integration interval does not yield any singularities due to the weight function. The coordinates and velocities are extrapolated and these extrapolations are substituted, so that the sum is indeed evaluated at the correct nodes.

3.3.3. *Fejér Quadrature.* The Gauss–Chebyshev quadratures discussed in the previous paragraph were defined with respect to non-trivial weight functions $\omega(x) = 1/\sqrt{1-x^2}$ and $\omega(x) = \sqrt{1-x^2}$ for the integration formulas based on the Chebyshev polynomials of the first and second kind, respectively. As for all Gauss quadratures rules, these can be defined relative to different weight functions. For $\omega(x) = 1$ one obtains the formulas due to Fejér [7]. The nodes for the integration rules based

on the Chebyshev polynomials of the first and second kind are identical to equations (15) and (19), respectively. However, the weights are now

$$w_k^{(1)} = \frac{2}{n}\left[1 - 2\sum_{j=1}^{\lfloor n/2\rfloor} \frac{\cos\left(2j\theta_k^{(1)}\right)}{4j^2-1}\right], \tag{21}$$

and

$$w_k^{(2)} = \frac{4\sin\theta_k^{(2)}}{n+1} \sum_{j=1}^{\lfloor (n+1)/2\rfloor} \frac{\sin\left((2j-1)\,\theta_k^{(2)}\right)}{2j-1}, \tag{22}$$

where $\theta_k^{(1)}$ and $\theta_k^{(2)}$ are as before.

Alternatively, the zeros of the nth-degree Chebyshev polynomial of the third kind $V_n(x)$ can be used,

$$x_k^{(3)} = \cos\theta_k^{(3)}, \qquad \theta_k^{(3)} = \frac{2k-1}{2n+1}\pi, \tag{23}$$

as well as those of the nth-degree Chebyshev polynomial of the fourth kind $W_n(x)$,

$$x_k^{(4)} = \cos\theta_k^{(4)}, \qquad \theta_k^{(4)} = \frac{2k}{2n+1}\pi. \tag{24}$$

The corresponding weights are

$$w_k^{(3)} = \frac{4\sin\theta_k^{(3)}}{n+\frac{1}{2}} \sum_{j=1}^{\lfloor (n+1)/2\rfloor} \frac{\sin\left((2j-1)\,\theta_k^{(3)}\right)}{2j-1}, \tag{25}$$

and

$$w_k^{(4)} = \frac{4\sin\theta_k^{(4)}}{n+\frac{1}{2}} \sum_{j=1}^{\lfloor (n+1)/2\rfloor} \frac{\sin\left((2j-1)\,\theta_k^{(4)}\right)}{2j-1}, \tag{26}$$

respectively, as shown by [26].

Related to Fejér quadrature formulas is the one by [5], which is nothing but Fejér's second rule with the nodes -1 and 1 added. Define

$$\theta_k = \frac{k-1}{n-1}\pi, \qquad k = 1,\ldots,n.$$

The Clenshaw–Curtis nodes are then simply $x_k = \cos\theta_k$, and the associated weights are given by

$$w_k = \frac{c_k}{n}\left[1 - 2\sum_{j=1}^{\lfloor (n+1)/2\rfloor}{}^{*} \frac{\cos 2j\theta_k}{4j^2-1}\right], \tag{27}$$

where $c_k = 2 - \delta_{0,k \bmod n}$, and $\sum{}^{*}$ signifies that the last term in the sum should be halved.

3.3.4. *Gauss–Lobatto Quadrature.* Additional Gaussian integration rules that include both endpoints are the Gauss–Lobatto ones:

$$\int_{-1}^{-1} f(x)\,\mathrm{d}x \approx \frac{2}{n(n-1)}\left[f(-1)+f(1)\right]+\sum_{k=2}^{n-1} w_k f(x_k). \tag{28}$$

The interior nodes are the zeros of the derivative of the Legendre polynomials, that is they satisfy $P'_{n-1}(x)=0$, and the interior weights can be calculated to be

$$w_k = \frac{2}{n(n-1)}\frac{1}{\left[P_{n-1}(x_k)\right]^2}. \tag{29}$$

3.4. **Chebyshev Quadrature.** Somewhat related to the quadrature formulas of the Gaussian type is the equal-weight integration formula by Chebyshev:

$$\int_{-1}^{-1} f(x)\,\mathrm{d}x \approx \frac{2}{n}\sum_{k=1}^{n} f(x_k). \tag{30}$$

The nodes are the solutions to the equation $G_n(x)=0$, where $G_n(x)$ is the polynomial part of [14]

$$F_n(x) = x^n \exp\left[\frac{n}{2}\int_{-1}^{1}\ln\left(1-\frac{t}{x}\right)\mathrm{d}t\right]. \tag{31}$$

The integral inside the exponential can be calculated easily,

$$\int_{-1}^{1}\ln\left(1-\frac{t}{x}\right)\mathrm{d}t = -2+(1+x)\ln\left(1+\frac{1}{x}\right)+(1-x)\ln\left(1-\frac{1}{x}\right).$$

The zeros of $G_n(x)$ are known to be real only for $n\le 7$ and $n=9$. Hence, the use of Chebyshev quadrature is restricted to these values.

3.5. **Takahasi–Mori Quadrature.** For the numerical computation of integrals over infinite intervals $(-\infty,\infty)$ the composite trapezium rule is noted for its excellent results in terms of accuracy and efficiency compared to quadrature formulas with the same density of sampling points [30], that is, for any analytical function g that vanishes at infinity,

$$\int_{-\infty}^{\infty} g(x)\,\mathrm{d}x \approx \eta\sum_{k=-\infty}^{\infty} g(k\eta),$$

where in practice the infinite sum itself converges often quite rapidly. We can take advantage of the performance of the trapezium rule by applying a variable transformation, $x\mapsto\varphi(t)$, to integrals over finite intervals:

$$\begin{aligned}\int_{-1}^{1} f(x)\,\mathrm{d}x &= \int_{-\infty}^{\infty} f(\varphi(t))\,\varphi'(t)\,\mathrm{d}t\\ &\approx \eta\sum_{k=-\infty}^{\infty} f(k\eta)\,\varphi'(k\eta).\end{aligned}$$

The method proposed by Schwartz [27] involves the transformation $\varphi(t)=\tanh t$, for which the resulting quadrature formula has an asymptotic error of $\mathcal{O}\left(\exp\left(-c\sqrt{N}\right)\right)$ with $\eta=\pi/\sqrt{N}$ [12], where N denotes the number of function evaluations, and $c\in\mathbb{R}$ depends on the integrand and the particular variable

transformation. For $\varphi(t) = \operatorname{erf} t$ the error is $\mathcal{O}\left(\exp\left(-c\sqrt[3]{N^2}\right)\right)$ asymptotically (see e.g. [25] for more details on these and other variable transformations). In fact, for all functions $f \in H^p(D)$, $1 < p \leq \infty$, the Hardy spaces on the unit disc $D = \{z \in \mathbb{C} \mid |z| < 1\}$, Andersson [2] has shown that the bound on the asymptotic error of any quadrature formula is $\mathcal{O}\left(N^{1-1/(2p)} \exp\left(-c\sqrt{N}\right)\right)$.

Double exponential quadrature formula dates back to the work by Takahasi and Mori [31], who improved on the transformation method by Schwartz [27]. Their integration rule accelerates the convergence of one-dimensional integrals by introducing a suitable variable transformation that result in double exponential decay of the integrand: $\varphi(t) = \tanh\left(\frac{\pi}{2}\sinh t\right)$. Rather than looking at functions that belong to the Hardy classes $H^p(D)$ with $p > 1$, we can focus on the more modest class of integrable functions over $(-1, 1)$, possibly with algebraic or logarithmic singularities at the endpoints ± 1, and a finite number of singularities outside the interval of integration. Then, the asymptotic error of the quadrature formula behaves as $\mathcal{O}(\exp(-cN/\ln N))$; the constant c is related to the location of the singularities of the integrand after the application of the variable transformation. The optimal value of

$$\eta = \frac{2}{N} \ln 2\Delta N,$$

where Δ is the distance between the real axis and the nearest singularity of the integrand after the variable transformation has been applied; the transformed integrand is thus regular in the strip $|\Im(z)| < \Delta$. In case the original function $f(z)$, $z \in \mathbb{C}$, only has a singularity at $z = \infty$, we easily compute that $\Delta = \frac{\pi}{2}$. At the optimal step η, the nodes in the interval $(-1, 1)$ tend to cluster near the boundaries, especially for small N.

The Takahasi–Mori, or tanh-sinh, formula,

$$\int_{-1}^{1} f(x)\,\mathrm{d}x \approx \eta \frac{\pi}{2} \sum_{k=-n}^{n} f\left(\tanh\left(\frac{\pi}{2}\sinh k\eta\right)\right) \frac{\cosh k\eta}{\cosh^2\left(\frac{\pi}{2}\sinh k\eta\right)}, \tag{32}$$

has been shown to be fast and accurate in high-precision experimental mathematics [3]; in practice we often choose η adaptively. Recently, Borwein and Ye [4] have shown that the Takahasi–Mori quadrature formula converges quadratically for all integrands $f \in H^2(D)$ in the limit of $N \to \infty$.

All these transformed quadrature formulas based on the trapezium rule have exponential decay of the asymptotic error, which basically means that halving the stepsize roughly doubles the number of correct digits. Note, however, that the quadrature formulas are not exact for polynomials, in contrast to the Gaussian quadrature formulas.

4. Examples

The symplectic partitioned Runge–Kutta methods form a well-known class of variational integrators for conservative dynamical systems. For non-conservative systems probably the best studied example is the symplectic Newmark algorithm, as described in [18]. Beyond these the number of variational integrators is limited, mainly because the manual effort to generate these (higher-order) variational integrators is substantial.

VarInt is a library that enables anyone with a Maple distribution to create and analyse new variational integrators with ease. The module VarInt has four main

procedures: `VarInt`, `CreateVarInt`, `ExtractAlgorithm`, and `IntegrateSystem`, which provides basic functionality for the numerical analysis of one-dimensional problems. `VarInt` computes the (forced) discrete Euler–Lagrange equations. In order to obtain an actual recipe that allows us to compute the discrete flow efficiently, we have to manipulate the expressions returned by `VarInt`, which depends highly on the functional form of the Lagrangian, and is hence best done interactively. For separable Lagrangians

$$L(q,\dot{q}) = T(\dot{q}) - V(q), \tag{33}$$

with $T\colon \mathbf{T}\mathbb{Q} \to \mathbb{R}$ a quadratic kinetic energy function and $V\colon \mathbb{Q} \to \mathbb{R}$ the potential energy, an ancillary procedure `ExtractAlgorithm` is included in VarInt. It aids in the extraction of such a one-step map, even for dynamical systems with generic non-conservative forces. As such, it greatly enhances the potential development variational integrators for non-conservative forces up to arbitrary order, which has only been touched upon scantily thus far.

The module `CreateVarInt` is similar in design as `VarInt` with the significant difference that the approximation to the discrete action can be supplied manually by specifying the nodes, weights and weight function of the numerical integration formula, and the interpolation procedure, which is polynomial by default. `CreateVarInt` therefore extends the `VarInt` by allowing new quadrature rules to be defined and the creation of non-polynomially fitted variational integration algorithms.

To see the full scope of VarInt, we shall first look at simple problems. Consider a two-point Newton–Cotes approximation of the action and the (non-conservative) Rayleigh force. Then, we can obtain the discrete Euler–Lagrange equations with `VarInt` as follows:

```
> restart;                                    #clear memory
> with(VarInt):                               #load VarInt
> dEL1:=VarInt(2,L,F,NewtonCotes,p,q,h);      #obtain dEL equations.
```

Since, we have not (yet) specified the functional forms of the Lagrangian and the Rayleigh force, we the expressions MAPLE returns are fully implicit. To obtain a more applicable representation of the two-point variational Newton–Cotes integrator, we define a separable Lagrangian (33), and extract the algorithm:

```
> L:=(q,Dq)->1/2*M*Dq^2-V(q):                 #define Lagrangian
> dEL2:=VarInt(2,L,F,NewtonCotes,p,q,h):      #obtain dEL equations
> ExtractAlgorithm(dEL2,p,q,V,F);             #obtain algorithm.
```

Here, M is the mass; in the case of vectorial coordinates and momenta, `M` has to be interpreted as the mass matrix. The one-step map $(q_0,p_0) \mapsto (q_1,p_1)$ reads

$$q_1 = q_0 + h\frac{p_0}{M} - \frac{h^2}{2M}\left[\nabla V(q_0) - F\left(q_0, \frac{q_1-q_0}{h}\right)\right], \tag{34a}$$

$$p_1 = p_0 - \frac{h}{2}\left[\nabla V(q_0) + \nabla V(q_1) - F\left(q_0, \frac{q_1-q_0}{h}\right) - F\left(q_1, \frac{q_1-q_0}{h}\right)\right], \tag{34b}$$

The algorithm is implicit for generic `F`. For conservative dynamical systems the algorithm reduces to the the famous second-order Störmer–Verlet algorithm, which

is sometimes referred to as the leapfrog:

$$q_1 = q_0 + h\frac{p_0}{M} - \frac{h^2}{2M}\nabla V\left(q_0\right), \tag{35a}$$

$$p_1 = p_0 - \frac{h}{2}\left[\nabla V\left(q_0\right) + \nabla V\left(q_1\right)\right], \tag{35b}$$

and is fully explicit. It can be obtained in the active MAPLE worksheet in several ways:

```
> eval(%,F=0);                                  #alternative 1
> F:=(q,Dq)->0:                                 #alternative 2
> dEL3:=VarInt(2,L,F,NewtonCotes,p,q,h);        #alternative 2 (cont'd)
> ExtractAlgorithm(dEL3,p,q,V,F);               #alternative 2 (cont'd)
> dEL4:=VarInt(2,L,0,NewtonCotes,p,q,h);        #alternative 3
> ExtractAlgorithm(dEL3,p,q,V,F);               #alternative 3 (cont'd).
```

As it happens, the Newton–Cotes, Romberg, Gauss–Lobatto and Clenshaw–Curtis quadrature rules with two nodes are identical, so that their variational integrators are the same.

Incidentally, for three nodes the Newton–Cotes, Gauss–Lobatto and Clenshaw–Curtis quadrature (Simpson's) formulas coincide. The MAPLE code

```
> dEL5:=VarInt(3,L,0,GaussLobatto,p,q,h);       #obtain dEL equations
> ExtractAlgorithm(dEL5,p,q,V,F);               #obtain algorithm
```

results in the fourth-order algorithm for conservative dynamical systems reported in [6],

$$q_1 = q_0 + \frac{h}{2}\frac{p_0}{M} - \frac{h^2}{24M}\left[2\nabla V\left(q_0\right) + \nabla V\left(q_1\right)\right], \tag{36a}$$

$$q_2 = q_0 + h\frac{p_0}{M} - \frac{h^2}{6M}\left[\nabla V\left(q_0\right) + 2\nabla V\left(q_1\right)\right], \tag{36b}$$

$$p_2 = p_0 - \frac{h}{6}\left[\nabla V\left(q_0\right) + 4\nabla V\left(q_1\right) + \nabla V\left(q_2\right)\right]. \tag{36c}$$

Equation (36a) has to be solved iteratively for generic (non-linear) potentials. Equations (36b)–(36c) are clearly explicit.

For four nodes these three families of quadrature rules lead to different variational integrators. The variational Newton–Cotes integrator, which is based on Simpson's $\frac{3}{8}$ rule, is easily found to be

$$q_1 = q_0 + \frac{h}{3}\frac{p_0}{M} - \frac{h^2}{648M}\left[27\nabla V\left(q_0\right) + 14\nabla V\left(q_1\right) - 5\nabla V\left(q_2\right)\right], \tag{37a}$$

$$q_2 = q_0 + \frac{2h}{3}\frac{p_0}{M} - \frac{h^2}{324M}\left[27\nabla V\left(q_0\right) + 38\nabla V\left(q_1\right) + 7\nabla V\left(q_2\right)\right], \tag{37b}$$

$$q_3 = q_0 + h\frac{p_0}{M} - \frac{h^2}{8M}\left[\nabla V\left(q_0\right) + 2\nabla V\left(q_1\right) + \nabla V\left(q_2\right)\right], \tag{37c}$$

$$p_3 = p_0 - \frac{h}{8}\left[\nabla V\left(q_0\right) + 3\nabla V\left(q_1\right) + 3\nabla V\left(q_2\right) + \nabla V\left(q_3\right)\right]. \tag{37d}$$

Similarly, the variational Clenshaw–Curtis integrator with four nodes is

$$q_1 = q_0 + \frac{3h}{14}\frac{p_0}{M} - \frac{h^2}{13440M}\left[320\nabla V(q_0) + 259\nabla V(q_1) - 21\nabla V(q_2)\right], \tag{38a}$$

$$q_2 = q_0 + \frac{6h}{7}\frac{p_0}{M} - \frac{h^2}{13440M}\left[1280\nabla V(q_0) + 3339\nabla V(q_1) + 259\nabla V(q_2)\right], \tag{38b}$$

$$q_3 = q_0 + \frac{15h}{14}\frac{p_0}{M} - \frac{h^2}{84M}\left[10\nabla V(q_0) + 28\nabla V(q_1) + 7\nabla V(q_2)\right], \tag{38c}$$

$$p_3 = p_0 - \frac{h}{18}\left[2\nabla V(q_0) + 7\nabla V(q_1) + 7\nabla V(q_2) + 2\nabla V(q_3)\right]. \tag{38d}$$

The variational integrators that derive from the Gauss–Lobatto quadrature rules correspond to the well-known Lobatto IIIA/IIIB algorithms, and their forms can be found in the literature.

All variational Gauss–Legendre integrators have been shown to be equal to the Gauss collocation methods. As an example, the Gauss–Legendre variational integrator with two nodes is easily found to be

$$q_1 = q_0 + h\frac{p_0}{m} - \frac{h^2}{12m}\left[c_-\nabla V\left(q_+\right) + c_+\nabla V\left(q_-\right)\right], \tag{39}$$

$$p_1 = p_0 - \frac{h}{2}\left[\nabla V\left(q_+\right) + \nabla V\left(q_-\right)\right], \tag{40}$$

where we have defined $q_\pm = \frac{1}{2}\left(q_0 + q_1\right) \pm \frac{1}{6}\sqrt{3}\left(q_0 - q_1\right)$, and $c_\pm = 3 \pm \sqrt{3}$. The Gauss–Legendre and the Chebyshev quadrature formulas with two nodes happen to coincide, so that their variational integrators are identical (39). More details and examples can be found in the help pages, which can be accessed by executing one of the following commands:

```
> ?VarInt                                  #package overview
> ?VarInt[VarInt]                          #help page
> ?VarInt[ExtractAlgorithm]                #help page
> ?VarInt[CreateVarInt]                    #help page
> ?VarInt[IntegrateSystem]                 #help page.
```

Finally, we shall take a look at the `CreateVarInt` module. The syntax is slightly different from `VarInt`, as one can see below:

```
> Digits:=16:                              #numerical precision
> x:=0.5904158239150231:                   #positive node
> w:=0.9964248649058515:                   #weight
> etc:=1,L,0,p,q,h:                        #shorthand
> CreateVarInt(-1..1,[-x,x],[w,w],etc):    #obtain dEL
> ExtractAlgorithm(%,p,q,V);               #obtain algorithm
```

The first argument is the range on which the nodes are defined, so that the nodes, supplied as a list as the second argument to `CreateVarInt`, can be transformed appropriately. The third argument is the list of weights associated with these nodes. The fourth argument is the weight function, which in this case is the unit function. The fifth through to the ninth argument are the Lagrangian function, the Rayleigh function, and the labels for the canonical momenta, canonical coordinates

and the time step, respectively. The tenth argument is optional, and it is not shown here; it takes the handle of an interpolation procedure, which must have the same syntax as the built-in procedures for data interpolation, as specified in the documentation of the `CurveFitting` package. If the tenth argument is omitted, the standard polynomial interpolation procedure `PolynomialInterpolation` (also known as `interp`) is used internally. As an example, consider a custom yet naive implementation of polynomial interpolation:

```
> Poly:=proc(xdata,ydata,z)                    #custom interpolation
    local c,n,Eqs,Var,Fun;
    n:=nops(xdata):
    Fun:=x->add(c[k]*x^(k-1),k=1..n):
    Eqs:={seq(Fun(xdata[m])=ydata[m],m=1..n)}:
    Var:={seq(c[m],m=1..n)}:
    assign(solve(Eqs,Var)):
    collect(factor(Fun(z)),z);
  end proc:
> etc:=1,L,0,p,q,h,Poly;                        #shorthand
> CreateVarInt(-1..1,[-1,1],[1,1],etc):         #obtain dEL
> ExtractAlgorithm(%,p,q,V);                    #obtain algorithm.
```

The code obviously yields the Störmer–Verlet algorithm (35).

The values for the nodes and weights shown are such that the underlying quadrature rule integrates any linear combinations of the set $\{e^{\pm\nu x}, x\,e^{\pm\nu x}\}$ with $\nu = 1$ exactly on the interval $[-1, 1]$. Recently, non-polynomially fitted quadrature rules have moved increasingly to the centre of attention [16, 35, 33], especially exponentially fitted ones for numerical integration algorithms for ordinary differential equations (see [34] and references therein for more details). The idea behind is to translate the philosophy behind Gaussian integration formulas, that is that they integrate polynomials exactly, to non-polynomial functions, in particular exponentials and trigonometric functions, based on the formalism developed by Ixaru [15]. That leads to a set non-linear conditions, from which the nodes and weights can be computed (numerically). Unfortunately, the nodes and corresponding weights for these exponentially fitted quadrature rules are not determined uniquely.

The optional argument enables us to provide alternative interpolation routines, which can be practical both as a diagnostic tool and as a interface to create new variational integrators that are designed for specific dynamical systems. Quadrature rules based on rational interpolation [32], for instance, might be of use in the simulations of dynamical systems with singularities, such as N-body problems in astrophysics and molecular dynamics for instance.

5. Conclusion

It is a well-established fact that simulations of (non-linear) dynamical systems, both with non-conservative forces and without, benefit greatly from the preservation of their geometric structures, especially over long time spans as compared to the characteristic time scales of the systems at hand. Variational integrators, and more generally geometric numerical integrators, are ideally suited for such simulations. The discrete variational formalism is both mathematically natural and

computationally practical. We have demonstrated that one can explore and design variational integrators systematically with a computer algebra system, such as MAPLE. Some of these variational integrators correspond to well-known classes of geometric numerical algorithms, such as the symplectic partitioned Runge–Kutta methods. However, few variational integrators have been reported that lie outside of the standard classification, although the discrete variational formalism is certainly not restricted to it. With the procedures we have presented to compute variational integrators based on different approximations of the action functional one can venture beyond the geometric numerical algorithms one usually encounters. The discrete flow maps one obtains can be either general, and serve as templates for generic problems, or optimized for a specific problem thanks to the symbolic capabilities of a computer algebra system.

REFERENCES

1. M. Abramowitz and I.A. Stegun (eds.), *Handbook of Mathematical Functions*, Dover Publications, Mineola, NY, 1972.
2. J.E. Andersson, *Optimal Quadrature of H^p Functions*, Mathematische Zeitschrift **172** (1980), 55–62.
3. D.H. Bailey, K. Jeyabalan, and X.S. Li, *A Comparison of Three High-Precision Quadrature Schemes*, Experimental Mathematics **14** (2005), no. 3, 317–329.
4. J.M. Borwein and L. Ye, *Quadratic Convergence of the* tanh-sinh *Quadrature Rule*, D-Drive Preprint #342, 2006.
5. C.W. Clenshaw and A.R. Curtis, *A Method for Numerical Integration on an Automatic Computer*, Numerische Mathematik **2** (1960), 197–205.
6. W.M. Farr and E. Bertschinger, *Variational Integrators for the Gravitational N-Body Problem*, The Astrophysical Journal **663** (2007), no. 2, 1420–1433.
7. L. Fejér, *Mechanische Quadraturen mit positiven Cotesschen Zahlen*, Mathematische Zeitschrift **37** (1933), 287–309.
8. W. Gautschi, *The Use of Rational Functions in Numerical Quadrature*, Journal of Computational and Applied Mathematics **133** (2001), no. 1-2, 111–126.
9. ———, *Orthogonal Polynomials and Special Functions. Computation and Applications*, Lecture Notes in Mathematics, vol. 1883, Springer, Berlin, Heidelberg, 2006.
10. Z. Ge and J.E. Marsden, *Lie–Poisson Hamilton–Jacobi Theory and Lie–Poisson Integrators*, Physics Letters A **133** (1988), no. 3, 134–139.
11. A. Griewank and A. Walther, *Evaluating Derivatives. Principles and Techniques of Algorithmic Differentiation*, Applied Mathematics, vol. 105, Society for Industrial and Applied Mathematics, Philadelphia, PA, 2008.
12. S. Haber, *The* tanh *Rule for Numerical Integration*, SIAM Journal on Numerical Analysis **14** (1977), no. 4, 668–685.
13. E. Hairer, C. Lubich, and G. Wanner, *Geometric Numerical Integration. Structure-Preserving Algorithms for Ordinary Differential Equations*, Springer Series in Computational Mathematics, vol. 31, Springer, Berlin, Heidelberg, New York, 2006.
14. F.B. Hildebrand, *Introduction to Numerical Analysis*, Dover Publications, Mineola, NY, 1987.
15. L.G. Ixaru, *Operations on Oscillatory Functions*, Computer Physics Communications **105** (1997), no. 1, 1–19.
16. L.G. Ixaru and B. Paternoster, *A Gauss Quadrature Rule for Oscillatory Integrands*, Computer Physics Communications **133** (2001), no. 2-3, 177–188.
17. O. Junge, J.E. Marsden, and S. Ober Blöbaum, *Discrete Mechanics and Optimal Control*, Proceedings of the 16th IFAC Conference on Decision and Control, 2005.
18. C. Kane, J.E. Marsden, M. Ortiz, and M. West, *Variational Integrators and the Newmark Algorithm for Conservative and Dissipative Mechanical Systems*, International Journal for Numerical Methods in Engineering **49** (2000), no. 10, 1295–1325.
19. L. Kharevych, Y. Weiwei, Y. Tong, E. Kanso, J.E. Marsden, P. Schröder, and M. Desbrun, *Geometric, Variational Integrators for Computer Animation*, Proceedings of the 2006 ACM

SIGGRAPH/Eurographics Symposium on Computer Animation (Aire-la-Ville, Switzerland), Eurographics Association, 2006, pp. 43–51.
20. B. Leimkuhler and S. Reich, *Simulating Hamiltonian Dynamics*, Cambridge Monographs on Applied and Computational Mathematics, vol. 14, Cambridge University Press, Cambridge, UK, 2005.
21. A. Lew, J.E. Marsden, M. Ortiz, and M. West, *Asynchronous Variational Integrators*, Archive for Rational Mechanics and Analysis **167** (2003), no. 2, 85–146.
22. ———, *Variational Time Integrators*, International Journal for Numerical Methods in Engineering **60** (2004), no. 1, 153–212.
23. G.G. Lorentz, K. Jetter, and S.D. Riemenschneider, *Birkhoff Interpolation*, Encyclopedia of Mathematics and Its Applications, vol. 19, Cambridge University Press, Cambridge, UK, 1984.
24. J.E. Marsden and M. West, *Discrete Mechanics and Variational Integrators*, Acta Numerica **10** (2001), 357–514.
25. M. Mori, *Quadrature Formulas Obtained by Variable Transformation and the DE-Rule*, Journal of Computational and Applied Mathematics **12-13** (1985), 119–130.
26. S.E. Notaris, *Interpolatory Quadrature Formulae with Chebyshev Abscissae of the Third or Fourth Kind*, Journal of Computational and Applied Mathematics **81** (1997), no. 1, 83–99.
27. C. Schwartz, *Numerical Integration of Analytic Functions*, Journal of Computational Physics **4** (1969), no. 1, 19–29.
28. J. Stoer and R. Bulirsch, *Introduction to Numerical Analysis*, Texts in Applied Mathematics, vol. 12, Springer, New York, NY, 2002.
29. J. Struckmeier, *Hamiltonian Dynamics on the Symplectic Extended Phase Space for Autonomous and Non-Autonomous Systems*, Journal of Physics A: Mathematical and General **38** (2005), no. 6, 1257–1278.
30. H. Takahasi and M. Mori, *Error Estimation in the Numerical Integration of Analytic Functions*, Report of the Computer Centre, University of Tokyo **3** (1970), 41–108.
31. ———, *Double Exponential Formulas for Numerical Integration*, Publications of the Research Institute for Mathematical Sciences **9** (1974), no. 3, 721–741.
32. W. Van Assche and I. Vanherwegen, *Quadrature Formulas Based on Rational Interpolation*, Mathematics of Computation **61** (1993), no. 204, 765–783.
33. G. Vanden Berghe and M. Van Daele, *Trigonometric Polynomial or Exponential Fitting Approach?*, Journal of Computational and Applied Mathematics **233** (2009), no. 4, 969–979.
34. ———, *Symplectic Exponentially-Fitted Four-Stage Runge–Kutta Methods of the Gauss Type*, Numerical Algorithms (2010), in press.
35. G. Vanden Berghe, M. Van Daele, and H. Vande Vyver, *Exponentially Fitted Quadrature Rules of The Gauss Type for Oscillatory Integrands*, Applied Numerical Mathematics **53** (2005), no. 2-4, 509–526.

Department of Physics and Astronomy, University of Turku, Finland
E-mail address: christian.hellstrom@utu.fi

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 123–133
ISSN 1930-1235: (2010)

VERIFICATION METHODS AND SYMBOLIC COMPUTATIONS

WALTER KRÄMER

Abstract. Our intpakX package extends the computer algebra system Maple. It allows, e.g., verified numerical calculations (computer-assisted proofs) built on arbitrary precision interval operations. Up to now, only the basic operations are supported in a guaranteed way. Concerning higher mathematical functions supported in Maple, there are no data about their accuracies available/published. Thus, it is not possible or at least very hard to build arbitrary precision interval functions using Maple's intrinsic mathematical functions (nevertheless, intpakX offers such function implementations using some guard digits in an experimental way, which - of course - is not really a reliable mathematical approach).

On the other hand there are software packages supporting reliable multiple precision interval functions like C-XSC, the MPFR and the MPFI libraries, and others. In the talk we discuss the features of some of these libraries in detail. We emphasize the different approaches (arbitrary precision arithmetic, staggered correction arithmetic, functions only for real arguments, functions for complex arguments, ...) and the most important resulting properties of the corresponding implementations. We also compare their performance and we comment on the actual integration of several of these libraries in C-XSC. The missing step is to bring together C-XSC and computer algebra packages like Maple and Mathematica. Combining fast verification methods and symbolic computations deeply extends the range of applications of rigorous mathematical methods.

Key words: Computer-assisted proofs, self-verifying methods, arbitrary precision, interval functions, intpakX, C-XSC.

1. Introduction and general remarks on computer-assisted proofs

It is well known that symbolic computations often suffer from exponential growth of formula strings (memory) and computing time consumption [9]. In many cases it is of great advantage to be able to circumvent this behaviour by applying self-validating numerical methods. The result of such methods are proved to be rigorous in the mathematical sense. These methods are based on the validity of mathematical theorems. Using e.g. interval computations, sufficient conditions for the validity of the mathematical theorems may be verified by the computer itself.

Let us give an example. Brouwer's fixed point theorem may be stated as follows: if a nonempty, convex, compact set X in $\mathbb{R}^n$ is mapped by a continuous function $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ into itself, this function has at least one fixed point $x^\star \in X$.

Typically, machine intervals are boxes in $\mathbb{R}^n$ with sides parallel to the axes [2, 12, 4, 8]. Such boxes are easily representable (e.g. using an infimum-supremum representation) and they are by their definition convex and compact. Now let F be

kraemer@math.uni-wuppertal.de.

an interval enclosure for the function f representable on the computer (e.g. replace all real operations and elementary function calls by the corresponding machine interval operations/functions). Such an enclosure allows the machine computation of sets containing the range of f over set-valued arguments, typically over machine intervals. Let X be a box (a convex and compact machine interval vector) and let $F(X)$, the result of the machine interval computation, be a subset of X. Then it holds $f(x)|x \in X \subseteq F(X) \subseteq X$. That means, we have proved by some interval machine computations that the continuos function f maps the (convex and compact) interval vector X into itself. The result of the computation assures that Brouwer's fixed point theorem is applicable in the concrete situation and it follows that there exists at least one fixed point x^* of f in X. We see, $F(X) \subseteq X$ can be verified by machine computations and the validity of this relation is sufficient for $\{f(x)|x \in X\} \subseteq X$. Possible conversion errors and rounding errors are captured by machine interval operations (worst case outward rounding). Possible overestimations due e.g. to some kind of wrapping effects or data dependencies do not invalidate the final result (of course, overestimations should be avoided as far as possible to allow $F(X) \subseteq X$ (if the overestimation in the computation of $F(X)$ is too large, this relation does not hold).

2. Newton method to find the zero of a function

Let us consider the simplest case of Newton's method to compute a zero of a continuosly differentiable function g in one real variable. To find the nth root $\sqrt[n]{a}$ of $a \in \mathbb{R}_+$ we proceed as follows:

Let

$$g(x) := x^n - a \tag{1}$$

with $g'(x) = nx^{n-1}$. Defining

$$N(x) = x - \frac{g(x)}{g'(x)}\,, \tag{2}$$

the classical Newton iteration computes the iterates

$$x_{k+1} = N(x_k),\ k = 0, 1, 2, \ldots \tag{3}$$

starting from a given initial value x_0.

2.1. **Symbolic computations and rational arithmetic.** We start the Newton iteration (3) for the function (1) with fixed values $n = 5$, $a = 32$ and with the rational starting value $x_0 = 1$ Then, obviously, all iterates x_k are rational numbers, i.e. they can be computed error-free using Maple's [11] rational arithmetic. In our case even the answer, i.e. the zero $\sqrt[n]{a}$ of g, is a rational number. What follows is the actual Maple code:

```
> restart;
  g := proc (x) options operator, arrow; x^5-32 end proc;
  dg := unapply(diff(g(x), x), x);

                          5
                     x -> x  - 32

                            4
```

```
x -> 5 x

> N := proc (x) options operator, arrow; x - g(x)/dg(x) end proc;

         g(x)
x -> x - -----
         dg(x)

> N := unapply(simplify(N(x)), x);

       / 5    \
     4 \x  + 8/
x -> ----------
           4
        5 x

> xk := 1;
  printf("x0: "); print(xk, 1.0*xk);
  printf("%c", "\n");
  for k to 8 do
    xk := N(xk);
    nodd := ceil(log10(op(1, xk)))+ceil(log10(op(2, xk)));
    printf("Number of decimal digits to represent x%d: %d  %c", k, nodd, "\n");
    if nodd < 100 then print(xk, 1.0*xk) else print(1.0*xk) end if
  end do;

x0:
                                  1, 1.0

Number of decimal digits to represent x1: 3
                                36
                                --, 7.200000000
                                5
Number of decimal digits to represent x2: 14
                               7561397
                               -------, 5.762381497
                               1312200

Number of decimal digits to represent x3: 69
              247489457843878885578773901331667 57
              ------------------------------------, 4.615709793
              536189381397022743293942086706025 0

Number of decimal digits to represent x4: 345
                                  3.706668058

Number of decimal digits to represent x5: 1722
                                  2.999237997
```

```
Number of decimal digits to represent x6: 8607
                                  2.478483071

Number of decimal digits to represent x7: 43032
                                  2.152390479

Number of decimal digits to represent x8: 215154
                                  2.020104202
```

To represent x_8 exactly as a rational number, already 215154 figures are necessary. However, as an approximation to the value $\sqrt[5]{32} = 2$, $x_8 = 2.0201\ldots$ is only accurate to two decimals! The length of the numerator expands by a factor of about 5 at each Newton step. Due to computing time and memory restrictions, the method is obviously not appropriate to compute more than the first few iterates.

2.2. **Interval Newton method using (arbitary precision) interval operations.** To compute the nth root of the value $a \in \mathbb{R}_+$ using an interval Newton method [4] we first introduce the so called Interval-Newton-operator

$$N(X) = N(X, y) := y - G(y)/G'(X)\ .$$

Here X denotes a closed real interval and y any point in X, e.g. the midpoint of X. If there is a root of g in X then this root is also contained in $N(X, y)$ (if $N(X, y)$ is computable at all). This may be shown by the Mean-Value theorem. The Interval-Newton-operator does not lose a zero of g contained in X. The capital letters G and G' emphasize that we need interval enclosures [4] of the corresponding real valued functions g and g', respectively. We start the interval iteration with starting interval $X_0 := [1/a, a]$ (this interval, and thus all iterates X_k, contain the nth root of a. Also the initial value $x_0 = 1$ of the rational iteration is contained in this starting interval.). The interval Newton method computes the nested sequence of intervals

$$X_{k+1} = N(X_k, \text{midpoint}(X_k)) \ \cap\ X_k,\ k = 0, 1, 2, \ldots$$

Let us again set $a = 32$ and $n = 5$. The following Maple code using our Maple Power Tool intpakX ([7, 3, 10] allows e.g. arbitrary precision interval computations) is slightly modified by hand to make it more compact.

Please note, that we use Maple's symbolic manipulation capabilities to automatically generate the first derivative $dg()$ of the function g. The `inapply` command is part of the intpakX package. It transforms a Maple function/expression into an interval function (this means basically that real quantities and real operations are replaced by corresponding interval enclosures and interval operations). This allows to compute verified range enclosures of the original real-valued Maple function/expression over intervals. `mid` indicates the midpoint and `&intersect` denotes an operator computing the intersection of its two interval operands.

```
> restart;
  libname := "/home/kraemer/projekte/braun/master", libname;
  with(intpakX);
> n := 5: a := 32.0:
  g := proc (x) options operator, arrow; x^n-a end proc:
  dg := unapply(diff(g(x), x), x):
```

```
> x := 'x':
  N := inapply( mid(x) - g(mid(x))/dg(x), x ): #Newton operator

> Digits := 40:

> xk := construct(1/a, a); #contains the root of g()
  printf("x0:"); print(xk);
  for k to 11 do  #perform some interval Newton steps
    xk := `&intersect`(N(xk), xk);
    printf("x%d:  %c", k, "\n"); print(xk);
  end do;

x0:
              [0.0312500000000000000000000000000000000000,
         32.000000000000000000000000000000000000000]
x1:
              [0.0312500000000000000000000000000000000000,
                 15.814652631803437365931586100487038493 17]
x2:
              [0.0312500000000000000000000000000000000000,
                 7.8232316228936325492733544353703678094 00]
x3:
              [0.0312500000000000000000000000000000000000,
                 3.8790697979050801840454818159272192648 84]
x4:
                [1.9581896296948014997122607014201557172 96,
                 3.8790697979050801840454818159272192648 84]
x5:
                [1.9581896296948014997122607014201557172 96,
                 2.7598215447097506582902625360640534921 03]
x6:
                [1.9581896296948014997122607014201557172 96,
                 2.2174708709746558449984874927953448262 69]
x7:
                [1.9834838735816231123769182650147606511 79,
                 2.0243754233514021899237849607022374936 04]
x8:
                [1.9998514757735690046672918613278840597 48,
                 2.0001711352387502883022815065486920806 10]
x9:
                [1.9999999651324014445256423629920770807 0,
                 2.0000000037409419107387741854534153358 88]
x10:
                [1.9999999999999999999097576080686540639748,
                 2.0000000000000000009347281696010079613 80]
x11:
                [1.9999999999999999999999999999999999999969,
```

```
2.000000000000000000000000000000000000031]
```

The value of the exact zero $\sqrt[5]{32}$ of g is the integer value 2. Thus, looking at the number of nines behind the leading 1 of the lower bound or at the number of zeros behind the leading 2 of the upper bound allows to see the quadratic convergence property of the Newton iteration. The number of correct digits is typically doubled in each additional step. Using arbitrary precision interval operations (manipulating the `Digits` variable) allow the efficient computation of enclosures of arbitrary accuracy. With this respect, arbitrary precision interval operations may be much more useful than rational operations (see the end of Subsection 2.1).

3. Additional remarks on the interval Newton method and computer-assisted proofs

In Section 2.2 we started the interval Newton iteration with an interval containing the correct answer (this was not checked by the computations but has been verified a priori analytically). But the interval Newton method also allows to check a sufficient criterion with the help of the computer: It is easy to show that if $N(X) \subseteq X$, then the interval X contains exactly one zero of f. The proof is based on Brouwer's fixed point theorem and the fact that $F'(X)$ does not contain 0 (otherwise a division by zero occurs, i.e. $N(X)$ is not defined for the argument X). Thus, the set of derivatives does not contain zero which means that the function g is monotone on X guaranteeing the uniqueness of the zero. The validity of $N(X) \subseteq X$ checked by the computer is a computer-assisted proof that the function f has exactly one zero in the interval X.

A computer-assisted proof for the fact that g has no zero in X results from $N(X) \cap X = \emptyset$. An empty intersection as a result of the corresponding machine interval operation is, again, sufficient for the assertion on g. And again overestimation in the computation of $N(X)$ by (machine) interval operations does not invalidate the sufficiency of the criterion result.

Maple and other computer algebra packages like Mathematica [23], MuPad etc. provide very well designed mathematical function implementations. But to the authors knowledge, the results are not guaranteed to be accurate to the last bit. Even worse, there are now guaranteed error bounds for the function implementation available/published. The function implementations also do not allow interval or complex interval arguments. `intpakX` guarantees interval computations based on the basic arithmetical operations. Computing mathematical functions on intervals is possible, but the realization of these interval functions is based on Maples point functions (accuracy not specified) just using some guard digits. This approach often gives correct results, but of course, it is not really reliable in a mathematical sense. To overcome this unpleasant situation we suggest to combine computer algebra packages with appropriate interval libraries/environments. In the following section we have a look on interval packages supplying their users with different kinds of interval mathematical functions.

