Albanian Journal of Mathematics

Për një Shqipëri të shkencës dhe kulturës.

Volume 12, 2018

www.albanian-j-math.com

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 3–7
ISSN: 1930-1235; (**2018**)

RINGS WHOSE ELEMENTS ARE SUMS OF THREE OR MINUS SUMS OF TWO COMMUTING IDEMPOTENTS

PETER V. DANCHEV

Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences
"Acad. G. Bonchev" str., bl. 8,
1113 Sofia, Bulgaria

Abstract. We classify up an isomorphism all rings having expressed their elements by at most three commuting idempotents. Our main result considerably extends certain important achievements established by Hirano-Tominaga [3], Ying et al. [6] and Tang et al. [5] as well as it somewhat strengthens recent results proved by the author in [1] and [2].

Mathematics Subject Classes 2010: Primary: 16U99; 16E50; Secondary: 13B99

Keywords: rings, idempotents, fields, Jacobson radical

1. Introduction and Background

Everywhere in the text of the present paper, all our rings R are assumed to be associative, containing the identity element 1, which in general differs from the zero element 0 of R, and all subrings are unital (i.e., containing the same identity as that of the former ring). Our terminology and notations are mainly in agreement with [4]. For instance, $U(R)$ denotes the set of all units in R, $Id(R)$ the set of all idempotents in R, and $Nil(R)$ the set of all nilpotents in R.

We here will be concerned with rings whose elements are representing by at most three commuting idempotents. Specifically, we start with the following new notion.

Definition 1.1. We shall say that a ring R is from the class $\mathcal{T}$ if, for each element $r \in R$ there are three commuting idempotents e_1, e_2, e_3 such that $r = e_1 + e_2 + e_3$ or $r = -e_1 - e_2$.

Under the substitution $r \to -r$, it takes the equivalent form $r = -e_1 - e_2 - e_3$ or $r = e_1 + e_2$.

E-mail address: danchev@math.bas.bg; pvdanchev@yahoo.com.
Date: Received: March 1, 2018. Accepted: July 7, 2018.

Immediate examples of such rings are $\mathbb{Z}_k$ where $k = 2, 3, 4, 5, 6$, whereas the direct product $\mathbb{Z}_5 \times \mathbb{Z}_5$ need not be so.

A brief history of the principally known results in the current subject is as follows: In [3] rings whose elements are sums of two commuting idempotents $e_1 + e_2$ were completely described. This was independently extended in both [1] and [5] to sums of three commuting idempotents $e_1 + e_2 + e_3$. Even something more, in [1] were classified those rings R whose elements are of the kind $e_1 + e_2 + e_3$ or $e_1 - e_2$. This is, however, a common expansion of the central statement from [6, Theorem 4.4], where the ring elements are written as $e_1 + e_2$ or $e_1 - e_2$. On the other hand, it is worthwhile noticing that the isomorphic structure of rings for which all elements are of the type $e_1 + e_2$ or $-e_1 - e_2$ was obtained in [2].

The goal of this article is to enlarge the aforementioned results, and especially the stated last one, by characterizing all rings from the class $\mathcal{T}$ as defined in Definition 1.1.

2. Main Results

We first begin with the following technicality.

Lemma 2.1. *Let R be a ring which belongs to the class $\mathcal{T}$. Then R can be decomposed as the direct product $R_1 \times R_2 \times R_3$, where $2^2 = 4 = 0$ in R_1, $3^2 = 9 = 0$ in R_2 and $5 = 0$ in R_3, and all of R_1, R_2, R_3 belong to the class $\mathcal{T}$.*

Proof. For an arbitrary element $x \in R$, we write that $x = e_1+e_2+e_3$ or $x = -e_1-e_2$ for some commuting idempotents e_1, e_2, e_3. We assert that $30^2 = 0$. In fact, if first $-3 = -e_1 - e_2$, then $-2 = (1 - e_1) - e_2$ and hence $(-2)^3 = -2$, i.e., $6 = 0$. If now $-3 = e_1 + e_2 + e_3$, one writes that $-4 = e_1 + e_2 - (1 - e_3) = e_1 + e_2 - e_3'$. Since $e_1 + e_2 - e_3' = e_1 + e_2(1 - e_3') - e_3'(1 - e_2) = e_1(1 - e_3'(1 - e_2)) + e_2(1 - e_3') - e_3'(1 - e_2)(1 - e_1)$ as all of these elements in the last record are commuting idempotents such that the first and the second ones are both orthogonal with the third one, we may with no loss of generality assume by replacing the existing idempotents that $e_1e_3' = e_2e_3' = 0$. Therefore, $6e_1e_2 = 0$ and thus $30e_1 = 0$ by multiplying with e_1 both sides of the equality $-4 = e_1 + e_2 - e_3'$ and the result by e_2. In a way of similarity, we get that $30e_2 = 0$. Furthermore, squaring $-4 = e_1 + e_2 - e_3'$ and manipulated subsequently with the obtained above facts, we infer that $6e_3' = 60$. Hence $-4 = e_1 + e_2 - e_3'$ multiplied by 30 leads to $180 = 0$ whence $30^2 = 0$ and so $30 \in Nil(R)$, as asserted. The Chinese Remainder Theorem now applies to write that $R \cong R_1 \times R_2 \times R_3$, where $2^2 = 4 = 0$ in R_1, $3^2 = 9 = 0$ in R_2 and, finally, $5 = 0$ in R_3, as asserted. The final part is now immediate. □

We next proceed by proving the following.

Proposition 2.2. *Suppose that R is a ring of characteristic 5. Then the following three conditions are equivalent:*

(i) $x^3 = x$ or $x^4 = 1$, $\forall x \in R$.

(ii) $x^3 = x$ or $x^3 = -x$, $\forall x \in R$.

(iii) R is isomorphic to the field $\mathbb{Z}_5$.

Proof. "(i) ⇒ (ii)". For an arbitrary but fixed $y \in R$ satisfying $y^4 = 1$ with $y^3 \neq y$, considering the element $y^2-1 \in R$, it must be that $(y^2-1)^4 = 1$ or $(y^2-1)^3 = y^2-1$.

In the first case, we receive $y^2=-1$ and thus equivalently $y^3=-y$, as required, while in the second one, we arrive at $y^2=1$ and so in an equivalent form $y^3=y$ which is against our initial assumption.

"(ii) $\Longleftrightarrow$ (iii)". Let P be the subring of R generated by 1, and thus note that $P\cong\mathbb{Z}_5$. We claim that $P=R$, so we assume in a way of contradiction that there exists $b\in R\setminus P$. With no loss of generality, we shall also assume that $b^3=b$ since $b^3=-b$ obviously implies that $(2b)^3=2b$ as $5=0$ and $b\notin P\iff 2b\notin P$.

Let us now $(1+b)^3=-(1+b)$. Hence $b=b^3$ along with $5=0$ enable us that $b^2=1$. This allows us to conclude that $(1+2b)^3\neq\pm(1+2b)$, however. In fact, if $(1+2b)^3=1+2b$, then one deduces that $2b=3\in P$ which is manifestly untrue. If now $(1+2b)^3=-1-2b$, then one infers that $2b=2\in P$ which is obviously false. That is why, only $(1+b)^3=1+b$ holds. This, in turn, guarantees that $b^2=-b$. Moreover, $b^3=b$ is equivalent to $(-b)^3=-b$ as well as $b^3=-b$ to $(-b)^3=-(-b)$ and thus, by what we have proved so far applied to $-b\notin P$, it follows that $-b=b^2=(-b)^2=-(-b)=b$. Consequently, $2b=0=6b=b\in P$ because $5=0$, which is the wanted contradiction. We thus conclude that $P=R$, as expected.

Conversely, it is trivial that the elements of $\mathbb{Z}_5=\{0,1,2,3,4\mid 5=0\}$ are solutions of one of the equations $x^3=x$ or $x^3=-x$.

"(iii) $\Rightarrow$ (i)". It is self-evident that all elements of $\mathbb{Z}_5=\{0,1,2,3,4\mid 5=0\}$ satisfy one of the equations $x^3=x$ or $x^4=1$. □

We now have all the ingredients necessary to prove our basic result.

Theorem 2.3. *A ring R lies in the class $\mathcal{T}$ if, and only if, R is decomposable as $R_1\times R_2\times R_3$, where*

(1) $R_1=\{0\}$, or R_1 is a non-zero commutative ring such that $4=0$ and $R_1/J(R_1)$ is a boolean ring with either $J(R_1)=\{0\}$ or nil $J(R_1)=2Id(R_1)$;

(2) $R_2=\{0\}$, or R_2 is a subdirect product of family of copies of the field $\mathbb{Z}_3$;

(3) $R_3=\{0\}$ (which is mandatory when $J(R_1)\neq\{0\}$), or $R_3\cong\mathbb{Z}_5$.

Proof. "**Necessity.**" With Lemma 2.1 at hand, one writes that $R\cong R_1\times R_2\times R_3$, where R_1 is either zero or R_1 is a nonzero ring in which $4=0$, where R_2 is either zero or R_2 is a nonzero ring in which $9=0$, and where R_3 is either zero or R_3 is a nonzero ring in which $5=0$, as well as R_1,R_2,R_3 remains in the class $\mathcal{T}$.

In order to describe the three direct factors, we distinguish three basic cases, namely:

Case 1: *Describing R_1.* We have $4=0$ and $2\in Nil(R_1)$ whence $2\in J(R_1)$, so that $R_1/J(R_1)$ is necessarily boolean being a factor-ring of characteristic 2 whose elements are sums of (at most three) commuting idempotents. What remains to prove is that $J(R_1)=2Id(R_1)$. In showing that, the case when any element from $J(R_1)$ is written as a sum of three commuting idempotents follows analogously to [1] getting that $J(R_1)=2Id(R_1)$. That is why, we will be now concerned with $z=-e-f$ for an arbitrary $z\in J(R_1)$, where $e,f\in Id(R_1)$ do commute. Multiplying by $1-f$, we get that $z(1-f)=-e(1-f)\in J(R_1)\cap(-Id(R_1))=\{0\}$ whence $e=ef$. Similarly, $ef=f$ and so $e=f$. Finally, $z=-2e\in-2Id(R_1)=2Id(R_1)$, because $4=0$, as promised.

Case 2: *Describing R_2.* We have $9=0$ and $3\in J(R_2)$. We assert that $J(R_2)=\{0\}$ and hence $3=0$ in R_2. In fact, as in the preceding case, it follows

that $J(R_2) = \pm 2Id(R_2) = \mp Id(R_2) = \{0\}$, as asserted. Furthermore, it is routinely checked that $x^3 = x$ for every $x \in R_2$ and thus, the main result from [3] applies to get our stated conclusion.

Case 3: *Describing* R_3. We have $5 = 0$ and $x^5 = x$ for all elements x in R_3. Now, for each $x \in R_3$, we write that $x = e + f + h$ or $x = -e - f$ for some three commuting idempotents e, f, h. For the first record, one deduces after squaring that $2x^3 - x^2 - x = 2efh$ because $x^3 = x + ef + fh + he + efh$, so that multiplying both sides by 3 it follows that $x^3 + 2x^2 + 2x = efh$ is an idempotent. This means that $(x^3 + 2x^2 + 2x)^2 = x^3 + 2x^2 + 2x$ which, after some usual tricks, amounts to $3x^4 + 2x^3 - 2x^2 + 2x = 0$. Multiplying this by 2, we finally arrive at $x^4 - x^3 + x^2 - x = 0$. Replacing x with $x - 1$ in the given last equality, one infers that $x^4 = 1$.

As for the second record, one derives after squaring that $x^3 - 2x^2 - 3x = x^3 - 2x^2 + 2x = 0$ because $x^3 = x - ef$ and so $(x - x^3)^2 = x - x^3$. Replacing x by $x - 1$ in the given equation, one infers that $x^3 = x$.

Now, since for any $x \in R_3$ it must be that $x^3 = x$ or $x^4 = 1$, we henceforth can successfully apply Proposition 2.2 to conclude that R_3 has to be isomorphic to the five element field $\mathbb{Z}_5$, as stated.

So, finally, the full description of R over, as formulated.

"**Sufficiency.**" A direct consultation with [3] enables us that every element of R_2 is a sum of two idempotents. Since it is pretty easy that each element in $\mathbb{Z}_5$ is a sum of three idempotents (e.g., 0, 1, 2 and 3) or minus a sum of two idempotents (e.g., 0 and 4), what remains to prove is that any element from R_1 is a sum of three idempotents. It is, really, well known that if $2 = 0$ in R_1 it must have a sum of two idempotents or even just a single idempotent. To that purpose, taking an arbitrary $r \in R_1$, we may write that $r + J(R_1)$ is an idempotent and thus $r - r^2 \in J(R_1) = 2Id(R_1)$. But $J(R_1)$ is nil with $J^2 = \{0\}$ (as $4 = 0$) and hence there exists an idempotent $g \in R_1$ with $r - g \in 2Id(R_1)$. This containment allows us to write that $r = g + 2h = g + h + h$ for some $h \in Id(R_1)$, as required. □

Remark 2.4. Considering the rings $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_5$, $\mathbb{Z}_3 \times \mathbb{Z}_5$ or $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, one says that they still are in the class $\mathcal{T}$, whereas as commented above the rings $\mathbb{Z}_4 \times \mathbb{Z}_5$ and $\mathbb{Z}_5 \times \mathbb{Z}_5$ are not. However, for any element x lying in the last direct product, x or $-x$ is a sum of three idempotents. That is why, it will be of interest to consider those rings having the mentioned property – see the problem posed below.

As for the direct product $\mathbb{Z}_4 \times \mathbb{Z}_5$, consider the element $(1, 4)$ which is not presentable neither as a sum of three idempotents nor as a minus sum of two idempotents. Nevertheless, $(1, 4) = (1, 0) - (0, 1)$. Reciprocally, the element $(2, 4) = -(1, 0) - (1, 1)$, but a routine check shows that $(2, 4)$ is not neither the sum of three idempotents nor the difference of two idempotents, as expected. Resuming, $(1, 4)$ lies in $\mathcal{K} \setminus \mathcal{T}$ as opposite to $(2, 4)$ which lies in $\mathcal{T} \setminus \mathcal{K}$.

Meanwhile, surprisingly, against this element-wise discrepancy, the present class $\mathcal{T}$ from Definition 1.1 coincides with the class $\mathcal{K}$ from [1]. Likewise, the class $\mathcal{C}$ from [2] is contained in the class $\mathcal{K}$ from [1]. As a matter of fact, if $x = e_1 + e_2$ or $x = -e_1 - e_2$ for any element x, then one can write that $x - 1 = e_1 + e_2$ or $x - 1 = -e_1 - e_2$ and thus one gets that $x = e_1 + e_2 + 1$ or $x = (1 - e_1) - e_2$, as required.

So, we end our work with the following well-motivated problem:

Problem 2.5. Describe the isomorphic structure of those rings whose elements are sums or minus sums of three commuting idempotents, that is, for any element a of a ring R it is fulfilled that $a = e_1 + e_2 + e_3$ or $a = -e_1 - e_2 - e_3$ for some three commuting idempotents e_1, e_2, e_3 of R. In other words, $\forall a \in R$: a or $-a$ is a sum of three commuting idempotents.

Here the ring $\mathbb{Z}_7$ arose quite naturally, which however not occurred in the statements above, so that some new techniques should be exploited.

References

[1] P.V. Danchev, *Rings whose elements are sums of three or differences of two commuting idempotents*, Bull. Iran. Math. Soc. **45** (2019).

[2] P.V. Danchev, *Rings whose elements are sums or minus sums of two commuting idempotents*, Boll. Un. Mat. Ital. **12** (2019).

[3] Y. Hirano, H. Tominaga, *Rings in which every element is the sum of two idempotents*, Bull. Austral. Math. Soc. **37** (1988), 161–164.

[4] T.Y. Lam, A First Course in Noncommutative Rings, Second Edition, Graduate Texts in Math., Vol. **131**, Springer-Verlag, Berlin-Heidelberg-New York, 2001.

[5] G. Tang, Y. Zhou and H. Su, *Matrices over a commutative ring as sums of three idempotents or three involutions*, Lin. and Multilin. Algebra (2018).

[6] Z. Ying, T. Koşan and Y. Zhou, *Rings in which every element is a sum of two tripotents*, Can. Math. Bull. (3) **59** (2016), 661–672.

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 8–14
ISSN: 1930-1235; (**2018**)

THE *abc* CONJECTURE IMPLIES THE WEAK DIVERSITY CONJECTURE

HILAF HASSON

University of Maryland,
College Park, MD 20742, USA

ANDREW OBUS

University of Virginia,
Charlottesville, VA 22904, USA

Abstract. We show that the *abc* Conjecture implies the Weak Diversity Conjecture of Bilu and Luca. In addition, we unconditionally reduce the Weak Diversity Conjecture to the case of cyclic covers of prime order.

MSC 2010: Primary: 11G30, 14G25; Secondary: 14H25, 14H30
Keywords: Hilbert irreducibility theorem, rational points

1. Introduction

This note concerns the Weak and Strong Diversity Conjectures. The Strong Diversity conjecture, due to Andrzej Schinzel, first appeared in [DZ], in the discussion following Theorem 2 of that paper. (The name "Strong Diversity" first appeared in [BL], as Conjecture 1.5.) Recall that a geometrically irreducible branched cover of curves over a number field is one where both the source and the target are irreducible after base change to $\overline{\mathbb{Q}}$.

Conjecture 1.1. *("Strong Diversity") Let $X \to \mathbb{A}^1_{\mathbb{Q}}$ be a geometrically irreducible branched cover of curves over $\mathbb{Q}$, such that not all of its branch points are $\mathbb{Q}$-rational, or such that the cover is not abelian. Let $k(N)$ be the compositum of the fields of rationality of the points in the fibers over $x = 1, ..., N$. Then there exists a positive constant c, independent of N, such that the degree of $k(N)$ over $\mathbb{Q}$ is at least e^{cN}.*

E-mail addresses: hilaf@math.umd.edu, andrewobus@gmail.com.
Date: Received: June 15, 2018. Accepted: July 15, 2018.
The second author was supported by NSF grant DMS-1602054.

We note that the hypotheses in the above conjecture are necessary, and we refer the reader to [DZ] for further discussion. The Strong Diversity Conjecture is closely related to the "Weak Diversity Conjecture" (Conjecture 1.4 in [BL]), which is itself an extension of a conjecture of Cutter, Granville, and Tucker ([CGT, Conjecture 1]).

Conjecture 1.2. *("Weak Diversity") Let K be a number field, and let $X \to \mathbb{A}^1_K$ be a non-trivial geometrically irreducible branched cover of curves over K. Then there exists a positive constant c such that the number of different fields appearing as residue fields of the points in the fibers over $x = 1, ..., N$ is at least cN for all N.*

We remark that the Weak Diversity Conjecture was only stated in [BL] for $K = \mathbb{Q}$, but we, in fact, prove the more general form of Conjecture 1.2 under the assumption of the *abc* Conjecture. Note also that for $K = \mathbb{Q}$, the consequence of Conjecture 1.1 implies the consequence of Conjecture 1.2. The hypotheses of Conjecture 1.2, however, are weaker. In [BL], Bilu and Luca prove Weak Diversity (for $K = \mathbb{Q}$) in the case not covered by Strong Diversity, namely for covers where the branch points are $\mathbb{Q}$-rational, and the cover is abelian. They therefore conclude that Strong Diversity implies Weak Diversity for $K = \mathbb{Q}$.

Remark 1.3. The Weak and Strong Diversity Conjectures were stated in [BL] in terms of residue fields of a *given* point in each fiber. In light of the quantitative version of Hilbert's Irreducibility Theorem ([S, Theorem, p. 134]), all fibers except negligibly many have only one point. So the formulations of [BL] are equivalent to our formulations above. For Weak Diversity, it would also be equivalent to look at the *compositum* of the residue fields of all points in each fiber. We use this formulation in Propositions 3.2 and 3.3.

While this was not mentioned in earlier discussions of this conjecture, we remark that the Weak Diversity Conjecture is also closely related to the following conjectural form of a uniform Faltings' Theorem (although we are not aware of any clear connection between the *abc* conjecture and this uniform Faltings' theorem beyond the fact that the *abc* conjecture implies the basic Faltings' theorem [E]). This form first appeared in [P], where Pacelli proves this conjecture under the assumption of Lang's conjecture about rational points on varieties of general type; see also [CHM].

Conjecture 1.4. *("Uniform Faltings' Theorem") Let $g \geq 2$ and d be natural numbers. Then there exists a constant $B_{d,g}$ such that for every number field L of degree d over $\mathbb{Q}$, and for every curve X of genus g over L, we have that $\#X(L) \leq B_{d,g}$.*

As we will soon see (Proposition 3.2), the Weak Diversity Conjecture can be reduced to the case of G-Galois covers $f : X \to \mathbb{A}^1_K$. In the Galois case, Conjecture 1.4 implies Weak Diversity for $g(X) \geq 2$, which will be shown in §5. In this way, Weak Diversity can be viewed as a weaker form of Conjecture 1.4 that, unlike Conjecture 1.4, also applies to genera 0 and 1. Note that Conjecture 1.4 is not even known for twists of a given curve; see related results in this direction in [S1] and [S2].

Strong Diversity is known in either of two cases: (a) when one of the branch points is of degree either 2 or 3 above $\mathbb{Q}$ ([DZ, Theorem 2(b)]), or (b) if the branch points are all $\mathbb{Q}$-rational and the normal closure of $X \to \mathbb{A}^1_{\mathbb{Q}}$ satisfies some condition (for example if its Galois group is either alternating, symmetric or non-abelian

simple group of non-square order; see [DZ]). Weak Diversity (but not Strong Diversity) was also proven ([CZ, Corollary 1]) in the case that X has at least 3 geometric points above ∞. See also Proposition 3.4, and preliminary discussion thereof, in this paper. We also remark that in [D], Dèbes proves a version of the strong diversity conjecture where one looks at fibers over $n+1, \ldots, n+N$ for some n depending on N.

In this paper we reduce Weak Diversity to the case of a cyclic Galois cover. As a consequence, we show that the *abc* Conjecture (for an appropriate number field) implies Weak Diversity (Theorem 4.2 — although this can be proven without our reduction, see Remark 4.4). We also show that *abc* implies Strong Diversity for the case that not all branch points are $\mathbb{Q}$-rational (Theorem 2.2).

We mention that Mochizuki claims to have proven the Vojta conjecture for all curves over number fields ([M, Discussion after Theorem A]), which implies the *abc* Conjecture over number fields. If Mochizuki's proof is verified, then Weak Diversity will hold unconditionally.

ACKNOWLEDGEMENTS

The authors thank Larry Washington for fruitful conversations, and Andrew Granville, Ram Murty and Taylor Dupuy for very thorough and helpful answers to their mathematical inquiries. They also thank Pierre Dèbes for useful comments.

2. PROOF OF THE NON-RATIONAL BRANCH POINT CASE OF STRONG DIVERSITY GIVEN *abc*

As was mentioned above, Dvornicich and Zannier proved Strong Diversity for $f : X \to \mathbb{A}^1_{\mathbb{Q}}$ whenever f has a branch point of index 2 or 3. Combining the *abc* Conjecture with a result of Granville allows us to weaken this assumption to f having a branch point not defined over the base field.

Lemma 2.1. *Assume the abc Conjecture. Then*

$$n = O(\#\{p \geq n \mid v_p(g(m)) = 1 \text{ for some } m \leq n\})$$

whenever $g \in \mathbb{Z}[x]$ is an irreducible polynomial of degree at least 2. If $\deg g \in \{2, 3\}$, then the abc Conjecture is not required.

Proof. By [DZ, Eq. (1) on p. 427], the lemma is true unconditionally if $v_p(g(m)) = 1$ is replaced by $p \mid g(m)$. So it suffices to show that

$$\#\{p \geq n \mid v_p(g(m)) > 1 \text{ for some } m \leq n\} = o(n).$$

If $\deg g \in \{2, 3\}$, this follows as on [DZ, p. 427], without the *abc* Conjecture. In any case, if $\deg g \geq 3$, this follows from [G, Theorem 8] applied to the homogenization of g, taking $N = n$ and $M = 1$. □

Theorem 2.2. *Suppose that the branch locus Δ of $f : X \to \mathbb{A}^1_{\mathbb{Q}}$ contains a point of degree ≥ 2 over $\mathbb{Q}$, and that the abc Conjecture is true. Then Strong Diversity holds for f.*

Proof. Let X' be a plane curve such that $X \dashrightarrow X' \xrightarrow{f'} \mathbb{A}^1_{\mathbb{Q}}$ is a factorization of f as a rational map with $X \dashrightarrow X'$ birational. To prove Strong Diversity for f, it suffices to prove it for f'.

Since X' is a plane curve, we are in the situation of [DZ]. If Δ has a point of degree 2 or 3 over $\mathbb{Q}$, then this is [DZ, Theorem 2(b)]. The only input to the proof in [DZ] that requires Δ to have a point of degree 2 or 3 is the result of Lemma 2.1 for some irreducible factor g of a polynomial cutting out Δ (see [DZ, (11), p. 437]). By our assumptions on Δ, there is such a factor of degree ≥ 2. Since we assume the *abc* Conjecture, the proposition follows from Lemma 2.1. □

3. Unconditional reduction of Weak Diversity to cyclic case

In this section, we reduce Weak Diversity to the case of cyclic covers of prime order. We do not assume the *abc* Conjecture.

Lemma 3.1. *If a cover $f : X \to \mathbb{A}^1_{K_0}$ is defined over a number field K_0, then Weak Diversity for f is equivalent to Weak Diversity for any base change f_K over a number field extension K/K_0.*

Proof. The residue field of a point in $f_K^{-1}(n)$ is the compositum of the residue field of the corresponding point of $f^{-1}(n)$ with K. If two number fields have distinct composita with K, they must be distinct. On the other hand, given a number field L, there are only finitely many distinct number fields whose compositum with K is L. The lemma follows. □

Proposition 3.2. *Suppose that $f : X \to \mathbb{A}^1_K$ is a cover defined over a number field K and L/K is a finite extension for which the Galois closure $f' : X' \to \mathbb{A}^1_L$ of the base-change f_L of f to L is geometrically irreducible and defined over L as a Galois cover. Then to prove Weak Diversity for f, it suffices to prove it for f'.*

Proof. By Lemma 3.1, we may assume that $L = K$ and $f_L = f$. Let L_n (resp. L'_n) be the field generated by the residue fields of the points of $f^{-1}(n)$ (resp. $(f')^{-1}(n)$). We note that L'_n is Galois over K and is contained in the Galois closure of L_n over K. So L'_n is the Galois closure of L_n over K. So if $L'_i \neq L'_j$, then $L_i \neq L_j$. Thus Weak Diversity for f' implies Weak Diversity for f. □

Proposition 3.3. *Suppose $f : X \to \mathbb{A}^1_K$ is a quotient cover of $g : Y \to \mathbb{A}^1_K$. Then Weak Diversity is true for g if it is true for f.*

Proof. Let L_n (resp. L'_n) be the field generated by the residue fields of the points of $f^{-1}(n)$ (resp. $g^{-1}(n)$). Then $L_n \subseteq L'_n$ and the degree of L'_n over the base field is bounded in terms of g, which means that there exists $d \in \mathbb{N}$ such that each L'_i can correspond to at most d non-isomorphic L_js. So if the number of distinct L'_n for $n \leq N$ is at least cN, then the number of distinct L_n for $n \leq N$ is at least cN/d. □

Proposition 3.4 below was stated in [BL] as a consequence of [CZ, Corollary 1], but we supply some more details on the proof here. Recall that if L is a number field and S is a finite set of places containing the archimedean places, then $\mathcal{O}_{L,S} \subset L$ is the subring of L consisting of elements whose valuations at all places outside of S are nonnegative.

Proposition 3.4. *Let $f : X \to \mathbb{A}^1_{K_0}$ be a branched cover defined over a number field K_0. If the smooth projective completion of f has at least three $\overline{\mathbb{Q}}$-points over ∞, then Weak Diversity holds for f.*

Proof. Embed $X \subset \mathbb{A}^m_{K_0}$ as an affine curve. If K/K_0 is a finite extension and S is a finite set of places of $\mathcal{O}_K$ including the archimedean places, [CZ, Corollary 1] implies that the number of $\mathcal{O}_{K,S}$-integral points of X is bounded in terms of the degree of K and the cardinality of S. Now, since the ring extension $K_0[X]/K_0[t]$ corresponding to f is generated by roots of finitely many monic polynomials over K_0, there is a finite set of places S_0 of K_0 such that the same is true for $\mathcal{O}_{K_0,S_0}[X]/\mathcal{O}_{K_0,S_0}[t]$. Taking S to be the set of places of K lying above S_0, we see that every K-point of X lying above an $\mathcal{O}_{K_0,S_0}$-point of $\mathbb{A}^1_{\mathcal{O}_{K_0,S_0}}$ is in fact an $\mathcal{O}_{K,S}$-point. Thus, the number of such points is bounded solely in terms of the degree of K.

Since any field L arising as the residue field of a point of $f^{-1}(n)$ for $n \in \mathbb{N}$ has degree at most $\deg(f)$ over K_0, there is an absolute bound, depending only on f, on the number of such points with residue field L. This immediately implies Weak Diversity for f. □

Proposition 3.5. *To prove Weak Diversity for a cover defined over a number field with a given branch locus Δ, it suffices to prove it for cyclic covers of prime order with branch locus contained in Δ.*

Proof. By Lemma 3.1 and Proposition 3.2, we may assume the cover is Galois for some group G. If the cover has at least three $\overline{\mathbb{Q}}$-points defined over ∞, then the proposition follows from Proposition 3.4, so assume there are at most two such points. Then the stabilizer of one of these points is a cyclic group of index at most 2 in G. So either G is cyclic or G has $\mathbb{Z}/2$ as a quotient. In either case, G has a cyclic group of prime order as a quotient, and the quotient cover has branch locus contained in Δ, so we are done by Proposition 3.3. □

Remark 3.6. The most difficult case for the Weak Diversity Conjecture seems to be that of a *quadratic* cover. In this case, it is tantamount to showing that for a separable polynomial $f \in K[x]$, the number of distinct square classes in the set $\{f(1), \ldots, f(N)\}$ is at least cN for some constant $c > 0$ and all N.

4. Proof of Weak Diversity given *abc*

Lemma 4.1. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let $f(x) \in \mathcal{O}_K[x]$ be a non-constant polynomial. Then there is a constant c, depending on f, such that for any ideal $I \subseteq \mathcal{O}_K$, the set $\{n \in \mathbb{N} \mid (f(n)) = I\}$ has cardinality bounded by c.*

Proof. It suffices to bound the number of n such that $N_{K/\mathbb{Q}}(f(n))$ equals any particular constant. But $N_{K/\mathbb{Q}}(f(n))$ is a polynomial in n over $\mathbb{Q}$, whose absolute value is easily seen to go to ∞ as $n \to \infty$. Thus it is non-constant, and the lemma follows. □

Theorem 4.2. *Let $f : X \to \mathbb{A}^1_K$ be a geometrically irreducible branched cover over some number field K, and let L be a number field such that each branch point of f is L-rational. Then the abc Conjecture[1] for L implies Weak Diversity holds for f.*

Proof. By Lemma 3.1 we may, without loss of generality, assume that $L = K$. By Proposition 3.5, we may assume that f is a $\mathbb{Z}/p$-cover, for some prime p. After a base change, and using Lemma 3.1 again, we may assume that f is given by an

[1] See, e.g., [V, p. 84]

equation $y^p = g(x)$, where $g(x) \in \mathcal{O}_K[x]$ is a polynomial with roots exactly at the branch points and all roots of $g(x)$ have order at most $p-1$.

Let $h(x) \in \mathcal{O}_K[x]$ be a separable polynomial with the same leading coefficient and roots as $g(x)$. By the number field version[2] of [G, Theorem 1], there exists a positive constant c and an ideal $I \subseteq \mathcal{O}_K$ such that for large enough N, the ideal $(h(n))I^{-1} \subseteq \mathcal{O}_K$ is squarefree for at least cN elements $n \in \{1, \dots, N\}$. By Lemma 4.1, after replacing c by a smaller positive constant, we can find cN elements $n \in \{1, \dots, N\}$ such that $(h(n))I^{-1}$ is squarefree and the ideals $(h(n))$ are pairwise distinct. After replacing c by yet a smaller constant, we may assume that the prime factorizations of the ideals $(h(n))$ are pairwise distinct even when prime factors of I and of (p) are ignored.

Now, $h(n) \mid g(n) \mid h(n)^{p-1}$, so the primes ramified in $K(g(n)^{1/p})/K$, other than those dividing I or (p), are exactly those primes dividing $(h(n))$. Thus the fields $K(g(n)^{1/p})$ are pairwise distinct, which proves Weak Diversity for f. □

Remark 4.3. Combining Theorem 4.2 with Theorem 2.2, we see that assuming the *abc* Conjecture over $\mathbb{Q}$ suffices to prove Weak Diversity for covers defined over $\mathbb{Q}$, even if the branch locus does not consist of $\mathbb{Q}$-points.

Remark 4.4. A similar argument to prove Theorem 4.2 can also be made combining the paper [G] with arguments from [DZ] using the discriminant of the cover f as a substitute for the Kummer generator $g(x)$ without first reducing to the cyclic case. Since [DZ] is is written in the context of covers over $\mathbb{Q}$, we provide the above proof so as not to have to adapt their result.

5. The Uniform Faltings' Theorem and Weak Diversity

In this section, we prove the following proposition.

Proposition 5.1. *Let $f : X \to \mathbb{A}^1_K$ be a Galois branched cover over a number field K with $g(X) \geq 2$. Then Conjecture 1.4 implies Weak Diversity for f.*

Proof. Let G be the Galois group of f and let K be a field Let T be a right G-torsor over K. There exists a twist X^T of X, defined over K such that for K-rational points P of $\mathbb{A}^1_K$, the restriction $X \times_{\mathbb{A}^1_K} \{P\}$ is isomorphic to T as a right G-torsor iff X^T has a K-rational point above P. See, for example, Lemma 3.3.1 of [H], and surrounding discussion. Since all of these twists have the same genus and are defined over K, Conjecture 1.4 implies that there is a uniform bound on the number of rational points on any given twist. This implies that for any given G-extension L/K, there is a uniform bound on the number of K-rational points $\{P\}$ of $\mathbb{A}^1_K$ such that $f^{-1}(P)$ is a point with residue field L. Combining this with Hilbert's irreducibility theorem as in Remark 1.3, we obtain Weak Diversity for f. □

Remark 5.2. Proposition 5.1 is more or less the same as the second statement in [D, Theorem 1.3]. The first statement of that same theorem shows that a weaker statement than Weak Diversity holds unconditionally.

[2] See the remark on [G, p. 993]

References

[DZ] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **21** (1994), no. 3, 421–443. MR1310635

[BL] Yuri Bilu and Florian Luca, *Diversity in parametric families of number fields*, 2016. Preprint, arXiv:1607.00904.

[CGT] Pamela Cutter, Andrew Granville, and Thomas J. Tucker, *The number of fields generated by the square root of values of a given polynomial*, Canad. Math. Bull. **46** (2003), no. 1, 71–79. MR1955614

[BL] Yuri Bilu and Florian Luca, *Number fields in fibers: the geometrically abelian case with rational critical values*, 2016. Preprint, arXiv:1606.09164.

[S] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Third, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR1757192

[E] Noam D. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices **7** (1991), 99–109. MR1141316

[P] Patricia L. Pacelli, *Uniform boundedness for rational points*, Duke Math. J. **88** (1997), no. 1, 77–102. MR1448017

[CHM] Lucia Caporaso, Joe Harris, and Barry Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35. MR1325796

[S1] Joseph H. Silverman, *A uniform bound for rational points on twists of a given curve*, J. London Math. Soc. (2) **47** (1993), no. 3, 385–394. MR1214903

[S2] Michael Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR2264661

[DZ] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions. II. (On a conjecture of Schinzel)*, Acta Arith. **72** (1995), no. 3, 201–210. MR1347486

[CZ] Pietro Corvaja and Umberto Zannier, *On the number of integral points on algebraic curves*, J. Reine Angew. Math. **565** (2003), 27–42. MR2024644

[D] Pierre Dèbes, *On a problem of Dvornicich and Zannier*, Acta Arith. **73** (1995), no. 4, 379–387. MR1366044

[M] Shinichi Mochizuki, *Inter-Universal Teichmuller theory IV: Log-volume computations and set-theoretic foundations*, 2012. Preprint.

[G] Andrew Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices **19** (1998), 991–1009. MR1654759

[V] Paul Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics, vol. 1239, Springer-Verlag, Berlin, 1987. MR883451

[H] Hilaf Hasson, *Minimal fields of definition for Galois action*, J. Pure Appl. Algebra **220** (2016), no. 9, 3327–3331. MR3486304

[D] Pierre Dèbes, *On the Malle conjecture and the self-twisted cover*, Israel J. Math. **218** (2017), no. 1, 101–131. MR3625127

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 15–23
ISSN: 1930-1235; (**2018**)

ON MACBEATH'S FORMULA FOR HYPERBOLIC MANIFOLDS

GRZEGORZ GROMADZKI

Faculty of Mathematics, Physics and Informatics,
Gdańsk University, Gdańsk, Poland

RUBÉN A. HIDALGO

Departamento de Matemática y Estadística,
Universidad de La Frontera, Temuco, Chile

In memory of Kay Magaard

Abstract. Around 1973, Macbeath provided a formula for the number of fixed points of an element in a group G of conformal automorphisms of a closed Riemann surface S of genus at least two. Such a formula was initially used to obtain the character of the representation associated to the induced action of G on the first homology group of S, and later turned out to be extremely useful in many other contexts. By using a simple counting procedure, we provide a similar formula for the number of connected components of an element in a finite group of isometries of a hyperbolic manifold.

MSC 2010: Primary: 30F40, 57M12; Secondary: 57M50, 57S30, 22E40
Keywords: Hyperbolic manifolds, fixed points, automorphisms

1. Introduction

Let S be a closed Riemann surface of genus at least two and let G be a (necessarily finite) group of conformal automorphisms of S. In 1973, Macbeath [14] found a formula for the number of fixed points of each $g \in G$ in terms of the topological action of G (see Section 4). Later, in [5, 6, 7, 12], a generalization of this formula to count the number of connected components of fixed points, has been found for the cases of anti-conformal automorphisms of compact Riemann surfaces and also for dianalytic automorphisms of bordered and unbordered compact Klein surfaces (both in orientable and non-orientable cases). Let us note that if H is a finite group

E-mail addresses: grom@mat.ug.edu.pl, ruben.hidalgo@ufrontera.cl.
Date: Received: September 1, 2018. Accepted: October 2, 2018.
G. Gromadzki was supported by Polish National Sciences Center by the grant NCN 2015/17/B/ST1/03235, R. A. Hidalgo was supported by Projects FONDECYT 1190001 .

of orientation-preserving homeomorphisms of a closed orientable surface X, then it is well known that on X there is the structure of a Riemann surface making H to act as a group of conformal automorphisms; so actually Macbeath's formulas can be applied for arbitrary periodic self-homeomorphisms. Furthermore, due to well known description of discrete cocompact groups of isometries of the hyperbolic plane, the formulas in the 2-dimensional case have more explicit character.

Now, let us assume we are given a pair (M, G), where M is an $(n+1)$-dimensional hyperbolic manifold, where $n \geq 1$, and G is a finite group of its isometries. Then there is a triple $(\mathcal{F}, \mathcal{K}, \theta)$, where $\mathcal{K}$ is a group of isometries of the hyperbolic $(n+1)$-dimensional space $\mathcal{H}^{n+1}$ and $\theta : \mathcal{K} \to G$ is a surjective homomorphism with a torsion free kernel $\mathcal{F}$, so that $M = \mathcal{H}^{n+1}/\mathcal{F}$ and $M/G = \mathcal{H}^{n+1}/\mathcal{K}$. Under the assumption that $\mathcal{K}$ is finitely generated and it has a finite number of conjugacy classes of finite order elements (we say that it is of finite type), by using an elementary counting method on G, we may obtain a formula, similar to Macbeath's one, to count the number of connected components of a non-trivial element $g \in G$ (see Theorem 3.3). It seems that a similar formula is not provided in the literature. Examples of Kleinian groups $\mathcal{K}$ of finite type are the geometrically finite ones [4, 13] and, for $n = 2$, the locus of geometrically finite Kleinian groups is dense on the space of finitely generated Kleinian groups [3, 18, 19]; two examples are provided in the last section.

We should remark that, by suitable modification of the proof of Theorem 3.3, it can be shown that the provided formula to count the number of connected components of isometries still valid for G being a finite group of isometries of a Riemannian manifold M for which its universal Riemannian cover space $\widetilde{M}$ has the property that its finite order isometries have non-empty and connected set of fixed points. Examples of these are for $\widetilde{M}$ being either (i) the Teichmüller space $\mathcal{T}_g$ of genus $g \geq 1$ Riemann surfaces or (ii) the Siegel space $\mathfrak{H}_g$ parametrizing principally polarized abelian varieties.

2. Preliminaries

In this section we recall some concepts and facts concerning isometries of hyperbolic spaces, (extended) Kleinian groups and its associated manifolds, which shall be used in the rest of this paper. Good references on these are, for instance, the classical books [16, 17].

2.1. **Hyperbolic space.** For $n \geq 1$, we shall use as a model of the $(n+1)$-dimensional hyperbolic space $\mathcal{H}^{n+1}$ the $(n+1)$-dimensional upper-half space $\{x = (x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} : x_{n+1} > 0\}$ equipped with the Riemannian metric $ds = \|dx\|/x_{n+1}$. Its conformal boundary is the n-dimensional sphere $\mathcal{S}^n = \mathbb{R}^n \cup \{\infty\}$. Each $(n-1)$-dimensional sphere $\Sigma \subset \mathcal{S}^n$ (for $n = 1$, Σ is understood as two different points) has associated a reflection $\sigma = \sigma_\Sigma$ having Σ as its locus of fixed points. By the Poincaré extension theorem, the reflection σ extends naturally to an order two orientation reversing isometry of $\mathcal{H}^{n+1}$; this being the reflection on the half-n-dimensional sphere inside $\mathcal{H}^{n+1}$ induced by Σ. A Möbius (respectively, extended Möbius) transformation of $\mathcal{S}^n$ is the composition of an even (respectively odd) number of reflections. By the classical complex analysis, for $n = 2$, and the Liouville Theorem, for $n \geq 3$, the group $\widehat{\mathcal{M}}^n$, composed by all Möbius and extended Möbius transformations, is the full group of conformal automorphisms of

$\mathcal{S}^n$. We shall denote denote by $\mathcal{M}^n$ its canonical subgroup of index two consisting of all Möbius transformations. Again, by the Poincaré extension theorem, every Möbius (respectively, extended Möbius) transformation extends to an orientation-preserving (respectively, orientation-reversing) isometry of $\mathcal{H}^{n+1}$ and all isometries of $\mathcal{H}^{n+1}$ are obtained in this way. This allows us to identify the group $\widehat{\mathcal{M}}^n$ with the group $\mathrm{Isom}(\mathcal{H}^{n+1})$ of all isometries of $\mathcal{H}^{n+1}$ and $\mathcal{M}^n$ with the index two subgroup $\mathrm{Isom}^+(\mathcal{H}^{n+1})$ of all its orientation-preserving isometries. An element of $\widehat{\mathcal{M}}^n$, viewed as an isometry of $\mathcal{H}^{n+1}$, may or may not have fixed points in $\mathcal{H}^{n+1}$ and if the former is the case, then it is called *elliptic* if it preserves orientation and *pseudo-elliptic* otherwise. The locus of fixed points, in the hyperbolic space, of an elliptic or pseudo-elliptic transformation is known to be either a point or a totally geodesic subspace of $\mathcal{H}^{n+1}$.

2.2. **Kleinian groups.** A *Kleinian group* is a discrete subgroup of $\mathcal{M}^n$ and an *extended Kleinian group* is a discrete subgroup of $\widehat{\mathcal{M}}^n$ not contained in $\mathcal{M}^n$. Elliptic or pseudo-elliptic transformations of a (extended) Kleinian group have necessarily finite orders. Let us note, from the definition, that a subgroup $\mathcal{K}$ of $\widehat{\mathcal{M}}^n$ is an extended Kleinian group if and only if $\mathcal{K}^+ = \mathcal{K} \cap \mathcal{M}^n$ is a Kleinian group.

Associated to an (extended) Kleinian group $\mathcal{F} < \mathcal{M}^n$ is a $(n+1)$-dimensional (orientable if it is Kleinian) hyperbolic orbifold $M_{\mathcal{F}} = \mathcal{H}^{n+1}/\mathcal{F}$. If, moreover, $\mathcal{F}$ is torsion free, then $M_{\mathcal{F}}$ is a $(n+1)$-dimensional hyperbolic manifold, which means that it carries a natural complete Riemannian metric of constant negative curvature inherited from the one of $\mathcal{H}^{n+1}$.

Assuming $\mathcal{F}$ to be a torsion free Kleinian group, so $\mathcal{M}_{\mathcal{F}}$ is an orientable hyperbolic manifold, by a *conformal automorphism* (respectively, *anti-conformal automorphism*) of $M_{\mathcal{F}}$ we means an orientation-preserving (respectively, orientation-reversing) self-isometry. We denote by $\mathrm{Aut}(M_{\mathcal{F}})$ the group of all conformal/anti-conformal automorphisms of $M_{\mathcal{F}}$.

A Kleinian group $\mathcal{F}$ is called *geometrically finite* if it has a finite-sided fundamental polyhedron in $\mathcal{H}^{n+1}$, in particular, it is finitely generated and the hyperbolic volume of $\mathrm{Hull}_\epsilon(\Lambda(\mathcal{F}))/\mathcal{F}$ is finite, where $\Lambda(\mathcal{F}) \subset \mathcal{S}^n$ stands for the limit set of $\mathcal{F}$ and $\mathrm{Hull}_\epsilon(\Lambda(\mathcal{F}))$ is the ϵ-neighborhood of the convex hull of $\Lambda(\mathcal{F})$ in $\mathcal{H}^{n+1}$. An extended Kleinian group is geometrically finite if its index two orientation-preserving half Kleinian group is so. Finite index extensions of geometrically finite groups are still geometrically finite. Another properties of geometrically finite groups can be found, for instance, in [1, 16].

2.3. **A finiteness property.** Let us consider an (extended) Kleinian group $\mathcal{K} < \mathcal{M}^n$. We will say that $\mathcal{K}$ is of *finite type* if it is finitely generated and it contains a finite number of conjugacy classes of elements of finite order.

Remark 2.1. If $n \in \{1, 2\}$ and $\mathcal{K}$ is finitely generated, then it is of finite type [4], but for $n \geq 3$, the finitely generated condition does not always ensure the finite type property [13], but it holds true if $\mathcal{K}$ is known to be geometrically finite.

So, if $\mathcal{K} < \mathcal{M}^n$ is of finite type, then we are able to find a collection of finite order elements $\{\kappa_1, \ldots, \kappa_r\} \subset \mathcal{K}$ so that the following holds:

(ecs1) each κ_i generates a maximal cyclic subgroup of $\mathcal{K}$;
(ecs2) the cyclic subgroups generated by $\kappa_1, \ldots, \kappa_r$ are pairwise non-conjugate in $\mathcal{K}$;

(ecs3) the collection is maximal with respect to the above two properties.

In the above, following the terminology used by Maclachlan in [15] for Fuchsian groups, we will say that the collection $\{\kappa_1, \dots, \kappa_r\}$ is an *elliptic complete system* (*e.c.s.* in short) and any of its elements is called a *canonical generating symmetry of* $\mathcal{K}$.

3. Quantitative aspects of the set of fixed points: Macbeath's formula

In this section, we let $\mathcal{K}$ be an (extended) Kleinian group of finite type, G a finite group and $\theta : \mathcal{K} \to G$ a surjective homomorphism with a torsion free (finitely generated) Kleinian group $\mathcal{F}$. Let us denote by $\pi : \mathcal{H}^{n+1} \to M_{\mathcal{F}}$ a universal covering with $\mathcal{F}$ as its group of deck transformations. The finite group $G =_\theta \mathcal{K}/\mathcal{F}$ is a subgroup of $\mathrm{Aut}(M_{\mathcal{F}})$. Next, we proceed to search for a Macbeath's formula that permits to count the number of connected components of fixed points of each non-trivial element $g \in G$.

If $\kappa \in \mathcal{K}$, $g = \theta(\kappa)$, $h \in \mathcal{H}^{n+1}$ and $x = \pi(h)$, then $g(x) = \pi(\kappa(h))$. We shall keep all these notations throughout the rest of this paper

Each finite order element $\kappa \in \mathcal{K}$ defines an automorphism $\theta(\kappa) \in G$ acting with fixed points (the set of fixed points of κ are sent by π to fixed points of $\theta(\kappa)$). The converse is clear as π is a local homeomorphism.

Lemma 3.1. *The sets of fixed points of two distinct non-trivial elements of $\mathcal{K}$ of finite orders inducing the same automorphisms of $M_{\mathcal{F}}$ are disjoint.*

Proof. Let κ, κ' be elements of finite order of $\mathcal{K}$ and let $\theta(\kappa) = \theta(\kappa')$. Let us assume they have non-disjoint connected components, say C and C', of their loci of fixed points. If $y \in C \cap C'$, then y is a fixed point of $\kappa^{-1}\kappa' \in \ker\theta = \mathcal{F}$. As $\mathcal{F}$ is torsion free and $\kappa^{-1}\kappa'$ has a fixed point, we must have that $\kappa^{-1}\kappa' = 1$. □

Since $\mathcal{K}$ is of finite type, we may find an e.c.s. $\{\kappa_1, \dots, \kappa_r\}$ for $\mathcal{K}$, which we assume, from now on, to be fixed. Let us denote by m_j the order of κ_j.

If $g \in G$ is a non-trivial element, say of order m, with fixed points, then property $(ecs3)$ ensures that $g = \theta(\kappa)$ for some elliptic element κ of $\mathcal{K}$ which is conjugated to a power of some canonical generating symmetry κ_j. Let $J(g)$ be the set of such $j \in \{1, \dots, r\}$ for which $g = \theta(\omega_j \kappa_j^{n_j} \omega_j^{-1})$ for some $\omega_j \in \mathcal{K}$ and some $n_j \in \{1, \dots, m_j - 1\}$. As $\ker\theta = \mathcal{F}$ is torsion free, we may see in the above equality that the order of g and that of $\kappa_j^{n_j}$ is the same, that is, $m = m_j/\gcd(m_j, n_j)$.

Remark 3.2. For $n = 1$, $\mathcal{K}$ is either a Fuchsian or an NEC group, so the set of fixed points of an elliptic element $\kappa \in \mathcal{K}$ consist in a single point and, as the only finite order orientation reversing isometries of the hyperbolic plane are reflections, the locus of fixed points in this case is a geodesic line. In particular, different elliptic elements of the same order have different sets of fixed points. Unfortunately, this is no longer true for symmetries of higher dimensional spaces and this is a one of the essential differences between Macbeath's formula for Riemann surfaces and our formula for hyperbolic manifolds of higher dimensions. For instance, Let $n \geq 4$ and take $A, B \in \mathrm{O}_n(\mathbb{R})$ generating a non-cyclic finite group $\mathcal{U}$. Assume that none of them has eigenvalue equal to 1 and so that they are non-conjugate in $\mathcal{U}$ (this can be done for $n \geq 4$). Let us consider the isometries of the hyperbolic $(n+1)$-space,

in this example modeled by the unit ball in $\mathbb{R}^{n+1}$, given by

$$T_A = \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}, \; T_B = \begin{bmatrix} B & 0 \\ 0 & 1 \end{bmatrix}.$$

Then, $\mathcal{K} = \langle T_A, T_B \rangle \cong \mathcal{U}$ is a finite extended Kleinian group, where T_A and T_B both share the same geodesic set of fixed points, but they are non-conjugated in $\mathcal{K}$.

As note in the above remark, although different canonical generating symmetries give rise to different connected components of their sets of fixed points, it is no longer true for their powers of the same order. In order to neutralize that deficiency while we count the number of connected components of $\mathrm{Fix}(g)$, for $g \in G - \{I\}$, we must define the following equivalence relation on $J(g)$:

$$j_1, j_2 \in J(g) : \; j_1 \sim j_2 \Leftrightarrow \mathrm{Fix}(\kappa_{j_1}^{n_{j_1}}) \cap \mathrm{Fix}(\kappa_{j_2}^{n_{j_2}}) \neq \emptyset.$$

The above relation is equivalent for the sets of fixed points of elliptic elements to be projected on the same subset of $M_{\mathcal{F}}$. Let $I(g)$ be a set of representatives for the quotient set $J(g)/\sim$.

Finally, as the set $\mathcal{C}$ of fixed point of an isometry of finite order $\kappa \in \mathcal{K}$ is a totally geodesic subspace of $\mathcal{H}^{n+1}$, its image $\ell = \pi(\mathcal{C})$ is a connected component of the set of fixed points of $\theta(\kappa)$; this being again a totally geodesic submanifold of $M_{\mathcal{F}}$. Let G_ℓ be the subgroup of G leaving ℓ set-wise invariant (the elements of G_ℓ permutes the points on ℓ and may or may not have fixed points on it).

We have now introduced all notations and facts needed to state and prove our main result concerning the number of connected components of the locus of fixed points of isometries in G.

Theorem 3.3 (Macbeath's formula for hyperbolic manifolds)**.** *Let $\mathcal{K}$ be an (extended) Kleinian group of finite type, G a finite abstract group and $\theta : \mathcal{K} \to G$ a surjective homomorphism whose kernel $\mathcal{F}$ is torsion free. Fix an elliptic complete system $\kappa_1, \ldots, \kappa_r$ for $\mathcal{K}$ and suppose that κ_i has order m_i. Let $g \in G$ be a non-trivial element of order m with non-empty set of fixed points. Then the number of connected components of the set of fixed points of g in the hyperbolic manifold $M_{\mathcal{F}}$ is*

$$|\mathcal{N}_G\langle g \rangle| \sum_{i \in I(g)} 1/n_i,$$

where $\mathcal{N}_G\langle g \rangle$ stands for the normalizer in G of the cyclic subgroup $\langle g \rangle$ and n_i is the order of the θ-image of the $\mathcal{K}$-normalizer of $\langle \kappa_i^{m_i/m} \rangle$.

Proof. Let π be a universal covering $\mathcal{H}^{n+1} \to M_{\mathcal{F}}$ induced by $\mathcal{F}$ and let $g \in G$ be non-trivial of order m acting with fixed points on $M_{\mathcal{F}}$. For each $j \in J(g)$ we also set $s_j := m_j/m = \gcd(m_j, n_j)$. Let $\kappa \in \mathcal{K}$ so that $\theta(\kappa) = g$. Then, for $h \in \mathcal{H}^{n+1}$, we have that $x = \pi(h)$ is a fixed point of g if and only if $\pi(h) = \pi(\kappa(h))$ and so if and only if $\gamma(h) = \kappa(h)$ for some $\gamma \in \mathcal{F}$. This means that $\gamma^{-1}\kappa \in \mathcal{K}$ has a fixed point and hence it is conjugate to a power of some element κ_i of *e.c.s.* and therefore $g = \theta(\omega \kappa_i^{\alpha s_i} \omega^{-1})$ for some α coprime with m and $\omega \in \mathcal{K}$. Clearly neither i, nor α and nor ω must be unique here. So given $i \in J(g)$ consider

$$N_i(g) = \{\omega \in \mathcal{K} : g = \theta(\omega \kappa_i^{t_i} \omega^{-1}) \text{ for some } t_i\}.$$

If we let $\mathcal{C}_i$ to be the totally geodesic subspace of the set of fixed points of $\kappa_i^{t_i}$ and if we denote by $\mathcal{K}_i$ its stabilizer in $\mathcal{K}$, which is the normalizer of $\langle \kappa_i^{s_i} \rangle$, then

$x \in \pi(\omega(\mathcal{C}_i))$. Conversely, given $\omega \in N_i(g)$, $\pi(\omega(\mathcal{C}_i)) \subseteq \mathrm{Fix}(g)$. It follows that

$$\mathrm{Fix}(g) = \bigcup_{i \in I(g)} \bigcup_{\omega \in N_i(g)} \pi(\omega(\mathcal{C}_i)).$$

Let us fix ω_i in $N_i(g)$. Then for any orther $\omega \in N_i(g)$, $\omega\mathcal{K}_i = \omega_i\mathcal{K}_i$ and so $N_i(g)$ is the left coset $\omega_i\mathcal{K}_i$. Furthermore $\omega \in N_i(g)$, gives $\theta(\omega_i^{-1}\omega) \in \mathcal{N}_G\langle g\rangle$ and so $\omega_i^{-1}\omega \in \theta^{-1}(\mathcal{N}_G\langle g\rangle)$ which in turn means that $N_i(g)$ is also left coset $\omega_i\,\theta^{-1}(\mathcal{N}_G\langle g\rangle)$. Now, $\ell_i = \pi(\omega(\mathcal{C}_i))$ is a one of the connected components of the set of fixed points of g and notice that $\theta(\omega\mathcal{K}_i\omega^{-1}) = G_{\ell_i}$. Given $\nu, \nu' \in \theta^{-1}(\mathcal{N}_G\langle g\rangle)$, we have the following chain of equivalences

$$\begin{array}{lcll}
\pi(\omega_i\nu(\mathcal{C}_i)) \cap \pi(\omega_i\nu'(\mathcal{C}_i)) \neq \emptyset & \Leftrightarrow & \pi(\omega_i\nu(\mathcal{C}_i)) = \pi(\omega_i\nu'(\mathcal{C}_i)) & \Leftrightarrow \\
\gamma\omega_i\nu(\mathcal{C}_i)) = \omega_i\nu'(\mathcal{C}_i), \text{ for some } \gamma \in \mathcal{F} & \Leftrightarrow & \gamma'\nu'^{-1}\nu(\mathcal{C}_i) = \mathcal{C}_i, \text{ for some } \gamma' \in \mathcal{F} & \Leftrightarrow \\
\theta(\nu'^{-1}\nu) \in G_{\ell_i} & \Leftrightarrow & \nu'^{-1}\nu \in \theta^{-1}(G_{\ell_i}) & \Leftrightarrow \\
\theta(\nu'^{-1})\theta(\nu) \in \theta(\omega\mathcal{K}_i\omega^{-1}). & & &
\end{array}$$

The first equivalence follows from Lemma 3.1, the third is a consequence of the normality of $\mathcal{F}$ in $\mathcal{K}$; the remainder are rather clear. Thus, each $i \in I(g)$ produces

$$[\theta^{-1}(\mathcal{N}_G\langle g\rangle) : \theta^{-1}(G_{\ell_i})] = \frac{|\mathcal{N}_G\langle g\rangle|}{|G_{\ell_i}|} = \frac{|\mathcal{N}_G\langle g\rangle|}{n_i}$$

connected components of the locus of fixed points of g. Finally, in order to get the desired formula, we need to prove that $\pi(\omega_i(\mathcal{C}_i)) \cap \pi(\omega_j(\mathcal{C}_j)) = \emptyset$, if $i, j \in I(g)$ with $i \neq j$. In fact, otherwise (by Lemma 3.1) if they intersect, then necessarily $\pi(\omega_i(\mathcal{C}_i)) = \pi(\omega_j(\mathcal{C}_j))$; so for arbitrary $c_i \in \mathcal{C}_i$ we have $\gamma\omega_i(c_i) = \omega_j(c_j)$ for some $c_j \in \mathcal{C}_j$ and some $\gamma \in \mathcal{F}$. Therefore $\omega_j^{-1}\gamma\omega_i(\mathcal{C}_i) = \mathcal{C}_j$. In other words, there is an element $\eta \in \mathcal{K}$ so that $\eta\kappa_i^{t_i}\eta^{-1}$ and $\kappa_j^{t_j}$ have the same set of fixed points, contradicting the definition of the set $I(g)$. □

It follows from the proof of the above Theorem the following upper bound.

Corollary 3.4. *Let $\mathcal{K}, \mathcal{F}, G, \theta, \pi$, κ_i and m_i be as in Theorem 3.3. Then the number of connected components of the set of fixed points of $g \in G$ does not exceed*

$$|\mathcal{N}_G\langle g\rangle| \sum_{j \in J(g)} 1/m_j.$$

Proof. Indeed $|I(g)| \leq |J(g)|$ and $m_i \leq n_i$. □

4. Comments concerning dimension two

Due to a better understanding and description of discrete cocompact groups of isometries of the hyperbolic plane $\mathcal{H}^2$, the formulas in Theorem 3.3 have a more explicit character. In fact, as the locus $\mathrm{Fix}(\kappa_i)$ of any canonical elliptic generator x_i of a Fuchsian group, is a single point p_i and $G_{\{p_i\}} = \langle x_i\rangle$, Theorem 3.3 reduces to Macbeath's counting formula in [14].

Corollary 4.1 (Macbeath's counting formula for Riemann surfaces [14])**.** *Let $\mathcal{K}$ be a finitely generated discrete group of orientation-preserving isometries of the hyperbolic plane $\mathcal{H}^2$ and let $x_1, \ldots, x_r$ be the a set of canonical elliptic generators of it of orders $m_1, \ldots, m_r$, respectively. Let G be a finite group and $\theta : \mathcal{K} \to G$ be a surjective homomorphism, whose kernel $\mathcal{F}$ is torsion free. We may consider the natural action of $G =_\theta \mathcal{K}/\mathcal{F}$, by orientation preserving automorphisms, of the*

Riemann surface $S = \mathcal{H}^2/\mathcal{F}$. Then the number of fixed points of $g \in G$ is given by the formula

$$|\mathcal{N}_G(\langle g\rangle)| \sum 1/m_i,$$

where $\mathcal{N}$ stands for the normalizer and the sum is taken over those i for which g is conjugate to a power of the image $\theta(x_i)$. In particular the number of fixed points of g is finite.

An anti-holomorphic automorphism of a compact Riemann surface of genus g, with fixed points, must be an involution; its locus of fixed points consist of $s \in \{1, \ldots, g+1\}$ disjoint sets, each of which is homeomorphic to a circle (ovals) by a well known result due to Harnack. A canonical elliptic generator c_i, of a NEC group, inducing an anti-holomorphic automorphisms (with fixed points) is a reflection, which is determined by its axis. In this way, we see that $G_\ell = \theta(C(\Lambda, c_i)))$ and therefore Theorem 3.3 reduces to the main result from [6].

Corollary 4.2. *Let $\mathcal{K}$ be an NEC-group, G be a finite group and let $\theta : \mathcal{K} \to G$ be a surjective homomorphism whose kernel is a torsion free cocompact Fuchsian group $\mathcal{F}$. Let us consider the action of G, under θ, on the compact Riemann surface $S = \mathcal{H}^2/\mathcal{F}$ as a group of conformal and anticonformal automorphisms. Then a symmetry σ with fixed points is conjugate to $\theta(c)$ for some canonical reflection c of $\mathcal{K}$ and it has*

$$\sum [\, C(G, \theta(c_i)) : \theta(C(\mathcal{K}, c_i))\,]$$

ovals, where C stands for thre centralizer, c_i run over nonconjugate canonical reflections of $\mathcal{K}$, whose images under θ belongs to the orbit of σ in G.

Remark 4.3. An algebraic structure of the centralizers of reflections in an NEC-group was found by Singerman in [20]. There is a simple method, based on the geometry of the hyperbolic plane, to find explicit formulas for them as described in [8]. Similarly, effective formulas are also known for periodic self-homeomorphisms of non-orientable or bordered compact surfaces [5, 7].

5. A couple of examples in hyperbolic 3-dimensional case

We shall give two examples of 3-dimensional hyperbolic manifolds, to see how our formula works in practice.

Example 5.1 (Generalized Fermat 3-manifolds)**.** Let $m, k \geq 3$ be integers. A *generalized Fermat manifold of type* (m, k) is a compact hyperbolic 3-manifold N admitting a group $H \cong \mathbb{Z}_m^k$ of isometries so that the hyperbolic orbifold M/G is homeomorphic (as orbifolds) to the orbifold $\mathcal{O}$ whose underlying space is the unit 3-dimensional sphere $\mathcal{S}^3$ and the conical locus is given by k disjoint loops (each one of index m) as shown in Figure 1 (for the case $k = 10$). In this case, the group H is called a *generalized Fermat group of type* (m, k) and the pair (N, H) a *generalized Fermat pair of type* (m, k). By Mostow's rigidity theorem, up to isometry, there is only one generalized Fermat pair of type (m, k). As the 3-orbifold $\mathcal{O}$ is closed, Haken and homotopically atoroidal, it has a hyperbolic structure [2, 9], that is, there is Kleinian group $\mathcal{K}$ for which $\mathcal{O} = \mathcal{H}^3/\mathcal{K}$ (see Figure 2). We have that $\mathcal{K}$ is generated by $x_1, \ldots, x_k$ subject to the relations:

$$x_1^m = \ldots = x_k^m = 1, x_i x_{i+1}^{-1} x_i^{-1} x_{i+1} = x_{i+1} x_{i+2}^{-1} x_{i+1}^{-1} x_{i+2},$$

where i are taken modulo k. The collection $x_1, \ldots, x_k$ is a elliptic complete system of $\mathcal{K}$ and the derived subgroup $\mathcal{K}'$ of $\mathcal{K}$ is torsion free [11]. So $M = \mathcal{H}^3/\mathcal{K}'$ is a closed hyperbolic 3-manifold with abelian group $G = \mathcal{K}/\mathcal{K}' \cong \mathbb{Z}_m^k$ of automorphisms. Let us now consider the canonical projection $\theta : \mathcal{K} \to G$ and set $a_i = \theta(x_i)$. By Theorem 3.3, the number of connected components of fixed points of each a_i is exactly m^{k-1}. In fact, in this example we have that $\mathcal{N}_G\langle a_i\rangle = G$, so $|\mathcal{N}_G\langle a_i\rangle| = m^k$, and $\mathcal{N}_{\mathcal{K}}\langle x_i\rangle = \langle x_i\rangle$.

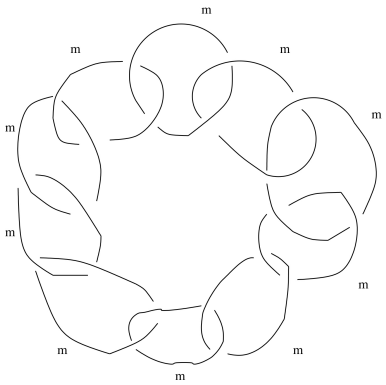

Figure 1. $k = 10$

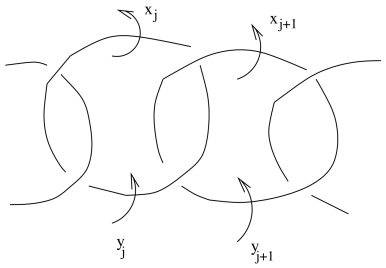

Figure 2. $\mathcal{O} = \mathcal{H}^3/\mathcal{K}$

Example 5.2 (Extended Schottky groups)**.** An *extended Schottky group of rank g* is an extended Kleinian group whose canonical subgroup of orientation preserving isometries is a Schottky group of rank g [10]. An example, of rank $g = 5$, is as follows. Choose three pairwise disjoint circles on the complex plane, all of them bounding a common 3-connected region. For each of these circles, we take either a reflection or an imaginary reflection that permutes both discs bounded by such a circle. Let us denote these transformations by κ_1, κ_2 and κ_3, and let $\mathcal{K}$ be the group generated by them. It happens that $\mathcal{K}$ is an extended Kleinian group isomorphic to the free product of three copies of $\mathbb{Z}_2$, $\mathcal{N}_{\mathcal{K}}\langle\kappa_i\rangle = \langle\kappa_i\rangle$ and $\{\kappa_1, \kappa_2, \kappa_3\}$ is a elliptic complete system of it. If we consider the surjective homomorphism $\theta : \mathcal{K} \to G = \mathbb{Z}_2^3 = \langle a_1, a_2, a_3\rangle$, defined by $\theta(\kappa_i) = a_i$, for $i = 1, 2, 3$, then its kernel

$$\mathcal{F} = \ker\theta = \langle\langle(\kappa_2\kappa_1)^2, (\kappa_2\kappa_3)^2, (\kappa_1\kappa_3)^2\rangle\rangle,$$

were the last stands for the normal closure, is a Schottky group of rank 5. So $M = \mathcal{H}^3/\mathcal{F}$ is homeomorphic to the interior of a handlebody of genus 5 admitting three symmetries a_1, a_2 and a_3, each one of order two. Since G is abelian, we have that $|\mathcal{N}_G\langle a_i\rangle| = 8$ and $|\theta(\mathcal{N}_{\mathcal{K}}\langle\kappa_i\rangle| = |\langle a_i\rangle| = 2$. It follows from the counting formula of Theorem 3.3 that each a_i has exactly 4 connected components of its set of fixed points; all of them being either isolated points or discs.

References

[1] B. Apanasov. *Conformal Geometry of Discrete Groups and Manifolds*. De Gruyter Expositions in Mathematics **32**. Berlin; New York, 2000.

[2] M. Boileau, S. Maillot, J. Porti. *Three-dimensional orbifolds and their geometric structures*. Panoramas et Synthèses, **15**, 2003, Société Mathématique de France.

[3] J. F. Brock and K. W. Bromberg. On the density of geometrically finite Kleinian groups. *Acta Math.* **192** (2004), 33–93.
[4] M. Feighn and G. Mess. Conjugacy classes of finite subgroups in Kleinian groups. *Amer. J. of Math.* **113** (1991), 179–188.
[5] J.M. Gamboa, G. Gromadzki. On the set of fixed points of automorphisms of bordered Klein surfaces. *Revista Mathematica Iberoamericana* **28** No. 1 (2012), 113–126.
[6] G. Gromadzki. On a Harnack-Natanzon theorem for the family of real forms of Riemann surfaces. *Journal Pure Appl. Algebra* **121** (1997) 253–269.
[7] G. Gromadzki. On fixed points of automorphisms of non-orientable unbordered Klein surfaces. *Publ. Mat.* **53** No. 1 (2009) 73–82.
[8] G. Gromadzki. Symmetries of Riemann surfaces from a combinatorial point of view. *London Mathematical Society Lecture Note Series*, Cambridge University Press **287** (2001), 91–112.
[9] H. Helling, A. C. Kim, J. L. Mennicke. Some honey-combs in hyperbolic 3-space. *Comm. Algebra* **23** No. 14 (1995), 5169–5206.
[10] R. A. Hidalgo and B. Maskit. On Klein-Schottky groups. *Pacific J. of Math.* (2) **220** (2005), 313–328.
[11] R. A. Hidalgo and A. Mednykh. Geometric orbifolds with torsion free derived subgroup. *Siberian Mathematical Journal* **51** No. 1 (2010) 38–47.
[12] M. Izquierdo, D. Singerman. On the fixed-point set of automorphisms of non-orientable surfaces without boundary. *Geom. Topol. Monogr.* **1** (1998) 295–301.
[13] M. Kapovich and L. Potyagailo. On absence of Ahlfors' and Sullivan's finiteness theorems for Kleinian groups in higher dimensions. *Siberian Math. Journ.* **32** (1991), 227–237.
[14] A.M. Macbeath. Action of automorphisms of a compact Riemann surface on the first homology group. *Bull. London Math. Soc.* **5** (1973) 103–108.
[15] C. Maclachlan. Maximal normal Fuchsian groups. *Illinois J. Math.* **15** (1971) 104–113.
[16] B. Maskit. *Kleinian Groups*, GMW, Springer–Verlag, 1987.
[17] K. Matsuzaki, M. Taniguchi. *Hyperbolic Manifolds and Kleinina Groups*. Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1998.
[18] H. Namazi and J. Souto. Non-realizability, ending laminations and the density conjecture. https://web.archive.org/web/20090715232851/http://www-personal.umich.edu/ jsouto/papers.html
[19] K. Ohshika. Realising end invariants by limits of minimally parabolic, geometrically finite groups. *Geometry and Topology* **15** (2) (2011), 827–890.
[20] D Singerman. On the structure of non-euclidean crystallographic groups. *Proc.Camb.Phil.Soc.* **76** (1974), 233–240.

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 24–31
ISSN: 1930-1235; (**2018**)

A NEGATIVE ANSWER TO A QUESTION OF ASCHBACHER

ROBERT A. WILSON

*School of Mathematical Sciences, Queen Mary University of London, Mile End Road, London E*1 4*NS, U.K.*

Dedicated to the memory of Kay Magaard

Abstract. We give infinitely many examples to show that, even for simple groups G, it is possible for the lattice of overgroups of a subgroup H to be the Boolean lattice of rank 2, in such a way that the two maximal overgroups of H are conjugate in G. This answers negatively a question posed by Aschbacher.

MSC 2010: Primary: 20E32, 20E34; Secondary: 20D05, 20D06
Keywords: Simple groups, maximal subgroups

1. The question

In a recent survey article on the subgroup structure of finite groups [1], in the context of discussing open problems on the possible structures of subgroup lattices of finite groups, Aschbacher poses the following specific question. Let G be a finite group, H a subgroup of G, and suppose that H is contained in exactly two maximal subgroups M_1 and M_2 of G, and that H is maximal in both M_1 and M_2. Does it follow that M_1 and M_2 are not conjugate in G? This is Question 8.1 in [1]. For G a general group, he asserts there is a counterexample, not given in [1], so he restricts this question to the case G almost simple, that is $S \leq G \leq \mathrm{Aut}(S)$ for some simple group S. This is Question 8.2 in [1].

2. The answer

In fact, the answer is no, even for simple groups G. Two or three examples can be read off from the Atlas of Finite Groups [4], if one knows where to look. For convenience, let us call a group G an *A-group* if the question has an affirmative answer for G, and a *non-A-group* otherwise. The smallest example of a non-A-group seems to be the simple Mathieu group M_{12} of order 95040.

E-mail address: r.a.wilson@qmul.ac.uk.

Theorem 1. *Let $G = \mathrm{M}_{12}$, and $H \cong A_5$ acting transitively on the 12 points permuted by M_{12}. Then H lies in exactly two other subgroups of G, both lying in the single conjugacy class of maximal subgroups $L_2(11)$.*

Proof. The maximal subgroups of G are well-known, and are listed in the Atlas of Finite Groups [4, p. 33]. From this list it follows that the only maximal subgroups of G that contain H are conjugates of the transitive subgroup $M \cong L_2(11)$. The maximal subgroups of $\mathrm{Aut}(G) \cong \mathrm{M}_{12}{:}2$ are determined in [9], where it is shown in particular that the normalizers in $\mathrm{Aut}(G)$ of H and M are $\mathrm{Aut}(H) \cong S_5$ and $\mathrm{Aut}(M) \cong PGL_2(11)$ respectively. Since $PGL_2(11)$ does not contain S_5, it follows that there are precisely two conjugates of M that contain H, and that these conjugates are interchanged by elements of $\mathrm{Aut}(H) \setminus H$. □

Of course, one example answers the specific question, but does not address the context in which the question was asked. One needs to consider rather how many examples there are, or whether the phenomenon just exhibited is relatively common or rare. The problem considered in [9] was to what extent the maximal subgroups of an automorphism group $\mathrm{Aut}(S)$ of a simple group S can be deduced from those of the simple group itself. The biggest obstruction to such a reduction turns out to be the existence of what were called *type 2 novelties*, that is maximal subgroups of $\mathrm{Aut}(S)$ whose intersection with S, say H, lies in exactly one conjugacy class of maximal subgroup of S.

In fact, type 2 novelties are a good source of examples of non-A-groups, although the maximality of H in M_i is an extra condition that needs to be checked separately. Indeed, the results of [9] can be used to deduce the existence of one more example, that is in the sporadic simple group of Held. The relevant subgroup information, obtained in [3, 9], is summarised in [4, p. 104].

Theorem 2. *Let $G = \mathrm{He}$ and $H \cong (A_5 \times A_5).2.2$. Then H is contained in just two other subgroups of G, both lying in the single class of maximal subgroups isomorphic to $S_4(4){:}2$.*

Proof. It is shown in [3] (see also [9]) that there is a unique class of $A_5 \times A_5$ in the Held group, and that the normalizer of any $A_5 \times A_5$ in G is a group H of shape $(A_5 \times A_5).2^2$, in which there is no normal A_5. It follows that H lies inside a maximal subgroup $M \cong S_4(4){:}2$. Now in $\mathrm{Aut}(G)$ the normalizers of H and M are $S_5 \wr 2$ and $S_4(4){:}4$ respectively. But $S_4(4){:}4$ does not contain $S_5 \wr 2$, so the elements of $\mathrm{Aut}(H) \setminus H$ interchange two G-conjugates of M that contain H. □

The above examples constitute the extent of general knowledge at the time of the publication of the Atlas.

3. Doubly-deleted doubly-transitive permutation representations

Both the examples given so far occur in sporadic groups G. There is also at least one example in which H is sporadic, but G is a classical simple group.

Theorem 3. *Let $G = \Omega^-_{10}(2)$ and $H \cong \mathrm{M}_{12}$. Then H is contained in exactly two other subgroups of G, both lying in the single conjugacy class of subgroups isomorphic to A_{12}.*

Proof. In this case there is a crucial error in [4, p. 147] and one needs to use the corrected list of maximal subgroups of G from [6] or [2]. Note in particular that

$\mathrm{Aut}(G) \cong \Omega_{10}^-(2)$:2 contains maximal subgroups S_{12} and $\mathrm{Aut}(\mathrm{M}_{12}) \cong \mathrm{M}_{12}$:2. Since S_{12} does not contain M_{12}:2, we have essentially the same situation as in the two previous examples. The only maximal subgroups of G that contain H are conjugates of $M \cong A_{12}$, and there are exactly two such conjugates, swapped by elements of $\mathrm{Aut}(H) \setminus H$. □

Analysing this example, it is clear that an important property of M_{12} that is being used here is that it has two distinct 2-transitive representations on 12 points, swapped by the outer automorphism. The smallest simple group with such a property is $L_3(2)$, which has two distinct 2-transitive representations on 7 points. In characteristic 7, therefore, there is a doubly-deleted permutation representation, giving rise to an embedding in $\Omega_5(7)$.

Theorem 4. *Let $G = \Omega_5(7)$ and $H \cong L_3(2) \cong L_2(7)$ be a subgroup of G, acting irreducibly on the 5-dimensional module. Then H is contained in exactly two other subgroups of G, both isomorphic to A_7, and lying in the same G-conjugacy class.*

Proof. Reading off the information about irreducible subgroups of $\Omega_5(7)$ and $SO_5(7)$ from [2, Table 8.23], we see that $G = \Omega_5(7)$ has a single class of irreducible subgroups $H = L_3(2)$, and these subgroups are contained in maximal subgroups $M = A_7$. Correspondingly, in $SO_5(7)$ there are maximal subgroups $L_3(2)$:2 and S_7. The outer automorphism of $L_3(2)$ therefore swaps two (G-conjugate) copies of A_7 containing $L_3(2)$. □

More generally, for all $n \geq 3$ and all prime powers q, the simple group $L_n(q)$ has two inequivalent 2-transitive permutation representations on $d := (q^n - 1)/(q - 1)$ points. Not all of these give rise to examples of non-A-groups, however. The case $L_3(3) < A_{13} < \Omega_{11}(13)$ can be analysed using the classification of maximal subgroups of orthogonal groups in 11 dimensions in [2], where we find that $\Omega_{11}(13)$ contains two classes of $L_3(3)$:2, so that $L_3(3)$ embeds in both A_{13} and $L_3(3)$:2. Similarly, the cases $L_4(2) < A_{15} < \Omega_{13}(\ell)$ for $\ell = 3, 5$ are described in [7]. There is one class of A_8, and two classes of S_{15}, in $\Omega_{13}(3)$, so A_8 is not second maximal in this case. There is one class of A_{15}, and two classes of S_8, in $\Omega_{13}(5)$, so A_8 is contained in three maximal subgroups in this case.

4. Infinite series of examples

If p is a prime bigger than 7, then there is an embedding $L_3(2) < A_7 < \Omega_6^\varepsilon(p)$, where $\varepsilon = +$ just when p is a quadratic residue modulo 7. For simplicity, restrict to the case $\varepsilon = +$. We read off the following properties from [2, Table 8.9]. The number of classes of A_7 is at least 2, and is exactly 2 when $p \equiv 3 \bmod 4$. The same is true for $L_3(2)$. In this case, the centre of $\Omega_6^+(p)$ is trivial, and the outer automorphism group has order 4, consisting of a diagonal automorphism δ, a graph automorphism γ, and their product $\delta\gamma$. Now A_7 is normalized by γ in all cases, while $L_3(2)$ is normalized by γ provided $p \equiv \pm 1 \bmod 8$, and by $\delta\gamma$ otherwise. Thus we must restrict to the case $p \equiv 7 \bmod 8$, and $p \equiv 1, 2, 4 \bmod 7$, that is $p \equiv 15, 23, 39 \bmod 56$. In these cases, the group $\Omega_6^+(p).\langle\gamma\rangle = SO_6^+(p)$ contains two classes of S_7, and two classes of $L_3(2)$:2. The automorphism δ swaps the two classes of S_7, and swaps the two classes of $L_3(2)$:2.

Theorem 5. *Let p be a prime, and suppose that $p \equiv 15, 23, 39 \bmod 56$. Let G be the simple group $\Omega_6^+(p) \cong PSL_4(p)$. Then G contains subgroups $L_3(2) < A_7$,*

both normalized by the tranpose-inverse automorphism of $L_4(p)$, to $L_3(2)$:2 and S_7 respectively. In particular, every such $L_3(2)$ lies in exactly two copies of A_7, and these two copies of A_7 are G-conjugate.

Proof. Consider a pair of subgroups $L_3(2) < A_7$ of G, and adjoin $\alpha\gamma$, where α is an inner automorphism of $\Omega_6^+(p)$, to extend A_7 to S_7. This swaps the two classes of $L_3(2)$ in A_7. But we can also adjoin $\beta\gamma$, where β is another inner automorphism, to normalize $L_3(2)$ to $L_3(2)$:2. Hence there is an inner automorphism of the form $\alpha\gamma\beta\gamma$, that conjugates an $L_3(2)$ of one class in A_7, to an $L_3(2)$ of the other class. The same argument with the roles of $L_3(2)$ and A_7 reversed shows that the two copies of A_7 in which $L_3(2)$ lies are conjugate in $\Omega_6^+(p)$. □

As a consequence, we have an infinite series of groups $PSL_4(p)$, for p any prime with $p \equiv 15, 23, 39 \bmod 56$, for which Aschbacher's question has a negative answer. There is a similar infinite series of groups $PSU_4(p)$, for $p \equiv 1 \bmod 8$ and $p \equiv 3, 5, 6 \bmod 7$, that is $p \equiv 17, 33, 41 \bmod 56$. This can be read off in a similar way from [2, Table 8.11].

Theorem 6. *Let p be a prime, and suppose that $p \equiv 17, 33, 41 \bmod 56$. Let G be the simple groups $\Omega_6^-(p) \cong PSU_4(p)$. Then G contains subgroups $L_3(2) < A_7$, both normalized by the field automorphism of $U_4(p)$, to $L_3(2)$:2 and S_7 respectively. In particular, every such $L_3(2)$ lies in exactly two copies of A_7, and these two copies of A_7 are conjugate in G.*

These last two results are essentially contained in [2, Proposition 4.8.4], where the fact that type 2 novelties arise in these cases is proved. The maximality of H in M_i is a triviality. The authors of [2] remark that type 2 novelties also arise for other values of p, but the conditions on p cannot be expressed as simple congruence conditions. There is an analogous embedding $L_2(11) < A_{11}$, which one might think gives similar series of examples in $\Omega_{10}^\varepsilon(p)$ for certain p. However, $L_2(11)$ is not maximal in A_{11}, so this fails.

5. More special examples

As we have just seen, the embedding $L_3(2) < A_7$ behaves differently in characteristic 7 (the *special* case) from other characteristics (the *generic* case). More generally, the embedding $L_n(q) < A_d$, where $d = (q^n - 1)/(q - 1)$, behaves differently in the special case (characteristic dividing d), compared to the generic case (characteristic prime to d).

The special case is easiest to analyse when d is itself prime. In this case, n is necessarily prime, but q need not be prime. This includes all Mersenne primes except 3, and others such as $(3^3 - 1)/(3 - 1) = 13$ and $(5^3 - 1)/(5 - 1) = 31$, for example. We then have embeddings $L_n(q) < A_d < \Omega_{d-2}(d)$. The Singer cycles in $L_n(q)$ are represented as d-cycles in A_d, and as regular unipotent elements in $\Omega_{d-2}(d)$. Now there is a unique class of regular unipotent elements in $SO_m(d)$ for all odd m, and these elements have order d provided $m \leq d$. The class splits into two classes in $\Omega_m(d)$, and these classes are rational if $m \equiv \pm 1 \bmod 8$, and irrational otherwise.

Since d is prime, the d-cycles in S_d split into two irrational classes in A_d (by Sylow's Theorem). The d-cycles are conjugate in A_d to their inverses just when $d \equiv 1 \pmod 4$. Since the regular unipotent elements have unipotent centralizer,

it follows that they are conjugate in $\Omega_{d-2}(d)$ to their inverses if and only if either $d \equiv 1 \bmod 4$ or $d-2 \equiv \pm 1 \bmod 8$, that is $d \equiv 1, 3, 5 \bmod 8$. Now the Singer cycles in $L_n(q)$ are inverted by the transpose-inverse automorphism, and we want this automorphism to be realised by an element of $SO_{d-2}(d) \setminus \Omega_{d-2}(d)$. This happens if and only if $d \equiv 7 \bmod 8$.

Theorem 7. *If q is a prime power, and $d := (q^n-1)/(q-1)$ is prime, with $d \equiv 7 \bmod 8$, let $H = P\Gamma L_n(q)$, $M = A_d$ and $G = \Omega_{d-2}(d)$. Then $H < M < G$, and H and M are unique up to conjugacy in G. Hence H and M extend to $H.2$ and $M.2$ in $G.2$, and H is contained in exactly two G-conjugates of M.*

The condition $d \equiv 7 \bmod 8$ is satisfied by all Mersenne primes (the case $q = 2$), except 3, but not by all primes of the form $(q^n-1)/(q-1)$. The condition can be re-written as a condition on the values of q and n modulo 8.

Lemma 1. *If $d = (q^n-1)/(q-1)$, then the condition $d \cong 7 \bmod 8$ is equivalent to the condition that, either*

- *$q = 2$ and $n > 2$, or*
- *$q \equiv 1 \bmod 8$ and $n \equiv 7 \bmod 8$, or*
- *$q \equiv 5 \bmod 8$ and $n \equiv 3 \bmod 8$.*

Only finitely many primes d of the form $(q^n-1)/(q-1)$ are known, but it is conjectured that there are infinitely many, including infinitely many Mersenne primes 2^n-1. Currently just 50 Mersenne primes are known, giving rise to examples with H isomorphic to $L_3(2)$, $L_5(2)$, $L_7(2)$, $L_{13}(2)$, ..., $L_{77232917}(2)$. Less effort has been expended on finding primes for larger values of q, but examples for $q = 5$ and $n \equiv 3 \bmod 8$ occur when $n = 3$, 11, 3407, 16519, 201359 and 1888279 (see A004061 in the On-line Encyclopedia of Integer Sequences [8]). I could find no examples with $q = 9$ or $q = 13$, but using GAP [5], one can easily find the examples $n = 7$, 47 and 71 for $q = 17$ and $n \equiv 7 \bmod 8$.

One can also search for examples by fixing n rather than q. For $n = 3$, examples with $q \equiv 5 \bmod 8$ and d prime include $q = 5, 101, 173, 293, 677, 701, 773$. A search with $n = 7$ turns up the examples $q = 17, 73, 89, 353, 1297, 1409, 1489, 1609, 1753, 2609, 2753, 3673, 4049, 4409$, etc., and similarly for $n = 11$, we can take $q = 53, 229, 389, 709, 1213, 2029, 5581, 5669, 5813, 5861, 7229$. For $n = 19$, there are examples for $q = 181, 277, 389, 509, 797, 1693, 1709$, etc. For $n = 23$, $q = 113$, 257, 857, 1801; for $n = 31$, $q = 241$, and so on.

In particular, examples of negative answers to Aschbacher's question arise in the cases of $L_3(5)$, $L_3(101)$, $L_{11}(5)$, $L_7(17)$, and $L_7(73)$. An extremely large example arises from the embedding of $L_{77232917}(2)$ in A_d and $\Omega_{d-2}(d)$, where $d = 2^{77232917}-1$ is the largest currently known Mersenne prime.

6. More generic examples

As we have seen, for all $n \geq 3$ and for all q, the simple groups $L_n(q)$ have two inequivalent permutation representations on $d := (q^n-1)/(q-1)$ points, and hence we obtain two inequivalent embeddings in A_d. In the generic case, when ℓ is a prime not dividing d, the alternating group A_d embeds irreducibly into $\Omega_{d-1}(\ell)$. However, the conditions on n, q, ℓ for this to give rise to a negative answer to Aschbacher's question, are subtle and complicated, as we already saw for the smallest case, $n = 3, q = 2$.

The next smallest case is $n = 3, q = 3$. To analyse this case, that is, the embedding $L_3(3) < A_{13} < P\Omega^{\pm}_{12}(p)$, we may use the information on maximal subgroups of $\Omega^{\pm}_{12}(p)$ provided in [2, Tables 8.83 and 8.85]. It follows from these tables that there are no examples here.

The next smallest case is $n = 4, q = 2$, and the embedding of $L_4(2) \cong A_8$ into A_{15} and thence into orthogonal groups in dimensions 13 and 14. The maximal subgroups of these orthogonal groups have been determined by Anna Schroeder, in her St Andrews PhD thesis [7]. In particular, the embeddings into $\Omega_{13}(3)$ and $\Omega_{13}(5)$ do not give examples.

In the dimension 14 case, however, it seems that there is a small but crucial error at exactly the point that interests us here: maximal subgroups S_8 are eliminated from the lists of maximal subgroups of $P\Omega^{\pm}_{14}(p)$ by the assertion, contained in the proof of [7, Propn. 6.4.17(iv)], that $S_8 \leq S_{15}$, which is manifestly false for this embedding. Indeed, Propositions 6.4.4 and 6.4.5 in [7] give the true picture, and show that S_8 is indeed a maximal subgroup of $SO^{\varepsilon}_{14}(p)$ for suitable congruences of ε and p. In the cases when the outer automorphism group of $\Omega^{\varepsilon}_{14}(p)$ is just 2^2, the calculations are quite straightforward. These are the cases when $\varepsilon p \equiv 3 \bmod 4$.

Theorem 8. *Let $p \equiv 19, 23, 31, 47 \bmod 60$, and let $G = \Omega^{+}_{14}(p)$. Let $H \cong A_8$ be a subgroup of G acting irreducibly in the 14-dimensional representation. Then H is contained in exactly two maximal subgroups of G, both isomorphic to A_{15}, and conjugate to each other in G.*

Proof. Indeed, it is shown in [7] that for $p \equiv 19, 23, 31, 47 \bmod 60$, there are two conjugacy classes of subgroups S_{15}, maximal in $SO^{+}_{14}(p)$, and swapped by the diagonal automorphism δ. Moreover, it is shown that the intersection of S_{15} with $\Omega^{+}_{14}(p)$ is A_{15}. Now the same argument applies to the group S_8, acting irreducibly in the 14-dimensional representation. Since for this embedding, S_8 does not lie in S_{15}, it follows that S_8 is maximal in $SO^{+}_{14}(p)$ in these cases. □

Exactly the same argument applies to the cases $p \equiv 13, 29, 37, 41 \bmod 60$ in $\Omega^{-}_{14}(p)$. It is possible that analogous examples also exist when $\varepsilon p \equiv 1 \bmod 4$, but in this case the outer automorphism group is D_8, and there are four classes each of S_8 and S_{15}, so the situation is more complicated.

7. Unbounded rank

From what we have done so far, if there are infinitely many Mersenne primes, then there are examples of non-A-groups of arbitrarily large Lie rank. However, in this section we shall show that this condition can be removed, by considering the generic rather than the special case.

Note first that, for n even, the representations of $L_n(2)$ of dimension $d-1$, where $d = 2^n - 1$, extend to emebeddings of $L_n(2)$:2 in $SO_d(p)$ for all p, while for n odd this happens only when the field of order p contains square roots of 2, that is, when $p \equiv \pm 1 \bmod 8$. Hence, for example, the embeddings $L_5(2) < A_{31} < \Omega^{\varepsilon}_{30}(p)$ provide examples of non-A-groups whenever all of the following conditions are satisfied:

- $\varepsilon p \equiv 3 \bmod 4$,
- $p \equiv \pm 1 \bmod 8$, and
- $p \equiv 1, 2, 4, 8, 16 \bmod 31$.

That is to say, for $\varepsilon = +$ we require $p \equiv 39, 47, 63, 95, 159 \bmod 248$, while for $\varepsilon = -$ we require $p \equiv 1, 33, 97, 225, 233 \bmod 248$.

For the purpose of demonstrating that examples of non-A-groups exist of arbitrarily large rank, and of arbitrarily large characteristic within a given rank, it is sufficient to consider any infinite subset of such primes. For simplicity, we restrict to the case when $\varepsilon = -$, and further to the case when $p \equiv 1 \bmod 4(d-1)$. In this case, the embedding of $L_n(2)$ into A_d and thence into $\Omega^-_{d-1}(p)$ gives an example of a negative answer to Aschbacher's question. Of course, there are many other examples.

Theorem 9. *Let p be a prime, and $\varepsilon = \pm$, such that $\varepsilon p \equiv 3 \bmod 4$. Let $n \geq 3$, and suppose that p is a square modulo $d := 2^n - 1$. If n is odd, suppose also that $p \equiv \pm 1 \bmod 8$. Let $G = \Omega^\varepsilon_{d-1}(p)$, and $H \cong L_n(2)$ a subgroup of G. Then H is contained in exactly two maximal subgroups of G, which are isomorphic to A_d and conjugate to each other.*

Proof. The above conditions ensure that G has outer automorphism group of order 4, and that both $L_n(2)$:2 and S_d embed in $SO^\varepsilon_{d-1}(p)$ but not in $\Omega^\varepsilon_{d-1}(p)$. Hence we have the same configuration as in all the other examples above. □

We have now shown that there is no bound on the Lie rank of non-A-groups. In these examples, there are two conjugacy classes of $L_n(2)$ in $\Omega^\varepsilon_{d-1}(p)$, and two conjugacy classes of A_d, interchanged by the diagonal automorphism. If instead $\varepsilon p \equiv 1 \bmod 4$, then there are four classes of each, and the outer automorphism group of $\Omega^\varepsilon_{d-1}(p)$ is D_8. In [2], two of the reflections in D_8 are described as graph automorphisms γ, and the other two as $\delta\gamma$, but unfortunately the two conjugates of γ are not distinguished from each other. For any particular choice of γ, two of the four classes of A_d extend to S_d, and the other two classes are interchanged.

8. Other classical groups

So far, all our examples with G a classical group have occurred when G is in fact orthogonal. There is no bound on the characteristic, and there is no bound on the rank. All three families of orthogonal groups (plus type, minus type, and odd dimension) occur. It would be interesting to know if the other classical groups, linear, unitary or symplectic, can occur.

Of course, the isomorphisms $L_4(p) \cong \Omega^+_6(p)$ and $U_4(p) \cong \Omega^-(p)$ imply the existence of examples in linear and unitary groups, but do examples exist in linear and unitary groups of larger dimension? So far, I have not found any examples. The large outer automorphism groups in these cases make the analysis very delicate. There are potential examples of the form $L_3(4) < U_4(3) < L_6(p)$, but there are three classes of each of $L_3(4)$ and $U_4(3)$, and the embeddings between them are not given explicitly in [2]. Hence one needs extra detailed information to resolve these cases. It seems likely, however, that this configuration does not give any examples.

In the case of symplectic groups, over fields of odd prime order, the outer automorphism group has order 2, which is the ideal situation for us. If one looks through the tables of maximal subgroups of symplectic groups in dimensions up to 12 given in [2], one finds, besides the case $L_3(2) < A_7 < S_4(7)$ already discussed, just one series of potential examples, given by the embeddings $A_5 < L_2(p) < S_6(p)$ for p a prime, $p \equiv \pm 11, \pm 19 \bmod 40$. However, in this case the embedding of $2\dot{\mathrm{A}}_5$ in $Sp_6(p)$ also goes via the tensor product $Sp_2(p) \circ GO_3(p)$, so this A_5 lies in more than two maximal subgroups of $Sp_6(p)$.

On the other hand, Anna Schroeder's PhD thesis [7] contains the lists of maximal subgroups of $S_{14}(q)$ and their automorphism groups. There one finds two more potential infinite series of examples, given by the embeddings $J_2 < S_6(p) < S_{14}(p)$ and $L_2(13) < S_6(p) < S_{14}(p)$ for suitable primes p. The relevant congruences are $p \equiv \pm 11, \pm 19 \bmod 40$ for J_2, and $p \equiv \pm 3, \pm 27, \pm 29, \pm 35, \pm 43, \pm 51 \bmod 104$ for $L_2(13)$. It is straightforward to check, in the same way as before, that these do indeed give examples of negative answers to Aschbacher's question.

Theorem 10. *Let $p \equiv \pm 11, \pm 19 \bmod 40$, and let $G = S_{14}(p)$. Let $H \cong \mathrm{J}_2$ be a subgroup of G. Then H is contained in exactly two maximal subgroups of G, both isomorphic to $S_6(p)$, and conjugate to each other in G.*

Theorem 11. *Let $p \equiv \pm 3, \pm 27, \pm 29, \pm 35, \pm 43, \pm 51 \bmod 104$, and let $G = S_{14}(p)$. Let $H \cong L_2(13)$ be a subgroup of G contained in $M \cong S_6(p)$. Then H is contained in exactly two maximal subgroups of G, both conjugate to M.*

9. Further remarks

Far-reaching as the above examples are, they have little, if any, impact on Aschbacher's programme. This is because they all occur in sporadic or classical groups, whereas Aschbacher is only proposing to use this approach for exceptional groups of Lie type. Our examples therefore merely show that his question is still too broad, and that the question needs to be restricted to a smaller class of groups than the class of almost simple groups.

The maximal subgroups are known completely for five of the ten families of exceptional groups of Lie type, and, of the remaining five, E_8 seems least likely to be a source of examples, since it admits neither diagonal nor graph automorphisms. Similarly, F_4 admits no diagonal automorphisms, and admits a graph automorphism only in characteristic 2. Probably the most promising places to look for examples of non-A-groups are in E_6 with a graph automorphism, and in E_7 with a diagonal automorphism. On the other hand, it is entirely conceivable that every finite exceptional group of Lie type is an A-group.

References

[1] M. Aschbacher, The subgroup structure of finite groups, *Finite simple groups: thirty years of the Atlas and beyond*, Contemp. Math. **694**, 111–121, AMS, 2017.

[2] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional classical groups*, LMS Lecture Notes **407**, Cambridge Univ. Press, 2013.

[3] G. Butler, The maximal subgroups of the sporadic simple group of Held, *J. Algebra* **69**, 67–81, 1981.

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An Atlas of Finite Groups*, Oxford Univ. Press, 1985.

[5] The GAP group, GAP – Groups, Algorithms, and Programming, Version 4.8.10; 2018. (https://www.gap-system.org)

[6] Ch. Jansen, K. Lux, R. A. Parker and R. A. Wilson, *An Atlas of Brauer Characters*, LMS Monographs **11**, Oxford Univ. Press, 1995.

[7] A. K. Schröder, The maximal subgroups of the classical groups in dimension 13, 14 and 15, PhD Thesis, University of St Andrews, 2015.

[8] N. J. A. Sloane, The On-line Encycopedia of Integer Sequences, https://oeis.org

[9] R. A. Wilson, Maximal subgroups of automorphism groups of simple groups, *J. London Math. Soc.* **32**, 460–466, 1985.

[10] Robert Wilson, Peter Walsh, Jonathan Tripp, Ibrahim Suleiman, Richard Parker, Simon Norton, Simon Nickerson, Stephen Linton, John Bray, Richard Barraclough and Rachel Abbott, *Atlas of Group Representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/`, 2005–.

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 33–35
ISSN: 1930-1235; (**2018**)

KAY MAGAARD (1962-2018)

We would like to dedicate this volume of the Albanian Journal of Mathematics to the memory of the former Editor and our dear friend and colleague, Kay Magaard (1962 – 2018). With Kay's passing, the mathematical community lost one of its most distinguished members, whose outstanding work is long lasting and has profoundly influenced many others.

Kay Magaard was an unusually broad and prolific mathematician. His research covers a great variety of topics in group theory, but also in many other fields of mathematics where groups, i.e. symmetries play a significant role. A particular focus of his work lies in groups of Lie type, finite and infinite, and related structures such as braid groups and Iwahori-Hecke algebras. Kay was well versed in all aspects of finite simple groups. He was in particular interested in enhancing the classification theorem by investigating maximal subgroups and irreducible representations of the finite simple groups, and then also in applying his findings to questions outside group theory. A recurrent feature of his work was his experimental and algorithmic approach.

Beginning with his PhD thesis from the year 1990, supervised by Michael Aschbacher, he was interested in the description and classification of maximal subgroups of groups of Lie type, and in particular classical groups. Since then, he has coauthored about ten publications devoted to this topic, although this is not always visible from a first glance at the titles. For example, his papers on the irreduciblilty of tensor products, symmetric and alternating powers of certain irreducible representations or the imprimitivity of irreducible representations of finite simple groups are motivated in part by Aschbacher's famous theorem on maximal subgroups of classical groups. An irreducible representation of a finite simple group (or more generally, a quasisimple group) yields an embedding of the group into a classical group. If this representation is also tensor decomposable or imprimitive, this embedding generally does not give rise to a maximal subgroup.

More than ten papers of Kay and coauthors are devoted to various other aspects of groups of Lie type. The majority of these is motivated by the constructive recognition problem for finite matrix groups. Topics are generation properties of particular series of groups of Lie type and identification algorithms using the black box model. Three papers contribute to the general representation theory theory of groups of Lie type.

A collection of seven papers of Kay reflects much of his recent work. These are devoted to the description and computation of the generic ordinary character tables of Sylow p-subgroups of series of groups of Lie type of characteristic p. The word "generic" refers to the fact that a description of the character tables is given in a parametrized form which applies to all groups in the series. An example is the series of Chevalley groups $D_4(q)$, where q is any prime power. Such generic tables are particularly useful in the ℓ-modular character theory of these groups for primes $\ell \neq p$.

Two papers of Kay deal with the representation theory of general finite groups, one with the character theory of a particular series of finite groups. Another two important papers, more than 150 pages in total, coauthored with Gernot Stroth, contribute a particular difficult piece to the revision project of the classification of the finite simple groups. Namely, the results build a bridge between two distinct strategies approaching this revision.

Four articles of Kay and coauthors are concerned with the theory of finite permutation groups. Particular impressive is his work towards a classification of those such groups, whose elements have only few fixed points. This program has been completed for permutation groups with each element having at most three fixed points. If the elements of a finite permutation group have at most one fixed point, this group either acts regularly or is a Frobenius group; the structure of Frobenius groups was elucidated by Frobenius. This series of papers thus continues Frobenius' work, but it also has applications to topology.

Much of the research of Kay was devoted to applications of the theory of finite simple groups, their subgroups and representations. These applications sometimes lie inside, sometimes outside group theory. An example of the latter is a major contribution to the classification of distance transitive graphs. Examples for the former are provided by a series of three important papers of Kay with coauthors dealing with the $k(GV)$-problem. This goes back to a famous question of Richard Brauer in modular representation theory. In this particular setting, which arises as a minimal configuration in the context of Brauer's question, G is a finite group acting faithfully and irreducibly on the finite vector space V with $|G|$ and $|V|$ coprime. In this situation, Brauer's question suggests that the number of conjugacy classes of the semidirect product GV should be at most equal to $|V|$. After a long tour of reductions and the handling of special cases by numerous authors including John Thompson, Kay and his collaborators managed to finally settle this problem which has been open for such a long time.

With more than 20 articles, applications to topology and algebraic geometry constitute the largest portion. These include applications to curves and surfaces, settling in particular a conjecture of Guralnick and Thompson on the composition factors of monodromy groups of Riemann surfaces of genus 0. Recent investigations are concerned with Beauville structures of quasisimple groups, where Kay and his coauthors prove a conjecture of Bauer, Catanese and Grunewald. A common feature of most of these investigations is the calculation of fixed point ratios of permutation groups and character ratios of groups of Lie type. These require detailed knowledge on the ordinary character tables of such groups, in particular deep insight into the results of Deligne-Lusztig theory. Kay was the main force behind the classification of the full automorphism groups of algebraic curves of a given genus $g \geq 2$ and determining the inclusion among the loci of curves with prescribed automorphism group in the moduli space of curves. Together with Shaska, Shpectorov, and Völklein they devised algorithms and wrote software to determine the braid orbits. With Shaska and Völklein, Kay studied geometrically decomposable 2-dimensional Jacobian varieties and with Völklein general curves of genus 3 and Weierstrass points on Hurwitz curves. His expertise in both computational group theory and algebraic geometry was truly impressive.

The breadth and the profoundness of Kay's contributions to mathematics, in particular to the theory of groups of Lie type and the finite simple groups, is

absolutely remarkable; no less impressive was his potential to identify relevant problems outside group theory, to which he could successfully apply his knowledge. His ability to inspire others for his ideas is also unmatched. His articles exhibit the incredible number of 67 coauthors. The undersigned are two of them. We gratefully acknowledge our fortune of having been able to profit from Kay's immense intuition and insight.

Gerhard Hiss
Tony Shaska

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 36–77
ISSN: 1930-1235; (**2018**)

ABSOLUTE REDUCTION OF BINARY FORMS

LUBJANA BESHAJ

Army Cyber Institute
West Point Military Academy
West Point, NY, 10996

Dedicated to the memory of Kay Magaard

Abstract. Reduction theory of binary forms has been studied by Julia in [23] and more recently by several other authors. In this paper we introduce the absolute reduction and give an algorithm to compute the absolutely reduced form of any binary form. Such method can be applied to determine the minimal Weierstrass equation of a superelliptic curve over an integral ring.

MSC 2010: Primary: 11E16, 11E76; Secondary: 11G30, 14H25
Keywords: integral binary forms, reduction theory

1. Introduction

Let $\mathcal{M}_g$ be the moduli space of genus $g \geq 2$ curves over an algebraically closed field F. For a moduli point $\mathfrak{p} \in \mathcal{M}_g$ we denote by K the minimal field of definition of $\mathfrak{p}$. It is a classical problem in algebraic geometry to find an equation of the curve $\mathcal{X}$ over K, corresponding to $\mathfrak{p}$. An algorithm to find such equations is known only for small genus g or for some classes of superelliptic curves (i.e. curves with affine equation $y^n = f(x)$). However such equations are not minimal, i.e., they do not have minimal height as defined in [32]. In this paper we introduce a method of finding a minimal equation for superelliptic curves defined over a ring of integers $\mathcal{O}_K$.

Any superelliptic curve with Weierstrass equation defined over the ring of integers $\mathcal{O}_K$ of a number field K is associated to a binary form $f(x, z)$ defined over $\mathcal{O}_K$. We associate to any binary form $f(x, z)$ a positive definite quadratic form $\mathcal{J}_f(x, z)$ called the Julia quadratic and therefore a point P_f in the upper half hyperbolic space $\mathcal{H}_3$. By an appropriate matrix $M \in \mathrm{SL}_2(\mathcal{O}_K)$ such a point is moved to a

E-mail address: Lubjana.Beshaj@westpoint.edu.
Date: Received: June 15, 2018. Accepted: Dec 15. 2018.

point P^M in the fundamental domain $\mathcal{F}_K$. This matrix moves f to a new binary form f^M, which is called the reduced form **red** (f) of f.

The form **red** (f) has small coefficients in its $\mathrm{SL}_2(\mathcal{O}_K)$-orbit, but it is not necessarily the form with the smallest height over $\mathcal{O}_K$. Therefore, it does not determine the superelliptic curve with the minimum height. Hence, we determine all twists $g_1,\ g_2, \ldots, g_r$ of **red** (f) with height less then or equal to the height of **red** (f), where r is the class number of the Julia quadratic $\mathcal{J}_f$.

We act on each of the twists by the transformations (ax, by) for certain a and b as explained in Thm. 9 to reduce the height even further. The minimal height among all the twists after such further reduction is called the *minimal absolute height*.

This paper is organized as follows. In the preliminaries we give some basics about fundamental domains. We start with the classical fundamental domain $\mathcal{F}$, which is obtain from the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathcal{H}_2$. Then, we describe the fundamental domain $\mathcal{F}_{\mathbb{Z}(i)}$ which is obtained by the action of the group $\Gamma_{\mathbb{Z}(i)} := \mathrm{SL}_2(\mathbb{Z}[i])/\{\pm I\}$ on the upper half space $\mathcal{H}_3$. Lastly we briefly discus fundamental domains of number fields, when such exists.

In Section 3 we start with giving some basic properties of binary forms and their invariants. Then, we define the height of binary forms and prove an equivalent of Northcot's theorem for binary form. See [32] for more details about this section.

In Section 4 we describe reduction theory of binary quadratics and binary quadratic Hermitian forms and then in Section 5 we describe reduction theory of higher degree binary forms. First, we explain in details the case of binary forms with real coefficients and then its generalization to binary forms with complex coefficients.

In Section 6 we explore some computational aspects of computing the Julia quadratic (invariant) and performing the reduction algorithm for higher degree binary forms. We give some geometric aspects of the reduction theory. Moreover, as we will see in Section 5 one of the key points of the reduction algorithm is computing the Jualia's quadratic. Expressing Julia's quadratic in terms of the covariants or the coefficients of the degree n binary form is only known for binary forms of degree 3, and 4. In Section 6 we provide a method how to compute the quadratic used for reduction for all possible signatures of binary forms with degree 5, and 6 in terms of the coefficients of the given binary form.

2. PRELIMINARIES

In this section we gice a brief review of what is well known in the literature, see [13, 16, 31, 35] for more details. We start with the classical fundamental domain which we denote by $\mathcal{F}$ and is obtained from the action of the classical modular group on the upper half plane. Then we explore how one can generalize this notion when we go to three dimensional space and consider the action of a discrete subgroup of $\mathbb{C}$ in the upper half space. Lastly, in this section we generalize the concept of fundamental domain for any number field K, for more details see [13], [16].

The concept of the fundamental domain is crucial in developing the theory of reduction. Most of the theory in this chapter will be used in Section 4 and Section 5.

2.1. Fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$.

Let $\mathbb{P}^1$ be the Riemann sphere and $\mathrm{GL}_2(\mathbb{C})$ the group of 2×2 matrices with entries in $\mathbb{C}$. The group $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{P}^1$ by linear fractional transformations as follows

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z = \frac{\alpha z + \beta}{\gamma z + \delta} \tag{1}$$

where $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ and $z \in \mathbb{P}^1$. It is easy to check that this is a group action. The $\mathrm{GL}_2(\mathbb{C})$ action on $\mathbb{P}^1$ is a transitive action, i.e. has only one orbit. Moreover, the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1$ is also transitive.