4. Some multiple-precision and arbitrary-precision interval packages

There are only a few interval packages supporting multiple-precision interval mathematical functions available [19, 20, 18, 13, 8]. One C++ library with a rather complete set of elementary mathematical functions (trigonometric functions and their inverses, hyperbolic functions and their inverses, exponentials, logarithms,

power functions, as well as some other functions) for real and complex machine intervals is C-XSC [8, 5, 6]. C-XSC offers the intrinsic interval data types `interval`, `cinterval` for real and complex intervals with IEEE double numbers as bounds and `l_interval` and `l_cinterval` for staggered precision real and complex intervals. There is also a C-XSC interface to the MPFR and MPFI libraries available. In this case the arbitrary precision data types are called `MPFRClass` and `MPFIClass`, respectively. However, the MPFR and MPFI libraries do not support complex intervals. An additional package to C-XSC is also available delivering staggered precision real and complex intervals with extremely wide exponent range. The data types are called `lx_interval` and `lx_cinterval`, respectively. These staggered data types [16] are based on unevaluated sums of IEEE double numbers. They typically allow precisions up to a several hundred decimal digits.

We first use a variable of the basic complex interval data type `cinterval` to compute an enclosure of the set $\ln(\sin(z))|z \in Z$ with $Z = [0,1] + i[2,3] \subset C$. Here Z denotes the rectangle with sides parallel to the axes and with lower left corner (0,2) and upper right corner (1,3). We want to compute a corresponding rectangle, again with sides parallel to the axes, containing the range of the sine function on X. Note, that the shape of the set $\{\ln(\sin(z))|z \in Z\}$ itself is more complex.

The C-XSC source code is as follows:

```
#include <iostream>
using namespace std;
#include <cinterval.hpp>   //complex interval operations
using namespace cxsc;

int main() {
  cinterval z(interval(0,1),interval(2,3)); //complex interval data type
  //complex interval [0,1] + i*[2,3]

  cout << "z: " << endl << z << endl;

  cout << "Enclosure of ln(sin(z)): " << endl << ln(sin(z)) << endl;
}
```

Running the program results in the following output:

```
z:
([  0.000000,  1.000000],[  2.000000,  3.000000])
Enclosure of ln(sin(z)):
([  0.672740,  2.574116],[  0.227314,  1.570797])
```

The computed result `[0.672740,  2.574116] + i*[0.227314,  1.570797]` is guaranteed to be an enclosure of the range of values $\{\ln(\sin(z))|z \in Z\}$.

Let us compute $\ln(\sin(1 + 3i))$ to about 45 good decimals using the staggered precision data type `l_cinterval`.

```
//...as in the listing above
#include <l_cinterval.hpp>   //staggered precision complex intervals

int main() {
  //the global C-XSC variable stagprec allows to control
  //the precision of staggerd-precision quantities:
```

```
  stagprec= 3; //about three-fold double precision

  cout << SetDotPrecision(50,45); //output format

  //create a complex interval in staggered-precision format
  l_cinterval z(interval(1,1),interval(3,3));
  //z is the complex (point) interval [1,1] + i*[3,3]

  cout << "z: " << endl << z << endl;

  cout << "Enclosure of ln(sin(z)): " << endl << ln(sin(z)) << endl; }
```

The output is

```
z:
([ 1.00000000000000000000000000000000000000000000000,
   1.00000000000000000000000000000000000000000000000 ],
 [ 3.00000000000000000000000000000000000000000000000,
   3.00000000000000000000000000000000000000000000000 ])
Enclosure of ln(sin(z)):
([ 2.30788634750649460182963196995720032491072743 2,
   2.30788634750649460182963196995720032491072743 3 ],
 [ 0.56854473020570595247691898551293554194230241 1,
   0.56854473020570595247691898551293554194230241 2 ])
```

The second displayed complex interval is guaranteed to contain the value $ln(sin(1+3i))$. We see that the enclosure is accurate up to the last digits displayed.

The staggered-precision data is a special kind of a multiple-precision data type lohner93,blom09. The operations are performed on floating-point vectors representing exact sums of floating point values. To this end the so called long accumulator (C-XSC dotprecision data type, [8, 24]) is used. It allows the exact computation of dot products of vectors with floating-point components. Because staggered precision numbers are stored as vectors with floating-point components, the precision of staggered numbers is limited by the exponent range of the underlying floating-point screen.

In the next example we perform some time measurements for arbitrary precision real and interval arithmetics based on the libraries MPFR [17, 22] and MPFI [22]. The MPFR library guarantees the best possible accuracy (exactly rounded results for all rounding modes) with respect to the precision used. The interval functions realized by the MPFI library are based on this feature. They give best possible interval enclosures (if the exact function value is representable, this value is return value of the MPFI function call). The set of interval functions realized in the MPFI library is very limited. Complex interval functions are not at all available.

Representable results are reproduced by the MPFI functions. Let x denote the interval $[2, 4]$. Then $\log 2(x) = [1, 2]$ and $\log 2(1/x) = \log 2([1/2, 1]) = [-2, -1]$.

```
#include <iostream>
#include <interval.hpp>  //C-XSC intervals
#include "mpficlass.hpp" //C-XSC interface to MPFI library
using namespace std;
using namespace MPFI;
using namespace cxsc;
```

```
int main() {
  long int prec= 10;
  MpfiClass::SetDefaultPrecision(prec);  //use prec bit for mantissa
  MpfiClass::SetBase(2);                 //base for input/output

  MpfiClass x(interval(2.0,4.0));        //interval [2,4]
  cout << "log2(x): " << log2(x) << endl;
  MpfiClass r;
  r= 1/x;
  cout << "log2(1/x)=log2(r): " << log2(r) << endl;
  cout << "log10(x): " << log10(x) << endl;
}
```

Running the program produces the following output:

```
log2(x):             [ 1.00000,    1.00000e1 ]
log2(1/x)=log2(r):   [-1.00000e1, -1.00000   ]
log10(x):            [ 1.00110e-2, 1.00111e-1]
```

Note that the interval bounds are printed as binary numbers. The results are as predicted.

The following program is used to do some time measurements for the arbitrary precision MPFI interval functions. We compute enclosures for the sine function at the point interval $[7, 7]$ with 1000 bit starting precision and doubling the precision within a loop until $2^9 \times 1000 = 512000$ bit are reached.

```
#include <interval.hpp>
#include "mpficlass.hpp"
#include "timer.hpp"
using namespace std;
using namespace MPFI;
using namespace cxsc;

int main() {
  double start;
  long int precision=1000; //number of mantissa bits

  for (int i= 0; i<= 9; i++) {
    MpfiClass x(interval(7), precision);  //point interval [7,7]
    cout << precision << " bits,  ";
    start= GetTime();
    sin(x);  //function call
    cout << "time used: " << GetTime()-start << " sec" << endl;
    precision+= precision; //precision doubling
  }
}
```

Running the program produces the following output:

```
  1000 bits,  time used: 0.000250101 sec
  2000 bits,  time used: 0.000307083 sec
  4000 bits,  time used: 0.000962019 sec
```

```
  8000 bits,  time used: 0.00355291 sec
 16000 bits,  time used: 0.0135369 sec
 32000 bits,  time used: 0.0501981 sec
 64000 bits,  time used: 0.191191 sec
128000 bits,  time used: 0.698907 sec
256000 bits,  time used: 2.63609 sec
512000 bits,  time used: 8.5943 sec
```

The time needed to compute the sine function using Maple at the point 7.0 to 100000 decimal places (about 332200 binary digits) measured by

```
restart: Digits:=100000; st:= time(): sin(7.0): time()-st;
```

is: `11.605` seconds.

The C-XSC as well as the Maple results have been computed on the same machine.

Maple's sine function implementation seems to be not as efficient as the interval sine function for MpfiClass interval variables in C-XSC. There is no guarantee of good digits in the Maple result whereas the MPFI/C-XSC enclosure is the best possible result (guaranteed by the MPFR and MPFI libraries) with respect to the actual precision setting.

5. Concluding remarks

We urgently need software tools combining symbolic computations and verification methods. There are several promisingly first approaches (see e.g. [14]). However, a lot of further work (theoretical research as well as highly demanding software development) has to be done to get really powerful hybrid methods. The author is confident that it's worth the effort. The outcome will allow the user to do more and more automatized rigorous mathematics on the computer, not only based on symbolic manipulations but also based on very fast floating-point (interval) computations. Also highly sophisticated but often unsafe approximate methods may be complemented by mathematically rigorous supplementations.

References

[1] Weblink to C-XSC
`http://www.math.uni-wuppertal.de/wrswt/xsc/cxsc_new.html`

[2] Alefeld, G., HerzbergerJ.: Introduction to Interval Computations. Academic Press, New York, 1983.

[3] Markus Grimmer.: Interval Arithmetic in Maple with intpakX. PAMM - Proceedings in Applied Mathematics and Mechanics, Vol. 2, Nr. 1, p. 442-443, Wiley-InterScience, 2003.

[4] Hammer, R., Hocks, M., Kulisch, U., Ratz, D.: Numerical Toolbox for Verified Computing I: Basic Numerical Problems. Springer Verlag, 1993.

[5] Hofschuster, W., Krämer, W.: C-XSC 2.0: A C++ Library for Extended Scientific Computing. Numerical Software with Result Verification, Lecture Notes in Computer Science, Volume 2991/2004, Springer-Verlag, Heidelberg, pp. 15 - 35, 2004.

[6] Hofschuster, W., Krämer, W., Neher, M.: C-XSC and Closely Related Software Packages. Preprint 2008/3, Universität Wuppertal, 2008; published in: Dagstuhl Seminar Proceedings 08021 - Numerical Validation in Current Hardware Architectures, LNCS 5492, Springer-Verlag, pp 68-102, 2008.

[7] `intpakX` link at the University of Wuppertal:
`http://www.math.uni-wuppertal.de/~xsc/software/intpakX/`

[8] Klatte, R., Kulisch, U., Wiethoff, A., Lawo, Chr., Rauch, M.: C-XSC - A C++ Class Library for Extended Scientific Computing. Springer-Verlag, Heidelberg, 1993.

[9] Krämer, W.: Accurate Computation of Chaotic Dynamical Systems. In: A. Aggarwal (ed): Proceedings to Mathematics and Computers in Biology and Chemistry (MCBC 07), Vancouver, Canada, pp. 74-79, 2007.
[10] Krämer, W.: intpakX - An Interval Arithmetic Package for Maple. Proceedings of the 12th GAMM-IMACS Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics, SCAN 2006, IEEE Computer Society, ISBN 0-7695-2821-X, 2007.
[11] Maplesoft: `http://www.maplesoft.com/applications/app_center_browse.aspx?CID=13&SCID=155`
[12] Neumaier, A.: Interval Methods for Systems of Equations. Encyclopedia of Mathematics and its Applications 37, Cambridge University Press, Cambridge, UK, 1990.
[13] Aberth, O.: Introduction to Precise Numerical Methods. Academic Press, New York, 2007.
[14] Popova, E., Krämer, W., Russev, M.: Integration of C-XSC Automatic Differentiation in Mathematica. Preprint 3/2010, IMI-BAS, Sofia, March, 2010. See `http://www.math.bas.bg/~epopova/papers/10-preprintAD.pdf`
[15] Adams, E., Kulisch, U.: Scientific Computing With Automatic Result Verification. Academic Press, Inc., 1993.
[16] Blomquist, F., Hofschuster, W., Krämer, W.: A Modified Staggered Correction Arithmetic with Enhanced Accuracy and Very Wide Exponent Range. Lecture Notes in Computer Science LNCS 5492, pp. 41-67, Springer, 2009.
[17] Fousse, L., Hanrot, G., Lefevre, V., Pelissier, P., Zimmermann, P.: MPFR: A Multiple-Precision Binary Floating-Point Library With Correct Rounding. ACM Transactions on Mathematical Software, Vol.33, No.2, Article 13, 2007.
[18] Grimmer, M., Petras, K., Revol, N.: Multiple Precision Interval Packages: Comparing Different Approaches. In Lecture Notes in Computer Science, Vol. 2991, pp. 64–90, Springer, 2004.
[19] Krämer, W.: Multiple Precision Computations With Result Verification. In [1], pp. 325–356, 1993.
[20] Krämer, W., Kulisch, U., Lohner, R.: Numerical Toolbox for Verified Computing II – Advanced Numerical Problems (draft). Chapter 7, Multiple-Precision Arithmetic Using Integer Operations, pp. 210–251, 1998.
Online availabe, see `http://www.math.uni-wuppertal.de/wrswt/literatur/tb2.ps.gz`
[21] Lohner, R.: Interval Arithmetic in Staggered Correction Format. In [1], pp. 301–342, 1993.
[22] Revol, N. and Rouillier, F.: Motivations for an Arbitrary Precision Interval Arithmetic and the MPFI Library. Reliable Computing, Vol. 11, pp. 275–290, 2005.
[23] Wolfram Research Inc.: *Mathematica*, Version 5.2, Champaign, IL, 2005.
[24] Zimmer, M., Krämer, W., Bohlender, G., Hofschuster, W.: Extension of the C-XSC Library With Scalar Products With Selectable Accuracy. Preprint BUW-WRSWT 2009/4, University of Wuppertal, 2009; in press, Serdica Journal of Computing, 2010.

Walter Krämer, Scientific Computing/Software Engineering, Faculty of Mathematics and Natural Sciences, University of Wuppertal, 42119 Wuppertal, Germany.

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 135–145
ISSN 1930-1235: (2010)

SCHUBERT CELLS IN LIE GEOMETRIES AND KEY EXCHANGE VIA SYMBOLIC COMPUTATIONS

VASYL USTIMENKO

Abstract. We propose some cryptographical algorithms based on finite BN-pair G defined over the fields F_q. We convert the adjacency graph for maximal flags of the geometry of group G into a finite Tits automaton by special colouring of arrows and treat the largest Schubert cell Sch $= {F_q}^N$ on this variety as a totality of possible initial states and a totality of accepting states at a time. The computation (encryption map) corresponds to some walk in the graph with the starting and ending points in Sch. To make algorithms fast we will use the embedding of geometry for G into Borel subalgebra of corresponding Lie algebra. We consider the induced subgraph of adjacency graph obtained by deleting all vertices outside of largest Schubert cell and corresponding automaton (Schubert automaton). We consider the following symbolic implementation of Tits and Schubert automata. The symbolic initial state is a string of variables x_α, where roots α are listed according Bruhat order, choice of label will be governed by linear expression in variables x_α, where α is a simple root.

Conjugations of such nonlinear map with element of affine group acting on ${\mathrm{F_q}}^N$ can be used in Diffie-Hellman key exchange algorithm based on the complexity of group theoretical discrete logarithm problem in case of Cremona group of this variety. We evaluate the degree of these polynomial maps from above and the maximal order of this transformation from below. For simplicity we assume that G is a simple Lie group of normal type but the algorithm can be easily generalised on wide classes of Tits geometries. In a spirit of algebraic geometry we generalise slightly the algorithm by change of linear governing functions for rational linear maps.

1. Introduction

According to Hilbert's approach to Geometry it is a special incidence system (or multipartite graph). Felix Klein thought that the Geometry was a group and proposed his famous Erlangen program. J. Tits combined those two ideas for the development of concept of a BN-pair, its geometry and flag system [28]. [29]. He created an axiomatic closure for such objects based on the definition of building [30].

Finite geometries $\Gamma(G(q))$ of BN-pair $G(q)$ with Weyl group W defined over finite field F_q, $q \to \infty$ form a family of small world graphs. Really, the diameters of the incidence graphs for $\Gamma(G(q))$ coincide with the diameter of Weyl geometry $\Gamma(W)$, but average degree is growing with the growth of parameter q. The problem

Key words and phrases. small world graphs, Lie geometries, symbolic computations, walks on graphs, Schubert cells, automata, cryptography, key exchange protocols.

Research supported by a project "Human - The Best Inwestment". The project is co-funded from the sources of the European Union within the European Social Fund.

of constructing infinite families of small world graphs has many remarkable applications in economics, natural sciences, computer sciences and even in sociology. For instance, the "small world graph" of binary relation "two person shake hands" on the set of people in the world has small diameter.

The algorithm of finding the shortest pass between two arbitrarily chosen vertexes of $\Gamma(G(q))$ is much faster than the action of general Dijkstra algorithm. One can find the pass in $\Gamma(G(q))$ for the time c, where c is a constant independent on q. Regular graphs of simple groups of Lie type of normal type of rank 2 (generalised m-gons for $m \in \{3, 4, 6\}$ support the sharpness of Erdös' bound from Even Circuit Theorem in cases of cycles of length $4, 6$ and 10 (see [3]).

One of the constructions which provide for each $k_0 \geq 2$ the infinite family of regular graphs of degree $k, k \geq k_0$ of large girth (length of minimal cycle) is based on the properties of the geometry of Kac-Moody BN-pair $G(q)$ with diagram $\tilde{A}_1$ (see [16], [17], [18])

The geometries of finite BN-pairs are traditionally used in classical Coding Theory. Foundations of this theory are based on the concept of finite distance-transitive or distance-regular metrics (distance regular and distance transitive graphs in other terminology [6]). Large number of known families of distance transitive graphs are constructed in terms of the incidence geometry of BN-pair or geometry of its Weyl group. Known constructions of families of distance - regular but not distance transitive graphs are also based on the properties of BN-pair geometries (see [6], [32]). Linear codes are just elements of projective geometry and all applications of Incidence Geometries to Coding Theory are hard to observe (see [12], [20], [22] and further references). Notice that some nonclassical areas like LDPS codes and turbocodes use objects constructed via BN-pair geometries: for the first constructions of LDPS codes Tanner [27] used finite generalised m-gons, the infinite family of graphs of large girth defined in [16] have been applied to constructions of the LDPS codes ([15], [13], [14], [25], [26] and further references)

Quite recent development gives an application of linear codes and their lattices to cryptography. Incidence geometries were used in [1] and [36] for the development of cryptographical algorithms (see also a [5], [20]).

In the paper we generalise some encryption algorithms of [36], [35] and consider the key exchange protocols based on geometries of BN-pairs.

2. Basic definitions in theory of BN-pairs, their geometries and flag systems

2.1. **Graphs and incidence system.** The missing definitions of graph-theoretical concepts which appears in this paper can be found in [2] or [3]. All graphs we consider are simple, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertices u and v (or neighbours). The sequence of distinct vertices $v_0, v_1, \ldots, v_t$, such that $v_i G v_{i+1}$ for $i = 1, \ldots, t-1$ is the pass in the graph. The length of a pass is a number of its edges. The distance $\mathrm{dist}(u, v)$ between two vertices is the length of the shortest pass between them. The diameter of the graph is the maximal distance between two vertices u and v of the graph. Let C_m denote the cycle of length m i.e.

the sequence of distinct vertices $v_0, \ldots, v_m$ such that $v_i G v_{i+1}$, $i = 1, \ldots, m-1$ and $v_m G v_1$. The girth of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G. The degree of vertex v is the number of its neighbours.

The incidence structure is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another is a line. We shall identify I with the simple graph of this incidence relation (bipartite graph). If number of neighbours of each element is finite and depends only from its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [7]). An incidence structure is a semiplane if two distinct lines are intersecting not more than in one point and two distinct points are incident not more than one line. As it follows from the definition, graphs of the semiplane have no cycles C_3 and C_4.

The graph is k-regular if each of its vertex has degree k, where k is a constant.

The incidence system is the triple (Γ, I, t) where I is a symmetric antireflexive relation (simple graph) on the vertex set Γ, $t : \Gamma \to \Delta$ is a *type function* onto the set of types Δ such that $\alpha I \beta$ and $t(\alpha) = t(\beta)$ implies $\alpha = \beta$.

The flag F is a nonempty subset in Γ such that $\alpha, \beta \in F$ implies $\alpha I \beta$. We assume that $t(F) = \{t(x) | x \in F\}$

We assume that two flags F_1 and F_2 are incident ($F_1 I F_2$) if $F_1 \cup F_2$ is also a flag and $t(F_1) \cap t(F_2) = \emptyset$. Let $GF(\Gamma)$ be the incidence graph of the incidence relation defined on the set of all flags from Γ, $GF_{I,J}(\Gamma)$, $I \cap J = \emptyset$ be the totality of flags of type I or J with the restriction of flag incidence on it. The type function is defined by $t(\alpha) = s$, where $\alpha = gG_s$ for some $s \in S$.

2.2. **Groups, Coxeter systems and BN-pairs.** An important example of the incidence system as above is the so-called *group incidence system* $\Gamma(G, G_s)_{s \in S}$. Here G is the abstract group and $G_{s s \in S}$ is the family of distinct subgroups of G. The objects of $\Gamma(G, G_s)_{s \in S}$ are the left cosets of G_s in G for all possible $s \in S$. Cosets α and β are incident precisely when $\alpha \cap \beta \neq \emptyset$. The type function is defined by $t(\alpha) = s$ where $\alpha = gG_s$ for some $s \in S$.

Let (W, S) be a Coxeter system, i.e. W is a group with set of distinguished generators given by $S = \{s_1, s_2, \ldots, s_l\}$ and generic relation $(s_i \times s_j)^{m_{i,j}} = e$. Here $M = (m_{i,j})$ is a symmetrical $l \times l$ matrix with $m_{i,i} = 1$ and off-diagonal entries satisfying $m_{i,j} \geq 2$ (allowing $m_{i,j} = \infty$ as a possibility, in which case the relation $(s_i \times s_j)^{m_{i,j}} = e$ is omitted). Letting $W_i =< S - \{s_i\} >$, $1 \leq i \leq l$ we obtain a group incidence system $\Gamma_W = \Gamma(W, W_i)_{1 \leq i \leq l}$ called the Coxeter geometry of W. The W_i are referred to as the *maximal standard subgroups* of W (see [8]).

Let G be a group, B and N subgroups of G, and S a collection of cosets of $B \cap N$ in N. We call (G, B, N, S) a *Tits system* (or we say that G *has a BN-pair*) if

(i) $G =< B, N >$ and $B \cap N$ is normal in N,

(ii) S is a set of involutions which generate $W = N/(B \cap N)$,

(iii) sBw is a subset in $BuB \cup BswB$ for any $s \in S$ and $w \in W$,

(iv) $sBs \neq B$ for all $s \in S$.

Properties (1)-(iv) imply that (W, S) is a Coxeter system (see [7], [8]). Whenever (G, B, N, S) is a Tits system, we call the group W the Weyl group of the system, or more usually the Weyl group of G. The subgroups P_i of G defined by BW_iB are called the *standard maximal parabolic subgroups* of G. The group incidence system $\Gamma_G = \Gamma(G, P_i)_{1 \leq ilel}$ is commonly referred to as the *Lie geometry* of G (see [6]). Note that the Lie geometry of G and the Coxeter geometry of the corresponding Weyl

group have the same rank. In fact there is a type preserving morphism from Γ_G onto Γ_W given by $gP_i \to wW_i$, where w is determined from the equality $BgP_i = BwP_i$. This morphism is called a *retraction* (see [30]).

3. Tits and Schubert automata and for symbolic computations

3.1. **Definitions of automata.** The geometry $\Gamma(G)$ of BN-pair G is the set of all left cosets by the standard maximal subgroups i.e. maximal subgroups P_i, $i = 1, 2, \ldots, ni$ of G containing standard Borel subgroup B. Two cosets $C_1 = gP_i$ and $C_2 = hP_j$ are incident $C_1 I C_2$ if and only if their intersection is not empty. It is clear, that $gP_i \cap hP_j \neq 0$ implies $i \neq j$. The maximal flag of the geometry is a subset $F = \{C_1, C_2, \ldots, C_n\}$ such that $C_i I C_j$ for each pair (i, j), $i \neq j$. Maximal flags form the set $\mathrm{F}\Gamma(G)$, they are in one to one correspondence with the left cosets by standard Borel subgroup. The largest Schubert cell Sch is the orbit of B acting on $\mathrm{F}\Gamma(G)$ containing largest number of elements. In case of group of normal type variety $\mathrm{Sch} = \mathrm{Sch}(G)$ is isomorphic to vector space ${F_q}^N$, where N is the number of positive roots.

We assume that two maximal flags F_1 and F_2 are adjacent if their intersection contains $n-1$ elements of geometry. Let $AF(G)$ be the simple graph of symmetric adjacency relation (flag graph for $\Gamma(G)$. The order of this simple regular graph is $|(G : B)|$, the degree is nq and diameter is n. Let us restrict the adjacency relation as above on the largest Schubert cell $\mathrm{Sch}(G)$. We obtain new graph $AS(G)$ which is a regular induced subgraph of $AF(G)$ of order q^N and degree $q-1$. We refer to $AS(G)$ as Schubert subgraph of the flag graph.

We convert the directed graph of adjacency relation of flags into the following automaton.

Let (F_1, F_2) be the ordered pair of adjacency flags such that $t(F_1 \cap F_2) = \{1, 2, \ldots, n\} - \{s\}$. So flags differs by geometry elements $C_1 = {C_s}^1$ and $C_2 = {C_s}^2$ of type s from (F_1, F_2), respectively. The following situations are possible.

(i) Element C_1 and C_2 are from the same Schubert cell. In that case there unique a transformation $u = x_\alpha(t)$, $t \neq 0$, shifting C_1 to C_2. Root α depends on $\mathrm{Retr}(F_1)$ only.

(ii) Elements C_1 and C_2 are from different Schubert cells and there is a group U_α such that $(F_1 \cap F_2) \cup \{u(C_2)\}$ is an adjacent flag to F_1 for each $u = x_\alpha(t)$. Notice, that case $t = 0$ is a possibility here. Root α depends on $\mathrm{Retr}(F_1)$ again.

(iii) Elements C_1 and C_2 are from different Schubert cells and Schubert cell contains C_2 as unique representative C such that flag $(F_1 \cap F_2) \cup \{C\}$ is adjacent to F_1.

Let us consider the following labelling of $F_1 \to F_2$ for cases of (i), (ii) and (iii) separately:

(i) put the label (s, t). where $t \neq 0$.

(ii) the label is (s, t), where $t \in F_q$ is defined by condition $x_\alpha(t)\mathrm{Retr}(C_2) = C_2$

(iii) put the label ∞.

So for fixed F_1 and fixed type s the label (s, t) in direction to s-adjacency flag is defined by parameter t taken from the "acceptable" set $\mathrm{Ac}(F_1) = F_q \cup \{\gamma\}$ where γ is one of the symbols 0 and ∞. We add the formal loop on state F_1 labelled by the unique symbol from $\{0, \infty\} - \{\gamma\}$.

So the transition function $T_{s,t}$ of taking the s-adjacent element of colour (s, t) for general flag is defined for each $t \in F_q \cup \{\infty\}$ We assume that the initial state

can be any flag from the largest Schubert cell Sch and this cell is the totality of all accepting states.

So algorithm can be given by the string of labels $(s_1, t_1), (s_2, t_2), \dots, (s_d, t_d)$ such that the composition $T = T(s_1, t_1)T(s_2, t_2)T(s_d, t_d)$ maps Sch into itself. We are interested only in irreducible computations for which $s_i \neq s_{i+1}$ for $i = 1.2, \dots d-1$

In case of group of normal type the alphabet contains exactly $n(q+1)$ symbols. The computation corresponds to special walks in the graph $AF(G)$ with the starting and ending point in $\mathrm{Sch}(G)$. Notice that C may be not a bijection. For instance $T(s, O)$, which image for Sch lays outside of the largest large Schubert cell, is not invertible.

We refer to such automaton as *Tits automaton* for group G. We would like to use it as tool for symbolic computations.

The unipotent group U acts regularly on Sch. So we can identify $v \in \mathrm{Sch}$ with certain product of $X_\alpha(t_\alpha)$, and positive roots $\alpha \in \mathrm{Root}$ are taken in Bruhat order. In fact, we identify the string $\mathrm{v} = t_\alpha \in F_q$, $\alpha \in \mathrm{Root}^+$ with the accepting state v.

We refer to the list $(t_{\alpha_1}, t_{\alpha_2}, \dots, t_{\alpha_n})$, where $\alpha_1, \alpha_2, \dots, \alpha_n$ is the set of all simple roots, as the color of v from plainspace. So we are colouring accepting states now but not arrows.

Let us consider irreducible computation within Tits automaton of kind $v \to v_s$, $v_1 = T(i_1, a_1)(v)$, $v_2 = T(i_2, a_2)(v_1), \dots, v_s = T(i_s, a_s)(v_{s-1})$, where $i_k \neq i_{k+1}$, $k = 1, \dots, s-1$, $a_k \in F_q \cup \infty$, element $\mathrm{Retr}(v) = \mathrm{Retr}(v_s)$ equals to the element $w \in W$ of maximal length. Notice, that in the sequence $\mathrm{Retr}(v_1), \mathrm{Retr}(v_2), \dots, \mathrm{Retr}(v_k)$ consecutive elements are adjacent in $\mathrm{F\Gamma}(W)$ or equal.

The computation is conducted into several steps. Each time we have one of the situations i, (ii) or (iii). In cases of kind (i) and (ii) when the corresponding root α is simple parameters a_j will be chosen as linear functions of kind $l(t_{\alpha_1}, t_{\alpha_2}, \dots t_{\alpha_n}) = c_1 t_{\alpha_1} + c_2 t\alpha_2 \dots, c_n t_{\alpha_n} + b$, where $c_1, c_2, \dots, c_n$ and b are elements of F_q and $(t_{\alpha_1}, t_{\alpha_2}, \dots, t_{\alpha_n})$ is a colour of our initial state. If α is not a simple root, we choose a_j as $c_j t_{\beta_j} + f_j((t_{\alpha_1}, t_{\alpha_2}, \dots t_{\alpha_n})$, where $c_j \neq 0$.

After the completion of our computation we get the accepting state $u = v_s$. It has a colour $(d_{\alpha_1}, d_{\alpha_2}, \dots, d_{\alpha_n}) = (t_{\alpha_1}, t_{\alpha_2}, \dots t_{\alpha_n})A + (b_1, b_2, \dots, b_n)$, where

the matrix A is defined by some linear expressions of kind $a_i = l_i(l(t_{\alpha_1}, t_{\alpha_2}, \dots t_{\alpha_n})$, which we used during the computation. We will require that the matrix A is invertible. Notice that we may use symbol ∞, where the design of algorithm allows such option.

After the completion of algorithm we obtain accepting state of colour $(d_{\alpha_1}, d_{\alpha_2}, \dots, d_{\alpha_n})$. The invertibility of A allows us to compute $(t_{\alpha_1}, t_{\alpha_2}, \dots t_{\alpha_n})$ as $((d_{\alpha_1}, d_{\alpha_2}, \dots d_{\alpha_n}) - (b_1, b_2, \dots, b_n))A^{-1}$. So we can compute all parameters a_i and create the reverse walk in the graph and compute the inverse map T^{-1} which sends the final accepting state to initial state.

Let us restrict Tits automaton on the largest Schubert cell, i. e delete all states outside $\mathrm{Sch}(G)$ together with corresponding output arrows. We obtain Schubert automaton over the alphabet (i, a), where $a \in F_q$, $1 \leq i \leq n$. Notice, that $a = 0$ corresponds to taking the loop.

3.2. **Tits and Schubert automata and related symmetric encryption.** Correspondents Alice and Bob may use the following symmetric encryption based on the Tits automaton. The plainspace is a vector space $\mathrm{Sch} = {F_q}^N$. The plaintext p we identify with the string $\mathrm{v} = t_\alpha \in F_q$, $\alpha \in \mathrm{Root}^+$. We may think that this is a

function p : $Root^+ \to F_q$. Alice has to compute the restriction of this function onto subsets of all simple roots and get the colour $(t_{\alpha_1}, t_{\alpha_2}, \dots, t_{\alpha_d})$ of the plainspace.

Correspondents share symbolic string of labels $(s_1, l_1), (s_2, l_2), \dots, (s_d, l_d)$, where $l_i.i = 1, 2, \dots, d$ is a linear expression of formal variables z_α, for each simple root α or ∞ and two affine invertible transformations τ_1 and τ_2. The vector space of all maps from the totality of simple roots to F_q has to be not invariant subspace for τ_i, $i = 1, 2$. Alice executing the specialization $z_\alpha = p_\alpha$ computing Corresponding numerical string $\mathrm{t} = (t_1, t_2, \dots, t_d)$. She has to hide that string by applications of affine maps τ_i. So she is adding to symbolic key two invertible Linear transformations τ_1 and τ_2 of the plainspace ${F_q}^N$ and compose τ_1, the automaton map corresponding to t and τ_2.

She sends to Bob the ciphertext

$$\mathrm{c} = \tau_1(T(s_1, t_1)T(s_2, t_2)\dots T(s_d, t_d)(\tau_1(\mathrm{p}))$$

Bob decrypt applying to c consequently ${\tau_2}^{-1}$, T^{-1}, where $T = T(s_1, t_1)T(s_2, t_2)\dots T(s_d, t_d)$ and ${\tau_1}^{-1}$,

Remark 1. If correspondents do not use ∞ in the shared symbolic key then T is the computation in Schubert automaton. Bob can simply compute T^{-1} as $T(s_d, -t_d)T(s_{d-1}, -t_{d-1})\dots T(s_1, -t_1)$.

Remark 2. We may generalise the above algorithms by changing affine maps τ_1, τ_2 and $(t_1, t_2, \dots, t_n) \to (t_1, t_2, \dots, t_d)A + (b_1, b_2, \dots, b_n)$ for general invertible polynomial maps.

4. Key exchange protocols based on incidence geometries

The automata as above can be considered over the general ground field F We can see that the computations in both automata do not use division. What is going on during the computations on a symbolic level. Let us assume now that the initial state is a formal string of variables x_α, where α is running throw the list of all positive roots. It is convenient for us to expand the ground field F_q to the field R of rational functions $r(x_1, x_2, \dots, x_N) = f(x_1, x_2, \dots, x_N)/g(x_1, x_2, \dots, x_N)$, where f and g are elements $F_q[x_1, x_2, \dots, x_N]$ Formal variables x_α and governing linear expressions $l(x_{\alpha_1}, x_{\alpha_2}, \dots, x_{\alpha_n}, x_\alpha)$, where α is not a simple root are elements of subring $F_q[x_1, x_2, \dots, x_N]$ in R. During its work Tits automaton newer use division. So after getting accepting state over R we got the vector of dimension N with polynomial components f_α. So the numerical encryption map is regular automorphism of ${F_q}^N$ (element of Cremona group for ${F_q}^N$) of kind.

$$x_i \to f_i(x_1, x_2, \dots, x_N), i = 1, 2, \dots, N$$

Special choice of symbolic key guarantee that the above transformation is bijective. Symbol ∞ play just formal role. Linearity of governing functions leads to rather small degree of the nonlinear map.

Such a walk produces a bijective transformation T of variety $\mathrm{Sch}(G)$ which is its regular automorphism (polynomial map of the variety into itself such that its inverse is also polynomial). We will conjugate T by invertible affine transformation $\tau \in AGL_N(F_q)$ and use $Y = \tau^{-1}T\tau$ as the instrument for the key exchange based in modified Diffie - Hellman method. So the Alice is computing a standard from for Y

$t_1 = f_1(t_1, t_2, \dots, t_N), t_2 = f_2(t_1, t_2, \dots, t_N), \dots, t_N = f_N(t_1, t_2, \dots, t_N),$

where $f_i \in F_q[t_1, t_2, \dots, t_N]$, $i = 1, 2, \dots, N$, and sending the map to Bob via open communication channel. Correspondents Alice and Bob (as usually) are choosing their keys k_A and k_B, respectively. They are executing computations $D_A = Y^{k_A}$ and $D_B = Y^{k_B}$. They exchange the outputs via the open channel.

Finally Alice and Bob are computing collision maps ${D_B}^{k_A}$ and ${D_A}^{k_B}$. So correspondents are getting common element.

We can modify the above scheme:

Alice chooses the maximal flag F from the largest large Schubert cell $\mathrm{Sch}(G)$ and sends it to Bob via open channel. Correspondence may use common flag ${D_A}^{k_B}(F) = {D_B}^{k_A}(F)$ as the key for their private key algorithm.

The security of the above key exchange algorithm based on the complexity of discrete logarithm problem for the Cremona group of variety $\mathrm{Sch}(G)$. In case of finite field F_q this group coincides with the symmetric group S_{q^N}. it is important that we use description of permutations in terms of polynomial algebra. So related discrete logarithm problem is formulated in terms of algebraic geometry.

Method allows various modification: we can use nonlinear invertible maps instead of affine transformation τ, the base of discrete logarithm can be non invertible polynomial map and etc. An interesting modifications can be obtained if we will allow noninvertible transformations of the variety. For instance we may consider fractional linear governing function l_i for the step i looks like $(a_1 X_{\alpha 1} + a_2 x_\alpha 2 + \dots a_{\alpha_n} x_{\alpha_n})/(b_1 X_{\alpha 1} + b_2 x_\alpha 2 + \dots b_{\alpha_n} X_{\alpha_n})$ if the root α on step i is simple, and l_i is a fraction of two linear combinations of x_α, $\alpha \in \mathrm{Root}^+$ if α is not a simple root. In case of such governing functions we refer to corresponding automata as birational Tits and Schubert automaton, respectively.

5. Embedding of the flag variety into the Lie Algebra and some complexity estimates

Throughout this section (G, B, N, S) is a Tits system which arises in connection with Chevalley group G, although we point that the results of this section remain valid in a far more general setting (see [30],[7], [8]). We write $G = X_l(K)$ to signify that G is the Chevalley group over the field K, with associated Dynkin diagram X_l. We are most interested in the case when K is finite, and we shall write $X_l(q)$ instead of $X_l(F_q)$ in that case.

So, fix Chevalley group $G = X_l(K)$ with corresponding Weyl group W. As in the previous section Γ_W and Γ_G their associated Coxeter and Lie geometries. Let $L = H + L^+ + L^-$ be the Lie algebra corresponding to G.

Following convention, we refer to H, L^+, L^- and $H + L^+$ as, respectively, the *Cartan subalgebras, positive root space, negative root space* and *Borel subalgebra* with respect to the given decomposition of L. We also use the familiar bracket notation $[,]$ to indicate Lie product [4], [24],

Below we turn out our attention to a method of embedding Γ_W and Γ_G in L. As the reader shall see, this method actually embeds Γ_W in the Cartan subalgebra H of L. Let us consider the embedding more precisely.

Let $A = (a_{i,j})$ be the Cartan matrix corresponding to the root system Ω of W. We consider the lattice R which is generated by simple roots $\alpha_1, \alpha_2, \dots, \alpha_l$ and the reflection $r_1, r_2, \dots r_l$ of R defined by the equality $(\alpha_i)^{r_j} = \alpha_i - a_{i,j}\alpha_j$.

Let $S = \{r_1, r_2, \dots, r_l\}$ is the set of Coxeter generators of Weyl group W. Let ${\alpha_1}^*, {\alpha_2}^*, \dots, {\alpha_l}^*$ be a dual basis of $\alpha_1, \alpha_2, \dots, \alpha_l$, i.e. ${\alpha_i}^*$ is the linear functional

on R which satisfies ${\alpha_i}^*(\alpha_j) = \delta_{i,j}$. We define the action of W on the dual lattice R^* by $l(x)^s = l(x^s)$, where $l(x) \in \mathrm{R}^*$ and $s \in S$.

Consider the orbit $H_i = \{{\alpha_i}^{*w} | w \in W\}$ of permutation group (W, R^*), which contains ${\alpha_1}^*$. Let H be the disjoint union of H_i. We give the set H the structure of an incidence system as follows. Linear functionals $l_1(x)$ and $l_2(x)$ are incident if and only if products $l_1(\alpha)l_2(\alpha) \geq 0$ for all $\alpha \in \Omega$. The type function t is defined by $t(l(x)) = i$ where $l(x) \in H_i$. It can be shown that (H, I, t) is isomorphic to Coxeter geometry Γ_W. (In fact there is a unique isomorphism of Γ_W with (H, I, t) which sends W_i to α_i, $1 \leq i \leq l$.) This gives the desired embedding since H is a subset in R^* and $\mathrm{R}^* \subset L_0$. Moreover this embedding still valid for a field K of sufficiently large characteristic, since, in that case H is a subset of $\mathrm{R} \times K = L_0$.

We now consider an analogous embedding of the Lie geometry Γ_G into the Borel subalgebra $U = L_0 + L^+$ of L. Let $d = {\alpha_1}^* + {\alpha_2}^* + \ldots {\alpha_l}^*$. Than we can take $\Omega^+ = \{\alpha \in \Omega | d(\alpha) \geq 0\}$ to be our set of positive roots in Ω. For any $l(x) \in \mathrm{R}^*$ define $\eta^-(L) = \alpha \in \Omega^+ | l(\alpha) < 0$.

Let L_α be the root space corresponding to positive root α. For each $h \in H$ we define the subalgebra L_h as the sum of L_α, $\alpha \in \eta^-(h)$. Let $U_i = \{h + v | h \in H_i, v \in L_h\}$ and U is a disjoint union of U_i. We give U the structure of an incident system as follows. Elements $h_1 + v_1$ and $h_2 + v_2$ are incident if and only if each of the following hold:

(i) $h_1(\alpha)h_2(\alpha) \geq 0$ for all $\alpha \in \Omega$, i.e. h_1 and h_2 are incident in (H, I, t).

(ii) $[h_1 + v_1, h_2 + v_2] = 0$

Element $h + v$ has type i if $h + v \in U_i$.

In [38] it is shown that this newly defined incident system is isomorphic to the Lie geometry Γ_G, provided that the characteristic of K is zero or sufficiently large to ensure the isomorphism at the level of the subgeometries (H, I, t) and Γ_W. Then analogous to the Weyl case, there exists a unique isomorphism Retr of $\Gamma(G)$ into (U, I, t) which sends P_i to α_i, $1 \leq i \leq l$.

Proposition 5.1. *Let $\Gamma = \Gamma(G)$ be the geometry of group $G = X_n(q)$. The above interpretation of $\Gamma(G)$ allows*

(i) generate Γ in $O(|\Gamma|)$ elementary steps and check whether or not two elements of Γ are incident for time $O(N^2)$, where N is the number of positive roots.

(ii) complete the computation in Tits and Schubert automaton consisting of k elementary steps for time $O(kN)$

Graphs of degree q and $SF(X_n(q)$, $q \geq 4$ of degree $q-1$ have orders $|X_n(q)|/|B|$ and q^N, respectively. They form families of small world graphs depending on two parameters n and q.

6. On the discrete logarithm problem with polynomial or birational base

Let F_p, where p is prime. be a finite field. Affine transformations $\mathrm{x} \to A\mathrm{x} + b$, where A is invertible matrix and $b \in (F_p)^n$, form an affine group $AGL_n(F_p)$ acting on ${F_p}^n$. It is known that polynomial transformation of kind $x_1 \to g_1(x_1, x_2, \ldots, x_n), x_2 \to g_2(x_1, x_2, \ldots, x_n), \ldots, x_n \to g_n(x_1, x_2, \ldots, x_n)$ form a symmetric group S_{p^n}.