For the rest of this section we will consider the action of $\mathrm{SL}_2(\mathbb{R})$ on the Riemann sphere. Notice that this action is not transitive. The action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{P}^1$ has three orbits, namely $\mathbb{R} \cup \infty$, the upper half plane, and the lower-half plane. Therefore we restrict this action to the upper half-plane. Let $\mathcal{H}_2$ be the complex upper half plane, i.e.

$$\mathcal{H}_2 = \Big\{ z = x + iy \in \mathbb{C} \;\Big|\; y > 0 \Big\} \subset \mathbb{C}.$$

The group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}_2$ via linear fractional transformations. This action preserves $\mathcal{H}_2$ and acts transitively on it, further for $g \in \mathrm{SL}_2(\mathbb{R})$ and $z \in \mathcal{H}_2$ we have

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}\, z}{|\gamma z + \delta|^2}.$$

But $\mathrm{SL}_2(\mathbb{R})$ does not act faithfully on $\mathcal{H}_2$ since the elements $\pm I$ act trivially on $\mathcal{H}_2$. Hence, consider the above action as $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ action. This group acts faithfully on $\mathcal{H}_2$.

Let S be a set and G a group acting on it. Two points s_1, s_2 are said to be **G-equivalent** if $s_2 = g s_1$ for some $g \in G$. For any group G acting on a set S to itself we call a **fundamental domain** $\mathcal{F}$, if one exists, a subset of S such that any point in S is G-equivalent to some point in $\mathcal{F}$, and no two points in the interior of $\mathcal{F}$ are G-equivalent.

The group $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ is called the **modular group**. It is easy to prove that the Γ action on $\mathcal{H}_2$ via linear fractional transformations is a group action. This action has a fundamental domain $\mathcal{F}$

$$\mathcal{F} = \Big\{ z \in \mathcal{H}_2 \;\Big|\; |z|^2 \geq 1 \text{ and } |Re(z)| \leq 1/2 \Big\}$$

displayed in Fig. 1.

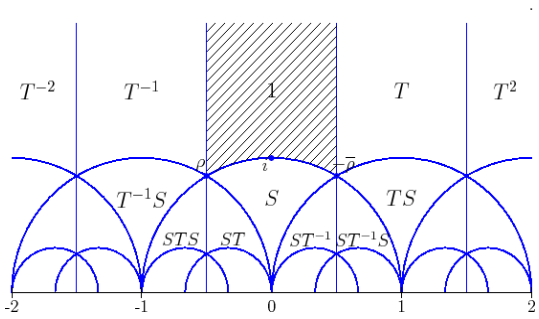

FIGURE 1. The action of the modular group on the upper half plane.

The following theorem proves that $\mathcal{F}$ is a fundamental domain, see [31] for proof.

Theorem 1. *i) Every $z \in \mathcal{H}_2$ is Γ-equivalent to a point in $\mathcal{F}$.*

ii) No two points in the interior of $\mathcal{F}$ are equivalent under Γ. If two distinct points z_1, z_2 of $\mathcal{F}$ are equivalent under Γ then $Re(z_1) = \pm 1/2$ and $z_1 = z_2 \pm 1$ or $|z_1| = 1$ and $z_2 = -1/z_1$.

iii) Let $z \in \mathcal{F}$ and $I(z) = \{g \,|\, g \in \Gamma, gz = z\}$ the stabilizer of $z \in \Gamma$. One has $I(z) = \{1\}$ except in the following cases:

$z = i$, in which case $I(z)$ is the group of order 2 generated by S;

$z = \rho = e^{2\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by ST;

$z = -\overline{\rho} = e^{\pi i/3}$, in which case $I(z)$ is the group of order 3 generated by TS.

The canonical map $\mathcal{F} \to \mathcal{H}_2/\Gamma$ is surjective and its restriction to the interior of $\mathcal{F}$ is injective. The modular group Γ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, where $S^2 = 1$ and $(ST)^3 = 1$. Note that $S^2 = 1$, so S has order 2, while $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ for any $k \in \mathbb{Z}$, so T has infinite order. For more details on the modular group and related arithmetic questions the reader can see [31] among others.

2.2. **Gaussian integers and the upper half space.** The upper half space $\mathcal{H}_3$ is defined as

$$\mathcal{H}_3 := \mathbb{C} \times (0, \infty) = \{(z, t) \,|\, z \in \mathbb{C}, t > 0\} = \{(x, y, t) | x, y \in \mathbb{R}, t > 0\}\,. \tag{2}$$

A point $P \in \mathcal{H}_3$ is given as $P = (z, t) = (x, y, t) = z + tj$, where $z = x + iy$ and $j = (0, 0, 1)$. The group $\mathrm{SL}_2(\mathbb{C})$ has a natural action on $\mathcal{H}_3$ by linear fractional transformations. Let $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$ and $P = z + tj \in \mathcal{H}_3$. Then $P^M = z^* + t^* j \in \mathcal{H}_3$ where

$$z^* = \frac{(\alpha z + \beta)(\bar{\gamma}\bar{z} + \bar{\delta}) + \alpha\bar{\gamma}t^2}{||\gamma z + \delta||^2 + ||\gamma||^2 t^2} \quad \text{and} \quad t^* = \frac{t}{||\gamma z + \delta||^2 + ||\gamma||^2 t^2}.$$

The group $\mathrm{SL}_2(\mathbb{C})$ is generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, where $a \in \mathbb{C}$. This generators act on (z, t), a point in $\mathcal{H}_3$, as follows

$$\begin{aligned} &\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} : (z, t) \to (z + \alpha, t) \\ &\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : (z, t) \to \left(\frac{-\bar{z}}{|z|^2 + t^2}, \frac{t}{|z|^2 + t^2} \right). \end{aligned} \tag{3}$$

In analogy with the previous section we consider the action of a discrete subgroup of $\mathrm{SL}_2(\mathbb{C})$ on $\mathcal{H}_3$. Let $\mathbb{Q}(i) \subset \mathbb{C}$ and $\mathbb{Z}[i]$ be the set of Gaussian integers. Then $\Gamma_{\mathbb{Z}(i)} := \mathrm{SL}_2(\mathbb{Z}[i])/\{\pm I\}$. A representation of $\Gamma_{\mathbb{Z}(i)}$ is given as follows

$$\Gamma_{\mathbb{Z}(i)} = \left\langle \; S, T, U, W \;\middle|\; \begin{array}{c} T^2 = U^2 = W^2 = 1 \\ (SW)^3 = (SU)^2 = (ST)^2 = 1 \\ (UW)^2 = (TW)^3 = 1 \end{array} \right\rangle$$

where

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

see [13, pg. 58-59] for more details. It is easy to prove that he group $\Gamma_{\mathbb{Z}[i]}$ is generated by S, T, U, W. The discrete group $\Gamma_{\mathbb{Z}[i]}$ acts on $\mathcal{H}_3$. Let $\mathcal{F}_{\mathbb{Z}(i)}$ be the following

$$\mathcal{F}_{\mathbb{Z}(i)} = \left\{ (z,t) \,|\, z = x+iy, -\frac{1}{2} \leq x \leq \frac{1}{2}, 0 \leq y \leq \frac{1}{2}, ||z||^2 + t^2 \geq 1 \right\}. \tag{4}$$

Given a point $\omega \in \mathcal{H}_3$ there exists $M \in \Gamma_{\mathbb{Z}[i]}$ such that $\omega^M \in \mathcal{F}_{\mathbb{Z}(i)}$. Moreover, if we suppose ω, and ω' are in the same Γ-orbit such that $\omega' = M\omega$ for $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_{\mathbb{Z}[i]}$. Assume $t(\omega) \leq t(\omega')$. Then we have one of the following three cases

i) $\gamma = 0$.
ii) $||\gamma|| = 1$, $t^2 \leq 1$.
iii) $||\gamma||^2 = 2$, $t^2 = 1/2$, ω is in the boundary of $\mathcal{F}_{\mathbb{Z}(i)}$, $\gamma z + \delta = 0$, $\delta = \pm 1, \pm i$.

Hence, from all the above we can conclude that $\mathcal{F}_{\mathbb{Z}(i)}$ is a fundamental domain of action of $\Gamma_{\mathbb{Z}[i]}$ on $\mathcal{H}_3$. Graphically $\mathcal{F}_{\mathbb{Z}(i)}$ is presented in Fig. 2.

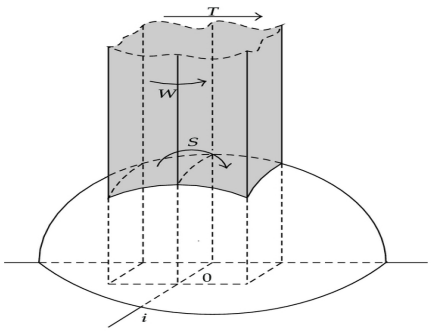

FIGURE 2. The fundamental domain $\mathcal{F}_{\mathbb{Z}(i)}$ in the upper half space

2.3. **Other algebraic number fields.** In this section we describe fundamental domains of other algebraic number fields. The action described in Eq. (1) makes sense when $\mathbb{C}$ is replaced by any number field K.

For analogy of $\mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R})$ we need to consider a discrete subring of $\mathbb{C}$. For any number field K with $\mathcal{O}_K$ its ring of integers the natural thing to consider is $\mathrm{SL}_2(\mathcal{O}_K)$, which is a discrete subgroup of $\mathrm{SL}_2(\mathbb{C})$. In an analogues way we can prove that the generators of $\mathrm{SL}_2(\mathcal{O}_K)$ are $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ for $a \in \mathcal{O}_K$. Next we want to consider for which number fields K the group $\mathrm{SL}_2(\mathcal{O}_K)$ acts transitively on $\mathbb{P}^1(K)$.

Let us recall some basic definitions from number theory, [30]. A **fractional ideal** is an $\mathcal{O}_K$-submodule $\mathfrak{a}$ contained in K such that there exists an element $c \neq 0$ in $\mathcal{O}_K$ satisfying $c\mathfrak{a} \subset \mathcal{O}_K$. Let $\mathfrak{P}$ be the subset of fractional ideals, then we write $\mathfrak{a} \sim \mathfrak{b}$ if there exists an element $\lambda \in K^*$ such that $\mathfrak{a} = (\lambda)\mathfrak{b}$, i.e. $\mathfrak{a}\mathfrak{b}^{-1}$ is a principal fractional ideal. The equivalence classes of fractional ideals form a finite group which we call the **ideal class group**. Its order is usually denoted by h_K and is called the **class number** of K. In [5, 31], amongst others, it is proved that for a

number field K, the number of orbits for $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathbb{P}^1(K)$ is the class number of K.

Hence, there is a bijection between the set of orbits of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathbb{P}^1(K)$ and the ideal class group of K. Moreover, $\mathrm{SL}_2(\mathcal{O}_K)$ acts transitively on $\mathbb{P}^1(K)$ if and only if K has class number 1.

Next we see how these results apply to imaginary quadratic number fields. Let $K = \mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{C}$ be an imaginary quadratic number field where $\Delta < 0$ a square-free integer, d_K the discriminant of K, and $\mathcal{O}_K$ its ring of integers. The group $\Gamma = \mathrm{PSL}_2(\mathcal{O}_K)$ is called the "**Bianchi group**" and is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{C})$.

It is easy to show that the Bianchi group acts on $\mathcal{H}_3$. This action has a fundamental domain, which we will denote as $\mathcal{F}_K$ and depends on K. For small discriminant this was determined by Bianchi and others in the 19^{th} century.

Consider the $\mathrm{PSL}_2(\mathcal{O}_K)$ action on $\mathcal{H}_3$, and define the following:

$$\begin{aligned}
\mathcal{B}_K &= \left\{ z + rj \in \mathcal{H}_3 \;\middle|\; |cz+d|^2 + |d|^2 r^2 \geq 1, \text{ for all } c, d \in \mathcal{O}_K : \langle c, d\rangle = \mathcal{O}_K \right\} \\
\mathcal{P}_K &= \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq \mathrm{Re}(z) \leq 1, \quad 0 \leq \mathrm{Im}(z) \leq \sqrt{|d_K|}/2 \right\} \\
F_K &= \mathcal{P}_K, \text{ for } \Delta \neq -3, -1 \\
F_{\mathbb{Q}(i)} &= \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq |\,\mathrm{Re}(z)| \leq \frac{1}{2}, \; 0 \leq \mathrm{Im}(z) \leq \frac{1}{2} \right\} \\
F_{\mathbb{Q}(\sqrt{-3})} &= \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq \mathrm{Re}(z), \; \frac{\sqrt{3}}{3}\,\mathrm{Re}(z) \leq \mathrm{Im}(z), \; \mathrm{Im}(z) \leq \frac{\sqrt{3}}{3}\Big(1 - \mathrm{Re}(z)\Big) \right\} \\
&\quad \cup \left\{ z \in \mathbb{C} \;\middle|\; 0 \leq \mathrm{Re}(z) \leq \frac{1}{2}, \; -\frac{\sqrt{3}}{3}\,\mathrm{Re}(z) \leq \mathrm{Im}(z) \leq \frac{\sqrt{3}}{3}\,\mathrm{Re}(z) \right\} \\
\mathcal{F}_K &= \left\{ z + rj \in \mathcal{B}_K \;\middle|\; z \in F_K \right\}.
\end{aligned}$$

Then the following theorem is true and see [16, pg 319] for the proof.

Theorem 2. *The set $\mathcal{F}_K$ is a fundamental domain for $\mathrm{PSL}_2(\mathcal{O}_K)$.*

Assume $(z, r) \in \mathcal{F}_K$, from the definition of the fundamental domain $\mathcal{F}_K$ we get obvious bounds for z. The following proposition gives a lower bound on r. The proof can be found in [16, pg. 316].

Proposition 1. *There is a constant $k \in \mathbb{R}^{>0}$ only depending on the number field K so that for any $z \in \mathbb{C} \setminus K$ there are infinitely many $\lambda, \mu \in \mathcal{O}_K$ with*

$$\left| z - \frac{\lambda}{\mu} \right| \leq \frac{k}{|\mu|^2}$$

and $\langle \lambda, \mu \rangle = \mathcal{O}_K$.

Hence for big enough μ we have $\frac{k}{|\mu|^2} < 1$ and therefore $\left| z - \frac{\lambda}{\mu} \right| < 1$. But from the definition of $\mathcal{B}_K$, as given above, for all $\lambda, \mu \in \mathcal{O}_K$ such that $\langle \lambda, \mu \rangle = \mathcal{O}_K$ we have $|\mu z - \lambda|^2 + |\mu|^2 r^2 \geq 1$, and we can conclude that $r \geq r_K$, for some r_K depending on the number field K. Consider the set

$$S_K = \left\{ z \in K \mid \; |z\mu + \lambda| \geq 1 \text{ for all } \langle \lambda, \mu \rangle = \mathcal{O}_K \right\}.$$

This is the set of singular points. In [16] it is proved that $z+rj \in \mathcal{F}_K$ for $z \in S_K$ are the only points in the fundamental domain such that r is not bounded from below. But when the number field K has class number one this set is empty. Hence, for an imaginary number field K, $h_K = 1$, there exists a constant r_K, only depending on K, such that $r \geq r_K$ for every $(z, r) \in \mathcal{F}_K$.

In [29] it is shown that when $K = \mathbb{Q}(\sqrt{-D})$ and D is one of 1, 2, ,3, 7, 11, 19, 43, 67, 163, then the value of r_K^2 is as given in Table Table 1.

TABLE 1. The value of r_K^2 for some number fields K

D	1	2	3	7	11	19	43	67	163
r_K^2	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{2}{3}$	$\frac{3}{7}$	$\frac{2}{11}$	$\frac{2}{19}$	$\frac{2}{43}$	$\frac{2}{67}$	$\frac{2}{163}$

This will be used in the following sections when we will introduce reduction theory of binary quadratics, as well as degree n binary forms. We can get bounds on the coefficients of a binary form depending only on the number field K, c.f. Section 4.

Lastly, let K be a number field. K is called **totally real** if for each embedding of K into the complex numbers the image lies inside the real numbers. Equivalently, K is generated over $\mathbb{Q}$ by one root of an integer polynomial P, all of the roots of P are real. If K is a totally real algebraic number field the group

$$\Gamma_K = \mathrm{PSL}_2(\mathcal{O}_K) = \mathrm{SL}_2(\mathcal{O}_K)/\{\pm I\}$$

is called the **Hilbert modular group** of K. If $[K : \mathbb{Q}] = n$ then the n-embeddings of K into $\mathbb{R}$ define an embedding of $\mathrm{PSL}_2(K)$ into $\mathrm{PSL}_2(\mathbb{R})^n$. When $n = 1$, we have the classical modular group described in Section 2.1.

The group Γ_K acts properly discontinuously on $\mathcal{H}^n$ which is contained in $\mathbb{P}^1(\mathbb{C}) \times \cdots \times \mathbb{P}^1(\mathbb{C})$, n-times. This generalizes the well known action of the classical modular group on the upper-half space $\mathcal{H}$. The orbits of $\mathbb{P}^1(K)$ under Γ_K or any group $\Gamma \subset \mathrm{PGL}_2(K)^+$ which is discrete in $\mathrm{PSL}_2(\mathbb{R})^+$ are called the **cusps** of Γ_K or Γ. For more details see [35].

3. HEIGHTS OF BINARY FORMS

In this section we give some of the basic properties of the binary forms and their invariants. We also define the height of a binary form, see [15, 19, 24, 32, 33] and others for more details.

Throughout this section k is an algebraically closed field of characteristic zero. Let $k[x, y]_n$ be the space of degree $n \geq 2$ homogenous polynomials. The group $k^\star$ acts on $k[x, y]_n$ by multiplication by a constant. The space of degree n binary forms with coefficients from k will be denoted by $V_{n,k} := k[x, y]_n/k^\star$. Thus, by a binary form $f \in V_{n,k}$ we will always mean the equivalence class of f.

The group $SL_2(k)$ acts on $V_{n,k}$ in the usual way. For an element $g \in V_{n,k}$ and $M \in SL_2(k)$, the action of M on g will be denoted by g^M. Two binary forms f and g are called k-*equivalent* if there is $M \in SL_2(k)$ such that $f = g^M$.

3.1. **Invariants and covariants.** Let $A_0, A_1, \ldots, A_n$ be coordinate functions on $V_{n,k}$. Then the coordinate ring of $V_{n,k}$ can be identified with $k[A_0, \ldots, A_n]$. For $I \in k[A_0, \ldots, A_n]$ and $M \in GL_2(k)$, define $I^M \in k[A_0, \ldots, A_n]$ as follows

$$I^M(f) = I(f^M) \tag{5}$$

for all $f \in V_{n,k}$. Then $I^{MN} = (I^M)^N$ and Eq. (5) defines an action of $GL_2(k)$ on $k[A_0, \ldots, A_n]$.

Definition 1. *Let $\mathcal{R}_n$ be the ring of $SL_2(k)$ invariants in $k[A_0, \ldots, A_n]$, i.e., the ring of all $I \in k[A_0, \ldots, A_n]$ with $I^M = I$ for all $M \in SL_2(k)$.*

A homogeneous polynomial $I \in k[A_0, \ldots, A_n, x, y]$ is called a **covariant** of index s if

$$I^M(f) = \delta^s I(f),$$

where $\delta = \det(M)$. The homogeneous degree in $A_1, \ldots, A_n$ is called the **degree** of I, and the homogeneous degree in x, y is called the **order** of I. A covariant of order zero is called an **invariant**. An invariant is a $SL_2(k)$-invariant on V_n. The discriminant of a binary form $f \in V_{n,k}$ is an $SL_2(k)$-invariant or order $2n-2$ which is denoted by Δ_f.

Since k is algebraically closed, any binary form $f(x, y)$ can be factored as

$$f(x,y) = (y_1 x - x_1 y) \cdots (y_d x - x_d y) = \prod_{1 \le i \le d} \det \begin{pmatrix} x & x_i \\ y & y_i \end{pmatrix} \tag{6}$$

The points with homogeneous coordinates $(x_i, y_i) \in \mathbb{P}^1$ are called the roots of the binary form f. Thus, for $M \in GL_2(k)$ we have

$$g(f(x,y)) = (\det(M))^d \cdot (y_1' x - x_1' y) \cdots (y_d' x - x_d' y),$$

where

$$\begin{pmatrix} x_i' \\ y_i' \end{pmatrix} = g^{-1} \begin{pmatrix} x_i \\ y_i \end{pmatrix}. \tag{7}$$

Now we define the height and the minimal height of a binary form. An extended overview of this section can be found in [32]. Let K be an algebraic number field, M_K denotes the set of valuations of K, and $f \in K[x, y]$ a degree n binary form given by

$$f(x,y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_{n_1} x y^{n-1} + a_n y^n$$

The **affine height** of f is defined as follows

$$H_K^{\mathbb{A}}(f) = \prod_{v \in M_K} \max \left\{ 1, |f|_v^{n_v} \right\}$$

where

$$|f|_v := \max_j \left\{ |a_j|_v \right\}$$

is the **Gauss norm** for any absolute value v. The **projective height** of a polynomial is the height of its coefficients taken as coordinates in the projective space. Thus,

$$H_K(f) = \prod_{v \in M_K} |f|_v^{n_v}$$

From now on, when we say "height" of a binary form f we will always mean the projective height $H_K(f)$. If $K = \mathbb{Q}$ then we will just use $H(f)$. The **(projective) absolute multiplicative height** is defined as follows

$$\begin{aligned} \mathrm{H} : \mathbb{P}^n(\mathbb{Q}) &\to [1, \infty) \\ \mathrm{H}(f) &= \mathrm{H}_K(f)^{1/[K:\mathbb{Q}]}, \end{aligned}$$

and in the same way $h(f)$, $\mathrm{H}^{\mathbb{A}}(f), h^{\mathbb{A}}(f)$. In [32] the authors prove the following.

Theorem 3. *Given $F(x, y) \in K[x, y]$. There are only finitely many polynomials $G(x, y) \in K[x, y]$ such that $\mathrm{H}_K(G) \leq \mathrm{H}_K(F)$.*

Let $f \in V_{n,\mathbb{C}}$. If there exists a matrix $M \in GL_2(\mathbb{C})$ such that $f^M \in \mathcal{O}_K[x, y]$ for some number field K, we say that f has an **integral model over** K. If f has an integral model over $\mathbb{Q}$ we simply say that f has an integral model. The main goal of this paper is to determine the integral model of a binary form f with minimal height when such model exists.

4. Reduction theory of binary quadratics

4.1. **Binary quadratic forms over $\mathbb{R}$.** First we present some basics about binary quadratic forms. Let $Q(X, Z) = aX^2 + bXZ + cZ^2$ be a binary quadratic in $\mathbb{R}[X, Z]$. We will use the following notation to represent the equivalence class of binary quadratics up to a scalar multiple, $Q(X, Z) = [a, b, c]$. The **discriminant** of Q is $\Delta = b^2 - 4ac$ and $Q(X, Z)$ is positive definite if $a > 0$ and $\Delta < 0$. Denote the set of positive definite binary quadratics with $V^+_{2,\mathbb{R}}$, i.e.

$$V^+_{2,\mathbb{R}} = \left\{ Q(X, Z) \in \mathbb{R}[X, Z] \;\middle|\; Q(X, Z) \text{ is positive definite} \right\}.$$

Let $\mathrm{SL}_2(\mathbb{R})$ act as usual on the set of positive definite binary quadratic forms

$$\begin{aligned} \mathrm{SL}_2(\mathbb{R}) \times V^+_{2,\mathbb{R}} &\to V^+_{2,\mathbb{R}} \\ \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix} \times \begin{pmatrix} X \\ Z \end{pmatrix} &\to Q(\alpha_1 X + \alpha_2 Z, \alpha_3 X + \alpha_4 Z) \end{aligned}$$

We will denote this new form with $Q^M(X, Z) = a'X^2 + b'XZ + c'Z^2$ where

$$\begin{aligned} a' &= a\alpha_1^2 + b\alpha_1\alpha_3 + c\alpha_3^2 \\ b' &= 2(a\alpha_1\alpha_2 + c\alpha_3\alpha_4) + b(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\ c' &= a\alpha_2^2 + b\alpha_2\alpha_4 + c\alpha_4^2 \end{aligned} \tag{8}$$

and

$$\Delta' = b'^2 - 4a'c' = (\det M)^2\Delta.$$

Obviously Δ is fixed under the $\mathrm{SL}_2(\mathbb{R})$ action and the leading coefficient of the new form Q^M will be $Q^M(1, 0) = Q(a, c) > 0$. Hence, $V^+_{2,\mathbb{R}}$ is preserved under this action.

Now, consider the following map which is called the **zero map**

$$\begin{aligned} \xi : V^+_{2,\mathbb{R}} &\to \mathcal{H}_2 \\ [a, b, c] \mapsto \xi(Q) &= \frac{-b + \sqrt{\Delta}}{2a} \end{aligned} \tag{9}$$

where $\mathrm{Re}(\xi(Q)) = -\frac{b}{2a}$, and $\mathrm{Im}(\xi(Q)) = \frac{\sqrt{|\Delta|}}{2a}$. This map is a bijection since given $z = x + iy$, we can find a, b, c such that $Q(X, Z)$ is positive definite given as $[1, -2x, x^2 + y^2]$.

Note that this map gives us a one-to-one correspondence between positive definite quadratic forms and points in $\mathcal{H}_2$. Let Γ be the modular group acting on $\mathcal{H}_2$, and on $V^+_{2,\mathbb{R}}$ as described above. Then the following theorem is proved in [5].

Lemma 1. *The zero map $\xi : V^+_{2,\mathbb{R}} \to \mathcal{H}_2$ is a Γ-equivariant map. In other words, $\xi(Q^M) = M^{-1}\xi(Q)$.*

4.2. **Reduction theory for binary quadratics.** We denoted with $V^+_{2,\mathbb{R}}$ the set of positive definite quadratics and we have defined an equivalence relation in this set. Define $Q = [a, b, c]$ to be **reduced** if $\xi(Q) \in \mathcal{F}$. Moreover, it is easy to prove that a positive definite quadratic form $Q \in V^+_{2,\mathbb{R}}$ is reduced if and only if $|b| \le a \le c$. This gives an arithmetic condition on the coefficients of a reduced positive definite binary quadratic.

Note that if Q is a reduced form with fixed discriminant $\Delta = -D$, then $b \le \sqrt{D/3}$. Moreover, the number of reduced forms of a fixed discriminant $\Delta = -D$ is finite. Every positive definite quadratic form Q with fixed discriminant is equivalent to a reduced form of the same discriminant. Two reduced binary quadratics are equivalent only in the following two cases $[a, b, a] \sim [a, -b, a]$, and $[a, a, c] \sim [a, -a, c]$. The proof of this fact can be found in [12, pg. 15]. Let $\Delta < 0$ be fixed, then the class number $h(\Delta)$ is equal to the number of primitive reduced forms of discriminant Δ.

In [5] the authors give an algorithm to list reduced forms with given discriminant. In [5, Table 1] the authors list (count the number of) reduced forms with fixed discriminant $\Delta \equiv 1 \bmod 4$, $\Delta \le 0$. Note that n represents the number of reduced forms with discriminant Δ.

From the equivalence classes of reduced quadratics there is one which has the smallest height. We call this class the special class and the corresponding height the minimal absolute height. Being able to construct such tables has two benefits. First we can count the equivalence classes and second we can find the quadratics with minimal height in their respective orbits.

The following theorem gives a connection between the concept of a reduced form and the height of the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class $[f]$ of a binary quadratic form f.

Theorem 4. *Let $f(X, Z) = aX^2 + bXZ + cZ^2$ be reduced (i.e. $|b| < a < c$). Then $\mathrm{H}([f]) = c$.*

Proof. We want to show that given any $M = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & a_4 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ acting on $f(X, Z)$ we have that $\max\{|a_1|, |b_1|, |c_1|\} \ge c$, where a_1, b_1, c_1 are the coefficients of the new form f^M. From Eq. (8) we have

$$\begin{aligned} a_1 &= a\alpha_1^2 + b\alpha_1\alpha_3 + c\alpha_3^2 \\ b_1 &= 2(a\alpha_1\alpha_2 + c\alpha_3\alpha_4) + b(\alpha_1\alpha_4 + \alpha_2\alpha_3) \\ c_1 &= a\alpha_2^2 + b\alpha_2\alpha_4 + c\alpha_4^2. \end{aligned}$$

We will prove it only for the generators of $\mathrm{SL}_2(\mathbb{Z})$, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. First, let $M = S$, then we have $[a_1, b_1, c_1] = [c, -b, a]$ and if $M = T$ then $[a_1, b_1, c_1] = [a, 2a + b, a + b + c]$ and the result is obvious. □

Corollary 1. *If f is a reduced quadratic then f has minimal height* $\mathrm{H}(f)$ *in its* Γ*-orbit.*

Proof. Above it is proved that $f(x,y) = ax^2+bxy+cy^2$ being reduced is equivalent to $|b| \leq a \leq c$. Moreover, $\mathrm{H}(f) = c$. This shows that f has minimal height in its Γ-orbit. □

Next we focus on binary Hermitian forms and then we can generalize the reduction theory for number fields, when possible.

4.3. **Binary Hermitian forms.** In this section first we give some basics from linear algebra about Hermitian matrices and Hermitian binary forms. Then we describe the $PSL_2(\mathbb{C})$ action on the 3-dimensional hyperbolic space, denoted by $\mathcal{H}_3$ and define the "zero" map which gives a one-to-one correspondence between positive definite Hermitian forms and points in $\mathcal{H}_3$. At the end of the section we will define reduction of Hermitian forms and give an algorithm how to perform reduction.

An $n \times n$ matrix A with complex entries is called Hermitian if $A^* = A$, where $A^* = \bar{A}^T$. Recall that $\bar{A}$ is obtained from A by applying complex conjugation to all elements and A^T is the transpose of A. By the definition we see that an Hermitian matrix is unchanged by taking its conjugate transpose. Note that any Hermitian matrix must have real diagonal entries.

Let R be a subring of $\mathbb{C}$ with $R = \bar{R}$, denote by $H(R)$ the set of 2×2 Hermitian matrices, i.e.

$$H(R) = \{A \in M_2(R) \,|\, A^* = A\}$$

A 2×2 matrix is in $H(R)$ if it is of the form $A = \begin{pmatrix} a & b \\ \bar{b} & d \end{pmatrix}$ where $a, d \in R \cap \mathbb{R}$ and $b \in R$. Every matrix $A \in H(R)$ defines a **binary Hermitian form** with entries in R. If $A \in H(R)$ then the associated binary Hermitian form is the semi-quadratic map

$$Q : \mathbb{C} \times \mathbb{C} \to R$$

defined as

$$Q(X,Z) = \begin{pmatrix} X \\ Z \end{pmatrix}^\star \begin{pmatrix} a & b \\ \bar{b} & d \end{pmatrix} \begin{pmatrix} X \\ Z \end{pmatrix} = aX\bar{X} + \bar{b}X\bar{Z} + b\bar{X}Z + dZ\bar{Z}.$$

The discriminant $\Delta(Q)$ of $Q \in H(R)$ is defined as $\Delta(Q) = \det(Q) = ad - |b|^2$. A binary Hermitian form $Q \in H(R)$ is **positive definite** if $Q(X,Z) > 0$ for every $(X,Z) \in \mathbb{C}\times\mathbb{C}\setminus\{0,0\}$. Q is called **negative definite** if $-Q$ is positive definite and **indefinite** if $\Delta(Q) < 0$. Denote by $H(R)^+$ the set of positive definite Hermitian forms, i.e.

$$H(R)^+ = \{Q \in H(R) \,|\, Q \textit{ is positive definite}\}$$

If $a \neq 0$, then

$$Q(X,Z) = a\left(\left|X + \frac{bZ}{a}\right|^2 + \frac{\Delta}{a^2}|Z|^2\right).$$

Hence, $Q \in H^+(R)$ if and only if $a > 0$ and $\Delta > 0$. The group $\mathrm{GL}_2(R)$, where $R \subset \mathbb{C}$, as in Section 4.3, acts on $H(R)$ as follows

$$\begin{aligned} \mathrm{GL}_2(R) \times H(R) &\to H(R) \\ (M, Q) &\mapsto M^\star Q M \end{aligned} \tag{10}$$

for $M \in \mathrm{GL}_2(R)$ and $Q \in H(R)$. We can define in an analogous way an $\mathrm{SL}_2(R)$-action on $H(R)$. Note that if A is the Hermitian matrix of Q then the Hermitian matrix of the new form is $M^\star AM$. It is easy to show that

$$\Delta(M(Q)) = |\det M|^2 \cdot \Delta(Q). \tag{11}$$

The group $\mathrm{GL}_2(R)$ leaves $H^+(R)$ invariant since for $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and $Q \in H^+(R)$, from Eq. (11) we have that $\Delta(M(Q)) > 0$ and also it is easy to check that the leading coefficient of $Q^M = Q(\alpha, \gamma) > 0$.

The group $\mathbb{R}^{>0}$ acts on $H^+(\mathbb{C})$ by scalar multiplication. We will denote by $\tilde{H}^+(\mathbb{C})$ the quotient space $H^+(\mathbb{C})/\mathbb{R}^{>0}$, and $[Q]$ the equivalence class of Q in $\tilde{H}^+(\mathbb{C})$. The action of $\mathrm{GL}_2(\mathbb{C})$ on $H(\mathbb{C})$ induces an action of $\mathrm{GL}_2(\mathbb{C})$ on $\tilde{H}^+(\mathbb{C})$.

The center of $\mathrm{SL}_2(\mathbb{C})$ acts trivially on $H(\mathbb{C})$, so we get an induced action of $\mathrm{PSL}_2(\mathbb{C})$ on $H(\mathbb{C})$ and $\tilde{H}^+(\mathbb{C})$.

Definition 2. *The map $\xi : H^+(\mathbb{C}) \to \mathcal{H}_3$ defined by*

$$\xi \begin{pmatrix} a & b \\ \bar{b} & d \end{pmatrix} \to -\frac{b}{a} + \frac{\sqrt{\Delta(Q)}}{a} \cdot j \tag{12}$$

*is called the "**zero map**" for binary quadratic Hermitian forms. Clearly ξ induces a map $\xi : \tilde{H}^+(\mathbb{C}) \to \mathcal{H}_3$.*

Since Q is positive definite we have that $a > 0$ and $\Delta > 0$, hence ξ is well defined and continuous. This map is a bijection since given $(z, t) \in \mathcal{H}_3$ we can find $Q = [1, -z, -\bar{z}, |z|^2 + t^2]$, i.e.

$$Q : (u, v) \to |u|^2 - zu\bar{v} - \bar{z}\bar{u}v + (|z|^2 + t^2)|v|^2$$

Therefore, this map gives a one-to-one correspondence between equivalence classes of positive definite binary quadratic Hermitian forms and points in $\mathcal{H}_3$. The following theorem holds.

Theorem 5. *The map $\xi : \tilde{H}^+(\mathbb{C}) \to \mathcal{H}_3$ defined by*

$$[Q] \to -\frac{b}{a} + \frac{\sqrt{\Delta(Q)}}{a} \cdot j$$

is a $\mathrm{PSL}_2(\mathbb{C})$ equivariant, i.e. ξ satisfies $\xi(Q^M) = M^{-1}\xi(Q)$ for every $M \in \mathrm{PSL}_2(\mathbb{C})$ and $Q \in \mathcal{H}^+(\mathbb{C})$.

Proof. See [5].

Note that Thm. 5 holds if we replace $\mathbb{C}$ by any number field K and the proof follows through in exactly the same way.

4.4. **Reduction theory of Hermitian forms.** Reduction of real binary quadratic forms with respect to the action of $\mathrm{SL}_2(\mathbb{Z})$, as described in Section 4.2, may be extended to a reduction theory for binary forms with complex coefficients (Hermitian binary forms) under the action of certain discrete subgroups of $\mathbb{C}$. In order to do that we need a discrete subring of $\mathbb{C}$ and then define the fundamental domain of this action.

Let $H(\mathcal{O}_K)$ denote the space of binary Hermitian forms with coefficients in $\mathcal{O}_K$, and by $H^+(\mathcal{O}_K)$ denote the set of positive definite Hermitian forms with coefficients in $\mathcal{O}_K$, and let $H^-(\mathcal{O}_K)$ the set of indefinite Hermitian forms with coefficients in

$\mathcal{O}_K$. It is easy to show that the **"Bianchi group"** $\Gamma = \mathrm{PSL}_2(\mathcal{O}_K)$ acts on $H^+(\mathcal{O}_K)$ preserving discriminants.

The following definition is analog to the one for positive definite binary quadratic forms.

Definition 3. *A positive definite Hermitian form $f \in H^+(\mathcal{O}_K)$ is called a* ***reduced Hermitian form*** *if $\xi(f) \in \mathcal{F}_K$.*

Let K be an imaginary quadratic number field and $\mathcal{O}_K$ its ring of integers. Define

$$H(\mathcal{O}_K, \Delta) = \{f \in H(\mathcal{O}_K) \,|\, \Delta(f) = \Delta\}$$

to be the subspace of $H(\mathcal{O}_K)$ with fixed discriminant Δ and

$$H^{\pm}(\mathcal{O}_K, \Delta) = \{f \in H^{\pm}(\mathcal{O}_K) \,|\, \Delta(f) = \Delta\}$$

the subspace of $H^{\pm}(\mathcal{O}_K)$ of fixed discriminant. Then the following theorem holds.

Theorem 6. *Given $\Delta \neq 0 \in \mathbb{Z}$, the number of reduced forms of $H(\mathcal{O}_K, \Delta)$ is finite.*

The proof can be found in [16, pg. 411].

Corollary 2. *For any $\Delta \in \mathbb{Z}$ with $\Delta \neq 0$ the set $H(\mathcal{O}_K, \Delta)$ (and $H^{\pm}(\mathcal{O}_K, \Delta)$) splits into finitely many $\mathrm{SL}_2(\mathcal{O}_K)$-orbits.*

Proof. This is an immediate consequence of Thm. 8 and Thm. 5 which says that every $f \in H(\mathcal{O}_K, \Delta)$ is $\mathrm{PSL}_2(\mathcal{O}_K)$-equivalent to a reduced form. □

For any $\Delta \in \mathbb{Z}$ with $\Delta \neq 0$ define

$$\tilde{H}(\mathcal{O}_K, \Delta) = \mathrm{SL}_2(\mathcal{O}_K) \backslash H(\mathcal{O}_K, \Delta),$$

and denote by $h(\mathcal{O}_K, \Delta) := \left| \tilde{H}(\mathcal{O}_K, \Delta) \right|$, where the number $h(\mathcal{O}_K, \Delta)$ is called the **class number of binary Hermitian forms of discriminant** Δ.

We define in the same way for positive definite Hermitian forms $\tilde{H}^+(\mathcal{O}_K, \Delta) = \mathrm{SL}_2(\mathcal{O}_K) \backslash H^+(\mathcal{O}_K, \Delta)$ such that $h^+(\mathcal{O}_K, \Delta) = \left| \tilde{H}^+(\mathcal{O}_K, \Delta) \right|$, and $h^+(\mathcal{O}_K, \Delta)$ is called the **class number of positive definite binary Hermitian forms of discriminant** Δ. Note that for $\Delta > 0$ we have that $h(\mathcal{O}_K, \Delta) = 2h^+(\mathcal{O}_K, \Delta)$.

Given $\mathcal{O}_K$ and the discriminant Δ it is always possible to compute the class number of positive definite binary Hermitian forms with given discriminant Δ. For a reduced binary Hermitian form we can get bounds on the coefficients of the form depending only on the number field K.

Let $Q(X, Z) = aX\bar{X} + \bar{b}X\bar{Z} + b\bar{X}Z + cZ\bar{Z}$ be a reduced Hermitian form, with discriminant Δ and let $D = |\Delta|$. We have

$$a \leq \frac{\sqrt{D}}{r_k}, \;\; |b|^2 \leq c_k a^2, \;\; \text{and } ac \leq \left(1 + \frac{c_k}{r_k}\right) D$$

for constant c_k depending only on the number field K.

Let us now consider the case when $K = \mathbb{Q}(i)$. The fundamental domain of this action is $\mathcal{F}_{\mathbb{Z}(i)}$, as shown in Eq.(4). We want to count the number of reduced positive definite binary Hermitian forms with a fixed discriminant Δ, i.e. $h^+(\mathbb{Z}[i], \Delta)$.

Let $f = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$ be a positive definite binary quadratic Hermitian form with coefficients in $Z[i]$ and non-zero discriminant Δ. The binary quadratic Hermitian form f is reduced if $\xi(f) \in \mathcal{F}_{\mathbb{Z}(i)}$.

Proposition 2. *Let $f(x,y) = ax\bar{x}+b\bar{x}y+\bar{b}x\bar{y}+cy\bar{y}$ be a binary quadratic Hermitian form. Then f is reduced over F if and only if*

$$-\frac{a}{2} \leq \mathrm{Re}(b) \leq \frac{a}{2}, \qquad 0 \leq \mathrm{Im}(b) \leq \frac{a}{2}, \qquad a \leq c.$$

Moreover, $||b|| \leq a \leq c$.

Proof. The binary quadratic Hermitian form f is reduced if $\xi(f) \in \mathcal{F}_{\mathbb{Z}(i)}$, i.e.,

$$\xi(f) = -\frac{b}{a} + \frac{\sqrt{\Delta}}{a} \cdot j \in \mathcal{F}_{\mathbb{Z}(i)}.$$

Denote by $z = -\frac{b}{a}$ and $t = \frac{\sqrt{\Delta}}{a}$. By the description of fundamental domain $\mathcal{F}_{\mathbb{Z}(i)}$ given in Eq. (4) we have $-\frac{a}{2} \leq \mathrm{Re}(b) \leq \frac{a}{2}$, $0 \leq \mathrm{Im}(b) \leq \frac{a}{2}$, and $||z||^2+t^2 \geq 1$. Since $||z||^2 + t^2 \geq 1$ we have

$$1 \leq \frac{||b||^2}{a^2} + \frac{\Delta}{a^2} = \frac{||b||^2 + ac - ||b||^2}{a^2} = \frac{c}{a}$$

i.e. $a \leq c$. Now consider

$$||b||^2 = \mathrm{Re}(b)^2 + \mathrm{Im}(b)^2 \leq \frac{a^2}{4} + \frac{a^2}{4} = \frac{a^2}{2}.$$

Hence, $||b|| \leq \frac{a\sqrt{2}}{2} \leq a \leq c$, which proves the last part. □

By discreteness of $\mathbb{Z}[i]$, the elements a and b may take on only finitely many values. The discriminant $\Delta = ac - b\bar{b}$, hence c is determined by a and b. Therefore, c may take on only finitely many values too.

In [5, Table 2] we list (count) the number of reduced binary quadratic Hermitian forms with fixed discriminant. To each tuple $[a,b,c]$ corresponds a binary quadratic Hermitian form

$$Q(X,Z) = aX\bar{X} + \bar{b}X\bar{Z} + b\bar{X}Z + cZ\bar{Z}.$$

In the first column is given the discriminant, in the second one the reduced forms $[a,b,c]$ with that given discriminant, and in the third column the number of reduced forms.

Proposition 3. *Let $f \in \mathrm{Her}^+(\mathcal{O}_F)$. If f is reduced over F then f has minimal height in its Γ_F-orbit.*

Proof. Since f is defined over the Gaussian integers, as shown in [5, Example 1], the height is just $\mathrm{H}(f) = \max\{\,|x_j|_\infty\}$. Since f is reduced, from above Prop. Prop. 2 we have that

$$\mathrm{H}_F(f) = \max\{||b||, |a|, |c|\} = c.$$

We need to show that this is the minimal height on its Γ_F-orbit. In analogy with the case of binary quadratic forms defined over the reals we will prove it only for the generators of Γ_F. Let Q be the matrix associated to the given binary quadratic Hermitian form. Consider first the action of S on f. We have

$$Q^S = S^\star Q S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ a+\bar{b} & a+2\,\mathrm{Re}(b)+c \end{pmatrix}$$

and

$$\mathrm{H}_F(f^S) = \max\Big\{\, ||a||, ||a+b||, ||a+\bar{b}||, ||a+2\,\mathrm{Re}(b)+c|| \Big\}.$$

Since $a > 0$, and $-\frac{a}{2} \leq \mathrm{Re}(b) \leq \frac{a}{2}$, then $||a + 2\,\mathrm{Re}(b) + c|| \geq c$. Therefore, $\mathrm{H}_F(f^S) \geq \mathrm{H}_F(f)$.

Let T act on f. The associated matrix to f^T is as follows

$$Q^T = T^\star Q T = \begin{pmatrix} -i & 0 \\ 1 & i \end{pmatrix} \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} i & 1 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} a & -ai + b \\ b + ic & a + 2\,\mathrm{Im}(b) + c \end{pmatrix}$$

and

$$\mathrm{H}_F(f^T) = \max\left\{ ||a||, || - ai + b||, ||b + ic||, ||a + 2\,\mathrm{Im}(b) + c|| \right\}.$$

But $a > 0$, and $0 \leq \mathrm{Im}(b) \leq \frac{a}{2}$, hence $||a + 2\,\mathrm{Im}(b) + c|| \geq c$. Therefore, $\mathrm{H}_F(f^T) \geq \mathrm{H}(f)$.

Let U act on f. The associated matrix to the form f^U is

$$Q^U = U^\star Q U = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} a & -b \\ -\bar{b} & c \end{pmatrix}.$$

Hence, $\mathrm{H}_F(f^U) = \mathrm{H}_F(f)$.

Lastly, let W act on f. The matrix associated to the new form f^W is

$$Q^W = W^\star Q W = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c & -\bar{b} \\ -b & a \end{pmatrix},$$

and the height of the new form does not change. Hence, we conclude $\mathrm{H}_F(f^M) \geq \mathrm{H}_F(f)$ for any $M \in \Gamma_F$. Therefore, f has minimal height in its Γ_F-orbit. □

In [5, Table 2] we display a table of classes of binary quadratic Hermitian forms with given discriminant. We list reduced forms representative of classes given by $[a, b, c]$ with a given discriminant Δ. The algorithm to compute this forms is similar with the one for computing binary quadratic forms with a given discriminant.

5. Reduction of higher degree binary forms

Next we give an algorithm such that for any form f with degree $n > 2$ defined over a ring of integers $\mathcal{O}_K$, we find a form with minimal height $\mathrm{H}(f)$ in its $\Gamma_{\mathcal{O}_K}$-orbit.

5.1. Julia quadratic of binary forms.

Julia quadratic was introduced in 1917 by Gaston Julia in his PhD thesis; see [23]. It did not get the attention that it deserved. Indeed Julia became known for most of his other work on Julia sets and fractals. However, in 1999 Cremona [14] used ideas of Julia to explore the reduction for cubic binary forms. More recently Cremona and Stoll in [34] gave a generalization of Julia's work for binary forms defined over $\mathbb{C}$.

Julia quadratic of binary forms with real coefficients. We will motivate and define the Julia quadratic of a binary form of degree $n \geq 2$ with real coefficients. We will try to follow as closely as possible the approach and notation used in Julia's original paper [23].

Let $f(x, y) \in \mathbb{R}[x, y]$ be a degree n binary form given as follows:

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n$$

and suppose that $a_0 \neq 0$. Let the real roots of $f(x, y)$ be α_i, for $1 \leq i \leq r$ and the pair of complex roots β_j, $\bar{\beta}_j$ for $1 \leq j \leq s$, where $r + 2s = n$. The form can be factored as

$$f(x,1) = \prod_{i=1}^{r}(x-\alpha_i)\cdot\prod_{i=1}^{s}(x-\beta_i)(x-\bar{\beta}_i). \tag{13}$$

The ordered pair (r,s) of numbers r and s is called the **signature** of the form f.

We associate to f the two quadratics $T_r(x,1)$ and $S_s(x,1)$ of degree r and s respectively given by the formulas

$$T_r(x,1) = \sum_{i=1}^{r} t_i^2(x-\alpha_i)^2, \quad \textit{and} \quad S_s(x,1) = \sum_{j=1}^{s} 2u_j^2(x-\beta_j)(x-\bar{\beta}_j), \tag{14}$$

where t_i, u_j are to be determined. Then

$$\begin{aligned} T_r(x,1) &= \left(\sum_{i=1}^{r} t_i^2\right)x^2 - 2\left(\sum_{i-1}^{r} t_i^2\alpha_i\right)x + \left(\sum_{i-1}^{r} t_i^2\alpha_i^2\right) \\ S_s(x,1) &= 2\left(\sum_{j=1}^{s} u_j^2\right)x^2 - 4\left(\sum_{j=1}^{s} u_j^2\,\mathrm{Re}(\beta_j)\right)x + 2\left(\sum_{j=1}^{s} u_j^2\cdot||\beta_j||^2\right). \end{aligned} \tag{15}$$

For a binary form f of signature (r,s) the quadratic Q_f is defined as

$$Q_f(x,1) = T_r(x,1) + S_s(x,1). \tag{16}$$

Let $\beta_i = a_i + b_i\cdot I$, for $i = 1,\ldots,s$. Then Q_f can be written as

$$\begin{aligned} Q_f &= \sum_{i=1}^{r} t_i^2(x^2 - 2\alpha_i\,x + \alpha_i^2) + 2\sum_{j=1}^{s} u_j^2\,\left(x^2 - 2a_j\cdot x + (a_j^2+b_j^2)\right), \\ &= \left(\sum_{i=1}^{r} t_i^2 + 2\sum_{j=1}^{s} u_j^2\right)x^2 - 2\left(\sum_{i=1}^{r}\alpha_i t_i^2 + 2\sum_{j=1}^{s} a_j u_j^2\right)x \\ &+ \left(\sum_{i=1}^{r} t_i^2\alpha_i^2 + 2\sum_{j=1}^{s} u_j^2\cdot(a_j^2+b_j^2)\right). \end{aligned} \tag{17}$$

The discriminant of Q_f is a degree 4 homogenous polynomial in $t_1,\ldots t_r$, $u_1,\ldots,u_s$. We would like to pick values for $t_1,\ldots t_r, u_1,\ldots,u_s$ such that this discriminant is square free and minimal. Then we can use the reduction theory of quadratics (with square free, minimal discriminant) to determine the reduced form for Q_f.

For quadratics T and S in Eq. (14) we define

$$\theta_T = \frac{a_0^2\cdot\Delta_T}{t_1^2\cdots t_r^2}, \qquad \theta_S = \frac{a_0^2\cdot\Delta_S}{u_1^4\cdots u_s^4} \tag{18}$$

Notice that T_r and S_s are given recursively as

$$T_r = T_{r-1} + t_r^2(x-\alpha_r)^2, \qquad S_s = S_{s-1} + u_s^4\left(x^2 - 2a_s x + (a_s^2+b_s^2)\right)$$

The next lemma gives formulas computing the discriminants of T and S.

Lemma 2. *Let T_r and S_s be quadratics given by*

$$T_r(x,1) = \sum_{i=1}^{r} t_i^2(x-\alpha_i)^2, \quad \textit{and} \quad S_s(x,1) = \sum_{j=1}^{s} 2u_j^2(x-\beta_j)(x-\bar{\beta}_j), \tag{19}$$

where $\beta_i = a_i + I\cdot b_i$, for $i = 1,\ldots,s$. Then $T_r \in V^+_{2,\mathbb{R}}$ and $S_s \in V^+_{2,\mathbb{R}}$.

Moreover,

$$\Delta(T_r) = -4\,(t_1^2\cdots t_r^2)\sum_{\substack{i,j=1\\ i\neq j\\ n_l\neq i, n_l\neq j}}^{r}\frac{(\alpha_i-\alpha_j)^2}{t_{n_1}^2\cdots t_{n_l}^2\cdots t_{n_{r-2}}^2} = -4\sum_{i<j}^{r} t_i^2 t_j^2\,(\alpha_i-\alpha_j)^2,$$

$$\Delta(S_s) = -16\left(\sum_{i<j} u_i^2u_j^2\left[(a_i-a_j)^2+(b_i^2+b_j^2)\right]+\sum_{j=1}^{s}u_j^4b_j^2\right). \tag{20}$$

Let $f\in V_{n,\mathbb{R}}$ with signature (r,s) and equation as in Eq. (13). Then Q_f is a positive definite quadratic form with discriminant $\mathfrak{D}_f$ given by the formula

$$\mathfrak{D}_f = \Delta(T_r)+\Delta(S_s)-8\sum_{i,j} t_i^2u_j^2\left((\alpha_i-a_j)^2+b_j^2\right). \tag{21}$$

From the above formula it can be seen that $\mathfrak{D}_f$ is expressed in terms of the root differences. Hence, $\mathfrak{D}_f$ is fixed by all the transpositions of the roots. However, it is not an invariant of the binary form. In order to get an invariant we need to fix it by all symmetries of the roots, hence by an element of order n. It will be seen later that $\mathfrak{D}_f^n$ is an invariant of the binary form f.

The above remark motivates the following definition. We define the θ_0 of a binary form as follows

$$\theta_0(f) = \frac{a_0^2\cdot|\mathfrak{D}_f|^{n/2}}{\prod_{i=1}^r t_i^2\prod_{j=1}^s u_j^4}.$$

Next we continue with the general theory. Consider the function

$$\theta_0(t_1,\ldots,t_r,u_1,\ldots,u_s)$$

as a multivariable function in the variables $t_1,\ldots,t_r,u_1,\ldots,u_s$. We would like to pick these variables such that Q_f is a reduced quadratic, hence $\mathfrak{D}_f$ is minimal. This is equivalent to $\theta_0(t_1,\ldots,t_r,u_1,\ldots,u_s)$ obtaining a minimal value.

Proposition 4. *The function $\theta_0:\mathbb{R}^{r+s}\to\mathbb{R}$ obtains a minimum at a unique point $(\bar{t}_1,\ldots,\bar{t}_r,\bar{u}_1,\ldots,\bar{u}_s)$.*

Proof. Julia in his thesis [23] proves existence and Stoll, and Cremona prove uniqueness in [34]. □

Choosing $(\bar{t}_1,\ldots,\bar{t}_r,\bar{u}_1,\ldots,\bar{u}_s)$ that make θ_0 minimal gives a unique positive definite quadratic $Q_f(X,Z)$. We call this unique quadratic $Q_f(X,Z)$ for such a choice of $(\bar{t}_1,\ldots,\bar{t}_r,\bar{u}_1,\ldots,\bar{u}_s)$ the **Julia quadratic** of $f(X,Z)$, denote it by $\mathcal{J}_f(X,Z)$, and the quantity $\theta_f := \theta_0(\bar{t}_1,\ldots,\bar{t}_r,\bar{u}_1,\ldots,\bar{u}_s)$ the **Julia invariant**. From the previous remarks, this is well defined.

The following lemma shows that θ is an invariant of binary forms and $\mathcal{J}$ a covariant of order 2.

Lemma 3. *Consider $\mathrm{GL}_2(\mathbb{C})$ acting on $V_{n,\mathbb{R}}$. Then θ is an invariant of binary forms and $\mathcal{J}$ is a covariant of order 2.*

We will prove this lemma in the next section for the general case, i.e. for binary forms over $\mathbb{C}$. Next, we make the necessary adjustments such that the above construction will work for binary forms with complex coefficients as well.