In the simplest case F_p, affine transformations form an affine group $AGL_n(F_p)$ of order $(p^n - 1)(p^n - p) \ldots (p^n - p^{n-1})$ in the symmetric group S_{p^n} of order $(p^n)!$. In [19] the maximality of $AGL_n(F_p)$ in S_{p^n} was proven. So we can present each

permutation π as a composition of several "seed" maps of kind $\tau_1 g \tau_2$, where $\tau_1, \tau_2 \in AGL_n(F_p)$ and g is a fixed map of degree ≥ 2. One may choose quadratic map of Imai - Matsumoto algorithm in case $p = 2$ (see [10], [21] for its description and cryptanalysis by J. Patarin) or graph based cubical maps [31] for general p.

We can choose the base of ${F_p}^n$ and write each permutation $g \in S_{p^n}$ as a "public rule":

$x_1 \to g_1(x_1, x_2, \ldots, x_n), x_2 \to g_2(x_1, x_2, \ldots, x_n), \ldots, x_n \to g_n(x_1, x_2, \ldots, x_n)$.

Let $g^k \in S_{p^n}$ be the new public rule obtained via iteration of g. Discrete logarithm problem of finding solution for k for $g^k = b$ can be difficult if the order of g is "sufficiently large". We have to avoid the linear growth of the degree g^k, when k is growing. Obvious bad example is the following: g sends x_i into ${x_i}^t$ for each i. In this case the solution is just a ratio of deg$b$ and deg$g$.

Let us consider the Cremona group $C(n, q)$ of all invertible polynomial automorphisms of the vector space ${F_q}^n$, where $q = p^m$, the semigroups $PC(n, q)$ and $BC(n, q)$ of polynomial and birational maps of ${F_q}^n$ into itself, respectively.

To avoid such trouble one can look at families of subgroups of increasing order G_n, $n \to \infty$ of S_{p^n} such that maximal degree of its element equals c, where c is independent constant (groups of degree c or groups of stable degree). We refer to an element g such that all its nonidentical powers are of degree c as element of stable degree.

It is clear that the family of affine subgroup $AGL_n(p)$ is a subgroup of stable degree for $c = 1$ and all nonidentical affine transformations are of stable degree. Notice that if g is a linear diagonalisable element of $AGL_n(p)$, then discrete logarithm problem for base g is equivalent to the classical number theoretical problem.

One can take a subgroup H of $AGL_n(p)$ and consider its conjugation with nonlinear bijective polynomial map f. Of course the group $H' = f^{-1}Hf$ will be also a stable group, but for most pairs f and H group H' will be of degree deg$f \times$ deg$f^{-1} \geq 4$ because of nonlinearity f and f^{-1}. So the problem of construction an infinite families of subgroups G_n in S_p^n of degree 2 and 3 may attract some attention.

The following questions are important because of Diffie Hellman type protocols (see [9]).

$Q1$; How to construct stable subgroups C of small degree c ($c = 2$ and $c = 3$ especially) of increasing order in $C(n, q)$?

We say refer to a semigroup Se generated by single elements as monogenetic semigroup of order |Se|.

$Q2$; How to construct stable monogenetical subsemigroups in $PC(n, q)$ and $BC(n, q)$ of small degree c ($c = 2$ and $c = 3$ especially) of increasing order in $C(n, q)$ of large order?

Finally, we announce the following statement

Theorem 6.1. *Let $X_n(F)$, $n \geq 2$ be a simple group of Lie type over the field F. Let $L(X_n(q)$ be a group of all invertible computations in Schubert automaton.*

In case of classical groups (diagrams A_n, B_n, C_n and D_n) groups $L(X_n(F))$, $n \to \infty$ form families of stable degree.

Remark: Groups $L(X_n(F))$ are of degree 3 in case of diagram B_n, C_n and D_n, and $L(A_n(F))$ are groups of degree 2.

We can demonstrate the existence of elements in $L(X_n(q))$ of rather large order. Really, take a permutation $i_1, i_2, \ldots, i_n$ on the nodes of Dynkin diagram and compute a composition g of generators $Z^{i_1}(l_1(x)), Z^{i_2}(l_2(x)), \ldots Z^{i_n}(l_n(x))$, where $l_i(x)$

are linear forms corresponding to the rows of Singer cycle matrix of order $q^n - 1$ (see, for instance, [11]). As it follows from the description of algorithm the order of g will be at least $q^n - 1$.

Similarly we can use Singer cycle to generate by Tits automata a stable monogenetic subgroup in $PC(n, q)$ and $BC(n, q)$.

References

[1] A. Beutelspachera, Enciphered Geometry. Some Applications of Geometry To Cryptography, Annals of Discrete Mathematics, V.37, 1988, 59-68.

[2] N. Biggs, *Algebraic Graph Theory* (2nd ed), Cambridge, University Press, 1993.

[3] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1972.

[4] N. Bourbaki, *Lie Groups and Lie Algebras*, Chapters 1 - 9, Springer, 1998-2008.

[5] A. A. Bruen , D. L. Wehlau, *Error-Correcting Codes, Finite Geometries and Cryptography*, AMS, 2010.

[6] A. Brower, A. Cohen, A. Nuemaier, *Distance regular graphs*, Springer, Berlin, 1989.

[7] F. Buekenhout (Editor), *Handbook on Incidence Geometry*, North Holland, Amsterdam, 1995.

[8] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York 1972.

[9] N. Coblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer, 1994, 237 p.

[10] N. Coblitz, *Algebraic Aspects of Cryptography*, Springer, 1998, 198 p.

[11] A. Cossidente, M. J. de Ressmine, *Remarks on Singer Cycle Groups and Their Normalizers*, Desighns, Codes and Cryptography, 32, 97-102, 2004.

[12] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[13] , 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.

[14] 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.

[15] Jon-Lark Kim, U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, *Explicit construction of families of LDPC codes with no 4-cycles* , Information Theory, IEEE Transactions, 2004, v. 50, Issue 10, 2378 - 2388.

[16] F. Lazebnik and V. Ustimenko, *Some Algebraic Constructions of Dense Graphs of Large Girth and of Large Size*, DIMACS series in Discrete Mathematics and Theoretical Computer Science, V. 10 (1993), 75-93.

[17] F. Lazebnik, V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.

[18] 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.

[19] B. Mortimer, *Permutation groups containing affine transformations of the same degree*, J. London Math. Soc., 1972, 15, N3, 445-455.

[20] H. Niederreiter, Chaoping Xing, *Algebraic Geometry in Coding Theory and Cryptography*, Princeton University Press, 2009).

[21] J. Patarin, *Cryptoanalysis of the Matsumoto and Imai public key scheme of the Eurocrypt '88*, Advances in Cryptology, Eurocrypt '96, Springer Verlag, 43-56.

[22] T. Richardson, R. Urbanke, *Modern Coding Theory* Cambridge University Press, 2008.

[23] , T. Shaska , W C Huffman, D. Joyner, V Ustimenko (Editors), Advances in Coding Theory and Crytography (Series on Coding Theory and Cryptology) World Scientific Publishing Company, 2007.

[24] J. P. Serre, *Lie Algebras and Lie groups*, N. Y., Lectures in Math., Springer, Berlin, 1974.

[25] T. Shaska, V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra and its Applications Article, Volume 430, Issue 7, 1 April 2009, Special Issue in Honor of Thomas J. Laffey.

[26] T. Shaska and V. Ustimenko, *On some applications of graph theory to cryptography and turbocoding*, Special issue of Albanian Journal of Mathematics:Proceedings of the NATO Advanced Studies Institute "New challenges in digital communications", May 2008, University of Vlora, 2008, v.2, issue 3, 249-255.
[27] R. Michiel Tanner, *A recursive approach to low density codes*, IEEE Trans. on Info Th., IT, 27(5):533-547, Sept.1984.
[28] J. Tits, *Sur la trialite at certains groupes qui s'en deduicent*, Publ. Math. I.H.E.S. 2 (1959), 15-20.
[29] J. Tits, *Les groupes simples de Suzuki et de Ree*, Seminaire Bourbaki 13 (210), 1960/1961, 1-18.
[30] J. Tits, *Buildings of spherical type and Finite BN-pairs, Lecture Notes in Math*, Springer Verlag, 1074.
[31] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, 2001, v. 2227, 278-287.
[32] V. A. Ustimenko, *On some properties of Chevalley groups and their generalisations*, In: Investigations in Algebraic Theory of Combinatorial objects, Moskow, Institute of System Studies, 1985, 134 - 138 (in Russian), Engl.trans.: Kluwer, Dordrecht, 1992, pp. 112-119
[33] V. A. Ustimenko, *Linear interpretation of Chevalley group flag geometries*, Ukraine Math. J. 43, Nos. 7,8 (1991), pp. 1055–1060 (in Russian).
[34] V. A. Ustimenko, *Geometries of twisted simple groups of Lie type as objects of linear algebra*, in Questions of Group Theory and Homological Algebra, University of Jaroslavl, Jaroslavl, 1990, 33-56 (in Russian).
[35] V. A. Ustimenko, *On the Varieties of Parabolic Subgroups, their Generalizations and Combinatorial Applications*, Acta Applicandae Mathematicae 52 (1998): pp. 223–238.
[36] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, 117-153.

Vayl Ustimenko, University of Maria Curie Sklodovska in Lublin
E-mail address: vasyl@hekor.umcs.lublin.pl

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 147–160
ISSN 1930-1235: (2010)

SINGULAR LOCUS ON THE SPACE OF GENUS 2 CURVES WITH DECOMPOSABLE JACOBIANS.

LUBJANA BESHAJ

Abstract. We study the singular locus on the algebraic surface $\mathfrak{S}_n$ of genus 2 curves with a (n,n)-split Jacobian. Such surface was computed by Shaska in [15] for $n=3$, and Shaska at al. in [3] for $n=5$. We show that the singular locus for $n=2$ is exactly th locus of the curves of automorphism group D_4 or D_6. For $n=3$ we use a birational parametrization of the surface $\mathfrak{S}_3$ discovered in [15] to show that the singular locus is a 0-dimensional subvariety consisting exactly of three genus 2 curves (up to isomorphism) which have automorphism group D_4 or D_6. We further show that the birational parametrization used in $\mathfrak{S}_3$ would work for all $n \geq 7$ if $\mathfrak{S}_n$ is a rational surface.

1. Introduction

We study the singular locus on the space of genus 2 curves with a (n,n)-split Jacobian. Such curves have been of much interest lately because of their use in many theoretical and applicative situations. The first part of the paper is based on several papers on the topic of genus two curves with split Jacobians; see [1,3–9,11–14,16–21] among others.

In the first section, we study genus 2 curves with split Jacobian. Let $\mathcal{X}$ be a genus 2 curve defined over an algebraically closed field k, of characteristic zero. Let $\psi : \mathcal{X} \to E$ 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 $\mathcal{X}$ 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 Jac $(\mathcal{X})$ of $\mathcal{X}$ and the product $E \times E'$. We say that $\mathcal{X}$ has (n,n)-split Jacobian.

The locus of genus two curves with (n,n)-split Jacobians is an irreducible 2-dimensional algebraic variety. There are many descriptions of it in the literature, but throughout this paper we will use only the embdedding of such space in the moduli space $\mathcal{M}_2$. In other words, we would like an equation of such space where every point corresponds precisely to one isomorphism class of genus 2 curves. We denote such surface by $\mathfrak{S}_n$ and always think of it given by an equation in terms of the absolute invariants i_1, i_2, i_3 of genus two curves; see [21]. We will call the surface $\mathfrak{S}_n$ the Shaska surface of level n.

The case with $(3,3)$-split Jacobian was studied in [15]. These are the curves with degree 3 elliptic subcovers. Shaska in [15] computed the locus of curves $\mathcal{X}$

2010 *Mathematics Subject Classification.* 14Q15, 14Q05, 68W30.
Key words and phrases. genus two curves, moduli spaces, hyperelliptic curve cryptography, modular polynomials.

with degree 3 elliptic subfield in the moduli space of genus 2 curves. We will give the explicit equation of this space and also a graphical representation of it. It was the first time that such an equation was computed other than the computationally trivial case for $n = 2$.

In [3] was studied the case with $(5, 5)$ - split Jacobian by Shaska, Magaard, and Voelklein. There was computed a normal form for the curves in the locus $\mathfrak{S}_5$ and its three distinguished subloci. Further, they have computed the equation of the elliptic subcover in all cases, gave a birational parametrization of the subloci of $\mathfrak{S}_5$ as subvarieties of $\mathcal{M}_2$ and classify all curves in these loci which have extra automorphisms.

In section 2 of this paper we compute the singular locus, $\mathcal{T}_2$, of the space $\mathfrak{S}_2$, and the singular locus $\mathcal{T}_3$ of the space $\mathfrak{S}_3$. The definition of the singular locus depends on the parametrization of the surface. For the case of $n = 2$ we prove that the singular locus of $\mathfrak{S}_2$ is exactly the locus of genus 2 curves with automorphism group D_4 or D_6. This computations were done using Maple 14.

If the surface $\mathfrak{S}_n$ is rational then we show how to obtain a birational parametrization for $\mathfrak{S}_n$ using the invariants of binary cubics, which were used first in [15].

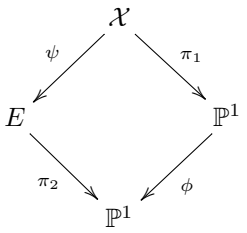
Throughout this paper by a genus two curve we mean the isomorphism class of a genus two curve defined over an algebraically closed field k. While most of the results are true for most characteristics, we assume throughout that the characteristic of k is zero.

2. Preliminaries

2.1. **Genus 2 curves with split Jacobian.** Let $\mathcal{X}$ be a genus 2 curve defined over an algebraically closed field k, of characteristic zero. The affine version of this curve is given by the equation $\mathcal{X} : y^2 = F(x)$, where $F(x)$ is a polynomial of degree 5 or 6 and discriminant different from zero. Let

$$\psi : \mathcal{X} \to E$$

be a degree n covering, where n is odd and E is an elliptic curve. The degree n covering $\psi : \mathcal{X} \to E$ induces a degree n cover $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ such that the following diagram commutes.



Here, $\pi_1 : \mathcal{X} \to \mathbb{P}_1$ and $\pi_2 : E \to \mathbb{P}_2$ are the hyperelliptic projections. So, $\phi \circ \pi_1 = \pi_2 \circ \psi$. From Riemann- Hurwitz formula the number of branch points is 4, or 5. The ramification of the function ϕ is as follows; there are $\frac{n-1}{2}$ points of index 2 in q_1, q_2 and q_3, and $\frac{n-3}{2}$ points of index 2 in q_4, and there is only one point of index 2 in q_5. We denote this type of ramification by

$$\left((2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-1}{2}}, (2)^{\frac{n-3}{2}}, (2)\right).$$

In the following figure bullets (resp., circles) represent places of ramification index 2 (resp., 1).

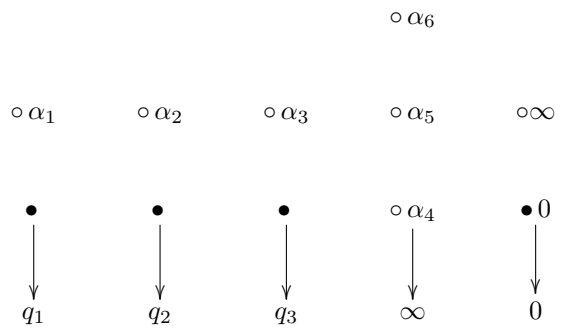


FIGURE 1. Ramification of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ when $n = 3$

The family of coverings $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, is an irreducible 2-dimensional algebraic variety. For every ϕ there exists a genus 2 curve C. Let $\mathcal{H}$ be the family of coverings. We have the map

$$\alpha : \mathcal{H} \to \mathcal{M}_2$$
$$[\phi] \to [\mathcal{X}]$$

Let $\alpha(\mathcal{H})$ be denoted by $\mathfrak{S}_n$. So, we say that these curves $\mathcal{X}$ are parametrized by an irreducible 2-dimensional subvariety $\mathfrak{S}_n$ of the moduli space $\mathcal{M}_2$ of genus 2 curves. The fact that $\mathfrak{S}_n$ is irreducible, for n odd, comes from the braid action on Nielsen classes. It is known that this is the case for all $n \cong 1 \mod 2$; see [20] among others. Computation of spaces $\mathfrak{S}_n$ as a subvariety of $\mathcal{M}_2$ has first computed by Shaska in [15] for $n = 3$ and then by Shaska, Magaard, and Voelklein for $n = 5$; see [3]. We will call the space $\alpha(\mathcal{H}) \hookrightarrow \mathcal{M}_2$ the **Shaska surface of level** n.

2.2. **Pairs of elliptic subcovers.** Let $\psi_1 : \mathcal{X} \longrightarrow E_1$ be a covering of degree n from a curve of genus 2 to an elliptic curve. The covering $\psi_1 : \mathcal{X} \longrightarrow E_1$ is called a **maximal covering** if it does not factor over 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 [20] for details.

Let $\psi_1 : \mathcal{X} \longrightarrow E_1$ be a covering as above which is maximal. Then ${\psi^*}_1 : E_1 \to J_C$ is injective and the kernel of $\psi_{1,*} : J_{\mathcal{X}} \to E_1$ is an elliptic curve which we denote by E_2, see [17] or [21]. For a fixed Weierstrass point $P \in C$, we can embed C to its Jacobian via

$$i_P : \mathcal{X} \longrightarrow J_C$$
$$x \to [(x) - (P)]$$

Let $g : E_2 \to J_C$ be the natural embedding of E_2 in J_C, then there exists $g_* : J_{\mathcal{X}} \to E_2$. Define $\psi_2 = g_* \circ i_P : \mathcal{X} \to E_2$. So we have the following exact sequence

$$0 \to E_2 \xrightarrow{g} J_{\mathcal{X}} \xrightarrow{\psi_{1,*}} E_1 \to 0$$

The dual sequence is also exact, see [20]

$$0 \to E_1 \xrightarrow{\psi_1^*} J_{\mathcal{X}} \xrightarrow{g_*} E_2 \to 0$$

The following lemma shows that ψ_2 has the same degree as ψ_1 and is maximal.

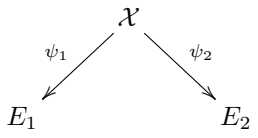


FIGURE 2. Splitting of the genus two curve

Lemma 1. *a) deg* $(\psi_2) = n$
b) ψ_2 *is maximal*

For the proof see [20]. If $deg(\psi_1)$ is an odd number then the maximal covering $\psi_2 : \mathcal{X} \to E_2$ is unique (up to isomorphism of elliptic curves).

To each of the covers $\psi_i : \mathcal{X} \longrightarrow E_i$, $i = 1, 2$, correspond covers $\phi_i : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$. If the cover $\psi_1 : \mathcal{X} \longrightarrow E_1$ is given, and therefore ϕ_1, we want to determine $\psi_2 : \mathcal{X} \longrightarrow E_2$ and ϕ_2. The study of the relation between the ramification structures of ϕ_1 and ϕ_2 provides information in this direction. The following lemma answers this question for the set of Weierstrass points $W = \{P_1, \ldots, P_6\}$ of $\mathcal{X}$ when the degree of the cover is odd.

Let $\psi_i : \mathcal{X} \longrightarrow E_i$, $i = 1, 2$, be maximal of odd degree n. Let $\mathcal{O}_i \in E_i[2]$ be the points which has three Weierstrass points in its fiber. Then, we have the following:

Lemma 2. *The sets* $\psi_1^{-1}(\mathcal{O}_1) \cap W$ *and* $\psi_2^{-1}(\mathcal{O}_2) \cap W$ *form a disjoint union of* W.

Thus, the elliptic subcovers occur in pairs.

2.3. **Describing the Shaska surface $\mathfrak{S}_n$ in $\mathcal{M}_2$.** Consider a genus two curve $\mathcal{X}$ defined over k, given with equation

$$\mathcal{X}: \quad y^2 = a_6X^6 + a_5X^5 + \cdots + a_0.$$

Igusa J-invariants $\{J_{2i}\}$ of $\mathcal{X}$ are homogeneous polynomials of degree $2i$ in

$$k[a_0, \ldots, a_6], \text{ for } i = 1, 2, 3, 5;$$

see [21], [10] for their definitions. Here J_{10} is simply the discriminant of $f(X, Z)$. These J_{2i} are invariant under the natural action of $SL_2(k)$ on sextics. Dividing such an invariant by another one of the same degree gives an invariant under $GL_2(k)$ action.

Two genus 2 fields K (resp., curves) in the standard form $Y^2 = f(X, 1)$ are isomorphic if and only if the corresponding sextics are $GL_2(k)$ conjugate. Thus if I is a $GL_2(k)$ invariant (resp., homogeneous $SL_2(k)$ invariant), then the expression $I(K)$ (resp., the condition $I(K) = 0$) is well defined. Thus the $GL_2(k)$ invariants are functions on the moduli space $\mathcal{M}_2$ of genus 2 curves. This $\mathcal{M}_2$ is an affine variety with coordinate ring

$$k[\mathcal{M}_2] = k[a_0, \ldots, a_6, J_{10}^{-1}]^{GL_2(k)}$$

which is the subring of degree 0 elements in $k[J_2, \ldots, J_{10}, J_{10}^{-1}]$. The *absolute invariants*

$$i_1 := 144\frac{J_4}{J_2^2}, \; i_2 := -1728\frac{J_2J_4 - 3J_6}{J_2^3}, \; i_3 := 486\frac{J_{10}}{J_2^5},$$

are even $GL_2(k)$-invariants. Two genus 2 curves with $J_2 \neq 0$ are isomorphic if and only if they have the same absolute invariants. If $J_2 = 0$ then we can define new

invariants as in [21]. For the rest of this paper if we say "there is a genus 2 curve $\mathcal{X}$ defined over k" we will mean the k-isomorphism class of $\mathcal{X}$.

Remark 1. *The definitions of i_1, i_2, i_3 with J_2 in the denominator is done simply for computational purposes.*

Let

$$F(X) = a_3X^3 + a_2X^2 + a_1X + a_0, \text{ and } G(X) = b_3X^3 + b_2X^2 + b_1X + b_0$$

be two cubic polynomials. We define the following invariants

$$H(F,G) := a_3b_0 - \frac{1}{3}a_2b_1 + \frac{1}{3}a_1b_2 - a_0b_3$$

We denote by $R(F,G)$ the resultant of F and G and by $D(F)$ the discriminant of F always with respect to X. Also,

$$r_1(F,G) = \frac{H(F,G)^3}{R(F,G)}, \quad r_2(F,G) = \frac{H(F,G)^4}{D(F)\,D(G)}.$$

In [2] it is shown that r_1, r_2, and $r_3 = \frac{H(F,G)^2}{J_2(F\,G)}$ form a complete system of invariants for unordered pairs of cubics.

Every curve $\mathcal{X}$ in $\mathfrak{S}_n$ is written as a product of two cubics. In other words, its equation is

$$y^2 = F(X)\cdot G(X)$$

for some $F(X), G(X) \in k[X]$. We will use the invariants r_1, r_2 in relation with these cubics. Since the discriminants of such cubics can not be zero (otherwise the curve is not a genus two curve) then $D(F), D(G)$ are nonzero. For the same reason $F(X)$ and $G(X)$ don't have any common factors. Hence, $R(F,G) \neq 0$. Thus, r_1, r_2 are everywhere defined.

3. Computation of singular locus $\mathcal{T}_n$

Throughout this section we will use x, y, z for absolute invariants i_1, i_2, i_3 respectively. Let $\mathfrak{S}_n$ be the Shaska surface of level n given by

$$\mathfrak{S}_n(x,y,z) = 0$$

Then, its singular set is defined as the solution of the system

$$\begin{cases} \dfrac{\partial \mathfrak{S}_n}{\partial x} = 0 \\ \dfrac{\partial \mathfrak{S}_n}{\partial x} = 0 \\ \dfrac{\partial \mathfrak{S}_n}{\partial x} = 0 \\ \mathfrak{S}_n(x,y,z) = 0 \end{cases} \tag{1}$$

3.1. The singular locus $\mathcal{T}_2$.

The equation of $\mathfrak{S}_2$ is given by

$$\begin{aligned}\mathfrak{S}_2(x,y,z) = {} & -27\,x^6 - 9459597312000\,z^2\,x^2 + 20639121408000\,z^2\,y + 111451255603200\,z^2\,x - 240734712102912\,z^2 \\ & - 55240704\,z\,x^4 - 18\,y^2\,x^4 - 8294400\,z\,y^2\,x^2 - 47278080\,z\,y\,x^3 - 264180754022400000\,z^3 \\ & - 2866544640000\,z^2\,y\,x + 2\,x^6\,y - 4\,x^3\,y^3 + 9\,x^7 + 331776\,z\,x^5 + 107495424\,z\,y\,x^2 - 27\,y^4 + 9\,x\,y^4 \\ & - 52254720\,z\,y^2\,x + 2\,y^5 + 161243136\,z\,y^2 + 161243136\,z\,x^3 - 12441600\,z\,y^3 + 54\,x^3\,y^2 = 0\end{aligned}$$

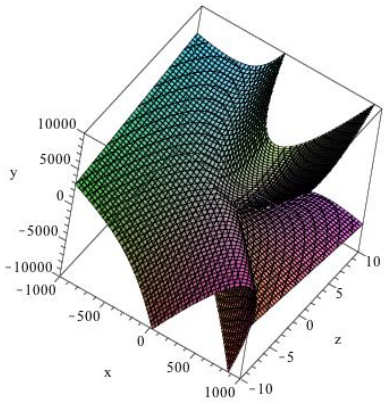


FIGURE 3. The surface $\mathfrak{S}_2$ graphed in $\mathbb{R}^3$.

Then we have the corresponding system from which we eliminate z and get

$$z = -\frac{1}{82944}\,\frac{\phi_1(x,y)}{\phi_2(x,y)}$$

where ϕ_1 and ϕ_2 are as follows;

$$\begin{aligned}\phi_1(x,y) &= 104976\,y^2 + 5211\,x^5 - 48600\,y^2x + 69984\,yx^2 + 3375\,yx^4 + 450\,x^3y^2 \\ &\quad - 50544\,x^4 - 675\,x^2y^2 + 104976\,x^3 + 2025\,xy^3 - 10800\,y^3 + 20\,x^6 + 250\,y^4 \\ &\quad - 37800\,x^3y \\ \phi_2(x,y) &= 1250\,yx^2 - 121500\,xy - 3779136 - 359100\,x^2 - 11250\,y^2 + 6375\,x^3 \\ &\quad + 421200\,y + 2274480\,x\end{aligned}$$

The locus $\mathcal{T}_2$ which has 3 irreducible components which we describe below algebraically and graphically.

The first component is given by

$$C_1: \quad 100\,y^2 - 1458\,y + 540\,xy - 243\,x^2 + 80\,x^3 = 0$$

it corresponds to the locus of genus two curves with automorphism group D_4.

The second component is given by

$$C_2 : 3888\,x - 1188\,x^2 + 5\,x^3 + 432\,y - 360\,xy - 25\,y^2 = 0$$

and it corresponds to the locus of genus two curves with automorphism group D_6.

The third component of $\mathcal{T}_2$ is given by the following system

$$C_3: \quad \begin{cases} 50\,x^4 - 7515\,x^3 - 825\,yx^2 + 20412\,x^2 - 23490\,xy - 4050\,y^2 + 52488\,y = 0 \\ 125\,y^2 - 1620\,y + 1125\,xy - 5832\,x + 1890\,x^2 + 25\,x^3 = 0 \end{cases}$$

The solution of the C_3 system is

$$\begin{cases} y = \dfrac{1}{75}\,\dfrac{408240\,x - 33525\,x^2 - 944784 + 250\,x^3}{-864 + 55\,x} \\ 125\,x^3 - 9450\,x^2 + 247860\,x - 944784 = 0 \end{cases}$$

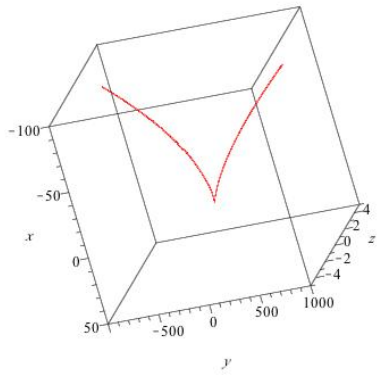


FIGURE 4. The component C_1

and the points (x, y) given by

$$\left(0, \frac{729}{50}\right), \left(\frac{81}{20}, -\frac{729}{200},\right), \left(-\frac{36}{5}, \frac{1512}{25}\right)$$

However, only the first point is on the variety and it is

$$\left(0, \frac{729}{50}, \frac{729}{12800000}\right)$$

and has automorphism groups are D_4 and therefore is contained in the first component.

We summarize in the following theorem:

Theorem 1. *The singular locus of $\mathcal{T}_2$ contains two components, the irreducible loci of curves of automorphism group D_4 and D_6.*

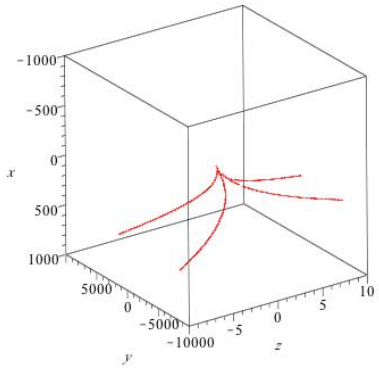


FIGURE 5. The component C_2

3.2. **The locus $\mathcal{T}_3$.** In this section we compute the singular locus $\mathcal{T}_3$ of $\mathfrak{S}_3$. The equation of $\mathfrak{S}_3$ is quite large and was computed in [15]. Below we display this equation $\mathfrak{S}(x,y,z) \mod 5$.

$$x^{20}+3x^{19}+3x^{18}y+4x^{17}y^2+3x^{18}+4x^{17}z+2x^{16}y^2+2x^{16}yz+2x^{15}y^3+4x^{16}z+2x^{15}y^2$$
$$+4x^{15}yz+x^{15}z^2+x^{13}y^3z+3x^{14}yz+x^{13}y^2z+x^{13}yz^2+4x^{12}y^3z+4x^{12}y^2z^2+x^{11}y^4z+x^{10}y^5z$$
$$+4x^{13}z^2+x^{12}y^2z+4x^{12}z^3+3x^{11}y^3z+3x^{11}y^2z^2+2x^{11}yz^3+4x^{10}y^4z+2x^{10}y^3z^2$$
$$+2x^9y^5z+2x^9y^4z^2+2x^8y^6z+x^7y^7z+4x^5y^{10}+3x^{12}z^2+3x^{11}yz^2+3x^{11}z^3+4x^{10}yz^3+4x^9y^4z$$
$$+3x^9y^3z^2+2x^9y^2z^3+3x^8y^5z+4x^8y^4z^2+3x^8y^3z^3+2x^7y^6z+2x^7y^5z^2+3x^5y^8z+2x^4y^{10}+x^4y^9z$$
$$+2x^3y^{11}+x^2y^{12}+2x^{10}z^3+3x^9y^2z^2+4x^9yz^3+x^9z^4+4x^8y^3z^2+4x^8y^2z^3+2x^8yz^4+3x^7y^4z^2$$
$$+2x^6y^6z+4x^6y^5z^2+2x^6y^4z^3+3x^5y^7z+x^5y^5z^3+4x^4y^7z^2+2x^3y^{10}+3x^3y^9z+4x^3y^8z^2+3xy^{12}$$
$$+4xy^{11}z+3y^{13}+4x^9z^3+x^8yz^3+3x^8z^4+2x^7y^2z^3+2x^7yz^4+2x^7z^5+x^6y^4z^2+x^6y^3z^3+3x^6y^2z^4$$
$$+x^6yz^5+4x^5y^5z^2+x^5y^4z^3+x^5y^3z^4+x^4y^6z^2+2x^4y^5z^3+x^4y^4z^4+3x^3y^6z^3+3x^2y^9z+3x^2y^8z^2$$
$$+4x^2y^7z^3+4xy^{10}z+3y^{12}+2y^{11}z+x^7z^4+x^6y^2z^3+3x^6yz^4+3x^6z^5+4x^5y^3z^3+x^5y^2z^4+3x^5yz^5$$
$$+3x^5z^6+2x^4y^4z^3+4x^4y^3z^4+x^4y^2z^5+4x^3y^4z^4+3x^3y^3z^5+2x^2y^7z^2+4x^2y^6z^3+2x^2y^5z^4$$
$$+2xy^8z^2+3xy^7z^3+3y^{10}z+3y^9z^2+2x^6z^4+3x^5yz^4+3x^5z^5+x^4y^2z^4+3x^4z^6+2x^3y^3z^4$$
$$+3x^3y^2z^5+3x^2y^5z^3+3x^2y^4z^4+3xy^6z^3+2xy^5z^4+2xy^4z^5+2y^7z^3+y^5z^5+2x^4z^5+x^3yz^5$$
$$+3x^3z^6+2x^2y^3z^4+2x^2y^2z^5+2x^2yz^6+2xy^4z^4+3y^5z^4+4y^4z^5+2x^3z^5+3x^2yz^5+4x^2z^6+xy^2z^5$$
$$+3y^2z^6+xz^6+3y^2z^5+4z^7+3z^6=0$$

Let $\mathcal{X}$ be a genus 2 curve in the locus $\mathfrak{S}_3$. Then, $\mathcal{X}$ is given by the equation

$$y^2=(4x^3v^2+x^2v^2+2xv+1)(x^3v^2+x^2uv+xv+1), \tag{2}$$

see [19] for details. In [15] was computed the equation of $\mathfrak{S}_3$ using the map

$$\theta:(u,v)\to(i_1,i_2,i_3)$$

where the absolute invariants i_1,i_2,i_3 in terms of u,v are

(3)

$$\begin{aligned}
i_1 =& \frac{144}{v(-405+252u+4u^2-54v-12uv+3v^2)^2}(1188u^3-8424uv+u^4v-24u^4\\
&+14580v-66u^3v+138uv^2+297u^2v+945v^2-36v^3+9u^2v^2)\\
i_2 =& -\frac{864}{v^2(-405+252u+4u^2-54v-12uv+3v^2)^3}(-81v^3u^4+2u^6v^2+234u^5v^2\\
&+3162402uv^2-21384v^3u+26676v^4-473121v^3-72u^6v-5832v^4u+14850v^3u^2\\
&-72v^3u^3+324v^4u^2-650268u^3v-5940u^3v^2-3346110v^2+432u^6-1350u^4v^2\\
&+136080u^4v-7020u^5v-307638u^2v^2\\
i_3 =& -243\frac{(v-27)(4u^3-u^2v-18uv+4v^2+27v)^3}{v^3(-405+252u+4u^2-54v-12uv+3v^2)^5}
\end{aligned}$$

The map

$$\theta:(u,v)\to(i_1,i_2,i_3)$$

given by (3) which has degree 2 and it is defined when $J_2\neq 0$. For now we assume that $J_2\neq 0$ (The case $J_2=0$ is treated in Section 4.2, of [15]). Denote the minors of the Jacobian matrix of θ by $M_1(u,v), M_2(u,v), M_3(u,v)$. The solutions of

$$\begin{cases} M_1(u,v) = 0 \\ M_2(u,v) = 0 \\ M_3(u,v) = 0 \end{cases} \tag{4}$$

consist of the (non-singular) curve

$$8v^3 + 27v^2 - 54uv^2 - u^2v^2 + 108u^2v + 4u^3v - 108u^3 = 0 \tag{5}$$

and 7 isolated solutions which we display in Table 1, together with the corresponding values (i_1, i_2, i_3), the automorphism group, and the number of elliptic subcovers.

(u,v)	(i_1,i_2,i_3)	$Aut(K)$	$e_3(K)$
$(-\frac{7}{2}, 2)$	$J_{10} = 0$, no associated genus 2 field K		
$(-\frac{775}{8}, \frac{125}{96})$, $(\frac{25}{2}, \frac{250}{9})$	$-\frac{8019}{20}, -\frac{1240029}{200}, \frac{531441}{100000}$	D_4	2
$(27 - \frac{77}{2}\sqrt{-1}, 23 + \frac{77}{9}\sqrt{-1})$, $(27 + \frac{77}{2}\sqrt{-1}, 23 - \frac{77}{9}\sqrt{-1})$	$(\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}$	D_4	2
$(-15 + \frac{35}{8}\sqrt{5}, \frac{25}{2} + \frac{35}{6}\sqrt{5})$, $(-15 - \frac{35}{8}\sqrt{5}, \frac{25}{2} - \frac{35}{6}\sqrt{5})$	$81, -\frac{5103}{25}, -\frac{729}{12500}$	D_6	2

TABLE 1. Exceptional points where $\det(Jac(\theta)) = 0$

Notice that the curve given by Eq. (5) corresponds to genus 2 curves with isomorphic degree 3 elliptic subcovers. Hence, the cover has singular branch locus on such cases. We will see next how this can be avoided when we use the invariants of a pair of cubics.

3.3. **Birational parametrization of $\mathfrak{S}_3$.** For $F(X) = (4x^3v^2 + x^2v^2 + 2xv + 1)$ and $G(X) = (x^3v^2 + x^2uv + xv + 1)$ we have

$$\begin{aligned} r_1(F,G) &= 27\frac{v(v-9-2u)^3}{4v^2 - 18uv + 27v - u^2v + 4u^3} \\ r_2(F,G) &= -1296\frac{v(v-9-2u)^4}{(v-27)(4v^2 - 18uv + 27v - u^2v + 4u^3)} \end{aligned} \tag{6}$$

Lemma 3. *The function field of* $\mathfrak{S}_3$ *is given by* $k(r_1, r_2)$. *In other words* $k(i_1, i_2, i_3) = k(r_1, r_2)$. *Moreover;*

(7)

$$i_1 = \frac{9}{4}\frac{(13824r_1^3r_2^2 + 442368r_1^2r_2^3 + 5308416r_1r_2^4 + 192r_1^4r_2 + r_1^5 + 786432r_1r_2^3 + 9437184r_2^4)}{r_1(-1152r_2^2 + 96r_2r_1 + r_1^2)^2}$$

$$\begin{aligned} i_2 = {} & \frac{27}{8r_1^2(-1152r_2^2 + 96r_2r_1 + r_1^2)^3}(+79626240r_1^4r_2^4 - 4076863488r_1^2r_2^5 + 34560r_1^6r_2^2 \\ & + 12230590464r_1^2r_2^6 + 32614907904r_1r_2^6 + 14495514624r_2^6 + 288r_1^7r_2 + 2211840r_1^5r_2^3 \\ & + r_1^8 - 212336640r_1^3r_2^4 + 1528823808r_1^3r_2^5 - 2359296r_1^4r_2^3) \end{aligned}$$

$$i_3 = -521838526464\frac{r_2^9}{r_1^2(-1152r_2^2 + 96r_2r_1 + r_1^2)^5}$$

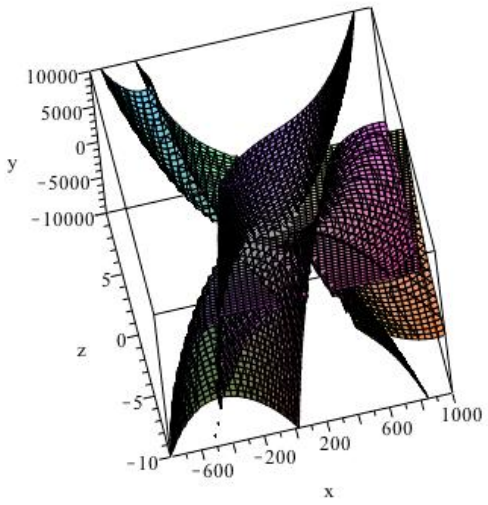


FIGURE 6. Shaska surface $\mathfrak{S}_3$

The solution of the system in

$$\begin{cases} M_1(r_1, r_2) = 0 \\ M_2(r_1, r_2) = 0 \\ M_3(r_1, r_2) = 0 \end{cases} \tag{8}$$

is

$$-1152r_2^2 + 96r_1r_2 + r_1^2 = 0 \tag{9}$$

and the system

$$\begin{cases} 3\,{r_1}^8 + 720\,{r_1}^7 r_2 + 69120\,{r_1}^6 {r_2}^2 + 2048\,{r_1}^5 {r_2}^2 + 3317760\,{r_1}^5 {r_2}^3 + 79626240\,{r_1}^4 {r_2}^4 - 417792\,{r_1}^4 {r_2}^3 \\ \quad - 24772608\,{r_1}^3 {r_2}^4 + 764411904\,{r_1}^3 {r_2}^5 - 113246208\,{r_1}^2 {r_2}^5 + 50331648\,r_1 {r_2}^5 \\ \quad - 5435817984\,r_1 {r_2}^6 - 2415919104\,{r_2}^6 = 0 \\ 9\,{r_1}^5 + 1296\,{r_1}^4 r_2 + 62208\,{r_1}^3 {r_2}^2 - 10240\,{r_1}^2 {r_2}^2 + 995328\,{r_1}^2 {r_2}^3 + 786432\,r_1 {r_2}^3 - 2359296\,{r_2}^4 = 0 \\ 9\,{r_1}^8 + 2160\,{r_1}^7 r_2 + 207360\,{r_1}^6 {r_2}^2 + 9953280\,{r_1}^5 {r_2}^3 + 38912\,{r_1}^5 {r_2}^2 + 238878720\,{r_1}^4 {r_2}^4 \\ \quad - 3735552\,{r_1}^4 {r_2}^3 + 2293235712\,{r_1}^3 {r_2}^5 - 247726080\,{r_1}^3 {r_2}^4 + 905969664\,{r_1}^2 {r_2}^5 \\ \quad + 201326592\,r_1 {r_2}^5 - 5435817984\,r_1 {r_2}^6 - 4831838208\,{r_2}^6 = 0 \end{cases}$$

Then we get the following singular points

$$(r_1, r_2) = \left(-\frac{512}{2187}, -\frac{256}{6561}\right), \left(\frac{2}{243}, \frac{1}{11664}\right), \left(-\frac{4000}{2187}, \frac{2500}{6561}\right)$$

and the corresponding points (respectively) in $\mathfrak{S}_3$ are:

$$\begin{aligned}(i_1, i_2, i_3) = &\left(-\frac{8019}{20}, -\frac{1240029}{200}, -\frac{531441}{100000}\right), \\ &\left(81, -\frac{5103}{25}, -\frac{729}{12500}\right), \\ &\left(\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}\right)\end{aligned}$$

which have automorphism groups respectively D_4, D_4, D_6, as seen from Table 1.

Notice that the Eq. (9) is exactly the case for $J_2 = 0$ where i_1, i_2, i_3 are not defined.

Corollary 1. *The singular locus $\mathcal{T}_3$ of $\mathfrak{S}_3$ are the points*

$$\left(-\frac{8019}{20}, -\frac{1240029}{200}, -\frac{531441}{100000}\right), \left(81, -\frac{5103}{25}, -\frac{729}{12500}\right), \left(\frac{729}{2116}, \frac{1240029}{97336}, \frac{531441}{13181630464}\right)$$

which have automorphisms group D_4, D_4, D_6 respectively.

Notice that we have to use a parametrization in order to get the singular locus, because it is difficult computationally to compute this locus via partial derivatives.

4. Some remarks for the general case.

Let's give a general approach how one can attempt to compute the surface $\mathfrak{S}_n$ for $n \geq 7$. For $n \geq 7$ we get the first general case where the symmetries between the fourth and the fifth branch points which occur for degree 5 do not occur any longer; see [3].

Suppose that $n \geq 7$. Then $\mathfrak{S}_n$ is parametrized by the r_1, r_2 invariants of two cubics. As in [20] we write a system of equations for the degree 7 covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.

Let $\mathcal{X}$ be a genus 2 curve in $\mathfrak{S}_n$ which has equation

$$y^2 = (x^3 + ax^2 + bx + c)\,(x^3 + ux^2 + vx + w)$$

such that a, b, c, u, v are expressed in terms of the two parameters u and v. Let r_1 and r_2 be the invariants of the two cubics. Then, there is a birational parametrization of $\mathfrak{S}_n$ in terms of parameters (r_1, r_2), i.e.

$$(r_1, r_2) \to (i_1, i_2, i_3)$$

such that $k(\mathfrak{S}_n) = k(r_1, r_2)$. Moreover, the singular locus of this parametrization contains the locus

$$J_2(r_1, r_2) = 0$$

While the computation of $\mathfrak{S}_n$ for $n \geq 7$ is more difficult because the degree is larger, it is also true that there are no other symmetries now other than the S_3 action on the first three branch points as described in [15] and [3] for cases $n = 3, 5$ respectively.

Acknowledgements: I would like to thank the Department of Mathematics at Oakland University for their support during the time that this article was written.

References

[1] L. Beshaj and T. Shaska, *The arithmetic of genus two curves*, Algebraic aspects of digital communications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 25, IOS, Amsterdam, 2011, pp. to appear.

[2] V. Krishnamoorthy, T. Shaska, and H. Völklein, *Invariants of binary forms*, Progress in Galois theory, Dev. Math., vol. 12, Springer, New York, 2005, pp. 101–122, DOI 10.1007/0-387-23534-5-6, (to appear in print). MR2148462 (2006b:13015)

[3] K. Magaard, T. Shaska, and H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566, DOI 10.1515/FORUM.2009.027. MR2526800 (2010h:14050)

[4] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

[5] N. Pjero, M. Ramasaço, and T. Shaska, *Degree even coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** (2008), no. 3, 241–248. MR2492097 (2010b:14058)

[6] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270. MR2367218 (2008k:14066)

[7] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[8] T. Shaska and V. Ustimenko, *On the homogeneous algebraic graphs of large girth and their applications*, Linear Algebra Appl. **430** (2009), no. 7, 1826–1837, DOI 10.1016/j.laa.2008.08.023. MR2494667 (2010a:05103)

[9] ———, *On some applications of graphs to cryptography and turbocoding*, Albanian J. Math. **2** (2008), no. 3, 249–255. MR2495815 (2010a:05102)

[10] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), Springer, Berlin, 2004, pp. 703–723. MR2037120 (2004m:14047)

[11] T. Shaska, G. S. Wijesiri, S. Wolf, and L. Woodland, *Degree 4 coverings of elliptic curves by genus 2 curves*, Albanian J. Math. **2** (2008), no. 4, 307–318. MR2470579 (2010b:14064)

[12] 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), DOI 10.1090/S0002-9939-07-09152-6. MR2361856 (2008m:11132)

[13] ———, *Theta functions and algebraic curves with automorphisms*, Algebraic aspects of digital communications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 24, IOS, Amsterdam, 2009, pp. 193–237. MR2605301

[14] T. Shaska, C. Shor, and S. Wijesiri, *Codes over rings of size p^2 and lattices over imaginary quadratic fields*, Finite Fields Appl. **16** (2010), no. 2, 75–87, DOI 10.1016/j.ffa.2010.01.005. MR2594505 (2011b:94059)

[15] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280, DOI 10.1515/form.2004.013. MR2039100 (2004m:11097)

[16] ———, *Some special families of hyperelliptic curves*, J. Algebra Appl. **3** (2004), no. 1, 75–89, DOI 10.1142/S0219498804000745. MR2047637 (2005i:14028)

[17] ———, *Computational aspects of hyperelliptic curves*, Computer mathematics, Lecture Notes Ser. Comput., vol. 10, World Sci. Publ., River Edge, NJ, 2003, pp. 248–257. MR2061839 (2005h:14073)

[18] ———, *Some open problems in computational algebraic geometry*, Albanian J. Math. **1** (2007), no. 4, 297–319. MR2367221 (2008k:14108)

[19] ———, *Genus 2 curves with* $(3,3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 205–218, DOI 10.1007/3-540-45455-1-17, (to appear in print). MR2041085 (2005e:14048)

[20] ———, *Curves of genus 2 with* (N,N) *decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617, DOI 10.1006/jsco.2001.0439. MR1828706 (2002m:14023)

[21] ———, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 206–231, DOI 10.1142/9789812701640-0013, (to appear in print). MR2182041 (2006g:14051)

Lubjana Beshaj, Department of Mathematics, University of Vlora, Albania.
E-mail address: lbeshaj@univlora.edu.al

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 161–170
ISSN 1930-1235: (2010)

ON THE KEY EXCHANGE WITH NONLINEAR POLYNOMIAL MAPS OF DEGREE 4

V. USTIMENKO AND A. WROBLEWSKA

The project is co-funded from the sources of the European Union
within the limit of the European Social Fund.

Human - The Best Inwestment

Abstract. We say that the sequence g_n, $n \geq 3$, $n \to \infty$ of polynomial transformation bijective maps of free module K^n over commutative ring K is a sequence of stable degree if the order of g_n is growing with n and the degree of each nonidentical polynomial map of kind ${g_n}^k$ is an independent constant c. A transformation $b = \tau {g_n}^k \tau^{-1}$, where τ is affine bijection, n is large and "k" is relatively small, can be used as a base of group theoretical Diffie-Hellman key exchange algorithm for the Cremona group $C(K^n)$ of all regular automorphisms of K^n. The specific feature of this method is that the order of the base may be unknown for the adversary because of the complexity of its computation. The exchange can be implemented by tools of Computer Algebra (symbolic computations). The adversary can not use the degree of righthand-side in $b^x = d$ to evaluate unknown x in this form for the discrete logarithm problem.

In the paper we introduce the explicit constructions of sequences of elements of stable degree for cases $c = 4$ for each commutative ring K containing at least 3 regular elements and discuss the implementation of related key exchange and public key algorithms.

1. Introduction

Discrete logarithm problem can be formulated for general finite group G. Find a positive integer x satisfying condition $g^x = b$ where $g \in G$ and $b \in G$. The problem has reputation to be a difficult one. But even the case of cyclic group Z_n there are many open questions. If $n = p - 1$ or $n = \phi(pq)$ where p and q are sufficiently large prime then the complexity of discrete logarithm problem justify classical Diffie-Hellman key exchange algorithm and RSA public key encryption, respectively. In most of other cases complexity of discrete logarithm problem is not

Received by the editors December 15, 2010.

Key words and phrases. Key exchange, public key cryptography, symbolic computations, graphs and digraphs of large girth .

Research supported by a project "Human - The Best Inwestment". The project is co-funded from the sources of the European Union within the European Social Fund.

investigated properly. The problem is very dependent on the choice of the base g and the way of presentation the data on the group. Group can be defined via generators and relations, as automorphism group of algebraic variety, as matrix group, as permutation group etc. In this paper we assume that G is a subgroup of S_{p^n} which is a group of polynomial bijective transformation of vector space ${F_p}^n$ into itself. Obviously $|S_{p^n}| = n!$, it is known that each permutation π can be written in the form $x_1 \to f_1(x_1, x_2, \dots x_n), x_2 \to f_2(x_1, x_2, \dots x_n), \dots, x_n \to f_n(x_1, x_2, \dots x_n)$, where f_i are multivariable polynomials from $F_p[x_1, x_2, \dots, x_n]$. The presentation of G as a subgroup of S_{p^n} is chosen because the Diffie Hellman algorithm here will be implemented by the tools of symbolic computations. Other reason is universality, as it follows from classical Cayley results each finite group G can be embedded in S_{p^n} for appropriate p and n in various ways.

Let F_p, where p is prime, be a finite field. Affine transformations $\mathrm{x} \to Ax + b$, where A is invertible matrix and $b \in (F_p)^n$, form an affine group $AGL_n(F_p)$ acting on ${F_p}^n$.

Affine transformations form an affine group $AGL_n(F_p)$ of order $(p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$ in the symmetric group S_{p^n} of order $(p^n)!$. In [15] the maximality of $AGL_n(F_p)$ in S_{p^n} was proven. So we can present each permutation π as a composition of several "seed" maps of kind $\tau_1 g \tau_2$, where $\tau_1, \tau_2 \in AGL_n(F_p)$ and g is a fixed map of degree ≥ 2.

We can choose the base of ${F_p}^n$ and write each permutation $g \in S_{p^n}$ as a "public rule":

$x_1 \to g_1(x_1, x_2, \dots, x_n), x_2 \to g_2(x_1, x_2, \dots, x_n), \dots, x_n \to g_n(x_1, x_2, \dots, x_n)$.

Let $g^k \in S_{p^n}$ be the new public rule obtained via iteration of g. We consider Diffie - Hellman algorithm for S_{p^n} for the key exchange in the case of group. Correspondents Alice and Bob establish $g \in S_{p^n}$ via open communication channel, they choose positive integers n_A and n_B, respectively. They exchange public rules $h_A = g^{n_A}$ and $h_B = g^{n_B}$ via open channel. Finally, Alice and Bob compute common transformation T as ${h_B}^{n_A}$ and ${h_A}^{n_B}$, respectively.

In practice they can establish common vector $v = (v_1, v_2, \dots, v_n)$, $v_i \in F_p$ via open channel and use the collision vector $T(v)$ as a password for their private key encryption algorithm.

This scheme of "symbolic Diffie - Hellman algorithm" can be secure, if the order of g is "sufficiently large" and adversary is not able to compute number n_A (or n_B) as functions from degrees for g and h_A. Obvious bad example is the following: g sends x_i into ${x_i}^t$ for each i. In this case n_A is just a ratio of $\deg h_A$ and $\deg g$.

To avoid such trouble one can look at family of subgroups G_n of S_{p^n}, $n \to \infty$ such that maximal degree of its elements equal c, where c is small independent constant (groups of degree c or groups of stable degree). Our paper is devoted to explicit constructions of such families.

We refer to a sequence of elements $g_n \in G_n$ such that all its nonidentical powers are of degree c as element of stable degree. This is equivalent to stability of families of cyclic groups generated by g_n. Of course, cyclic groups are important for the Diffie- Hellman type protocols.

It is clear that affine groups $AGL_n(p)$, $n \to \infty$ form a family of subgroups of stable degree for $c = 1$ and all nonidentical affine transformations are of stable degree. Notice that if g is a linear diagonalisable element of $AGL_n(p)$, then discrete logarithm problem for base g is equivalent to the classical number theoretical problem. Obviously, in this case we are loosing the flavor of symbolic computations.

General problem of construction an infinite families of stable subgroups G_n of S_{p^n} of degree c satisfying some additional conditions (unbounded growth of minimal order of nonidentical group elements, existence of well defined projective limit, etc) can be also interesting because of possible applications in cryptography.

Notice that even we conjugate nonlinear C with invertible linear transformation $\tau \in AGL_n(F_p)$, some of important cryptographical parameters of C and $C' = \tau^{-1}C\tau$ can be different. Of course conjugate generators g and g' have the same number of fixed points, same cyclic structure as permutations, but counting of equal coordinates for pairs $(x, g(x))$ and $(x\ , g'(x))$ may bring very different results.

So two conjugate families of stable degree are not quite equivalent because corresponding cryptoanalitical problems may have different complexity.

We generalize the above problem for the case of Cremona group of the free module K^n, where K is arbitrary commutative ring K. For the cryptography case of finite rings is the most important. Finite field F_{p^n}, $n \geq 1$ and cyclic rings Z_m (especially $m = 27$ (ASCII codes), $m = 28$ (binary codes), $m = 216$ (arithmetic), $m = 232$ (double precision arithmetic)) are especially popular. Case of infinite rings K of characteristic zero (especially Z or C) is an interesting as well because of Matijasevich multivariable prime approximation polynomials can be defined there (see, for instance [24] and further references).

So it is natural to change a vector space ${F_p}^n$ for free module K^n (Cartesian power of K) and the family and symmetric group S_{p^n} for Cremona group $C_n(K)$ of all polynomial automorphisms of K^n.

We repeat our definition for more general situation of commutative ring.

Let G_n, $n \geq 3$, $n \to \infty$ be a sequence of subgroups of $C_n(K)$. We say that G_n is a family of groups of stable degree (or subgroup of degree c) if the maximal degree of representative $g \in G_n$ is some independent constant c.

The first family of stable subgroups of $C_n(F_q)$, $K = F_q$ with degree 3 was practically established in [25], where the degrees of polynomial graph based public key maps were evaluated. But group theoretical language was not used there and the problem of the key exchange was not considered.

Those results are based on the construction of the family $D(n, q)$ of graphs with large girth and the descryption of their connected components $CD(n, q)$. The existence of infinite families of graphs of large girth had been proven by Paul Erdös' (see [2]). Together with famous Ramanujan graphs introduced by G. Margulis [14] and investigated in [13] graphs $CD(n, q)$ is one of the first explicit constructions of such a families with unbounded degree. Graphs $D(n, q)$ had been used for the construction of LDPS codes and turbocodes which were used in real satellite communications (see [5], [6], [7]), for the development of private key encryption algorithms [21],[22], [17],[9], the option to use them for public key cryptography was considered in [20], [19] and in [18] , where the related dynamical system had been introduced (see also surveys [23], [24]).

The computer simulation show that stable subgroups related to $D(n, q)$ contain elements of very large order but our theoretical linear bounds on the order are relatively weak. We hope to improve this gap in future and justify the use of $D(n, q)$ for the key exchange.

First family of stable groups were obtained via studies of simple algebraic graphs defined over F_q. For new constructions of stable groups over commutative ring K we use directed graphs with the special colouring. The main result of the paper is the following statement.

Theorem 1. *For each commutative ring K with at least 3 regular elements there are families Q_n of Cremona group $C(K^n)$ of degrees 4 such that the projective limit Q of Q_n, $n \to \infty$ is well defined, the group Q is of infinite order, it contains elements g of infinite order, such that there exists a sequence $g_n \in Q_n$ $n \to \infty$ of stable elements such that* $\lim g_n = g$.

The family Q_n is obtained via explicit constructions. So we may use in the finite ring K with at least 3 regular elements the sequence equivalent to g_n for the key exchange. We show that the growth of the order of g_n when n is growing can be bounded from below by some linear function $\alpha \times n + \beta$. In case of such a sequences of groups $G_n = Q_n$ or $G_n = T_n$ we can modify a sequence g_i of elements of stable degree by conjugation with $h_i \in G_i$. New sequence $d_i = {h_i}^{-1} g_i h_i$ can be also a sequence of elements of stable degree.

Let us discuss the asymmetry of our modified Diffie-Hellman algorithms of the key exchange in details. Correspondents Alice and Bob are in different shoes. Alice chooses dimension n, element g_n as in theorem above, element $h \in Q_n$ and affine transformation $\tau \in AGL_n(K)$. So she obtains the base $b = \tau^{-1} h^{-1} g_n h \tau$ and sends it in the form of standard polynomial map to Bob.

Our groups Q_n are defined by the set of their generators and Alice can compute words $h^{-1} g_n h$, b and its powers very fast. So Alice chooses rather large number n_A computes $c_A = b^{n_A}$ and sends it to Bob. At his turn Bob chooses own key n_B computes $c_B = b^{n_B}$. He and Alice are getting the collision map c as ${c_A}^{n_B}$ and ${c_B}^{n_A}$, respectively.

Remark Notice that the adversary is in the same shoes with public user Bob. He (or she) need to solve one of the equations $b^x = c_B$ or $b^x = c_A$. The algorithm is implemented in the cases of finite fields and rings Z_m for family of groups Q_n. We present its time evaluation (generation of b and b_A^n by Alice and computation of b_B^c by Bob) in the last section of paper. We continue studies of orders of g_i theoretically and by computer simulation.

The computer simulation show that the number of monomial expressions of kind $x^{i_1} x^{i_2} x^{i_3} x^{i_4}$ with nonzero coefficient is rather close to binomial coefficient C_n^3. So the time of computation b^{n_B}, ${c_B}^{n_A}$ and ${c_A}^{n_B}$ can be evaluated via the complexity of computation of the composition of several general cubical polynomial maps in n variable.

2. Walks on infinite forest $D(q)$ and corresponding groups

2.1. **Graphs and incidence system.** The missing definitions of graph-theoretical concepts which appears in this paper can be found in [2]. All graphs we consider are simple, i.e. undirected without loops and multiple edges. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. A path in G is called *simple* if all its vertices are distinct. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertices u and v (or neighbors). The sequence of distinct vertices $v_0, v_1, \ldots, v_t$, such that $v_i G v_{i+1}$ for $i = 1, \ldots, t-1$ is the pass in the graph. The length of a pass is a number of its edges. The distance $\mathrm{dist}(u, v)$ between two vertices is the length of the shortest pass between them. The diameter of the graph is the maximal distance between two vertices u and v of the graph. Let C_m denote the cycle of length m i.e. the sequence of distinct vertices

$v_0, \ldots, v_m$ such that $v_i G v_{i+1}$, $i = 1, \ldots, m-1$ and $v_m G v_1$. The girth of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G. The degree of vertex v is the number of its neighbors (see [1] or [2]).

The incidence structure is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another is a line. We shall identify I with the simple graph of this incidence relation (bipartite graph). If number of neighbours of each element is finite and depends only from its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [15]). The graph is k-regular if each of its vertex has degree k, where k is a constant. In this section we reformulate results of [10], [11] where the q-regular tree was described in terms of equations over finite field F_q.

Let q be a prime power, and let P and L be two countably infinite 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 adopt the notation for coordinates of points and lines introduced in [14]:

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \ldots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \ldots),$$
$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \ldots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \ldots).$$

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:

$$\begin{aligned} l_{11} - p_{11} &= l_1 p_1 \\ l_{12} - p_{12} &= l_{11} p_1 \\ l_{21} - p_{21} &= l_1 p_{11} \\ l_{ii} - p_{ii} &= l_1 p_{i-1,i} \\ l'_{ii} - p'_{ii} &= l_{i,i-1} p_1 \\ l_{i,i+1} - p_{i,i+1} &= l_{ii} p_1 \\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{ii} \end{aligned} \tag{1}$$

(The last four relations are defined for $i \geq 2$.) This incidence structure (P, L, I) we denote as $D(q)$. We speak now of the *incidence graph* of (P, L, I), which has the vertex set $P \cup L$ and edge set consisting of all pairs $\{(p), [l]\}$ for which $(p)I[l]$.

To facilitate notation in future results, it will be convenient for us to define $p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{0,0} = l_{0,0} = -1$, $p'_{0,0} = l'_{0,0} = 1$, $p_{0,1} = p_2$, $l_{1,0} = l_1$, $l'_{1,1} = l_{1,1}$, $p'_{1,1} = p_{1,1}$, and to rewrite (1) in the form :

$$\begin{aligned} l_{ii} - p_{ii} &= l_1 p_{i-1,i} \\ l'_{ii} - p'_{ii} &= l_{i,i-1} p_1 \\ l_{i,i+1} - p_{i,i+1} &= l_{ii} p_1 \\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{ii} \end{aligned}$$

for $i = 0, 1, 2, \ldots$

Notice that for $i = 0$, the four conditions (1) are satisfied by every point and line, and, for $i = 1$, the first two equations coincide and give $l_{1,1} - p_{1,1} = l_1 p_1$.

For each positive integer $k \geq 2$ we obtain an incidence structure (P_k, L_k, I_k) as follows. First, P_k and L_k are obtained from P and L, respectively, by simply projecting each vector onto its k initial coordinates. The incidence I_k is then defined by imposing the first k–1 incidence relations and ignoring all others. For fixed q, the incidence graph corresponding to the structure (P_k, L_k, I_k) is denoted by $D(k, q)$. It is convenient to define $D(1, q)$ to be equal to $D(2, q)$. The properties of the graphs $D(k, q)$ that we are concerned with described in the following proposition.

Theorem 2 (11)**.** *Let q be a prime power, and $k \geq 2$. Then*
(i) $D(k, q)$ is a q-regular edge-transitive bipartite graph of order $2q^k$;
(ii) for odd k, $g(D(k, q)) \geq k + 5$, for even k, $g(D(k, q)) \geq k + 4$.

We have a natural one to one correspondence between the coordinates $2, 3, \ldots, n, \ldots$ of tuples (points or lines) and equations. It is convenient for us to rename by $i + 2$ the coordinate which corresponds to the equation with the number i and write $[l] = [l_1, l_3, \ldots, l_n, \ldots]$ and $(p) = (p_1, p_3, \ldots, p_n, \ldots)$ (line and point in "natural coordinates").

Let η_i be the map "deleting all coordinates with numbers $> i$" from $D(q)$ to $D(i, q)$, and $\eta_{i,j}$ be map "deleting all coordinates with numbers $> i$ " from $D(j, q)$, $j > i$ into $D(i, q)$.

The following statement follows directly from the definitions:

Proposition 1. *([11]) The projective limit of $D(i, q), \eta_{i,j}$, $i \to \infty$ is an an infinite forest $D(q)$.*

Let us consider the description of connected components of the graphs.

Let $k \geq 6$, $t = [(k + 2)/4]$, and let $u = (u_i, u_{11}, \cdots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \cdots)$ be a vertex of $D(k, q)$. (It does not matter whether u is a point or a line). For every r, $2 \leq r \leq t$, let

$a_r = a_r(u) = \sum_{i=0,m} (u_{ii} u'_{r-i,r-i} - u_{i,i+1} u_{r-i,r-i-1})$,

and $a = a(u) = (a_2, a_3, \cdots, a_t)$. (Here we define

$p_{0,-1} = l_{0,-1} = p_{1,0} = l_{0,1} = 0$, $p_{00} = l_{00} = -1$, $p_{0,1} = p_1$, $l_{1,0} = l_1$, $l'_{11} = l_{11}$, $p'_{1,1} = p_{1,1}$).

In [10] the following statement was proved.

Proposition 2. *. Let u and v be vertices from the same component of $D(k, q)$. Then $a(u) = a(v)$. Moreover, for any $t-1$ field elements $x_i \in GF(q)$, $2 \leq it \geq [(k+2)/4]$, there exists a vertex v of $D(k, q)$ for which*
$a(v) = (x_2, \ldots, x_t) = (x)$.

Let us consider the following equivalence relation $\tau : u\tau v$ iff $a(u) = a(v)$ on the set $P \cup L$ of vertices of $D(k, q)$ $(D(q))$. The equivalence class of τ containing the vertex v satisfying $a(v) = (x)$ can be considered as the set of vertices for the induced subgraph $EQ_{(x)}(k, q)$ $(EQ_{(x)}(q))$ of the graph $D(k, q)$ (respectively, $D(q)$). When $(x) = (0, \ldots, 0)$, we will omit the index v and write simply $EQ(k, q)$.

Let $CD(q)$ be the connected component of $D(q)$ which contains $(0, 0, \ldots)$. Let τ' be an equivalence relation on $V(D(k, K))$ $(D(q))$ such that the equivalences classes are the totality of connected components of this graph. Obviously $u\tau v$ implies $u\tau' v$. If char $GF(q)$ is an odd number, the converse of the last proposition is true (see [24] and further references).

Proposition 3. *Let q be an odd number. Vertices u and v of $D(q)$ $(D(k,q))$ belong to the same connected component iff $a(u) = a(v)$, i.e., $\tau = \tau'$ and $EQ(q) = CD(q)$ $(EQ(k,q) = CD(k,q))$.*

The condition $charGF(q) \neq 2$ in the last proposition is essential. For instance, the graph $EQ(k,4))$, $k > 3$, contains 2 isomorphic connected components. Clearly $EQ(k,2)$ is a union of cycles $CD(k,2)$. Thus neither $EQ(k,2)$ nor $CD(k,2)$ is an interesting family of graphs of high girth. But the case of graphs $EQ(k,q)$, q is a power of 2, $q > 2$ is very important for coding theory.

Corollary 1. *Let us consider a general vertex*

$$x = (x_j, x_{1,1}, x_{2,1}, x_{1,2} \ldots, x_{i,i}, x_{i,i}^{'}, x_{i+1,i}, x_{i,i+1}, \ldots),$$

$j = 1$ or 2, $i = 2, 3, \ldots$ of the connected component $CD(k,F)$, which contains a chosen vertex v. Then coordinates $x_{i,i}$, $x_{i,i+1}$, $x_{i+1,i}$ can be chosen independently as "free parameters" from F and $x'_{i,i}$ could be computed consequently as the unique solutions of the equations $a_i(x) = a_i(v)$, $i = 1, \ldots$.

3. On the regular directed graph with special colouring

Directed graph - an irreflexive binary relation $\phi \subset V \times V$, where V is the set of vertices.

Let introduce two sets

$$id(v) = \{x \in V | (a,x) \in \phi\},$$
$$od(v) = \{x \in V | (x,a) \in \phi\}$$

as sets of inputs and outputs of vertex v. Regularity means the cardinality of these two sets (input or output degree) are the same for each vertex.

Let Γ be regular directed graph, $E(\Gamma)$ be the set of arrows of graph Γ. Let us assume that additionally we have a colouring function i.e. the map $\pi : E \to M$ onto set of colours M such that for each vertex $v \in V$ and $\alpha \in M$ there exist unique neighbor $u \in V$ with property $\pi((v,u)) = \alpha$ and the operator $N_a(v) := N(a,v)$ of taking the neighbor u of a vertex v within the arrow $v \to u$ of colour α i a bijection. In this case we refer to Γ as *rainbow like graph.*

For each string of colours $(\alpha_1, \alpha_2, \ldots, \alpha_m)$, $\alpha_i \in M$ we can generate a permutation π which is a composition $N_{\alpha_1} \times N_{\alpha_2} \times \cdots \times N_{\alpha_m}$ of bijective maps $N_{\alpha_i} : V(\Gamma) \to V(\Gamma)$. Let us assume that the map $u \to N_\alpha(u)$ is a bijection. For given vertex $v \in V(\Gamma)$ the computation π corresponds to the chain in the graph:

$$v \to v_1 = N(\alpha_1, v) \to v_2 = N(\alpha_2, v_1) \to \cdots \to v_n = N(\alpha_m, v_{m-1}) = v'.$$

Let G_π be the group generated by permutations π as above.

Let us consider the following graph (triple graph defined in terms of $D(n,K)$ (or $D(K)$). Let F_1 be the totality of all walks of length 3 in $D(n,K)$ of kind $u = (p_1)I[l]I(p_2)$. We consider similar variety F_2 of triples $[l_1](p)[l_2]$ Now we define the relation between vertices of the new graph:

$$\langle (p^1), [l], (p^2) \rangle R \{[l'^1], (p'), [l'^2]\} \Leftrightarrow$$
$$\Leftrightarrow [l] = [l'^1] \ \& \ (p^2) = (p') \ \& \ l'^2_{0,1} - p^2{}_{1,0} \in RegK$$

$$\{[l^1], (p), [l^2]\} R \langle (p'^1), [l'], (p'^2) \rangle \Leftrightarrow$$
$$\Leftrightarrow (p) = (p'^1) \ \& \ [l^2] = [l'] \ \& \ p'^2_{1,0} - l^2_{0,1} \in RegK$$

The colour of the arrow between $u = (p^1)I[l]I(p^2)$ and $u' = [l]I(p^2)I[l']$ is $l'_{0,1} - {p^2}_{1,0}$. Similarly the colour of the arrow between $u' = [l]I(p)I[l']$ and $u = (p)I[l'](p')$ is $p'_{1,0} - l'_{0,1}$. We define rainbow like colouring π.

Let us consider the permutation group $TF'_n(K)$ ($TF'(K)$) acting on $F_1 = K^{n+2}$ (K^∞, respectively) corresponding to the triple graph with the colouring π. Let $TF_n(K)$ ($TF(K)$) be the subgroup of products of even number of generators.

Theorem 3. *Sequence of subgroups $TF_n(K)$ of Cremona group $C_n(K)$ form a family of subgroups of degree 4.*

Proof. To find a family of subgroups of degree 4 we give a construction of triple directed graph. To this eend we would like to connect three vertices of the graph defined in section 2 to get two sets of vertices of new graph:

$$F = \left\{\langle (p^1), [l], (p^2)\rangle \mid (p^1)I[l]I(p^2)\right\}$$

$$F^{'} = \left\{\{[l^1], (p), [l^2]\} \mid [l^1]I(p)I[l^2]\right\}.$$

Now we have the following relation between vertices of the new graph:

$$\langle (p^1), [l], (p^2)\rangle R\{[l'^1], (p'), [l'^2]\} \Leftrightarrow$$

$$\Leftrightarrow [l] = [l'^1] \ \&\ (p^2) = (p') \ \&\ {l'}^2_{0,1} - {p^2}_{1,0} \in RegK$$

$$\{[l^1], (p), [l^2]\} R\langle (p'^1), [l'], (p'^2)\rangle \Leftrightarrow$$

$$\Leftrightarrow (p) = (p'^1) \ \&\ [l^2] = [l'] \ \&\ {p'}^2_{1,0} - l^2_{0,1} \in RegK$$

Using induction we can see that in steps (2k) and (2k+1) we get vertices with corresponding degrees:

$$\langle (p^{2k-2}), [l^{2k-1}], (p^{2k})\rangle =$$

$$= (p_{1,0}+\alpha_1+\ldots+\alpha_{(2k-3)}, p_{1,1}, \ldots, p_{i,j}, l^2_{0,1}+\alpha_2+\ldots+\alpha_{(2k-2)}, p_{1,0}+\alpha_1+\ldots+\alpha_{(2k-1)}),$$

$$\{[l^{2k-1}], (p^{2k}), [l^{2k+1}]\} =$$

$$= (l^2_{0,1}+\alpha_2+\ldots+\alpha_{(2k-2)}, l_{1,1}, \ldots, l_{i,j}, p_{1,0}+\alpha_1+\ldots+\alpha_{(2k-1)}, l^2_{0,1}+\alpha_2+\ldots+\alpha_{(2k)})$$

where

$$\deg p^{(2k)}_{i,j}(l_1, l_2, \ldots, l_k, p_1, l_12) = \begin{cases} 3, & (i,j) = (i,i)^{'} \text{ or } (i,j) = (i,i+1), \\ 4, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i) \end{cases}$$

and

$$\deg l^{(2k+1)}_{i,j}(l_1, l_2, \ldots, l_k, p_1, l_12) = \begin{cases} 4, & (i,j) = (i,i)^{'} \text{ or } (i,j) = (i,i+1), \\ 3, & (i,j) = (i,i) \text{ or } (i,j) = (i+1,i) \end{cases}$$

Finally using the affine transformation in the same way as in [25], independently from the length of the password we get the polynomials of degree 4. □

Canonical graph homomorphisms $D(n,K) \to D(n-1,K)$ can be naturally expanded to group homomorphism $TF_{n+2}(K)$ onto $TF_{n+1}(K)$. It means that group $TF(K)$ is a projective limit of $TF_n(K)$. Let δ_n be a canonical homomorphism of $TF(K)$ onto $TF_n(K)$.

Proposition 4. *The order of a product g of generators $s_{\alpha,\beta}$ of $TF(K)$, such that α and β are elements of* Reg(K) *is infinity. Let $g \in CD(K)$ be an element of length $l(g) = k$, then the order of $g_n = \delta_n(g)$, where $[n+5]/2 \geq k$, is bounded below by $[n+5]/2k$. The sequence g_n forms a family of stable elements.*

That statement follows from the fact that the orbit of g containing triple (0)[0](0) is an infinite set.

So element $h = \tau^{-1}h^{-1}g_n h\tau$, where $\tau \in AGL_n(K)$, $h \in TF_n(k)$ is an element for which $h^{-1}g_n h$ is a cubical map, can be used as the base for Diffie-Hellman algorithm as above.

4. Remarks on the complexity of public rules

The combination T_1NT_2 of graph transformation N with two affine transformations T_1 and T_2 can be used as polynomial public rules. Public user getting a formula:

$$y = (F_1(x_1, \dots, x_n), \dots, F_n(x_1, \dots, x_n)),$$

where $F_i(x_1, \dots, x_n)$ are polynomials of n variables of degree 4.

Hence the process of straightforward encryption can be done in polynomial time $O(n^5)$. 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 4. We know that the variety of solution has the dimension 0. So general algorithm for finding the solution of system of polynomials cubic equations has exponential time $4^{O(n)}$.

References

[1] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73–80.

[2] B. Bollobás, *Extremal Graph Theory*, Academic Press,

[3] Neal Coblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer, 1994, 237 p.

[4] Neal Coblitz, *Algebraic Aspects of Cryptography*, Springer, 1998, 198 p.

[5] , 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.

[6] 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.

[7] Jon-Lark Kim, U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, *Explicit construction of families of LDPC codes with no 4-cycles* , Information Theory, IEEE Transactions, 2004, v. 50, Issue 10, 2378 - 2388.

[8] M. Klissowski, V. Ustimenko, *On the implementation of public keys algorithms based on algebraic graphs over finite commutative rings*, Proceedings of International CANA conference, Wisla, 2010.

[9] S. Kotorowicz, V. Ustimenko, *On the implementation of cryptoalgorithms based on algebraic graphs over some commutative rings*, Condensed Matter Physics, 2008, vol. 11, No. 2(54), (2008) 347–360.

[10] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, *A Characterization of the Components of the graphs $D(k, q)$*, Discrete Mathematics, 157 (1996) 271–283.

[11] 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.

[12] 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.

[13] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.

[14] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.

[15] E. H. Moore, *Tactical Memoranda*, Amer. J. Math., v.18, 1886, 264-303.

[16] B. Mortimer, *Permutation groups containing affine transformations of the same degree*, J. London Math. Soc., 1972, 15, N3, 445-455.

[17] V. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.

[18] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.

[19] 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).

[20] V. A. Ustimenko, *Maximality of affine group, and hidden graph cryptosystems*, J. Algebra and Discrete Math., 10 (October 2004), 51-65.

[21] 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.

[22] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer,2001, v. 2227, 278-287.

[23] 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).

[24] V. A. Ustimenko, *On the cryptographical properties of extremal algebraic graphs*, in Algebraic Aspects of Digital Communications, NATO Science for Peace and Security Series - D: Information and Communication Security, Volume 24, July 2009, 296 pp.

[25] A. Wroblewska *On some properties of graph based public keys* , Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234 p.

Maria Curie-Sklodowska University in Lublin (Poland)
E-mail address: ustymenko_vasyl@yahoo.com, awroblewska@hektor.umcs.lublin.pl

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 171–179
ISSN 1930-1235: (2010)

A PARALLEL ALGORITHM FOR ANALYTICAL SOLVING OF PARTIAL DIFFERENTIAL EQUATIONS SYSTEMS.

NATALIA MALASCHONOK

Abstract. There is produced a parallel algorithm for symbolic solving systems of partial differential equations by means of multivariate Laplace-Carson transform. There is considered a system of n equations with m as the greatest order of partial derivatives and right hand parts of a special type. Initial and conditions are input. As a result of Laplace-Carson transform of the system according to initial condition we obtain an algebraic system of equations. A method to obtain compatibility conditions is discussed.

1. Introduction

The Laplace and Laplace–Carson transform is useful in many problems of solving differential equations (for example [1, 2, 4]) It reduces a system of partial differential equations to an algebraic linear system with polynomial coefficients. Parallel algorithms for solving such systems are being developed actively (for example, [5, 3]). It enables to construct parallel algorithms for solving linear partial differential equations with constant coefficients and systems of equations of various order, size and types. The application of Laplace–Carson transform permits to obtain compatibility conditions in symbolic way for many types of PDE equations and systems of PDE equations.

2. Problem statement

Denote $\widetilde{m} = (m_1, \ldots, m_n)$. Consider a system

$$\sum_{k=1}^{K} \sum_{m=0}^{M} \sum_{\widetilde{m}} a^j_{\widetilde{m}k} \frac{\partial^m}{\partial^{m_1} x_1 \ldots \partial^{m_n} x_n} u_k(x) = f_j(x), \tag{1}$$

where $j = 1, \ldots, K$, $u_k(x)$, $k = 1, \ldots, K$, — are unknown functions of $x = (x_1, \ldots, x_n) \in \mathbf{R}^n_+$, $f_j \in S$, $a^j_{\widetilde{m}k}$ are real numbers, m is the order of a derivative, and k –the number of an unknown function. Here and further summing by $\widetilde{m} = (m_1, \ldots, m_n)$ is executed for $m_1 + \ldots + m_n = m$.

We consider all input functions reducible to the form;

$f_j(t) = f^i_j(x)$, $x^i_j < t < t^{i+1}_j$, $i = 1, \ldots, I_j, x^1_l = 0, t^{I_j+1}_j = \infty$,

where

$$f^i_j(t) = \sum_{s=1}^{S^i_j} P^i_{js}(t) e^{b^i_{js} t}, \quad i = 1, \ldots, I_j, \quad j = 1, \ldots, k, \tag{2}$$

Supported by RFBR, No.05-01-00074a, the Sci. Program "Devel. Sci. Potent. High. School", RNP.2.1.1.351.

and $P^i_{js}(x) = \sum_{l=0}^{L^i_{j_s}} c^{ji}_{sl} x^l$.

Denote by **A** a class of functions which are reducible to the form (2).

We solve a problem with initial conditions for each variable. Introduce notations for them. Denote by Γ^ν a set of vectors $\gamma = (\gamma_1, \ldots, \gamma_n)$ such that $\gamma_\nu = 1$, $\gamma_i = 0$, if $i < \nu$, and γ_i equals 0 or 1 in all possible combinations for $i > \nu$. The number of elements in Γ^ν equals $2^{\nu-1}$.

Denote $\beta = (\beta_1, \ldots, \beta_n)$, $\beta_i = 0, \ldots, m_i$, a set of indexes such that the derivative of $u^k(x)$ of the order β_i with respect to the variables with numbers i equals $u^k_{\beta,\gamma}(x^{(\gamma)})$ at the point $x = x^\gamma$ with zeros at the positions μ for which the coordinates γ_μ of γ equal 1. For example, if zeros stand only at the places with the numbers $1, 2, 3$, then $\gamma = (1, 1, 1, 0, \ldots, 0)$. Functions $u^k_{\beta,\gamma}(x^{(\gamma)})$ must also belong to **A**. To be short we shall not write down the expressions for $u^k_{\beta,\Gamma}(x^{(\gamma)})$.

The algorithm component is the definition of compatible initial conditions. The system (1) is to be solved under such conditions.

Data file contains the coefficients, the initial conditions and the right-hand members f_j,
$l = 1, \ldots, K$.

The data for functions f_j consists of the polynomial coefficients, parameters of exponents, the bounds of smoothness intervals.

3. Laplace–Carson transform

Consider the space S of functions $f(x)$, $x = (x_1, \ldots, x_n) \in \mathbf{R}^n_+$, $\mathbf{R}^n_+ = \{x : x_i \geq 0, i = 1, \ldots, n\}$, for which $\mathcal{M} > 0, a = (a_1, \ldots, a_n) \in \mathbf{R}^n$, $a_i > 0$, $i = 1, \ldots, n$, exist such that for all $x \in \mathbf{R}^n_+$ the following is true: $|f(x)| \leq \mathcal{M} e^{ax}$, $ax = \sum\limits_{i=1}^{n} a_i x_i$.

On the space S the Laplace–Carson transform (**LC**) is defined as follows:

$$LC : f(x) \mapsto F(p) = p^1 \int_0^\infty e^{-px} f(x) dx,$$

$$p = (p_1, \ldots, p_n), \quad p^1 = p_1 \ldots p_n,$$

$$px = \sum_{i=1}^{n} p_i x_i, \quad dx = dx_1 \ldots dx_n.$$

LC is performed symbolically at the class **A**.

4. Parallel Laplace–Carson algorithm

The steps, at which parallel calculations are possible and reasonable we denote by term **Block**. If indexes are contained, the ways of parallelization are pointed by them.

4.1. **LC of a system.** Let $LC : u^k \mapsto U^k, u^k_{\beta,\gamma}(x^{(\gamma)}) \mapsto U^k_{\beta,\gamma}(p^{(\gamma)}), f_j \mapsto F_j$, the notation $p^{(\gamma)}$ is correspondent to the notation $x^{(\gamma)}$. Denote by $\|\gamma\|$ the "length" of γ — the number of units in γ, $p^{\widetilde{m}} = p_1^{m_1} \ldots p_n^{m_n}$.

Block 10

The LC of the left-hand side of the system (1) excluding images of initial conditions is written formally.

Block 1r

r runs trough the set of multiindexes of $u^k_{\beta,\Gamma}(x^\Gamma)$.