Julia's quadratic for binary forms with complex coefficients. Suppose we are given a binary form $f \in V_{n,\mathbb{C}}$ with $f(x,y) = \sum_{i=0}^{n} x^{n-i}y^i$ and assume that $a_0 \neq 0$. Then $f(x,y)$ can be factored as

$$f(x,y) = a_0(y_1x - x_1y)(y_2x - x_2y)\cdots(y_nx - x_ny), \tag{22}$$

for $[x_i, y_i] \in \mathbb{P}^1$, $i = 1, \ldots n$. Construct a quadratic form

(23)

$$\begin{aligned} Q(x,y) &= \sum_{i=1}^{n} t_i^2 \cdot ||y_ix - x_iy||^2 \\ &= \left(\sum_{i=1}^{n} t_i^2||y_i||^2\right) x\bar{x} - \left(\sum_{i=1}^{n} t_i^2 y_i\bar{x}_i\right) x\bar{y} - \left(\sum_{i=1}^{n} t_i^2 x\bar{y}_i\right) \bar{x}y + \left(\sum_{i=1}^{n} t_i^2 \cdot ||x_i||^2\right) y\bar{y} \end{aligned}$$

where t_j are non-zero real numbers that have to be determined. Computing the discriminant of the quadratic $Q(X,Z)$ and simplifying it we get

$$\mathfrak{D}_f = \sum_{1=i<j=n} t_i^2t_j^2 \cdot ||y_ix_j - x_iy_j||^2 = \sum_{1=i<j=n} t_i^2t_j^2 \cdot ||\beta_{ij}||^2. \tag{24}$$

Note that $||\beta_{ij}|| := ||y_ix_j - x_iy_j||$. Since the leading coefficient of Q and $\mathfrak{D}_f$ are both positive then Q is a positive definite quadratic Hermitian form. We define the quantity θ_0 as

$$\theta_0(Q_f) = \frac{||a_0||^2 \cdot \mathfrak{D}_f^{n/2}}{t_1^2 \cdots t_n^2}.$$

Consider θ_0 as a function

$$\begin{aligned} \theta_0 : \mathbb{P}^{n-1}\backslash\{(0,\ldots,0)\} &\to \mathbb{P}^1 \\ (t_1,\ldots,t_n) &\mapsto \theta_0(t_1,\ldots,t_n). \end{aligned}$$

Since this is a function defined on $\mathbb{P}^{n-1}$ then we take its domain to be

$$D = \left\{ (t_1,\ldots,t_n) \in \mathbb{P}^n : \ t_1^2 \cdot t_2^2 \cdots t_n^2 = 1 \right\}.$$

We would like to choose $t_1, \ldots, t_n$ such that Q_f is a reduced quadratic, hence a quadratic with minimal discriminant. Then θ_0 obtains a minimum exactly when $\mathfrak{D}_f$ obtains a minimum, under the assumption $t_1^2 \cdots t_n^2 = 1$. Our next task is to determine in what values for $(t_1, \ldots, t_n)$ this minimum occurs. For simplicity denote by $h = \mathfrak{D}_f$. To find the critical points in the interior of D we need to solve $\nabla_h = 0$, i.e.

$$2t_i \sum_{\substack{j=1 \\ j\neq i}} t_j^2 \cdot ||y_ix_j - x_iy_j||^2 = 0, \qquad i = 1, \ldots n.$$

Note that the only critical point in the interior D° is the tuple $(0, \ldots, 0)$, which is not in the domain.

Next, determine the critical points on the boundary of D. Denote by $g = \prod_{i=1}^{n} t_i^2 = 1$. Using Lagrange multipliers we have to solve the system

$$\begin{cases} \nabla_h = \lambda\nabla_g \\ t_1^2 \cdots t_n^2 = 1 \end{cases}$$

for $\lambda \neq 0$. For convenience denote

$$\boxed{u_i = t_i^2 \quad \textit{and} \quad \alpha_{i,j} = ||\beta_{i,j}||^2 = ||y_ix_j - x_iy_j||^2}$$

and we have

$$\begin{cases} \sum_{\substack{j=1\\ i\neq j}}^{n} u_j \cdot \alpha_{i,j} = \lambda \cdot \prod_{i\neq j} u_j, & i = 1, \dots, n \\ \prod_{i=1}^{n} u_i = 1 \end{cases}$$

or equivalently

$$\begin{cases} u_i \sum_{\substack{j=1\\ i\neq j}}^{n} u_j \cdot \alpha_{i,j} = \lambda \\ \prod_{i=1}^{n} u_i = 1 \end{cases} \tag{25}$$

Summing up the first n-equations of the system in Eq. (25), we get

$$\sum_{\substack{i,j=1\\ i<j}}^{n} u_i\, u_j\, \alpha_{i,j} = n \cdot \lambda \tag{26}$$

Then the left hand side of Eq. (26) is equal to $2 \cdot \mathfrak{D}_f$. Therefore, $2 \cdot \mathfrak{D}_f = n \cdot \lambda$ and $\lambda = \frac{2 \cdot \mathfrak{D}_f}{n}$

$$\lambda = \frac{2}{n} \cdot \sum_{i<j} u_i u_j \alpha_{i,j}. \tag{27}$$

Substituting λ in the system in Eq. (25) we have

$$\begin{cases} n \cdot u_1 \left(u_2\alpha_{1,2} + u_3\alpha_{1,3} + \cdots + u_n\alpha_{1,n}\right) = 2 \cdot \sum_{i<j} u_i u_j \alpha_{i,j} \\ n \cdot u_2 \left(u_1\alpha_{1,2} + u_3\alpha_{2,3} + \cdots + u_n\alpha_{2,n}\right) = 2 \cdot \sum_{i<j} u_i u_j \alpha_{i,j} \\ \vdots \\ n \cdot u_n \left(u_1\alpha_{2,n} + u_3\alpha_{3,n} + \cdots + u_{n-1}\alpha_{n-1,n}\right) = 2 \cdot \sum_{i<j} u_i u_j \alpha_{i,j} \\ u_1 \cdot u_2 \cdots u_n = 1. \end{cases} \tag{28}$$

Consider the first row. We have

$$\begin{aligned} u_1u_2\alpha_{1,2} + u_1u_3\alpha_{1,3} + \cdots + u_1u_n\alpha_{1,n} = \frac{2}{n} \cdot (&u_1u_2\alpha_{1,2} + \cdots + u_1u_n\alpha_{1,n} + \\ &u_2u_3\alpha_{2,3} + \cdots + u_2u_n\alpha_{2,n} + \\ &\vdots \\ &+ u_{n-1}u_n\alpha_{n-1,n}) \end{aligned}$$

and combining like terms we have

$$\begin{aligned} (n-2)(u_1u_2\alpha_{1,2} + u_1u_3\alpha_{1,3} + \cdots + u_1u_n\alpha_{1,n}) = 2 \cdot (&u_2u_3\alpha_{2,3} + \cdots + u_2u_n\alpha_{2,n} + \\ &u_3u_4\alpha_{3,4} + \cdots + u_3u_n\alpha_{2,n} + \\ &\vdots \\ &+ u_{n-1}u_n\alpha_{n-1,n}). \end{aligned}$$

The i'th row for $i = 1, \dots, n$ will look like

$$(n-2) \cdot \sum_{i<j} u_i u_j \alpha_{i,j} = 2 \cdot \sum_{\substack{l<k\\ l,k\neq i}} u_l u_k \alpha_{l,k}. \tag{29}$$

Remark 1. *We can make the substitution $\gamma_{i,j} = u_i u_j \alpha_{i,j}$, since in the formula for the Julia invariant these are the terms that appear. Then the system becomes a linear system with n equations and $\binom{n}{2}$ variables. Obviously $n = \binom{n}{2}$, when $n = 3$. Hence, the case of cubics is very easy.*

Let V be the variety defined by the Eq. (28). We have the following result.

Theorem 7. *V is a zero dimensional variety over $\mathbb{C}$. Moreover, V has exactly one real point given by*

$$u_i = \frac{2}{n} \cdot \frac{t^2}{(||z - \alpha_i||^2 + t^2)},$$

where t and z satisfy the following system

$$\begin{cases} \displaystyle\sum_{j=1}^{n} \frac{t^2}{||z - \alpha_j||^2 + t^2} = \frac{n}{2} \\ \displaystyle\sum_{j=1}^{n} \frac{z - \alpha_j}{||z - \alpha_j||^2 + t^2} = 0 \end{cases} \tag{30}$$

Proof. A solution to the Eq. (28) determines the Julia quadratic and therefore a point in $\mathcal{H}_3$. Let $(z, t) \in \mathcal{H}_3$ be such a point. The quadratic associated to (z, t) is equal to the Julia quadratic as in Eq. (23). Hence,

$$Q(x, y) = S\left(|x + zy|^2 + t|y|^2\right)$$

where

$$S = \sum_{i=1}^{n} t_i^2, \quad Sz = \sum_{i=1}^{n} \alpha_i t_i^2, \quad S(||z||^2 + t^2) = \sum_{i=1}^{n} ||\alpha_i||^2 t_i^2$$

and $\frac{1}{4}\mathfrak{D}_f = S^2 t^2$. Consider Eq. (25). Note that

$$\sum_{j=1}^{n} u_j \alpha_{i,j} = S(||z - \alpha_i||^2 + t^2)$$

because

$$\begin{aligned} \sum_{j=1}^{n} u_j \alpha_{i,j} &= \sum_{j=1}^{n} u_j ||\alpha_i - \alpha_j||^2 = \sum_{j=1}^{n} u_j \left(||\alpha_i||^2 - \alpha_i \bar{\alpha}_j - \bar{\alpha}_i \alpha_j + ||\alpha_j||^2\right) \\ &= ||\alpha_i||^2 \sum_{j=1}^{n} u_j - \alpha_i \sum_{j=1}^{n} u_j \bar{\alpha}_j - \bar{\alpha}_i \sum_{j=1}^{n} u_j \alpha_j + \sum_{j=1}^{n} u_j ||\alpha_j||^2 \\ &= ||\alpha_i||^2 \cdot S - \alpha_i \cdot \bar{z} S - \bar{\alpha}_i \cdot z S + S(||z||^2 + t^2) \\ &= S\left(||\alpha_i||^2 - \alpha_i \cdot \bar{z} - \bar{\alpha}_i \cdot z + ||z||^2\right) + St^2 = S\left(||z - \alpha_i||^2 + t^2\right). \end{aligned}$$

Hence, the system in Eq. (25) becomes

$$\begin{cases} u_1 \cdot S(||z - \alpha_1||^2 + t^2) = \lambda \\ u_2 \cdot S(||z - \alpha_2||^2 + t^2) = \lambda \\ \vdots \\ u_n \cdot S(||z - \alpha_n||^2 + t^2) = \lambda \\ u_1 \cdot u_2 \cdots u_n = 1. \end{cases} \tag{31}$$

Since $2\mathfrak{D}_f = n\lambda$, we have $\lambda = \frac{2S^2t^2}{n}$ and

$$u_i = \frac{2}{n} \cdot \frac{S^2t^2}{S(||z-\alpha_i||^2 + t^2)},$$

for each $i = 1, \ldots, n$. We can assume that $S = 1$ and take the Julia quadratic to be a monic. Then

$$u_i = \frac{2}{n} \cdot \frac{t^2}{(||z-\alpha_i||^2 + t^2)}.$$

Since $S = \sum_{i=1}^n t_i^2$ and $Sz = \sum_{i=1}^n \alpha_i t_i^2$, the system in Eq. (28) becomes as follows

$$\begin{cases} \displaystyle\sum_{j=1}^n \frac{t^2}{||z-\alpha_j||^2 + t^2} = \frac{n}{2} \\ \displaystyle\sum_{j=1}^n \frac{z-\alpha_j}{||z-\alpha_j||^2 + t^2} = 0. \end{cases} \tag{32}$$

To prove the theorem it is enough to show that this system has a unique solution (z,t) for $z \in \mathbb{C}$, and $t \in \mathbb{R}^+$. We make the convenient substitution $t^2 = \bar{t}$. We have two equations of degree $2n$ and $2n-1$ in z and of degree n and $n-1$ in t, as displayed below:

$$F_1(\bar{t}, u) = 0 \quad \text{and} \quad F_2(\bar{t}, u) = 0 \tag{33}$$

By Prop. Prop. 4 this has a unique positive real root which is t. □

Let $(\bar{u}_1, \ldots, \bar{u}_n) \in \mathbb{R}^n$ be the unique real point of V. From now on by θ_f we will denote the function θ_0 evaluated at this unique point. The quadratic $Q(f)$ for the above values $(\bar{u}_1, \ldots, \bar{u}_n)$ will be denoted by $\mathcal{J}_f$ and is called **Julia's quadratic**.

Lemma 4. *Let* $\mathrm{GL}_2(\mathbb{C})$ *act on* $V_{n,\mathbb{C}}$. *Then the following are true:*
i) θ_f *is an invariant*
ii) $\mathfrak{D}_f^n$ *is an invariant.*

Proof. Let $f \in V_{n,\mathbb{C}}$ be a binary form which is factored over $\mathbb{C}$ as follows

$$f(x,y) = \prod_{i=1}^n (x - \alpha_i y).$$

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$ act on f as follows

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}.$$

The roots of f^M are respectively $\gamma_i = M^{-1}\alpha_i$. Assume first that none of the roots of f go to infinity under M. Then the substitution for $(x - \alpha_i y)$ is

$$ax_1 + by_1 - \frac{a\gamma_i + b}{c\gamma_i + d} \cdot (cx_1 + dy_1) = (a - c\alpha_i)(x_1 - \gamma_i y_1).$$

Therefore,

$$f(ax_1 + by_1, cx_1 + dy_1) = A_0 \prod_{i=1}^n (x_1 - \gamma_i y_1)$$

where

$$A_0 = a_0 \prod_{i=1}^{n} (a - \alpha_i c). \tag{34}$$

Acting by the same matrix M on the positive definite binary quadratic Q_f associated to f we get

$$Q_f^M = \sum_{i=1}^{r} \tau_i^2 (x_1 - \gamma_i y_1)^2$$

where τ_i^2 is given as follows

$$\tau_i^2 = t_i^2 (a - \alpha_i c)^2.$$

Recall that $\mathfrak{D}_f := \Delta(Q_f)$, and when we act on a binary quadratic form by a matrix M, with $\det(M) = \lambda$, the determinant is fixed. Then

$$\theta_0(f^M) = \frac{A_0^2 \sqrt{\mathfrak{D}_{f^M}^n}}{\prod_{i=1}^n \tau_i^2} = \frac{\left[a_0 \prod_{i=1}^n (a - \alpha_i c)\right]^2 \cdot \sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^n t_i^2 (a - \alpha_i c)^2} = \frac{a_0^2 \cdot \sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^n t_i^2} = \theta_0(f).$$

Now, assume the first p real roots of $f(x, y)$ are equal to $\frac{a}{c}$, i.e. the first p-real roots of f go to infinity under M. Then the substitution for $(x - \alpha_i y)$ for $i = 1, \cdots, p$ becomes

$$ax_1 + by_1 - \frac{a}{c}(cx_1 + dy_1) = -\frac{y_1}{c}.$$

Hence,

$$F(ax_1 + by_1, cx_1 + dy_1) = A_0 \cdot y_1^p \prod_{i=1}^{n} (x_1 - \gamma_i y_1)$$

where

$$A_0 = \frac{(-1)^p}{c^p} \cdot a_0 \prod_{i=p+1}^{n} (a - \alpha_i c).$$

The positive definite binary quadratic form associated to $f(x_1, y_1)$ is

$$Q_f^M = \sum_{i=1}^{p} \tau_i^2 y_1^2 + \sum_{i=p+1}^{n} \tau_i^2 (x_1 - \gamma_i y_1)^2$$

where

$$\tau_i^2 = \begin{cases} \frac{t_i^2}{c^2} & i = 1, \cdots, p \\ t_i^2 (a - \alpha_i c)^2 & i = p+1, \cdots, n. \end{cases}$$

By calculating the Julia invariant of $f(x_1, y_1)$ and simplifying it we get

$$\begin{aligned} \theta_0(f^M) &= \frac{A_0^2 \sqrt{\mathfrak{D}_{f^M}^n}}{\prod_{i=1}^n \tau_i^2} \\ &= \frac{\left(\frac{(-1)^p}{c^p} \cdot a_0 \prod_{i=p+1}^n (a - \alpha_i c)\right)^2 \cdot \sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^p \frac{t_i^2}{c^2} \prod_{i=p+1}^n t_i^2 (a - \alpha_i c)^2} = \frac{a_0^2 \cdot \sqrt{\mathfrak{D}_f^n}}{\prod_{i=1}^n t_i^2} = \theta_0(f). \end{aligned}$$

Thus, $\theta_0(f^M) = \theta_0(f)$ and therefore θ_0 is an invariant. Part ii) is a direct consequence of the definition of θ. □

Corollary 3. *Let $f \in V_{n,\mathbb{C}}$ and F_f its field of moduli. Then,*

i) $\theta_f \in F_f$.

ii) $a_0^4 \mathfrak{D}_f^n \in F_f(\theta_f^2)$.

Proof. It is by definition that $\theta_f \in F_f$ and $\mathcal{J}_f$ has coefficients in $F_f[x, y]$. Part iii) is a consequence of the definition of θ_f. □

Problem 1. *An open question is to express θ in terms of generators of the rings of invariants for degree n binary forms or absolute invariants of f which determine the field of moduli of f.*

5.2. **Reducing binary forms of higher degree.** In this section we will describe reduction theory of higher degree binary forms. First, we will explain the case of binary forms with real coefficients and then its generalization to binary forms with complex coefficients.

Binary forms with real coefficients. To any form $f \in V_{n,\mathbb{R}}$ we associate a positive definite quadratic $\mathcal{J}_f \in V^+_{2,\mathbb{R}}$ as showed above. In Section 4 we proved that binary quadratic forms in $V^+_{2,\mathbb{R}}$ are in one-to-one correspondence with points in the upper half plane $\mathcal{H}_2$. Hence, we have the following maps

$$\begin{aligned} \zeta : V_{n,\mathbb{R}} &\to V^+_{2,\mathbb{R}} \to \mathcal{H}_2 \\ f &\mapsto \mathcal{J}_f \mapsto \xi(\mathcal{J}_f). \end{aligned}$$

We call this map the **zero map** and denote it by $\zeta(f) := \xi(\mathcal{J}_f)$. The map $\zeta : V_{n,\mathbb{R}} \to \mathcal{H}_2$ is $\mathrm{SL}_2(\mathbb{R})$-equivariant.

The proof of the above is easy and it will be proved in the next subsection for the more general case, i.e. binary forms with complex coefficients. A binary form $f \in V_{n,\mathbb{R}}$ is **reduced** if $\zeta(f) \in \mathcal{F}_2$. Next, we will adapt this to binary forms with complex coefficients.

Binary forms with complex coefficients. For any form $f \in V_{n,\mathbb{C}}$ the corresponding Julia quadratic is a positive definite Hermitian form. Previously we proved that binary quadratic forms in $\mathrm{Her}^+(\mathbb{C})$ are in a one-to-one correspondence with points in $\mathcal{H}_3$. Hence, we have the maps:

$$\begin{aligned} \zeta : V_{n,\mathbb{C}} &\longrightarrow \mathrm{Her}^+(\mathbb{C}) \longrightarrow \mathcal{H}_3 \\ f &\mapsto \mathcal{J}_f \mapsto \xi(\mathcal{J}_f) \end{aligned}$$

where ξ is as defined in Eq. (12). Note that $\xi(\mathcal{J}_f)$ is the point in $\mathcal{H}_3$ associated to the Hermitian form $\mathcal{J}_f$.

Lemma 5. *The map $j : V_{n,\mathbb{C}} \longrightarrow \mathrm{Her}^+(\mathbb{C})$ is an $\mathrm{SL}_2(\mathbb{C})$-equivariant map, i.e. for every $f \in V_{n,\mathbb{C}}$, $H \in \mathrm{Her}^+(\mathbb{C})$ and $M \in \mathrm{SL}_2(\mathbb{C})$ we have $j(f^M) = j(f)^M$ which is equivalent to saying $H_{f^M} = H_f^M$.*

Proof. We will prove it only for the generators of $\mathrm{SL}_2(\mathbb{C})$, i.e. for $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ where $m \in \mathbb{C}$. First, for $f \in V_{n,\mathbb{C}}$ such that

$$f = a_0(x - \alpha_1 y) \cdots (x - \alpha_n y)$$

and $H \in \mathrm{Her}^+(\mathbb{C})$ we want to prove that $H_{f^S} = H_f^S$. We have

$$f^S = A_0(x - \gamma_1 y) \cdots (x - \gamma_n y)$$

where $A_0 = a_0\alpha_i^n$ and $\gamma_i = -\frac{1}{\alpha_i}$.

The binary quadratic Hermitian form associated to f^S is

$$H_{f^S} = \sum \tau_i^2 ||x - \gamma_i y||^2.$$

On the other side,

$$\begin{aligned} H_f^S &= \sum t_i^2 ||y - \alpha_i(-x)||^2 = \sum t_i^2 \left|\left|\alpha_i \left(x - \frac{y}{-\alpha_i}\right)\right|\right|^2 \\ &= \sum t_i^2 ||\alpha_i||^2 ||x - \gamma_i y||^2. \end{aligned}$$

Notice that for $\tau_i^2 = t_i^2 ||\alpha_i||^2$, we have that $H_f^S = H_{f^S}$. Now let us show $H_{f^T} = H_f^T$. For $f = a_0(x - \alpha_1 y) \cdots (x - \alpha_n y)$ and T as above we have

$$f^T = A_0(x - \gamma_1 y) \cdots (x - \gamma_n y)$$

where $A_0 = a_0$ and $\gamma_i = \alpha_i - m$. The binary quadratic Hermitian form associated to f^T is

$$H_{f^T} = \sum \tau_i^2 ||x - \gamma_i y||^2.$$

On the other side,

$$H_f^T = \sum t_i^2 ||x + my - \alpha_i y||^2 = \sum t_i^2 ||x - (\alpha_i - m)y||^2 = \sum t_i^2 ||x - \gamma_i y||^2.$$

Hence, for $\tau_i^2 = t_i^2$ we have $H_f^T = H_{f^T}$ and we are done. □

The map $\zeta : V_{n,\mathbb{C}} \to \mathcal{H}_3$ is $\mathrm{SL}_2(\mathbb{C})$-equivariant.

Let K be a field of definition of f. Without loss of generality assume that f has an integral model over $\mathcal{O}_K$. We call $f(x, y)$ to be **reduced** over K if $\zeta(f)$ is in a fixed fundamental domain for the action of Γ_K on $\mathcal{H}_3$, when such a fundamental domain exists.

Definition 4. *Let $f \in V_{n,\mathbb{C}}$ be such that it has an integral model over some algebraic number field K. We say $f(x, y)$ is reduced if $\zeta(f)$ is in a fixed fundamental domain for the action of $\mathrm{SL}_2(\mathcal{O}_K)$ on $\mathcal{H}_3$, when such a domain exists.*

Let f be a given degree n binary form. To find the reduced form in its $\mathrm{SL}_2(\mathcal{O}_K)$-orbit we compute $\zeta(f)$. If $\zeta(f)$ is in the fundamental domain $\mathcal{F}_{\mathcal{O}_K}$ we are done, the given form is the reduced one. Otherwise, compute $M \in \Gamma_{\mathcal{O}_K}$ such that $\zeta(f)^M \in \mathcal{F}_{\mathcal{O}_K}$ and $f^{M^{-1}}$ is the reduced form in its $\mathrm{SL}_2(\mathcal{O}_K)$-orbit.

A natural question to ask is the following; Does the reduced binary form computed this way have minimal height in its $\mathrm{SL}_2(\mathcal{O}_K)$-orbit? We will address this question in the remainder of this section.

Consider f a degree n binary form and K its minimal field of definition. Let $M \in \mathrm{SL}_2(\mathcal{O}_K)$ be a matrix such that f^M is reduced, i.e. $\bar{\xi}(f^M) \in \mathcal{F}_K$ where $\mathcal{F}_K$ is the fundamental domain of $\mathrm{SL}_2(\mathcal{O}_K)$ acting on $\mathcal{H}_3$.

First we give a bound on the height of the reduced binary form with respect to the Julia invariant.

Lemma 6. *Let f be a binary form with signature $(n, 0)$ factored as follows*

$$f(x, 1) = a_0 \prod_{i=1}^{n} (x - \alpha_i)$$

Then the height of this form can be bounded by Julia's invariant as

$$\mathrm{H}(f) \leq c \cdot \theta_f^{n/2}$$

where

$$c = \left(\frac{1}{3}\right)^{\frac{n^2}{4}} \left(\frac{4}{n-1}\right)^{\frac{n(n-1)}{2}} \frac{1}{a_0^n}$$

Proof. Let f be the reduced form given as above. It is easy to prove that the roots of the binary form can be bounded by the Julia invariant θ as follows

$$||\alpha_i||^2 \leq \frac{4^{n-1}}{(n-1)^{n-1}\, 3^{n/2}} \cdot \frac{1}{a_0^2} \cdot \theta_f,$$

see [23] for more details how to get this bound. Then the symmetric polynomials can be bounded as follows

$$\begin{aligned} s_r = \sum_{i=1}^{\binom{n}{r}} \alpha_i \cdots \alpha_r &\leq \binom{n}{r} \left(\sqrt{\frac{4^{n-1}}{(n-1)^{n-1}\, 3^{n/2}} \cdot \frac{1}{a_0^2} \cdot \theta_f} \right)^r \\ &\leq \binom{n}{r} \cdot \frac{1}{a_0^r} \cdot \sqrt{\frac{4^{r(n-1)}}{(n-1)^{r(n-1)}\, 3^{rn/2}}} \cdot \theta_f^{n/2} \end{aligned}$$

Hence, since the symmetric polynomials represent the coefficient of the binary form we have that

$$\mathrm{H}(f) \leq \binom{n}{r} \left(\frac{1}{3}\right)^{\frac{rn}{4}} \left(\frac{4}{n-1}\right)^{\frac{r(n-1)}{2}} \frac{1}{a_0^r} \cdot \theta_f^{n/2}$$

for all $r = 1, \ldots, n$. Hence, $\mathrm{H}(f) \leq c \cdot \theta_f^{n//2}$ for all $r = 1, \ldots, n$ and θ_f is minimal. Consider the function

$$f(n, r) = \binom{n}{r} \left(\frac{1}{3}\right)^{\frac{rn}{4}} \left(\frac{4}{n-1}\right)^{\frac{r(n-1)}{2}} \frac{1}{a_0^r}$$

We want to check if this is a decreasing or increasing function with respect to n

$$\begin{aligned} \frac{f(n+1,r)}{f(n,r)} &= \frac{\binom{n+1}{r} \left(\frac{1}{3}\right)^{\frac{(n+1)r}{4}} \left(\frac{4}{n-1}\right)^{\frac{rn}{2}} \frac{1}{a_0^r}}{\binom{n}{r} \left(\frac{1}{3}\right)^{\frac{rn}{4}} \left(\frac{4}{n-1}\right)^{\frac{r(n-1)}{2}} \frac{1}{a_0^r}} = \frac{\binom{n+1}{r}}{\binom{n}{r}} \left(\frac{1}{3}\right)^{\frac{r}{4}} \left(\frac{4}{n-1}\right)^{\frac{r}{2}} \\ &= \frac{n+1}{n+r-1} \left(\frac{1}{3}\right)^{\frac{r}{4}} \left(\frac{4}{n-1}\right)^{\frac{r}{2}} = \frac{n+1}{n+r-1}\, 2^r \left(\frac{1}{n-1}\right)^{\frac{r}{2}} \left(\frac{1}{3}\right)^{\frac{r}{4}} \end{aligned}$$

Since $n \geq 3$ and $r = 1, \ldots, n$ we have that $\frac{f(n+1,r)}{f(n,r)} > 1$. Hence, $f(n, r)$ is an increasing function and the above bound becomes

$$\mathrm{H}(f) \leq \left(\frac{1}{3}\right)^{\frac{n^2}{4}} \left(\frac{4}{n-1}\right)^{\frac{n(n-1)}{2}} \frac{1}{a_0^n} \cdot \theta_f^{n/2}.$$

This completes the proof. □

In the following remark we will see that for binary cubics it is possible to express this bound in terms of the discriminant of the cubic and then we compare this bound with bounds obtained in [18].

Remark 2. *If we consider a binary cubic with signature* $(3, 0)$ *then from Lem. 6 we have*

$$\mathrm{H}(f) \leq 2^3 \left(\frac{1}{3}\right)^{\frac{9}{4}} \frac{1}{a_0^3} \cdot \theta_f^{3/2}$$

Moreover, $\theta_f = a_0^6\, 3^{\frac{3}{2}}\ |\Delta_f|^{\frac{1}{2}}$, *(cf. Lem. 10). We can express the above bound in terms of the discriminant of the binary form* f

$$\mathrm{H}(f) \leq 2^3\, a_0^6\ \cdot |\Delta_f|^{3/4}.$$

In [18, Thm 2, pg 162] *it is proved that for a binary form* f

$$\mathrm{H}(f) \leq C \cdot |\Delta_f|^{\frac{21}{2}},$$

where C *is some constant.*

The results in [18] are in line with previous results of the author and his collaborators in bounding the height of the binary forms in terms of the discriminants. There are many results comparing the height $\mathrm{H}(f)$ and Δ_f by many authors, including Mordell [28], Lewis [26], Mahler [27], Györy [20], Birch [9], Bombieri [10], and others.

5.3. **The minimal absolute height of binary forms.** Let K be a number field and $\mathcal{O}_K$ its ring of integers. We want to develop a reduction theory in the following sense: given a binary form $f(x, y)$ over $\mathcal{O}_K$ we determine its integral model with minimal height $\mathrm{H}(f)$ over $\overline{K}$.

Lemma 7. *Let* f *and* g *be two binary forms of degree* n *and* M *a matrix in* $\mathrm{SL}_2(\mathcal{O}_K)$ *such that* $g = f^M$. *Associate to these binary forms* f *and* g *respectively the Julia quadratics* $\mathcal{J}_f$ *and* $\mathcal{J}_g$. *Then the following holds:*

i) $\mathcal{J}_g = \mathcal{J}_f^M$

ii) $\Delta_{\mathcal{J}_f} = \Delta_{\mathcal{J}_g}$

Proof. The proof is trivial. Part i) follows directly from Lem. 5 and part ii) is true since we are acting with a matrix of discriminant one. □

Hence, the discriminant $\mathfrak{D}_f$ of the Julia quadratic is an invariant of the binary form. An interesting problem to consider would be to express $\mathfrak{D}_f$ in terms of the generators of the invariant ring $\mathcal{R}_n$.

The following theorem gives us a method to find the form with minimal height among all $\mathrm{SL}_2(\mathcal{O}_K)$-orbits.

Theorem 8. *Let* f *be a degree* n *binary form defined over* K *and* $\mathcal{J}_f$ *its Julia quadratic,* $\mathfrak{D}_f$ *its discriminant, and* $L = K(\mathfrak{D}_f)$. *Then* $[L : K] \leq n$. *Let* r *be the class number of* $\mathcal{J}_f$ *over* L *and* $M_1, \ldots, M_r$ *the matrices with entries in* $\mathrm{SL}_2(\mathcal{O}_K)$ *that send* $\mathcal{J}_f$ *respectively to* $\{J_1, \ldots, J_r\}$. *The form* f^{M_j} *for some* $j = 1, \ldots, r$ *has minimal height over* $\mathrm{SL}_2(\mathcal{O}_K)$.

Proof. Let $\mathfrak{D}_f = \Delta_{\mathcal{J}_f}$ be the discriminant of the Julia quadratic associated to the degree n binary form. From Cor. Cor. 2 for any $\Delta \in \mathcal{O}_L$ with $\Delta \neq 0$ the set $V_{2,\mathcal{O}_L}(\Delta)$, i.e. the set of binary quadratics with that fixed discriminant, splits into finitely many $\mathrm{SL}_2(\mathcal{O}_L)$-orbits. Assume r is the class number of $\mathcal{J}_f$ over L and $\{J_1, \ldots, J_r\}$ are representative reduced quadratics of each of these orbits. Let

$$\{M_1, \ldots, M_r\} \in \mathrm{SL}_2(\mathcal{O}_L) \ \text{ such that } \ \mathcal{J}_f^{M_i} = J_i.$$

Act with the same matrices on the form f to get $f^{M_1}, \ldots, f^{M_r}$, these are well defined from Lem. 7. The form with minimal height over all $\mathrm{SL}_2(\mathcal{O}_L)$-orbits will be the one with smallest height among $\{f^{M_1}, \ldots, f^{M_r}\}$. This way we are finding the "best" binary form amongst all $\mathrm{SL}_2(\mathcal{O}_L)$-orbits. □

Once we find the "best" binary form amongst all $\mathrm{SL}_2(\mathcal{O}_L)$-orbits we can lower the height of the reduced form if we consider diagonal matrices with entries in $\mathcal{O}_K$. This is done as follows. Let f be a reduced form of degree $n \geq 3$ given by

$$f = a_n x^n + \cdots + a_0 y^n,$$

where $a_0, \ldots, a_n \in \mathcal{O}_K$. Consider $M = \mathrm{diag}\ (\alpha, \beta)$ the diagonal matrix with $\alpha, \beta \in \mathcal{O}_K$. Hence, $f^M = (\alpha x, \beta y)$.

Consider $f(\alpha x, y)$. The height $\mathrm{H}(f)$ can be lowered only if all coefficients of $f(\alpha x, y)$ have a common factor. Hence, we must choose α such that $\alpha \,|\, a_0$.

By the same argument, we choose β such that $\beta \,|\, a_n$. Obviously there are only finitely many choices for $M = \mathrm{diag}\ (\alpha, \beta)$. Among all such choices we choose M that gives the smallest height. Obviously, $M \notin \mathrm{SL}_2(\mathcal{O}_K)$ therefore acting with M on the reduced form will lower the height. Hence, we have the following:

Theorem 9. *Let $f = \sum_{i=0}^{n} a_i x^i y^{n-i}$ be a reduced binary form. Choose $M = \mathrm{diag}\ (\alpha, \beta)$ such that $\alpha \,|\, a_0$ and $\beta \,|\, a_n$ and*

$$\mathrm{H}(f^M) = \min\left\{\mathrm{H}\left(f^{\mathit{diag}\ (\alpha,\beta)}\right)\right\}$$

Then $\mathrm{H}(f^M) < \mathrm{H}(f)$.

Proof. Let $f = \sum_{i=0}^{n} a_i x^i y^{n-i}$ be a reduced binary form. Pick α and β such that $\alpha \,|\, a_0$ and $\beta \,|\, a_n$. Then

$$f(\alpha x, \beta y) = \sum_{i=0}^{n} a_i \alpha^i \beta^{n-i}\, x^i y^{n-i}$$

The content of this new polynomial is $\gcd(a_0, a_1\alpha\beta^{n-1}, \ldots, a_n\alpha^n)$. We choose the form with the smallest height among all primitives of $f(\alpha x, \beta y)$, where α, β are as above. □

5.4. **An algorithm to find the minimum absolute height.** We put everything together in the following algorithm, which finds the form with minimal height among all $\mathrm{GL}_2(\mathcal{O}_K)$-orbits is as follows.

ALGORITHM: Computing the binary form with minimal absolute height.

Input: A degree n binary form $f(x, y) \in V_{n,\mathcal{O}_K}$
Output: A binary form $F \in V_{n,\mathcal{O}_K}$ which is $\mathrm{GL}_2(\bar{K})$-equivalent to f and has minimal absolute height.

STEP 1: Compute the Julia quadratic $\mathcal{J}_f$ associated to the binary form f, as explained in Eq. (5.1).
STEP 2: Compute the zero map $\xi(\mathcal{J}_f) \in \mathcal{H}$, using Eq. (12).
STEP 3: Find the matrix A such that $\xi(\mathcal{J}_f)^{A^{-1}} \in \mathcal{F}_{\mathcal{O}_K}$.
STEP 4: Assign $f := \mathbf{red}\ (f) = f^A$ and $J := J_f^{A^{-1}}$.
STEP 5: Compute the discriminant $\mathfrak{D}_f$ of the quadratic form J.
STEP 6: Let $L := K(\mathfrak{D}_f)$ and $h_L(\mathcal{J}) := r$ be the class number of J over L.
STEP 7: Determine all quadratics $\{J_1, \ldots, J_r\}$ equivalent to J over L and let $M_1, \ldots, M_r \in \mathrm{GL}_2(L)$ be the matrices such that $J = J_i^{M_i}$, for $i = 1, \ldots, r$.
STEP 8: Compute the set of forms

$$f_1 := f^{M_1}, \ldots, f_r := f^{M_r}.$$

STEP 9: For each $i = 1, \dots, r$, repeat steps 1-4 to compute **red** (f_i).
STEP 10: For each $j = 1, \dots, r$ and $f_j = \sum_{i=0}^{n} a_i x^i y^{n-i}$ do the following:
Choose $M = \text{diag}\ (\alpha, \beta)$ such that $\alpha \,|\, a_0$ and $\beta \,|\, a_n$ and pick
$g_j := f^{\text{diag}\ (\alpha,\beta)}$ such that

$$\mathrm{H}(f^M) = \min\left\{\mathrm{H}\left(f^{\text{diag}\ (\alpha,\beta)}\right)\right\}$$

is minimal.

STEP 11: Pick the form $F \in V_{n,\mathcal{O}_K}$ with smallest height among $g_1, \dots, g_r$.
Return F

Next we highlight a few remarks about the efficiency of the algorithm.

Remark 3. 1) *For practical purposes computing $\zeta(f)$ numerically is satisfactory since we can find $A \in \Gamma$ such that $\zeta(f)^A \in \mathcal{F}$. Hence, the algorithm can be made rather efficient.*

2) *The reduced form **red** (f) has smaller coefficients and expected minimal height in its Γ-orbit.*

6. Computational aspects of reduction theory

In this section we explore some of the computational aspects of computing the Julia invariant and performing the reduction algorithm for higher degree binary forms. In this first section we give a brief description of the geometric aspects of the zero map and show that $\xi(f)$ corresponds to the centroid of a convex polygon determined by the roots, when to every root α_i we assign the weight t_i from the definition of the Julia quadratic as in Section 5. In the following sections we study forms with signature $(r, 0)$ and $(0, s)$ and compute the Julia quadratic for forms with degree $n = 3, 4, 5, 6$.

6.1. **Geometric interpretation of the zero map.** One approach to find the unique point (z, t) in the upper half space that makes θ minimal is solving the system given in Eq. (32). There is also another approach to find this point, a geometric approach. This is equivalent to finding the centroid of a convex polyhedron and weighted vertices. Julia in his thesis [23] solved the optimization problem geometrically for the case of binary cubics and quartics. He explicitly found $(t_1^2, \dots, t_n^2)$, hence (z, t), for all possible signatures of binary cubics and quartics.

In this section, we will describe briefly this geometric approach and show how it generalizes to solving the optimization problem for higher degree binary forms. We will consider separately the case of binary forms with real and complex coefficients.

Binary forms with real coefficients. Let $f(x, 1)$ be a degree n binary form with real coefficients and signature (r, s), i.e. $\alpha_1, \dots, \alpha_r$ its real roots and $\beta_1, \bar{\beta}_1, \dots, \beta_s, \bar{\beta}_s$ its complex. Associate to it the quadratic

$$Q(x, 1) = \sum_{i=1}^{r} t_i^2 \cdot (x - \alpha_i)^2 + \sum_{i=1}^{s} 2u_i^2 \cdot (x - \beta_i)(x - \bar{\beta}_i)$$

where the t_i's and u_i's are nonzero real numbers that make the Julia invariant θ_0 minimal.

Let A_i be the zero of the quadratic $(x - \alpha_i)^2$ and B_i the point in the upper half space representing the quadratic $(x - \beta_i)(x - \bar{\beta}_i)$. Then $A_1, \dots, A_r$ are the points on the real line with their x-coordinate equal to $\alpha_1, \dots, \alpha_r$ and $B_1, \dots, B_s$

are points in the upper half plane with coordinates $(\mathrm{Re}(\beta_i), \mathrm{Im}(\beta_i))$. Attach to the $A_1, \ldots, A_r$, $B_1, \ldots, B_s$ respectively the weights $t_1^2, \ldots, t_r^2, 2u_1^2, \ldots, 2u_s^2$. Construct the smallest convex polygon which contains on its boundary or its interior the A_i's together with their respective masses. This polygon obtained this way by the roots of the forms will be called the polygon associated to the form f. Then the following is true.

Lemma 8. *The zero map $\zeta : V_{n,\mathbb{R}} \to \mathcal{H}_2$, as in Eq. (9), maps the binary form $f \in V_{n,\mathbb{R}}$ to the centroid of the polygon $A_1, \ldots, A_r, B_1, \ldots, B_s$ weighted respectively by $t_1^2, \ldots, t_r^2, 2u_1^2, \ldots, 2u_s^2$.*

Proof. Let $f \in V_{n,\mathbb{R}}$ be a binary form and $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ be its roots, then the quadratic associated to f is given as $Q(x,1) = Ax^2 - 2Bx + C$ where

$$\begin{aligned} A &= \sum_{i=1}^{r} t_i^2 + \sum_{i=1}^{s} 2u_i^2, \\ B &= \sum_{i=1}^{r} t_i^2 \alpha_i + \sum_{i=1}^{s} 2u_i^2 (\beta_i + \bar{\beta}_i), \\ C &= \sum_{i=1}^{r} t_i^2 \alpha_i^2 + \sum_{i=1}^{s} 2u_i^2 \beta_i \bar{\beta}_i \end{aligned} \tag{35}$$

are as computed in Eq. (23). By Eq. (12) the root in the upper half plane of this quadratic is

$$\xi(f) = -\frac{B}{2A} + \frac{\sqrt{|\mathfrak{D}_f|}}{2A} \cdot i.$$

Given as a point $z = (x, y) \in \mathcal{H}_2$ we have that

$$x = \frac{\sum_{i=1}^{r} t_i^2 \alpha_i + \sum_{i=1}^{s} 2u_i^2 (\beta_i + \bar{\beta}_i)}{\sum_{i=1}^{r} t_i^2 + \sum_{i=1}^{s} 2u_i^2}$$

and

$$||z||^2 = \frac{\sum_{i=1}^{r} t_i^2 \alpha_i^2 + \sum_{i=1}^{s} 2u_i^2 \beta_i \cdot \bar{\beta}_i}{\sum_{i=1}^{r} t_i^2 + \sum_{i=1}^{s} 2u_i^2}.$$

On the other side the centroid C_P of the convex polygon is

$$C_P = \frac{\sum_{i=1}^{r} t_i^2 A_i + \sum_{i=1}^{s} 2u_i^2 B_i}{\sum_{i=1}^{r} t_i^2 + \sum_{i=1}^{s} 2u_i^2}.$$

It is easy to prove that the real coordinate and the distance from the origin of the centroid C_P agrees respectively with x, and $||z||$ as computed above. This completes the proof. □

The following problems are interesting to consider.

Problem 2. *Let P_n be the polygon associated to a degree n binary form as explained above. Let $A_1, \ldots, A_r, B_1, \ldots, B_s$, such that $r + 2s = n$ be the vertices of the polygon with masses $w_1, \ldots, w_n$ respectively. Find $w_1, \ldots, w_n$ such that the quantity $\sum_{1=i<j=n} w_i w_j (\alpha_i - \alpha_j)^2$ is minimal.*

Problem 3. *Let $f \in V_{n,\mathbb{R}}$ be a binary form, $\alpha_1, \ldots, \alpha_r$ its real roots and $\beta_1, \ldots, \beta_s$ its complex roots. Construct the convex polygon which contains the roots in its boundary or its interior. Compute the centroid of this convex polygon and move it to the fundamental domain, using the generators of the modular group S, and*

T. How do the symmetric polynomials of the new form compare to the ones of the given form f.

Reduction of binary forms can be done from a purely geometric approach. In [23], Julia proved that the point $\zeta(f)$ is tied to the roots of the form f with relations of non-euclidean geometry that are preserved when the modular group acts on them. Hence, this point is a covariant of the roots of the form for all modular transformations.

This geometric approach is helpful for forms which have special properties that make it easy to determine this point, as explained in [23].

Binary forms with complex coefficients. Let $f(x,1)$ be a degree n binary form with complex coefficients and roots $\alpha_1,\dots,\alpha_n$. Associate to it the quadratic Hermitian

$$H(x,1)=\sum_{i=1}^{n} t_i^2\cdot||x-\alpha_i||^2 \tag{36}$$

where the t_i's are nonzero real number such that make the Julia's invariant θ_0 minimal. We want to solve this optimization problem geometrically.

Let P_i be the zero in the upper half space of the quadratic $||x-\alpha_i||^2$, i.e. $P_1,\dots,P_n$ are points in the upper half space given as follows

$$P_i=(z_i,r_i)=(\alpha_i,0).$$

Attach to $P_1,\dots,P_n$ the masses $t_1^2,\dots,t_n^2$ respectively. Construct the smallest convex polyhedron which contains in the boundary or its interior the P_i's together with their respective masses. This polyhedron obtained this way by the roots of the forms will be called the polyhedron associated to the form f. Then the following is true.

Lemma 9. *The point $\zeta(f)$, which is the zero in the upper half space $\mathcal{H}_3$ of the quadratic given in Eq. (36) is the centroid of this polyhedron.*

Proof. Let $f\in V_{n,\mathbb{C}}$ be a binary form and $\alpha_1,\dots,\alpha_n$ be its roots, then the binary quadratic Hermitian form associated to it is given as

$$H(x,1)=A||x||^2-Bx-\bar{B}\bar{x}+C$$

where

$$A=\sum_{i=1}^{n}t_i^2,\qquad B=\sum_{i=1}^{n}t_i^2\alpha_i,\qquad \bar{B}=\sum_{i=1}^{n}t_i^2\bar{\alpha}_i,\qquad C=\sum_{i=1}^{n}t_i^2||\alpha_i||^2$$

are as computed in Eq. (23). By Eq. (12) the root in the upper half space of this binary quadratic Hermitian form is

$$\xi(f)=-\frac{B}{A}+\frac{\sqrt{\mathfrak{D}_f}}{A}\cdot j.$$

or equivalently the point $P=(z,r)\in\mathcal{H}_3$ such that the projection in the complex plane is

$$\frac{\sum_{i=1}^{n}t_i^2\alpha_i}{\sum_{i=1}^{n}t_i^2}$$

and the distance from the origin is

$$\frac{\sum_{i=1}^{n}t_i^2||\alpha_i||^2}{\sum_{i=1}^{n}t_i^2}.$$

On the other side the centroid C_P of the convex polygon is

$$C_P = \frac{\sum_{i=1}^{n} t_i^2 P_i}{\sum_{i=1}^{n} t_i^2}.$$

It is easy to prove that the distance of this point C_P from the origin and its projection to the complex plane agree with the ones of $\xi(f)$. This completes the proof. □

The problem of finding the Julia quadratic in this way can be formulated as follows.

Problem 4. *Let P_n be the polyhedron associated to a degree n binary form as above. Let $A_1, \dots, A_n$ be the vertices of the polyhedron with masses $w_1, \dots, w_n$ respectively. Find $w_1, \dots, w_n$ such that the centroid of the polyhedron is invariant under $\mathrm{SL}_2(\mathbb{C})$ action and makes the quantity $\sum_{1=i<j=n} w_i w_j \alpha_i \alpha_j$ (where α_i are complex numbers that we get by the projection of A_i's in the complex plane) minimal.*

In an analogues way with the previous section another interesting problem to consider here is the following.

Problem 5. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $f \in V_{n,K}$ be a binary form, $\alpha_1, \dots, \alpha_n$ its roots. Construct the convex polyhedron which contains in the boundary or its interior the roots of the given form. Compute the centroid of this convex polyhedron and move it to the fundamental domain, when such exists. How do the symmetric polynomials of the new form compare to the ones of the given form f.*

While there is a huge amount of literature on optimization problems of this type, we are not aware of any specific results that apply to this situation.

6.2. **Totally real forms.** Let $f \in V_{n,\mathbb{R}}$ such that f has signature $(n, 0)$. Such forms are called **totally real forms**. Let f be a generic form in $V_{n,\mathbb{R}}$ given by

$$f(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_1 x y^{n-1} + a_0 y^n$$

where $a_0, \dots, a_n$ are transcendentals. Identify $a_0, \dots, a_n$ respectively with $1, \dots, n+1$. Then the symmetric group S_{n+1} acts on $\mathbb{R}[a_0, \dots a_n][x, y]$ by permuting $a_0, \dots, a_n$. For any permutation $\tau \in S_{n+1}$ and $f \in \mathbb{R}[a_0, \dots a_n][x, y]$ we denote by $\tau(f) = f^\tau$. Then

$$f^\tau(x, y) = \tau(a_n)\, x^n + \tau(a_{n-1})\, x^{n-1} y + \cdots + \tau(a_1)\, x y^{n-1} + \tau(a_0)\, y^n.$$

Define $G(x, y)$ as follows

$$G(x, y) = \frac{x \cdot f_x(-f_y(x, y), f_x(x, y)) + y \cdot f_y(-f_y(x, y), f_x(x, y))}{n\, f(x, y)}. \tag{37}$$

In [34] Stoll and Cremona was proved that $G(x, y)$ is a degree $d = (n-1)(n-2)$ homogenous polynomial in $\mathbb{R}[a_0, \dots a_n][x, y]$ and $\mathcal{J}_f(x, y) \mid G(x, y)$; see [34] for details. Therefore, this polynomial can be used to reduce totally real binary forms.

Note that, for $\sigma \in S_{n+1}$ we have an involution

$$\sigma = \begin{cases} (1, n+1)(2, n) \cdots \left(\frac{n}{2}, \frac{n}{2} + 2\right), & \text{if } n \text{ is even} \\ (1, n+1)(2, n) \cdots \left(\frac{n+1}{2}, \frac{n+3}{2}\right), & \text{if } n \text{ is odd.} \end{cases}$$

The polynomial $G(x, y)$ satisfies the following.

Theorem 10. *Let $f \in V_{n,\mathbb{R}}$ with distinct roots, sig $(f) = (n, 0)$, and G_f as above. Then*

i) $G(x, y)$ is a covariant of f of degree $(n-1)$ and order $(n-1)(n-2)$.

ii) $G(x, y)$ has a unique quadratic factor over $\mathbb{R}$, which is $\mathcal{J}_f$.

iii) $G^\sigma(x, y) = (-1)^{n-1} G(x, y)$. Moreover, if $G_f = \sum_{i=1}^{d} g_i\, x^i y^{d-i}$, then

$$g_i^\sigma = (-1)^{n-1}\, g_{d-i},$$

for all $i = 0, ..., d$.

Proof. The fact that $G(x, y)$ is a polynomial is a direct consequence of the Euler's theorem on homogenous functions and it is shown in [34].

Let $F(x, y) = (f, xy)^1$ be the 1-transvection. It is a covariant of order n and degree 1. From Euler's theorem of homogenous functions we have that $F(x, y) = xf_x + yf_y = nf(x, y)$.

Let us denote by $A = -f_y(x, y)$ and $B = f_x(x, y)$. Both are covariants of f of order $(n-1)$ and degree 1. Then $f_x(A, B) = \sum_{i=0}^{n} i\, a_i\, A^{i-1}\, B^{n-i}$ has degree n as a covariant and similarly for $f_y(A, B)$. Therefore,

$$\frac{xf_x(A, B) + yf_y(A, B)}{nf(x, y)}$$

is a covariant of degree $(n-1)$. Obviously, it has order $d = (n-1)(n-2)$. This completes the proof of part i). Part ii) is a restatement of the result proved in [34].

To prove part iii), it is enough to show that $g_i^\sigma = (-1)^{n-1}\, g_{d-i}$ for all $i = 0, ..., d$. Let $\tau = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. If we show that $G^\tau(x, y) = G(x, y)$, then this immediately implies that $g_i^\sigma = (-1)^{n-1}\, g_{d-i}$ for all $i = 0, ..., d$.

For any binary form $F(x, y)$, we have that $F^\tau(x, y) = F(-y, -x) = (-1)^n\, F(x, y)$. Such a rule also applies to f_x and f_y in Eq. (37). It is now elementary to verify that $G(-y, -x) = G(x, y)$. This completes the proof. □

Next, we compute this covariant G_f for some small degree binary forms.

Example 1 (Cubics)**.** *When $n = 3$, $G(x, y)$ is the Hessian of the binary cubic. It is given by the formula*

$$G_f = (3a_3a_1 - a_2^2)x^2 + (9a_3a_0 - a_2a_1)xy + (3a_2a_0 - a_1^2)y^2$$

when $f = \sum_{i=0}^{3} a_i x^i y^{3-i}$. This formula was known to Stoll and Cremona in [34].

The permutation σ is $\sigma = (a_0, a_3)(a_1, a_2)$. Notice that $G^\sigma = G$. Moreover, $\Delta_G = -3 \cdot \Delta_f$.

Totally real quartics. Let $f \in V_{4,\mathbb{R}}$ with distinct real roots and

$$f(x, y) = \sum_{i=0}^{4} a_i x^i y^{4-i}.$$

Then G_f is a degree 6 homogenous polynomial given as follows

$$G_f = \sum_{i=0}^{6} g_i x^i y^{6-i},$$

where

$$g_6 = -\left(a_3^3 + 4\, a_2a_3a_4 - 8\, a_1a_4^2\right)$$

$$
\begin{aligned}
g_5 &= 2\left(a_2a_3^2 + 16\,a_0a_4^2 + 2\,a_4a_1a_3 - 4\,a_4{a_2}^2\right)\\
g_4 &= 5\,\left(a_1a_3^2 - 4\,a_4a_1a_2 + 8\,a_4a_0a_3\right)\\
g_3 &= 20\,\left(a_0a_3^2 - a_1^2a_4\right)\\
g_2 &= -5\,\left(a_3a_1^2 - 4\,a_0a_3a_2 + 8\,a_0a_4a_1\right)\\
g_1 &= -2\left(a_2a_1^2 + 16\,a_4a_0^2 + 2\,a_0a_3a_1 - 4\,a_0{a_2}^2\right)\\
g_0 &= a_1^3 + 4\,a_2a_0a_1 - 8\,a_0^2a_3
\end{aligned}
$$

In this case $\sigma = (15)(24)$, which in terms of the coefficients $a_0, \ldots, a_4$ becomes $\sigma := (a_0, a_4)(a_1, a_3)$. Then it is easy to check that

$$\sigma(g_6) = -g_0, \quad \sigma(g_5) = -g_1, \quad \sigma(g_4) = -g_2, \quad \sigma(g_3) = -g_3.$$

The discriminant of G in terms of $a_0, \ldots, a_4$ is given by

$$
\begin{aligned}
\Delta_G = -\,2^{28}\,&\left(a_1^2{a_2}^2a_3^2 - 4\,a_1^2{a_2}^3a_4 - 4\,a_1^3a_3^3 + 18\,a_1^3a_2a_4a_3 - 27\,a_1^4a_4^2\right.\\
&- 4\,a_0{a_2}^3a_3^2 + 16\,a_0{a_2}^4a_4 + 18\,a_0a_1a_3^3a_2 - 80\,a_0a_1a_3a_4{a_2}^2 - 6\,a_0a_1^2a_3^2a_4\\
&+ 144\,a_1^2a_2a_0a_4^2 - 27\,a_0^2a_3^4 + 144\,a_0^2a_4a_2a_3^2 - 128\,a_0^2{a_2}^2a_4^2\\
&\left.-192\,a_0^2a_1a_3a_4^2 + 256\,a_0^3{a_4}^3\right)^5
\end{aligned}
$$

It is easily verified that

$$\Delta_G = -2^{28}\cdot\Delta_f^5 = -4^{14}\cdot\Delta_f^5.$$

Remark 4. *We expect that in general $\Delta_G = r\cdot\Delta_f^{n+1}$, for some constant r. This fact has not been noticed before by previous authors.*

Totally real quintics. Let $f \in V_{5,\mathbb{R}}$ be a binary quintic $f = \sum_{i=0}^5 a_i x^i y^{5-i}$. Its signature is one of the following $\operatorname{sig}(f) = \{(5,0),(3,1),(1,2)\}$.