Then

$$LC: \frac{\partial^m}{\partial^{m_1}x_1\dots\partial^{m_n}x_n}u_k(x) \ \mapsto$$

$$p^{\widetilde{m}}U^k(p) \ + \sum_{\nu=1}^{n}\sum_{\beta_\nu=0}^{m_\nu}\sum_{\gamma\in\Gamma^\nu}(-1)^{\|\gamma\|}p_1^{m_1-\beta_1-\gamma_1}\dots p_n^{m_n-\beta_n-\gamma_n}U^k_{\beta,\gamma}(p^{(\gamma)}).$$

Denote

$$\Phi^j_{mk}=\sum_{\widetilde{m}}a^j_{\widetilde{m}k}\sum_{\nu=1}^{n}\sum_{\beta_\nu=0}^{m_\nu}\sum_{\gamma\in\Gamma^\nu}(-1)^{\|\gamma\|}p_1^{m_1-\beta_1-\gamma_1}\dots p_n^{m_n-\beta_n-\gamma_n}U^k_{\beta,\gamma}(p^{(\gamma)}).$$

As a result of Laplace–Carson transform of the system (1) according to initial conditions we obtain an algebraic system relative to U^k

$$\sum_{k=1}^{K}\sum_{m=0}^{M}\sum_{\widetilde{m}}a^j_{\widetilde{m}k}p^{\widetilde{m}}U^k(p)=F_j-\sum_{k=1}^{K}\sum_{m=0}^{M}\Phi^j_{mk}, j=1,\dots,K. \tag{3}$$

Block 2k

k runs from 1 to K.

These blocks performs LC of the right-hand parts of (1). The properties of **A** allow a further parallelization of calculations.

4.2. **Solution of algebraic system. Block 3**

As a result of Laplace–Carson transform of the system (1) according to initial conditions we obtain the algebraic system (3) relative to U^k.

Efficient methods of parallel solving such systems are developed (for example [5], [3]).

At this stage the problem of definition of compatibility conditions arises (see blocks 4s,5). With respect to compatible conditions we use the inverse Laplace–Carson transform and obtain the correct solution of PDE system.

4.3. **Compatibility conditions.** Call a rational fraction *"a proper fraction"* if the degree of each variable (over **C**) in numerator is less then its degree in denominator.

Call by the class **B** a set of equations, defined by conditions

• the solutions of algebraic system may be represented as sums of proper fractions with exponential coefficients,

• the denominators of these proper fractions may be reduced to a product of linear functions.

.

The class **B** admits symbolic implementation of further calculations.

Denote by D the determinant of the system (3), D_i the maximal order minors of the extended matrix of (3). A case when there is a set $\mathcal{Q}$ of zeros of D with infinite limit point at $\operatorname{Re} p_k > 0$, $k=1,\dots,n$, is of most interest. Solving the system (1) we obtain U^k as fractions with D in the denominators. The inverse Laplace–Carson transform is possible if α_k, $k=1,\dots,n$, exist such that these functions are holomorphic in the domain $\operatorname{Re} p_k > \alpha_k$. So we make a demand: D_i has zeros at $\mathcal{Q}$ of multiplicity not less than multiplicity of corresponding zeros of D. This demand produces requirements to the LC images of initial conditions functions, and after

LC^{-1} transform – to initial conditions. They turn to be dependent. We obtain the so-called compatibility conditions.

Block 4s
s depends upon the number of relations, from which the compatibility conditions arise.

The blocks calculate the values of numerators at zeros of denominators.

Block 5

The block implements parallel solving of the system of equations, produced by relations for compatibility conditions.

Block 6k

The blocks perform the LC^{-1} of U^k. Note, that the steps of calculation of multivariate LC^{-1} are produced sequentially.

5. Examples

5.1. **Example 1.** To demonstrate the LC algorithm let us consider in details solving of a system of three equations with three unknown functions $f(x,y,z)$, $g(x,y,z)$, $h(x,y,z)$ on $\mathbf{R}^3_+$.

$$\begin{array}{rcl} \frac{\partial}{\partial x}f + \frac{\partial}{\partial z}g + \frac{\partial}{\partial y}h & = & x \\ \frac{\partial}{\partial z}f + \frac{\partial}{\partial x}g + \frac{\partial}{\partial y}h & = & y \\ \frac{\partial}{\partial y}f + \frac{\partial}{\partial x}g + \frac{\partial}{\partial z}h & = & z \end{array} \tag{1}$$

We shall consider the problem when values of unknown function at zeros of x, y, z are taken as initial conditions.

As we have the derivatives of the first order with respect to each variable we need nine initial conditions – three for every unknown function – at $(0,y,z)$, $(x,0,z)$, $(x,y,0)$, correspondingly to the order of the derivative. A requirement is a coincidence of correspondent functions values at the intersection of these planes.

Block 1r , r=1,2,3.

Denote values of functions at these points as follows:

$$\begin{array}{lll} f(0,y,z) = f^x, & g(0,y,z) = g^x, & h(0,y,z) = h^x, \\ f(x,0,z) = f^y, & g(x,0,z) = g^y, & h(x,0,z) = h^y, \\ f(x,y,0) = f^z, & g(x,y,0) = g^z, & h(x,y,0) = h^z. \end{array}$$

Denote the images of LC transform of f, g, h, respectively by u, v, w.

To be transparent in the example we denote LC images of the initial conditions functions by nine various Greek letters $\alpha, \beta, \gamma, \delta, \delta, \varepsilon, \xi, \tau, \sigma$, correspondingly:

	(q,r)	(p,r)	(p,q)
f	α	η	δ
g	ε	ξ	β
h	τ	γ	σ

Table 1

In the table the first column points the functions for which the LC images of the initial conditions are considered, the first line indicates the variables upon which these images depend.

Block 3

Applying the Laplace-Carson transform to the system (1) we obtain the algebraic system

$$\begin{aligned} pu + rv + qw - p\alpha - r\beta - q\gamma &= \tfrac{1}{p},\\ ru + pv + qw - r\delta - p\varepsilon - q\gamma &= \tfrac{1}{q},\\ qu + pv + rw - q\eta - p\varepsilon - r\sigma &= \tfrac{1}{r}. \end{aligned} \tag{2}$$

The solution of this system is

$$u = -\frac{-pq^2 + pqr + qr^2 - r^3}{qr(p-r)(q-r)(p+q+r)} - \frac{(-p^2q^2r + p^2qr^2)\alpha + (-pq^2r^2 + pqr^3)\beta + (pq^2r^2 - q^2r^3)\gamma}{qr(p-r)(q-r)(p+q+r)} - \frac{(pq^2r^2 - qr^4)\delta + (pq^2r^2 - pqr^3)\varepsilon + (-pq^3r + q^3r^2)\eta + (-pq^2r^2 + q^2r^3)\sigma}{qr(p-r)(q-r)(p+q+r)},$$

$$v = -\frac{-p^2q^2 + q^3r + p^2r^2 - qr^3}{pqr(p-r)(q-r)(p+q+r)} - \frac{(p^2q^3r - p^2qr^3)\alpha + (pq^3r^2 - pqr^4)\beta + (p^2q^2r^2 - pq^2r^3)\gamma}{pqr(p-r)(q-r)(p+q+r)} - \frac{(-pq^3r^2 + p^2qr^3)\delta - (p^3q^2r + p^2q^3r - p^3qr^2)\varepsilon}{pqr(p-r)(q-r)(p+q+r)} + \frac{(-p^2q^3r + pq^3r^2)\eta + (-p^2q^2r^2 + pq^2r^3)\sigma}{pqr(p-r)(q-r)(p+q+r)},$$

$$w = \frac{-p^2q + q^2r + p^2r - qr^2}{qr(p-r)(q-r)(p+q+r)} + \frac{(p^2q^2r - p^2qr^2)\alpha + (pq^2r^2 - pqr^3)\beta + (p^2q^2r + pq^3r - pq^2r^2 - q^3r^2)\gamma}{qr(p-r)(q-r)(p+q+r)} + \frac{(-q^2r^3 + p^2qr^2)\delta - (pq^2r^2 - pqr^3)\varepsilon + (-p^2q^2r + q^2r^3)\eta + (-p^2qr^2 + qr^4)\sigma}{qr(p-r)(q-r)(p+q+r)}$$

The determinant D of the system equals

$$D = -(p-r)(q-r)(p+q+r).$$

The bracket $(p+q+r)$ is not important for solving the problem of compatibility – its zeros do not belong to $\mathcal{Q}$.

Block 4s, $s = 1, \ldots, 6$.

Consider the sets $p = r$, $q = r$. We demand the numerators of the solutions be zero on these sets. To indicate that the functions of initial conditions are taken for $p = r$ or $q = r$ we use the notations displaced in the following table. If for a function $p = r$ is put we use this function with the index 1, if there is put $q = r$, we use this function with the index 2. To demonstrate the algorithm of getting compatibility conditions display initial conditions and their transformations after substituting of points of $\mathcal{Q}$ into the table.

	$p=r$	$q=r$
$\alpha(q,r)$	$\alpha(q,r)$	$\alpha_2(q,r)$
$\varepsilon(q,r)$	$\varepsilon(q,r)$	$\varepsilon_2(r,r)$
$\tau(q,r)$	$\tau(q,r)$	$\tau_2(r,r)$
$\theta(p,r)$	$\theta_1(r,r)$	$\theta(p,r)$
$\xi(p,r)$	$\xi_1(r,r)$	$\xi(p,r)$
$\gamma(p,r)$	$\gamma_1(r,r)$	$\gamma(p,r)$
$\delta(p,q)$	$\delta_1(r,q)$	$\delta_2(p,r)$
$\beta(p,q)$	$\beta_1(r,q)$	$\beta_2(p,r)$
$\sigma(p,q)$	$\sigma_1(r,q)$	$\sigma_2(p,r)$

Table 2

Substituting $p=r$ and $q=r$ into the numerators of u, v, w, we obtain a system of 6 equations, that connect functions $\alpha, \beta, \gamma, \delta, \delta, \ldots, \delta_2$.

$$\begin{cases} -rq^2+2qr^2-r^3-(r^3q^2-qr^4)\alpha+(-q^2r^3+qr^4)\beta_1 & + \\ \qquad +(q^2r^3-qr^4)\delta_1+(q^2r^3-qr^4)\varepsilon & = 0 \\ q^3r-q^2r^2-qr^3+r^4+(q^3r^3-qr^5)\alpha+(q^3r^3-qr^5)\beta_1 & - \\ \qquad -(q^3r^3-qr^5)\delta_1-(q^3r^3-qr^5)\varepsilon & = 0 \\ -q^2r+2qr^2-r^3+(-q^2r^3+qr^4)\alpha+(-q^2r^3+qr^4)\beta_1 & + \\ \qquad +(q^2r^3-qr^4)\delta_1+(q^2r^3-qr^4)\varepsilon & = 0 \\ (pr^4-r^5)\gamma+(pr^4-r^5)\delta_2+(-pr^4+r^5)\eta+(-pr^4+r^5)\sigma_2 & = 0 \\ (p^2r^4-pr^5)\gamma+(p^2r^4-pr^5)\delta_2+(-p^2r^4+pr^5)\eta+(-p^2r^4+pr^5)\sigma_2 & = 0 \\ (-p^2r^3+r^5)\gamma+(-p^2r^3+r^5)\delta_2+(p^2r^3-r^5)\eta+(p^2r^3-r^5)\sigma_2 & = 0 \end{cases}$$

Block 5

Solving it with respect to these variables, we get two conditions on them:

$$\begin{array}{rcl} \alpha & = & -\frac{q-r}{qr^2}-\beta_1+\delta_1+\varepsilon, \\ \gamma & = & -\delta_2+\eta+\sigma_2. \end{array} \tag{3}$$

We may take arbitrarily all images of initial conditions except of α and γ and obtain α and γ according to the conditions (3).

For example, we may take the following functions in the table 1.

	(q,r)	(p,r)	(p,q)
f	$-\frac{1}{r^2}+\frac{2}{qr^2}$	$\frac{1}{pr}$	$\frac{1}{p^2q}$
g	$\frac{1}{qr^2}$	$\frac{1}{p^2r}$	$\frac{1}{pq}$
h	$\frac{1}{qr}$	$\frac{1}{pr^2}-\frac{1}{p^2r}+\frac{1}{pr}$	$\frac{1}{pq^2}$

Table 3

The correspondent initial conditions are the follows:

$$f^x=\frac{1}{2}\left(-z^2+2yz\right), \quad g^x=\frac{yz^2}{2}, \quad h^x=yz,$$

$$f^y=xz, \quad g^y=\frac{x^2z}{2}, \quad h^y=\frac{1}{2}\left(2xz-x^2z+xz^2\right),$$

$$f^z=\frac{x^2y}{2}, \quad g^z=xy, \quad h^z=\frac{xy^2}{2}. \tag{4}$$

Block 6k, $k = 1, 2, 3$.

Substituting the functions $\alpha, \beta, \gamma, \dots$ from the table 3 into the solution u, v, w, after inverse LC transform we obtain the solution of the system (1) correspondent to the initial conditions (4):

$$f = 1/6(3x^2y - 6xyz + 6yz^2 - 2z^3 - 3(x-z)^2H(-x+y)H(-x+z)+$$
$$+2(-x+z)^3H(-x+y)H(-x+z) + 6y(y-z)H(-y+z)+$$
$$+6x(-y+z)H(-y+z) + 2(-y+z)^3H(-y+z) + 6x(y-z)H(-x+y)H(-y+z)+$$
$$+2(y-z)^3H(-x+y)H(-y+z) + 6y(-y+z)H(-x+y)H(-y+z));$$
$$g = 1/6(6xy + 6xz - 12xyz + 3z^2 + 3yz^2 - 2z^3 - 3(x-z)^2H(-x+y)H(-x+z)+$$
$$+2(-x+z)^3H(-x+y)H(-x+z) + 6y(y-z)H(-y+z) + 6x(-y+z)H(-y+z)+$$
$$+2(-y+z)^3H(-y+z) + 6x(y-z)H(-x+y)H(-y+z)+$$
$$+2(y-z)^3H(-x+y)H(-y+z) + 6y(-y+z)H(-x+y)H(-y+z));$$
$$h = 1/6(3xy^2 - 3x^2z - 6yz + 3xz^2 + 6yz^2 - 2z^3 - 3(x-z)^2H(-x+y)H(-x+z)+$$
$$+2(-x+z)^3H(-x+y)H(-x+z) + 6y(y-z)H(-y+z) + 6x(-y+z)H(-y+z)+$$
$$+2(-y+z)^3H(-y+z) + 6x(y-z)H(-x+y)H(-y+z)+$$
$$+2(y-z)^3H(-x+y)H(-y+z) + 6y(-y+z)H(-x+y)H(-y+z)),$$

where $H(x)$ is the Heaviside step function.

5.2. **Example 2.** The LC algorithm permits to solve equations of various types and of any order if input functions belong to **A**, and the equation is from the class **B**. To demonstrate the application of the algorithm to an equation of the fourth order let us consider the equation of forced vibration of elastic rod:

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^4 f}{\partial y} = xy.$$

Initial conditions:
$f(0,y) = a(y)$; $\frac{\partial f(x,y)}{\partial x}\big|_{x=0} = b(y)$;
$f(x,0) = c(x)$; $\frac{\partial f(x,y)}{\partial y}\big|_{y=0} = d(x)$;
$\frac{\partial^2 f(x,y)}{\partial y^2}\big|_{y=0} = g(x)$; $\frac{\partial^3 f(x,y)}{\partial y^3}\big|_{y=0} = h(x)$

Block 1 .

$$LC : f(x,y) \mapsto u(p,q),$$

$a(y) \mapsto \alpha(q)$, $b(y) \mapsto \beta(q)$,
$c(x) \mapsto \gamma(p)$, $d(x) \mapsto \delta(p)$,
$g(x) \mapsto \sigma(p)$, $h(x) \mapsto \tau(p)$.

Block 3

As a result of LC we obtain the algebraic equation:

$$p^2u - p^2\alpha - p\beta - qu + q\gamma qu + q\gamma = \frac{1}{pq}$$

$D = p^2 + q^2$

Then

$$u = \frac{1 + p^3q\alpha + p^2q\beta + pq^5\gamma + pq^4\delta + pq^3\sigma + pq^2\tau}{pq(p^2+q^4)};.$$

Block 4s , $s = 1, 2$.

There are two Q sets of zeros of the denominator

$$D = p^2 + q^2,$$

these sets are defined by the conditions

$p = iq^2$, $p = -iq^2$.

At this sets the numerator of u equals correspondingly

$$A1 = 1 - iq^7\alpha - q^5\beta + iq^7\gamma_1 + iq^6\delta_1 + iq^5\sigma_1 + iq^4\tau_1;$$
$$A2 = 1 + iq^7\alpha - q^5\beta - iq^7\gamma_2 - iq^6\delta_2 - iq^5\sigma_2 - iq^4\tau_2,$$

where

$\gamma_1,\ \delta_1,\ \sigma_1,\ \tau_1$

are the values of functions $\gamma,\ \delta,\ \sigma,\ \tau$ at $p = iq^2$,

$\gamma_1,\ \delta_1,\ \sigma_1,\ \tau_1$

– at $p = iq^2$.

The functions with indexes 1 and 2 depend on different arguments iq^2 and $-iq^2$, correspondingly. So it is convenient to take the originals c, d, g, h of $\gamma,\ \delta,\ \sigma,\ \tau$ as data functions of initial conditions and to find a, b as compatible with them. Note that this is a characteristic speciality of equations of such type, for example of elliptic equations.

Solve

$$\begin{cases} A1 &= 0, \\ A2 &= 0 \end{cases}$$

with respect to α, β.

Block 5 ,

Compatibility conditions on images of LC:

$$\alpha = -\frac{-q^3\gamma_1 - q^3\gamma_2 - q^2\delta_1 - q^2\delta_2 - q\sigma_1 - q\sigma_2 - \tau_1 - \tau_2}{2q^3};$$

$$\beta = \frac{i(-2i + q^7\gamma_1 - q^7\gamma_2 + q^6\delta_1 - q^6\delta_2 + q^5\sigma_1 - q^5\sigma_2 + q^4\tau_1 - q^4\tau_2)}{2q^5}.$$

Taking concrete functions $c(t), d(t), g(t), h(t)$ of initial conditions, we obtain $a(x)$ and $b(x)$ as compatible with them. In such way we may define, for example, the following compatible initial conditions:

$a = 1 - \frac{x^4}{12},\ b = \frac{x^5}{120}, c = 1 + t^2$.

Finally we obtain the solution satisfying the initial conditions:

$$f(t, x) = 1 + t^2 - \frac{x^4}{12} + \frac{tx^5}{120}.$$

References

[1] Dahiya R.S., Jabar Saberi-Nadjafi: Theorems on n-dimensional Laplace transforms and their applications. 15th Annual Conf. of Applied Math., Univ. of Central Oklahoma, Electr. Journ. of Differential Equations, Conf.02 (1999) 61-74

[2] I.Dimovski, M.Spiridonova. Computational approach to nonlocal boundary value problems by multivariate operational calculus. Mathem. Sciences Research Journal, ISSN 1537-5978, Dec.2005, V.9, No.12, 315-329.

[3] *Malaschonok G.I.* Parallel Algorithms of Computer Algebra // Materials of the conference dedicated for the 75 years of the Mathematical and Physical Dep. of Tambov State University. (November 22-24, 2005). Tambov: TSU, 2005. P. 44-56.

[4] Malaschonok N.: Parallel Laplace Method with Assured Accuracy for Solutions of Differential Equations by symbolic computations. In: Computer Algebra and Scientific Computing, CASC 2006, LNCS 4196, Springer, Berlin (2006) 251-261

[5] *Watt S.M.* Pivot-Free Block Matrix Inversion, Proc 8th International Symposium on Symbolic and Numeric Algorithms in Symbolic Computation (SYNASC), IEEE Computer Society, 2006. P. 151-155. URL: http://www.csd.uwo.ca/ watt/pub/reprints/2006-synasc-bminv.pdf.

Tambov State University, Internatsionalnaya 33, 392622 Tambov, Russia
E-mail address: nmalaschonok@yandex.ru

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 181–193
ISSN 1930-1235: (2010)

CONVERSION BETWEEN HERMITE AND POPOV NORMAL FORMS USING AN FGLM-LIKE APPROACH

JOHANNES MIDDEKE

Abstract. We are working with matrices over a ring $K[\partial;\sigma,\vartheta]$ of Ore polynomials over a skew field K. Extending a result of [18] for usual polynomials it is shown that in this setting the Hermite and Popov normal forms correspond to Gröbner bases with respect to certain orders. The FGLM algorithm is adapted to this setting and used for converting Popov forms into Hermite forms and vice versa. The approach works for arbitrary, that is, not necessarily square matrices where we establish termination criteria to deal with infinitely dimensional factor spaces.

1. Introduction

Since long, normal forms have played a prominent rôle in those branches of mathematics that involve the study of equational systems. Among these, polynomial systems form a major subclass. But also systems of ordinary linear equations are important for applications. Usually, these systems are modelled by matrices. The computation of normal forms can answer some important questions about the structure of the underlying system.

Linear systems can be represented by matrices with entries being linear operators. In this paper we will consider Ore polynomials—which some authors also call skew polynomials. This is a class of non-commutative polynomials that was introduced by Øystein Ore in [21]. They are a generalisation of the ordinary (commutative) polynomials that includes linear differential operators and shift operators.

We will tread Ore polynomials in section 2. There we will also introduce some notations for matrices that are used in later sections.

Among those normal forms that are used in practise, we will concentrate on the Hermite and Popov forms. These are both one-sided normal forms, that is, normal forms with respect to elementary row operations. Invented by Charles Hermite in [14], the Hermite form was originally a row echelon form for square matrices over the integers. It has later been extended to non-square matrices and other domains.

The Popov normal form was introduced by Vasile Mihai Popov in [22, 23]. It is related to row-reduction—a concept that has been described by [12] for commutative polynomials. We will give definitions for this forms in section 3.

Gröbner bases were first considered in Bruno Buchberger's PhD thesis [4]—named after his advisor Wolfgang Gröbner. They are very useful to solve problems

Key words and phrases. 15B33, 34M03, 47B39 .

This work was supported by the Austrian Science Foundation (FWF) under the project DIFFOP (P20 336-N18).

that are related to polynomial ideals algorithmically, most importantly the solving of polynomial equations and the ideal membership problem.

It is possible to define Gröbner bases for modules—see, for example, [1]. In [18] it was shown that matrices in Hermite or Popov form are in fact Gröbner bases with respect to this definition. In section 4 we will introduce Gröbner bases over Ore polynomials based on [5]. We will extend the result of [18] to this case.

Gröbner bases usually suffer from high computational complexity. In [11] the authors Jean-Charles Faugère, Patrizia M. Gianni, Daniel Lazard and Teo Mora therefor attacked a special problem: Compute the Gröbner basis of an zero-dimensional ideal fast—provided that a Gröbner basis with respect to a different monomial ordering is already known. Breaking down the problem to linear algebra, they managed to obtain an efficient algorithm for that task.

In section 5 of this paper we will adapt the FGLM algorithm to modules over Ore polynomials. We will modify it in such a way that it also handles sub-modules that are not "zero-dimensional". We also will give an estimation of the complexity of this algorithm in the special case of converting Popov and Hermite forms.

There are other approaches for converting matrices in Popov and Hermite normal form into each other. One, for example, may be found in [24]. To our best knowledge, this paper is the first though that explores the connection of normal forms and Gröbner bases to complete this task.

We also compiled a technical report about this topic that contains a MAPLE™ implementation for the conversion of Popov into Hermite forms as well as detailed examples.

2. Basic notations

Ore polynomials—also called skew polynomials by some authors—are a generalisation of the usual polynomials with a non-commutative multiplication. They are named after Øystein Ore who was the first to describe them in [21]. We will only give an informal description of Ore polynomials here. A more rigid description may be found in [9, Chapter 0.10] or [10, Chapter 5.2].

Let K be a (computable) skew field, and let $\sigma\colon K \to K$ be an automorphism. A map $\vartheta\colon K \to K$ such that

$$\vartheta(a+b) = \vartheta(a) + \vartheta(b) \qquad \text{and} \qquad \vartheta(ab) = \sigma(a)\vartheta(b) + \vartheta(a)b$$

for all $a, b \in K$ is called a *σ-derivation* of K. (The second identity is sometimes referred to as *σ-Leibniz rule*.) Let now ∂ be a variable. An *Ore polynomial* is just a polynomial expression

$$a_n\partial^n + a_{n-1}\partial^{n-1} + \ldots + a_2\partial^2 + a_1\partial + a_0$$

where $n \geqslant 0$ and where the coefficients $a_0, \ldots, a_n$ are in K. The set of all Ore polynomials is denoted by $K[\partial; \sigma, \vartheta]$. Two Ore polynomials in $K[\partial; \sigma, \vartheta]$ are added in the same way as usual polynomials. The multiplication of Ore polynomials is given by extending the *commutation rule*

$$\partial a = \sigma(a)\partial + \vartheta(a)$$

with $a \in K$ assuming associativity and distributivity. This defines a ring structure on $K[\partial; \sigma, \vartheta]$. For a proof see [9, Theorem 10.1].

Example 1. The typical examples of Ore polynomials are the following. See also [10, Page 186] or [8, Table 2] for further examples.

(1) For $K = \mathbb{Q}$, $\sigma = \mathrm{id}$ and $\vartheta = 0$ (that is, the identity and the constant zero function respectively) we obtain just the usual commutative polynomials with the commutation rule $\partial a = a\partial$.
(2) For $K = \mathbb{Q}(x)$ (or K being the meromorphic functions in x), $\sigma = \mathrm{id}$ and $\vartheta = d/dx$ we obtain *differential operators* with the commutation rule $\partial f = f\partial + \frac{df}{dx}$ reflecting the composition of linear differential operators.
(3) For $K = \mathbb{Q}(n)$, $\sigma(a(n)) = a(n+1)$ and $\vartheta = 0$ we obtain the *shift operators* having the commutation rule $\partial a(n) = a(n+1)\partial$.

Obviously, the multiplication of Ore polynomials needs not to be commutative. (Thus it is also important that we write coefficients always on the left hand side.) Still, they retain a lot of the usual properties of ordinary polynomials. Given $f = a_n\partial^n + \ldots + a_1\partial + a_0$ where $a_0, \ldots, a_n \in K$ and $a_n \neq 0$, we define the *degree* of f as $\deg f = n$. We refer to $\operatorname{lcoeff}(f) = a_n$ as the *leading coefficient* of f. For convenience, we set $\deg 0 = -\infty$. Degree and leading coefficient fulfill the identities

$$\deg(fg) = \deg f + \deg g \qquad \text{and} \qquad \operatorname{lcoeff}(fg) = \operatorname{lcoeff}(f)\sigma^{\deg f}(\operatorname{lcoeff}(g))$$

for all Ore polynomials f and g.

Using this degree function we can do polynomial long division almost as in the commutative case. We have to distinguish between division from the left and from the right, though. Furthermore, we can compute left greatest common divisors and right greatest common divisors. See [10, Theorem 5.8] or [3] for the algorithms and their proofs of correctness.

For any ring R, we denote the set of $m \times n$ matrices over R by $R^{m\times n}$. The $n \times n$ identity matrix is denoted by $\mathbf{1}_n$ and the $m \times n$ zero matrix is written as $\mathbf{0}_{m\times n}$. A square matrix $M \in R^{n\times n}$ that has a two-sided inverse $M^{-1} \in R^{n\times n}$ is called *unimodular*. The set of $n \times n$ unimodular matrices is denoted by $\mathrm{GL}(R, n)$.

We will need to extract certain rows or columns from our matrices. For $M = (a_{ij}) \in R^{m\times n}$ and $1 \leqslant i \leqslant m$ we denote the i^{th} row by $M_{i,\bullet} = (a_{i,1}, \ldots, a_{i,n})$. Similarly, for $1 \leqslant j \leqslant n$ the j^{th} column is denoted by $M_{\bullet,j} = {}^t(a_{1,j}, \ldots, a_{m,j})$, where ${}^t\bullet$ denotes transposition.

The set of row vectors with entries in R of size n will be written as $R^{1\times n}$ and the set of column vectors of size m is denoted by R^m. In this paper, row vectors are treated as left module over R and column vectors form a right module over R. We will often regard vectors as matrices with only one row or column respectively.

If in particular $R = K[\partial; \sigma, \vartheta]$ is a ring of Ore polynomials, then for a matrix $M = (a_{i,j}) \in R^{m\times n}$ we define $\deg M = \max\{\deg a_{i,j} \mid i = 1, \ldots, m \text{ and } j = 1, \ldots, n\}$. As a further abbreviation we also define the i^{th} row degree for $1 \leqslant i \leqslant m$ as $\operatorname{rdeg}_i M = \deg M_{i,\bullet} = \max\{\deg a_{i,j} \mid j = 1, \ldots, n\}$. Finally, we will need the *leading vector* $\operatorname{lvec}(M) = \big(\operatorname{coeff}_\partial(\deg M, a_{i,j})\big)_{i,j} \in K^{m\times n}$. (We use the name "leading vector" instead of "leading matrix" because it will mostly be applied to vectors.)

3. Hermite and Popov normal forms

We will now define the main concepts we are dealing with in this paper, namely Hermite and Popov normal forms. Let again K be any skew field with automorphism $\sigma\colon K \to K$, σ-derivation $\vartheta\colon K \to K$, and let $R = K[\partial; \sigma, \vartheta]$.

We will start with the Hermite normal form. Our definition is taken from [13, Definition 3.2]. A matrix in Hermite form is basically just in row echelon form with some additional properties of the degrees of the entries.

Definition 2 (Hermite normal form)**.** A matrix $M = (a_{i,j}) \in R^{m\times n}$ is in *Hermite normal form* if and only if there exists indices $j_1 > j_2 > \ldots > j_m$ that are called *pivot indices* such that

(1) $a_{i,k} = 0$ if $k < j_i$,
(2) the entries a_{i,j_i} are monic, and
(3) $\deg a_{i,j_i} > \deg a_{k,j_i}$ for $k \neq i$.

Every matrix $N \in R^{m\times n}$ can be transformed using elementary row operations into a matrix M whose non-zero rows form a matrix in Hermite normal form. That is, for every such N there exists an invertible matrix $S \in \mathrm{GL}(R, m)$ such that

$$SN = \begin{pmatrix} M \\ \mathbf{0}_{m-s\times n} \end{pmatrix}$$

where $M \in R^{s\times n}$ is in Hermite form. Sometimes we will a little bit sloppily also refer to the whole right hand side—that is, with zero rows included—as the Hermite form of N. The computations can be done applying the (matrix form of the) Euclidean algorithm to the columns of N to achieve a row echelon form and then using polynomial division to enforce the degree restrictions. See [13, Theorem 3.2] for a more detailed description in the case of square matrices. We will show later in corollary 15 that the Hermite form of N is actually uniquely determined.

The definition of the Popov normal form is slightly more involved. We need to proceed in two steps. First we will introduce the concept of row-reducedness and afterwards as second step we define the Popov as a row-reduced matrix with additional properties.

Row-reducedness was first introduced in [12] for commutative polynomials. A presentation for Ore polynomials can be found in [2]. We repeat the definitions here for the convenience of the reader. Let $M \in R^{m\times n}$. When we multiply M from the left by the matrix $D = \mathrm{diag}(\partial^{\deg M - \mathrm{rdeg}_1 M}, \ldots, \partial^{\deg M - \mathrm{rdeg}_m M})$, we obtain a matrix DM with all rows having the same degree $\deg M$. Its leading vector

$$\mathrm{lvec}(DM) = \begin{pmatrix} \sigma^{\deg M - \mathrm{rdeg}_1 M}(\mathrm{lvec}(M_{1,\bullet})) \\ \vdots \\ \sigma^{\deg M - \mathrm{rdeg}_m M}(\mathrm{lvec}(M_{m,\bullet})) \end{pmatrix} \in K^{m\times n}$$

is called the *leading (row) coefficient matrix* of M. We denote it by $\mathrm{LC}(M)$.

Definition 3 (Row-reducedness)**.** A matrix $M \in R^{m\times n}$ is called *row reduced* if $\mathrm{LC}(M)$ has full left row rank.

Being row-reduced is the most important requirement for being in Popov normal form. The other points in the following definition basically just make sure that the matrix is uniquely determined. One can show that a matrix in Popov form has a leading coefficient matrix in row-echelon form. See for example [19, Lemma 14] for a proof. The definition is taken from [18, Definition 1].

Definition 4 (Popov normal form)**.** A matrix $M = (a_{i,j})ij \in R^{m\times n}$ is said to be in *Popov normal form*, if

(1) M is row-reduced and $\operatorname{rdeg}_i M \leqslant \operatorname{rdeg}_{i+1} M$ for all i;
(2) for the i^{th} row there exists a column index j_i (the *pivot index*) such that
   (a) a_{i,j_i} is monic and $\deg a_{i,j_i} = \operatorname{rdeg}_i M$;
   (b) $\deg a_{i,k} < \operatorname{rdeg}_i M$ if $k < j_i$;
   (c) $\deg a_{k,j_i} < \operatorname{rdeg}_i M$ if $k \neq i$; and
   (d) if $\operatorname{rdeg}_i M = \operatorname{rdeg}_k M$ and $i < k$ then $j_i < j_k$ (that is, pivot indices are ordered increasingly).

Also Popov forms are normal forms in the sense that each matrix can be transformed by elementary row operations into a matrix whose non-zero rows are in Popov form. Again this later matrix is sometimes simply referred to as the Popov form. The conversion can be done by first applying row-reduction—which is described, for example, in [2, Theorem 2.2]—and then using similar operations to achieve the degree constraints in the definition. See [6, Section 2.5.1] for a more detailed description.

Remark 5. Hermite forms clearly have independent rows since they are in row echelon form. But also the rows of matrices in Popov form are linearly independent—actually row-reducedness is already sufficient for that: By the so-called *predictable degree property* [2, Lemma A.1 (a)], if $v \in R^{1\times m}$ and $M \in R^{m\times n}$, then $vM = 0$ is only possible if $\deg v_i + \operatorname{rdeg}_i M < 0$ for all $1 \leqslant i \leqslant m$. This implies immediately that $v = 0$, since the rows of M are all non-zero.

4. Gröbner bases

Gröbner bases have been invented by Bruno Buchberger in [4]. Though initially defined for multivariate commutative polynomials, the concept has since been extended to more general domains such as Ore polynomials (see, for example, [8]) or modules over polynomial rings (see, for example, [20]). In this paper we will use the nice description of Gröbner bases of modules over Poincaré-Birkhoff-Witt rings given in [5, Chapter 5]. Poincaré-Birkhoff-Witt rings are a more general class of non-commutative domains that includes Ore polynomials. See [5, Definition 2.2.5] for the definition of Poincaré-Birkhoff-Witt rings and [5, Corollary 2.3.3] for the proof that Ore polynomials are included. An approach exclusively for Ore polynomials may be found in [8]—but there seems to be no extension to modules.

We include some of the results of [5] here for completeness and in order to adapt them to our notation. Let once more K be any skew field with automorphism $\sigma\colon K \to K$ and σ-derivation $\vartheta\colon K \to K$. Also, let $R = K[\partial; \sigma, \vartheta]$. We will just briefly skip through the most important definitions and provide pointers to the corresponding sections of [5]. Readers who are familiar with commutative Gröbner bases will find that everything translates well to the non-commutative case.

For $i = 1, \ldots, n$, let $\mathfrak{e}_i$ denote the i^{th} unit vector in $R^{1\times n}$. A *monomial* is a product $\partial^\alpha \mathfrak{e}_i$ of a power of ∂ and a unit vector where $\alpha \geqslant 0$ and $1 \leqslant i \leqslant n$. A *term* is the product of a scalar (that is, an element in K) and a monomial. There are two obvious ways of introducing a total ordering on monomials. See also [5, Definitions 5.3.8 and 5.3.9] and the definition of admissible orderings [5, Definition 5.3.7].

Definition 6 (Position over term/term over position ordering)**.** Let $\partial^\alpha \mathfrak{e}_i$ and $\partial^\beta \mathfrak{e}_j$ be monomials in $R^{1\times n}$ with $\alpha, \beta \geqslant 0$ and $1 \leqslant i, j \leqslant n$.

(1) The *position over term (POT)* ordering is defined by

$$\partial^\alpha \mathfrak{e}_i <_{\text{POT}} \partial^\beta \mathfrak{e}_j \quad :\Longleftrightarrow \quad i > j \vee (i = j \wedge \alpha < \beta);$$

(2) the *term over position (TOP)* ordering is given by

$$\partial^\alpha \mathfrak{e}_i <_{\text{TOP}} \partial^\beta \mathfrak{e}_j \quad :\Longleftrightarrow \quad \alpha < \beta \vee (\alpha = \beta \wedge i > j).$$

We will use $\leqslant_{\text{POT}}$, $\geqslant_{\text{POT}}$, $>_{\text{POT}}$, and $\leqslant_{\text{TOP}}$, $\geqslant_{\text{TOP}}$, $>_{\text{TOP}}$ in the usual way.

It is important to note here that we fixed an ordering on the indices (positions). The reason is that, although for Gröbner basis theory any ordering of the indices would be fine, for our application to Hermite and Popov forms this particular ordering is crucial.

If, for example, $n = 3$ then the smallest monomials with respect to the position over term ordering are

$$\begin{aligned}(0,0,1) <_{\text{POT}} (0,0,\partial) <_{\text{POT}} (0,0,\partial^2) <_{\text{POT}} \ldots <_{\text{POT}} (0,1,0) <_{\text{POT}} (0,\partial,0)\\ <_{\text{POT}} (0,\partial^2,0) <_{\text{POT}} \ldots <_{\text{POT}} (1,0,0) <_{\text{POT}} (\partial,0,0) <_{\text{POT}} (\partial^2,0,0) <_{\text{POT}} \ldots\end{aligned}$$

while with respect to the term over position ordering we obtain the chain

$$\begin{aligned}(0,0,1) <_{\text{TOP}} (0,1,0) <_{\text{TOP}} (1,0,0) <_{\text{TOP}} (0,0,\partial) <_{\text{TOP}} (0,\partial,0)\\ <_{\text{TOP}} (\partial,0,0) <_{\text{TOP}} (0,0,\partial^2) <_{\text{TOP}} (0,\partial^2,0) <_{\text{TOP}} (\partial^2,0,0) <_{\text{TOP}} \ldots.\end{aligned}$$

Thus, the position over term ordering has similarities to the lexicographic ordering in the usual commutative Gröbner basis theory while the term over position ordering corresponds to the degree lexicographic ordering.

Let now for a while $<$ denote either $<_{\text{POT}}$ or $<_{\text{TOP}}$. Any vector in $R^{1\times n}$ may be written as K-linear combination of monomials. That is, taking $v \in R^{1\times n}$ there are $k \geqslant 0$, $c_1, \ldots, c_k \in K$ and monomials $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ such that $v = c_1\mathfrak{m}_1 + \ldots + c_k\mathfrak{m}_k$. If $c_1 \neq 0$ and $\mathfrak{m}_1 > \mathfrak{m}_j$ for $2 \leqslant j \leqslant k$, then we call $\mathfrak{m}_1 = \operatorname{lmonom}_<(v)$ the *leading monomial* of v with respect to $<$. In this case, $c_1 = \operatorname{lcoeff}_<(v)$ is the *leading coefficient* and $c_1\mathfrak{m}_1 = \operatorname{lterm}_<(v)$ is the *leading term*. (Note the difference between leading coefficient and leading vector). If no confusion about to which order we confer may arise, then we just write $\operatorname{lmonom}(v)$ instead of $\operatorname{lmonom}_<(v)$ and the same for $\operatorname{lcoeff}(v)$ and $\operatorname{lterm}(v)$. Leading monomial, term and coefficient of the zero vector remain undefined.

Example 7. With respect to the position over term ordering, the leading monomial of a non-zero vector $v \in R^{1\times n}$ corresponds to the term of highest degree of the left-most non-zero entry of v. With respect to the term over position ordering, the leading term corresponds to the left-most of the entries of highest degree.

Using the above definition of leading term, reduction is defined as in the commutative case. That is, if $v = c_1\mathfrak{m}_1 + \ldots + c_k\mathfrak{m}_k$ is as above and if $W \subseteq R^{1\times n} \setminus \{0\}$ is given, then v is said to be *reducible* by W if there are $w \in W$, $1 \leqslant i \leqslant k$ and $\alpha \geqslant 0$ such that $\mathfrak{m}_i = \partial^\alpha \operatorname{lmonom}(w)$. Otherwise, v is called *irreducible*.

Theorem 8. *Given $v \in R^{1\times n}$ and $\{w_1, \ldots, w_s\} \subseteq R^{1\times n} \setminus \{0\}$, there are elements $u_1, \ldots, u_s \in R$ and $r \in R^{1\times n}$ such that*

$$v = u_1w_1 + \ldots + u_sw_s + r$$

where r is not reducible by $\{w_1, \ldots, w_s\}$.

We will call r the remainder *of the division of v by $\{w_1, \ldots, w_n\}$.*

Proof. This is [5, Theorem 5.4.3]. Directly after the theorem—namely in [5, Algorithm 10]—the division method is explained in detail. □

We have now everything set in order to define Gröbner bases. We start with [5, Definition 5.4.7].

Definition 9 (Gröbner basis)**.** Let $\mathfrak{M}$ be an R-submodule of $R^{1\times n}$. A finite set $G \subseteq \mathfrak{M}$ is a *Gröbner basis* for $\mathfrak{M}$ if for all $v \in \mathfrak{M}$ there is $\alpha \geqslant 0$ and $g \in G$ such that $\operatorname{lmonom}(v) = \partial^\alpha \operatorname{lmonom}(g)$.

Lemma 10. *Every non-zero submodule $\mathfrak{M} \subseteq R^{1\times n}$ has a Gröbner basis G, $\mathfrak{M}$ is generated by G as a left R-module and the remainder of the division of an element $v \in R^{1\times n}$ by G does not dependent on the order of the elements in G.*

Furthermore, $v \in \mathfrak{M}$ if and only the remainder by division with G is zero.

Proof. These statements are found in [5, Proposition 5.4.8, Corollary 4.10 and Theorem 5.4.9]. □

The following definition is [5, Definition 4.17].

Definition 11 (Reduced Gröbner bases)**.** A Gröbner basis G of $\mathfrak{M} \subseteq R^{1\times n}$ is *reduced* if for all $g \in G$ we have $\operatorname{lcoeff}(g) = 1$ and there is no $h \in G \setminus \{g\}$ such that $\operatorname{lmonom}(h)$ divides a term in g.

As in the usual, commutative Gröbner basis theory one may define *S-polynomials* and prove a *Buchberger criterion* for Gröbner bases in $R^{1\times n}$. This can be found in [5, Definition 5.4.11 and Theorem 5.4.13]. But since we will not need the full Buchberger criterion in our proofs, we will be content with stating a corollary here.