Assume that $\operatorname{sig}(f) = (r,s) = (5,0)$. In the notation of the previous section, we have $Q_f = T_5$. The discriminant of T_5 in terms of the roots α_i of the form is given by the formula

$$
\begin{aligned}
\Delta(T_5) = -4t_1^2\cdots t_5^2\Bigg(&\frac{(\alpha_1-\alpha_2)^2}{t_3^2t_4^2t_5^2} + \frac{(\alpha_1-\alpha_3)^2}{t_2^2t_4^2t_5^2} + \frac{(\alpha_1-\alpha_4)^2}{t_3^2t_2^2t_5^2} + \frac{(\alpha_1-\alpha_5)^2}{t_2^2t_3^2t_4^2}\\
&+ \frac{(\alpha_2-\alpha_3)^2}{t_1^2t_4^2t_5^2} + \frac{(\alpha_2-\alpha_4)^2}{t_1^2t_3^2t_5^2} + \frac{(\alpha_2-\alpha_5)^2}{t_1^2t_3^2t_4^2} + \frac{(\alpha_3-\alpha_4)^2}{t_1^2t_2^2t_5^2}\\
&+ \frac{(\alpha_3-\alpha_5)^2}{t_1^2t_2^2t_4^2} + \frac{(\alpha_4-\alpha_5)^2}{t_1^2t_2^2t_3^2}\Bigg).
\end{aligned}
$$

In this case $\sigma = (1,6)(2,5)(3,4)$ which correspond to $\sigma = (a_0,a_5)(a_1,a_4)(a_2,a_3)$. Then computing $G(x,y)$ as in Eq. (37) we have

$$G(x,y) = c_{12}x^{12} + c_{11}x^{11}y + \cdots c_1xy^{11} + c_0y^{12} \tag{38}$$

where the coefficients are given as follows:

$$
\begin{aligned}
c_{12} &= 125\,a_1{a_5}^3 - 50\,a_2a_4{a_5}^2 + 15\,a_3a_4^2a_5 - 3\,a_4^4\\
c_{11} &= 625\,a_0{a_5}^3 + 175\,a_1a_4{a_5}^2 - 100\,a_2a_3{a_5}^2 - 55\,a_2a_4^2a_5 + 60\,a_3^2a_4a_5 - 9\,a_3a_4^3\\
c_{10} &= 1375\,a_0a_4{a_5}^2 - 25\,a_1a_3{a_5}^2 + 65\,a_1a_4^2a_5 - 150\,{a_2}^2{a_5}^2 - 30\,a_2a_3a_4a_5\\
&\quad - 41\,a_2a_4^3 + 60\,a_3^3a_5 + 3\,a_3^2a_4^2
\end{aligned}
$$

$$
\begin{aligned}
c_9 &= 875\,a_0a_3{a_5}^2 + 1025\,a_0a_4^2a_5 - 425\,a_1a_2{a_5}^2 + 30\,a_1a_3a_4a_5 - 33\,a_1a_4^3 \\
&\quad - 130\,{a_2}^2a_4a_5 + 160\,a_2a_3^2a_5 - 86\,a_2a_3a_4^2 + 24\,a_3^3a_4 \\
c_8 &= 125\,a_0a_2{a_5}^2 + 1500\,a_0a_3a_4a_5 + 215\,a_0a_4^3 - 425\,a_1^2{a_5}^2 - 450\,a_1a_2a_4a_5 \\
&\quad + 175\,a_1a_3^2a_5 - 128\,a_1a_3a_4^2 + 175\,{a_2}^2a_3a_5 - 97\,{a_2}^2a_4^2 + 8\,a_2a_3^2a_4 + 12\,a_3^4 \\
c_7 &= -750\,a_0a_1{a_5}^2 + 500\,a_0a_2a_4a_5 + 775\,a_0a_3^2a_5 + 430\,a_0a_3a_4^2 - 530\,a_1^2a_4a_5 \\
&\quad + 310\,a_1a_2a_3a_5 - 322\,a_1a_2a_4^2 - 61\,a_1a_3^2a_4 + 105\,{a_2}^3a_5 - 33\,{a_2}^2a_3a_4 + 32\,a_2a_3^3 \\
c_6 &= -625\,a_0^2{a_5}^2 - 800\,a_0a_1a_4a_5 + 1200\,a_0a_2a_3a_5 + 30\,a_0a_2a_4^2 + 365\,a_0a_3^2a_4 \\
&\quad + 30\,a_1^2a_3a_5 - 303\,a_1^2a_4^2 + 365\,a_1{a_2}^2a_5 - 268\,a_1a_2a_3a_4 + a_1a_3^3 + {a_2}^3a_4 + 37\,{a_2}^2a_3^2 \\
c_5 &= -750\,a_0^2a_4a_5 + 500\,a_0a_1a_3a_5 - 530\,a_0a_1a_4^2 + 775\,a_0{a_2}^2a_5 + 310\,a_0a_2a_3a_4 \\
&\quad + 105\,a_0{a_3}^3 + 430\,a_1^2a_2a_5 - 322\,a_1^2a_3a_4 - 61\,a_1{a_2}^2a_4 - 33\,a_1a_2a_3^2 + 32\,{a_2}^3a_3 \\
c_4 &= 125\,a_0^2a_3a_5 - 425\,a_0^2a_4^2 + 1500\,a_0a_1a_2a_5 - 450\,a_0a_1a_3a_4 + 175\,a_0{a_2}^2a_4 \\
&\quad + 175\,a_0a_2a_3^2 + 215\,a_1^3a_5 - 128\,a_1^2a_2a_4 - 97\,a_1^2a_3^2 + 8\,a_1{a_2}^2a_3 + 12\,{a_2}^4 \\
c_3 &= 875\,{a_0}^2a_2a_5 - 425\,a_0^2a_3a_4 + 1025\,a_0a_1^2a_5 + 30\,a_0a_1a_2a_4 - 130\,a_0a_1a_3^2 \\
&\quad + 160\,a_0{a_2}^2a_3 - 33\,a_1^3a_4 - 86\,a_1^2a_2a_3 + 24\,a_1{a_2}^3 \\
c_2 &= 1375\,a_0^2a_1a_5 - 25\,a_0^2a_2a_4 - 150\,a_0^2a_3^2 + 65\,a_0a_1^2a_4 - 30\,a_0a_1a_2a_3 + 60\,a_0{a_2}^3 \\
&\quad - 41\,a_1^3a_3 + 3\,a_1^2{a_2}^2 \\
c_1 &= 625\,a_0^3a_5 + 175\,a_0^2a_1a_4 - 100\,a_0^2a_2a_3 - 55\,a_0a_1^2a_3 + 60\,a_0a_1{a_2}^2 - 9\,a_1^3a_2 \\
c_0 &= 125\,a_0^3a_4 - 50\,a_0^2a_1a_3 + 15\,a_0a_1^2a_2 - 3\,a_1^4
\end{aligned}
$$

The following is an immediate consequence of Thm. 10.

Corollary 4. *Let $f \in V_{5,\mathbb{R}}$ with signature $(5,0)$. Then $G^\sigma = G$ the above coefficients give a computational confirmation that $G^\sigma = G$ and $c_i^\sigma = c_{5-i}$ for all $i = 1, \ldots, 5$.*

Next we will study binary forms where all the roots are complex and will see the similarity of such forms with totally real forms.

6.3. **Totally complex forms.** Let $f(x,y) \in \mathbb{R}$ be a degree $n = 2s$ binary form with signature $(0,s)$. We will call such forms **totally complex forms**. Then $f(x,y)$ can be factored as follows

$$f(x,1) = \prod_{i=1}^{s}(x-\alpha_i)(x-\bar{\alpha}_i) = \prod_{i=1}^{s}(x^2 + A_ix + B_i).$$

and assume $\alpha_i = a_i + I\,b_i$, for $i = 1, \ldots s$. Associate to it the quadratic

$$S(x,y) = 2\sum_{i=1}^{s} u_i^2(x^2 + A_ixy + B_iy^2).$$

The discriminant of $S(x,1)$ is computed in Eq. (20) and is

$$\Delta_S = -16\left(\sum_{i<j} u_i^2u_j^2\left[(a_i-a_j)^2 + (b_i^2+b_j^2)\right] + \sum_{j=1}^{s} u_j^4b_j^2\right)$$

In analogy with the theory explained in Section 5.1 let $h = \Delta_S$ and $g = u_1^4 \cdots u_s^4$. We have to solve the following system

$$\begin{cases} \nabla_h = \lambda \nabla_g \\ u_1^4 \cdots u_s^4 = 1 \end{cases}$$

for $\lambda \neq 0$. For all $i = 1, \ldots, s$ the partial derivative of Δ_S with respect to u_i is

$$-16 \left(2 \sum_{i<j} u_i u_j^2 \left[(a_i - a_j)^2 + (b_i^2 + b_j^2) \right] + 4 \sum_{j=1}^{s} u_j^3 b_j^2 \right)$$

and the above system Eq. (6.3) is

$$\begin{cases} -16 \left(2 \sum_{i<j} u_1 u_j^2 \left[(a_1 - a_j)^2 + (b_1^2 + b_j^2) \right] + 4 \sum_{j=1}^{s} u_j^3 b_j^2 \right) = 4\lambda u_1^3 \cdots u_s^4 \\ \qquad \vdots \\ -16 \left(2 \sum_{i<j} u_s u_j^2 \left[(a_s - a_j)^2 + (b_s^2 + b_j^2) \right] + 4 \sum_{j=1}^{s} u_j^3 b_j^2 \right) = 4\lambda u_1^4 \cdots u_s^3 \\ u_1^4 \cdots u_s^4 = 1 \end{cases} \tag{39}$$

To find the point in the upper half plane that is used for reduction we need to find the unique solution of the above system. Next, we compute the Julia quadratic of totally complex binary quartics and sextics.

Totally complex quartics. Let f be a binary quartic with signature $(0, 2)$ and factored as follows $f(x, y) = \sum_{i=1}^{2}(x^2 + a_i xy + b_i y^2)$. Associate to f the quadratic Q_f, where

$$Q_f(x, 1) = 2u_1^2(x^2 + a_1 x + b_1) + 2u_2^2(x^2 + a_2 x + b_2)$$

To find u_1, and u_2 we set up the system as in Eq. (39) and solve for the u_i's. The discriminant of the quadratic which is

$$\Delta_Q = {a_1}^2 {u_1}^2 + 2\, a_1 a_2 u_1 u_2 + {a_2}^2 {u_2}^2 - 4\, b_1 {u_1}^2 - 4\, b_1 u_1 u_2 - 4\, b_2 u_1 u_2 - 4\, b_2 {u_2}^2.$$

Next, compute the partial derivatives of Δ_Q with respect to u_1, u_2, and then set up the system. This is done in Maple but we do not display the system here. The system is given in terms of u_i's, a_i's, b_i's and λ, the Lagrange multiplier. Solving for λ we get

$$\lambda = -2\, \frac{({a_1}^2 - a_1 a_2 - 2\, b_1 + 2\, b_2)x^2 + 2x(\, a_1 b_1 - 2\, a_2 b_1 + a_1 b_2) + {a_1}^2 b_2 - a_1 a_2 b_1 + 2\, {b_1}^2 - 2\, b_1 b_2}{x^2 + x a_1 + b_1}$$

Substitute λ as computed in the system (39) and add to this system the equation $Q(x, 1) = 0$. Using this approach we can compute the point $\xi(f)$ in the upper half plane corresponding to the Julia quadratic. Eliminating u_1, and u_2 we get a degree 4 polynomial

$$G_f = \sum_{i=0}^{4} c_i x^i y^{4-i}, \tag{40}$$

with coefficients as follows

$$\begin{aligned}
c_4 &= -2\,{a_1}^2 + 2\,{a_2}^2 + 8\,b_1 - 8\,b_2\\
c_3 &= -4\,{a_1}^2 a_2 + 4\,a_1{a_2}^2 - 16\,a_1 b_2 + 16\,a_2 b_1\\
c_2 &= -12\,{a_1}^2 b_2 + 12\,{a_2}^2 b_1\\
c_1 &= -4\,{a_1}^2 a_2 b_2 + 4\,a_1{a_2}^2 b_1 - 16\,a_1 b_1 b_2 + 16\,a_2 b_1 b_2\\
c_0 &= -2\,{a_1}^2 {b_2}^2 + 2\,{a_2}^2 {b_1}^2 - 8\,{b_1}^2 b_2 + 8\,b_1 {b_2}^2.
\end{aligned}$$

If we let $b_1 = b_2 = 1$ then $G_f(x, y)$ is a palindromic polynomial, i.e.

$$\begin{aligned}
c_4 &= c_0 = -2\,{a_1}^2 + 2\,{a_2}^2\\
c_3 &= c_1 = -4\,{a_1}^2 a_2 + 4\,a_1{a_2}^2 - 16a_1 + 16a_2\\
c_2 &= -12\,{a_1}^2 + 12\,{a_2}^2.
\end{aligned}$$

This degree 4 polynomial has a unique quadratic factor which is the Julia's quadratic and will be used to reduce the given form.

Totally complex sextics. Let f be a binary sextic with signature $(0, 3)$ and factored as follows

$$f(x, y) = (x^2 + a_1xy + b_1y^2)(x^2 + a_2xy + b_2y^2)(x^2 + a_3xy + b_3y^2).$$

Associate to f the quadratic

$$Q(x, 1) = 2u_1^2(x^2 + a_1x + b_1) + 2u_2^2(x^2 + a_2x + b_2) + 2u_3^2(x^2 + a_3x + b_3)$$

where the u_i's are real numbers that make θ_f minimal. To find u_1, u_2 and u_3 that satisfy this condition we need to set up the system in eq (39) and solve for the u_i's. Compute first the discriminant of the quadratic which is as follows

$$\begin{aligned}
\Delta_Q =& 4\,{a_1}^2 {u_1}^4 + 8\,a_1 a_2 {u_1}^2 {u_2}^2 + 8\,a_1 a_3 {u_1}^2 {u_3}^2 + 4\,{a_2}^2 {u_2}^4 + 8\,a_2 a_3 {u_2}^2 {u_3}^2\\
&+ 4\,{a_3}^2 {u_3}^4 - 16\,b_1 {u_1}^4 - 16\,b_1 {u_1}^2 {u_2}^2 - 16\,b_1 {u_1}^2 {u_3}^2 - 16\,b_2 {u_1}^2 {u_2}^2\\
&- 16\,b_2 {u_2}^4 - 16\,b_2 {u_2}^2 {u_3}^2 - 16\,b_3 {u_1}^2 {u_3}^2 - 16\,b_3 {u_2}^2 {u_3}^2 - 16\,b_3 {u_3}^4
\end{aligned}$$

Next, compute the partial derivatives of Δ_Q with respect to u_1, u_2, and u_3 and then set up the system. This is done in Maple but we do not display the system here because is to big. The system is given in terms of u_i's, a_i's, b_i's and λ, the Lagrange multiplier. Solving for λ we get

$$\lambda = \frac{4(a_3 {u_1}^2 a_1 + a_3 {u_2}^2 a_2 + {u_3}^2 {a_3}^2 - 2\,{u_1}^2 b_1 - 2\,{u_2}^2 b_2 - 2\,b_3 {u_1}^2 - 2\,b_3 {u_2}^2 - 4\,{u_3}^2 b_3)}{{u_3}^2 {u_1}^4 {u_2}^4}$$

Substitute λ as computed in the system (39) and add to this system the equation $Q(x, 1) = 0$. Using this approach we can compute the point $\xi(f)$ in the upper half plane corresponding to the Julia quadratic. Computationally it is too difficult to eliminate all three u_1, u_2, and u_3 at the same time, so first we eliminate u_1, and u_2 and then at a second step eliminate u_3. Eliminating all three of them we get a degree 8 polynomial

$$G_f = \sum_{i=0}^{8} c_i x^i y^{8-i}, \tag{41}$$

with coefficients given in [6]. This degree 8 polynomial has a unique quadratic factor which is the Julia quadratic and will be used to reduce the given form.

As a special case, consider the case when we let $b_1 = b_2 = b_3 = 1$. The binary form f is given as follows

$$f(x,y) = \prod_{i=1}^{3}(x^2 + a_i xy + y^2).$$

The function $G_f(x,y)$ associated to this binary form has coefficients as follows

$$\begin{aligned}
c_8 &= -c_0 = 3\,(a_2-a_3)\,(a_1-a_3)\,(a_1-a_2)\,(a_1a_2+a_1a_3+a_2a_3)\\
c_7 &= -c_1 = 3\,(a_2-a_3)\,(a_1-a_3)\,(a_1-a_2)\,(3\,a_1a_2a_3+8\,a_1+8\,a_2+8\,a_3)\\
c_6 &= -c_2 = 6\,(a_2-a_3)\,(a_1-a_3)\,(a_1-a_2)\,(5\,a_1a_2+5\,a_1a_3+5\,a_2a_3+24)\\
c_5 &= -c_3 = 9\,(a_2-a_3)\,(a_1-a_3)\,(a_1-a_2)\,(a_1a_2a_3+8\,a_1+8\,a_2+8\,a_3)\\
c_4 &= 0.
\end{aligned}$$

Note that $G_f(x,y)$ is a palindromic polynomial.

Remark 5. *If $f = \prod_{i=1}^{n}(x^2 + a_i xy + y^2)$, then f is a palindromic form. In this case, the Julia quadratic is a factor of G_f, where G_f is also a palindromic form.*

6.4. **Julia's quadratic of binary forms of small degree.** We give examples when $n = 3, 4$ to illustrate the theory in Section 5 and to show explicitly how the u_i's can be determined using the system given in Eq. (28).

Binary cubic forms. Let $f \in V_{3,\mathbb{C}}$ and let denote its roots by $\alpha_1, \alpha_2, \alpha_3$, then

$$f(x,1) = a_0(x-\alpha_1)(x-\alpha_2)(x-\alpha_3), \tag{42}$$

for some $a_0 \in \mathbb{C}$. We associate to f the following positive definite quadratic form

$$\begin{aligned}
Q_f(\alpha,1) =& t_1^2(x-\alpha_1)(\bar{x}-\bar{\alpha}_1) + t_2^2(x-\alpha_2)(\bar{x}-\bar{\alpha}_2) + t_3^2(x-\alpha_3)(\bar{x}-\bar{\alpha}_3)\\
=& \left(t_1^2+t_2^2+t_3^2\right)x\bar{x} - \left(t_1^2\bar{\alpha}_1 + t_2^2\bar{\alpha}_2 + t_3^2\bar{\alpha}_3\right)\,x\\
&- \left(t_1^2\alpha_1 + t_2^2\alpha_2 + t_3^2\alpha_3\right)\,\bar{x} + \left(t_1^2||\alpha_1||^2 + t_2^2||\alpha_2||^2 + t_3^2||\alpha_3||^2\right).
\end{aligned} \tag{43}$$

The discriminant of $Q_f(x,y)$ is given as follows

$$\Delta_Q = {t_1}^2{t_2}^2\,||\alpha_1-\alpha_2|\,|^2 + t_1^2t_3^2||\alpha_1-\alpha_3||^2 + t_2^2t_3^2||\alpha_2-\alpha_3||^2.$$

For simplicity in the computations denote by $h = \Delta_Q$, then compute its gradient and replace $\alpha_{i,j} := ||\alpha_i - \alpha_j||^2$. We have

$$\nabla_h = \left\langle\, 2t_1t_2^2\alpha_{12} + 2t_1t_3^2\alpha_{13},\ 2t_2t_1^2\alpha_{12} + 2t_2t_3^2\alpha_{23},\ 2t_3t_1^2\alpha_{13} + 2t_3t_2^2\alpha_{23}\right\rangle.$$

As in Section 5.1 we take $g = t_1^2 \cdot t_2^2 \cdot t_3^2 = 1$, and its gradient is

$$\nabla_g = \left\langle\, 2t_1t_2^2t_3^2,\ 2t_2t_1^2t_3^2,\ 2t_3t_1^2t_2^2\right\rangle.$$

Then the system in Eq. (5.1) is as follows

$$\begin{cases}
2t_1t_2^2\alpha_{12} + 2t_1t_3^2\alpha_{13} = 2\lambda t_1t_2^2\,t_3^2\\
2t_2t_1^2\alpha_{12} + 2t_2t_3^2\alpha_{23} = 2\lambda t_2t_1^2\,t_3^2\\
2t_3t_1^2\alpha_{13} + 2t_3t_2^2\alpha_{23} = 2\lambda t_3t_1^2\,t_2^2\\
t_1^2 \cdot t_2^2 \cdot t_3^2 = 1.
\end{cases}$$

Simplifying and substituting $t_1^2 \cdot t_2^2 \cdot t_3^2 = 1$ we have

$$\begin{cases} t_1^2(t_2^2\alpha_{12} + t_3^2\alpha_{13}) = \lambda \\ t_2^2(t_1^2\alpha_{12} + t_3^2\alpha_{23}) = \lambda \\ t_3^2(t_1^2\alpha_{13} + t_2^2\alpha_{23}) = \lambda \\ t_1^2 \cdot t_2^2 \cdot t_3^2 = 1. \end{cases}$$

Substitute $\lambda = \frac{2}{3} \cdot (u_1u_2\alpha_{1,2} + u_2u_3\alpha_{2,3} + u_1u_3\alpha_{1,3})$ as in Eq. (27), write everything in terms of u's and $\alpha_{i,j}$'s, and then combine like terms

$$\begin{cases} u_1u_2\alpha_{12} + u_1u_3\alpha_{13} = 2u_2u_3\alpha_{2,3} \\ u_1u_2\alpha_{12} + u_2u_3\alpha_{23} = 2u_1u_3\alpha_{1,3} \\ u_1u_3\alpha_{13} + u_2u_3\alpha_{23} = 2u_1u_2\alpha_{1,2} \\ u_1 \cdot u_2 \cdot u_3 = 1. \end{cases}$$

We further normalize by letting $\alpha_{1,2} \cdot \alpha_{1,3} \cdot \alpha_{2,3} = 1$. Solving the above system for u_1, u_2, u_3 we get

$$\begin{cases} u_1 = \frac{\alpha_{1,2}}{\alpha_{1,3}{u_3}^2} \\ u_2 = \frac{\alpha_{1,3}u_3}{\alpha_{1,2}} \\ \alpha_{1,3}u_3\left({\alpha_{1,2}}^2 - \alpha_{1,3}\alpha_{2,3}{u_3}^3\right) = 0. \end{cases}$$

Consider $\alpha_{1,3}u_3\left({\alpha_{1,2}}^2 - \alpha_{1,3}\alpha_{2,3}{u_3}^3\right) = 0$. Since, $u_i \neq 0$ we have

$$\left({\alpha_{1,2}}^2 - \alpha_{1,3}\alpha_{2,3}{u_3}^3\right) = 0.$$

Multiply both sides of the above with $\alpha_{1,2}$ and then making the substitution $\alpha_{1,2} \cdot \alpha_{1,3} \cdot \alpha_{2,3} = 1$ we get $u_3^3 = \alpha_{1,2}^3$. By the definition of the quadratic $Q(x,1)$ associated to $f(x,1)$, all u_i are non zero real numbers, then this equation $u_3^3 = \alpha_{1,2}^3$ has a unique real solution, namely $u_3 = \alpha_{1,2}$. Therefore, the unique solution to the above system is

$$u_1 = \alpha_{2,3},\ u_2 = \alpha_{1,3},\ u_3 = \alpha_{1,2}.$$

Substituting these values of u_1, u_2, u_3, which are the values that minimize θ_0, into Eq. (43) we get Julia's quadratic $\mathcal{J}_f$.

$$\mathcal{J}_f(x,1) = ||\alpha_2 - \alpha_3||^2(x-\alpha_1)^2 + ||\alpha_1 - \alpha_3||^2(x-\alpha_2)^2 + ||\alpha_1 - \alpha_2||^2(x-\alpha_3)^2.$$

Let p, q, r denote the coefficients of Julia quadratic, then they are respectively

$$p := 2\,{\alpha_1}^2 - 2\,\alpha_1\alpha_2 - 2\,\alpha_1\alpha_3 + 2\,{\alpha_2}^2 - 2\,\alpha_2\alpha_3 + 2\,{\alpha_3}^2$$

$$q := -2\,{\alpha_1}^2\alpha_2 - 2\,{\alpha_1}^2\alpha_3 - 2\,\alpha_1{\alpha_2}^2 + 12\,\alpha_1\alpha_2\alpha_3 - 2\,\alpha_1{\alpha_3}^2 - 2\,{\alpha_2}^2\alpha_3 - 2\,\alpha_2{\alpha_3}^2$$

$$r := 2\,{\alpha_1}^2{\alpha_2}^2 - 2\,{\alpha_1}^2\alpha_2\alpha_3 + 2\,{\alpha_1}^2{\alpha_3}^2 - 2\,\alpha_1{\alpha_2}^2\alpha_3 - 2\,\alpha_1\alpha_2\alpha_3^2 + 2\,{\alpha_2}^2{\alpha_3}^2$$

Now, let f be a generic cubic given as follows

$$f(x,1) = ax^3 + bx^2 + cx + d$$

where $a = a_0$, $b = \alpha_1 + \alpha_2 + \alpha_3$, $c = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$, and $d = \alpha_1\alpha_2\alpha_3$. Eliminating the roots we can express Julia's quadratic coefficient in terms of the coefficient of $f(X)$ as follows

$$p = b^2 - 3ac,\ q = bc - 9ad,\ r = c^2 - 3bd$$

up to a constant factor.

Notice that $\mathfrak{D}_f = -3 \cdot \Delta_f$, where Δ_f is the discriminant of the cubic. In this case the discriminant of the Julia quadratic is an $\mathrm{SL}_2(\mathbb{Z})$ invariant of the binary form. We summarize as follows:

Lemma 10. *Let f be a stable binary cubic with equation*

$$f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Then its Julia quadratic is given by

$$\mathcal{J}_f = (b^2 - 3ac)\,x^2 + (bc - 9ad)\,xy + (c^2 - 3bd)y^2 \tag{44}$$

and its discriminant is $\Delta(J_f) = -3\,\Delta_f$, where Δ_f is the discriminant of f. Moreover, its θ-invariant is

$$\theta_f = a_0^6\, 3^{\frac{3}{2}}\ |\Delta_f|^{\frac{1}{2}}.$$

As we will see in the next section the situation is more complicated for forms of higher degree.

Binary quartics. We illustrate the case of binary quartics. Let f be a binary quartic given as follows

$$f(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \tag{45}$$

and $\alpha_1, \ldots, \alpha_4$ its roots when $y = 1$. To this binary quartic we associate a positive definite quadratic form as follows

$$Q(x,1) = \sum_{i=1}^{4} t_i^2 (x - \alpha_i)^2 \tag{46}$$

and its discriminant as computed in Eq. (24)

$$\Delta_Q = \sum_{1=i<j=4} u_i\, u_j\, \alpha_{i,j}$$

where as above $u_i = t_i^2$ and $\alpha_{i,j} = (\alpha_i - \alpha_j)^2$, for $i < j$. Compute the gradient of the discriminant of $Q(x,1)$ with respect to u_i's. Then the system in Eq. (25) in this case will be

$$\begin{cases} u_1(\alpha_{1,2}u_2 + \alpha_{1,3}u_3 + \alpha_{1,4}u_4) = (1/2)\ \sum_{1=i<j=4} u_i\, u_j\, \alpha_{i,j} \\ u_2(\alpha_{1,2}u_1 + \alpha_{2,3}u_3 + \alpha_{2,4}u_4) = (1/2)\ \sum_{1=i<j=4} u_i\, u_j\, \alpha_{i,j} \\ u_3(\alpha_{1,3}u_1 + \alpha_{2,3}u_2 + \alpha_{3,4}u_4) = (1/2)\ \sum_{1=i<j=4} u_i\, u_j\, \alpha_{i,j} \\ u_4(\alpha_{1,4}u_1 + \alpha_{2,4}u_2 + \alpha_{3,4}u_3) = (1/2)\ \sum_{1=i<j=4} u_i\, u_j\, \alpha_{i,j}. \\ u_1u_2u_3u_4 - 1 = 0. \end{cases}$$

Combining like terms and simplifying we have

$$\begin{cases} u_1u_2\alpha_{1,2} + u_1u_3\alpha_{1,3} + u_1u_4\alpha_{1,4} - u_2u_3\alpha_{2,3} - u_2u_4\alpha_{2,4} - u_3u_4\alpha_{3,4} = 0 \\ u_1u_2\alpha_{1,2} + u_2u_3\alpha_{2,3} + u_2u_4\alpha_{2,4} - u_1u_3\alpha_{1,3} - u_1u_4\alpha_{1,4} - u_3u_4\alpha_{3,4} = 0 \\ u_1u_3\alpha_{1,3} + u_2u_3\alpha_{2,3} + u_3u_4\alpha_{3,4} - u_1u_2\alpha_{1,2} - u_1u_4\alpha_{1,4} - u_2u_4\alpha_{2,4} = 0 \\ u_1u_4\alpha_{1,4} + u_2u_4\alpha_{2,4} + u_3u_4\alpha_{3,4} - u_1u_2\alpha_{1,2} - u_1u_3\alpha_{1,3} - u_2u_3\alpha_{2,3} = 0 \\ u_1u_2u_3u_4 - 1 = 0. \end{cases}$$

We want to solve the above system for $u_1, \ldots, u_4$. Add up the first and second equation, then first and third, and lastly first and fourth to get

$$\begin{cases} u_1u_2\alpha_{1,2} = u_3u_4\alpha_{3,4} \\ u_1u_3\alpha_{1,3} = u_2u_4\alpha_{2,4} \\ u_1u_4\alpha_{1,4} = u_2u_3\alpha_{2,3}. \end{cases}$$

Then multiplying each side of the above system we get

$$u_1^3 = u_2u_3u_4 \cdot \frac{\alpha_{2,3}\alpha_{2,4}\alpha_{3,4}}{\alpha_{1,2}\alpha_{1,3}\alpha_{1,4}}.$$

Multiplying both sides with u_1 we get

$$u_1^4 = \frac{\alpha_{2,3}\alpha_{2,4}\alpha_{3,4}}{\alpha_{1,2}\alpha_{1,3}\alpha_{1,4}}.$$

The same way we can compute u_2^4, u_3^4, u_4^4. This proves the following.

Lemma 11. *The degree of the field extension* $[k(u_1,\dots,u_4) : k(\alpha_{i,j})] = 4$. *Moreover,*

$$u_1^4 = \frac{\alpha_{2,3}\alpha_{2,4}\alpha_{3,4}}{\alpha_{1,2}\alpha_{1,3}\alpha_{1,4}},\ u_2^4 = \frac{\alpha_{1,3}\alpha_{1,4}\alpha_{3,4}}{\alpha_{1,2}\alpha_{2,3}\alpha_{2,4}},$$
$$u_3^4 = \frac{\alpha_{1,2}\alpha_{1,4}\alpha_{2,4}}{\alpha_{1,3}\alpha_{2,3}\alpha_{3,4}},\ u_4^4 = \frac{\alpha_{1,2}\alpha_{1,3}\alpha_{2,3}}{\alpha_{1,4}\alpha_{2,4}\alpha_{3,4}}.$$

Hence, we have the following diagram of field extensions.

$$\begin{array}{c} k(\alpha_1,\dots,\alpha_4) \\ \Big| 6 \\ k(u_1,\dots,u_4) \\ \Big| 4 \\ k(\alpha_{i,j}) \end{array}$$

The proof of $[k(\alpha_1,\dots,\alpha_4) : k(u_1,\dots,u_4)] = 6$ is done computationally via Maple.

Remark 6. *For any given 4-tuple* $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ *we have a unique positive real solution* (u_1,u_2,u_3,u_4). *Hence, as expected the coefficients of the Julia quadratic are uniquely defined.*

Therefore, the Julia quadratic of the given quartic is

$$\mathcal{J}_f = px^2 - 2qx + r \tag{47}$$

where p, q, and r are as follows

$$\begin{aligned} p\cdot d =&(\alpha_3-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)+(\alpha_3-\alpha_4)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)+\\ &(\alpha_1-\alpha_2)(\alpha_2-\alpha_4)(\alpha_1-\alpha_4)+(\alpha_1-\alpha_2)((\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\\ q\cdot d =&\alpha_1(\alpha_3-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)+\alpha_2(\alpha_3-\alpha_4)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)+\\ &\alpha_3(\alpha_1-\alpha_2)(\alpha_2-\alpha_4)(\alpha_1-\alpha_4)+\alpha_4(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3)\\ r\cdot d =&\alpha_1^2(\alpha_3-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)+\alpha_2^2(\alpha_3-\alpha_4)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)+\\ &\alpha_3^2(\alpha_1-\alpha_2)(\alpha_2-\alpha_4)(\alpha_1-\alpha_4)+\alpha_4^2(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) \end{aligned}$$

where

$$d = \Big((\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_4)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)(\alpha_2-\alpha_4)\Big)^{\frac{1}{2}}$$

Computing Julia's quadratic discriminant we have

$$\mathfrak{D}_f = \frac{-4\,a^3\,(\alpha_2-\alpha_4)(\alpha_1-\alpha_3)}{\Delta_f^{1/2}}.$$

In an analogues way with the cubics, we want to express Julia's quadratic coefficients in terms of the coefficients of the binary quartic form. Write down the

symmetric polynomials, as well as the coefficients of Julia's quadratic and then eliminate the roots of the quartic $\alpha_1, \ldots, \alpha_4$. In this case, the computations show that the coefficients of the Julia quadratic cannot be expressed nicely in terms of the coefficient of the binary quadratic, as in the case of binary cubics. The case of binary quintics and sextics is done in detail in [7]. The main results are given in the following theorems.

Theorem 11. *Let $f \in V_{5,\mathbb{R}}$. The quadratic Q_f associated to f is as follows.*

i) If sig $(f) = (5,0)$ then $Q_f = T_5$, where T_5 is the unique quadratic factor of Eq. (38).

ii) If sig $(f) = (3,1)$ then $Q_f = T_3 + S_1$, where T_3 is the quadratic given in Eq. (44) and S_1 as

$$S_1 = 2u_1^2\left(x^2 - 2\,\mathrm{Re}(\beta)x + ||\beta||^2\right)$$

for some $\beta \in \mathcal{H}_2$ such that $f(\beta) = 0$.

iii) If sig $(f) = (1,2)$ then $Q_f = T_1 + S_2$, where S_2 is the unique quadratic factor of Eq. (40) and T_1 as follows

$$T_1 = t_1^2\,(x - \alpha)^2$$

for some $\alpha \in \mathbb{R}$ such that $f(\alpha) = 0$.

And for binary sextics we have the following.

Theorem 12. *Let $f \in V_{6,\mathbb{R}}$. The quadratic Q_f associated to f is as follows.*

i) If sig $(f) = (6,0)$ then $Q_f = T_6$, where T_6 is the unique quadratic factor of the equation given in [6, Appendix].

ii) If sig $(f) = (4,1)$ then $Q_f = T_4 + S_1$, where T_4 is the quadratic given in Eq. (47) and S_1 as

$$S_1 = 2u_1^2\left(x^2 - 2\,\mathrm{Re}(\beta)x + ||\beta||^2\right)$$

for some $\beta \in \mathcal{H}_2$ such that $f(\beta) = 0$.

iii) If sig $(f) = (2,2)$ then $Q_f = T_2 + S_2$, where T_2 is given as

$$T_2 = t_1^2\,(x - \alpha_1)^2 + t_2^2\,(x - \alpha_2)^2$$

and S_2 is the unique quadratic factor of Eq. (40).

iv) If sig $(f) = (0,3)$ then $Q_f = S_3$, where S_3 is the unique quadratic factor of the equation given in [6, Appendix].

REFERENCES

[1] L. Beshaj, R. Hidalgo, S. Kruk, A. Malmendier, S. Quispe, and T. Shaska, *Rational points in the moduli space of genus two*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 83–115. MR3782461

[2] L. Beshaj and T. Shaska, *Decomposition of some jacobian varieties of dimension 3*, Artificial intelligence and symbolic computation, 2015, pp. 193–204.

[3] L. Beshaj, T. Shaska, and C. Shor, *On Jacobians of curves with superelliptic components*, Riemann and Klein surfaces, automorphisms, symmetries and moduli spaces, 2014, pp. 1–14.

[4] L. Beshaj and F. Thompson, *Equations for superelliptic curves over their minimal field of definition*, Albanian J. Math. **8** (2014), no. 1, 3–10.

[5] Lubjana Beshaj, *Reduction theory of binary forms*, Advances on superelliptic curves and their applications, 2015, pp. 84–116. MR3525574

[6] ———, *Integral binary forms with minimal height*, ProQuest LLC, Ann Arbor, MI, 2016. Thesis (Ph.D.)–Oakland University. MR3579531

[7] ———, *Minimal integral Weierstrass equations for genus 2 curves*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 63–82. MR3782460

[8] Lubjana Beshaj and Takuya Yamauchi, *On Prym varieties for the coverings of some singular plane curves*, Manuscripta Math. **158** (2019), no. 1-2, 205–222. MR3895755
[9] B. J. Birch and J. R. Merriman, *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. (3) **24** (1972), 385–394. MR0306119
[10] E. Bombieri and J. Vaaler, *On Siegel's lemma*, Invent. Math. **73** (1983), no. 1, 11–32. MR707346
[11] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774 (2007a:11092)
[12] Ducan A. Buell, *Binary quadratic forms*, Springer-Verlag, 1989.
[13] A. W. Reid C. Maclachlan, *The arithmetic of hyperbolic 3-manifolds*, Springer, 2003.
[14] John E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput Math **2** (1999), 64–94.
[15] Jacques Dixmier, *Quelques aspects de la théorie des invariants*, Gaz. Math. **43** (1990), 39–64. Translated by J.-R. Billuard. MR1035388
[16] J. Elstrodt, F. Gruenewald, and J. Mennicke, *Groups acting on hyperbolic space*, Springer, 1998.
[17] Jan-Hendrik Evertse, *Estimates for discriminants and resultants of binary forms*, Advances in number theory (Kingston, ON, 1991), 1993, pp. 367–380. MR1368433 (96i:11074)
[18] ———, *Estimates for reduced binary forms*, J. Reine Angew. Math. **434** (1993), 159–190. MR1195694 (94h:11037)
[19] Paul Gordan, *Vorlesungen über Invariantentheorie*, Second, Chelsea Publishing Co., New York, 1987. Erster Band: Determinanten. [Vol. I: Determinants], Zweiter Band: Binare Formen. [Vol. II: Binary forms], Edited by Georg Kerschensteiner. MR917266
[20] K. Gyory, *On pairs of binary forms with given resultant or given semi-resultant*, Math. Pannon. **4** (1993), no. 2, 169–180. MR1258923 (94k:11044)
[21] C. Hooley, *On totally reducible binary forms. I*, Proc. Indian Acad. Sci. Math. Sci. **111** (2001), no. 3, 249–262. MR1851090 (2002f:11128)
[22] ———, *On totally reducible binary forms. II*, Hardy-Ramanujan J. **25** (2002), 22–50. MR1939587 (2003j:11112)
[23] Gaston Julia, *Étude sur les formes binaires non quadratiques à indéterminées réelles ou complexes.*, Mémories de lAcadémie des Sciences de lInsitut de France **55** (1917), 1–296.
[24] Joseph P. S. Kung and Gian-Carlo Rota, *The invariant theory of binary forms*, Bull. Amer. Math. Soc. (N.S.) **10** (1984), no. 1, 27–85. MR722856
[25] T. Y. Lam, *Introduction to quadratic forms over fields*, American Mathematical Soc., 2005.
[26] D. J. Lewis and K. Mahler, *On the representation of integers by binary forms*, Acta Arith. **6** (1960/1961), 333–363. MR0120195
[27] K. Mahler, *On some inequalities for polynomials in several variables*, J. London Math. Soc. **37** (1962), 341–344. MR0138593
[28] L. J. Mordell, *On numbers represented by binary cubic forms*, Proc. London Math. Soc. (2) **48** (1943), 198–228. MR0009610
[29] Anna Morra, *An algorithm to compute relative cubic fields*, Mathematics of Computation **82** (2013), no. 284, 2343–2361.
[30] Jürgen Neukrich, *Algebraic number theory* (1, ed.), Vol. 322, Springer-Verlag, Berlin Heidelberg, 1999.
[31] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7. MR0344216 (49 #8956)
[32] T. Shaska and L. Beshaj, *Heights on algebraic curves*, Advances on superelliptic curves and their applications, 2015, pp. 137–175. MR3525576
[33] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210 (87g:11070)
[34] Michael Stoll and John E. Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99. MR2024647 (2005e:11091)
[35] Gerard van der Geer, *Hilbert modular surfaces*, Springer-Verlag, 1988.

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 79–88
ISSN: 1930-1235; (**2018**)

CHARACTER DEGREES OF GROUPS ASSOCIATED WITH FINITE SPLIT BASIC ALGEBRAS WITH INVOLUTION

CARLOS A. M. ANDRÉ

Dedicated to the memory of Kay Magaard

Abstract. Let $\mathcal{A}$ be a finite-dimensional split basic algebra over a finite field $\Bbbk$ with odd characteristic, and assume that $\mathcal{A}$ is endowed with an involution $\sigma\colon \mathcal{A} \to \mathcal{A}$. We determine the degrees of the irreducible characters of the group $C_G(\sigma) = \{x \in G\colon \sigma(x^{-1}) = x\}$ where $G = \mathcal{A}^\times$ is the unit group of $\mathcal{A}$, and prove that every irreducible character of $C_G(\sigma)$ is induced by a linear character of some subgroup. As a particular case, our results hold for the Sylow p-subgroups of the finite classical groups of Lie type, and extend (in a uniform way) the results obtained by B. Szegedy in [11].

Mathematics Subject Classes 2010: 20C15; 20G40
Keywords: finite algebra group; irreducible character; classical group

Let p be an odd prime, let $\Bbbk$ be a finite field of characteristic p, and let $\mathcal{A}$ be a finite-dimensional associative $\Bbbk$-algebra (with identity). We recall that an *involution* on $\mathcal{A}$ is a map $\sigma\colon \mathcal{A} \to \mathcal{A}$ satisfying the following conditions:

(1) $\sigma(a+b) = \sigma(a) + \sigma(b)$ for all $a, b \in \mathcal{A}$;
(2) $\sigma(ab) = \sigma(b)\sigma(a)$ for all $a, b \in \mathcal{A}$;
(3) $\sigma^2(a) = a$ for all $a \in \mathcal{A}$.

We note that an involution σ is not required to be $\Bbbk$-linear; however, we will assume that the field $\Bbbk = \Bbbk \cdot 1$ is preserved by σ. Then, σ defines a field automorphism of $\Bbbk$ which is either the identity or has order 2; we say that σ is *of the first kind* if σ fixes $\Bbbk$, and *of the second kind* if its restriction $\sigma_{\Bbbk}$ to $\Bbbk$ has order 2. In any case, we let $\Bbbk^\sigma = \{\alpha \in \Bbbk\colon \sigma(\alpha) = \alpha\}$ denote the σ-fixed subfield of $\Bbbk$, and consider $\mathcal{A}$ as a finite dimensional associative $\Bbbk^\sigma$-algebra. We observe that σ is of the second kind if and only if the field extension $\Bbbk^\sigma \subseteq \Bbbk$ has degree 2, and $\sigma\colon \Bbbk \to \Bbbk$ is the *Frobenius map* defined by the mapping $\alpha \mapsto \alpha^q$ where $q = |\Bbbk^\sigma|$; hence, $\Bbbk^\sigma = \mathbb{F}_q$ and $\Bbbk = \mathbb{F}_{q^2}$. For simplicity of writing, we will the bar notation $\overline{\alpha} = \alpha^q$ for $\alpha \in \Bbbk$.

Let $G = \mathcal{A}^\times$ denote the unit group of the $\Bbbk$-algebra $\mathcal{A}$. Then, for any involution $\sigma\colon \mathcal{A} \to \mathcal{A}$, the cyclic group $\langle\sigma\rangle$ acts on G as a group of automorphisms by means of $x^\sigma = \sigma(x^{-1})$ for all $x \in G$ (x^σ should not be confused with $\sigma(x)$). For any

This research was made within the activities of the Group for Linear, Algebraic and Combinatorial Structures of the Center for Functional Analysis, Linear Structures and Applications (University of Lisbon, Portugal), and was partially supported by the Fundação para a Ciência e Tecnologia (Lisbon, Portugal) through the Strategic Project UID/MAT/04721/2013.

σ-invariant subgroup $H \leq G$, we denote by $C_H(\sigma)$ the subgroup of H consisting of all σ-fixed elements; that is,

$$C_H(\sigma) = \{x \in H \colon x^\sigma = x\} = \{x \in H \colon \sigma(x^{-1}) = x\}.$$

The main purpose of this paper is to determine the degree of any irreducible (complex) character of the group $C_G(\sigma)$ in the case where $\mathcal{A}$ is an arbitrary basic $\Bbbk$-algebra endowed with an involution $\sigma \colon \mathcal{A} \to \mathcal{A}$. By definition, a $\Bbbk$-algebra $\mathcal{A}$ is said to be *basic* if the Jacobson radical $\operatorname{Rad}(\mathcal{A}) \leq \mathcal{A}$ equals the set consisting of all nilpotent elements of $\mathcal{A}$; equivalently, the semisimple $\Bbbk$-algebra $\mathcal{A}/\operatorname{Rad}(\mathcal{A})$ is isomorphic to a direct sum $\Bbbk_1 \oplus \cdots \oplus \Bbbk_n$ of field extensions $\Bbbk_1, \ldots, \Bbbk_n$ of $\Bbbk$ (in the paper [10], B. Szegedy refers to $\mathcal{A}$ as an *N-algebra* over $\Bbbk$; see, in particular, [10, Lemma 2.1]). We note that every subalgebra (containing the identity) of a basic $\Bbbk$-algebra is also a basic $\Bbbk$-algebra; moreover, if $\mathcal{I}$ is any (two-sided) ideal of $\mathcal{A}$, then $\mathcal{A}/\mathcal{I}$ is also a basic $\Bbbk$-algebra. In the case where $\Bbbk_i \cong \Bbbk$ for all $1 \leq i \leq n$, we refer to $\mathcal{A}$ as a *split basic* $\Bbbk$*-algebra* (or, in the terminology of [10], as a *DN-algebra*); we observe that subalgebras (containing the identity) and quotient algebras of a split basic $\Bbbk$-algebra are also slit basic $\Bbbk$-algebras (see, for example, [10, Lemmas 2.2 and 2.3]).

As a standard example, let $\mathcal{M}_n(\Bbbk)$ be the full matrix algebra over $\Bbbk$ consisting of all $n \times n$ matrices with entries in $\Bbbk$, so that $\mathcal{M}_n(\Bbbk)^\times = \mathrm{GL}_n(\Bbbk)$ is the general linear group consisting of all invertible matrices in $\mathcal{M}_n(\Bbbk)$. The $\Bbbk$-algebra $\mathcal{M}_n(\Bbbk)$ is canonically endowed with the *transpose involution* defined by the mapping $a \mapsto a^\intercal$ where $a^\intercal$ denotes the transpose of $a \in \mathcal{M}_n(\Bbbk)$. Let $q = |\Bbbk^\sigma|$, let $F \colon \mathcal{M}_n(\Bbbk) \to \mathcal{M}_n(\Bbbk)$ be the Frobenius morphism defined by $F(a_{ij}) = (\overline{a_{ij}}) = (a_{ij}{}^q)$ for all $(a_{ij}) \in \mathcal{M}_n(\Bbbk)$, and set $a^* = F(a)^\intercal$ for all $a \in \mathcal{M}_n(\Bbbk)$. Then, the mapping $a \mapsto a^*$ defines an involution on $\mathcal{M}_n(\Bbbk)$; notice that, if $\Bbbk^\sigma = \Bbbk$, then $a^* = a^\intercal$ for all $a \in \mathcal{M}_n(\Bbbk)$. If $\sigma \colon \mathcal{M}_n(\Bbbk) \to \mathcal{M}_n(\Bbbk)$ is an involution of the first kind, then there exists $u \in \mathrm{GL}_n(\Bbbk)$ with $u^\intercal = \pm u$ and such that $\sigma(a) = u^{-1}a^\intercal u$ for all $a \in \mathcal{M}_n(\Bbbk)$; moreover, the matrix u is uniquely determined up to a factor in $\Bbbk^\times$. On the other hand, if $\sigma \colon \mathcal{M}_n(\Bbbk) \to \mathcal{M}_n(\Bbbk)$ is an involution of the second kind, then there exists $u \in \mathrm{GL}_n(\Bbbk)$ with $u^* = u$ and such that $\sigma(a) = u^{-1}a^* u$ for all $a \in \mathcal{M}_n(\Bbbk)$; moreover, the matrix u is uniquely determined up to a factor in $(\Bbbk^\sigma)^\times$. (The proofs can be found in the book [8] by M.-A. Knus *et al.* where the complete classification of involutions is also given for arbitrary central $\Bbbk$-algebras.) For simplicity, for $u \in \mathrm{GL}_n(\Bbbk)$ as above, we will denote by σ_u the involution on $\mathcal{M}_n(\Bbbk)$ given by the mapping $a \mapsto u^{-1}a^* u$; as usual, we say that σ_u is *symplectic* if σ_u is of the first kind and $u^\intercal = -u$, *orthogonal* if σ_u is of the first kind and $u^\intercal = u$, and *unitary* if σ_u is of the second kind and $u^* = u$.

For an arbitrary involution $\sigma \colon \mathcal{M}_n(\Bbbk) \to \mathcal{M}_n(\Bbbk)$ the group $C_{\mathrm{GL}_n(\Bbbk)}(\sigma)$ is isomorphic to one of the well-known *finite classical groups of Lie type* (defined over $\Bbbk$): the *symplectic group* $\mathrm{Sp}_{2m}(q)$ if σ is symplectic (and $\Bbbk = \mathbb{F}_q$), the *orthogonal groups* $\mathrm{O}^+_{2m}(q)$, $\mathrm{O}_{2m+1}(q)$, or $\mathrm{O}^-_{2m+2}(q)$ if σ is orthogonal (and $\Bbbk = \mathbb{F}_q$), and the *unitary group* $\mathrm{U}_n(q^2)$ if σ is unitary (and $\Bbbk = \mathbb{F}_{q^2}$). (For the details on the definition of the classical groups, we refer to Chapter I the book [2] by R. Carter.) In fact, up to isomorphism, these groups may be defined by the involution $\sigma = \sigma_u$ where $u \in \mathrm{GL}_n(\Bbbk)$ is defined as follows; here, J_m denotes the $m \times m$ matrix with 1's along the anti-diagonal and 0's elsewhere.

(1) For $\mathrm{Sp}_{2m}(q)$, we choose $\Bbbk = \mathbb{F}_q$ and $u = \left(\begin{smallmatrix} 0 & J_m \\ -J_m & 0 \end{smallmatrix}\right)$.

(2) For $\mathrm{O}^+_{2m}(q)$ or $O_{2m+1}(q)$, we choose $\Bbbk = \mathbb{F}_q$ and $u = J_n$ where, either $n = 2m$, or $n = 2m+1$.
(3) For $\mathrm{O}^-_{2m+2}(q)$, we choose $\Bbbk = \mathbb{F}_q$ and $u = \left(\begin{smallmatrix} 0 & 0 & J_m \\ 0 & c & 0 \\ J_m & 0 & 0 \end{smallmatrix}\right)$ where $c = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -\varepsilon \end{smallmatrix}\right)$ for $\varepsilon \in \mathbb{F}_q^\times - (\mathbb{F}_q^\times)^2$.
(4) For $\mathrm{U}_n(q^2)$, we choose $\Bbbk = \mathbb{F}_{q^2}$ and $u = J_n$. (In this case, we have $\Bbbk^\sigma = \mathbb{F}_q$.)

Let $\mathcal{A} = \mathfrak{b}_n(\Bbbk)$ be the *Borel subalgebra* of $\mathcal{M}_n(\Bbbk)$ consisting of all upper-triangular matrices; hence, $G = \mathcal{A}^\times$ is the standard Borel subgroup $B_n(\Bbbk)$ of $\mathrm{GL}_n(\Bbbk)$. Then, $\mathcal{A}$ is a split basic $\Bbbk$-algebra; in fact, the Jacobson radical $\mathrm{Rad}(\mathcal{A})$ is the (upper) niltriangular subalgebra $\mathfrak{ut}_n(\Bbbk) \leq \mathfrak{b}_n(\Bbbk)$ consisting of all upper-triangular matrices with 0's on the main diagonal, and $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ is isomorphic to a direct sum of n copies of $\Bbbk$; indeed, $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$ is isomorphic to the diagonal subalgebra $\mathfrak{d}_n(\Bbbk)$ consisting of all diagonal matrices in $\mathcal{M}_n(\Bbbk)$. Further, $\mathcal{A}$ is a σ-invariant subalgebra of $\mathcal{M}_n(\Bbbk)$, and the $C_G(\sigma)$ is a (standard) Borel subgroup of the corresponding finite classical group.

In the general situation, let $\mathcal{A}$ be a split basic $\Bbbk$-algebra with an involution $\sigma\colon \mathcal{A} \to \mathcal{A}$. For any (nilpotent) subalgebra $\mathcal{J}$ of $\mathrm{Rad}(\mathcal{A})$, the set $1+\mathcal{J}$ is a p-subgroup of the unit group $G = \mathcal{A}^\times$ to which we refer as an *algebra subgroup* of G (as defined in [6]). In the particular case where $\mathcal{J} = \mathrm{Rad}(\mathcal{A})$, it is clear that $P = 1 + \mathrm{Rad}(\mathcal{A})$ is a normal subgroup of G, and that it is the unique Sylow p-subgroup of G. Furthermore, G is the semidirect product $G = TP$ where $T \leq G$ is isomorphic to the unit group of $\mathcal{A}/\mathrm{Rad}(\mathcal{A})$; hence, T is isomorphic to the direct product $\Bbbk_1^\times \times \cdots \times \Bbbk_n^\times$ where $\Bbbk_1, \ldots, \Bbbk_n$ are field extensions of $\Bbbk$ such that $\mathcal{A}/\mathrm{Rad}(\mathcal{A}) \cong \Bbbk_1 \oplus \cdots \oplus \Bbbk_n$. Since $\mathcal{A}$ is split, we have $\Bbbk_i \cong \Bbbk$ for all $1 \leq i \leq n$, and in fact there are nonzero orthogonal idempotents $e_1, \ldots, e_n \in \mathcal{A}$ with $1 = e_1 + \cdots + e_n$, and such that $\mathcal{A} = \mathcal{D} \oplus \mathrm{Rad}(\mathcal{A})$ for $\mathcal{D} = \Bbbk e_1 \oplus \cdots \oplus \Bbbk e_n$; this follows easily from the usual process of "lifting idempotents" (see, for example, [9, Chapter VII]; see also [5, Lemma 2.1]). Then, $T = \mathcal{D}^\times$ is the unit group of the subalgebra $\mathcal{D}$; we will refer to $\mathcal{D}$ as the *diagonal subalgebra* of $\mathcal{A}$, and to T as the *diagonal subgroup* of $G = \mathcal{A}^\times$. In particular, we have $|G| = |\Bbbk|^r(|\Bbbk| - 1)^n$ where $r = \dim \mathrm{Rad}(\mathcal{A})$.

On the other hand, let $x \in G$ be arbitrary, and denote by $C_G(x)$ the centraliser of x in G (with respect to conjugation). It is clear that $C_G(x)$ is the unit group of the subalgebra $C_\mathcal{A}(x) = \{a \in \mathcal{A}\colon ax = xa\}$ of $\mathcal{A}$. Since every subalgebra of a split basic $\Bbbk$-algebra is also a split basic $\Bbbk$-algebra (see [10, Lemma 2.2]), $C_\mathcal{A}(x)$ is a split basic $\Bbbk$-algebra, and thus $|C_G(x)| = |\Bbbk|^s(|\Bbbk| - 1)^m$ for some nonnegative integers s and m (with $s \leq r$ and $m \leq n$). Since $(|\Bbbk|, |\Bbbk| - 1) = 1$, we deduce the following result.

Theorem 1 (Szegedy; see [10, Lemma 2.4])**.** *Let $\mathcal{A}$ be a split basic $\Bbbk$-algebra, let $G = \mathcal{A}^\times$, and let $\mathcal{K}$ be a conjugacy class of G. Then, $|\mathcal{K}| = |\Bbbk|^k(|\Bbbk| - 1)^l$ for some nonnegative integers k and l.*

Next, we consider the involution $\sigma\colon \mathcal{A} \to \mathcal{A}$, and determine the order of the σ-fixed subgroup $C_G(\sigma)$. We start by proving the following elementary result.

Lemma 1. *Let $\mathcal{A}$ be a $\Bbbk$-algebra with an involution $\sigma\colon \mathcal{A} \to \mathcal{A}$, let $\mathcal{J}$ be a σ-invariant nilpotent subalgebra of $\mathcal{A}$, and let $Q = 1 + \mathcal{J}$. Then, $|C_Q(\sigma)|$ is a power of $|\Bbbk^\sigma|$.*

Proof. Let $\varphi\colon \mathcal{J} \to Q$ be the Cayley transform defined by $\varphi(a) = (1-a)(1+a)^{-1}$ for all $a \in \mathcal{J}$. Since p is odd, the map φ is bijective, and it is easy to check that

$C_Q(\sigma) = \varphi(C_{\mathcal{J}}(\sigma))$ where $C_{\mathcal{J}}(\sigma) = \{a \in \mathcal{J} \colon \sigma(a) = -a\}$. The result follows because $C_{\mathcal{J}}(\sigma)$ is a vector space over $\Bbbk^\sigma$. □

On the other hand, we have the following.

Theorem 2. *Let $\mathcal{A}$ be a split basic $\Bbbk$-algebra with an involution $\sigma \colon \mathcal{A} \to \mathcal{A}$, let $G = \mathcal{A}^\times$ be the unit group of $\mathcal{A}$, and let $P = 1 + \mathrm{Rad}(\mathcal{A})$. Let $\Bbbk^\sigma$ be the σ-fixed field of $\Bbbk$, and let $q = |\Bbbk^\sigma|$. Then, $C_G(\sigma)/C_P(\sigma) \cong H \times K$ where H is a direct product of copies of $\Bbbk^\times$, and K is a direct product of cyclic groups of order $(q-1)/2$ if σ is of the first kind, and $q-1$ if σ is of the second kind. In particular, there exist nonnegative integers k and r such that*

$$|C_G(\sigma) : C_P(\sigma)| = \begin{cases} 2^{-k}(q-1)^r, & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k(q-1)^r, & \text{if } \sigma \text{ is of the second kind.} \end{cases}$$

Further, we have $C_G(\sigma)P/P = C_{G/P}(\sigma)$.

Proof. Let $e_1, \dots, e_n \in \mathcal{A}$ be nonzero orthogonal idempotents, and consider the diagonal subalgebra $\mathcal{D} = \Bbbk e_1 \oplus \cdots \oplus \Bbbk e_n$ of $\mathcal{A}$; moreover, for simplicity, we set $\mathcal{J} = \mathrm{Rad}(\mathcal{A})$.

Let S_n denote the symmetric group on $\{1, 2, \dots, n\}$. Since $\sigma(e_1), \cdots, \sigma(e_n)$ are nonzero orthogonal idempotents satisfying $1 = \sigma(e_1) + \cdots + \sigma(e_n)$, there exist a permutation $\pi \in S_n$ and an invertible element $x \in P = 1 + \mathcal{J}$ such that $\sigma(e_i) = xe_{\pi(i)}x^{-1}$ for all $1 \le i \le n$ (see, for example, [9, Theorem VII.13]). In particular, we see that $\sigma(e_i) \in e_{\pi(i)} + \mathcal{J}$, and thus $\sigma(\Bbbk e_i) = \Bbbk\sigma(e_i) \subseteq \Bbbk e_{\pi(i)} + \mathcal{J}$ for all $1 \le i \le n$. Moreover, since σ is an involution, we clearly have $\pi^2 = 1$.

The involution $\sigma \colon \mathcal{A} \to \mathcal{A}$ defines naturally an involution on the $\Bbbk$-algebra $\mathcal{A}/\mathcal{J}$; if we denote this involution also by σ, then $\sigma(a+\mathcal{J}) = \sigma(a)+\mathcal{J}$ for all $a \in \mathcal{A}$. Hence, σ defines an automorphism of the group $G/P \cong (A/\mathcal{J})^\times$ by means of $(xP)^\sigma = x^\sigma P$ for all $x \in G$. Since $\mathcal{A} = \mathcal{D} \oplus \mathcal{J}$, we have $\mathcal{A}/\mathcal{J} \cong \mathcal{D}$, and thus $G/P \cong T$ where $T = \mathcal{D}^\times$ is the diagonal subgroup of G. For every $t \in T$, we have $tP \in C_{G/P}(\sigma)$ if and only if $t^{-1}t^\sigma \in P$, and so $C_{G/P}(\sigma) = \{tP \colon t^{-1}t^\sigma \in P\}$. On the other hand, since $\mathcal{D} = \Bbbk e_1 \oplus \cdots \oplus \Bbbk e_n$, every element of $t \in T = \mathcal{D}^\times$ is uniquely expressed as a sum $t = \alpha_1 e_1 + \cdots + \alpha_n e_n$ where $\alpha_1, \dots, \alpha_n \in \Bbbk^\times$. In particular, for every $1 \le i \le n$ and every $\alpha \in \Bbbk^\times$, the element

$$t_i(\alpha) = \alpha e_i + \sum_{1 \le j \ne i \le n} e_i$$

lies in T; indeed, every $t \in T$ factorises uniquely as a product $t = t_1(\alpha_1) \cdots t_n(\alpha_n)$ where $\alpha_1, \dots, \alpha_n \in \Bbbk^\times$. For every $1 \le i \le n$, let $T_i = \{t_i(\alpha) \colon \alpha \in \Bbbk^\times\}$; notice that $T_1, \dots, T_n$ are subgroups of T and that T is the (internal) direct product $T = T_1 \cdots T_n$. Similarly, if we define $\overline{T}_i = T_iP/P$ for all $1 \le i \le n$, then G/P is the direct product $G/P = \overline{T}_1 \cdots \overline{T}_n$; moreover, since $\sigma(\Bbbk e_i) \subseteq \Bbbk e_{\pi(i)} + \mathcal{J}$, we must have $(\overline{T}_i)^\sigma \subseteq \overline{T}_{\pi(i)}$, and hence $(\overline{T}_i)^\sigma = \overline{T}_{\pi(i)}$ for all $1 \le i \le n$.

Now, if $t \in T$ is arbitrary and $t = t_1 \cdots t_n$ where $t_i \in T_i$ for all $1 \le i \le n$, then $t^{-1}t^\sigma = (t_1^{-1}(t_{\pi(1)})^\sigma) \cdots (t_n^{-1}(t_{\pi(n)})^\sigma)$ where $t_i^{-1}(t_{\pi(i)})^\sigma \in T_iP$ for all $1 \le i \le n$, and so $t^{-1}t^\sigma \in P$ if and only if $t_i^{-1}(t_{\pi(i)})^\sigma \in P$ for all $1 \le i \le n$; in other words, we have $tP \in C_{G/P}(\sigma)$ if and only if $t_i^{-1}(t_{\pi(i)})^\sigma \in P$ for all $1 \le i \le n$. In particular, if we set $\bar{t}_i(\alpha) = t_i(\alpha)P$, then $\bar{t}_i(\alpha)\bar{t}_i(\alpha)^\sigma \in C_{G/P}(\sigma)$ for all $\alpha \in \Bbbk^\times$ and all $1 \le i \le n$. In fact, it is straightforward to check that, for all $1 \le i \le n$, the

mapping $\alpha \mapsto \bar{t}_i(\alpha)\bar{t}_i(\alpha)^\sigma$ defines a group homomorphism $\gamma_i \colon \Bbbk^\times \to C_{G/P}(\sigma)$, and that $C_{G/P}(\sigma) = \prod_{i\in I} \operatorname{Im}(\gamma_i)$ where I is a complete set of representatives of the π-orbits on $\{1, 2, \ldots, n\}$. In particular, we conclude that

$$|C_{G/P}(\sigma)| = \prod_{i\in I} |\operatorname{Im}(\gamma_i)|.$$

It is clear that γ_i is injective whenever $i \in I$ is such that $\pi(i) \neq i$. On the other hand, let $i \in I$ be such that $\pi(i) = i$. In this case, $(\Bbbk e_i + \mathcal{J})/\mathcal{J} = \Bbbk \bar{e}_i$ where $\bar{e}_i = e_i + \mathcal{J}$, and we have $\sigma(\alpha\bar{e}_i) = \alpha^q e_i + \mathcal{J}$ for all $\alpha \in \Bbbk$. In particular, for any $\alpha \in \Bbbk^\times$, we deduce that $\alpha \in \ker(\gamma_i)$ if and only if $\alpha = \alpha^q$, and so

$$|\operatorname{Im}(\gamma_i)| = \begin{cases} q-1, & \text{if } \Bbbk^\sigma = \Bbbk, \\ (q-1)/2, & \text{if } \Bbbk^\sigma \neq \Bbbk. \end{cases}$$

Furthermore, we conclude that $C_{G/P}(\sigma)$ is isomorphic to a direct product $H \times K$ where H is a direct product of copies of $\Bbbk^\times$, and K is a direct product of cyclic groups of order $(q-1)/2$ if σ is of the first kind, or $q-1$ if σ is of the second kind. In particular, there exist nonnegative integers k and r such that

$$|C_{G/P}(\sigma)| = \begin{cases} 2^{-k}(q-1)^r, & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k(q-1)^r, & \text{if } \sigma \text{ is of the second kind.} \end{cases}$$

If we assume further that the diagonal subalgebra $\mathcal{D} \leq \mathcal{A}$ is σ-invariant, we clearly have a semidirect product $C_G(\sigma) = C_T(\sigma)C_P(\sigma)$ where $T = \mathcal{D}^\times$, and thus $C_{G/P}(\sigma) \cong C_T(\sigma) \cong C_G(\sigma)/C_P(\sigma)$. Therefore, in this situation, we conclude that there exist nonnegative integers k and r such that

$$|C_G(\sigma) : C_P(\sigma)| = \begin{cases} 2^{-k}(q-1)^r, & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k(q-1)^r, & \text{if } \sigma \text{ is of the second kind.} \end{cases}$$

In the general situation, let $\widetilde{G}$ be the semidirect product $\widetilde{G} = G \ltimes \langle\sigma\rangle$ of G by the cyclic group $\langle\sigma\rangle$. Since $\widetilde{G}$ is solvable and $\sigma \in \widetilde{G}$ has order 2, Hall's Theorem (see [3, Theorem 6.41]) asserts that there exists a Hall p'-subgroup $\widetilde{S} \leq \widetilde{G}$ with $\sigma \in \widetilde{S}$. Then, $S = \widetilde{S} \cap G$ is a Hall p'-subgroup of G, and we have $G = PS$ (by order considerations); moreover, since $\sigma \in \widetilde{S}$, the subgroup S is clearly σ-invariant. It follows that $C_G(\sigma)$ is the semidirect product $C_G(\sigma) = C_P(\sigma)C_S(\sigma)$, and hence $C_G(\sigma)P/P \cong C_S(\sigma) \cong C_{G/P}(\sigma)$. □

We are now able to determine the size of any conjugacy class of $C_G(\sigma)$.

Theorem 3. *Let $\mathcal{A}$ be a split basic $\Bbbk$-algebra with an involution $\sigma \colon \mathcal{A} \to \mathcal{A}$, let $G = \mathcal{A}^\times$, and let $\mathcal{K}$ be a conjugacy class of $C_G(\sigma)$. Then, there exist nonnegative integers k, r and s such that*

$$|\mathcal{K}| = \begin{cases} 2^{-k}(q-1)^r q^s, & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k(q-1)^r q^s, & \text{if } \sigma \text{ is of the second kind,} \end{cases}$$

where $q = |\Bbbk^\sigma|$.

Proof. Let $x \in \mathcal{K}$ be arbitrary, and recall that $C_G(x)$ is the unit group $H = \mathcal{B}^\times$ of the subalgebra $\mathcal{B} = C_{\mathcal{A}}(x)$ of $\mathcal{A}$. Since $x \in C_G(\sigma)$, it is clear that $\mathcal{B}$ is σ-invariant. Since $C_H(\sigma) = H \cap C_G(\sigma)$, we have $|\mathcal{K}| = |C_G(\sigma) : C_H(\sigma)|$, and thus

$$|\mathcal{K}| = |C_G(\sigma) : C_P(\sigma)|\, |C_H(\sigma) : C_Q(\sigma)|^{-1} |C_P(\sigma) : C_Q(\sigma)|$$

where $Q = P \cap H = 1 + \mathrm{Rad}(\mathcal{B})$. The result follows by Lemma 1 and by the previous theorem. □

Next, we consider the irreducible characters of $C_G(\sigma)$. Our goal is to prove the following main result. (We observe that, in the case where σ is an involution of the first kind, this result is essentially [11, Theorem 6].)

Theorem 4. *Let $\mathcal{A}$ be a split basic $\Bbbk$-algebra with an involution $\sigma\colon \mathcal{A} \to \mathcal{A}$, let $G = \mathcal{A}^\times$ be the unit group of $\mathcal{A}$, and let χ be an arbitrary irreducible character of $C_G(\sigma)$. Then, there exist nonnegative integers k, r and s such that*

$$\chi(1) = \begin{cases} 2^{-k}(q-1)^r q^s, & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k (q-1)^r q^s, & \text{if } \sigma \text{ is of the second kind,} \end{cases}$$

where $q = |\Bbbk^\sigma|$.

The following reduction result will be crucial for the proof of this theorem. As usual, given an arbitrary function $\chi\colon G \to \mathbb{C}$ of a group G and an arbitrary element $g \in G$, we define the function $\chi^g\colon G \to \mathbb{C}$ by the rule $\chi^g(x) = \chi(gxg^{-1})$ for all $x \in G$; similarly, given an arbitrary subset $\mathcal{X}$ of G and an arbitrary element $g \in G$, we define $\mathcal{X}^g = \{x^g\colon x \in \mathcal{X}\}$ where $x^g = gxg^{-1}$ for all $x \in G$.

Theorem 5. *Let $\mathcal{A}$ be a split basic $\Bbbk$-algebra with an involution $\sigma\colon \mathcal{A} \to \mathcal{A}$, let $G = \mathcal{A}^\times$ be the unit group of $\mathcal{A}$, and let $P = 1 + \mathrm{Rad}(\mathcal{A})$. Let χ be a σ-invariant irreducible character of P, and let $I_G(\chi) = \{g \in G\colon \chi^g = \chi\}$ be the inertia group of χ. Then, $I_G(\chi) = \mathcal{B}^\times$ for some σ-invariant subalgebra $\mathcal{B} \leq \mathcal{A}$.*

Proof. Let $\widetilde{G}$ be the semidirect product $\widetilde{G} = G \ltimes \langle\sigma\rangle$ of G by the cyclic group $\langle\sigma\rangle$. Since $P = 1 + \mathrm{Rad}(\mathcal{A})$ is σ-invariant, P is a normal subgroup of $\widetilde{G}$. As in the proof of Theorem 2, we may choose a Hall p'-subgroup $S \leq \widetilde{G}$ with $\sigma \in S$ and such that $\widetilde{G}$ is the semidirect product $\widetilde{G} = PS$.

The group S acts naturally on the set $\mathrm{Irr}(P)$ of irreducible characters of P and on the set $\mathrm{Cl}(P)$ of conjugacy classes of P. By [7, Theorem 13.24], these actions are permutation isomorphic. Let $\beta\colon \mathrm{Irr}(P) \to \mathrm{Cl}(P)$ be a S-equivariant bijection, and let $\mathcal{K} = \beta(\chi)$. Then, $C_S(\chi) = \{s \in S\colon \mathcal{K}^s = \mathcal{K}\}$. Since $C_S(\chi)$ is a p'-group, Glauberman's Lemma (see [7, Lemma 13.8]) implies that there exists $x \in \mathcal{K}$ such that $x^s = x$ for all $s \in C_S(\chi)$; in particular, since χ is σ-invariant, we have $\sigma \in C_S(\chi)$, and thus $x^\sigma = x$.

We now claim that $I_G(\chi) = PC_G(x)$. In fact, let $g \in G$ be arbitrary. Since $\widetilde{G} = PS$, there are uniquely determined elements $h \in P$ and $s \in S \cap G$ such that $g = hs$; thus, we have $\mathcal{K}^g = \mathcal{K}^s$ and $\chi^g = \chi^s$. On the one hand, suppose that $g \in C_G(x)$. Then, $\mathcal{K}^s = \mathcal{K}^g = \mathcal{K}$, and so $s \in C_{S\cap G}(\chi) \leq I_G(\chi)$. On the other hand, suppose that $g \in I_G(\chi)$. Then, $\chi^s = \chi^g = \chi$, and so $s \in C_S(\chi)$. By the choice of x, we conclude that $s \in C_G(x)$, and thus $g = hs \in PC_G(x)$. The claim follows.

To complete the proof it is enough to take $\mathcal{B} = C_{\mathcal{A}}(x) + \mathrm{Rad}(\mathcal{A})$ where $C_{\mathcal{A}}(x) = \{a \in \mathcal{A}\colon xa = ax\}$; it is clear that $\mathcal{B}$ is a σ-invariant subalgebra of $\mathcal{A}$, and that $\mathcal{B}^\times = PC_G(x) = I_G(x)$. □

We now proceed with the proof of Theorem 4.

Proof of Theorem 4. We start by recalling the Glauberman correspondence between σ-invariant irreducible characters of $P = 1 + \mathrm{Rad}(\mathcal{A})$ and irreducible characters of $C_P(\sigma)$; our main reference is [7, Chapter 13]. As usual, we denote by $\mathrm{Irr}(P)$ the set consisting of all irreducible characters of P (and extend this notation to any finite group), and by $\mathrm{Irr}_\sigma(P)$ the subset of $\mathrm{Irr}(P)$ consisting of all σ-invariant irreducible characters. Since p is odd, the Glauberman correspondence asserts that there exists a uniquely defined bijective map $\pi_P\colon \mathrm{Irr}_\sigma(P) \to \mathrm{Irr}(C_P(\sigma))$ such that, for any $\widehat{\varphi} \in \mathrm{Irr}_\sigma(P)$, the image $\varphi = \pi_P(\widehat{\varphi})$ is the unique irreducible constituent of the restriction $\widehat{\varphi}_{C_P(\sigma)}$ which occurs with odd multiplicity (see [7, Theorem 13.1]).

Now, let χ be an arbitrary irreducible character of $C_G(\sigma)$, let $\varphi \in \mathrm{Irr}(C_P(\sigma))$ be an irreducible constituent of $\chi_{C_P(\sigma)}$, and let $\widehat{\varphi} \in \mathrm{Irr}_\sigma(P)$ be such that $\pi_P(\widehat{\varphi}) = \varphi$. We consider the inertia group $I_G(\widehat{\varphi})$ of $\widehat{\varphi}$, and observe that

$$I_{C_G(\sigma)}(\varphi) = I_G(\widehat{\varphi}) \cap C_G(\sigma).$$

In fact, let $g \in C_G(\sigma)$ be arbitrary. Then, it is clear that $\widehat{\varphi}^g \in \mathrm{Irr}_\sigma(P)$; moreover, we have $\pi_P(\widehat{\varphi}^g) = \varphi^g$ (by [7, Theorem 13.1] because $\langle \varphi^g, (\widehat{\varphi}^g)_{C_P(\sigma)} \rangle = \langle \varphi, \widehat{\varphi}_{C_P(\sigma)} \rangle$). Since π_P is bijective, we conclude that $\widehat{\varphi}^g = \widehat{\varphi}$ if and only if $\varphi^g = \varphi$. On the other hand, by Theorem 5, $I_G(\widehat{\varphi})$ is the unit group $H = \mathcal{B}^\times$ of some subalgebra $\mathcal{B} \leq \mathcal{A}$; we note that $\mathrm{Rad}(\mathcal{B}) = \mathrm{Rad}(\mathcal{A})$. By Theorem 2, we conclude that there are nonnegative integers k and r such that

$$|C_G(\sigma) : I_{C_G(\sigma)}(\varphi)| = \begin{cases} 2^{-k}(q-1)^r, & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k(q-1)^r, & \text{if } \sigma \text{ is of the second kind;} \end{cases}$$

in fact, $I_{C_G(\sigma)}(\varphi) = C_G(\sigma) \cap I_G(\widehat{\varphi}) = C_G(\sigma) \cap H = C_H(\sigma)$. Since χ is an irreducible constituent of $\varphi^{C_G(\sigma)}$, Clifford correspondence (see [7, Theorem 6.11]) implies that $\chi = \psi^{C_G(\sigma)}$ for some irreducible character ψ of $I_{C_G(\sigma)}(\chi) = C_H(\sigma)$, and hence

$$\chi(1) = \begin{cases} 2^{-k}(q-1)^r\psi(1), & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k(q-1)^r\psi(1), & \text{if } \sigma \text{ is of the second kind.} \end{cases}$$

Since $p \nmid |C_H(\sigma) : C_P(\sigma)|$, [7, Corollary 6.28] implies that φ is extendible to $C_H(\sigma)$; in other words, there exists $\psi' \in \mathrm{Irr}(C_H(\sigma))$ such that $\psi'_{C_P(\sigma)} = \varphi$. Since $C_H(\sigma)/C_P(\sigma)$ is abelian, we have

$$\varphi^{C_H(\sigma)} = \sum_{\omega \in \mathrm{Irr}(C_H(\sigma)/C_P(\sigma))} \omega\psi'$$

(by Gallagher's Theorem; see [7, Corollary 6.17]), and so $\psi = \omega\psi'$ for some $\omega \in \mathrm{Irr}(C_H(\sigma))$ with $C_P(\sigma) \subseteq \ker(\omega)$. It follows that $\psi_{C_P(\sigma)} = \varphi$, and hence ψ is an also extension of φ. Therefore,

$$\chi(1) = \begin{cases} 2^{-k}(q-1)^r\varphi(1), & \text{if } \sigma \text{ is of the first kind,} \\ (q+1)^k(q-1)^r\varphi(1), & \text{if } \sigma \text{ is of the second kind.} \end{cases}$$

The proof of Theorem 4 is complete because $\varphi(1)$ is a power of q (by [1, Theorem 1.3]; see also [11, Theorem 1]). □

Finally, we prove that $C_G(\sigma)$ is in fact an *M-group*; that is, every irreducible character $\chi \in \mathrm{Irr}(C_G(\sigma))$ is induced by a linear character of some subgroup of $C_G(\sigma)$. More precisely, we shall prove the following result. (For a particular situation, see [11, Theorem 4].)

Theorem 6. *Let $\mathcal{A}$ be a split basic $\Bbbk$-algebra with an involution $\sigma\colon \mathcal{A} \to \mathcal{A}$, let $G = \mathcal{A}^\times$ be the unit group of $\mathcal{A}$, and let χ be an irreducible character of $C_G(\sigma)$. Then, there exist a σ-invariant subgroup $H \leq G$ and a linear character ϑ of $C_H(\sigma)$ such that $\chi = \vartheta^{C_G(\sigma)}$.*

Proof. Let $P = 1 + \mathcal{J}$ where $\mathcal{J} = \mathrm{Rad}(\mathcal{A})$, let $\varphi \in \mathrm{Irr}(C_P(\sigma))$ be an irreducible constituent of the restriction $\chi_{C_P(\sigma)}$, and let $\widehat{\varphi} \in \mathrm{Irr}_\sigma(P)$ be the Glauberman correspondent of φ. By Theorem 5 and by the proof of Theorem 4, we may assume that $\widehat{\varphi}$ is G-invariant; hence, φ is also $C_G(\sigma)$-invariant, and we have $\chi_{C_G(\sigma)} = \varphi$ (see the proof of Theorem 4). As in the proof of Theorem 2, let $\widetilde{G}$ be the semidirect product $\widetilde{G} = G \ltimes \langle\sigma\rangle$ of G by the cyclic group $\langle\sigma\rangle$, and let $\widetilde{S}$ be a Hall p'-subgroup of $\widetilde{G}$ with $\sigma \in \widetilde{S}$. Then, $S = G \cap \widetilde{S}$ is a σ-invariant Hall p'-subgroup of G, and we have a semidirect product $G = PS$; on the other hand, $C_G(\sigma)$ is the semidirect product $C_G(\sigma) = C_P(\sigma)C_S(\sigma)$ (see the proof of Theorem 2).

Now, consider the σ-fixed subgroup $C_{\widetilde{S}}(\sigma)$, and observe that $C_{\widetilde{S}}(\sigma)$ is the direct product $C_{\widetilde{S}}(\sigma) = C_S(\sigma) \times \langle\sigma\rangle$; indeed, σ centralizes $C_S(\sigma)$. Thus, by Theorem 2, $C_{\widetilde{S}}(\sigma)$ is an abelian p'-group with exponent dividing $q-1$ where $q = |\Bbbk^\sigma|$; moreover, it is clear that $C_{\widetilde{S}}(\sigma)$ acts on $\mathcal{J}$ as a group of $\Bbbk^\sigma$-linear ring automorphisms (here, $\mathcal{J}$ is naturally considered as a vector space over $\Bbbk^\sigma$). We note that the character $\widehat{\varphi} \in \mathrm{Irr}(P)$ is $C_{\widetilde{S}}(\sigma)$-invariant, and claim that $\widehat{\varphi} = \widehat{\tau}^P$ for some $C_{\widetilde{S}}(\sigma)$-invariant $\Bbbk^\sigma$-algebra subgroup Q of P and some $C_{\widetilde{S}}(\sigma)$-invariant linear character $\widehat{\tau}$ of Q; as in [6], a subgroup Q of P is said to be a *$\Bbbk^\sigma$-algebra subgroup* if $Q = 1 + \mathcal{U}$ for some $\Bbbk^\sigma$-subalgebra $\mathcal{U}$ of $\mathcal{J}$. To prove this, we proceed by induction on the dimension of $\mathcal{J}$. We consider the ($\Bbbk$-)algebra subgroup $N = 1 + \mathcal{J}^2$ of P; in fact, N is an ideal subgroup (and hence a normal subgroup) of P; an algebra subgroup of P is said to be an *ideal subgroup* if it is of the form $1 + \mathcal{I}$ for some (two-sided) ideal $\mathcal{I}$ of $\mathcal{J}$. Since $C_{\widetilde{S}}(\sigma)$ and P have coprime orders, [7, Theorem 13.27] asserts that there exists $\widehat{\eta} \in \mathrm{Irr}_{C_{\widetilde{S}}(\sigma)}(N)$ such that $\langle \widehat{\varphi}_N, \widehat{\eta}\rangle \neq 0$.

Firstly, assume that $\widehat{\eta}$ is not P-invariant. In this case, $I_P(\widehat{\eta})$ is a proper algebra subgroup of P (see [5, Lemma 3.3]); moreover, since $\widehat{\eta}$ is $C_{\widetilde{S}}(\sigma)$-invariant, $I_P(\widehat{\eta})$ is also $C_{\widetilde{S}}(\sigma)$-invariant. By [5, Lemma 3.2], there exists $\widehat{\varrho} \in \mathrm{Irr}_{C_{\widetilde{S}}(\sigma)}(I_P(\widehat{\eta}))$ such that $\langle \widehat{\varrho}, \widehat{\varphi}_N\rangle \neq 0$ and $\langle \widehat{\varrho}_N, \widehat{\eta}\rangle \neq 0$. By Clifford's correspondence (see [7, Theorem 6.11]), we must have $\widehat{\varphi} = \widehat{\varrho}^P$, and the claim follows by induction.

On the other hand, suppose that $\widehat{\eta}$ is P-invariant. In this case, we have $\widehat{\varphi}_N = e\widehat{\eta}$ for some positive integer e; moreover, [4, Theorem 1.3] asserts that $\widehat{\eta}$ is a linear character (and hence $e = \widehat{\varphi}(1)$). Let L be a $C_{\widetilde{S}}(\sigma)$-invariant $\Bbbk^\sigma$-algebra subgroup of P which is maximal with respect to the condition that $\widehat{\eta}$ is extendible to L. By [5, Lemma 3.2], there exists $\widehat{\tau} \in \mathrm{Irr}_{C_{\widetilde{S}}(\sigma)}(L)$ with $\langle \widehat{\tau}, \widehat{\varphi}_L\rangle \neq 0$ and $\langle \widehat{\tau}_N, \widehat{\eta}\rangle \neq 0$; since L/N is abelian, Gallager's theorem (see [7, Corollary 6.17] implies that $\widehat{\tau}_N = \widehat{\eta}$. We shall now prove that $\widehat{\varphi} = \widehat{\tau}^P$. To see this, we consider the inertia group $I_P(\widehat{\tau})$ and assume that $I_P(\widehat{\tau}) \neq L$. Let $\mathcal{I}$ and $\mathcal{I}'$ be the $\Bbbk^\sigma$-subalgebras of $\mathcal{J}$ such that $L = 1 + \mathcal{I}$ and $I_P(\widehat{\tau}) = 1 + \mathcal{I}'$; notice that $I_P(\widehat{\tau})$ is a $\Bbbk^\sigma$-algebra subgroup of P by [5, Lemma 3.3] (moreover, since $\mathcal{J}^2 \subseteq \mathcal{I}, \mathcal{I}'$, both $\mathcal{I}$ and $\mathcal{I}'$ are necessarily $\Bbbk^\sigma$-ideals of $\mathcal{J}$). Let $\Bbbk^\sigma[C_{\widetilde{S}}(\sigma)]$ denote the group algebra of $C_{\widetilde{S}}(\sigma)$ over the σ-fixed field $\Bbbk^\sigma$, and consider the left $\Bbbk^\sigma[C_{\widetilde{S}}(\sigma)]$-module $\mathcal{I}'/\mathcal{I}$. Let $\mathcal{V}$ be an irreducible $\Bbbk^\sigma[C_{\widetilde{S}}(\sigma)]$-submodule of $\mathcal{I}'/\mathcal{I}$; notice that we are assuming that $\mathcal{I}'/\mathcal{I}$ is non-zero. Since the exponent of $C_{\widetilde{S}}(\sigma)$ divides $q-1$ where $q = |\Bbbk^\sigma|$, $\Bbbk^\sigma$ is a splitting field for $C_{\widetilde{S}}(\sigma)$ (see [7, Corollary 9.25]), and thus $\mathcal{V}$ is one-dimensional (because $C_{\widetilde{S}}(\sigma)$ is abelian).

It follows that there exists $a \in \mathcal{I}' \setminus \mathcal{I}$ such that $\mathcal{I} + \Bbbk^\sigma a$ is an $C_{\widetilde{S}}(\sigma)$-invariant $\Bbbk^\sigma$-ideal of $\mathcal{J}$, and hence $L_a = 1 + \mathcal{I} + \Bbbk^\sigma a$ is an $C_{\widetilde{S}}(\sigma)$-invariant $\Bbbk^\sigma$-algebra subgroup of $1 + \mathcal{I}' = I_P(\widehat{\tau})$ such that $L \subseteq L_a$ and $|L_a : L| = q$. By [7, Theorem 13.28], there exists $\widehat{\tau}' \in \mathrm{Irr}_{C_{\widetilde{S}}(\sigma)}(L_a)$ such that $\langle \widehat{\tau}', \widehat{\tau}^{L_a} \rangle \neq 0$; hence, $\langle \widehat{\tau}'_L, \widehat{\tau} \rangle \neq 0$. By [6, Theorem A], both $\widehat{\tau}$ and $\widehat{\tau}'$ have q-power degree, and thus either $\widehat{\tau}'_L = \widehat{\tau}$ or $\widehat{\tau}' = \widehat{\tau}^{L_a}$. The first case cannot occur by the maximal choice of L. Therefore, $\widehat{\tau}' = \widehat{\tau}^{L_a}$, and thus $I_{L_a}(\widehat{\tau}) = L$ (by [7, Problem 6.1]). Since $L_a \subseteq I_P(\widehat{\tau})$, we conclude that $L_a \subseteq L$, a contradiction. It follows that $I_P(\widehat{\tau}) = L$, and this implies that $\widehat{\tau}^P \in \mathrm{Irr}(P)$ (by [7, Problem 6.1]). Since $\langle \widehat{\varphi}, \widehat{\tau}^P \rangle = \langle \widehat{\varphi}_L, \widehat{\tau} \rangle \neq 0$, we conclude that $\widehat{\varphi} = \widehat{\tau}^P$, as required.

Our claim is now proved; that is, there exist a $C_{\widetilde{S}}(\sigma)$-invariant $\Bbbk^\sigma$-algebra subgroup Q of P and a $C_{\widetilde{S}}(\sigma)$-invariant linear character $\widehat{\tau}$ of Q such that $\widehat{\varphi} = \widehat{\tau}^P$. In particular, Q is σ-invariant, and $\widehat{\tau} \in \mathrm{Irr}_\sigma(Q)$. Let $\tau = \pi_Q(\widehat{\tau}) \in \mathrm{Irr}(C_Q(\sigma))$; since $\widehat{\tau}$ is linear, it is clear that $\tau = \widehat{\tau}_{C_Q(\sigma)}$, and hence τ is linear and $C_{\widetilde{S}}(\sigma)$-invariant. By [1, Proposition 2.8], we conclude that $\varphi = \tau^{C_P(\sigma)}$; we recall that σ defines an $\Bbbk^\sigma$-linear automorphism of $\mathcal{J}$.

Finally, let $H = C_S(\sigma)Q$; we note that, since Q is $C_{\widetilde{S}}(\sigma)$-invariant (and $C_S(\sigma) \leq C_{\widetilde{S}}(\sigma)$), H is a subgroup of G satisfying $C_H(\sigma) = C_S(\sigma)C_Q(\sigma)$. Since τ is $C_{\widetilde{S}}(\sigma)$-invariant and $p \nmid |C_H(\sigma) : C_Q(\sigma)|$, [7, Corollary 6.28] implies that τ is extendible to $C_H(\sigma)$; in other words, there exists $\tau' \in \mathrm{Irr}(C_H(\sigma))$ such that $\tau'_{C_Q(\sigma)} = \tau$. Since $C_H(\sigma)/C_Q(\sigma)$ is abelian, we have

$$\tau^{C_H(\sigma)} = \sum_{\omega \in \mathrm{Irr}(C_H(\sigma)/C_Q(\sigma))} \omega\tau'$$

(by Gallagher's Theorem; see [7, Corollary 6.17]), and so

$$\varphi^{C_G(\sigma)} = (\tau^{C_P(\sigma)})^{C_G(\sigma)} = \tau^{C_G(\sigma)} = \sum_{\omega \in \mathrm{Irr}(C_H(\sigma)/C_Q(\sigma))} (\omega\tau')^{C_G(\sigma)}.$$

On the other hand, since $C_G(\sigma) = C_H(\sigma)C_P(\sigma)$ and $C_H(\sigma) \cap C_P(\sigma) = C_Q(\sigma)$, we deduce that

$$((\omega\tau')^{C_G(\sigma)})_{C_P(\sigma)} = ((\omega\tau')_{C_Q(\sigma)})^{C_P(\sigma)} = \tau^{C_P(\sigma)} = \varphi,$$

and thus $(\omega\tau')^{C_G(\sigma)}$ is irreducible for all $\omega \in \mathrm{Irr}(C_H(\sigma)/C_Q(\sigma))$. Since χ is an irreducible constituent of $\varphi^{C_G(\sigma)}$, we conclude that $\chi = (\omega\tau')^{C_G(\sigma)}$ for some $\omega \in \mathrm{Irr}(C_H(\sigma)/C_Q(\sigma))$, and this completes the proof of the theorem. □

REFERENCES

[1] C. André, *Irreducible characters of groups associated with finite nilpotent algebras with involution*, J. Algebra **324** (2010), no. 9, 2405–2417. MR2684146

[2] R.W. Carter, *Simple groups of Lie type*, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1989. Reprint of the 1972 original, A Wiley-Interscience Publication. MR1013112

[3] D. Gorenstein, *Finite groups*, Second, Chelsea Publishing Co., New York, 1980. MR569209

[4] Z. Halasi, *On the characters and commutators of finite algebra groups*, J. Algebra **275** (2004), no. 2, 481–487. MR2052621

[5] ———, *On the characters of the unit group of DN-algebras*, J. Algebra **302** (2006), no. 2, 678–685. MR2293776

[6] I.M. Isaacs, *Characters of groups associated with finite algebras*, J. Algebra **177** (1995), no. 3, 708–730. MR1358482

[7] ———, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. MR2270898

[8] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits. MR1632779

[9] B.R. McDonald, *Finite rings with identity*, Marcel Dekker, Inc., New York, 1974. Pure and Applied Mathematics, Vol. 28. MR0354768

[10] B. Szegedy, *On the characters of the group of upper-triangular matrices*, J. Algebra **186** (1996), no. 1, 113–119. MR1418042

[11] ———, *Characters of the Borel and Sylow subgroups of classical groups*, J. Algebra **267** (2003), no. 1, 130–136. MR1993470

CENTRO DE ANÁLISE FUNCIONAL, ESTRUTURAS LINEARES E APLICAÇÕES (CEAFEL) & DEPARTAMENTO DE MATEMÁTICA, FACULDADE DE CIÊNCIAS DA UNIVERSIDADE DE LISBOA, CAMPO GRANDE, EDIFÍCIO C6, PISO 2, 1749-016 LISBOA, PORTUGAL

E-mail address: caandre@ciencias.ulisboa.pt

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 89–129
ISSN: 1930-1235; (**2018**)

USING STRONG BRANCHING TO FIND AUTOMORPHISM GROUPS OF n-GONAL SURFACES

S. ALLEN BROUGHTON, CHARLES CAMACHO, JENNIFER PAULHUS,
REBECCA R. WINARSKI, AND AARON WOOTTON

Dedicated to the memory of Kay Magaard

Abstract. The problem of finding full automorphism groups of compact Riemann surfaces is classical, though complete results are only known for a few families. One tool used in some classification schemes is strong branching; a condition derived by Accola in [1]. In the following, we survey the main ideas behind strong branching including a general survey of current results. We also provide new results for families for which we can find the full automorphism group using strong branching and an inductive version of strong branching.

MSC 2010: Primary: 14J10, 14J50; Secondary: 30F10, 30F20
Keywords: automorphism groups of surfaces, hyperelliptic surfaces, superelliptic surfaces, strong branching

1. Introduction

Ideally, we would like to be able to determine the full automorphism group of a Riemann surface given some partial information about the surface such as defining equations, uniformization by a Fuchsian group, a branched covering map to a known surface, or a "sufficiently large"group of automorphisms. In this paper we are particularly interested in the interplay of the last two items. For our purposes, a subgroup G of the automorphism group of a Riemann surface S is called "sufficiently large" if S/G has genus zero. Alternatively, S is called a *regular n-gonal surface*. A regular n-gonal surface is one for which the quotient map $\pi_G : S \to S/G \backsimeq \mathbb{P}^1(\mathbb{C})$ is a regular branched covering of the sphere $\mathbb{P}^1(\mathbb{C})$ of degree $n = |G|$, branched over a finite set of points $B_G = \{Q_1, \ldots, Q_t\}$. This class of surfaces includes these important cases: hyperelliptic surfaces, superelliptic surfaces, cyclic n-gonal surfaces, quasi-platonic surfaces, as well as many others. In the moduli space of surfaces of fixed genus $\sigma \geq 2$ the "most common" surfaces with automorphisms are regular n-gonal surfaces. We use this fact and the important cases described above as justification for focusing on the study on regular n-gonal surfaces. The notion of "most common" can be made precise using Breuer's data on low genus actions [5], see the end of Section 4.2.

Finding automorphism groups of n-gonal surfaces.

Let us describe an approach to finding the full automorphism group of an n-gonal surface. We assume we are given a group, G, of automorphisms with genus zero quotient S/G. We will also assume that we have very precise information about how G acts on S and the map $\pi_G : S \to \mathbb{P}^1(\mathbb{C})$. Throughout the paper let $A = \mathrm{Aut}(S)$, $N = \mathrm{Nor}_A(G)$, and $K = N/G$. Since N normalizes G, then K acts as a group of automorphisms of $S/G \backsimeq \mathbb{P}^1(\mathbb{C})$. The candidate groups K are precisely known and given the structure of the map $\pi_G : S \to \mathbb{P}^1(\mathbb{C})$, the structure of the group N may be determined, as well as the map $\pi_N : S \to S/N \backsimeq \mathbb{P}^1(\mathbb{C})$. See Section 3.1 for details.

If $N = A$ then we are done. Otherwise we have *exceptional automorphisms* in $A - N$. The branched covering $\pi_{A/N} : S/N \to S/A$ is a rational map of the sphere, and its monodromy can be determined. The monodromy may then be used to construct the extension $N < A$. The latter situation is unusual and takes considerable work using MAGMA [4] or GAP [11] to solve. See Section 3.2 for details.

A tricky step in the aforementioned process is deciding whether or not G is normal in A without any prior knowledge of A. In general, an answer to this question is likely very difficult. However, if the map π_G is *strongly branched* – a concept introduced by Accola [1] – G is guaranteed to have a subgroup M that is normal in A. Strong branching is checked by an easily verifiable inequality. Using strong branching, the classification process splits up into two cases:

(1) The genus of S is larger than a lower bound determined by strong branching, and there is a normal subgroup $M \trianglelefteq A$ contained in G. If $G = M$, then $A = N$, and we can compute A as described above. If M is a proper subgroup of G then $\overline{S} = S/M$ is a surface upon which both $\overline{A} = A/M$ and $\overline{G} = G/M$ act, and $\overline{A} \leq \mathrm{Aut}(\overline{S})$. Presumably we can compute $\overline{A} \leq \mathrm{Aut}(\overline{S})$, since it is a smaller genus problem, and then construct A from $M \hookrightarrow A \twoheadrightarrow \overline{A}$. See Proposition 4.4.

(2) The genus of S is less than or equal to the critical genus. Then, we have to look for exceptional automorphisms (after finding the normalizer) in a finite number of cases, working as noted above.

Since strong branching simplifies the process of finding A, there is much potential for its use in determining full automorphism groups, possibly inductively as suggested by case 1. To date, strong branching has been used for a number of different families, with perhaps the most comprehensive use in determining full automorphism groups of cyclic p-gonal surfaces, see [22] and Subsection 5.1.1 (a surface is cyclic p-gonal when G has prime order).

Our main motivational goal in the following is to provide tools and techniques derived from the concept of strong branching to help classify full automorphism groups, and to provide explicit examples of how these techniques are used. We shall do this through first describing the general idea behind strong branching and surveying the current results in classification of automorphism groups that can be attributed to strong branching. Following this, we shall provide new classification results using strong branching, both single stage and inductively.

Outline of paper

The outline of our work is as follows. In Section 2 we covering preliminaries on branched coverings and ramification, the Riemann-Hurwitz theorem, group actions, and families of surfaces with a simultaneous group action. In Section 3 we provide details on how to determine whether or not an n-gonal group G extends to some larger automorphism group, providing very explicit results in certain special cases. In Section 4 we introduce strong branching, weakly normal actions and trivial core actions. In Section 5 we apply the concepts and methods of Sections 2 and 4, particularly strong branching, to finding full automorphism groups of families of n-gonal surfaces, surveying the known results and presenting new ones.

Acknowledgement

This work was initiated with Kay Magaard at the BIRS workshop "Symmetries of Surfaces, Maps and Dessins" in September 2017. The authors are grateful to Kay for sharing his deep insight into the problem, especially introducing us to works [2], [13] and [16] (of which he is a coauthor), and we dedicate this work to his memory. We would also like to thank BIRS, and the organizers of the workshop for providing us a beautiful venue to work on this project together.

2. PRELIMINARIES

There are several tools for working with group actions on Riemann surfaces: Fuchsian groups, function fields, and branched covering theory. In this paper we use branched covering theory since strong branching and group actions are conveniently formulated in these terms. Moreover, these methods work in positive characteristic.

2.1. **Branched coverings and differentials.** Let S_1, S_2 be two Riemann surfaces of genus σ_1 and σ_2, respectively, and $\pi : S_1 \to S_2$ a branched covering (holomorphic map) of degree n. Some items related to the map π, useful in understanding the Riemann Hurwitz formula are:

(1) The differential map on tangent bundles

$$d\pi : T_P(S_1) \to T_{\pi(P)}(S_2)$$

and its dual pullback map of meromorphic differential 1-forms

$$d\pi^* : \Omega^1(S_2) \to \Omega^1(S_1).$$

(2) A divisor $(d\pi)$ defined on S_1 by

$$(d\pi) = \sum_{P \in S_1} ord_P(d\pi)P.$$

The value $ord_P(d\pi)$ is computed by first writing, in local coordinates centered at 0 in the domain and target,

$$\pi(z) = z^{e(P)} f(z), \ f(z) \neq 0.$$

Then

$$d\pi = z^{e(P)-1}(e(P)f(z)dz + zdf(z)).$$

Since

$$e(P)f(z)dz + zdf(z) = e(P)f(0)dz$$

at $z = 0$ then $ord_P(d\pi) = e(P)-1$. Now $e(P) \geq 1$ for all P, it is independent of the coordinatization, and $e(P) > 1$ for at most finitely many points. Thus the divisor $(d\pi)$ of the differential $d\pi$ is given by

$$(d\pi) = \sum_{P \in S_1} (e(P) - 1)\, P. \tag{1}$$

2.2. **Ramification and the Riemann-Hurwitz equation.**

Definition 2.1. The *total ramification* of a branched covering π is the degree of the divisor in equation (1):

$$R_\pi = \sum_{P \in S_1} (e(P) - 1)\,. \tag{2}$$

If ω is a differential form on S_2 then the degree of the divisor $(d\pi^*(\omega))$ may be computed in two ways: first as a differential form on S_1 with degree $2(\sigma_1 - 1)$ and, secondly, as the degree of the pullback $d\pi^*(\omega)$ to get $2n(\sigma_2-1)+\sum_{P\in S_1}(e(P)-1)$. The first term comes from pulling back the zeros and poles of ω and the second term comes from the ramification of the branched covering. The Riemann-Hurwitz equation may then be written:

$$2(\sigma_1 - 1) = 2n(\sigma_2 - 1) + \sum_{P \in S_1} (e(P) - 1) \tag{3}$$

or

$$2(\sigma_1 - 1) - 2n(\sigma_2 - 1) = R_\pi. \tag{4}$$

Note that we may use equation (4) to compute either σ_1, σ_2 or n. Specifically, for the index we must have:

$$n = \frac{2(\sigma_1 - 1) - R_\pi}{2(\sigma_2 - 1)}. \tag{5}$$

If $Q_1, \ldots, Q_t$ are the points on S_2 over which π is ramified, then another version of the Riemann-Hurwitz equation which emphasizes this branching is:

$$R_\pi = \sum_{P \in S_1} (e(P) - 1) = \sum_{j=1}^{t} \sum_{\pi(P)=Q_j} (e(P) - 1)\,.$$

Now $\sum_{\pi(P)=Q_j} (e(P) - 1) = n - \left|\pi^{-1}(Q_j)\right|$, so that we also have:

$$R_\pi = n \sum_{j=1}^{t} \left(1 - \frac{\left|\pi^{-1}(Q_j)\right|}{n}\right). \tag{6}$$

It follows that if we can count singular preimages, the total ramification is easily calculated.

2.3. **Group actions, generating vectors, and signatures.** We now survey the main tools we need to describe group actions on surfaces.

Actions and surface kernel epimorphisms

The finite group G *acts conformally* on the Riemann surface S if there is a monomorphism:

$$\epsilon : G \hookrightarrow \mathrm{Aut}(S).$$

When there is no confusion we will identify G with it image $\epsilon(G)$. Such actions of G allow us to construct surfaces and analyze their automorphism groups with the group G as the starting point. Our primary tool for working with actions are surface kernel epimorphisms and the corresponding generating vectors, which we proceed to define.

The quotient surface $S/G = T$ is a closed Riemann surface of genus τ with a unique conformal structure such that

$$\pi_G : S \to S/G = T \tag{7}$$

is holomorphic. The quotient map $\pi_G : S \to T$ is ramified uniformly (all branching orders are the same on a given fiber) over a finite set $B_G = \{Q_1, \ldots, Q_t\}$ such that π_G is an unramified covering exactly over $T^\circ = T - B_G$. Let $S^\circ = \pi_G^{-1}(T^\circ)$ so that $\pi_G : S^\circ \to T^\circ$ is an unramified covering space whose group of deck transformation equals $\epsilon(G)$, restricted to S°. This covering determines a normal subgroup $\Pi_G = \pi_1(S^\circ) \lhd \pi_1(T^\circ)$ and an exact sequence $\Pi_G \hookrightarrow \pi_1(T^\circ) \twoheadrightarrow \epsilon(G)$ by mapping loops to deck transformations, via path lifting. Combine the last map with $\epsilon(G) \overset{\epsilon^{-1}}{\to} G$ to get an exact sequence

$$\Pi_G \hookrightarrow \pi_1(T^\circ) \overset{\xi}{\twoheadrightarrow} G. \tag{8}$$

The map ξ, which we call a *surface kernel epimorphism,* is an analogue to surface kernel epimorphisms for Fuchsian groups. The map ξ is well-defined only up to automorphisms of G. We detail this dependence and some questions related to computations with ξ at the end of this subsection.

Generating systems and generating vectors

The fundamental group $\pi_1(T^\circ)$ has presentation:

$$\left\{ \alpha_i, \beta_i, \gamma_j, 1 \le i \le \tau, 1 \le j \le t \middle| \prod_{i=1}^{\tau} [\alpha_i, \beta_i] \prod_{j=1}^{t} \gamma_j = 1 \right\}. \tag{9}$$

We denote the ordered generating set $(\alpha_1, \ldots, \alpha_\tau, \beta_1, \ldots, \beta_\tau, \gamma_1, \ldots, \gamma_t)$ by $\mathcal{G}$, noting that it is not unique.

Define

$$a_i = \xi(\alpha_i), b_i = \xi(\beta_i), c_j = \xi(\gamma_j).$$

The $2\tau + t$ tuple

$$\mathcal{V} = (a_1, \ldots, a_\tau, b_1, \ldots, b_\tau, c_1, \ldots, c_t) \tag{10}$$

is called a *generating vector* for the action. We observe that

$$G = \langle a_1, \ldots, a_\tau, b_1, \ldots, b_\tau, c_1, \ldots, c_t \rangle, \tag{11}$$

as ξ is surjective. Since the element c_j generates the stabilizer of some point P_j lying over Q_j, we have:

$$o(c_j) = n_j, \tag{12}$$

the ramification degree at P_j. Finally, the relation in (9), combined with equation (12), shows that a generating vector satisfies the following relations:

$$\prod_{i=1}^{\tau} [a_i, b_i] \prod_{j=1}^{t} c_j = c_1^{n_1} = \cdots = c_t^{n_t} = 1. \tag{13}$$

The *signature* of the action – actually of the generating vector – is $(\tau; n_1, \ldots, n_t)$. For conciseness, we call the "vector" $\mathcal{V}$ given in equation (10) a $(\tau; n_1, \ldots, n_t)$-generating vector of G. We call the number τ (the genus of S/G) the *orbit genus* and the numbers $n_1, \ldots, n_t$ the *periods* of the signature. In the n-gonal case with $\tau = 0$ we write $(n_1, \ldots, n_t)$. By the orbit-stabilizer theorem, $|G| = n_j \left|\pi_G^{-1}(Q_j)\right|$. Therefore, when the action of a group G on a compact Riemann surface S of genus σ is described using the signature $(\tau; n_1, \ldots, n_t)$ the Riemann-Hurwitz formula can be rewritten as a genus formula:

$$\sigma = 1 + n(\tau - 1) + \frac{n}{2} \sum_{j=1}^{t} \left(1 - \frac{1}{n_j}\right), \tag{14}$$

or the area of a fundamental domain

$$\frac{\text{Area}(S/G)}{2\pi} = \frac{2\sigma - 2}{|G|} = (2\tau - 2) + \sum_{j=1}^{t} \left(1 - \frac{1}{n_j}\right). \tag{15}$$

Any $2\tau + t$ tuple of elements of G satisfying conditions (11)-(13) is called a $(\tau; n_1, \ldots, n_t)$-generating vector, even though it may not have arisen from a G action. However, all such arbitrary generating vectors do arise from surfaces with a G action. We state this as a proposition and show the construction in the proof sketch.

Proposition 2.1. *Suppose we are given a surface T of genus τ, a branch set $B_G = \{Q_1, \ldots, Q_t\} \subset T$, $Q_0 \in T^\circ = T - B_G$ and generating set $\mathcal{G}$ of $\pi_1(T^\circ, Q_0)$ as given in (9). Then, given an arbitrary generating vector $\mathcal{V}$, as in equation (10), with signature $(\tau; n_1, \ldots, n_t)$ we may construct a surface S with G action such that $S/G = T$, π_G is branched over B_G, and such that $\mathcal{V}$ is the generating vector of the action.*

Proof. Using the generating vector $\mathcal{V}$ we can construct a surface kernel epimorphism $\Pi_G \hookrightarrow \pi_1(T^\circ, Q_0) \overset{\xi}{\twoheadrightarrow} G$. The subgroup Π_G defines a holomorphic unbranched covering of $S^\circ \to T^\circ$ with deck group G. Using the Riemann removable singularity theorem we can close up S° and T° to a branched covering $S \to T$ with G action. □

Example 2.1. If G is cyclic of order 7 with generator x, then (x, x, x^5) is a $(7, 7, 7)$-generating vector for G. Using the Riemann-Hurwitz formula, we see that we get a G action with signature $(7, 7, 7)$ on a surface of genus 3.

In the case of n-gonal actions, the primary focus of this paper, we only have the generators $\gamma_1, \ldots, \gamma_t$. We need to describe $\gamma_1, \ldots, \gamma_t$ so that we may compute the action of conformal maps upon them.

Construction 2.2. *Such a system may be constructed as follows.*

1. *Select a system of arcs from the base point Q_0 to the Q_j so that the arcs only intersect at Q_0.*
2. *Moreover, in a small neighborhood of Q_0 the counterclockwise order of the arcs is determined by the given order $Q_1, \ldots, Q_t$ of the end points.*
3. *To construct γ_j we start out from Q_0 along the arc to Q_j, stopping just short of Q_j, encircling Q_j counterclockwise once in a small circle centered at Q_j, and then return to Q_0 along the initial path.*

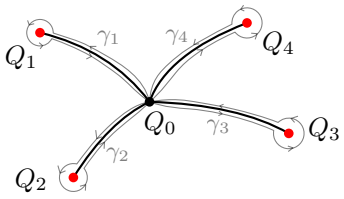

FIGURE 1. Construction 2.2.

It follows from the construction that the γ_j generate the group and that $\gamma_1 \cdots \gamma_t = 1$. See Figure 1.