Theorem 12. *Let $G = \{g_1, \ldots, g_s\} \subseteq R^{1\times n}$ with leading monomials $\operatorname{lmonom}(g_k) = \partial^{\alpha_k}\mathfrak{e}_{j_k}$ for $1 \leqslant k \leqslant s$. If $j_i \neq j_k$ whenever $i \neq k$ then G is a Gröbner basis for the submodule $Rg_1 + \ldots + Rg_s \subseteq R^{1\times n}$ generated by its elements.*

Proof. This is [5, Corollary 5.4.14]. □

We will now draw the connection from Gröbner bases to normal forms. For this we have to make the transition between matrices and sets of row vectors. We will say that a matrix $M \in R^{m\times n}$ is a (reduced) Gröbner basis with respect to a certain term ordering if the set of its rows $\{M_{1,\bullet}, \ldots, M_{m,\bullet}\}$ is a (reduced) Gröbner basis for its row space $R^{1\times m}M$.

The following two theorems are generalisations of [18, Proposition 2 and 4] to Ore polynomials.

Theorem 13. *Let $M \in R^{m\times n}$ with the rows sorted in descending order with respect to position over term ordering. Then M is in Hermite form if and only if the non-zero rows of M form a reduced Gröbner basis for $R^{1\times m}M$ with respect to position over term ordering.*

Proof. By example 7, with respect to position over term ordering, the leading terms of the rows are exactly those corresponding to the pivot indices in the sense of definition 2. Since the pivot indices are all different, M is a Gröbner basis by theorem 12, and since the corresponding entries are monic and the entries in the rows above are of lower degree, we even have a reduced Gröbner bases.

Conversely, one easily sees, that for a reduced Gröbner bases the leading terms must be in different positions. Setting these as the pivot indices, from this observation one deduces all properties listed in definition 2. □

Theorem 14. *Let $M \in R^{m\times n}$ with the rows sorted in ascending order with respect to term over position ordering. Then M is in Popov form if and only if the non-zero rows of M form a reduced Gröbner basis for $R^{1\times m}M$ with respect to term over position ordering.*

Proof. Analogously to the Hermite form, here the leading terms with respect to position over term ordering are those corresponding to the pivot indices—this time in the sense of definition 4. Again, they are in different positions and thus we obtain a Gröbner basis. As before, the properties listed in definition 4 make sure that the Gröbner basis is reduced. Also the converse is easily proven by letting the pivot indices be the positions of the leading terms and checking the properties in the definition. (For the row-reducedness note that the pivot indices are in different columns and hence the leading coefficient matrix must be in row echelon form.) □

Since reduced Gröbner bases for submodules by [5, Theorem 5.4.18] are unique, from the previous theorems we obtain (together with the existence considerations from section 3)

Corollary 15. *Every matrix has exactly one Hermite form and exactly one Popov form.*

5. FGLM

The first version of the FGLM algorithm—named after its inventors—was presented in [11]. It solves the following problem: Given a Gröbner basis of a zero-dimensional ideal I in a ring $F[x]$ of commutative polynomials over a field F with respect to a certain term order, compute the Gröbner basis of I with respect to another term order. That is, the FGLM algorithm allows to convert Gröbner bases between different term orderings. Since it does so quite efficiently, it is thus possible to compute a Gröbner basis for a "slow" term ordering by first computing it with respect to a "fast" term ordering and then using FGLM for conversion.

The main achievement of [11] is, that they managed to break this problem down to a linear algebra problem: Instead of calculating in $F[x]$ they solve the task in $F[x]/I$ which is a finite dimensional vector space over F. In this space they iterate over all (representatives of) monomials deciding whether they are leading monomials of an element of the new Gröbner basis or not.

Let again K be a skew field with automorphism $\sigma\colon K \to K$ and σ-derivation $\vartheta\colon K \to K$. As before we abbreviate $K[\partial;\sigma,\vartheta]$ by R. Let $M \in R^{m\times n}$ be a Gröbner bases for the term over position or for the position over term ordering. It will turn out that the FGLM algorithm translates quite nicely to this setting. There is one problem, though, namely that $R^{1\times n}/R^{1\times m}M$ needs not to be finite dimensional. That is, we possibly have to traverse over infinitely many monomials.

Our first goal is thus to limit the number of monomials we have to search. For this we will need the next two lemmata that will give an estimate on the degrees of Popov and Hermite forms of a given matrix.

Lemma 16. *Let $A \in R^{m\times n}$ be any matrix and $M \in R^{m\times n}$ its Popov form. Then* $\deg M \leqslant \deg A$.

Proof. By [2, Theorem 2.2] does row-reduction applied to A at most lower the degree. Furthermore, since the Popov form M is by definition also row-reduced, by [2, Lemma A.1 (d)] we may conclude that its degree is the same as that of the result of the row-reduction and thus not larger than the degree of A, too. □

The next lemma is [13, Corollary 3.4]. Although in the reference the result is only stated for square matrices over rings of differential operators (see example 1), following the proofs one easily sees that they generalise to arbitrary Ore polynomials and to matrices that are not necessarily square.

Lemma 17. *Let $A \in R^{m\times n}$ be a matrix of full left row-rank, and let $M \in R^{m\times n}$ be its Hermite form. Then* $\deg M \leqslant m \deg A$.

Proof. See [13, Corollary 3.4]. □

Having thus established degree bounds for Hermite and Popov forms, we may use them to limit our search space. The correctness of this statement is proven below in theorem 21. But we first need to introduce a few notations and definitions which are necessary for the formulation of the algorithm.

For any set $\mathfrak{S} \subseteq R^{1\times n}$ we denote the set of elements of degree at most $d \geqslant 0$ in $\mathfrak{S}$ by $\mathfrak{S}_{\leqslant d} = \{v \in \mathfrak{S} \mid \deg v \leqslant d\}$. Let M be in Hermite or Popov form. We write the set of all those monomials which are not reducible by M as $\mathfrak{B}$. By [5, Proposition 5.6.3] $\overline{\mathfrak{B}} = \{\overline{\mathfrak{m}} \mid \mathfrak{m} \in \mathfrak{B}\}$ is a K-basis of $R^{1\times n}/R^{1\times m}M$ where the bar denotes residue classes modulo M. We would like to emphasise here that $\mathfrak{B}$ depends on the monomial ordering in respect to which M is a Gröbner basis. For any $u \in R^{1\times n}$ we will write the coordinate vector of u in $R^{1\times n}/R^{1\times m}M$ with respect to $\overline{\mathfrak{B}}$ as $u_{\overline{\mathfrak{B}}}$.

The factor module $R^{1\times n}/R^{1\times m}M$ is not only a vector space but also a left R-module. Hence, the multiplication by ∂ induces a map of $R^{1\times n}/R^{1\times m}M$ into itself that we will call $\partial\bullet$. It has the properties that

$$\partial(\overline{v} + \overline{w}) = \partial\overline{v} + \partial\overline{w} \qquad \text{and} \qquad \partial(a\overline{v}) = \sigma(a)\partial\overline{v} + \vartheta(a)\overline{v}.$$

for all v and $w \in R^{1\times n}$ and $a \in K$. Such a map is called *pseudo-linear* in [15].

Fix a degree bound. We will consider the *truncated basis* $\overline{\mathfrak{B}_{\leqslant d}}$. Let π be the projection of $R^{1\times n}/R^{1\times m}M$ onto the K-span $\langle\overline{\mathfrak{B}_{\leqslant d}}\rangle$ of the truncated basis. We introduce the *truncated ∂-multiplication* $\tau = \pi\circ(\partial\bullet)|_{\langle\overline{\mathfrak{B}_{\leqslant d}}\rangle}$ as a map of $\langle\overline{\mathfrak{B}_{\leqslant d}}\rangle$. (The composition with π lets us ignore products which are not in $\langle\overline{\mathfrak{B}_{\leqslant d}}\rangle$ any more.) Let $v = \pi v \in \langle\overline{\mathfrak{B}_{\leqslant d}}\rangle$. Then $\tau(a\pi(v)) = \pi\circ(\partial\bullet)(a\pi(v)) = \sigma(a)\big(\pi\circ(\partial\bullet)\big)(\pi v) + \vartheta(a)\pi^2(v) = \sigma(a)\tau(\pi(v)) + \vartheta(a)\pi(v)$ since $\pi^2 = \pi$. Thus, τ is also a pseudo-linear map. By [15, Section 2] we may construct a matrix $T \in K^{|\mathfrak{B}_{\leqslant d}|\times|\mathfrak{B}_{\leqslant d}|}$ such that

$$\tau(u)_{\overline{\mathfrak{B}_{\leqslant d}}} = \sigma(u_{\overline{\mathfrak{B}_{\leqslant d}}})T + \vartheta(u_{\overline{\mathfrak{B}_{\leqslant d}}})$$

where σ and ϑ are applied to vectors component-wise. The truncated multiplication matrix T is called a *τ-connection* in [7].

Remark 18. Computing T is actually quite easy. If for $\mathfrak{m} \in \mathfrak{B}_{\leqslant d}$ also $\partial\mathfrak{m} \in \mathfrak{B}_{\leqslant d}$, then the row corresponding to $\overline{\mathfrak{m}}$ in T is a unit vector. If otherwise $\partial\mathfrak{m} \notin \mathfrak{B}_{\leqslant d}$, then there are two possibilities. Either $\partial\mathfrak{m} \in \mathfrak{B}$ or $\partial\mathfrak{m}$ is divisible by a row in M.

In the first case the row of $\overline{\mathfrak{m}}$ in T will just be zero. In the second case, there is a leading monomial $\mathfrak{n}$ of a row $M_{i,\bullet}$ of M and $\alpha \geqslant 0$ such that $\partial^\alpha \mathfrak{n} = \partial\mathfrak{m}$. Since $\mathfrak{m}$ is irreducible, we may conclude that $\alpha = 0$, that is, that $\mathfrak{n} = \partial\mathfrak{m}$. Thus, the remainder is $\mathfrak{n} - M_{i,\bullet} \in \mathfrak{B}_{\leqslant d}$ which is irreducible since M is a reduced Gröbner basis. The corresponding row in T is then just $(\overline{\mathfrak{n} - M_{i,\bullet}})_{\overline{\mathfrak{B}_{\leqslant d}}}$. The coordinates may hence be plainly read off from the coefficients in $M_{i,\bullet}$.

In example 7 we already established the correspondence between the pivot indices and the leading monomials in M. This allows us to write down $\mathfrak{B}_{\leqslant d}$ quite easily as

$$\mathfrak{B}_{\leqslant d} = \left\{ \partial^\alpha \mathfrak{e}_j \;\middle|\; j = j_i \in J \wedge \alpha < \operatorname{rdeg}_i M \right\} \cup \left\{ \partial^\alpha \mathfrak{e}_j \middle| j \notin J \wedge \alpha \leqslant d \right\}$$

where $J = \{j_1, \dots, j_m\}$ is the set of all pivot indices. We may compute the coordinates of the residue classes of the unit vectors $\overline{\mathfrak{e}_1}, \dots, \overline{\mathfrak{e}_n}$ in the same way as the we computed T. From them we can compute the residue class of any $\partial^\alpha \mathfrak{e}_k \in \mathfrak{B}_{\leqslant d}$ just by using T.

We are now ready to state the algorithm. Although the only admissible orderings we have considered are the position over term and the term over position ordering, the algorithm would also work for other orderings. We denote lists (that is, ordered sets) by enclosing their elements in square brackets, that is, we write $L = [L_1, \dots, L_k]$. If ℓ is an element, then $\ell : L$ denote the list with its first element being ℓ and then the elements of L following in order, that is, $\ell : L = [\ell, L_1, \dots, L_k]$.

Algorithm 19 (FGLM with degree bound)**.**

Input: A reduced Gröbner basis $M \in R^{m \times n}$ with respect to the admissible ordering $<_1$ and an admissible ordering $<_2$ as well as a degree bound d for the reduced Gröbner basis with respect to $<_2$.

Output: The reduced Gröbner basis with respect to $<_2$.

Procedure:

(1) Let $\mathfrak{B}_1$ be the truncated basis with respect to $<_1$ and d, and let T be the corresponding multiplication matrix.

(2) Initialise $C \leftarrow [\,]$, $\mathfrak{B}_2 \leftarrow [\,]$ and $G_2 \leftarrow \varnothing$.
Upon termination, G_2 will be the reduced Gröbner basis, $\mathfrak{B}_2$ will be the truncated basis with respect to $<_2$ and d, and C will contain the coordinate vectors of the elements of $\mathfrak{B}_2$ with respect to $\overline{\mathfrak{B}_1}$.

(3) If there are monomials of degree less or equal to d that are not divisible by G_2, then:

  (a) Choose the smallest such monomial $\mathfrak{m}$ with respect to $<_2$ and compute its coordinate vector $w = \overline{\mathfrak{m}}_{\overline{\mathfrak{B}_1}}$ using T.

  (b) If $w : C$ is K-linear independent, then set $C \leftarrow w : C$ and $\mathfrak{B}_2 \leftarrow \mathfrak{m} : \mathfrak{B}_2$.

  (c) Else there are $a_j \in K$ such that $w = \sum_j a_j C_j$. Set $G_2 \leftarrow G_2 \cup \{\mathfrak{m} - \sum_j a_j (\mathfrak{B}_2)_j\}$.

  (d) Go to step 3.

(4) Else stop and return G_2 as a matrix with the rows sorted with respect to $<_2$.

Remark 20. If $<_2 = <_{\text{POT}}$, then the sequence of monomials that are chosen in step 3a can be computed as follows. Set $j \leftarrow n$ and start with $\mathfrak{m} \leftarrow \mathfrak{e}_j = \mathfrak{e}_n$ which

is the smallest element. If in step 3b w does not depend on C, then set $\mu \leftarrow \partial\mu$, $w \leftarrow \sigma(w)T + \vartheta(w)$ and go to step 3b. Else, set $j \leftarrow j-1$ and continue with the next $\mathfrak{m}$ being $\mathfrak{e}_j$. The sorting in step 4 can be omitted if G_2 is maintained as a list with new elements added in front.

If $<_2 = <_{\mathrm{TOP}}$, then we maintain a list $\mathfrak{M}$ of monomials which initially is just $[\mathfrak{e}_n, \ldots, \mathfrak{e}_1]$ and a corresponding list of coordinate vectors W. We iterate over $(\mathfrak{m}, w)$ in the zipped list $(\mathfrak{M}, W)$. If in step 3b we find a linear dependence, then we remove $(\mathfrak{m}, w)$ from $(\mathfrak{M}, W)$. Once we are through the list, if $\mathfrak{M} \neq [\,]$ we set $\mathfrak{M} \leftarrow [\partial\mathfrak{m} \mid \mathfrak{m} \in \mathfrak{M}]$ and $W \leftarrow [\sigma(w)T + \vartheta(w) \mid w \in W]$ and continue. Also here, the sorting in step 4 is not necessary if G_2 is a list with the elements added at the end.

Theorem 21. *Algorithm 19 is correct and terminates.*

Proof. The iteration considers only monomials up to certain degree. Since there are only finitely many of them, the algorithm clearly terminates.

It remains to prove the correctness. We will use the notations from the algorithm. First, we note that the elements in C are always linearly independent by construction. Since they are just the $\overline{\mathfrak{B}_1}$-coordinate vectors of the elements in $\mathfrak{B}_2$—and since the coordinate map is K-linear—also $\mathfrak{B}_2$ is linear independent modulo $R^{1\times m}M$.

Moreover, we claim that the elements of G_2 are in $R^{1\times m}M$. Let in step 3c $g = \mathfrak{m} - \sum_j a_j(\mathfrak{B}_2)_j$. Let $r = g - uM$ be the remainder of g by division with M where $u \in R^{1\times m}$ contains the coefficients from theorem 8. We have $\overline{r} = \overline{g - uM} = \overline{g} = w - \sum_j a_j C_j = 0$. Since r is irreducible, this implies $r = 0$, that is, $g \in R^{1\times m}M$.

Let $\mathrm{LM}(G_2) = \{\partial^\alpha \mathfrak{m} \mid \mathfrak{m} \in G_2 \text{ and } \alpha \geqslant 0\}$. We claim that $\mathfrak{B}_2 \cap \mathrm{LM}(G_2) = \varnothing$. This holds in step 2 and cannot be destroyed if we add elements to $\mathfrak{B}_2$ in step 3b. In step 3c, if an element is added to G_2 it is bigger than all elements in $\mathfrak{B}_2$ with respect to $<_2$ since we iterate over all monomials in order. Using the definition of admissible orderings in [5, Defintion 2], we see that it cannot divide any monomial in $\mathfrak{B}_2$. Since we consider all monomials of degree at most d, we obtain

$$\mathfrak{M}_{\leqslant d} := \{\mathfrak{m} \text{ monomial} \mid \deg \mathfrak{m} \leqslant d\} = \mathrm{LM}(G_2)_{\leqslant d} \dot\cup \mathfrak{B}_2.$$

Let $\tilde{G}$ be the Gröbner basis of $R^{1\times m}M$ with respect to $<_2$ and let $\tilde{\mathfrak{B}} \subseteq \mathfrak{M}_{\leqslant d}$ denote the corresponding truncated basis. Since $G_2 \subseteq R^{1\times m}M$, we must have $\tilde{\mathfrak{B}} \subseteq \mathfrak{B}_2$. We claim that $\mathrm{lmonom}(g) \in \mathrm{LM}(G_2)$ for any $g \in \tilde{G}$. By our degree bound, we know that $\mathrm{lmonom}(g) \in \mathfrak{M}_{\leqslant d}$. Assume $\mathrm{lmonom}(g)$ was in $\mathfrak{B}_2$. This meant that we could reduce an element of $\mathfrak{B}_2$ contradicting the linear independence of $\mathfrak{B}_2$ modulo $R^{1\times m}M$. Thus $\mathrm{LM}(\tilde{G}) \subseteq \mathrm{LM}(G_2)$. Hence, by definition 9, G_2 must be a Gröbner basis.

By construction, the leading monomials of G_2 are monic and do not divide each other. Further more, since for each $g \in G_2$ we have $g - \mathrm{lmonom}(g) \in \langle \mathfrak{B}_2 \rangle$, we see that g is irreducible by $G_2 \setminus \{g\}$. Thus, G_2 is the unique reduced Gröbner basis of $R^{1\times m}M$ with respect to $<_2$. □

Corollary 22 (Main theorem)**.** *Because of the degree bound in the lemmata 16 and 17, we may use algorithm 19 to convert Hermite forms into Popov form and vice versa.*

Proof. Let $H \in R^{m\times n}$ be in Hermite form and assume $P \in R^{s\times n}$ is the output of algorithm 19. Then P is in Popov form and using Gröbner basis division we may compute $A \in R^{m\times s}$ such that $H = AP$. Since also H is a Gröbner basis we can find $B \in R^{s\times m}$ such that $BH = P$. Now, since H and P have linearly independent rows by remark 5, we conclude $AB = \mathbf{1}_m$ and $BA = \mathbf{1}_s$. By [16, p. 32] (applicable since by [10, Theorem 5.8] Ore polynomials can be embedded in skew fields) this implies $m = s$ and hence $A = B^{-1} \in \mathrm{GL}(R, s)$. Thus, P really is the Popov form of H. Analogously, also for a Popov form as input we receive the corresponding Hermite form. □

Finally, we would like to reason about the complexity of algorithm 19. We will consider only the conversion from Popov to Hermite form. In the steps 1 and 2 there is not much to do, since the computation of T involves just the copying of the coefficients of M by remark 18. The real work is done in step 3. Here, we have to compute all the candidates for leading monomials and their coordinate vectors, and we have to check sets of monomials for linear dependence. Let $d = \deg M$. The degree bound is md in this case. The number of monomials generated (and also the size of $\mathfrak{B}_1$) does thus not exceed $\mathcal{O}(nmd)$. To generate a monomial we either look it up from a list containing the unit vectors and their coordinates (as can be precomputed analogously to T) or by remark 20 we compute it as a product with ∂ and the previous monomial. In the later case to compute the coordinates we need $\mathcal{O}(mnd)$ applications of σ and ϑ and $\mathcal{O}((mnd)^2)$ multiplications and additions in K for the multiplication by T. The most expensive step is to solve the $\mathcal{O}(nmd)$ variables system in step 3b which needs $\mathcal{O}((nmd)^3)$ operations in K by [17, Bemerkung 2.19 (2)]. Since $\mathfrak{B}_2$ contains only (different) monomials, computation of $\mathfrak{m} - \sum_j a_j(\mathfrak{B}_2)_j$ is again just copying coefficients.

The estimate becomes tighter if M is a square matrix. Then, the degree bound is never needed because there will be a pivot in every row of M. Hence, $R^{1\times n}/R^{1\times m}M$ is finite. This corresponds to the case of zero-dimensional ideals in the theory of commutative polynomials. We need to consider at most $\mathcal{O}(md)$ monomials. This bound can even be lowered using the *index* of M which is $\operatorname{ind} M = \sum_i \operatorname{rdeg}_i M$ as introduced in [12]. This yields a total complexity of $\mathcal{O}((\operatorname{ind} M)^4)$.

Remark 23 (Complexity)**.** For the conversion of a Hermite form in $M \in R^{m\times n}$ into Popov form one needs $\mathcal{O}((mnd)^4)$ operations in K where $d = \deg M$. If M is square, then $\mathcal{O}((\operatorname{ind} M)^4) \leqslant \mathcal{O}((md)^4)$ operations are sufficient.

6. Conclusion

In this paper we have extended the result of [18] that Hermite and Popov forms are Gröbner bases to a general Ore polynomial setting. We adapted the classical FGLM algorithm for this case and used it to convert matrices from Hermite form into Popov form and vice versa. The complexity of this is polynomial and not to far away from other approaches as for example [24]. The version presented here is slightly more general though as it works with arbitrary Ore polynomials.

References

[1] Adams, W. W., and Loustaunau, P. *An introduction to Gröbner bases.* Graduate studies in mathematics. AMS, 1994.

[2] Beckermann, B., Cheng, H., and Labahn, G. Fraction-free row reduction of matrices of Ore polynomials. *Journal of Symbolic Computation 41* (2006), 513 – 543.

[3] Bronstein, M., and Petkovšek, M. An introduction to pseudo-linear algebra. *Theoretical Computer Science 157, 3-33 157* (1996), 3–33.

[4] Buchberger, B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)*. PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965. (English translation to appear in Journal of Symbolic Computation, 2004).

[5] Bueso, J. L., Gómez-Torrecillas, J., and Verschoren, A. *Algorithmic methods in non-commutative algebra*, vol. 17 of *Mathematical modelling: Theory and applications*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2003.

[6] Cheng, H. *Algorithms for normal forms for matrices of polynomials and Ore polynomials*. PhD thesis, University of Waterloo, 2003. Advisor: George Labahn.

[7] Churchill, R. C., and Kovacic, J. J. Cyclic vectors. In *Differential algebra and related topics* (2002), L. Guo, P. J. Cassidy, W. F. Keigher, and W. Y. Sit, Eds., World Scientific Publishing Co. Pte. Ltd., pp. 191–218.

[8] Chyzak, F., and Salvy, B. Non-commutative elimination in Ore algebras proves multivariate identities. *Journal of Symbolic Computation 26*, 2 (1998), 187–227.

[9] Cohn, P. M. *Free rings and their relations*, 2nd edition ed. Academic press inc. (London) Ltd, 1985.

[10] Cohn, P. M. *An introduction to ring theory*. Springer, Berlin Heidelberg New York, 2000.

[11] Faugère, J.-C., Gianni, P. M., Lazard, D., and Mora, T. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comput. 16*, 4 (1993), 329–344.

[12] Forney jr., G. D. Minimal bases of rational vector spaces with applications to multivariable linear systems. *SIAM J. Control 13* (May 1975), 493 – 520.

[13] Giesbrecht, M., and Kim, M. S. *Computer Algebra in Scientific Computing*, vol. 5743 of *Lecture Notes in Computer Science*. Springer, Berlin / Heidelberg, 2009, ch. On Computing the Hermite Form of a Matrix of Differential Polynomials, pp. 118–129.

[14] Hermite, C. Sur l'introduction des variables continues dans la théorie des nombres. *Journal der reinen und angewandten Mathematik*, 41 (1851), 191–216.

[15] Jacobson, N. Pseudo-linear transformations. *The Annals of Mathematics 38*, 2 (1937), 484–507.

[16] Jacobson, N. *The theory of rings*, vol. 2 of *Mathematical Surveys and Monographs*. American Mathematical Society, 1943.

[17] Kiyek, K.-H., and Schwarz, F. *Mathematik für Informatiker*, vol. 1. Teubner, 1989.

[18] Kojima, C., Rapisarda, P., and Takaba, K. Canonical forms for polynomial and quadratic differential operators. *System & Control Letters* (2007), 678–684.

[19] Middeke, J. Converting between the Popov and the Hermite form of matrices of differential operators using an FGLM-like algorithm. Tech. Rep. 10-16, RISC Report Series, University of Linz, Austria, 2010.

[20] Mora, F., and Möller, H. New constructive methods classical ideal theory. *Journal of Algebra 100*, 1 (1986), 138–178.

[21] Ore, O. Theory of non-commutative polynomials. *Annals of Mathematics 34* (1933), 480 – 508.

[22] Popov, V. M. Some properties of the control systems with irreducible matrix-transfer functions. In *Seminar on Differential Equations and Dynamical Systems, II*, Lecture Notes in Mathematics. Springer, Berlin / Heidelberg, 1970, pp. 169–180.

[23] Popov, V. M. Invariant description of linear, time-invariant controllable systems. *SIAM Journal on Controll*, 2 (May 1972), 252–264.

[24] Villard, G. Computing Popov and Hermite forms of polynomial matrices. In *ISSAC* (1996), pp. 250–258.

Research Institute for Symbolic Computation (RISC), Linz, Austria
E-mail address: jmiddeke@risc.jku.at

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 195–201
ISSN 1930-1235: (2010)

RELATIONS BETWEEN HEUN EQUATIONS AND PAINLEVE EQUATIONS

S.YU. SLAVYANOV, A.YA. KAZAKOV, F. R. VUKAJLOVIĆ

Special functions play significant role in Computer Algebra packages. Here we can mention all-purpose packages as Mathematika or Maple as well as specialized packages as SFTools. Further development would without doubt be focused on Heun functions and closely related Painleve transcendents. Partly the relationship between Heun equations and Painleve equations is presented in the package SFTools. However new studies induce revision of presentation of these relations. The items of these revisions are the following.

1. Relations between equations belonging to Heun class, the corresponding deformed equations with added apparent singularity and the corresponding 2×2 systems. It is needed to stress that two different 2×2 systems correspond to one deformed equation.
2. Relations between integral transforms linking different equations belonging to Heun class and Okamoto-type transforms linking Painleve equations. These give rise to symmetries in the class of corresponding functions.
3. Relations between known physical models which are solved in terms of Heun functions like two-Coulomb centers problem, Stark effect etc. and the corresponding problems in classical dynamics.

In the publications [1, 2] and later in the the book [3] the author formulated the statement that every equation belonging to Heun class induces the corresponding equation belonging to Painleve class. This statement has been implemented in the package SFTools which supplied different information on special functions [4]. The mentioned induction called later as "antiquantization" is realised by substitution instead of quantum variables: coordinate and momentum – in the hamiltonian for Heun equations – the classical variables in the corresponding classical Lagrangian. Newtonian equations of motion appear to be Painleve equations. However several aspects of the theory were missing at that stage. These there:

1. What transforms of Painleve equations are induced by s-homotopic transformations of Heun equations?
2. What are the deformed Heun equations generated from Heun equation by adding an apparent singularity?
3. What are the relations to 2×2 first order linear systems which often are assumed as basic in handling with Painleve equations?
4. Are there other linear systems related to Painleve equations?
5. What transforms of Painleve equations are induced by integral transforms of Heun equations?
6. What classical physical problems are related to the well-known quantum problems exposed in terms of particular equations belonging to Heun class?

In view of a large number of Heun equations the detailed answer to posed questions is rather complicated and needs to be coded in a software package. Here is given a general approach to basic Heun equation. The presentation is referring to previous publications of the author with collaborators. The canonical form of Heun equation is chosen as

$$w'' + \left[\frac{1-\theta_1}{z} + \frac{1-\theta_2}{z-1} + \frac{1-\theta_3}{z-t}\right] w' + \left[\frac{\alpha\beta}{z(z-1)} - \frac{t(t-1)H}{z(z-1)(z-t)}\right] w = 0. \tag{1}$$

Here θ_j are characteristic exponents for the solutions with singularities at the points z_j, $z_1 = 0$, $z_2 = 1$, $z_3 = t$.

Parameters α, β – are characteristic exponents at infinity. According to Fuchs theorem it holds

$$\sum_{j=1}^{3} \theta_j + \alpha + \beta = 1. \tag{2}$$

Parameter H is assumed to be the energy. It is normalized in such a way that the residue of of the corresponding term at $z = t$ is unity. A more general Heun equation can be obtained by applying linear transformation of independent variable and s-homotopic transformations [3] of dependent variable

$$y := (z - z_k)^{\gamma_k} w.$$

It is as following

$$\sigma(z)y''(z) + \sum_{j=1}^{3}(1-b_j)\sigma_j(z)y'(z) + \left[\sum_{j=1}^{3}\frac{a_j\sigma_j(z)}{(z-z_j)} + \delta(z-z_3) - \left(\frac{\lambda\sigma_3(z_3)}{(z_2-z_1)} + \frac{1}{2}\sum_{j=1}^{2}(1-b_3)(1-b_j)\frac{\sigma_3(z_3)}{z_3-z_j}\right)\right] y(z) = 0. \tag{3}$$

Here

$$b_j = (\rho_{1j} + \rho_{2j}), \quad a_j = \rho_{1j}\rho_{2j},\ j = 1,2,3, \quad a_\infty = \kappa_1\kappa_2,$$

$$\sigma(z) = \prod_{j=1}^{3}(z - z_j), \quad \sigma_j(z) = \frac{\sigma(z)}{z - z_j},$$

$$\delta = a_\infty - \sum_{j=1}^{3} a_j,$$

where ρ_{mj} are characteristic exponents at finite singular points and κ_1, κ_2 are characteristic exponents at infinity. It can be shown that the quantity λ stays invariant under transforms mentioned above. The other invariants are squares of differences between characteristic exponents

$$\Delta_j = (\rho_{1j} - \rho_{2j})^2,\ j = 1,2,3 \quad \Delta_\infty = (\kappa_1 - \kappa_2)^2.$$

Applying the antiquantization procedure we arrive to the following equation [5]

$$\frac{2\sigma_3(t)}{\sqrt{\sigma(q)}}\frac{d}{dt}\frac{\dot{q}\sigma_3(t)}{\sqrt{\sigma(q)}}+\frac{\dot{q}\sigma_3^2(t)}{\sigma(q)(q-t)}+$$

$$\left[-\Delta_\infty+\sum_{j=1}^{2}\frac{(\Delta_j+1-2b_j)\sigma_j(z_j)}{(q-z_j)^2}+\frac{(\Delta_3-1)\sigma_3(t)}{(q-t)^2}\right]=0. \tag{4}$$

This is a general form of the Painlevé equation P^6 generated by general form Heun equation. Two important features of equation (4) should be emphasized.

1. The role of the singular point $z_3 = t$ in (1) is specific in (4) compared to the other points z_1, z_2.
2. The only influence of generalization due to s-homotopic transformation is a slight dependence on b_j $j = 1, 2$ in (4).

Deformed Heun equations. Here only the canonical form of Heun equation is studied. The deformed Heun equation termed as Heun1 arises by adding an apparent singularity into Heun equation thus increasing the number of Fuchsian singular points up to five. It can be written as following.

$$w''+\left[\frac{1-\theta_1}{z}+\frac{1-\theta_2}{z-1}+\frac{1-\theta_3}{z-t}-\frac{1}{z-q}\right]w'+$$

$$+\left[\frac{\alpha\beta}{z(z-1)}+\frac{q(q-1)p}{z(z-1)(z-q)}-\frac{t(t-1)H}{z(z-1)(z-t)}\right]w=0, \tag{5}$$

where θ_j, $j = 1, 2, 3$, are the characteristic exponents for solutions with singularities at the singular points z_j. The set of parameters θ_1, θ_2, α, β, t, q and p corresponds to this equation. We note that θ_3 is considered a dependent parameter because the Fuchs condition slightly different from (2)

$$\sum_{j=1}^{3}\theta_j+\alpha+\beta=0 \tag{6}$$

related to the characteristic exponents at singularities must be satisfied (the choice of the one dependent parameter θ_3 among θ_1, θ_2, and θ_3 is arbitrary). The parameter H is not an independent parameter of (5) either; it is determined from the condition that the point $z = q$ is an apparent singularity of the equation. This condition leads to an explicit expression for H in terms of the parameters θ_1, θ_2, α, β, q, p, and t.

$$H=\frac{1}{\sigma_3(t)}\left[\sigma(q)p^2+p\sum_{j=1}^{3}\sigma_j(q)(1-\theta_j)+\alpha\beta(q-t)\right]. \tag{7}$$

These considerations can be inverted. Namely, if dependence on t is assumed for functions $p(t)$ and $q(t)$ then the property of the apparent singularity to stay an apparent singularity along the path $p(t)$, $q(t)$ in the phase space if $p(t)$, $q(t)$ obey the Hamilton system of equations generated by the hamiltonian H. This latter system is equivalent to P^6 derived above.

First order 2×2 linear system. Historically Painlevé equations are more often related to first order 2×2 systems. However the explicit derivation of P^6 from such systems is to the authors experience extremely boring. Moreover, several additional conditions on the system should be posed and it is not clear to what extent they are necessary. A thorough explanation of this general situation is presented in the recent article by M.V. Babich ([6]). Here we present a more particular approach to this problem referring to ([7]). What are the demands to the system if it is assumed to generate (5)?

1. Firstly, regular singularities of this system must be $z_1=0$, $z_2=1$, $z_3=t$, $z_4=\infty$.
2. Secondly characteristic exponents at infinity must be α, β.
3. Transform from the system to a second order equation must lead to only one apparent singularity

The system for a vector function W is assumed to be

$$MW'=NW \tag{8}$$

with the following values of the matrix coefficients for matrices M and N

$$\begin{pmatrix} z^2-z & \rho(z-1)\\ z & z-t-\rho\end{pmatrix}W'=\begin{pmatrix}-\alpha z+e_1 & e_2\\ e_3 & -\beta\end{pmatrix}W. \tag{9}$$

Demands 1. and 2. can be easily checked. System (8) can be brought to the form

$$W'=TW,\qquad T=M^{-1}N=\big(\sigma(z)\big)^{-1}S, \tag{10}$$

where

$$\sigma(z)=\det M=\prod_{j=1}^{3}(z-z_j).$$

Solving system (10) for $w_1(z)$, we obtain the second-order equation

$$w_1''(z)+f^{(1)}(z)w_1'(z)+g^{(1)}(z)w_1(z)=0, \tag{11}$$

where

$$f^{(1)}(z)=-T_{12}'T_{12}^{-1}-\mathrm{tr}T,\qquad g^{(1)}(z)=T_{12}'T_{12}^{-1}T_{11}-T_{11}'+\det T.$$

Next, solving system(10) for $w_2(z)$, we obtain the second-order equation

$$w_2''(z)+f^{(2)}(z)w_2'(z)+g^{(2)}(z)w_2(z)=0, \tag{12}$$

where

$$f^{(2)}(z)=-T_{21}'T_{21}^{-1}-\mathrm{tr}T,\qquad g^{(2)}(z)=T_{21}'T_{21}^{-1}T_{22}-T_{22}'+\det T.$$

The matrix $S(z)$ is evaluated in accordance with (10) and is given by

$$\begin{pmatrix}-\alpha z^2+z\big(e_1-\rho g_2+\alpha t\big)-te_1+\rho f_2 & g_1z-f_1\\ g_2z^2-zf_1 & -\beta z^2+z(\beta-e_2)\end{pmatrix} \tag{13}$$

with

$$f_1=\rho\beta+t-\rho e_2,\quad f_2=e_3+e_1.$$

$$g_1=\rho\beta+e_2,\quad g_2=e_3+\alpha.$$

This implies that in addition to the regular singularities coincident with the regular singularities of system (10), Eqs. (11) and (12) each have only one apparent singularity,

$$q^{(1)} = \frac{\rho\beta + (t-\rho)e_2}{\rho\beta + e_2} \qquad \text{and} \qquad q^{(2)} = \frac{e_3 + e_1}{e_3 + \alpha}. \tag{14}$$

Therefore, these equation are Heun1 equations. We evaluate $\mathrm{tr}T$ and $\det T$, which are the same for Eqs.(11) and (12):

$$\begin{aligned} -\mathrm{tr}T &= \frac{e_1}{z} + \frac{\alpha - e_1}{z-1} + \frac{\beta}{z-t} + \frac{\rho f_2}{z(z-t)} - \frac{1}{z-1}\left(\frac{e_2 - \rho(e_1-\alpha)}{t-1}\right) - \\ &\quad + \frac{1}{z-t}\left(\frac{e_2 - \rho(e_1-\alpha)}{t-1}\right), \\ \det T &= \frac{\alpha\beta}{z(z-1)} + \frac{t\alpha\beta - \beta e_1 - e_2 e_3}{\sigma}. \end{aligned} \tag{15}$$

From (15), we obtain the residue of $\mathrm{tr}T$ at infinity:

$$\lim_{z\to\infty} z\ \mathrm{tr}T = -\alpha - \beta. \tag{16}$$

Using (13), we next evaluate the following expressions, which determine the coefficients of Eqs. (11) and (12):

$$\begin{aligned} -T'_{12}T_{12}^{-1} &= -\frac{1}{z-q^{(1)}} + \sum_{j=1}^{3}\frac{1}{z-z_j}, \quad -T'_{21}T_{21}^{-1} = -\frac{1}{z-q^{(2)}} + \sum_{j=2}^{3}\frac{1}{z-z_j}, \\ T'_{12}T_{12}^{-1}T_{11} - T'_{11} &= \frac{\alpha}{z(z-1)} + \left[\alpha t - e_1 + \rho\frac{f_2 - q^{(1)}g_2}{t-q^{(1)}}\right]\frac{1}{\sigma} + \\ &\quad + \left[-\alpha q^{(1)} + e_1 - \rho\frac{f_2 - q^{(1)}g_2}{t-q^{(1)}}\right]\frac{1}{\sigma^{(1)}}, \\ T'_{21}T_{21}^{-1}T_{22} - T'_{22} &= \frac{e_2 + \beta(q^{(2)}-1)}{t-q^{(2)}}\left(\frac{q^{(2)}}{\sigma^{(2)}} - \frac{t}{\sigma}\right), \end{aligned} \tag{17}$$

where

$$\sigma^{(k)}(z) = z(z-1)\big(z-q^{(k)}\big), \quad k = 1, 2.$$

This preliminary computations enable to find explicit expressions for the coefficients of Eqs. (11) and (12) and as a result explicit formulas for ρ, e_j, $j = 1, 2, 3$ in terms of θ_j, $j = 1, 2$, and p, q. The calculations are troublesome and can be simplified by Computer Algebra systems. Here are given final results only for equation (12) omitting index $^{(2)}$.

$$\begin{aligned} e_1 &= -\sigma_3(q)p - \frac{1}{q-t}(t(q-1)(\theta_1-1) + q(t-1)(\theta_2-\alpha) + \beta\sigma_3(q)), \\ e_2 &= -\sigma_1(q)p - \beta(q-1), \\ e_3 &= -qp - \frac{1}{q-t}\left(t(\theta_1-1) + \frac{q}{q-1}(t-1)\theta_2 + q(\alpha+\beta)\right), \\ \rho &= t\frac{q-1}{q}\frac{e_1+\theta_1-1}{e_1-\alpha} \end{aligned} \tag{18}$$

Of course, inverse formulas can also be obtained.

Integral transform for 2×2 systems. We have studied the Fuchsian system of equations

$$(z^2A+zB+C)\frac{dW}{dz}=(-\alpha zA+E)W, \tag{19}$$

where A, B, C, and E are 2×2 matrices independent on z

$$A=\begin{pmatrix}1&0\\0&0\end{pmatrix}, B=\begin{pmatrix}-1&\rho\\1&1\end{pmatrix}, C=\begin{pmatrix}0&-\rho\\0&\rho-t\end{pmatrix}, E=\begin{pmatrix}e_1&e_2\\e_3&-\beta\end{pmatrix}.$$

If the solution of system (19) is represented as

$$W(z)=\int_L (z-\xi)^{-\alpha}\Phi(\xi)\,dt, \tag{20}$$

where $\Phi(t)$ is a two-vector function and the integration contour L in the complex plane is specified properly then $\Phi(\xi)$ should be a solution of the similar system but with modified matrix coefficients

$$(\xi^2A+\xi B+C)\frac{d\Phi(\xi)}{d\xi}=\big((\alpha-2)\xi A+E+(\alpha-1)B\big)\Phi(\xi)=0, \tag{21}$$

Therefore we arrive to the following chain: Heun1 $\to$ Fuchsian system $\to$ modified Fuchsian system $\to$ modified Heun1. If at the first stage the Painlevé equation is generated then at the end the transformed Painleve equation is obtained. This transformation of Painlevé equations belongs to the Okamoto-type transforms. The other way of derivation the Okamoto transforms was proposed in [8].

Fuchsian system 3×3. A particular Fuchsian system of 3×3 first order equations with three Fuchsian singularities at finite points z_j can also be regarded in respect to Heun equation

$$A(z)\vec{w}'(z)=B\vec{w}(z),\quad \vec{w}(z)=\begin{pmatrix}w_1(z)\\w_2(z)\\w_3(z)\end{pmatrix}. \tag{22}$$

The matrices $A(z)$ and B is supposed to be of the form

$$A(z)=\begin{pmatrix}z-z_1&0&0\\0&z-z_2&0\\0&0&z-z_3\end{pmatrix},\quad B=\begin{pmatrix}b_{11}&b_{12}&b_{13}\\b_{21}&b_{22}&b_{23}\\b_{31}&b_{32}&b_{33}\end{pmatrix}. \tag{23}$$

The particularity of (22) is determined by the specific values of Frobenius exponents at singularities

$$\rho_{mj}=0,1,b_{jj}$$

With already introduced notation for σ and σ_j and parameters k and q introduced by

$$k=b_{13}B_{21}+b_{12}B_{31}$$

$$q=\frac{b_{13}B_{21}z_2+b_{12}B_{31}z_3}{b_{13}B_{21}+b_{12}B_{31}}$$

the following third order Fuchsian equation can be derived [9]

$$\sigma(z)w_1'''(z) - \left(\sum_{j=1}^{3}\sigma_j(z)(b_{jj}-1) - \sigma_1(z) + \frac{\sigma}{z-q}\right)w_1''(z) + \left(\sum_{j=1}^{3}B_{jj}(z-z_j) - \frac{(1-b_{11})\sigma_1}{z-q} + \frac{B_{11}b_{13}b_{12}(z_2-z_3)z}{k(z-q)}\right)w_1' - \frac{(z_2-z_3)b_{13}b_{12}\det B}{k(z-q)}w_1 = 0. \tag{24}$$

It has Fuchsian singularities at $z = z_j$ and one additional apparent singularity at $z = q$.