Dependence on base points

We have left out base points to simplify the exposition, and so ξ is ambiguous up to inner automorphisms. First suppose that $Q_0 \in T^\circ$, and that path lifting $\pi_1(T^\circ) \twoheadrightarrow \epsilon(G)$ is defined with respect to the point P_0 lying over Q_0. If another point gP_0 is selected and ξ' is the new surface kernel epimorphism then

$$\xi' = Ad_g \circ \xi, \tag{16}$$

where $Ad_g(x) = gxg^{-1}$. Next, given two base points $Q_0, Q_0' \in T^\circ$ and a path δ from Q_0 to Q_0', the loop concatenation map $\varphi_\delta : \pi_1(T^\circ, Q_0) \to \pi_1(T^\circ, Q_0')$, $\varphi_\delta : \alpha \to \delta^{-1} * \alpha * \delta$ is an isomorphism unique up to an inner automorphisms of $\pi_1(T^\circ, Q_0)$ and $\pi_1(T^\circ, Q_0')$. For, if δ_1, δ_2 are two different paths Q_0 to Q_0' then

$$\varphi_{\delta_2} = \varphi_{\delta_1} \circ Ad_{\delta_2 * \delta_1^{-1}}$$

and

$$\varphi_{\delta_2} = Ad_{\delta_1^{-1} * \delta_2} \circ \varphi_{\delta_1}.$$

Now suppose that ξ and ξ' are defined with respect to $P_0 \in \pi_G^{-1}(Q_0)$ and $P_0' \in \pi_G^{-1}(Q_0')$, $\widetilde{\delta}$ is a path from P_0 to P_0' in S°, and $\delta = \pi_G(\widetilde{\delta}\,)$. Then

$$\xi = \xi' \circ \varphi_\delta. \tag{17}$$

If δ' is any other path from Q_0 to Q_0' then

$$\begin{aligned} \xi' \circ \varphi_{\delta'} &= \xi' \circ Ad_{\delta^{-1} * \delta'} \circ \varphi_\delta \\ &= Ad_{\xi'(\delta^{-1} * \delta')} \circ \xi' \circ \varphi_\delta \\ &= Ad_{\xi'(\delta^{-1} * \delta')} \circ \xi. \end{aligned} \tag{18}$$

Action on generating vectors

Generating vectors for actions are not unique. We may first apply any automorphism ω of G to the G action ϵ to obtain $\omega \circ \epsilon$. The result $\mathcal{V} \to \omega\mathcal{V}$ on the generating vector is

$$(a_1, \ldots, a_\tau, b_1, \ldots, b_\tau, c_1, \ldots, c_t) \to (\omega a_1, \ldots, \omega a_\tau, \omega b_1, \ldots, \omega b_\tau, \omega c_1, \ldots, \omega c_t)\,.$$

The action of an automorphism does not affect the surface constructed from the generating vector since the subgroup Π_G is not affected by ω. This is consistent with our observations on the dependence on base points in equations (16),(17), and (18).

Secondly, we may use a different generating set $\mathcal{G}'$, and in turn this change of generating set has an effect on generating vectors. In the n-gonal case it can be

shown that any such transformation $\mathcal{G} \to \mathcal{G}'$ has the form

$$\gamma_j \to \psi_j \gamma_{\theta(j)} \psi_j^{-1} \tag{19}$$

where ψ_j is a word in $\gamma_1, \ldots, \gamma_t$, and θ is a permutation of $1, \ldots, t$. The action on the generating vectors is

$$c_j \to w_j c_{\theta(j)} w_j^{-1}, \tag{20}$$

where w_j is obtained by replacing γ_i by c_i, for all i, in ψ_j. In the Abelian case the transformation is given by

$$c_j \to c_{\theta(j)}. \tag{21}$$

We call the actions given by equations (19) and (20) *braid actions*. Any two generating vectors $(c_1, \ldots, c_t)$ and $(c'_1, \ldots, c'_t)$ are called *braid equivalent* if $c'_j = w_j c_{\theta(j)} w_j^{-1}$ under the braid action. If θ is trivial we say that the vectors are *pure braid equivalent*. The origin of the term braid action is given in Remark 2.1. The braid action on the surfaces lying over (T, B_G) is discussed at the end of Section 2.5.

Also see [16] for more on the braid action.

Remark 2.1. Here is the connection to braid groups and the justification for calling the action in (19) and (20) the braid action. We may continuously move one branch set $\{Q_1, \ldots, Q_t\}$ to another via a path $(Q_1(s), \ldots, Q_t(s)), 0 \leq s \leq 1$, with $(Q_1(0), \ldots, Q_t(0)) = (Q_1, \ldots, Q_t)$ By standard theory, there is a family of homeomorphisms

$$h_s : T - \{Q_1, \ldots, Q_t\} \to T - \{Q_1(s), \ldots, Q_t(s)\}.$$

If $\{Q_1(1), \ldots, Q_t(1)\} = \{Q_1, \ldots, Q_t\}$ as sets then the homeomorphism h_1 is a homeomorphism of T° inducing the transformations in equations (19) and (20). The path

$$(Q_1(s), \ldots, Q_t(s)), 0 \leq s \leq 1$$

with $\{Q_1(1), \ldots, Q_t(1)\} = \{Q_1, \ldots, Q_t\}$ is a braid and hence we use the term braid action.

2.4. **Generating vectors and signatures of subgroups.** Our main approach to determining the full automorphism group of a surface will be to start with a group which we know acts on a surface, and then see if it extends to a larger group. Accordingly, we need to know how signatures of groups are related to their subgroups. Fortunately, once a G action has been specified via a $(\tau; n_1, \ldots, n_t)$-generating vector, we can recover the signature of a subgroup $G \leq A$ using the following theorem of Singerman [20].

Theorem 2.3. *For a group A, given a $(\tau_A; n_1, \ldots, n_t)$-generating vector*

$$(a_1, \ldots, a_{\tau_A}, b_1, \ldots, b_{\tau_A}, c_1, \ldots, c_t)$$

for A, the signature of the subgroup G with index d is

$$(\tau_G; m_{1,1}, m_{1,2}, \ldots, m_{1,\theta_1}, \ldots m_{t,\theta_t})$$

where

(1) *If $\Phi \colon A \to S_d$ is the permutation representation of A on the cosets of G, then the permutation $\Phi(c_j)$ has precisely θ_j cycles of length less than n_j, the lengths of these cycles being*

$$n_j/m_{j,1}, \ldots n_j/m_{j,\theta_j}.$$

(2) *The index d satisfies*

$$d = \frac{2\tau_G - 2 + \sum_{j=1}^{t} \sum_{i=1}^{\theta_j} \left(1 - \frac{1}{m_{j,i}}\right)}{2\tau_A - 2 + \sum_{j=1}^{t} \left(1 - \frac{1}{n_j}\right)}. \tag{22}$$

When G is normal in A, so that $A = N$, the cycles of $\Phi(c_j)$ all have the same length. Thus by considering the action of N/G on S/G, Theorem 2.3 can be simplified to:

Proposition 2.4. *For a group N, given a $(\tau_N; n_1, \ldots, n_t)$-generating vector*

$$(a_1, \ldots, a_{\tau_N}, b_1, \ldots, b_{\tau_N}, c_1, \ldots, c_t)$$

for N, the signature of the normal subgroup G of index d is

$$(\tau_G; m_{1,1}, m_{1,2}, \ldots, m_{1,\theta_1}, \ldots m_{t,\theta_t})$$

where:

(1) *$m_{j,i} = n_j/l_j$ and $\theta_j = d/l_j$ where l_j is the order of $c_j G$ in N/G, and*
(2) *the index d satisfies*

$$d = \frac{2\tau_G - 2}{2\tau_N - 2 + \sum_{j=1}^{t} \left(1 - \frac{1}{l_j}\right)}. \tag{23}$$

Remark 2.2. Let A be a group acting on the surface S with signature $(\tau_A; n_1, \ldots, n_t)$. Let $G < A$ act on S with signature $(\tau_G; m_1, \ldots, m_s)$. We can compute the index $d = |A| / |G|$ without knowing the structure of $S/G \to S/A$. Specifically, as in Theorem 2.3, or using equation (15),we have

$$d = |A| / |G| = \frac{(2\sigma - 2)/|G|}{(2\sigma - 2)/|A|} = \frac{2\tau_G - 2 + \sum_{j=1}^{s} \left(1 - \frac{1}{m_j}\right)}{2\tau_A - 2 + \sum_{j=1}^{t} \left(1 - \frac{1}{n_j}\right)}. \tag{24}$$

Remark 2.3. Using Theorem 2.3, a MAGMA script can be written that takes a finite group A and a generating vector $\mathcal{V} = (c_1, \ldots, c_t)$ and computes the genus σ of the surface S, defined by A and $\mathcal{V}$ and the signature of the action for every subgroup $G \leq A$. We use this script to look for interesting n-gonal subgroup actions given a proposed full automorphism group.

2.5. **Equivalence, families, and equisymmetry of actions.** When trying to extend the known action of a n-gonal group G to a larger, normalizing group, the notion of conformal equivalence of actions naturally arises, specifically the diagram (26). In turn, this leads to looking for relations among the branch points on the quotient surface. The notion of strong branching, to be discussed in the next section, automatically forces an action to have numerous branch points. By varying the branch points we get families of surface with the "same" action. Thus, in our quest to classify surface automorphism groups, it is useful to introduce the interrelated, clarifying concepts of conformal equivalence of actions, families of actions, and equisymmetry of actions.

Equivalence of actions

Two actions ϵ_1, ϵ_2 of G on possibly different surfaces S_1, S_2 are conformally equivalent if there is an equivariant, conformal homeomorphism $h : S_1 \to S_2$ and an automorphism $\omega \in \mathrm{Aut}(G)$ such that $h\epsilon_1(\omega(g)) = \epsilon_2(g)h$, or more conveniently:

$$\epsilon_2(g) = h\epsilon_1(\omega(g))h^{-1}, \forall g \in G. \tag{25}$$

The conformal map $h : S_1 \to S_2$ induces a conformal map $\overline{h} : T_1 \to T_2$, and in diagram form we have:

$$\begin{array}{ccc} S_1 & \xrightarrow{h} & S_2 \\ \downarrow{\scriptstyle \pi_{G_1}} & & \downarrow{\scriptstyle \pi_{G_2}} \\ T_1 & \xrightarrow{\overline{h}} & T_2 \end{array} \tag{26}$$

where G_1 and G_2 denote the subgroups $\epsilon_1(G) \leq \mathrm{Aut}(S_1)$, $\epsilon_2(G) \leq \mathrm{Aut}(S_2)$. The conformal homeomorphism $\overline{h} : T_1 \to T_2$ must preserve branch points and their orders and hence defines a conformal homeomorphism $T_1^\circ \to T_2^\circ$. Frequently, we shall start with the bottom of diagram (26) given and want to fill in the top.

We start our discussion with the following proposition expressing conformal equivalence in terms of generating vectors.

Proposition 2.5. *Let S_1 and S_2 be surfaces, and let $G_1 \leq \mathrm{Aut}(S_1)$ and $G_2 \leq \mathrm{Aut}(S_2)$ be subgroups (that are not initially assumed to be of the form $\epsilon_1(G)$ and $\epsilon_2(G)$), but satisfy diagram (26). Let T_1 and T_2, be the respective quotients. Also, let*

$$\mathcal{G} = \{\alpha_1, \ldots, \alpha_\tau, \beta_1, \ldots, \beta_\tau, \gamma_1, \ldots, \gamma_t\}$$

be a generating system for $\pi_1(T_1^\circ, Q_0)$ and $(a_1, \ldots, a_\tau, b_1, \ldots, b_\tau, c_1, \ldots, c_t)$ the corresponding generating vector for G_1, determined by a point P_0, lying over Q_0. Then the following hold:

1. *The group $G_2 = hG_1h^{-1}$ and hence $G_1 = \epsilon_1(G)$ and $G_2 = \epsilon_2(G)$ for a common group G acting on S_1 and S_2.*
2. *The map $\overline{h}$ maps the branch points of π_{G_1} to branch points of π_{G_2} of the same order. Hence $\overline{h} : T_1^\circ \to T_2^\circ$ is a conformal homeomorphism.*
3. *Let*

$$\mathcal{G}' = \{\alpha'_1, \ldots, \alpha'_\tau, \beta'_1, \ldots, \beta'_\tau, \gamma'_1, \ldots, \gamma'_t\}$$

be the generating system for $\pi_1(T_2^\circ, \overline{h}(Q_0))$ obtained by applying $\overline{h}$ to $\mathcal{G}$, and $(a'_1, \ldots, a'_\tau, b'_1, \ldots, b'_\tau, c'_1, \ldots, c'_t)$ the generating vector of G_2 derived from $\mathcal{G}'$ at

the point $h(P_0)$. Then

$$a'_i = ha_ih^{-1}, b'_i = hb_ih^{-1}, c'_j = hc_jh^{-1} \tag{27}$$

for all i and j.

Proof. To see statement 1, observe that h maps G_1 orbits to G_2 orbits, namely $h(G_1P) = G_2h(P)$ for all $P \in S_1$. For any $P \in S_1$, and $g \in G_1$

$$h(g(P)) = g'(h(P))$$

for some $g' \in G_2$. Setting $P = h^{-1}(P')$ we get

$$h(g(h^{-1}(P'))) = g'(h(h^{-1}(P'))) = g'(P').$$

It follows that $hgh^{-1} \in G_2$. Thus $g \to hgh^{-1}$ maps G_1 to G_2 with inverse $g' \to h^{-1}g'h$.

By statement 1, we observe that $|G_1| = |G_2|$. For statement 2, observe that the branching order at a point $Q = \pi_{G_1}(P)$ equals $|G_1| / \left|\pi_{G_1}^{-1}(Q)\right| = |G_2| / \left|\pi_{G_2}^{-1}(\overline{h}(Q))\right|$, so branching orders are preserved.

For equation 3, let P_0 lie over Q_0, $\alpha \in \pi_1(T_1^\circ, Q_0)$ and let $\widetilde{\alpha}$ be the lift of α to S_1° that is based at P_0. The lift of $\overline{h}(\alpha)$ to S_2° starting at $h(P_0)$ will be $h(\widetilde{\alpha})$. Thus $\xi'(\overline{h}(\alpha))$ is the element $x \in G_2$ such that

$$\begin{aligned} h(\widetilde{\alpha})(1) &= x(h(P_0)), \\ h(\xi(\alpha)P_0) &= x(h(P_0)), \\ h\xi(\alpha)h^{-1} &= x. \end{aligned}$$

This establishes criterion (27). □

Now, assume that the bottom and sides of the diagram (26) are given. If we want to fill in the top as in diagram (28), where the map, h, to be filled in is denoted by a dashed arrow, we need a criterion that, when satisfied, guarantees the existence of the covering transformation h.

$$\begin{array}{ccc} S_1 & \overset{h}{\dashrightarrow} & S_2 \\ \downarrow{\scriptstyle \pi_{\epsilon_1(G)}} & & \downarrow{\scriptstyle \pi_{\epsilon_2(G)}} \\ T_1 & \xrightarrow{\overline{h}} & T_2 \end{array} \tag{28}$$

Proposition 2.6. *Suppose that we have two actions ϵ_1, ϵ_2 of the same group G on two surfaces S_1, S_2 as diagram (28). Suppose further that $\overline{h}$ is a conformal homeomorphism, and that h is a map to be found as indicated by the dotted line. We also assume that:*

(1) *The map $\overline{h}$ maps the branch points of $\pi_{\epsilon_1(G)}$ to branch points of $\pi_{\epsilon_2(G)}$ of the same order. Hence $\overline{h} : T_1^\circ \to T_2^\circ$ is a conformal homeomorphism.*

(2) *Let*

$$\mathcal{G} = \{\alpha_1, \ldots, \alpha_\tau, \beta_1, \ldots, \beta_\tau, \gamma_1, \ldots, \gamma_t\}$$

be a generating system for $\pi_1(T_1^\circ, Q_0)$ and $(a_1, \ldots, a_\tau, b_1, \ldots, b_\tau, c_1, \ldots, c_t)$ the corresponding generating vector of G obtained from $\mathcal{G}$ and a specific P_0 lying over Q_0. Let $Q_0' = \overline{h}(Q_0)$, $P_0' \in \pi_{\epsilon_2(G)}^{-1}(Q_0')$ and

$$\mathcal{G}' = \{\alpha_1', \ldots, \alpha_\tau', \beta_1', \ldots, \beta_\tau', \gamma_1', \ldots, \gamma_t'\}$$

be the generating system for $\pi_1(T_2^\circ, Q_0')$ obtained by applying $\overline{h}$ to $\mathcal{G}$, and $(a_1', \ldots, a_\tau', b_1', \ldots, b_\tau', c_1', \ldots, c_t')$ the generating vector of G derived from $\mathcal{G}'$, with lifting starting at P_0'.

Then there exists an invertible conformal map h as in diagram (28) with $h(P_0) = P_0'$, if and only if there is a automorphism ω of G such that

$$a_i' = \omega(a_i), b_i' = \omega(b_i), c_j' = \omega(c_j). \tag{29}$$

for all i and j.

Proof. If $h : S_1 \to S_2$ exists, completing the diagram (28), then as we saw in Proposition 2.5 the automorphism ω is induced by conjugation by h, pulled back to G.

For the other direction let us assume that the criterion (29) holds and prove that h exists. From covering space theory, the map h exists (with the branch points and preimages removed) if and only if

$$\overline{h}_* \circ \left(\pi_{\epsilon_1(G)}\right)_* (\pi_1(S_1^\circ, P_0)) = \left(\pi_{\epsilon_2(G)}\right)_* (\pi_1(S_2^\circ, P_0')).$$

Consider the diagram

$$\begin{array}{ccc}
\pi_1(S_1^\circ, P_0) & \overset{\overline{h}_*}{\dashrightarrow} & \pi_1(S_2^\circ, P_0') \\
\downarrow{\scriptstyle (\pi_{\epsilon_1(G)})_*} & & \downarrow{\scriptstyle (\pi_{\epsilon_2(G)})_*} \\
\pi_1(T_1^\circ, Q_0) & \xrightarrow{\overline{h}_*} & \pi_1(T_2^\circ, Q_0') \\
\downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \xi'} \\
G & \xrightarrow{\omega} & G
\end{array}$$

We are proposing that putting the map $\overline{h}_*$ (suitably restricted) into the top row gives a commutative diagram. In particular, we need to prove that the image is as suggested. The only arrow in question is the top row, indicated by the dashed arrow. The subdiagram formed from the bottom two rows is commutative since the commutativity requirement holds for every element of the generating set $\mathcal{G}$ of $\pi_1(T_1^\circ, Q_0)$, according to equation (29). Furthermore, the horizontal maps are isomorphisms and the vertical maps are surjections. Now consider the subdiagram formed from the top two rows. The vertical maps are injective because the columns of diagram (28) are covering spaces. Since the columns of the entire diagram are exact and the bottom subdiagram commutes then $\overline{h}_*$ in the top row maps the kernels isomorphically as suggested. Thus, by covering space theory, we have constructed a partial map $h : S_1^\circ \to S_2^\circ$. As shown in the proof of Proposition 2.1, the map h may be completed to a conformal homeomorphism $h : S_1 \to S_2$ satisfying the requirements. □

Remark 2.4. If we allow h in equation (25) to be just a homeomorphism then the actions are said to be *topologically equivalent*. For a given genus there are only finitely many topological equivalence classes. For more detail see [6] and [7].

Remark 2.5. Suppose we have fixed a quotient surface T, (ordered) branch set $B_G = \{Q_1, \ldots, Q_t\}$, and signature $\mathcal{S} = (\tau, n_1, \ldots, n_t)$. Once we have fixed a generating set $\mathcal{G} \subset \pi_1(T^\circ, Q_0)$ we can enumerate the surfaces $S \to T$ and actions $\epsilon : G \to \mathrm{Aut}(S)$ with the given T, B_G, $\mathcal{S}$ by means of generating vectors. The actions are in $1-1$ correspondence with the generating vectors. The automorphism group $\mathrm{Aut}(G)$ acts freely on the generating vectors. Each $\mathrm{Aut}(G)$ class of vectors determines a unique branched covering space $S \to T$ with G-action and a unique subgroup $\epsilon(G) \leq \mathrm{Aut}(S)$. Two such coverings $S_1 \to T$, $S_2 \to T$, are equivalent if and only if the diagram (28) can be completed with $T_1 = T_2$ and $\overline{h} \in \mathrm{Aut}(T, B_G, \mathcal{S})$, the group of conformal automorphism of T respecting the branch points and signature. Thus the set of all covers $S \to T$ and equivalence classes of actions $\epsilon : G \to \mathrm{Aut}(S)$ are the equivalence classes of generating vectors under the action of $\mathrm{Aut}(T, B_G, \mathcal{S}) \times \mathrm{Aut}(G)$. For more detail see [6] and [7].

Families of curves and equisymmetry

Special placement of the branch points allows for extra automorphisms beyond the action of G. For instance Shaska [19] determines which hyperelliptic curves have

extra automorphisms by means of equations in the coefficients of the defining equations of hyperelliptic curves. In [16] Magaard, Shaska, Shpectorov, and Völklein discuss families of curves in moduli space and the links to the braid action and Hurwitz spaces. Our notion of family is very informal and is closer to a Hurwitz space than the equisymmetric strata of the branch locus of moduli space, discussed in [6]. Our definition will allow for curves in positive characteristic, so we use the term curve instead of surface. The example of cyclic n-gonal curves, in Section 5.1, is a simple tractable example.

A *family of curves* $\{S_b : b \in B\}$ is a morphism $\pi : E \to B$ such that each $S_b = \pi^{-1}(b)$, $b \in B$ is a smooth closed curve (compact Riemann surface). We assume that B is an irreducible variety or connected manifold. A *family of actions* for a family of smooth curves $\pi : E \to B$ is a family of monomorphisms

$$\epsilon_b : G \to \mathrm{Aut}(\pi^{-1}(b)),\ b \in B$$

such that: for each $g \in G$ the map $(b, x) \to (b, \epsilon_b(g)x)$ is an automorphism of the variety (manifold) $V = \{(b, x) : \pi(x) = b\}$. In [12], Guerrero discusses an expanded version of families of curves by using *holomorphic families of curves* where now the map $\pi : E \to B$ is holomorphic and B is a connected, complex manifold.

We also allow holomorphic families, since it is useful in studying the moduli space and Teichmüller space of surfaces. However, in the positive characteristic case, B must be an irreducible, locally-closed variety.

Two actions $\epsilon_1 : G \to \mathrm{Aut}(S_1)$ and $\epsilon_2 : G \to \mathrm{Aut}(S_2)$ of G on S_1 and S_2 are *(directly) equisymmetric* $\epsilon_1 \sim_D \epsilon_2$ if there is a family of curves $\pi : E \to B$ with a family of actions $\epsilon_b : G \to \mathrm{Aut}(\pi^{-1}(b))$, $b \in B$ such that there are $b_1, b_2 \in B$ with isomorphisms $\phi_i : \pi^{-1}(b_i) \backsimeq S_i$ and $\epsilon_i = \phi_i \circ \epsilon_{b_i} \circ \phi_i^{-1}$. Two actions $\epsilon_1 : G \to \mathrm{Aut}(S_1)$ and $\epsilon_m : G \to \mathrm{Aut}(S_m)$ are equisymmetric if there is a sequence of surfaces S_i and actions $\epsilon_i : G \to \mathrm{Aut}(S_i)$ such that $\epsilon_1 \sim_D \epsilon_2$, $\epsilon_2 \sim_D \epsilon_3, \ldots, \epsilon_{m-1} \sim_D \epsilon_m$. Typically the relations $\epsilon_i \sim_D \epsilon_{i+1}$ come from distinct families as i varies.

Remark 2.6. It is possible that two G actions are equisymmetric without the automorphism groups of the surfaces being isomorphic. In such a case we may have $\epsilon_i(G) \lneq \mathrm{Aut}(S_i)$ even though $\epsilon_b(G) = \mathrm{Aut}(\pi^{-1}(b))$ generically. In fact these are the very cases we are interested in.

More on the braid action

Now we want to consider the effect of a change in basis. The change of generating set $\mathcal{G} \to \mathcal{G}'$ for n-gonal actions over a fixed pair (T, B_G) induces an automorphism $\Phi : \pi_1(T^\circ, Q_0) \to \pi_1(T^\circ, Q_0)$. This induces a right action of $\mathrm{Aut}(\pi_1(T^\circ, Q_0))$ on generating vectors via the action on surface kernel epimorphisms given by

$$\xi \to \xi^\Phi = \xi \circ \Phi. \tag{30}$$

Now suppose that $\mathcal{G}$, $\mathcal{G}', \mathcal{V} = (c_1, \ldots, c_t)$, and $\mathcal{V}' = (c_1', \ldots, c_t')$ are related by

$$\mathcal{G}' = \Phi(\mathcal{G})$$

and

$$\xi = \xi(\mathcal{G}') = \xi(\Phi(\mathcal{G})) = \xi^\Phi(\mathcal{G}) = \mathcal{V}^\Phi. \tag{31}$$

The explicit equations, derived from (19) and (20), are

$$\gamma_j' = \Phi(\gamma_j) = \psi_j \gamma_{\theta(j)} \psi_j^{-1} \tag{32}$$

and

$$c'_j = c_j^{\Phi} = w_j c_{\theta(j)} w_j^{-1}. \tag{33}$$

The equations $\mathcal{G}' = \Phi(\mathcal{G})$ and $\mathcal{V}' = \mathcal{V}^{\Phi}$ simply say that the surface constructed from T, B_G, $\mathcal{G}'$, ξ, and $\mathcal{V}'$ is the same as the surface constructed from T, B_G, $\mathcal{G}$, ξ^{Φ}, and $\mathcal{V}'$. Thus we can restrict our attention to a single generating set $\mathcal{G}$. Two surfaces constructed in such a way will be called *braid companions*.

Proposition 2.7. *Let G, T, $B_G = \{Q_1, \ldots, Q_t\}$, $\mathcal{S}$, $\mathcal{G}$, and $\pi_1(T^\circ, Q_0) \overset{\xi}{\twoheadrightarrow} G$ be as defined above and held fixed. Then we have:*

1. *The surfaces S with G-action such that $S/G = T$ and $S \to T$ is branched over B with signature $\mathcal{S}$ are in 1-1 correspondence with the $\mathcal{S}$-generating vectors of G.*
2. *Let $\Phi \in \mathrm{Aut}(\pi_1(T^\circ, Q_0))$. Then Φ is induced by a homeomorphism h of T° and the generating vector of the G-action on the surface induced by $\xi \circ \Phi$ is $\mathcal{V}^{\Phi}$ defined by equation (33).*
3. *If the homeomorphism h above is orientation preserving then Φ is induced by a braid $(Q_1(s), \ldots, Q_t(s)), 0 \le s \le 1$ in $\mathbb{P}^1(\mathbb{C})^t$ as in Remark 2.1. Braid equivalent actions are equisymmetric.*
4. *The set of generating vectors $\{\mathcal{V}\}$ and the corresponding induced surfaces $\{S_{\mathcal{V}}\}$ with the given signature $\mathcal{S}$ consists of several orbits of the group $\mathrm{Aut}_{\mathcal{S}}(\pi_1(T^\circ, Q_0))$ where the subscript denotes the subgroup of automorphisms preserving the signature. Specifically the permutation θ in equation (33) should preserve the signature $\mathcal{S}$.*
5. *The braid action is generated by the following transformations.*

$$c'_{j+1} = c_j, \ c'_j = c_j c_{j+1} c_j^{-1},$$
$$c'_k = c_k, \ \text{otherwise.}$$

Proof. Statements 1, 2, and 4 follow from previous discussion. Statements 3 and 5 are well known from the literature [3]. □

3. Finding automorphism groups and their signatures for n-gonal surfaces

In this section we describe processes for determining automorphism groups of n-gonal surfaces by examining whether or not an n-gonal action of G extends to a larger group A. For some results on cyclic groups see [10]. These processes naturally break up into two cases depending on whether G is normal in A as suggested in the introduction. We deal with each case separately in the next two subsections. We approach the problem with two different methods depending on the chosen equivalence type: topological or conformal. We first briefly describe the methods and then give some details and examples in the next two subsections. In each subsection we first describe signature theorems that apply to Method 1 and then give some details about Method 2. In Section 5, Method 1 is extensively used.

Method 1: topological equivalence

The first method is "moduli free", namely we try to extend the G action up to topological equivalence. We are not too concerned about the actual configuration of B_G, just the associated signature $\mathcal{S}$.

For this method, we first find possible N and then possible A algebraically. In each case the structures of the inclusions $G \lhd N$ and $N < A$ and the given signature $\mathcal{S}$ of the G action restrict the possibilities for N and A and their signatures. Next, generating vectors for N and then A are sought, which is a purely computational problem. The action of A on a surface restricts to one of G, and the signature of the action of G can be computed by Theorem 2.3. If G is n-gonal then we compare its signature with $\mathcal{S}$. With more work (beyond the scope of this paper) we may compute a generating vector for the action of G by using the monodromy representation of A on A/G and compare the vectors in order to understand if they are topologically equivalent. In this paper we mainly focus the question of which signatures extend.

Method 2: conformal equivalence

Before starting we recall the definition of the core of a subgroup of a group. If $G < H$ the core of G in H is given by

$$\text{Core}_H(G) = \bigcap_{x \in H} xGx^{-1}. \tag{34}$$

We say that G has a trivial core in H or $G < H$ is a trivial core pair if

$$\text{Core}_H(G) = \{1\}. \tag{35}$$

In our second method we retain the information on B_G so when we extend, the extensions that are permissible depend on B_G. We keep on extending the action of G to larger groups in a stepwise fashion. Given the available computational tools, especially the primitive groups database, we use an inductive method with three cases. For $G < A$ consider any chain of subgroups

$$G = G_0 < G_1 < \cdots < G_s = A \tag{36}$$

where for each successive pair $G_j < G_{j+1}$ we have one of the following cases:

(1) Case 1: The subgroup $G_j \lhd G_{j+1}$.
(2) Case 2: The coset space G_{j+1}/G_j is a faithful, primitive action space for G_{j+1}, namely $\text{Core}_{G_{j+1}}(G_j) = \{1\}$ and there are no intermediate groups $G_j < H < G_{j+1}$.
(3) Case 3: There is $\{1\} \lhd M < G_j$ with $M \lhd G_{j+1}$.

Any chain of groups can be refined into such a chain. Case 3 is the general case and Cases 1 and 2 are the missing extreme cases where the core is trivial or all of G_j. In Case 2 we want a primitive action space so that we can use the primitive groups database. The transitive group database could be used but it is too unwieldily and does not have the range of the primitive groups database.

Starting with G, a branch set B_G, signature $(0; n_1 \ldots, n_t)$, and generating vector $(c_1 \ldots, c_t)$ we construct successive extensions $G_j < G_{j+1}$. Assuming we have constructed an action of G_{j+1}, the map $\pi_{j+1} : S/G_j \to S/G_{j+1}$ is a rational map of $\mathbb{P}^1$ to itself and the branch set B_{G_j} lies over $B_{G_{j+1}}$ via π_{j+1}. Furthermore, to construct the action of G_{j+1}, a generating vector $\mathcal{V}_{j+1}$ for G_{j+1}, with signature $\mathcal{S}_{j+1}$, needs to be computed with respect to a generating set $\mathcal{G}_{j+1} \subset \pi_1(\mathbb{P}^1 - B_{G_{j+1}})$ that is compatible with the map π_{j+1}. We discuss the construction of the generating vector and action in the next two subsections. When we can no longer extend the chain we have found the automorphism group of S. The Hurwitz bound $H \leq 84\,(\sigma - 1)$

forces

$$\frac{|H|}{|G|} \leq 42 \cdot \left(\sum_{j=1}^{t} \left(1 - \frac{1}{n_i}\right) - 2 \right), \tag{37}$$

so that the process terminates.

Remark 3.1. We note that the sequence (36) depends on the configuration of the branch set B_G. Typically it is difficult to precisely determine the branch set B_{G_j} and generating vector $\mathcal{V}_j$. The scope of this paper allows us say the following: we can find all extensions $G < H$, and all generating vectors for n-gonal actions of H on a surface S such that the signature of the restricted G action on S has the initial signature $(n_1 \ldots, n_t)$. In principal, the branch set B_H can be lifted all the way up to S/G to produce branch set B'_G, and likewise a generating set $\mathcal{G}'_0 \subset \pi_1(\mathbb{P}^1 - B_G)$ and generating vector $\mathcal{V}'_0$. Even if $B'_G = B_G$, the generating vectors $\mathcal{V}'_0$ and $\mathcal{V}$ may not be easily comparable since the original generating sets $\mathcal{G}$ and $\mathcal{G}'_0$ may not be equal. So we can say that there is a G action on a surface S' that "looks like" the original G-action and extends to H. More precisely in the general family of surfaces with G-action with a fixed signature $\mathcal{S}$ there is a subfamily where the action extends to H. Typically "looks like" will mean that S' and S will be braid companions.

Remark 3.2. Though not directly relevant to our work here, the papers [2] and [13] discuss the possible monodromy groups of rational maps $\phi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$. Our maps $S/G \to S/A$ are such maps, so the cited works allow us to say general things about the extensions $G < A$.

3.1. **The normal extension case.**

3.1.1. *Platonic Groups.* Given an n-gonal group G, since G is normal in N, the group $K = N/G$ acts on the surface $S/G = \mathbb{P}^1$, so that K is a finite subgroup of $\mathrm{PSL}(2, \mathbb{C})$. All such groups, and their signatures, are well known:

Theorem 3.1. *Any finite $K \leq \mathrm{PSL}(2, \mathbb{C})$ is isomorphic to one of C_k, D_k, A_4, S_4 or S_5 (C_k is cyclic group of order k and D_k dihedral group of order $2k$). The signatures for each such group are given in Table 1.*

Group	Signature
C_k	(k, k)
D_k	$(2, 2, k)$
A_4	$(2, 3, 3)$
S_4	$(2, 3, 4)$
A_5	$(2, 3, 5)$

TABLE 1. Groups of Automorphisms and Signatures of $\mathbb{P}^1$

Notation 3.2. *An orbit $K \cdot P$ is called singular if $K_P \neq \{1\}$ and is called regular if $K_P = \{1\}$.*

Thus the possible N's satisfy the short exact sequence

$$G \hookrightarrow N \twoheadrightarrow K$$

which can be solved for a given G and K.

3.1.2. *Signatures for N.* The possible signatures for a normal extension N can be recovered from G and K using Proposition 2.4. Specifically, we have the following, which is a generalization of [22, Proposition 4.1]:

Proposition 3.3. *Suppose the signature of $K = N/G$ is (d_1, d_2, d_3) (with d_3 deleted if $K = C_k$) and let $\mathcal{O}(G)$ denote the set of orders of elements in G.*

(1) *The signature of N is of the form*

$$(a_1 d_1, a_2 d_2, a_3 d_3, m_1, \ldots, m_s)$$

where $a_i \in \mathcal{O}(G)$ and $m_i \in \mathcal{O}(G)\backslash\{1\}$.

(2) *The signature of G is*

$$\Big(\underbrace{a_1, \ldots a_1}_{|K|/d_1-times}, \underbrace{a_2, \ldots a_2}_{|K|/d_2-times}, \underbrace{a_3, \ldots a_3}_{|K|/d_3-times}, \underbrace{m_1, \ldots m_1}_{|K|-times}, \ldots \underbrace{m_r, \ldots m_s}_{|K|-times}\Big)$$

where any 1's are removed.

Technically speaking, the way Proposition 3.3 has been stated, we are starting with the signature for N and finding the signature for G. However, given a specific signature for G, it is not hard to see how to reverse this process to determine the possible K's which could extend G and the corresponding signatures for N. We illustrate with a example.

Example 3.1. Example 2.1 shows the cyclic group G of order 7 acts on a genus 3 surface with signature $(7, 7, 7)$. We determine the signatures of possible normal extensions.

First, since none of the periods are divisible by 2, we can only have $K = C_k$ for some k. This means that N has signature of the form $(a_1 k, a_2 k, 7)$ where $a_1, a_2 \in \{1, 7\}$. Since G has just three periods, we must have $k \leq 3$. When $k = 3$, we must have $a_1 = a_2 = 1$ and N has signature $(3, 3, 7)$. When $k = 2$, must have exactly one of a_1 or a_2 equal to 7, and N has signature $(2, 7 \cdot 2, 7)$.

We note that just because a given N and corresponding signature for N exist does not mean that an n-gonal group G extends to N acting on an n-gonal surface. Thus next we consider conditions on generating vectors for an n-gonal group G which ensures the extension to some larger group N.

3.1.3. *Normally extending actions by cyclic groups.* Fix a branch set $B_G = \{Q_1, \ldots, Q_t\}$, a generating system $\mathcal{G} = (\gamma_1, \ldots, \gamma_t)$, and signature $\mathcal{S} = (n_1, \ldots, n_t)$. As in Remark 2.5, all possible n-gonal G actions with given B_G and $\mathcal{S}$ are determined by a generating vector $(c_1, \ldots, c_t)$ with respect to $\mathcal{G}$. When classifying and analyzing actions via generating vectors, all vectors need to be computed with respect to the given $\mathcal{G}$. When trying to extend a given action with respect to a subgroup of $\mathrm{Aut}(T, B_G, \mathcal{S})$ (see Remark 2.5) we need to choose a $\mathcal{G}$ adapted to transformations in $\mathrm{Aut}(T, B_G, \mathcal{S})$. We now consider the simple case that an automorphism h of S normalizes the action of G, so $K = C_k = \langle h \rangle$. Since h normalizes G we have the following diagram

$$\begin{array}{ccc} S & \xrightarrow{h} & S \\ \downarrow{\scriptstyle \pi_G} & & \downarrow{\scriptstyle \pi_G} \\ T & \xrightarrow{\overline{h}} & T \end{array} \tag{38}$$

where $\overline{h}$ is the induced map. We will construct a set of loops in T° adapted to the action of $\overline{h}$ and compute the action.

Construction 3.4. *For the purpose of discussion, we may assume that $\overline{h} : z \to uz$ is a rotation where u is a kth root of 1. It follows then that the set B_G consists of possible singular $\langle \overline{h} \rangle$ orbits $\{0\}$ and/or $\{\infty\}$ and p regular orbits $\{z_i, \dots u^{k-1} z_i\}$ for various distinct z_i in $\mathbb{C}^*$.*

(1) *Select a ray ℓ from 0 to ∞ that contains no point of B_G. The k transforms $u^j \ell$ of ℓ cut up $\mathbb{C}$ into k wedges $W_1, \dots, W_k$, where W_j is the wedge bounded by $u^{j-1}\ell$ and $u^j \ell$. Each of the orbits $\{z_i, \dots u^{k-1} z_i\}$ meets each wedge in a unique interior point $u^j z_i$. We assume that $z_i \in W_1$ for all i.*
(2) *Order the z_i so that $|z_1| \leq \cdots \leq |z_p|$.*
(3) *Next we draw a simple, smooth arc $\zeta(t)$, $0 \leq t \leq 1$, lying in W_1, that starts at z_1, ends at z_p and passes through all the intermediate z_i in order. Modify the arc ζ slightly so that z_i lies slightly to the right of the curve as we traverse from start to finish.*
(4) *Select a point Q_0 on ℓ with $0 < |Q_0| < |z_1|$.*
(5) *We construct a series of p loops $\gamma_{i,1}$ defined as follows:*
   (a) *Follow a path from Q_0 to $\zeta(0)$ (the same path for each z_i).*
   (b) *Follow a path from $\zeta(0)$ to a point $\zeta(t_i)$ very near z_i. Pick $t_1 = 0$, $t_p = 1$, and the other t_i increasing in value.*
   (c) *Make a short excursion from $\zeta(t_i)$ towards z_i.*
   (d) *Make a small counterclockwise circle that lies entirely to the left of ζ.*
   (e) *After circling z_i return to Q_0 reversing the steps in a,b,c.*
(6) *The transformation $z \to u^{j-1} z$ maps W_1 to W_j and maps $\gamma_{i,1}$ to $u_*^{i-1}(\gamma_{i,1})$ Let δ_j be the counterclockwise arc from Q_0 to $u^{j-1} Q_0$ along the circle $|z| = |Q_0|$.*
(7) *Define*
$$\gamma_{i,j} = \delta_j u_*^{j-1}(\gamma_{i,1})\, \delta_j^{-1}.$$
(8) *Let γ_1 be the arc that travels along ℓ towards 0 encircles 0 in a small circle about the origin and reverses course along ℓ back to Q_0. Let γ_2 be the arc that travels along ℓ towards ∞ encircles all the finite branch points by a large circle about the origin and then reverses course along ℓ back to Q_0.*

Let $\mathcal{G} = (\gamma_2, \gamma_{1,1}, \dots, \gamma_{p,1}, \dots, \gamma_{1,k}, \dots, \gamma_{p,k}, \gamma_1)$. By construction the paths can be jiggled slightly so that the conditions of Construction 2.2 are satisfied. Denoting $\left(\prod_{i=1}^{p} \gamma_{i,j}\right)$ by Γ_j we have,

$$\gamma_2 \prod_{j=1}^{k} \left(\prod_{i=1}^{p} \gamma_{i,j} \right) \gamma_1 = \gamma_2 \left(\prod_{j=1}^{k} \Gamma_j \right) \gamma_1 = 1.$$

The inside product Γ_j is an ordered product over the branch points in a wedge. See Figure 2.

Proposition 3.5. *Let all notation be as in Construction 3.4 and let*

$$\mathcal{V} = (c_2, c_{1,1}, \dots, c_{p,1}, \dots, c_{1,k}, \dots, c_{p,k}, c_1)$$

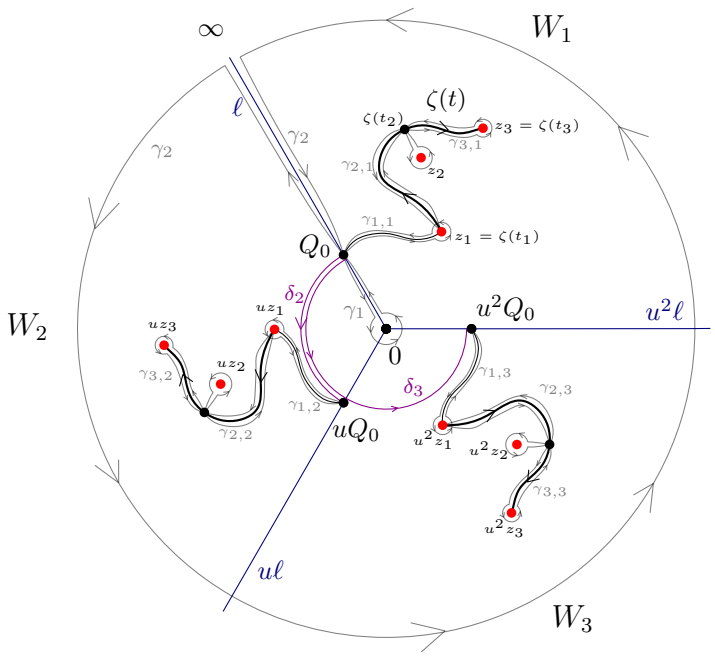

FIGURE 2. Construction 3.4.

be the corresponding generating vector. Then

$$\begin{aligned}
\delta_1\overline{h}_*(\gamma_1)\delta_1^{-1} &= \gamma_1\\
\delta_1\overline{h}_*(\gamma_2)\delta_1^{-1} &= \Gamma_1^{-1}\gamma_2\Gamma_1\\
\delta_1\overline{h}_*(\gamma_{i,j})\delta_1^{-1} &= \gamma_{i,j+1},\ 1\le i\le p,\ 1\le j\le k-1\\
\delta_1\overline{h}_*(\gamma_{i,k})\delta_1^{-1} &= \gamma_1\gamma_{i,1}\gamma_1^{-1},\ 1\le i\le p.
\end{aligned}$$

Letting $C_i = \left(\prod_{i=1}^{p} c_{i,j}\right)$*,then the* G *action extends to an action* $\widetilde{G}$ *on* S *with* $G \hookrightarrow \widetilde{G} \twoheadrightarrow \langle\overline{h}\rangle$ *if and only if there is an automorphism* ω *of* G *such that*

$$\begin{aligned}
\omega(c_1) &= c_1\\
\omega(c_2) &= C_1^{-1}c_2C_1\\
\omega(c_{i,j}) &= c_{i.j+1}, 1\le i\le p,\ 1\le j\le k-1\\
\omega(c_{i,k}) &= c_1c_{i,1}c_1^{-1}, 1\le i\le p.
\end{aligned}$$

Moreover

$$\widetilde{G} = \left\langle h, G : h^k\in G, hgh^{-1} = \omega(g), g\in G\right\rangle.$$

Proof. We leave to the reader the proofs of the first, third, and fourth formulas for the transforms of the elements of $\mathcal{G}$. For the second formula we write

$$\gamma_2\Gamma_1\cdots\Gamma_k\gamma_1 = 1$$

and denoting $\gamma \to \gamma'$ the transform $\gamma' = \delta_1 \overline{h}_*(\gamma)\delta_1^{-1}$ we see that $\Gamma'_j = \Gamma_{j+1}$ for $1 \le j \le k-1$, and $\Gamma'_k = \gamma_1\Gamma_1\gamma_1^{-1}$. It follows that

$$\begin{aligned}\gamma'_2\Gamma'_1\cdots\Gamma'_k\gamma'_1 &= 1\\ \gamma'_2\Gamma_2\cdots\Gamma_k\gamma_1\Gamma_1\gamma_1^{-1}\gamma_1 &= 1\\ \gamma'_2\Gamma_2\cdots\Gamma_k\gamma_1\Gamma_1 &= 1\\ \gamma'_2\Gamma_2\cdots\Gamma_k\Gamma_1\Gamma_1^{-1}\gamma_1\Gamma_1 &= 1.\end{aligned}$$

Now

$$\begin{aligned}\Gamma_1\cdots\Gamma_k &= \gamma_2^{-1}\gamma_1^{-1}\\ \Gamma_2\cdots\Gamma_k\Gamma_1 &= \Gamma_1^{-1}\gamma_2^{-1}\gamma_1^{-1}\Gamma_1,\end{aligned}$$

and

$$\begin{aligned}1 &= \gamma'_2\Gamma_2\cdots\Gamma_k\Gamma_1\Gamma_1^{-1}\gamma_1\Gamma_1\\ &= \gamma'_2\Gamma_1^{-1}\gamma_2^{-1}\gamma_1^{-1}\Gamma_1\Gamma_1^{-1}\gamma_1\Gamma_1\\ &= \gamma'_2\Gamma_1^{-1}\gamma_2^{-1}\Gamma_1.\end{aligned}$$

It follows that

$$\gamma'_2 = \Gamma_1^{-1}\gamma_2\Gamma_1.$$

The rest of the proof is a straightforward application of Proposition 2.6. □

Example 3.2. Let G be the cyclic group of order 7 with generator x. From Example 3.1, we know there is a possible C_3 extension where N has signature $(3,3,7)$. Letting $B_G = \{1, u, u^2\}$ where u is a third root of unity, generating vectors from Proposition 3.5 will be of the form $(1, x^a, x^b, x^c, 1)$ where $a+b+c$ is divisible by 7 (note: c_1 and c_2 are trivial since neither 0 nor ∞ are in B_G, so the corresponding loops are trivial in the fundamental group). One such generating vector is $(1, x, x^2, x^4, 1)$. For this generating vector, it is easy to check that $\omega(x) = x^2$ is an automorphism of G which satisfies the given properties in Proposition 3.5 for extension. Thus $N = \langle x, h : hxh^{-1} = x^2\rangle$ is an extension of G.

Extending actions for more general groups

To determine other possible normal extensions by other groups we proceed as follows. For each possible K, we first find a representative of K so that $\{Q_1, \ldots, Q_t\}$ is a union of complete orbits of K. Then:

(1) For a given K find a set generators of K.
(2) For each generator $\overline{h}$ of a generating set for K carry out the analysis for a single automorphism to see if $\overline{h}$ lifts.

3.2. **The non-normal extension case.**

3.2.1. *Finding Possible Signatures for A.* Finding the possible signatures for A is more difficult than for N, so rather than provide an explicit statement, we describe the basic process.

The first step in this process is finding the possible indices of N in A. Now, since we are assuming A is an automorphism group of a compact Riemann surface of genus σ, there are natural bounds on the size of A, with maximal values arising when the signature for A has just three periods. For example, Table 2 from Lemma 3.2 in [21] gives all possible signatures for A when $|A| \ge \frac{13}{2}(2\sigma - 2)$.

Signature	Additional Conditions	$\lvert A\rvert$
$(3,3,n)$	$4 \leq n \leq 5$	$\frac{3n}{n-3}(2\sigma-2)$
$(2,5,5)$		$10(2\sigma-2)$
$(2,4,n)$	$4 \leq n \leq 10$	$\frac{4n}{n-4}(2\sigma-2)$
$(2,3,n)$	$7 \leq n \leq 78$	$\frac{6n}{n-6}(2\sigma-2)$

TABLE 2. Signatures for Large Automorphism Groups

Using these bounds, we get corresponding bounds on d, the index of N in A. Specifically, either

$$d = \frac{|A|}{|N|} \leq \frac{13}{2} \cdot \left(\sum_{i=1}^{s} \left(1 - \frac{1}{m_i}\right) - 2 \right), \tag{39}$$

where $(m_1, \ldots, m_s)$ is the signature of N or the signature of A appears in Table 2 and the index d can be calculated exactly.

Next, if A does not have signature from Table 2, we can build the possible signatures for A as follows. Let $t_1, \ldots t_o$ denote the orders of non-trivial elements of N. For a given index d which satisfies the inequality in equation (39), letting $d_1, \ldots, d_q$ denote the divisors of d (including 1), A will have a signature of the form $((t_1 d_1)^{a_{1,1}}, (t_2 d_1)^{a_{2,1}}, \ldots, (t_o d_q)^{a_{o,q}})$ where:

- the signatures for N and A and the index d satisfy equation (22)
- for each m_i, there exists an n_j with $m_i | n_j$
- the signatures for N and A are compatible with some permutation representation Φ given in part (1) of Theorem 2.3.

Remark 3.3. We do not need to build the explicit representation given in the last step – just know that a compatible representation exists.

Remark 3.4. The process we have described for building signatures for A can be streamlined significantly, especially when we know the specific structure of N and its corresponding signature.

We illustrate with an example.

Example 3.3. Starting with the group action with signature $(3,3,7)$ from Example 3.2, we find the possible signatures for non-normal extensions. First, equation (39) yields

$$d \leq \frac{13}{2} \cdot \frac{4}{21} < 2,$$

which is impossible, and so any signatures for non-normal extensions must come from Table 2. Since there must be periods divisible by both 3 and 7, this just leaves signatures of the form $(2,3,n)$ where n is divisible by 7. Calculation shows that the only possible one of these signatures which satisfy equation (22) is $(2,3,7)$, so in particular, this is the only possible signature for a non-normal extension.

Remark 3.5. We note that the inclusion of signatures in Example 3.3 is already well known. Our purpose however was to illustrate the basic process of finding signatures for non-normal extensions.

3.2.2. *Primitive trivial core extensions.* Now suppose we have a non-normal extension $G < H$. We are going to focus on Case 3 described at the beginning of this section. We may find all H, generating vectors $\mathcal{V}_H$, the corresponding $S/G \to S/H$, and lifted branch sets, lifted generating sets $\mathcal{G}_G$, and generating vectors $\mathcal{V}_C$ in the steps below. Once the candidates have been found they need to be compared to the original B_G, $\mathcal{G}$, and $\mathcal{V}$.

Steps to find H:

1. Find the possible indices $d = |H| / |G|$ using the bound in (37).
2. For each d, search for primitive groups H of degree d whose point stabilizer is isomorphic to G.
3. For each H so determined, find all n-gonal signatures $\mathcal{S}_H$ such that an H-action with the given signature produces an n-gonal surface S with the given genus σ. Use the Riemann Hurwitz Theorem.

Steps to find signatures and generating vectors:

4. Using Theorem **2.3,** and the permutation representation of H on H/G find out which signatures $\mathcal{S}_H$ induce an n-gonal action of G with signature $\mathcal{S}$. Generating vectors are not needed at this stage, just the conjugacy classes of the elements of a generating vector.
5. For each signature found in Step 4 find all generating vectors $\mathcal{V}_H$ of H with the given signature.

Lifting Steps:

6. For each generating vector in Step 5 determine the map $S/G \to S/H$ as a rational function.
7. For each generating vector in Step 5 determine a lifted generating set $\mathcal{G}_H$.
8. For each map in Step 6 lift B_H to a branch set B on S/G.
9. For each generating vector $\mathcal{V}_H$ find a generating vector $\mathcal{V}_G$ of the G action (details below).

Comparison steps:

10. For each lift B in Step 7 compare B_H to B_G.
11. Compare the generating vector $\mathcal{V}_G$ with the original $\mathcal{V}$ (details below)

In the rest of the section we illustrate the steps above through example.

Finding H

Example 3.4. We start by considering the smallest non-Abelian example, $G = \Sigma_3$. Then G acts on a surface of genus 8 with signature $(2, 2, 2, 2, 2, 2)$ and generating vector $((1, 2), (1, 2), (2, 3), (2, 3), (1, 3), (1, 3))$. From equation (37) we get $d \leq 42 \times 1$. Here is a table of possible extensions computed using MAGMA.

H	t	$\lvert H/G\rvert$	potential $\mathcal{S}_H$	$\#\ \mathcal{V}_H/\lvert\mathrm{Aut}(H)\rvert$
Σ_4	3	4	$(4, 4, 4)$	0
Σ_4	4	4	$(2, 2, 2, 4)$	4
A_5	3	10	$(2, 5, 5)$	1

We see from the third column that there are two possible extensions. In the second row there are generically 4 different surfaces though for certain configurations some of the surfaces may be conformally equivalent.

Example 3.5. We consider the smallest simple example $G = A_5$. Using the primitive groups database in MAGMA we can check which primitive groups H have A_5 as a point stabilizer. There are 11 such groups H with primitive permutation degree less than 250. Among the groups, we have A_5, $A_5 \times A_5$, $SL(2,11)$, $PSL(2,q)$ for $q = 16, 19, 29, 31$, and $A_5 \ltimes \mathbb{F}_q^r$ for $(q,r) = (2,4), (3,4)$, and $(5,3)$.

Finding a $\mathcal{G}$ and $\mathcal{V}$

Let $U = S/H$, $B_H = \{R_1, \dots R_r\}$ and $\mathcal{H} = \{\delta_1, \dots, \delta_r\}$ be a generating set for $\pi_1(U^\circ, R_0)$, with Q_0 lying over R_0, and $(d_1, \dots, d_r)$ a generating vector for the H action. By covering space theory it may be shown that there are words $\psi_j \in \pi_1(U^\circ, R_0)$ such that

$$\gamma_j = \psi_j \left(\delta_{\zeta(j)}\right)^{e_j} \psi_j^{-1} \tag{40}$$

where $\pi_{H/G}(Q_j) = R_{\zeta(j)}$ and $e_j = o(d_{\zeta(j)})/o(c_j)$. Once we have $\mathcal{H}$ then we can compute an induced generating vector from a generating vector $\mathcal{V}_H = (d_1, \dots, d_r)$ via:

$$c_j = w_j \left(d_{\zeta(j)}\right)^{e_j} w_j^{-1}. \tag{41}$$

One way to compute the words in (40) is to have an explicit geometric model for $\pi_{H/G} : S/G \to S/H$ and then compute the images $\pi_{H/G}^*$ directly. This can be done for small examples.

Example 3.6. Let $G = \Sigma_3$, $H = \Sigma_4, \mathcal{V}_H = ((1,2),(2,3),(3,4),(1,2,3,4))$. If we let $R_4 = \infty$ the $\pi_{H/G}$ is a polynomial and a plausible map for $\pi_{H/G}$ is

$$\pi_{H/G} : z \to z^2 \left(3z^2 - 4(\lambda+1)z + 6\lambda\right),$$

where λ is a parameter. In the domain of $\pi_{H/G}$ there is a ramification point of order 4 at ∞, and ramification point of order 2 at 0. The other ramification points are the other zeros of the derivative $\pi'_{H/G}(z) = 12z\,(z-1)\,(z-\lambda)$, namely 1 and λ. The images of $0, 1, \lambda$ and ∞ under $\pi_{H/G}$ are $0, 2\lambda - 1, \lambda^3\,(2-\lambda)$, and ∞, respectively. Certain values of λ must be excluded to keep the values distinct. The preimages as formulae in λ could be computed but the solutions are ungainly. For $\lambda = 3$ we get:

$$\begin{aligned}
\pi_{H/G}^{-1}(0) &= \left\{0, 0, \frac{8}{3} + \frac{1}{3}\sqrt{10}, \frac{8}{3} - \frac{1}{3}\sqrt{10}\right\},\\
\pi_{H/G}^{-1}(5) &= \left\{1, 1, \frac{5}{3} + \frac{2}{3}\sqrt{10}, \frac{5}{3} - \frac{2}{3}\sqrt{10}\right\},\\
\pi_{H/G}^{-1}(-27) &= \left\{3, 3, -\frac{1}{3} + \frac{2}{3}i\sqrt{2}, -\frac{1}{3} - \frac{2}{3}i\sqrt{2}\right\},\\
\pi_{H/G}^{-1}(\infty) &= \{\infty, \infty, \infty, \infty\}.
\end{aligned}$$

Repeated entries indicate a ramification point.