Along with (24) a particular Fuchsian third-order equation with singularities located at the points $z_1 = 0$, $z_2 = 1$, $z_3 = t$ can be considered

$$\sigma y(z)''' + \sum_{j=1}^{3} b_j\sigma_j y(z)'' + ((\Delta_2+\Delta_1+1)(z-z_3)+\lambda)y(z)' + \Delta_3 y(z) = 0. \tag{25}$$

Here Δ_1, Δ_2, Δ_3 are standard symmetric functions of three parameters a, b, c

$$\Delta_1 = a+b+c, \quad \Delta_2 = ab+bc+ac, \quad \Delta_3 = abc.$$

Parameters a, b, c, b_j, $j = 1, 2, 3$ determine local behaviour of solutions at singularities z_j and ∞. Parameter λ is an accessory parameter. The Riemann scheme for this equation

$$\begin{pmatrix} z_1 & z_2 & z_3 & \infty & z \\ 0 & 0 & 0 & a & \lambda \\ 1 & 1 & 1 & b & \\ 2-b_1 & 2-b_2 & 2-b_3 & c & \end{pmatrix} \tag{26}$$

shows the Frobenius characteristic exponents. It means that at each finite singularity there is one holomorphic solution depending on two initial data and one solution which in general is not holomorphic.

Comparing (24) and (25) one sees that in principle they only differ in existence of an additional apparent singularity in (24). Equation (25) is obtained from (24) by specification of parameters and additional s-homotopic transform. Assuming, for example, $a = 0$ we arrive to one equation with the solution equal to a sum of a constant and general solution of Heun equation. The other possibility to obtain this result is the use of an appropriate Euler transform [10].

References

[1] S. Slavyanov, J.Phys A., 29, 7329-7335, (1996).
[2] S. Slavyanov, Theor. Mat. Phys., **123**,744-753, (2000).
[3] S. Slavyanov, W. Lay, Special functions: a unified theory based on singularities. OUP, 2000.
[4] S. Slavyanov, W. Lay, A. Akopyan, A. Pirozhnikov, V. Dmitriev, A. Yatzik, V. Zhegunov, SIGSAM Bulletin, **33**, 21-27, (1999).
[5] S. Slavyanov, Operator theory: Advances and Applications, **132**, 395-402, (2002).
[6] M.V. Babich, Russian Math. Surv. **64**, 45-127, (2009).
[7] A.Ya. Kazakov, S.Yu. Slavyanov, Theor. Math. Phys, **155**, 721-732, (2008).
[8] D.P. Novikov, Theor. Math. Phys., **146**, 355-364,(2006).
[9] S.Yu. Slavyanov, F.R. Vukajlović,Theor. Math. Phys., **150**, 123-131, (2007).
[10] A.Ya. Kazakov,Theor. Math. Phys, **116**, 323-329, (1998).

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 203–211
ISSN 1930-1235: (2010)

ON THE KEY EXCHANGE WITH MATRICES OF LARGE ORDER AND GRAPH BASED NONLINEAR MAPS

URSZULA ROMAŃCZUK AND VASYL USTIMENKO

The project is co-funded from the sources of the European Union
within the limit of the European Social Fund.

Human - The Best Inwestment

Abstract. In the paper we discuss the group theoretical algorithm of Diffie - Hellman key exchange in the cases of symmetrical group S_{p^n} and more general Cremona group of polynomial automorphisms of free module $\mathbb{K}^n$ over arbitrary commutative ring $\mathbb{K}$. We show that conjugation of affine map with nonlinear polynomial map f can be element of large order and small degree. Same properties hold for each element of cyclic group generated by such elements. We consider some algorithms for generation of subgroups of large order and small degree of their elements.

1. Introduction

It is a well-known fact that the discrete logarithm problem can be formulated for general finite group G. Find a positive integer x satisfying condition $g^x = b$ where $g \in G$ and $b \in G$. The problem has a reputation to be a difficult one. But even in the case of cyclic group $\mathbb{Z}_n^*$ there are many open questions. If $n = p$ or $n = pq$ where p and q are sufficiently large prime then the complexity of discrete logarithm problem justify classical Diffie-Hellman key exchange algorithm and RSA public key encryption, respectively. In most other cases complexity of discrete logarithm problem is not investigated properly. The problem is very dependent on the choice of the base g and the way of presentation the data on the group. Group can be defined via generators and relations, as automorphism group of algebraic variety, as matrix group, as permutation group etc. in this paper we assume that G is a subgroup of S_{p^n} which is a group of polynomial bijective transformation of vector space ${\mathbb{F}_p}^n$ into itself. Obviously $|S_{p^n}| = p^n!$, each permutation π can be written in the form

Key words and phrases. Key exchange, Public Key Cryptography, Symbolic Computations .

$$x_1 \to f_1(x_1, x_2, \dots, x_n),$$
$$x_2 \to f_2(x_1, x_2, \dots, x_n),$$
$$\dots$$
$$x_n \to f_n(x_1, x_2, \dots, x_n),$$

where f_i are multivariable polynomials from $\mathbb{F}_p[x_1, x_2, \dots, x_n]$. The presentation of G as a subgroup of S_{p^n} is chosen because the Diffie Hellman algorithm here will be implemented by the tools of symbolic computations. Other reason is universality: as it follows from classical Cayley results each finite group G can be embedded in S_{p^n} for appropriate p and n in various ways.

The Diffie Hellman key exchange is another breakthrough in public-key cryptography of the 1970s, invented by Whitfield Diffie and Martin Hellman in their groundbreaking 1976 paper New Directions in Cryptography. Algorithm Diffie-Hellman allows two users (Alice and Bob) to establish a shared secret key used by encryption algorithms, such as DES or MD5, over an insecure communications channel.

Algorithm 1. ***Symbolic Diffie-Hellman algorithm***

1. The first step Alice and Bob take is to agree on a finite group G, $G < S_{p^n}$ and a polynomial map g in G of large order in a group G. This is usually done long before the rest of the protocol. The next step is for Alice to pick a secret integer n_A that she does not reveal to anyone, while at the same time Bob picks an integer n_B that he keeps secret.
3. Bob and Alice use their secret integers to compute $A = g^{n_A}$ and $B = g^{n_B}$ in S_{p^n}, respectively. They use composition of multivariable map g with itself.
4. They next exchange these computed values, Alice sends A to Bob and Bob sends B to Alice.
5. Finally, Bob and Alice again use their secret integers to compute

$$AB \equiv B^{n_A} \equiv (g^{n_B})^{n_A} = g^{n_A n_B} \qquad \text{and} \qquad AB \equiv A^{n_B} \equiv (g^{n_A})^{n_B} = g^{n_A n_B}$$

Eavesdropper only learns p, g, g^{n_A} and g^{n_B}, but cannot calculate $g^{n_A n_B}$ without the computationally difficult discrete logarithm problem of A or B for the group G.

The security of the protocol depends heavily on the choice of the base g. It has to be an element of large order $|g|$, prime decomposition of $|g|$ is very important.

This scheme of "symbolic Diffie-Hellman algorithm" can be secure, if the adversary is not able to compute number n_A (or n_B) as functions from degrees for g and h_A. Obvious bad example is the following: g sends x_i into ${x_i}^t$ for each i. In this case n_A is just a ratio of $\deg h_A$ and $\deg g$.

To avoid such trouble one can look at the element (base) g of S_{p^n} such that all its nonidentical powers q^k are of small degree $f(n)$, which is independent of parameter k. We refer to such g as stable element. In the of prime field $\mathbb{F}_p$, affine transformations form an affine group $AGL_n(\mathbb{F}_p)$ of order $(p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$ in the symmetric group S_{p^n} of order $(p^n)!$. In [6] the maximality of $AGL_n(\mathbb{F}_p)$ in S_{p^n} was proven. So we can present each permutation π as a composition of several "seed" maps of kind $\tau_1 g \tau_2$, where $\tau_1, \tau_2 \in AGL_n(\mathbb{F}_p)$ and g is a fixed map of degree

≥ 2. One may choose quadratic map of Imai - Matsumoto algorithm in case $p = 2$ (see [4]0 for its description and cryptanalysis by J. Patarin) or graph based cubical maps for general p ([12], [14], [16], [17]).

One of the obvious source of stable elements is the group $AGL_n(\mathbb{F}_p)$ of affine transformations. We can take the group G in the form $\tau H\tau^{-1}$, where H is a subgroup of $AGL_n(\mathbb{F}_p)$ and τ is a fixed element of S_{p^n}. Degree of each representative of $AGL_n(\mathbb{F}_p)$ is 1, this group contains elements of large order, like famous Singer cycle of order $p^n - 1$ (see [5] and further references) . The choice of nonlinear τ is important, it eliminates the usage of standard tools of linear algebra for studies of H-invariant subspaces.

One can consider the product of a Singer cycle with the matrix whose order is mutually prime with $p^n - 1$ to make the order flexible.

We refer to an element g of kind $f\tau f^{-1}$, where $\tau \in AGL_n(\mathbb{F}_p)$, f and f^{-1} are polynomial maps of ${\mathbb{F}_p}^n$ into itself of the same degree such as $f\tau \neq \tau f$ as quasi linear map. We say that $g = f\tau f^{-1}$ is of *irreducible degree* if $\deg(g) = \deg(f)\deg(f^{-1})$. In case of stable pseudo linear element g of irreducible degree all its nonidentical powers are of irreducible degree.

We suggest the following scheme:

(1) Choose an affine transformation τ of large order S (for instance a product of Singer cycle with the matrix of order t such that $gcd(t, p^n - 1) = 1$).
(2) Construct invertible polynomial transformation f of large degree of rather general form.
(3) Compute $b = f\tau f^{-1}$ ("most" elements of that kind $f\tau^k f^{-1}$ will be of maximal degree $\deg(f)\deg(f^{-1})$).

Method of construction of sequences of stable elements in S_{p^n} of nonpseudolinear nature with large degree and order are consider in the papers of [16].

We believe that independently on our scheme problems of generation of matrices of large order and construction of invertible polynomials of large degree are of applied nature.

We generalize the above problem for the case of Cremona group of the free module $\mathbb{K}^n$, where $\mathbb{K}$ is arbitrary commutative ring. So we need change ${\mathbb{F}_p}^n$ for free module $\mathbb{K}^n$ (Carthesian power of $\mathbb{K}$) and the family and symmetric group S_{p^n} for Cremona group $C_n(\mathbb{K})$ of all polynomial automorphisms of $\mathbb{K}^n$.

2. Linguistic graphs and nonlinear elements of Cremona group

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [1]. Let $V(G)$ and $E(G)$ denote the set of vertices and the set of edges of G, respectively. Then $|V(G)|$ is called the *order* of G, and $|E(G)|$ is called the *size* of G. A path in G is called *simple* if all its vertices are distinct. When it is convenient, we shall identify G with the corresponding anti-reflexive binary relation on $V(G)$, i.e. $E(G)$ is a subset of $V(G) \times V(G)$ and write vGu for the adjacent vertices u and v (or neighbors). The sequence of distinct vertices $v_0, v_1, \ldots, v_t$, such that v_iGv_{i+1} for $i = 1, \ldots, t-1$ is the *pass* in the graph. The *length of a pass* is a number of its edges. The *distance* $\mathrm{dist}(u, v)$ between two vertices is the length of the shortest pass between them. The *diameter* of the graph is the maximal distance between two vertices u and v of the graph. Let C_m denote the *cycle* of length m i.e. the sequence of distinct vertices $v_0, \ldots, v_m$ such that v_iGv_{i+1}, $i = 1, \ldots, m-1$ and v_mGv_1. The *girth* of a graph G, denoted by $g = g(G)$, is the length of the shortest

cycle in G. The *degree of vertex* v is the number of its neighbors (see , for instance [1]).

The *incidence structure* is the set V with partition sets P (points) and L (lines) and symmetric binary relation I such that the incidence of two elements implies that one of them is a point and another is a line. We shall identify I with the simple graph of this incidence relation (bipartite graph). If number of neighbors of each element is finite and depends only on its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [7]).

Definition 1. Let Γ be a bipartite graph with partition sets P_i, $i = 1, 2$. Suppose that M be a disjoint union of finite sets M_1 and M_2. We say that Γ is a *bipartite parallelotopic graph* over (M_1, M_2) if

(*i*) there exists a function $\pi : V(\Gamma) \to M$ such that if $p \in P_i$, then $\pi(p) \in M_i$,
(*ii*) for every pair (p, j), $p \in P_i$, $j \in M_i$, there is a unique neighbour u with given $\pi(u) = j$.

It is clear that the bipartite parallelotopic graph Γ is a $(|M_1|, |M_2|)$ - biregular graph.

We refer also to the function π in the definition of bipartite parallelotopic graph as a *labelling*. We will often omit the term "bipartite", because all our simple graphs are bipartite.

Let P and L be two copies of n-dimensional free module $\mathbb{K}^n$ over the finite commutative ring $\mathbb{K}$. 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 choose two fixed bases and write:

$$(p) = (p_1, \dots, p_n, c_1, c_2, \dots, c_r)$$
$$[l] = [l_1, \dots, l_n, t_1, t_2, \dots, t_s]$$

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:

$$\begin{aligned} a_1 l_1 - b_1 p_1 &= f_1(c_1, \dots c_r, t_1, \dots, t_s) \\ &\dots \\ a_i l_i - b_i p_i &= f_i(c_1, \dots c_r, t_1, \dots, t_s, l_1, \dots, l_{i-1}, p_1, \dots, l_{i-1}) \\ &\dots \\ a_n l_n - b_n p_n &= f_n(c_1, \dots c_r, t_1, \dots, t_s, l_1, \dots l_{n-1}, p_1, \dots, p_{n-1}) \end{aligned} \tag{1}$$

where f_i, $i = 2, \dots, n$ can be any polynomial expressions in variables c_1, $\dots$, c_r, t_1, $\dots$, t_s, l_1, $\dots$, l_{i-1}, p_1, $\dots$, p_{i-1} over $\mathbb{K}$, a_i, b_i can be any nonzero elements from $\mathbb{K}$.

It is easy to see that the above graph is a parallelotopic graph such that tuples $c_1, \dots c_r$ and $t_1, \dots, t_s$ be the "colours" of (p) and $[l]$, respectively. Let $C(P) = \mathbb{K}^r$ and $C(L) = \mathbb{K}^s$ are sets of colours for points and Lines

Let us refer to the graph $I = I(n, r, s)$ defined by above equations as *linguistic graphs of triangular type over* $\mathbb{K}$ of type (r, s, n). We assume that one of the expressions f_i, $i = 1, 2, \dots, n$ has degree ≥ 2.

The *colour function* π for such a graph is just a projection of tuples $(p) \in P$ and $[l] \in L$ onto r and s last components, respectively. We assume that $N_c(v)$ is the operator of taking the neighbour of v of colour c in our parallelotopic graph.

The linguistic graphs naturally appear as induced subgraphs of Incidence Geometries of Finite Simple Groups of Lie type. They play an important role in studies of Large Schubert cell related to the geometry ([10], [11]). The following examples are induced subgraphs of incidence geometries of rank 2. The theory of incidence geometries corresponding to finite simple groups of Lie type the reader can find in [2], [9]. Special dynamical systems related to linguistic graphs were introduced in [15].

Example 1. Let $P = \{(x_1, x_2)|x_i \in GF(q)\}$, $L = \{[y_1, y_2]|y_i \in GF(q)\}$. Let us define an incidence relation I_1 as: $(a, b)I_1[x, y]$ if and only if $y - b = xa$. Let us consider the function $\pi : P \cup L \to GF(q)$, such that $\pi((x_1, x_2)) = x_1$, $\pi([y_1, y_2]) = y_1$. It is easy to check that π is a labelling for the graph I_1. It is a linguistic graph of type $(1, 1, 1)$ over $GF(q)$. This is the induced subgraph of the incidence graph of the geometry for simple group $A_2(q)$ (classical Desargues projective plane).

Example 2. Let $P = \{(x_1, x_2, x_3)|x_i \in GF(q)\}$, $L = \{[y_1, y_2, y_3]|y_i \in GF(q)\}$. Let us define an incidence relation I_2 as: $(a, b, c)I_2[x, y, z]$ if and only if

$$y - b = xa \text{ and } z - c = xb.$$

Let us assume that $\pi((x_1, x_2, x_3)) = x_1$ and $\pi([y_1, y_2, y_3]) = y_1$. It is clear, that I_2 defines a family of linguistic graphs over $GF(q)$ with parameters (1, 1, 2). This is the induced subgraph of the incidence graph of the geometry for simple group $B_2(q)$ (classical regular generalised quadragon). So the girth of I_2 (length of minimal cycle) is at least 8.

Example 3. Let $P = \{(x_1, x_2, x_3, x_4, x_5)|x_i \in GF(q)\}$, $L = \{[y_1, y_2, y_3, y_4, y_5]|y_i \in GF(q)\}$. Let us define an incidence relation I_3 as: $(a, b, c, d, e)I_3[x, y, z, u, v]$ if and only if

$$\begin{aligned} y - b &= xa \\ z - 2c &= -2xb \\ u - 3d &= -3xc \\ 2v - 3e &= 3zb - 3yc - ua \end{aligned}$$

From the equations above, it follows that $\pi : \pi((x_1, x_2, x_3, x_4, x_5)) = x_1$ and $\pi([y_1, y_2, y_3, y_4, y_5]) = y_1$ is a labelling for I_3.

This is the induced subgraph of the geometry of group $G_2(q)$ (generalised gexagon).

If char$GF(q) > 3$ then the girth of this graph is at least 12. Directly from the equations above we can get that I_3 is the linguistic graph with parameters (1, 1, 4) over $GF(q)$.

Example 4. Let $GF(q^2)$ be the quadratic extension of $GF(q)$ and $x \to x^q$ be the Frobenius automorphism of $GF(q^2)$. Let $P = \{(x_1, x_2, x_3)|x_1 \in GF(q), x_2 \in GF(q^2), x_3 \in GF(q)\}$, $L = \{[y_1, y_2, y_3]|y_1 \in GF(q^2), y_2 \in GF(q^2), y_3 \in GF(q)\}$. Let us define the incidence relation I_4 as: $(a, b, c)I_4[x, y, z]$ if and only if

$$\begin{aligned} y - b &= xa \\ z - c &= ay + ay^q. \end{aligned}$$

It is clear that rules $\pi((x_1, x_2, x_3)) = x_1$ and $\pi([y_1, y_2, y_3]) = y_1$ define the parallelotopic graph over $GF(q^2)$, It is a linguistic graph over $\mathbb{F}_q$ of the type it's parameters are $(1, 2, 3)$.

Algorithm 2. Let us consider the sequence of linguistic graphs $I_1, I_2, \ldots, I_d$ of the same type (n, r, s) over commutative ring $\mathbb{K}$.

Let $C_j(P)$ and $C_j(L)$ be sets of colours for points and lines in the graph I_j. Let η_j, $j = 2, 3, \ldots, d$ and $\eta_j{}'$, $j = 1, 2, \ldots, d-1$ be the affine maps from $C_1(P)$ to $C_j(P)$ and $C_j(L)$, respectively. Let us assume that η_d is an invertible affine map.

We need also an invertible affine transformations $\delta_1$and δ_2 of the point set P_1 and the point set P_d within the graphs I_1 and I_d, respectively.

We take general point $\mathrm{x} = (x_1, x_2, \ldots x_{n+r})$ from P_1 and compute $v_1 = \delta_1(\mathrm{x})$ and the color $c_1 = \pi(v_1)$. After that we are compute consequently colours $c_j{}' = \eta'_j(c_1)$, $j = 1, 2, \ldots, d-1$, $c_j = \eta_j(c_1)$, $j = 2, 3, \ldots, d$. It allows us to compute the bijective composition of $\delta_1 N_{c'_1} N_{c_2} N_{c'_2} \ldots N_{c_{d-1}} N_{c'_{d-1}} N_{c_d} \delta_2$. Let

$$u = \delta_1 N_{c'_1} N_{c_2} N_{c'_2} \ldots N_{c_{d-1}} N_{c'_{d-1}} N_{c_d} \delta_2(\mathrm{x}).$$

The inverse of our map is the following one. We apply ${\delta_2}^{-1}$ to u and get the vertex u' of the graph of colour $c_d = \eta_d(\pi(v_1))$. The map η_d is invertible. So we compute c_1 and all colours c_j and $c_j{}'$. It allows us to compute x as $N_{c'_{d-1}} N_{c_{d-1}} \ldots N_{c_2} N_{c'_1} {N_{c_1}}{\delta_1}^{-1}(u')$.

Remark 1. In case of regular linguistic graphs we can also add $c'_d = \eta'_d(c_1)$.

Example 5. Let us consider the following bipartite algebraic graph $A = A(n, \mathbb{K})$ ($a$lternating graph) defined over commutative ring $\mathbb{K}$ by the following rules.

Partition sets P and L are two copies of the free module $\mathbb{K}^n$. Brackets and paranthesis allow us to distinguish point $\mathrm{p} = (p_1, p_2, \ldots, p_n)$ and line $\mathrm{l} = [l_1, l_2, \ldots, l_n]$. In case of even $n = 2t$ point p is incident to line l if and only if the following equations hold:

(1) $l_{2s} - p_{2s} = l_1 p_{2s-1}$ for $s = 1, 2, \ldots t$, $t = [n/2]$
(2) $l_{2s-1} - p_{2s-1} = p_1 l_{2s-2}$ for $s = 2, 3, \ldots, d$,

where $d = t$ for even n and d=t+1 if n is odd.

The graph is a linguistic graphs of triangular type over $\mathbb{K}$ of type $(1, 1, n-1)$.

We announce here the following statement.

Proposition 1. If we set $I_1 = A(n, \mathbb{K}), I_2 = A(n, \mathbb{K}), \ldots, I_d = A(n, \mathbb{K})$, $n \geq 2$, $d \leq n$ and nonidentical map η_d of $\mathbb{K}$ onto itself, then the algorithm 2 produces a cubical map of $\mathbb{K}^n$ onto itself.

Let $C_j(P)$ and $C_j(L)$ be sets of colours for points and lines in the graph I_j. Let η_j, $j = 2, 3 \ldots, d$ and $j = 1, 2 \ldots, d$ and $\eta_j{}'$, $j = 2, 3 \ldots, d$ be the affine maps from $C_1(P)$ to $C_j(L)$ and $C_j(L)$, respectively. Let us assume that η_d is an invertible affine map. We implement the key exchange algorithm in the case $\mathbb{K} = \mathbb{F}_q$ with the base $b = f^{-1} A f$ where f is a cubical map as in Proposition 1 and A is a linear map corresponding to Singer cycle of order $q^n - 1$. Alternatively we can use different cubical map defined in [12], [14], [16], [7]. Obviously the order of b is $q^n - 1$ and degree of each b^k is bounded by 9.

2.1. **Symbolic computations on flags of linguistic graphs.** Let us consider a tactical configuration of order (s, t) for biregular bipartite simple graphs with

bidegrees $s+1$ and $r+1$. It corresponds to incidence structure with the point set P, line set L and symmetric incidence relation I. Its size can be computed as $|P|(s+1)$ or $|L|(t+1)$. For the simplicity we choose $t=s$

Directed graph is an irreflexive binary relation $\phi \subset V \times V$, where V is the set of vertices (see [1]).

Let us introduce two sets

$$id(v) = \{x \in V | (v,x) \in \phi\},$$

$$od(v) = \{x \in V | (x,v) \in \phi\}$$

as sets of inputs and outputs of vertex v. Regularity means the cardinality of these two sets (input or output degree) are the same for each vertex.

Let Γ be regular directed graph, $E(\Gamma)$ be the set of arrows of graph Γ.

Let $F = \{(p,l) | p \in P,\ l \in L,\ pIl\}$ be the totality of flags for the regular tactical configuration T with partition sets P (point set) and L (line set) and incidence relation I. We define the following irreflexive binary relation ϕ on the set F: Let (P,L,I) be the incidence structure corresponding to regular tactical configuration of order t.

Let $F_1 = \{(l,p) | l \in L, p \in P, lIp\}$ and $F_2 = \{[l,p] | l \in L, p \in P, lIp\}$ be two copies of the totality of flags for (P,L,I). Brackets and parenthesis allow us to distinguish elements from F_1 and F_2. Let $DF(I)$ be the directed graph (double directed flag graph) on the disjoint union of F_1 with F_2 defined by the following rules:

(i) $(l_1,p_1) \to [l_2,p_2]$ if and only if $p_1 = p_2$ and $l_1 \neq l_2$,
(ii) $[l_2,p_2] \to (l_1,p_1)$ if and only if $l_1 = l_2$ and $p_1 \neq p_2$.

Let Γ be a directed graph as above on the set of vertices $F_1 \cup F_2$.

Let us assume that additionally we have a parallelotopic colouring π on T . Then we assume that $\pi[l,p] = \pi(l)$ and $\pi(l,p) = \pi(p)$.

Then for each vertex v of double directed graph and each colour c we have unique vertex u such that $\pi(u) = c$ and $v \to u$. We assume that $N_c(v) = u$.

Algorithm 3. Let us consider the sequence of regular linguistic graphs I_1, I_2, ..., I_d of the same type (r,r,n) over commutative ring $\mathbb{K}$. Suppose that $N_c^i(v)$, $i = 2,,3 \ldots, d$ be the sequence of the operators taking the neighbour of v of colour c in graph I_i. Let $\eta_i,\ i = 2,3,\ldots,d$ be the sequence of affine maps of $\mathbb{K}^r$ into $\mathbb{K}^r$. We take η^d as inveritable map.

We need also an invariable affine transformations δ_i, $i = 1,2$ of the free module $\mathbb{K}^{n+2r}$ into itself.

We take the general flag x = $(x_1,\ x_2,\ldots,\ x_{n+2r})$ from F_1 and the colour $c_1 \in \mathbb{K}^r$ and compute $N_{c_2}^2(\mathrm{x}) = v \in F_2$. After we compute the consequently colours $c_i = \eta_2(c_1)$, $i = 2,3,\ldots,d$.

It allow us to compute symbolically the map $f = \delta_1 N_{c_3}^3 N_{c_4}^4 \cdots N_{c_{d-1}}^{d-1} N_{c_d}^d \delta_2$ of the free module $\mathbb{K}^{n+2r}$ into itself. The output of our algorithm is the flag $w = f(v)$.

Constructing an inverse mapping to f, we assume that the vertices which belong to F_1 now belong to F_2 and vice versa, vertices belonging to F_2 now belong to F_1. The map η_d is inveritable, so we compute c_1 and c_j, $j = 2,3,\ldots,d$. It allows as to compute v as $\delta_2^{-1} N_{c_{d-2}}^{d-1} N_{c_{d-3}}^{d-2} \cdots N_{c_2}^3 N_{c_1}^2 \delta_1^{-1}(w)$.

Remark 2. *The above algorithm can be easily generalised on the sequence of biregular linguistic graphs of the same type* (r,s,n).

TABLE 1. Time of public key generation

	$d=10$	$d=20$	$d=30$	$p=40$	$d=50$	$d=60$
$n=10$	7	7	8	15	15	16
$n=20$	54	125	195	265	343	421
$n=30$	304	742	1234	1703	2234	2805
$n=40$	1109	3696	6414	9109	12284	14812
$n=50$	2750	8937	17039	24976	33374	41164
$n=60$	6101	21312	43961	69453	96421	121267
$n=70$	11371	40726	84625	143094	202750	268320
$n=80$	23007	82937	175320	309960	455890	601187
$n=90$	46062	166320	354429	631469	947328	1262682
$n=100$	929625	293641	641305	1110305	1752766	244981

Proposition 2. If we set $I_1 = A(n,\mathbb{K}), I_2 = A(n,\mathbb{K}), \ldots, I_d = A(n,\mathbb{K})$, $n \geq 2$, $d \leq n$ and nonidentical map η_d of K onto itself, then the algorithm 2 also produces a cubical map of $\mathbb{K}^n$ onto itself.

3. Time evaluation of the generation of the map f

The parameter n is the dimension of point space ${\mathbb{F}_{2^k}}^n$ of our graph. Below you can find time evaluation tables for symbolic computations of f in cases of finite fields $\mathbb{K} = \mathbb{F}_{2^k}$, $k \in \{8, 16, 32\}$.

All the tests were run on a computer with parameters:

- AMD Athlon 1.46 GHz processor
- 1 GB RAM memory
- Windows XP operating system.

The table **??** presents the time (in milliseconds) of the generation of the symbolic base depending on the number of variables (n) and the size of parameter (d). In fact we ignore the restriction $d < n$. In all cases the base is a cubical map. We use sparse linear transformations $\delta_i, i = 1, 2$ of kind $x_1 \to a_1x_2 + a_2x_3 + \ldots, a_nx_n$, $x_j \to x_j$, $j = 2, 3, \ldots$ where a_i are fixed nonzero field elements.

4. Remarks on the b^k as a public rule

The transformation b or b^k can be used as a public rules. Hence the process of straightforward computation of b for chosen point p can be done in polynomial time $O(n^{10})$. But the adversary having only a standard formula for b, has a very hard task to solve the system of n equations in n variables of degree 9 . We know that the variety of solution has the dimension 0. Therefore, general algorithm for finding the solution of system of polynomials cubic equations has exponential time $9^{O(n)}$.

References

[1] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1982
[2] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York, 1977. (1972).
[3] Neal Coblitz, *A Course in Number Theory and Cryptography*, Second Edition, Springer, 1994, 237 p.
[4] Neal Coblitz, *Algebraic Aspects of Cryptography*, Springer, 1998, 198 p.

[5] A. Cossidente, M. J. de Ressmine, *Remarks on Singer Cycle Groups and Their Normalizers*, Desighns, Codes and Cryptography, 32, 97-102, 2004.
[6] B. Mortimer, *Permutation groups containing affine transformations of the same degree*, J. London Math. Soc., 1972, 15, N3, 445-455.
[7] E. H. Moore, *Tactical Memoranda*, Amer. J. Math., v.18, 1886, 264-303.
[8] J. Tits, *Sur la trialite at certains groupes qui s'en deduicent*, Publ. Math. I.H.E.S. 2 (1959), 15-20.
[9] J. Tits, *Buildings of spherical type and Finite BN-pairs, Lecture Notes in Math*, Springer Verlag, 1074.
[10] V. A. Ustimenko, *On the Varieties of Parabolic Subgroups, their Generalizations and Combinatorial Applications*, Acta Applicandae Mathematicae 52 (1998): pp. 223–238.
[11] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, vol. 71, N2, November 2002, 117-153.
[12] V. A. Ustimenko, *Maximality of affine group, and hidden graph cryptosystems*, J. Algebra and Discrete Math., 10 (October 2004), 51-65.
[13] V. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, v. 2227, 278-287.
[14] 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).
[15] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.
[16] V. A. Ustimenko, A. Wróblewska, *On the key exchange with nonlinear polynomial maps of degree 4* (to appear)
[17] A. Wróblewska *On some properties of graph based public keys* , Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234 p.

Maria Curie-Sklodowska University in Lublin (Poland)
E-mail address: urszula_romanczuk@yahoo.pl, and ustimenko_vasyl@yahoo.com

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 213–221
ISSN 1930-1235: (2010)

SOME COMPUTATION PROBLEMS ARISING IN FONTAINE THEORY

RADU GABA AND BENJAMIN JUSTUS

Abstract. In this note we construct special types of rings $A_{\max,\mathrm{n}}$ which are used in sequel work to define new types of families of continuous Fontaine sheaves. We also study the maps θ_n and q_n providing explicit description of their kernels. Finally, we implement an algorithm which leads to the computation of these kernels.

1. Introduction

Let us fix a prime integer p and a finite extension K of $\mathbb{Q}_p$ with residue field k and ring of integers $\mathcal{O}_K$ and denote by G_K the Galois group of $\overline{K}$ over K where $\overline{K}$ is a fixed algebraic closure of K. Write K_0 for the maximal unramified extension of $\mathbb{Q}_p$ in K. Also let X be a smooth, proper and connected scheme over K and denote by $X_{\overline{K}}$ the geometric generic fiber of X.

In order to decide the nature of the G_K-representation $H^i_{\mathrm{et}}(X_{\overline{K}},\mathbb{Q}_p)$, $i\geq 0$ one needs to use "comparison isomorphisms theorems" i.e. theorems comparing p-adic étale cohomology of $X_{\overline{K}}$ to other cohomology theories associated to X. For example, if X has good reduction the cohomology theory we refer to is the crystalline cohomology of the special fiber of a smooth proper model of X over $\mathcal{O}_K$. Denote this special fiber by $\overline{X}$.

The crystalline comparison conjecture was formulated by J.-M. Fontaine in [Fo1] and proved by G. Faltings in [Fa]:

Theorem 1.1. *For every $i\geq 0$ there is a canonical isomorphism of B_{cris}-modules, which respects the G_K-actions, the Frobenii and the filtrations*

$$H^i_{\mathrm{et}}(X_{\overline{K}},\mathbb{Q}_p)\otimes_{\mathbb{Q}_p} B_{\mathrm{cris}}\cong H^i_{\mathrm{cris}}(\overline{X}/\mathcal{O}_K)\otimes_{\mathcal{O}_K} B_{\mathrm{cris}},$$

where B_{cris} is the crystalline period ring defined by J.-M. Fontaine in [Fo1].

In [AI] a new method of attacking comparison isomorphisms is supplied provided $K=K_0$ i.e. K is unramified over $\mathbb{Q}_p$.

One defines the Faltings's topology $\mathfrak{X}_{\overline{K}}$ on the smooth proper model of X over $\mathcal{O}_K$ (see [AI] for details).

A. Iovita and F. Andreatta are defining in [AI] new sheaves of rings $\mathbb{A}^{\nabla}_{\mathrm{cris}}$ and $\mathbb{A}_{\mathrm{cris}}$ on $\mathfrak{X}_{\overline{K}}$ and they prove the following:

Theorem 1.2. $H^i_{\mathrm{et}}(X_{\overline{K}},\mathbb{Q}_p)\otimes_{\mathbb{Q}_p} B_{\mathrm{cris}}\cong H^i(\mathfrak{X}_{\overline{K}},\mathbb{A}^{\nabla}_{\mathrm{cris}})\otimes_{A_{\mathrm{cris}}} B_{\mathrm{cris}}\cong H^i_{\mathrm{cris}}(\overline{X},K_0)\otimes_{K_0} B_{\mathrm{cris}}$.

This article deals with the construction of certain families of rings $(A_{\max,\mathrm{n}})_{n\geq 1}$, $(A'_{\max,\mathrm{n}})_{n\geq 1}$. The construction of these rings are carried out in section 4. We study the maps θ_n, q_n, $\bar{q}_n$ and provide explicit description of their kernels in section 3. In section 5, we discuss algorithms which allow us to compute the kernels of θ_n and q_n. The details of the computational experiments and relevant results are included in the same section. We begin in section 2 by recalling some basic facts of Fontaine theory and set out the notations that are used throughout the paper. In the appendix, the readers will find an algorithm which was used in the paper.

One uses the rings $A_{\max,\mathrm{n}}$ to construct a family of sheaves of rings $(\mathbb{A}^{\nabla}_{\max,\mathrm{n}})_{n\geq 1}$ on Faltings's topology $\mathfrak{X}_{\overline{K}}$ associated to X and a smooth, proper model of it and study their properties, most important the localization over small affines (see [Ga] for details). The second family of rings namely $(A'_{\max,\mathrm{n}})_{n\geq 1}$ is used to define the sheaves of rings $(\mathbb{A}'^{\nabla}_{\max,\mathrm{n}})_{n\geq 1}$ which are related to the first family of sheaves via the isomorphism

Received by the editors June 15, 2010 .
2000 *Mathematics Subject Classification.* Primary: 14F30; Secondary: 14F25.
Key words and phrases. Fontaine sheaves, p-adic cohomology, crystalline cohomology.

$\mathbb{A}^{\nabla}_{\mathrm{max,m}}/p^n\mathbb{A}^{\nabla}_{\mathrm{max,m}} \cong \mathbb{A}'^{\nabla}_{\mathrm{max,n}}$ for $m \geq n+2$ (see [Ga], Lemma 3.2.5) and which plays a key role in proving the localization over small affines theorem (see [Ga], Theorem 3.2.7).

The rings $A_{\mathrm{max,n}}$ will also be used in sequel work to define a Riemann-Hilbert correspondence between p-adic locally constant sheaves on X and F-isocrystals on the special fiber of the fixed smooth model of X over $\mathcal{O}_K$.

The first four sections of the paper were written by the first author while the next three were the joint work of both authors.

2. Notations and Background

Let us fix as before a prime integer p, a finite extension K of $\mathbb{Q}_p$ with residue field k and an algebraic closure of K, $\overline{K}$ with residue field $\overline{k}$. Denote by G_K the Galois group of $\overline{K}$ over K, by $\mathcal{O}_K$ the ring of integers of K and by $\mathcal{O}_{\overline{K}}$ the ring of integers of $\overline{K}$. Also denote by $\mathbb{C}_K$ the completion of $\overline{K}$ for the p-adic topology. It is an algebraically closed field and it has a p-adic valuation v normalized by $v(p)=1$.

One defines the $\mathbb{F}_p$-algebra:

$$R := \varprojlim \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}},$$

where the inverse limit is taken with respect to Frobenius. An element $x \in R$ is then a sequence $(x_n)_{n\in\mathbb{N}}$ of elements of $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ satisfying $x_{n+1}^p = x_n$ for all n. R is a perfect $\mathbb{F}_p$-algebra of characteristic p and one has a bijection from $\varprojlim \mathcal{O}_{\overline{K}}$ to $\varprojlim \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ which is defined by

$$(x^{(n)})_{n\geq 0} \mapsto (x^{(n)}(\mathrm{mod}p)).$$

The inverse of the map is:

$$(x_n)_{n\geq 0} \mapsto (x^{(n)})_{n\geq 0},$$

where $x^{(n)} = \lim_{m\to\infty} \widehat{x_{n+m}}^{p^m}$ for arbitrary lifts $\hat{x}_i \in \mathcal{O}_{\overline{K}}$ of $x_i \in \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ for all $i \geq 0$, the limit being independent of the choice of the lifts (see [Fo2], 1.2.2]).

The laws of multiplication and addition are given by the following formulae: for any $x, y \in R$ and $n \in \mathbb{N}$,

$$\begin{aligned}(xy)^{(n)} &= x^{(n)}y^{(n)}\\ (x+y)^{(n)} &= \lim_{m\to\infty}(x^{(n+m)}+y^{(n+m)})^{p^m}\end{aligned}$$

One gives R a valuation by defining $v_R(x) = v(x^{(0)})$ for all $x \in R$. One can prove that v_R is a valuation on R and that R is v_R-adically separated and complete with residue field $\overline{k}$ (see [BC], Lemma 4.3.3]).

Now for positive integers $n \geq 1$, let $W_n := \mathbb{W}_n(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$ be the ring of Witt vectors of length n (on $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ valued points). We have a ring homomorphism:

$$\begin{aligned}\theta_n : \quad & W_n \longrightarrow \mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}}\\ & (s_0,...,s_{n-1}) \longmapsto \sum_{i=0}^{n-1} p^i \tilde{s_i}^{p^{n-1-i}}\end{aligned}$$

where $\tilde{s_i} \in \mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}}$ are lifts of s_i. Denote by $u_n : W_{n+1} \to W_n$ the homomorphism defined by Frobenius composed with the truncation map (i.e. u_n sends $(s_0, s_1, ..., s_n)$ to $(s_0^p, s_1^p, ..., s_{n-1}^p)$). Also let $v_n : \mathcal{O}_{\overline{K}}/p^{n+1}\mathcal{O}_{\overline{K}} \to \mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}}$ be the truncation map. We have that $\theta_n \circ u_n = v_n \circ \theta_{n+1}$ for every n. Furthermore one has a G_K-equivariant morphism:

$$\theta : \quad \varprojlim_{u_n} \mathbb{W}_n(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}) \to \varprojlim_{v_n} \mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}} = \mathcal{O}_{\mathbb{C}_K}$$

The inverse limit of the projective system $(\mathbb{W}_n(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}), u_n)_{n\in\mathbb{N}}$ is identified with the ring of Witt vectors $\mathbb{W}(R)$ which we denote by A_{inf}^+.

3. Explicit kernel descriptions

We remark that $\mathbb{W}_n(R) \cong A^+_{\inf}/p^n A^+_{\inf}$ since R is perfect and since for each n the projection map

$$\pi_n : A^+_{\inf} \to \mathbb{W}_n(R)$$
$$(s_0, s_1, ..., s_n, ...) \mapsto (s_0, s_1, ..., s_{n-1}).$$

has the kernel equal to:

$$\{(s_0, s_1, ...s_n, ...) \in A^+_{\inf} \mid s_0 = s_1 = ... = s_{n-1} = 0\} = p^n A^+_{\inf}.$$

We now describe the kernels of the maps θ and θ_n. The explicit kernel computations and related issues can be found in section 5.

Choose $\tilde{p} \in R$ such that $\tilde{p}^{(0)} = p$ (so $\tilde{p} = (p, p^{1/p}, p^{1/p^2}, ...)$), $\tilde{p}^{(n)} = p^{1/p^n}$). Then the element $\xi := [\tilde{p}] - p \in A^+_{\inf}$ is a generator of $ker(\theta)$ (see [BC], Proposition 4.4.3). Also denote by $\tilde{p}_n := [p^{1/p^{n-1}}] \in W_n$ the Teichmueller lift of $p^{1/p^{n-1}} \in \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ and let $\xi_n := \tilde{p}_n - p \in W_n$. Remark that the sequence $\xi = \{\xi_n\}_n$ is compatible since $u_n(\xi_{n+1}) = \xi_n$ for all $n \geq 1$ and that ξ_n is a generator of $ker(\theta_n)$ because of the following proposition.

Let us first make the identification $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}} = \mathcal{O}_{\mathbb{C}_K}/p\mathcal{O}_{\mathbb{C}_K}$.

Proposition 1. *The ideal $ker(\theta_n) \subseteq \mathbb{W}_n(\mathcal{O}_{\mathbb{C}_K}/p\mathcal{O}_{\mathbb{C}_K})$ is the principal ideal generated by ξ_n.*

Proof. We have the following commutative diagram:

$$\begin{array}{ccccc} \mathbb{W}(R) & \xrightarrow{\pi_n} & \mathbb{W}_n(R) & \xrightarrow{q_{n,n-1}} & \mathbb{W}_n(\mathcal{O}_{\mathbb{C}_K}/p\mathcal{O}_{\mathbb{C}_K}) \\ \downarrow{\scriptstyle \theta} & & & \swarrow{\scriptstyle \theta_n} & \\ \mathcal{O}_{\mathbb{C}_K} & \longrightarrow & \mathcal{O}_{\mathbb{C}_K}/p^n\mathcal{O}_{\mathbb{C}_K} & & \end{array}$$

where the bottom map is the reduction modulo p^n and the map $q_{n,n-1} : \mathbb{W}_n(R) \to \mathbb{W}_n(\mathcal{O}_{\mathbb{C}_K}/p\mathcal{O}_{\mathbb{C}_K})$ is given by

$$(s_0, s_1, ..., s_{n-1}) \overset{q_{n,n-1}}{\longmapsto} (s_0^{(n-1)}(\mathrm{mod}p), s_1^{(n-1)}(\mathrm{mod}p), \ldots, s_{n-1}^{(n-1)}(\mathrm{mod}p))$$

with $(s_0, s_1, ..., s_{n-1}) \in \mathbb{W}_n(R)$. Denote by $f_n := q_{n,n-1} \circ \pi_n$ and remark that it is a surjective ring homomorphism. We first prove that the map induced by θ at the level of kernels namely $\theta_{|\ker(f_n)} : \ker(f_n) \to \ker(\mathrm{mod}p^n)$ is surjective. For this, let $s \in \ker(\mathrm{mod}p^n) = p^n\mathcal{O}_{\mathbb{C}_K}$ so $s = p^n \cdot t$ for some $t \in \mathcal{O}_{\mathbb{C}_K}$. Since θ is surjective, we have that $t = \theta(r)$ for some $r \in \mathbb{W}(R)$ and hence $s = p^n \cdot \theta(r) = \theta(p^n) \cdot \theta(r) = \theta(p^n \cdot r)$. Moreover, $p^n \cdot r \in p^n\mathbb{W}(R) \subset \ker(f_n)$. It follows that $\theta_{|\ker(f_n)}$ is surjective.

The inclusion $p^n\mathbb{W}(R) \subset \ker(f_n)$ follows easily: let $w := (w_0, w_1, ...) \in \mathbb{W}(R)$. We then have that $p^n \cdot w = (\underbrace{0, ..., 0}_{n}, w_0^{p^n}, w_1^{p^n}, ...) \in p^n\mathbb{W}(R)$ and consequently $f_n(p^n \cdot w) = q_{n,n-1}(\pi_n(\underbrace{0, ..., 0}_{n}, w_0^{p^n}, w_1^{p^n}, ...)) = q_{n,n-1}(0, ..., 0) = (0, ..., 0)$ hence $p^n \cdot w \in \ker(f_n)$.

We apply now the Snake Lemma in the above diagram and since $\mathrm{coker}(\theta_{|\ker(f_n)}) = 0$ we obtain that the map induced by f_n at the level of kernels namely $\ker(\theta) \to \ker(\theta_n)$ is surjective. Consequently, since $\ker(\theta) \subseteq \mathbb{W}(R)$ is the principal ideal generated by ξ ([BC], Proposition 4.4.3), one obtains that the ideal $\ker(\theta_n) \subseteq \mathbb{W}_n(\mathcal{O}_{\mathbb{C}_K}/p\mathcal{O}_{\mathbb{C}_K})$ is principal and generated by $f_n(\xi) = \xi_n$. □

The following two propositions are results quoted in [AI] and left as exercises. We give here the complete proof.

Proposition 2. *The kernel of the projection map*

$$\bar{q}_n : R = \varprojlim \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}} \to \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$$

on the $n+1$-th factor of the limit is generated by $\tilde{p}^{p^n}$.

Proof. For this, let $x=(x_m)_{m\geq 0}\in R$. Then $\bar{q}_n$ sends $(x_m)_{m\geq 0}$ to x_n.

Remark that since

$$v_R(x)=v(x^{(0)})=v((x^{(n)})^{p^n})=p^nv(x^{(n)})\quad n\geq 0,$$

then

$$v_R(x)\geq p^n\Leftrightarrow v(x^{(n)})\geq 1\Leftrightarrow x^{(n)}(\mathrm{mod}p)=0.$$

One obtains in this way a better description of $ker(\bar{q}_n)$

$$ker(\bar{q}_n)=\{x\in R/v_R(x)\geq p^n\}=\{x\in R/x^{(n)}(\mathrm{mod}p)=0\}.$$

Now since $v_R(\tilde{p}^{p^n})=v(p^{p^n})=p^n$, it is true that $(\tilde{p}^{p^n})\subseteq ker(\bar{q}_n)$. For the other inclusion, let $x\in ker(\bar{q}_n)$. Subsequently, $v(x^{(0)})\geq p^n$ hence $x^{(0)}=p^{p^n}y^{(0)}$, for some $y^{(0)}\in\mathcal{O}_{\overline{K}}$. Since $(x^{(n)})_n$ is compatible we have that $(x^{(1)})^p=x^{(0)}=p^{p^n}y^{(0)}$ and one obtains $x^{(1)}=p^{p^{n-1}}y^{(1)}$, $y^{(1)}\in\mathcal{O}_{\overline{K}}$ and moreover $(y^{(1)})^p=y^{(0)}$ (recall that the multiplication in R (through the above mentioned bijection) is $(st)^{(n)}=(s)^{(n)}(t)^{(n)}$ and that $\mathcal{O}_{\overline{K}}$ is normal). We construct in this way a compatible sequence $y=(y^{(n)})_n\in R$ such that $x=\tilde{p}^{p^n}y$. □

The projection $\bar{q}_n$ induces a ring homomorphism:

$$q_n:\mathbb{W}_n(R)\to\mathbb{W}_n(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$$
$$(s_0,s_1,...,s_{n-1})\mapsto(s_0^{(n)}(\mathrm{mod}p),s_1^{(n)}(\mathrm{mod}p),\cdots,s_{n-1}^{(n)}(\mathrm{mod}p)).$$

Since q_n is surjective, we have the isomorphism:

$$\mathbb{W}_n(R)/ker(q_n)\cong\mathbb{W}_n(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})=W_n.$$

Denote by $V:\mathbb{W}_n(R)\to\mathbb{W}_{n+1}(R)$ the Verschiebung i.e.

$$V((s_0,s_1,...,s_{n-1}))=(0,s_0,s_1,...,s_{n-1}),\ (s_0,s_1,...,s_{n-1})\in\mathbb{W}_n(R).$$

The following proposition describes the kernel of the map q_n.

Proposition 3. *The kernel of the ring homomorphism q_n is the ideal generated by*

$$\{[\tilde{p}]^{p^n},V([\tilde{p}]^{p^n}),V^2([\tilde{p}]^{p^n}),\cdots,V^{n-1}([\tilde{p}]^{p^n})\}.$$

Proof. For $n=1$ the statement is obvious by using Proposition 2. For $n\geq 2$ we have the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{W}_{n-1}(R) & \xrightarrow{V\circ(*)^p} & \mathbb{W}_n(R) & \xrightarrow{pr_1\circ(*)^{1/p^n}} & \mathbb{W}_1(R) & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle q_{n-1}} & & \downarrow{\scriptstyle q_n} & & \downarrow{\scriptstyle q_1} & & \\
0 & \longrightarrow & \mathbb{W}_{n-1}(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}) & \xrightarrow{V} & \mathbb{W}_n(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}) & \xrightarrow{pr_1} & \mathbb{W}_1(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}) & \longrightarrow & 0
\end{array}$$

where by pr_1 we denote the projection map on the first component.

One can easily check the exactness of the second row so we omit it. For the first one, remark that $(V\circ(*)^p)((s_0,s_1,...,s_{n-2}))=(0,s_0^p,s_1^p,...,s_{n-2}^p)$, $s_i\in R$, $0\leq i\leq n-2$, and that $(pr_1\circ(*)^{1/p^n})((0,s_0^p,s_1^p,...,s_{n-2}^p))=pr_1((0,s_0^{1/p^{n-1}},s_1^{1/p^{n-1}},...,s_{n-2}^{1/p^{n-1}}))=0$.

On the other hand, $V\circ(*)^p$ is injective since Verschiebung is injective and $(*)^p$ is bijective due to the fact that R is perfect. Similarly, $pr_1\circ(*)^{1/p^n}$ remains surjective (for $s_0\in\mathbb{W}_1(R)$, we have that $(pr_1\circ(*)^{1/p^n})((s_0^{p^n},s_1,...,s_{n-1}))=s_0$, where $(s_0^{p^n},s_1,...,s_{n-1})\in\mathbb{W}_n(R)$).

Take now $(s_0,s_1,...,s_{n-1})\in ker(pr_1\circ(*)^{1/p^n})$ so $s_0^{1/p^n}=0$. Since R is perfect it follows that $s_0=0$ and consequently $(s_0,s_1,...,s_{n-1})=(V\circ(*)^p)((s_1^{1/p},s_2^{1/p},...,s_{n-1}^{1/p}))$ hence $ker(pr_1\circ(*)^{1/p^n})\subseteq Im(V\circ(*)^p)$.

One obtains that the first row is exact. Note that the first square diagram is exact since, for a choice of $s_i\in R$, $0\leq i\leq n-2$, we have:

$$\begin{array}{ccc}(s_0,s_1,...,s_{n-2}) & \xrightarrow{V\circ(*)^p} & (0,s_0^p,s_1^p,...,s_{n-2}^p)\\ \downarrow{\scriptstyle q_{n-1}} & & \downarrow{\scriptstyle q_n}\\ (s_0^{(n-1)}(p),s_1^{(n-1)}(p),...,s_{n-2}^{(n-1)}(p)) & \xrightarrow{V} & (0,s_0^{(n-1)}(p),s_1^{(n-1)}(p),...,s_{n-2}^{(n-1)}(p))\end{array}$$

Also the second square diagram commutes since, for a choice of $s_i \in R$, $0 \leq i \leq n-1$, we have:

$$\begin{array}{ccc}(s_0,s_1,...,s_{n-1}) & \xrightarrow{pr_1\circ(*)^{1/p^n}} & (s_0^{1/p^n})\\ \downarrow{\scriptstyle q_n} & & \downarrow{\scriptstyle q_1}\\ (s_0^{(n)}(p),s_1^{(n)}(p),...,s_{n-1}^{(n)}(p)) & \xrightarrow{pr_1} & (s_0^{(n)}(p))\end{array}$$

One applies further the induction hypothesis at the level of kernels in the main diagram. □

4. Constructing the rings $A_{\max,\mathrm{n}}$

Definition 1. Let A be a p-adically complete $\mathcal{O}_K$-algebra and T a variable. Define

$$A\{T\} := \varprojlim A[T]/p^nA[T].$$

Also define

$$\begin{aligned}A_{\max,\mathrm{n}} &:= W_n[\delta]/(p\delta-\xi_n)\\ A_{\max} &:= \varprojlim_n A_{\max,\mathrm{n}}.\end{aligned}$$

Using these definitions, we then have

$$\begin{aligned}A_{\max} &= A_{\inf}^+\left\{\left[\frac{\xi}{p}\right]\right\} = A_{\inf}^+\{\delta\}/(p\delta-\xi)\\ &= \left\{\sum_{i\geq 0} a_i\delta^i \text{ such that } a_i \in A_{\inf}^+ \text{ and } a_i \overset{i\to\infty}{\longrightarrow} 0\right\}.\end{aligned}$$

i.e. we recover the ring introduced by Colmez in [Col].

Let $A'_{\max,\mathrm{n}} := W_n[\delta]/(p\delta-\xi_{n+1})$. (By ξ_{n+1} we mean here the projection on the first n components of this vector namely $pr_n(\xi_{n+1}) = \underbrace{(p^{1/p^n},-1,0,...,0)}_{n})$. Note that we also have that:

$$\begin{aligned}V^i([\tilde{p}]^{p^n}) &= p^i([\tilde{p}]^{p^n})^{p^{-i}} = p^i[\tilde{p}]^{p^{n-i}} = p^i(\xi+p)^{p^{n-i}} = p^i(p(\delta+1))^{p^{n-i}}\\ &\equiv p^{i+p^{n-i}}\delta^{p^{n-i}} \equiv 0(\mathrm{mod}p^nA_{\max}),\end{aligned}$$

where for the first equality one uses the Witt coordinatization $((r_0,r_1,...) = \sum p^n[r_n^{p^{-n}}]$ (or one computes it directly)).

By using Proposition 3 one obtains that $ker(q_n) \subseteq p^nA_{\max}$. We will use this fact in the proof of the following:

Proposition 4.

$$A_{\max}/p^nA_{\max} \cong A'_{\max,\mathrm{n}}.$$

Proof. Since $ker(q_n) \subseteq p^nA_{\max}$, we obtain that:

$$\frac{A_{\max}}{p^n A_{\max}} = A_{\max}/(p^n, ker(q_n))A_{\max} = \frac{A^+_{\inf}\{\delta\}/(p\delta-\xi)}{(p^n, ker(q_n))(A^+_{\inf}\{\delta\}/(p\delta-\xi))}$$
$$= \frac{A^+_{\inf}\{\delta\}/(p\delta-\xi)}{(p^n, ker(q_n), p\delta-\xi)A^+_{\inf}\{\delta\}/(p\delta-\xi)} \cong A^+_{\inf}[\delta]/(p^n, ker(q_n), p\delta-\xi)A^+_{\inf}[\delta]$$
$$\cong \frac{A^+_{\inf}[\delta]/p^n A^+_{\inf}[\delta]}{(p^n, ker(q_n), p\delta-\xi)A^+_{\inf}[\delta]/p^n A^+_{\inf}[\delta]} \cong \frac{(A^+_{\inf}/p^n A^+_{\inf})[\delta]}{(ker(q_n), p\delta-\xi(\mathrm{mod}p^n))(A^+_{\inf}[\delta]/p^n A^+_{\inf}[\delta])}.$$

By using now the isomorphisms of rings

$$A^+_{\inf}/p^n A^+_{\inf} \cong \mathbb{W}_n(R) \text{ and } A^+_{\inf}[\delta]/p^n A^+_{\inf}[\delta] \cong (A^+_{\inf}/p^n A^+_{\inf})[\delta]$$

one obtains that

$$A_{\max}/p^n A_{\max} \cong \mathbb{W}_n(R)[\delta]/(ker(q_n), p\delta-\xi(\mathrm{mod}p^n)).$$

Since $\mathbb{W}_n(R)/ker(q_n) \cong W_n$ and $q_n(\xi(\mathrm{mod}p^n)) = pr_n(\xi_{n+1})$, q_n induces the isomorphism

$$\mathbb{W}_n(R)[\delta]/(ker(q_n), p\delta-\xi(\mathrm{mod}p^n)) \cong W_n[\delta]/(p\delta - pr_n(\xi_{n+1})) =: A'_{\max,\mathrm{n}}.$$

We obtain that $A_{\max}/p^n A_{\max} \cong A'_{\max,\mathrm{n}}$. □

Remark 1. One can also prove the previous proposition by showing that there is a surjective map $A_{\max} \twoheadrightarrow A'_{\max,\mathrm{n}}$ whose kernel is $p^n A_{\max}$. One can prove (see [Ga], Lemma 3.2.5) that for any positive integers $m > n$ there is an isomorphism of rings $A_{\max}/p^n A_{\max} \cong A_{\max,\mathrm{m}}/p^n A_{\max,\mathrm{m}}$.

Note that, via the isomorphism $A_{\max}/p^n A_{\max} \cong A'_{\max,\mathrm{n}}$, we have a surjective map of rings:

$$q'_n : A_{\max}/p^n A_{\max} \to A_{\max,\mathrm{n}}$$

sending $pr_n(\xi_{n+1}) \to \xi_n$, induced by Frobenius on W_n and that we also have a map:

$$u_n : A_{\max,\mathrm{n+1}} \to A_{\max}/p^n A_{\max}$$

sending $\xi_{n+1} \to pr_n(\xi_{n+1})$, induced by the natural projection $W_{n+1} \to W_n$.

One further uses the rings $A_{\max,\mathrm{n}}$ to construct the family of sheaves $(\mathbb{A}^{\nabla}_{\max,\mathrm{n}})_{n\geq 1}$ and study their properties (see [Ga] for details).

5. Computing the kernels of θ_n and θ

As we have seen in section 3, computing of the kernels of the map θ (w.r.p θ_n) amounts to the task of computing Witt vectors of finite length in the Witt ring $A^+_{\inf}$ (w.r.p W_n). In this section, we present two approaches that will facilitate the computation task at hand.

First let us recall some basic facts about Witt vectors. The readers may consult [Se, chapter 2] for more details on the topic. Let p be a prime and n a positive integer. The n'th Witt polynomial is by definition

$$W_n(X_0, \ldots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^n X_n. \tag{1}$$

There exist polynomials S_n, P_n in $\mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots Y_n]$ satisfying

$$W_n(S_0, \ldots, S_n) = W_n(X_0, \ldots, X_n) + W_n(Y_0, \ldots, Y_n) \tag{2}$$

and

$$W_n(P_0, \ldots, P_n) = W_n(X_0, \ldots, X_n) \cdot W_n(Y_0, \ldots, Y_n). \tag{3}$$

Let A be a commutative ring. Suppose $\mathbf{a} = (a_0, a_1 \ldots)$ and $\mathbf{b} = (b_0, b_1, \ldots)$ are elements of $A^{\mathbb{N}}$, set

$$\mathbf{a} + \mathbf{b} = (S_0(\mathbf{a}, \mathbf{b}), S_1(\mathbf{a}, \mathbf{b}), \ldots)$$
$$\mathbf{a} \cdot \mathbf{b} = (P_0(\mathbf{a}, \mathbf{b}), P_1(\mathbf{a}, \mathbf{b}), \ldots).$$

p	no. terms	CPU time
11	2672	0.421s
19	22856	6.739s
23	48644	54.554s
29	121886	1102.459s
31	158812	2808.408s

TABLE 1. Polynomial S_2 calculation for various p

The laws of composition defined above make $A^{\mathbb{N}}$ into a commutative unitary ring (called the ring of Witt vectors).

Thus in order to compute $\mathbf{a}+\mathbf{b}$ (w.r.p. $\mathbf{a}\cdot\mathbf{b}$), one has to compute $S_n(\mathbf{a},\mathbf{b})$ (w.r.p. $P_n(\mathbf{a},\mathbf{b})$) for all n. In what follows, we present two approaches for computing S_n (w.r.p. P_n). For the sake of clarity, we have chosen to focus on the computation of S_n. The computation of P_n follows in a similar line. The first approach computes the polynomials S_n explicitly, the evaluation $S_n(\mathbf{a},\mathbf{b})$ is achieved by evaluating S_n at $\mathbf{a},\mathbf{b}$. The second approach is to use the recursion formula (6) (derived below) to compute $S_n(\mathbf{a},\mathbf{b})$ directly from the already computed values $S_0(\mathbf{a},\mathbf{b}), S_1(\mathbf{a},\mathbf{b}),\ldots,S_{n-1}(\mathbf{a},\mathbf{b})$.

5.1. **Polynomial Evaluation.** In the first place, we may use (2) to explicitly compute the polynomial functions $S_0, S_1, S_2, \ldots, S_n$ successively in $\mathbb{Z}[X_0,\ldots,X_n,Y_0,\ldots Y_n]$. $S_n(\mathbf{a},\mathbf{b})$ is then computed by evaluating S_n at $\mathbf{a},\mathbf{b}$.

For $n\leq 2$, we have

$$S_0 = X_0+Y_0, \qquad S_1 = X_1+Y_1+\frac{1}{p}\left(X_0^p+Y_0^p-(X_0+Y_0)^p\right); \tag{4}$$

and

$$\begin{aligned} S_2 &= X_2+Y_2+\frac{1}{p}\left(X_1^p+Y_1^p-\left(X_1+Y_1+\frac{X_0^p+Y_0^p-(X_0+Y_0)^p}{p}\right)^p\right)\\ &\quad+\frac{X_0^{p^2}+Y_0^{p^2}-(X_0+Y_0)^{p^2}}{p^2}\\ &\vdots \end{aligned} \tag{5}$$

In expanded form, the polynomial S_1 has $p+1$ terms. As we can see, the number of terms for S_n when $n>1$ gets large very quickly. It turns out that even in the case of S_2, the computing becomes inefficient for a small p. Experimentally, we carried out the task of computing the polynomial S_2 explicitly for various small p. The calculations are done using MAPLE 12 on a Dell laptop with a Intel Duo CPU at 2.10GHz and 4 GB RAM. The table 5.1 summaries the experiment results.

We have for each p recorded the number of monomials of S_2 in expanded form and the CPU time it took to complete the calculation.

5.2. **Recursion Formula.** Alternatively, we may derive using definition (1) a recursion formula. More explicitly, we have for $n\geq 1$

$$S_n = (X_n+Y_n)+\frac{1}{p}(X_{n-1}^p+Y_{n-1}^p-S_{n-1}^p)+\cdots+\frac{1}{p^n}(X_0^{p^n}+Y_0^{p^n}-S_0^{p^n}), \tag{6}$$

p	CPU time
541	0.078s
1223	1.217s
2011	2.044s
3181	6.224s
4409	10.390s
5279	15.927s
6133	21.185s
7001	27.238s
7499	out of memory

TABLE 2. Recursive evaluation of S_2

and

$$\begin{aligned} P_n &= \frac{1}{p^n}\left((X_0^{p^n} + \cdots p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - (P_0^{p^n} + \cdots + p^{n-1}P_{n-1}^p\right) \\ &= (X_0^{p^n}Y_n + X_1^{p^{n-1}}Y_{n-1}^p + \cdots + X_n Y_0^{p^n}) \\ &+ \frac{1}{p}(X_0^{p^n}Y_{n-1}^p + \cdots X_{n-1}^p Y_0^{p^n}) \\ &\vdots \\ &+ \frac{1}{p^n}(X_0^{p^n}Y_0^{p^n}) - \frac{1}{p^n}P_0^{p^n} - \cdots - \frac{1}{p}P_{n-1}^p \\ &+ p(X_1^{p^{n-1}}Y_n + X_2^{p^{n-2}}(Y_{n-1}^p + pY_n) + \cdots). \end{aligned} \tag{7}$$

Example 5.1. As we have seen in Proposition 1, the kernel of θ_n is a principal ideal generated by ξ_n. Let

$$\begin{aligned} a &= (p^{1/p^n}, 0, 0, \ldots, 0) = (a_0, a_1, \ldots, a_n) \\ b &= (0, -1, 0, \ldots, 0) = (b_0, b_1, \ldots, b_n). \end{aligned}$$

Then using (6), for every n

$$\xi_{n+1} := \tilde{p}_{n+1} - p = [p^{1/p^n}] - p = a + b = (p^{1/p^n}, -1, 0, \ldots, 0).$$

The recursion formula (6) can be coded. For instance, the reader will find in the appendix a MAPLE code for the evaluation of $S_n(\mathbf{a}, \mathbf{b})$ with input Witt vectors $\mathbf{a}, \mathbf{b}$ in a field characteristic p. Observe that in order to compute $S_j = S_j(\mathbf{a}, \mathbf{b})$, one has to compute $S_0, S_1, \ldots, S_{j-1}$ a priori. Therefore the complexity of the algorithm is $\mathcal{O}(n^2)$ for computing S_n. The table 5.2 summaries the experiment we carried out on the same laptop with a Intel Duo CPU at 2.10GHz and 4GB RAM. We first randomly generate Witt vectors $\mathbf{a}, \mathbf{b}$. We then evaluated $S_2(\mathbf{a}, \mathbf{b})$ for various primes p using the MAPLE code provided in the appendix.

6. APPENDIX

The following Maple code calculates S_n using formula (6).

Algorithm 1 INPUT: prime p, positive integer n and Witt vectors $\mathbf{a}, \mathbf{b}$. Output: $S_n(\mathbf{a}, \mathbf{b})$.

$S := proc(a, b, p, n)$
if $n = 1$ **then**
  $(a_1 + b_1) \bmod p$
else
  $add(p^{n-k-1} * (a_{n-k}^{p^k} + b_{n-k}^{p^k} - S(a, b, p, n-k)^{p^k}, k = 1..n-1))/p^{n-1} + (a_n + b_n) \bmod p$
end if;

References

[AI] F. Andreatta, A. Iovita, *Crystalline comparison isomorphisms for formal schemes*, preprint available at URL: www.mathstat.concordia.ca/faculty/iovita/research.html.

[BC] O. Brinon, B. Conrad, *CMI summer school notes on p-adic Hodge Theory*, September 2009, available at URL: http://math.stanford.edu/∼ conrad/papers/notes.pdf.

[Col] P. Colmez, *Théorie d'Iwasawa des représentations de de Rham d'un corp local*, Annals of Math. 148(1998), 485-571.

[Fa] G. Faltings, *Crystalline cohomology and p-adic Galois representations*, "Algebraic Analysis, Geometry and Number theory" (J.I. Igusa ed.), John Hopkins University Press, Baltimore, 25-80(1988).

[Fo1] J-M. Fontaine, *Sur certaines types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Annals of Maths, 115(1982), 529-577.

[Fo2] J-M. Fontaine, *Le corps des périodes p-adiques, Astérisque 223(1994)*, 59-111.

[Ga] R. Gaba, *On Fontaine Sheaves*, Ph.D. Thesis. Available at http://www.radugaba.com/r.gaba_thesis.pdf

[Ro] Alain M. Robert, *A course in p-adic Analysis*, GTM 198, Springer-Verlag, New York, 2000.

[Se] J-P. Serre, *Local fields*, GTM 67, Springer-Verlag, New York, 1979.

Department of Mathematics, Concordia University, Montréal, QC H3G 1M8, CANADA & Institute of Mathematics "Simion Stoilow" of the Romanian Academy, P.O. BOX 1-764 RO-014700 Bucharest, ROMANIA

E-mail address, Radu Gaba: rgaba@live.concordia.ca

Bonn-Aachen International Center for Information Technology, Universität Bonn, 53113 Bonn, Germany

E-mail address, Benjamin Justus: justus@bit.uni-bonn.de

ALBANIAN JOURNAL
OF MATHEMATICS
Volume 4, Number 4, Pages 223–230
ISSN 1930-1235: (2010)

IMPROVING THE TEACHING OF MATHEMATICS TO STUDENTS OF SCIENCE AND ENGINEERING

M. B. MONAGAN AND J. F. OGILVIE

Abstract. To improve the teaching of mathematics to students of science and engineering, an holistic approach strongly based on the use of software for symbolic computation with numerical and graphical capabilities is advocated. Within three semesters the quality and quantity of mathematics understood and implementable by those students can be significantly enhanced with this approach, which was tested during an accelerated course that covered all pertinent content within eight weeks.

1. Introduction

In 2010 most instructors of mathematics at the tertiary educational level employ, to some but variable extent for purposes of illustration, software for symbolic computation in their teaching of standard courses such as calculus and linear algebra [1]. Software of this type certainly provides valuable facilities for such purposes through its graphical capabilities, its algebraic operations and its capability of numerical tests over wide ranges. There is, however, much more that is achievable for pedagogical purposes through enlightened use of this software.

When those instructors merely teach the traditional courses in a manner slightly modified to include illustrative demonstrations to students of science and engineering [2], they fail the primary objective of those courses, which is to prepare adequately their students for a technical career that lasts typically five to thirty years after graduation; during all that period the graduate is challenged to apply his mathematical knowledge and expertise to solve problems in his profession. Mathematics is the language of science and technology, but for all subjects other than mathematics the required courses on particular topics in mathematics fall far short of encompassing the full gamut of mathematical knowledge that is desirable for the eventual practice of a technical profession. This enduring and persistent application during a career far transcends the transitory tasks of drill and practice, exercises and examinations on particular topics that occupy the immediate attention of both students and instructors within a particular teaching unit or semester. Moreover, although those illustrations incontestably improve the teaching and learning of mathematical concepts, that software can serve far more effectively in the application to the mathematical component of technical problems during that career, provided that a student becomes satisfactorily acquainted with its capabilities during the learning process. For these reasons we advocate a fundamental reorientation of the teaching of mathematics for it to become based on software for symbolic computation, such that both the learning of concepts and principles and

an implementation of those principles reinforces the mathematical capabilities of the student to solve technical problems.

A major obstacle to the application of mathematics as a tool in a technical career is that few academic programmes in subjects other than mathematics include the broad range of mathematical topics that will arise within that technical career. Statistics and data analysis are commonly neglected, and even differential and integral equations are afforded scant coverage in conventional curricula that require as little as three semester courses in mathematics to support biology, chemistry or geology as principal scientific disciplines, with somewhat more for students of physics, engineering or computing. Complex analysis, graph theory, group theory, numerical analysis and vector calculus are mere names that a student of science or engineering might encounter as he or she proceeds through the typically required few courses including differential, integral and multivariate calculus, and perhaps also linear algebra, within the minimum degree requirements for other science subjects. For students that seek to become specialist in mathematics, most degree programs have some vague requirement of other science courses, presumably for cultural reasons, to conform to regulations in a faculty of science, and perhaps some courses in computing; in contrast, for students of science and engineering, courses in mathematics to support their major subject are crucial. Whether a graduate in mathematics becomes employed as a teacher or in industry or commerce, those computer methods can serve as the means to apply the mathematics for whatever purpose. For other science subjects, courses in computing or modeling lack the tradition of mathematics as being an intrinsic component of common degree regulations, but computers will likely play a large and increasing role in the application of mathematics during a technical career.

All these deficiencies can be effectively remedied through the teaching of mathematics based on software for symbolic computation, including extensive graphical and numerical capabilities and an interactive language, in a programme designed holistically to include mathematical topics over a broad range. The duration of such courses within a degree program in science might be as little as two semesters, although realistically three semesters are preferable. The replacing of traditional drill and practice, in particular for aspects of differential and integral calculus and of linear algebra involving manual operations, by the use of computer software enables a great saving of time, which can thus be devoted to increase the range and depth of mathematical topics. Furthermore, the understanding of not only the mathematical concepts and principles but also their implementation with computer software, including the associated limitations, can exceed that in conventional courses, with or without software illustrations, because the details of methods of integration, for instance, can obscure those principles for students who are confronted with the necessity to solve formal mathematical exercises and problems on examinations for the purpose of proceeding through their academic programs in other subjects. Although the use of software for symbolic computation has been much discussed in regard to particular traditional courses, such as calculus, few authors considered implementing the total regiment of mathematics that students in service courses require [3]. In that sense we advocate a possibly radical approach, but one that has already been proved practicable (vide infra).

2. Structure of curriculum

The use of software for symbolic computation inevitably involves learning the language of particular software and thereby becoming acquainted with the programming of computers. Although in the first instance one particular software would likely be encountered, other software for computer algebra has similar design and operation; for that reason, migrating from one software title to another is much less onerous than an initial coming to grips with any particular software, and a careful choice of a particular software to have a gentle learning curve can mitigate the initial barrier. For these reasons we advocate the following approach to teach mathematics with computer software, assuming that a student proceeds through three, likely consecutive, semesters taught with the same software. In the first semester, as a vehicle to become familiar with the basic commands and instructions, the topics include

- arithmetic of integers, real and complex numbers,
- solution of equations and inequalities,
- factoring polynomials,
- elementary functions,
- plots of functions and data in two and three dimensions,
- descriptive geometry,
- trigonometry and
- transformation in complex space,

and differential calculus of a single independent variable includes

- limit,
- derivative,
- explicit and implicit differentiation, and
- differential.

Although much of this material might seem to repeat the content of preceding years of mathematics in school in some environments, an instructor can take advantage of this condition to review those topics, and to explore them from a mature outlook, so to deepen their understanding, while the student learns how to invoke the corresponding operations with the software. Arithmetic can, for example, here include some discussion of number theory and primality, and trigonometry includes consideration of both circular and hyperbolic functions. The first semester of traditional university courses in mathematics is typically concerned mostly with differential calculus; for that reason, at the end of that first semester the student pursuing the new approach is at the same level as with the old approach, although he or she has acquired valuable experience in use of the software as well as reinforcing the understanding of preceding branches of mathematics.

In the second semester, the student proceeds through integral calculus,

- definite integral,
- indefinite integral,
- improper integral,
- numerical quadrature,

with appropriate geometric illustrations and applications of each topic, and multivariate calculus including analytic geometry,

- partial derivative,
- tangent plane and minimization,

- multivariate Taylor and Fourier series,
- exact differential,
- multiple integration,

into linear algebra,

- matrix and determinant,
- matrix inverse and solving linear systems, and
- vector and orthogonality.

The third semester continues with linear algebra in

- eigenvalue and eigenvector,
- vector calculus,
- tensor,
- spreadsheet for mathematical applications,

and progresses through

- ordinary differential equation,
- systems of differential equations of first order,
- partial differential equation,
- integral equation,

into statistical topics,

- probability,
- distribution,
- analysis of variance,
- linear regression,
- non-linear regression, and
- linear and non-linear optimization,

for the treatment of real data. In the process of his or her intensive use of the software, the student becomes, even unconsciously, acquainted with the mechanism of the software, which implies an acquaintance with programming even though little formal programming might at this stage seem to be involved in the use of the current highly sophisticated software for computer algebra. Some basic programming skills are valuable for applications in a technical career; learning a separate language, such as Java or C++, is recommended.

In each of the three semesters, the formal teaching would preferably involve about two hours per week of lecture demonstration of concepts and principles, with another two hours of scheduled and supervised practice in a computer laboratory; further practice and study by the student beyond those hours are naturally expected, for which purpose the software should be generally available in an accessible computer laboratory or on the student's own computer. As the progress through a semester requires an intimate association of students with computers, so must the assessment require the use of a computer, rather than attempting to test any manual skills of the student. An instructor must be aware that, in almost all cases outside the mathematical profession, the practice of mathematics by a scientist or engineer within a few years of graduation has traditionally involved working not manually but instead with extensive consultation of tables of numerical or algebraic content, such as for integrals or differential equations; computer software that is far more powerful than any single reference book or compilation makes such printed tables obsolete.

The advantage of our developed approach is that a student of science and engineering can become proficient in the use of mathematical software to solve technical problems, based on a profound understanding of mathematical and statistical concepts and principles and a practised knowledge of their implementation to solve practical problems. A disadvantage of our approach is that initially a student might have a manual ability less well developed than with traditional courses, but in any case that ability fades rapidly after the completion of particular courses in which it is developed. Another disadvantage might be the additional cost of operating practical sessions, depending on the arrangements of physical and human resources in a particular institution; such analogous laboratory sessions are an accepted and essential component of teaching other science and engineering subjects.

Most mathematicians have been aware of the general ideas discussed above for two or three decades; in that sense the present approach is not novel, but for the teaching of such an integrated course a textbook of appropriate design would be a great asset. Most instructors at university level teach the textbook to a greater or lesser extent, and an assigned textbook has certainly inestimable value to a typical undergraduate student. Many textbooks on particular branches of mathematics, such as calculus or linear algebra, already exist (in printed form!) in which the authors attempt some amalgam of traditional instruction and usage of software. For a course based on computer software, the textbook should, however, have an intrinsically electronic form, but pages or sections could be printed as desired. To prove the practicality of the approach, such a textbook has been developed and published [4]. Even though this book in the form of nine separate computer files is designed particularly for chemistry, the didactic content of those files is nearly all pure mathematics; at those points at which applications or examples in chemistry seem appropriate, advantage is taken of the opportunity to include exercises or illustrations with a chemical or physical theme, such as basic thermodynamic relations in multivariate differential calculus and standard differential equations to treat the kinetics of chemical reactions. In conjunction with the accompanying software, such a textbook is amenable even to self study, thus requiring neither instructor nor classes, and any enterprising student who must suffer under the obsolescent format of traditional courses would do well to supplement his class experience with such a source. As this textbook has been composed from the point of view of a professor of chemistry who seeks to have his students possess not only a broad and profound knowledge of mathematical concepts and principles but also their implementation to solve problems that arise in general, analytical, inorganic, organic, physical and theoretical chemistry, including the treatment of numerical data from teaching and research laboratories, the emphasis has been placed on functionality rather than formality by way of theorems and proofs; recourse to contemporary mathematical textbooks demonstrates that even mathematicians have mostly discarded a purely axiomatic approach to teaching, especially in service courses. The participation in the development of this book by professional mathematicians in various manners has, however, assured that the electronic book has an internal cohesion and a mathematical outlook consistent with almost a standard mathematical point of view. The content of the book has been assembled in the light of the content of traditional textbooks; practically no significant topic of calculus, linear algebra or differential equations that appears in multiple standard textbooks is absent from this electronic book. Numerical aspects, typically neglected in core courses taught

by pure mathematicians but essential for practical applications in science and engineering, have been included in a systematic manner.

We endorse the view that, to teach mathematics to students of science and engineering, the instructors should generally be professionally qualified mathematicians, because any student should be exposed to varied points of view from experts in their particular subjects. For the book Mathematics for Chemistry, a mathematician would have adequate scope to teach the mathematics without distraction from chemical or physical digressions, but a student of chemistry could profitably study the chemical examples and undertake the exercises with a chemical context. We present here no example of this approach to the teaching of mathematical topics; the best way to become acquainted with our approach is through scrutiny of the book and the direct operation of its executable commands in a sequence for any selected topic. The printed page here is an inadequate medium to convey the power of this approach, but a few examples are mentioned elsewhere [5].

3. Practical implementation

Although three semesters are considered likely an optimal duration for the teaching and learning of the pertinent material for students of science and engineering, we are unaware of an actual implementation of such a programme, but intensive teaching of the same material has been proved practicable within a smaller period. For instance, a course, of title Mathematical Preparation for Analytical and Physical Chemistry, has been delivered in Universidad de Costa Rica that covered all material outlined above within eight weeks; this course comprised three sessions per week, each of duration four hours, of which the first 75 minutes (on average) was occupied with lecture demonstration of the mathematical concepts and principles and their implementation; the remaining time was devoted to supervised practice. The prerequisite for this course entailed the equivalent of integral calculus but not multivariate calculus. According to this regimen, during the first four weeks the mathematics was formally a review of what the students had already encountered; within this period the objective was to have the students become familiar with the provided software (Maple 13) [6]. During the next four weeks new mathematics was introduced, namely multivariate calculus, linear algebra, differential and integral equations and statistical topics, as outlined above. The criterion for successful completion of this course was stated to be satisfactory fulfillment of 80 per cent of the assigned exercises, which numbered 230 in total, so averaging ten per period. Some exercises consisted of applications to chemistry, but most were purely mathematical in nature, designed to reinforce the concepts discussed during the lecture and described at sufficient length in the assigned worksheets extracted from the textbook [4]; some exercises comprised a single part devoted to the solution of a particular problem by algebraic, numerical or graphical means, and other exercises with multiple parts were designed to explore various aspects of a particular topic through selected examples. For no student was the period of four hours sufficient for the solution of these exercises; because most students had no other course or formal activity during this summer season, they were able to allocate whatever additional time was necessary for the work, either in the computer laboratory of the course or on computers elsewhere to which they had access. The response to this course by the students was unanimously positive: they felt not only that they had learned much useful mathematics that they could apply in whatever chemical

studies or technical activities might follow, but also, and more importantly, that they had sufficiently mastered both the concepts and the software to an extent that enabled them to implement therewith the mathematical operations to solve whatever technical problems might arise. The students would naturally rely on various electronically stored materials, including the textbook, for additional guidance, just as students of traditional courses rely on reference books and tables. A subsequent survey, after one semester, of students who completed this course verified that they applied the software in their study of chemistry and enhanced their understanding of the chemical topics through an improved facility with the mathematical underpinning. The circumstances under which this course operated were atypical: even though we recommend three semesters as an optimal duration of the total program of content, the fact of the actual delivery within eight weeks and the emphatic success of this course demonstrate the creative possibilities that teaching and learning with computer software open.

Some universities in Europe operate on a block system whereby students devote their attention to a single course for a few weeks. To cover all the content of the above lists, this system is obviously applicable to teach the mathematics with the available software and textbook in one, two or three such blocks.

4. Conclusion

To prepare for a productive technical career in this era of the computer whether in developed or developing countries, students of science and engineering need more and better education in mathematics and statistics than what they have been receiving within the traditional required courses. Symbolic computation within a program designed to encompass a broad range of topics can provide not only that improved and expanded learning within a similar number of semester courses but also a means to enhance greatly the capability to solve technical problems. Departments of mathematics that fail to respond to these conditions are abdicating their responsibility to provide timely and effective mathematical education for students of science and engineering.

References

[1] Z. Lavicza, *Examining the use of computer algebra systems in university-level mathematics teaching*, Journal of Computers in Mathematics and Science Teaching, 28 (2), 99-111 (2009)

[2] F. Simons, *Computer algebra in service courses*, CTI Math & Stats Newsletter, 8 (3), 1-4 (1997)
`http://www.cecm.sfu.ca/CAG/papers/FSimonsCA.pdf`

[3] C. Buteau, N. Marshall, D. Jarvis, *Integrating computer-algebra systems in post-secondary mathematics education*, International Journal for Technology in Mathematics Education, 17 (2), 57-68 (2010)

[4] J. F. Ogilvie, G. Doggett, G. J. Fee, M. B. Monagan, *Mathematics for Chemistry with Symbolic Computation*, first edition (2005); Maplesoft Inc., Waterloo Ontario Canada, second edition (2008)
`http://www.cecm.sfu.ca`

[5] J. F. Ogilvie, M. B. Monagan, *Teaching mathematics to chemistry students with symbolic computation* , Journal of Chemical Education, 84 (5), 889-896 (2007)
`http://www.cecm.sfu.ca/research/MthChemEd.pdf`

[6] M. B. Monagan, K. O. Geddes, K. M. Heal, G. Lagahn, S. M. Vorkoetter, J. McCarron, P. DeMarco, *Maple Introductory Programming Guide*, Waterloo Maple Inc., Waterloo Canada (2009)

Centre for Experimental and Constructive Mathematics,Simon Fraser University, Burnaby, Canada, V5A 1S6
E-mail address: ogilvie@cecm.sfu.ca and monagan@cecm.sfu.ca

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.