Example 3.7. Let G and H be as in the example above, let $\mathcal{H} = \{\delta_1, \delta_2, \delta_3, \delta_4\}$ be a generating system for the H action. The monodromy vector for the action of H is the same as the generating vector. Using only the information in the monodromy vector, one can draw a lift of the system $\mathcal{H}$ in S/H to S/G via $\pi_{H/G} : S/G \to S/H$ with appropriate punctures. The lift is a system of arcs and loops in S/G. One can select loops $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$ that encircle $\{Q_1, Q_2, Q_3, Q_4, Q_5, Q_6\}$ in some order. The $\{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6\}$ can be modified by braid operations to achieve the

correct ordering on B_G. For the sake of argument we are going to assume that no reordering is necessary.

$$\gamma_1 = \delta_4^{-1}\delta_1\delta_4,\ \gamma_2 = \delta_4^{-1}\delta_2\delta_4,\ \gamma_3 = \delta_1\delta_2\delta_3\delta_2^{-1}\delta_1^{-1}$$
$$\gamma_4 = \delta_1\delta_3\delta_1^{-1},\ \gamma_5 = \delta_2,\ \gamma_6 = \delta_3$$

and

$$c_1 = d_4^{-1}d_1d_4,\ c_2 = d_4^{-1}d_2d_4,\ c_3 = d_1d_2d_2^{-1}d_1^{-1}$$
$$c_4 = d_1d_3d_1^{-1},\ c_5 = d_2,\ c_6 = d_3.$$

We compute:

$$c_1 = (2,3), c_2 = (3,4), c_3 = (2,3)$$
$$c_4 = (3,4), c_5 = (2,3), c_6 = (3,4).$$

The group generated by the c_j is the symmetric group on $\{2,3,4\}$, the stabilizer of 1. To compare the generating vector with the original, we first conjugate the stabilizer of 1 to Σ_3 and then use the braid action.

Remark 3.6. In general the map $\pi_1(T^\circ, Q_0) \to \pi_1(U^\circ, R_0)$ can be computed directly from the monodromy vector $(\Phi(d_1), \ldots, \Phi(d_r))$, where $\Phi : H \to \Sigma_d$ is the monodromy representation the cosets of H/G.

4. Strong branching and weakly malnormal actions

In this section, we introduce the main ideas behind strong branching. We also introduce an additional condition which, when combined with strong branching, ensures the n-gonal subgroup is normal in the full automorphism group.

4.1. **Strong branching.**

In [1], Accola introduced strong branching.

Definition 4.1. Let $\pi : S_1 \to S_2$ be a branched covering of degree n. The covering π is *strongly branched* if

$$R_\pi > 2n(n-1)(\sigma_2 + 1), \tag{42}$$

or, equivalently,

$$\sigma_1 > n^2\sigma_2 + (n-1)^2. \tag{43}$$

If the conditions do not hold then π is a called *weakly branched*.

Remark 4.1. If S_2 has genus 0 then the formulas become

$$R_\pi > 2n(n-1) \tag{44}$$

$$\sigma_1 > (n-1)^2. \tag{45}$$

For conciseness, if the map $S \to S/G$ is strongly branched, we shall also say that the group action of G is strongly branched.

In the context of finding automorphism groups, as indicated in Section 3, for a given n-gonal group, finding a normal extension (if one exists) is a difficult but tractable problem. In contrast however, finding non-normal extensions seems much more difficult. Strong branching ensures the existence of certain normal subgroups in the full automorphism group of a surface, thus making calculation of A more straightforward. Specifically, we have:

Proposition 4.1. *Let G be a group of automorphisms acting on a surface S such that $S \to S/G$ is strongly branched. Then there is a unique, normal, non-trivial subgroup M of $Aut(S)$ such that $M \leq G$, and $S \to S/M$ is strongly branched.*

Proof. By the proof of Corollary 3 of [1] there is a unique, maximal intermediate surface $S \to U \to S/G$ such that $S \to U$ is a Galois, strongly branched covering of degree exceeding one. Accordingly, there is a non-trivial subgroup $M \leq G$ such that $U = S/M$, and, as U is unique, M must be normal. □

4.2. **Number of branch points and families of actions.** Next we focus on the number of branch points for each action.

Number of branch points

One unfortunate drawback of using strong branching is that either the cut-off genus in equation (45) tends to be large or the number of branch points in the quotient is large. When considering surfaces as regular, branched coverings of quotients with branch points, it is more natural to use the number and order of the branch points, action signatures, and group orders as constraints rather than the genus of S, as in equation (45). Specifically, assuming a regular n-gonal action $\pi : S \to S/G$, and using equation (6), the strong branching criterion (44) can be written

$$\sum_{j=1}^{t} \left(1 - \frac{1}{n_j}\right) > 2(n-1), \tag{46}$$

upon noting that $\left|\pi^{-1}(Q_j)\right| n = n/n_j$.

If all the $n_j = n$, as in the prime cyclic case and the superelliptic case then we must have:

$$t > 2n. \tag{47}$$

The worst possible case (largest t) is when $n_j = 2$ for all j and then we must have $t > 4(n-1)$. For a weaker lower bound on t, if we replace all the $1 - \frac{1}{n_j}$ by 1 we must have

$$t > 2(n-1). \tag{48}$$

We can use equation (46) to estimate the number of weakly branched, potential signatures for a G action. Let $e_1, \ldots, e_r$ be the orders of non-trivial elements of G, In a given n-gonal signature $(n_1, \ldots, n_t)$, let $x_k = |\{j : n_j = e_k\}|$, then from equation (46) a signature is weakly branched if

$$\sum_{k=1}^{r} \left(1 - \frac{1}{e_k}\right) x_k \leq 2(n-1). \tag{49}$$

The number of nonnegative integer solutions to this equation has a reasonable approximation (lower bound) by the volume of the simplex in the positive $\mathbb{R}^r$orthant bounded by the hyperplane $\sum_{k=1}^{r} \frac{e_k - 1}{e_k} x_k = 2(n-1)$. Thus

$$\#signatures \geq \frac{(2n-2)^r}{r!} \prod_{k=1}^{r} \frac{e_k}{e_k - 1}.$$

For $G = A_5$ the smallest non-Abelian simple group, $e_1 = 2, e_2 = 3, e_3 = 5$ and

$$\#signatures \geq \frac{118^3}{3!}\frac{2}{1}\frac{3}{2}\frac{5}{4} = 1026895.$$

The actual number of potential n-gonal signatures is 1053238, directly computed using MAGMA.

The proportions of strongly branched actions and n-gonal actions

One obvious lingering question underlying our work is how frequently strong branching can be used in determining full automorphism groups. Specifically, our goal is to develop methods to find full automorphism groups for n-gonal surfaces and for surfaces which admit strongly branched group actions (and combinations of both). In this context, the question of how frequently these methods can be used for a fixed genus comes down to what proportion of group-signature pairs are either strongly branched or n-gonal for a fixed genus. The large bound on the number of branch points and/or quotient genus suggests that group-signature pairs with groups that are strongly branched are rare. In contrast however, the high frequency of genus-0 actions suggests that group-signature pairs for automorphism groups of n-gonal surfaces should actually be quite frequent. It is not immediately clear how to prove such assertions in general, but the available data for low genus actions (such as Breuer's lists, up to genus 48, in [5]) supports the following:

- In a fixed genus, the proportion of total actions which are strongly branched lies roughly between 2% and 5%.
- The number of group-signature pairs for n-gonal actions is a substantial proportion of all actions. Indeed, over all genera less that 49, 55% of actions are n-gonal.
- In a fixed genus, the proportion of n-gonal actions which are strongly branched is around 10% on average.

In particular, the frequency with which n-gonal surfaces seem to occur certainly supports further development of techniques to find their automorphism groups. Though strong branching occurs less frequently, further study of strongly branched actions makes sense since they are more tractable than the general case and the strong branching condition provides a good theoretical cut-off point.

Remark 4.2. According to equations (46), (47), and (48), in the presence of strong branching, we have a large dimensional family $\pi : E \to B$ where the typical fiber has a G action with a given signature $(n_1, \ldots, n_t)$, e.g., the cyclic n-gonal families. In many cases, for a typical fiber $\pi^{-1}(b)$ the action of G on $\pi^{-1}(b)$ constitutes the full automorphism group A, and strong branching does not tell us anything special since the guaranteed normal subgroup satisfies $M = G = A$. In this case we have a large open set $B^\circ \subset B$ of G-equisymmetry. For special values of b (actually subvarieties) $\mathrm{Aut}(\pi^{-1}(b))$ is strictly larger than the image of G. The various possibilities for $M \leq G \leq A$ with $M \lhd A$ correspond to subvarieties of B, with equisymmetric actions of A.

4.3. **Weakly malnormal actions.** We now introduce a key concept that allows us to use strong branching to guarantee normality. Recall that a subgroup G of a group A is called malnormal if $G \cap xGx^{-1}$is trivial whenever $x \notin G$. We generalize this definition.

Definition 4.2. A subgroup G of a group A is said to be *weakly malnormal* if and only if $G \cap xGx^{-1}$ is trivial when $x \notin N_A(G)$. Now suppose that G acts on S via $\epsilon : G \hookrightarrow \mathrm{Aut}(S)$. We say that the action of G on S is weakly malnormal if $\epsilon(G)$ is a weakly malnormal subgroup of A, the full automorphism group S.

Next, we present some useful facts about weak malnormality.

Proposition 4.2. *Let G act on S and $A = \mathrm{Aut}(S)$. The following statements characterize weakly malnormal actions:*

(1) *If $G \trianglelefteq A$, then G is automatically weakly malnormal in A.*
(2) *If G is weakly malnormal in A, but not normal, then G has a trivial core in A.*
(3) *If the subgroup $G < A$ is weakly malnormal then for any non-trivial $M \leq G$, we must have $N_A(M) \leq N_A(G)$.*
(4) *If G is cyclic then $N_A(G) = N_A(M)$ for any non-trivial $M \leq G$ if and only if G is weakly malnormal in A.*

Proof. Statements 1 and 2 are left to the reader. To prove statement 3, suppose $x \in N_A(M)$. Then for all $x \in A$, $G \cap xGx^{-1} \geq M \cap xMx^{-1} = M > \{1\}$. Since G is weakly malnormal, it follows that $x \in N_A(G)$. For statement 4, suppose that G is cyclic and weakly malnormal in A. We already have $N_A(M) \leq N_A(G)$. Suppose that $x \in N_A(G)$. Then M and xMx^{-1} both lie in G and so must equal each other since G has a unique subgroup of order $|M|$. It follows that $x \in N_A(M)$ and $N_A(G) = N_A(M)$. For the converse that $x \in A - N$ and suppose that $M = G \cap xGx^{-1}$ is not trivial, then both $M \leq G$ and $x^{-1}Mx \leq G$, so that M and $x^{-1}Mx$ both equal the unique subgroup of G of order $|M|$. Thus $x \in N_A(M) = N_A(G)$. This contradicts $x \in A - N$ so that we must have $G \cap xGx^{-1} = \{1\}$. □

In the next Proposition we see how to use strong branching and weak normality to prove normality results.

Proposition 4.3. *Suppose that G has a weakly malnormal action on S and that $\pi_G : S \to S/G$ is strongly branched. Then G is normal in A.*

Proof. Let M be the non-trivial normal subgroup of A contained in G guaranteed by Proposition 4.1. If G is not normal then

$$M = \bigcap_{x \in A} xMx^{-1} \leq \bigcap_{x \in A} xGx^{-1} = \{1\},$$

a contradiction. □

According to Proposition 4.1 if $S \to S/G$ is strongly branched then $\mathrm{Core}_A(G)$ is not trivial since G is guaranteed to have a non-trivial normal subgroup. In the introduction it was suggested that if $M = \mathrm{Core}_A(G) < G$ then we look at actions on S/M. Some useful properties of such actions are summarized in the next proposition.

Proposition 4.4. *Let S is a Riemann surface, $A = \mathrm{Aut}(S)$ and $G \leq A$ and let $M = \mathrm{Core}_A(G)$ be a proper subgroup of G. Then $\overline{S} = S/M$ is a surface upon which both $\overline{A} = A/M$ and $\overline{G} = G/M$ act naturally, and $\overline{A} \leq \mathrm{Aut}(\overline{S})$. Moreover, if $G \lneq A$ then $\overline{S} \to \overline{S}/\overline{G}$ is not strongly branched.*

Proof. The proof that $\overline{S}$ is a Riemann surface and that $\overline{A}$ and $\overline{G}$ act naturally is straightforward.

To show that if $G \lneq A$, then $\overline{S} \to \overline{S}/\overline{G}$ is not strongly branched, we proceed by contradiction. If $\overline{S} \to \overline{S}/\overline{G}$ is strongly branched then there would be a non-trivial subgroup of $\overline{G}$ that is normal in $\mathrm{Aut}(\overline{S})$. However, if $G \lneq A$, then

$$\mathrm{Core}_{\overline{A}}(\overline{G}) = \bigcap_{\overline{x}\in\overline{A}} \overline{x}\overline{G}\overline{x}^{-1} = \bigcap_{x\in A} \left(xGx^{-1}/M\right) = M/M = \{1\}$$

and

$$\mathrm{Core}_{\mathrm{Aut}(\overline{S})}(\overline{G}) \leq \mathrm{Core}_{\overline{A}}(\overline{G}) = \{1\}\,.$$

Therefore G does not contain a non-trivial subgroup that is normal in $\mathrm{Aut}(\overline{S})$, a contradiction. □

5. Determining Automorphism Groups

We finish by illustrating the tools and techniques we have developed to determine full automorphism groups of families of surfaces through explicit examples. We shall start with the most well known family – cyclic n-gonal surfaces – providing a brief survey of the known results, and introducing new ones. Following this, we shall provide a general outline of how to use strong branching in determining full automorphism groups when there is an n-gonal group which is simple, and then illustrate by exploring in detail the family of surfaces with n-gonal group isomorphic to the alternating group A_5. Throughout the whole section, we provide explicit details of how the techniques we employ can be used or adapted to other similar families. Where we feel confident, we will also provide conjectures that we hope will motivate further work.

5.1. **Cyclic n-gonal actions.** A ubiquitous and important case of group actions are those for which G is cyclic and S/G has genus 0. Such surfaces have tractable equations. A convenient form for such surfaces is given in the following.

Example 5.1. Let $m_1, \ldots, m_t$, and n be integers satisfying:

(1) $1 \leq m_j < n$,
(2) n divides $m_1 + \cdots + m_t$, and
(3) $\gcd(m_1, \ldots, m_t) = 1$.

Then the surface $\overline{S}$ defined by

$$y^n = (x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_t)^{m_t}, \tag{50}$$

where the $a_1, \ldots, a_t$, are distinct, is an irreducible cyclic n-gonal surface. If $m_j > 1$ the point $(a_j, 0)$ is singular. There are $d_j = \gcd(m_j, n)$ local branches of $\overline{S}$ at $(a_j, 0)$. The normalization map $\nu : S \to \overline{S}$ resolves the singularities and d_j points lie over $(a_j, 0)$. The action of $G = C_n$ on $\overline{S}$ is defined by $(x, y) \to (x, u^k y)$ where $u = \exp(2\pi i/n)$. This action lifts to S and the quotient map $\pi_G : S \to S/G$, called the n-gonal morphism, is given by $\pi_G : S \xrightarrow{\upsilon} \overline{S} \xrightarrow{\pi} \mathbb{P}^1$ where $\pi(x, y) = x$. The map π_G is branched over each $Q_j = a_j$, but is unbranched at ∞, by condition 2. Letting g be the automorphism $(x, y) \to (x, uy)$, we have $c_j = g^{m_j}$ and c_j fixes the d_j points lying over Q_j. The order of c_j is n/d_j so $n = n_j d_j$. For more details see [7].

Remark 5.1. If $n = p$ is prime we call the surface p-gonal.

Example 5.2. Two interesting special cases of cyclic n-gonal surfaces are *superelliptic surfaces* and *generalized superelliptic surfaces*. Superelliptic surfaces are those surfaces of the form

$$y^n = f(x)$$

where $f(x)$ is square free and n does not divide the degree of f. The point at ∞ will be a point of ramification. Of special interest is the case $n = p$ a prime. A *generalized superelliptic surface* has an equation as given in (50) where $\gcd(m_j, n) = 1$, or alternatively those cyclic n-gonal surfaces whose cyclic group of automorphisms has signature $(n, \ldots, n)$.

Example 5.3. Continuing Example 5.1, consider the family of curves defined by

$$y^n = (x - a_1)^{m_1} \cdot \cdots \cdot (x - a_t)^{m_t} \tag{51}$$

with $(a_1, \ldots, a_t) \in \mathbb{C}^t - \Delta$, where Δ is the multidiagonal. The family is constructed by first taking all points of the form $(x, y, a_1, \ldots, a_t) \in \mathbb{C}^{t+2}$ that satisfy (51) and then forming the closure E_1 of these points in $\mathbb{P}^2 \times (\mathbb{C}^t - \Delta)$. After normalizing E_1 we get $\pi : E \to B = \mathbb{C}^t - \Delta$ such that $\pi(x, y, a_1, \ldots, a_t) = (a_1, \ldots, a_t)$. The action ϵ_b, $b \in B$ of $G = C_n$ on E_1 is defined by $(x, y) \to (x, u^k y)$ where $u = \exp(2\pi i/n)$. The action is then lifted to E.

Remark 5.2. Every n-gonal action of a group G branched over t points can be included in a family $\pi : E \to B$ where B is a finite covering of $\mathbb{C}^t - \Delta$ (Hurwitz space).

5.1.1. *Determining automorphism groups of cyclic p-gonal surfaces.* Though full results are known, see for example [22], we briefly describe how to determine the full automorphism group when G has prime order p. In this case, the strong branching cut-off is $\sigma = (p-1)^2$ and so we have:

Proposition 5.1. *For prime $|G|$, if $\sigma > (p-1)^2$ then G is normal in A.*

As outlined in Section 1, we split up the classification of automorphism groups into the two cases of whether or not G is normal.

The normal case

Assuming that G is normal, then $N = A$ satisfies the short exact sequence

$$G \hookrightarrow N \twoheadrightarrow K$$

Determining the possible solutions for N is straightforward, with most cases being split extensions. Next, for each possible N, we can use Proposition 3.3 to construct possible signatures for N and then determine whether or not such an action exists by constructing generating vectors, or showing none exist. We illustrate with an example.

Example 5.4. When $K = C_k$, the solutions to the short exact sequence

$$G \hookrightarrow N \twoheadrightarrow C_k.$$

are a direct product $G \times C_k$, a semi-direct product $G \rtimes C_k$ and the cyclic group C_{kp} (note that for certain k, these groups might coincide).

Since the signature of C_k is (k,k) and the signature of G is $(\underbrace{p,\dots,p}_{r-times})$, using Proposition 3.3, the possible signatures of N are

$$(0;k,k,\underbrace{p,\dots,p}_{r/k-\text{times}}),(0k,kp,\underbrace{p,\dots,p}_{(r-1)/k-\text{times}}),(0;kp,kp,\underbrace{p,\dots,p}_{(r-2)/k-\text{times}}).$$

When a non-trivial semi-direct product $G\rtimes C_k$ exists, the only possible signature for which there can exist a generating vector is $(0;k,k,p,\dots,p)$.

If $\gcd(p,k)=1$, then $C_k\times C_p=C_{kp}$, and any of the three signatures could act as the signature of such a group action.

Finally, if $\gcd(p,k)=p$, then $C_k\times C_p$ and C_{kp} are distinct. In this case, when $A=C_k\times C_p$, a generating vector could only exist for the signature $(0;k,k,p,\dots,p)$ and for $A=C_{kp}$, a generating vector could only exist for the signature $(0;kp,kp,p,\dots,p)$.

In nearly all cases, a generating vector for the given group exists and is easy to construct. We leave the details to the reader.

See [8] for additional examples on normal extensions of cyclic actions.

The non-normal case

Now suppose that G is not normal in A. In this case, as expected, determining the possible A and signatures requires some ad hoc argumentation, so we refer to [22] for full details. We survey the basic steps here simplifying where possible.

We first note that automorphism groups for small primes can be found computationally using Breuer's database, [5]. For a given p, the strong branching cut-off is $\sigma=(p-1)^2$, and so each A for $p\le 7$ can be determined. Using this database, we obtain four different automorphisms groups whose details we summarize in the first four rows of Table 3. We henceforth then assume that $p\ge 11$.

Next, using the strong branching cut-off and the Riemann-Hurwitz formula, it is easy to show that when $p\ge 11$, any Sylow subgroup S of A has order either p^2 or p. We analyze these two cases individually.

First suppose that S, a Sylow p-subgroup of A, has order p^2. If S is cyclic, it must have signature $(p^2,p^2,\underbrace{p,\dots,p}_{\ell-\text{times}})$, see Example 5.4. For signatures of this form, the strong branching cut-off yields (p^2,p^2,p) as the only possibility. If S is elementary Abelian, then it must have signature $(\underbrace{p,\dots,p}_{\ell-\text{times}})$, and again using the strong branching cut-off, we must have $\ell=3$ or $\ell=4$. Each of these signatures can now be analyzed individually, and by doing so we find three different families of surfaces with non-normal overgroup, see the last three rows in Table 3.

Now suppose that $p^2\nmid|A|$. By Corollary 3.4 of [22], we know that $N>G$, and for the sake of simplicity, we also assume $K\neq C_k$. By looking at stabilizers of fixed points, we see that the signature of A differs only slightly from the signature of N, see Lemma 7.1 of [22]. Specifically:

Lemma 5.2. *There exists integers $m_1,\dots,m_{\nu_1},o_1,\dots,o_\tau$, o_i a multiple of p and each integer m_j and o_i/p relatively prime to p such that:*

(1) *the signature of N is $(m_1,\dots,m_{\nu_1},o_1,\dots,o_\tau,\underbrace{p,\dots,p}_{\ell\ times})$,*

(2) *the signature of K is $(m_1,\dots,m_{\nu_1},o_1/p,\dots,o_\tau/p)$*

(3) *the signature of* A *is* $(n_1, \ldots, n_{\nu_2}, o_1, \ldots, o_\tau, \underbrace{p, \ldots, p}_{\ell \text{ times}})$.

Moreover, each m_i *must divide at least one* n_j.

Next, instead of estimating the index d of N in A as outlined in Section 3.2, we can use Lemma 5.2 and equation (22) to calculate it explicitly:

$$d = \frac{-2 + \sum_{i=1}^{\nu_1} \left(1 - \frac{1}{m_i}\right) + \sum_{i=1}^{\tau} \left(1 - \frac{1}{o_i}\right) + l\left(\frac{p-1}{p}\right)}{-2 + \sum_{i=1}^{\nu_2} \left(1 - \frac{1}{n_i}\right) + \sum_{i=1}^{\tau} \left(1 - \frac{1}{o_i}\right) + l\left(\frac{p-1}{p}\right)} \tag{52}$$

which we can then simplify to:

$$d = 1 + \frac{\sum_{i=1}^{\nu_1} \left(1 - \frac{1}{m_1}\right) - \sum_{i=1}^{\nu_2} \left(1 - \frac{1}{n_i}\right)}{-2 + \sum_{i=1}^{\nu_2} \left(1 - \frac{1}{n_i}\right) + \sum_{i=1}^{\tau} \left(1 - \frac{1}{o_i}\right) + l\left(\frac{p-1}{p}\right)}. \tag{53}$$

Under the assumption that $p \geq 11$, we know all the possible signatures for K. Therefore it is straightforward, though time consuming, to show, except for a small number of cases which can be easily checked by hand, that if the extension is not normal, we must have $d < 12$. However, by Sylow theory, we know the index d of N in A has to be congruent to 1 modulo p, which is impossible since $p \geq 11$. Hence there are no further non-normal extensions of p-gonal groups to those already appearing in Table 3.

p	Signature of A	Signature of N	Genus	Group A
3	$(0; 2, 3, 8)$	$(0; 2, 2, 2, 3)$	2	$GL(2, 3)$
3	$(0; 2, 3, 12)$	$(0; 3, 4, 12)$	3	$[48, 33]$
5	$(0; 2, 4, 5)$	$(0; 4, 4, 5)$	4	S_5
7	$(0; 2, 3, 7)$	$(0; 3, 3, 7)$	3	$\mathrm{PSL}(2, 7)$
$p \geq 5$	$(0; 2, 3, 2p)$	$(0; 2, p, 2p)$	$\frac{(p-1)(p-2)}{2}$	$(C_p \times C_p) \rtimes S_3$
$p \geq 3$	$(0; 2, 2, 2, p)$	$(0; 2, 2, p, p)$	$(p-1)^2$	$(C_p \times C_p) \rtimes V_4$
$p \geq 3$	$(0; 2, 4, 2p)$	$(0; 2, 2p, 2p)$	$(p-1)^2$	$(C_p \times C_p) \rtimes D_4$

TABLE 3. Automorphism Groups of p-gonal Surfaces when $A \neq N$

5.1.2. *Strong branching and general cyclic n-gonal surfaces.* The obvious natural question to ask is whether the techniques we adopted for cyclic p-gonal surfaces can be used to determine full automorphism groups for other cyclic n-gonal surfaces. Strong branching played a key role in determining these groups as it ensured that there were only finitely many cases for which $A \neq N$, and from there we could apply ad hoc argumentation to construct the signature of A from the signature of N. Unfortunately the following example shows that for general cyclic n-gonal surfaces, strong branching does not ensure normality, and in particular, it is possible to construct infinitely many n-gonal surfaces for which $A \neq N$.

Example 5.5. Let $A = \langle x, y | x^4 = y^3 = xyx^{-1} = y^{-1} \rangle$, and $G = \langle x \rangle$. The group A has order 12 and G is a cyclic subgroup of order 4. We can define a generating vector for A with signature $(0; \underbrace{2, \ldots, 2}_{r \text{ times}}, 4, 4, 4, 4)$ for r even as follows:

$$(x^2, x^2, \ldots, x^2, x, x^{-1}, x, x^{-1}y^2)$$

Using Theorem 2.3, it is easy to show that the signature of the subgroup G is $(0; \underbrace{2, \ldots, 2}_{3r \text{ times}}, 4, 4, 4, 4)$ and the corresponding genus of the surface S on which A acts is $\sigma = 3r + 7$.

In the context of determining full automorphism groups, we observe that S is cyclic 4-gonal and the group G is never normal in A. However, the genus of S can be made arbitrarily large, so in particular, we can construct infinitely many cyclic 4-gonal surfaces of arbitrarily large genus for which a cyclic 4-gonal subgroup is not normal in A. A similar example can be constructed for $n = 9 = 3^2$, though the same construction fails for larger primes.

These group actions provide examples of strongly branched actions where the subgroup M from Proposition 4.1 is strictly contained in G.

5.1.3. *Generalized superelliptic surfaces.* The key result in determining automorphism groups for p-gonal surfaces was the fact that there were only finitely many group-signature pairs for which $A \neq N$, and this was due to strong branching – provided $\sigma > (p-1)^2$, G was guaranteed to be normal. In contrast, Example 5.5 showed there is little hope that strong branching will allow us to easily determine automorphism groups of all cyclic n-gonal surfaces. Therefore, this leads to the question of whether there are families of cyclic n-gonal surfaces, aside from the p-gonal ones, for which strong branching ensures normality of the cyclic n-gonal group in the full automorphism group. One such class is the generalized superelliptic surfaces (which includes the superelliptic surfaces).

Proposition 5.3. *Suppose that S is a generalized superelliptic n-gonal surface with cyclic automorphism group G. Further suppose that $S \to S/G$ is strongly branched, $\sigma > (n-1)^2$, $n = |G|$. Then G is normal in A.*

Proof. Since S is generalized superelliptic, then the stabilizer subgroup of G of any fixed point P is of order n, or equivalently $G_P = G$, if $G_P > \{1\}$. Let M be the normal subgroup of A contained in G, guaranteed by Proposition 4.1. Now suppose that P is any fixed point of G and that $x \in A - N$ satisfying $G \cap xGx^{-1} = M > \{1\}$. Then $G_P \geq M > \{1\}$ and so $G_P = G$. Next $G_{xP} = xG_Px^{-1} = xGx^{-1} \geq M > \{1\}$. It follows that $G_{xP} = G$ and $xGx^{-1} = G_{xP} = G$, a contradiction to $x \in A - N$. □

The importance of Proposition 5.3 is that G is normal when $\sigma > (n-1)^2$, and hence just like with the p-gonal case, for a given n, there are only finitely many possible A's for which $A \neq N$. Now, for a superelliptic surface S, when $A = N$, all possible A and the corresponding signatures were determined in [18]. In particular, the problem of complete classification comes down to analyzing just the A for which $A \neq N$.

To date, such a classification remains elusive. However, computational results for small n ($n \leq 12$), and attempts at generalizing the tools and techniques used for the cyclic p-gonal case suggest that there are no further families of groups, see

[9]. Consequently, we conjecture that the families already discovered (extended for all n) are the only possible ones for which $A \neq N$. Specifically:

Conjecture 5.4. *Suppose S is generalized superelliptic with $A \neq N$. Then A is one of the groups given in Table 3.*

See [15] for additional details on generalized superelliptic surfaces.

5.1.4. *Cyclic n-gonal cases which are not superelliptic.* Suppose now that $G = C_n$, and let S, A and N be as before. The strong branching condition only guarantees that there is cyclic subgroup $M = C_m \trianglelefteq A$ with $1 < m \leq n$. We would like to study cases where C_m is a proper subgroup of G, and to be specific we will focus on examples where $n = p^2$. The analysis using strong branching works as follows, assuming a classification of surfaces of any genus, with action group C_m.

(1) Assume $S \to S/G$ is strongly branched to obtain $M \trianglelefteq G$ with $\{1\} < M \trianglelefteq A$. We may assume that $M = \mathrm{Core}_A(G)$.
   (a) If $M = G$ then compute $A = N$ as an extension of G using the methods in Section 3.1.
   (b) If $G \not\trianglelefteq A$ then consider the quotient case $\overline{S} = S/M$, and the series of groups $\overline{G} \leq \overline{A} \leq \mathrm{Aut}(S')$ where $G' = G/M$, $A' = A/M$, $A'' = \mathrm{Aut}(S')$. Determine A' as a subgroup of A'' and then solve $M \hookrightarrow A \twoheadrightarrow A'$.
(2) If $S \to S/G$ is not strongly branched then use the methods of Section 3.2 to find A, assuming $A \neq N$. There are only finitely many cases to consider.

We will only consider what happens where $M < G$. Let us first consider the generalities of case $n = p^2$, and then work specific examples for low primes. To help with the bookkeeping of the numerous branch points we use the following notation. For $0 < k < n$ define

$$u_k = \left|\left\{j : c_j = x^k\right\}\right|.$$

A branch point has order p or p^2. If we let t_1 be the number of branch points of order p and t_2 be the number of branch points of order p^2, then we have:

$$\sum_{k=1}^{p^2-1} k u_k = 0 \bmod p^2,$$

$$t_1 = \sum_{k=1}^{p-1} u_{pk},$$

$$t_2 = t - t_1 \geq 2.$$

We need $t_2 \geq 2$, otherwise $|\langle c_1, \ldots, c_t\rangle| = p < |G|$. Thus

$$R_{\pi_G} = n \sum_{j=1}^{t} \left(1 - \frac{1}{n_j}\right) = p(p-1)t_1 + \left(p^2 - 1\right) t_2. \tag{54}$$

Using equation (14) the genus of S is given by

$$\begin{aligned}\sigma &= 1 + p^2(-1) + \frac{p^2}{2}\left(\frac{p-1}{p}t_1 + \frac{p^2-1}{p^2}t_2\right)\\ &= 1 - p^2 + \frac{p(p-1)}{2}t_1 + \frac{p^2-1}{2}t_2.\end{aligned}$$

Using equations (46) and (54), we see how many branch points are needed for strong branching:

$$\frac{p-1}{p}t_1 + \frac{p^2-1}{p^2}t_2 > 2(p^2-1)$$

or

$$t_1 > 2p(p+1) - \frac{p+1}{p}t_2. \tag{55}$$

Suppose $G = \langle x \rangle$, and assume the non-trivial subgroup guaranteed by strong branching is $M = \langle x^p \rangle$. According to Proposition 2.4 the number of ramification points of M acting on S is $pt_1 + t_2$ each with ramification order p and so $R_{\pi_M} = (pt_1 + t_2)(p-1)$. By equation (4) the genus σ' satisfies

$$\begin{aligned}\sigma' &= 1 + \frac{1}{2p}\left(2(\sigma-1) - R_{\pi_M}\right) \\ &= 1 + \frac{1}{2p}\left(2\left(-p^2 + \frac{p(p-1)}{2}t_1 + \frac{p^2-1}{2}t_2\right) - (pt_1+t_2)(p-1)\right) \\ &= \frac{(p-1)}{2}t_2 + 1 - p.\end{aligned}$$

The possible automorphism groups of S' are known from the classification of p-groups, except that extra work is needed for $\sigma' = 0, 1$. The automorphism group of S can be pieced together from $Aut(S')$ and M. If we assume that G is not normal in A then M is normal by the strong branching condition.

Example 5.6. Let us make a table of σ, σ' and the describe the cases for small primes $p = 2, 3, 5, 7$. According to Harvey, t_2 must be even when $p = 2$. Assuming strong branching we get

p	σ	σ'	restriction
2	$-3 + t_1 + 3\frac{t_2}{2}$	$\frac{t_2}{2} - 1$	$t_1 > 12 - 3\frac{t_2}{2}$
3	$-8 + 3t_1 + 4t_2$	$t_2 - 2$	$t_1 > 24 - \frac{4}{3}t_2$
5	$-24 + 10t_1 + 12t_2$	$2t_2 - 4$	$t_1 > 60 - \frac{6}{5}t_2$
7	$-48 + 21t_1 + 24t_2$	$3t_2 - 6$	$t_1 > 112 - \frac{8}{7}t_2$

Let us now describe examples of such possible groups.

Example 5.7. Let p and q be primes such that p divides $q-1$. Write $C_{p^2} = \langle x \rangle$ and $C_q = \langle y \rangle$ in multiplicative format. Let $a \in C_q^* = \mathrm{Aut}(C_q)$ be such that $a^p = 1 \bmod q$ which exists by divisibility conditions. Let C_{p^2} act upon $C_q = \langle y \rangle$ by

$$\theta : C_{p^2} \to C_q^* = \mathrm{Aut}(C_q)$$
$$x^j \cdot y^k = \theta(x^j)(y^k) \to \left(y^k\right)^{a^j}.$$

Then the semi-direct product

$$A = C_{p^2} \ltimes C_q = \left\langle x, y : x^{p^2} = y^q = 1, x^{-1}yx = y^a \right\rangle$$

satisfies:

- $\langle y \rangle$, $\langle x^p \rangle \lhd A$,
- $x^p y$ has order pq, and
- $\langle x \rangle \not\lhd A$. Indeed any cyclic subgroup of order p^2 is self-normalizing.

Example 5.8. Let $A = C_9 \ltimes C_7 = \langle x, y : x^9 = y^7 = 1, x^{-1}yx = y^2 \rangle$. ($A$ is SmallGroup(63,1) in MAGMA). The vector $\mathcal{V} = (x^7, xy, xy^5)$ is a generating vector with signature $(9, 9, 9)$, yielding a surface of genus 22. Using MAGMA as in Remark 2.3 we see that there is a cyclic subgroup of order 9 whose signature is $(3, 3, 3, 3, 3, 3, 9, 9, 9)$. This action is not strongly branched and so the non-normal extension is not a surprise. Next consider a generating vector obtained from $\mathcal{V}$ prepending 3 copies of x^3 to $\mathcal{V}$, i.e., $(x^3, x^3, x^3, x^7, xy, xy^5)$. The signature of the action of G has signature $(3^{27}, 9^3)$ and the surface has genus 85. This action is strongly branched. It is conceivable that the automorphism group is larger but the subgroup M must be $\langle x^3 \rangle$. Also of interest, in this case $\sigma' = 1$ and so the quotient S/G is a torus that supports a group of automorphisms of the form $C_3 \ltimes C_7$.

5.2. **Simple n-gonal groups and strong branching.** In the current literature, the only families for which strong branching has been used to determine full automorphism groups are cyclic groups, but there are other families for which strong branching should provide the framework for determining all possible automorphism groups. The most obvious of these is the family of simple groups. Specifically, since simple groups have no normal subgroups, we have:

Proposition 5.5. *For G simple, if $\sigma > (|G| - 1)^2$ then G is normal in A.*

In particular, for a given simple n-gonal group G, Proposition 5.5 ensures that there are only finitely many possible A for which $A \neq N$ and so we can use the same techniques for finding A as we have previously outlined.

The normal case for simple groups

When $A = N$, so G is normal in its full automorphism group, the possible signatures for A satisfy Proposition 3.3 with the possible A being solutions to the short exact sequence:

$$G \hookrightarrow A \twoheadrightarrow K,$$

We note that for a given simple group G, there could be a tremendous number of solutions to this short exact sequence, Moreover, there is no guarantee that these solutions should all split as we saw with the cyclic p-gonal case. In particular, for an arbitrary simple group, the normal case actually seems significantly more difficult than we have seen before. Fortunately however, for many simple groups, the following result of Rose ensures that this sequence splits, see [17, Theorem 2.7].

Theorem 5.6. *If the center of G is trivial and the automorphism group of G splits over its inner automorphism group, then all extensions over G split.*

In particular, when the conditions of Theorem 5.6 are satisfied, such as with most alternating groups, then $A \cong K \ltimes G$, and finding all such groups of this form is significantly more tractable than the general case.

The non-normal case for simple groups

For the case $A \neq N$, the problem is purely computational with only finitely many solutions, so in principle, the groups and signatures can be calculated using GAP or MAGMA. In practice of course, complete classification is not likely since the strong branching cut-off for an arbitrary simple group is going to be quite large, and finite group databases do not typically include groups of high enough order. However, through additional ad hoc argumentation, and by restricting to

intermediate extensions as outlined in Section 3, restrictions can be imposed on the possible groups and signatures which allow for steps to be made towards a more comprehensive classification. The following is an example of the types of computational results we can obtain to restrict our search.

Proposition 5.7. *If G is simple, $A \neq N$, and d is the index of N in A, then the number of periods r of the signature of A is bounded by:*

$$4\left(\frac{|G|-2}{d}+1\right) \geq r \geq 3.$$

Proof. Since $A \neq N$, we must have $\sigma \leq (|G|-1)^2$. Suppose that $(m_1, \ldots, m_r)$ is the signature of A. By the Riemann-Hurwitz formula,

$$\sigma - 1 = |A|\left(-1 + \frac{1}{2}\sum_{i=1}^{r}\left(1-\frac{1}{m_i}\right)\right).$$

Using the bound on σ then gives us

$$\frac{|G|(|G|-2)}{|A|} \geq -1 + \frac{1}{2}\sum_{i=1}^{r}\left(1-\frac{1}{m_i}\right).$$

Rewrite this as

$$2\left(\frac{|G|-2}{d}+1\right) \geq \sum_{i=1}^{r}\left(1-\frac{1}{m_i}\right). \tag{56}$$

Since $m_i \geq 2$ for each i,

$$\sum_{i=1}^{r}\left(1-\frac{1}{m_i}\right) \geq \frac{r}{2}$$

and thus

$$4\left(\frac{|G|-2}{d}+1\right) \geq r \geq 3.$$

□

Remark 5.3. We note that Proposition 5.7 actually holds provided the action of the group is weakly malnormal.

5.2.1. *Determining Automorphism Groups when $G = A_5$.* We finish by illustrating how such a classification might proceed by providing partial results for the first non-trivial case of this: when $G = A_5$. As is standard, we break the classification into two cases depending upon whether or not A_5 is normal in A.

The normal case when $G = A_5$

First we consider the case where $A = N$. Now we know any such group satisfies the short exact sequence

$$G \hookrightarrow A \twoheadrightarrow K$$

where K is one of the groups from Table 1. Moreover, since A_5 satisfies the hypotheses of Theorem 5.6, this sequence splits. In particular, A is a semidirect product which, for convenience, we consider as an outer semi-direct product $A_5 \rtimes_\psi K$ where $\psi\colon K \to \mathrm{Aut}(A_5) = S_5$ is the corresponding homomorphism defined by conjugation of elements of K on A_5. We can use these facts to determine all possible A's.

Proposition 5.8. *Suppose that $G = A_5$ and $A = N$. Then the possibilities for A are as follows:*

(1) *For all K, the direct product $A = A_5 \times K$.*
(2) *For $K = S_4$, $K = C_k$ for k even or $K = D_k$ for any k, we have an additional non-trivial semi-direct product $A_5 \rtimes_\psi K$ where $\psi\colon K \to Aut(A_5) = S_5$ is defined to have image $\langle(1,2)\rangle$ with kernel the unique index 2 subgroup of K.*
(3) *Further, for $K = D_k$, k even and $k > 2$, we have a second non-trivial semi-direct product $A_5 \rtimes K$ where $\psi\colon K \to Aut(A_5) = S_5$ is defined to have image $\langle(1,2)\rangle$ with kernel an index 2 dihedral group.*

Proof. Since $A = A_5 \rtimes_\psi K$, we just need to describe all such semi-direct products for each K. For $K = A_4$, S_4 and A_5, this can be done computationally using GAP and we attain the stated results. We need to explore in more detail the two infinite families $K = C_k$ and $K = D_k$

For $A = A_5 \rtimes_\psi K$, let K_1 be the kernel of ψ. Then the group $A_5 \rtimes_{\bar\psi} (K/K_1)$ where $\bar\psi$ is the induced homomorphism is either a non-trivial semi-direct product where $\bar\psi$ has trivial kernel, or it is isomorphic to A_5 and consequently A is a direct product $A_5 \times K$. Thus we consider $A_5 \rtimes_{\bar\psi} K/K_1$ for each possible K and K_1.

First suppose that $K = C_k$. Then K/K_1 is cyclic, and since it is a subgroup of $\mathrm{Aut}(A_5) = S_5$ it is either order 2, 3, 4 or 5. However, for each of these possibilities, simple computation using GAP gives a non-trivial semi-direct product $A_5 \rtimes_{\bar\psi} K/K_1$ only when K/K_1 is cyclic of order 2, and in this case $\bar\psi$ can be defined as in the statement of the theorem. The result follows.

Next suppose that $K = D_k$. Then K/K_1 is either cyclic of order 2 or dihedral. Therefore, since it is a subgroup of $\mathrm{Aut}(A_5) = S_5$ it is either cyclic of order 2 or dihedral of order 4, 6, 8, or 10. Again, for each of these possibilities, simple computation using GAP gives a non-trivial semi-direct product $A_5 \rtimes_{\bar\psi} K/K_1$ only when K/K_1 is cyclic of order 2 with the image of $\bar\psi$ as defined in the statement of the theorem. When k is odd, there is precisely one possible non-trivial kernel being the index 2 cyclic subgroup. When k is even and $k > 2$, there are three possible non-trivial kernels: the index two cyclic subgroup and the two index 2 dihedral subgroups, though the latter two yield isomorphic semi-direct products. The result follows.

□

The possible signatures with which the different normal extensions can act can be determined using Proposition 3.3. For a given such signature, determining whether or not an action exists depends on whether or not we can construct a generating vector, and this can in principle be done exhaustively. We note however that for a given A, there are many simple arguments which will eliminate signatures without having to consider generating vectors. Rather than presenting all possible signatures for all possible A, we illustrate with an example of how the general process follows, noting that for other A, the same general process holds. First, we fix the following notation.

Notation 5.9. *In a signature, we use the expression $m_i^{(k_i)}$ to denote k_i copies of the periods m_i.*

Example 5.9. Suppose that $K = C_2$, the cyclic group of order 2. Then there are two possibilities for A: the direct product $A_5 \times C_2$ and the semidirect product $A_5 \rtimes C_2$ which is isomorphic to the symmetric group S_5. Since the signature of K is $(2, 2)$, the possible signatures for each A are of the form

$$(2a_1, 2a_2, 2^{(a)}, 3^{(b)}, 5^{(c)}) \tag{57}$$

where $a_1, a_2 \in \{1, 2, 3, 5\}$. We now proceed by cases.

First suppose that $A = C_2 \times A_5$. Then A contains elements of orders $2, 3, 5, 6$ and 10, but not 4, so in particular, we can only have $a_1, a_2 \in \{1, 3, 5\}$. Of all remaining possible signatures of the form given in (57), the only ones for which a generating vector for A with n-gonal subgroup A_5 cannot be created are $(2 \cdot 3, 2 \cdot 3, 3)$ and $(2{\cdot}3, 2{\cdot}3, 2)$. Hence $A = C_2 \times A_5$ acts on an n-gonal surface S with n-gonal subgroup A_5 with all signatures of the form $(2a_1, 2a_2, 2^{(a)}, 3^{(b)}, 5^{(c)})$ for $a_1, a_2 \in \{1, 3, 5\}$ except $(2 \cdot 3, 2 \cdot 3, 3)$ and $(2 \cdot 3, 2 \cdot 3, 2)$.

Next suppose that $A = S_5$. Then A contains elements of order $2, 3, 4, 5$ and 6 but not 10 so in particular, we can only have $a_1, a_2 \in \{1, 2, 3\}$. Of all remaining possible signatures of the form given in (57), the only ones for which a generating vector for A with n-gonal subgroup A_5 cannot be created are $(2, 2, 3, 3)$ and $(2, 2, 2, 3)$. Hence $A = S_5$ acts on an n-gonal surface S with n-gonal subgroup A_5 with all signatures of the form $(2a_1, 2a_2, 2^{(a)}, 3^{(b)}, 5^{(c)})$ for $a_1, a_2 \in \{1, 2, 3\}$ except $(2, 2, 3, 3)$ and $(2, 2, 2, 3)$.

5.3. **The non-normal case when $G = A_5$.** Now suppose that $A \neq N$. Based on the computational evidence so far (see Example 3.5), there appear to be far more non-normal cases than we saw in the cyclic p-gonal case and at least currently there seems no obvious way to nicely categorize these non-normal extensions as we did in the cyclic p-gonal case. Therefore, rather than providing complete results, which currently seems computationally intractable, we shall provide some first steps to the general problem, and then illustrate with a few specific examples.

General facts for the non-normal case

By the strong branching condition, we know if $A \neq N$, then the genus of S must satisfy $\sigma < (|A_5| - 1)^2 = 3481$. Application of the Hurwitz bound then implies that the order of A and the index d of N in A satisfy

$$|A| \leq 84(\sigma - 1) = 292,320 \text{ and } d \leq 4872.$$

We know any signature for A_5 is of the form $(2^{(a)}, 3^{(b)}, 5^{(c)})$ for integers a, b and c so we can use the strong branching cut-off and the Riemann-Hurwitz formula to determine bounds on a, b and c. Specifically we have:

$$(60-1)^2 - 1 \geq \sigma - 1 = -60 + \frac{60}{2}\left(a\left(1 - \frac{1}{2}\right) + b\left(1 - \frac{1}{2}\right) + c\left(1 - \frac{1}{2}\right)\right)$$

which simplifies to

$$3540 \geq 15a + 20b + 24c.$$

It follows that

$$a \leq 230, \quad b \leq 172, \quad c \leq 147.$$

We note that not all choices of a, b and c are valid signatures and some may give a genus beyond the strong branching cut-off.

Next we observe by Proposition 5.7 that the number of periods of A satisfies

$$r \leq 4\left(\frac{58}{d}+1\right).$$

In particular, as d increases, the number of possible periods for A decreases, and in particular, when $d > 232$, then A has just three or four periods.

These conditions significantly reduce the number of possible non-normal extensions and the possible signatures, so at this point, to proceed with determining non-normal n-gonal extensions of A_5, we would follow the steps outlined in Section 3.

Determining alternating extensions of A_5

To illustrate our work, we consider n-gonal extensions of A_5 to all the alternating groups within the strong branching cut-off. Since $|A| \leq 292,320$, this gives A_6, A_7 and A_8 as possibilities. Also, we know that $A_5 < A_6 < A_7 < A_8$ with each containment being maximal, so the intermediate extensions are each primitive.

Consider first A_6 actions. The signature of an A_6 action will be of the form $(0; 2^{a_1}, 3^{b_1}, 4^{c_1}, 5^{d_1})$. As with A_5, we can use the strong branching cut-off and Riemann-Hurwitz formula to determine bounds on a_1, b_1, c_1 and d_1, see equation (5.3). Specifically, we get:

$$3480 \geq 360\left(-1+\frac{1}{2}\left(\frac{a_1}{2}+\frac{2b_1}{3}+\frac{3c_1}{4}+\frac{4d_1}{5}\right)\right)$$

which simplifies to

$$3840 \geq 90a_1 + 120b_1 + 135c_1 + 144d_1.$$

There are 38 164 solutions to this inequality, but with A_6 being relatively small in order, for each of these signatures, we can construct all possible generating vectors, and then apply Theorem 2.3 to each of the conjugacy classes of subgroups isomorphic to A_5 to check which ones are n-gonal. Using this process, we obtain 22 distinct solutions corresponding to actual signatures for n-gonal A_6 actions with a n-gonal A_5 subgroup. This is given in Table 4.

Sig(A_6)	Sig(A_5)	σ	Sig(A_6)	Sig(A_5)	σ
$(2,4,5)$	$(2^{(3)},5)$	10	$(2^{(5)})$	$(2^{(10)})$	91
$(3^{(2)},4)$	$(2,3^{(3)})$	16	$(2,3^{(3)})$	$(2^{(2)},3^{(6)})$	91
$(2,5^{(2)})$	$(2^{(2)},5^{(2)})$	19	$(2,3^{(2)},4)$	$(2^{(3)},3^{(6)})$	106
$(3^{(2)},5)$	$(3^{(3)},5)$	25	$(2,3^{(2)},5)$	$(2^{(2)},3^{(6)},5)$	115
$(3,4,5)$	$(2,3^{(3)},5)$	40	$(2^{(4)},3)$	$(2^{(8)},3^{(3)})$	121
$(2^{(3)},4)$	$(2^{(7)})$	46	$(3^{(3)},4)$	$(2,3^{(9)})$	136
$(3^{(2)},5)$	$(3^{(3)},5^{(2)})$	49	$(3^{(3)},5)$	$(3^{(9)},5)$	145
$(2^{(3)},5)$	$(2^{(6)},5)$	55	$(2^{(3)},3^{(2)})$	$(2^{(6)},3^{(6)})$	151
$(2^{(2)},3^{(2)})$	$(2^{(4)},3^{(3)})$	61	$(2^{(2)},3^{(3)})$	$(2^{(4)},3^{(9)})$	181
$(2^{(2)},3,4)$	$(2^{(5)},3^{(3)})$	76	$(2,3^{(4)})$	$(2^{(2)},3^{(12)})$	211
$(2^{(2)},3,5)$	$(2^{(4)},3^{(3)},5)$	85	$(3^{(5)})$	$(3^{(15)})$	241

TABLE 4. Signatures of n-gonal A_6 actions on surfaces of genus σ with corresponding signatures of n-gonal A_5 subgroups.

Remark 5.4. We note that in Table 4, we have only listed group signatures pairs and have not specified the number of distinct actions. In many cases, there are multiple actions up to the different types of equivalency, such as topological equivalence or simultaneous conjugation.

Next we consider n-gonal A_7 actions. Similar computations yield just 1021 possible signatures for A_7 that satisfy the strong branching cut-off. Once again, for each of these signatures, we can construct all possible generating vectors, and apply Theorem 2.3 to each of the conjugacy classes of subgroups isomorphic to A_5 to check which ones are n-gonal, and in this case, we obtain no possible solutions. In particular, there is no surface on which A_7 acts as an n-gonal group on which A_5 also acts as an n-gonal group.

Finally, since there are no solutions for A_7, and every subgroup of A_8 isomorphic to A_5 is contained in an intermediate subgroup isomorphic to A_7, there cannot be any solutions for A_8 either. Hence, the only alternating n-gonal extensions of an n-gonal group A_5 are given in Table 4.

Remark 5.5. One of the main results which allowed for complete results in determining non-normal extensions of cyclic p-gonal surfaces was the fact that when G is not the full automorphism group then G is not self-normalizing, see Corollary 3.3 of [22]. Since A_5 is maximal and non-normal in A_6, we see that this result does not extend to other groups.

REFERENCES

[1] Accola, R.D.M. *Strongly branched coverings of closed Riemann surfaces.* Proc. Amer. Math. Soc. **26** (1970), 315–322.

[2] Aschbacher M. *On Conjectures of Guralnick and Thompson.* J. of Algebra **135** (1990), no. 2, 277–343

[3] Birman, J. S. *Braids, links, and mapping class groups.* Annals of Mathematics Studies, No. 82. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1974.

[4] Bosma, W. Cannon, J. and Playoust, C., 'The Magma algebra system. I. The user language' *J. Symbolic Comput.* 24 (1997) 235–265. http://magma.maths.usyd.edu.au

[5] Breuer, T. *Characters and automorphism groups of compact Riemann surfaces.* Cambridge University Press, 2000.

[6] Broughton, S.A. *The equisymmetric stratification of the moduli space and the Krull dimension of mapping class groups.* Topology Appl. **37** (1990), no. 2, 101–113.

[7] Broughton, S.A. *Classifying finite group actions on surfaces of low genus.* J. Pure Appl. Algebra **69** (1991), no. 3, 233–270.

[8] Broughton, S.A. and Wootton, A. *Cyclic n-gonal Surfaces and their Automorphism Groups.* UNED Geometry Seminar, Disertaciones del Seminario de Matematicas Fundamentales no. 44, UNED, Madrid (2010).

[9] Broughton, S.A. and Wootton, A. *Exceptional automorphisms of (generalized) super elliptic surfaces*, Riemann and Klein Surfaces, Automorphisms, Symmetries and Moduli Spaces, Contemporary Mathematics series #629 Amer Math Soc (2014) http://dx.doi.org/10.1090/conm/629/12573

[10] Bujalance, E., Cirre, F. J. and Conder, M. *On extendability of group actions on compact Riemann surfaces.* Trans. Amer. Math. Soc. **355** (2003), no. 4, 1537–1557.

[11] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.10.0*; 2018, (https://www.gap-system.org).

[12] Guerrero, I. *Holomorphic families of compact Riemann surfaces with automorphisms.* Illinois J. Math. **26,** (1982), no. 2, 212–225.

[13] Guralnick, R.M. and Thompson, J.G. *Finite Groups of Genus Zero.* J. of Algebra **131** (1990), no. 2, 303–341

[14] Harvey, W. J. *Cyclic groups of automorphisms of a compact Riemann surface.* Quart. J. Math. Oxford Ser. (2) **17** (1966) 86–97

[15] Kontogeorgis, A. *The group of automorphisms of cyclic extensions of rational function fields.* J. Algebra **216** (1999), no. 2, 665–706.
[16] Magaard, K., Shaska, T., Shpectorov, S. and Völklein, H. *The locus of curves with prescribed automorphism group.* Communications in arithmetic fundamental groups (Kyoto, 1999/2001).
[17] Rose, J. S. *Splitting properties of group extensions.* Proc. London Math. Soc. (3) **22** (1971), 1–23.
[18] Sanjeewa, R. *Automorphism groups of cyclic curves defined over finite fields of any characteristics.* Albanian J. Math. **3** (2009), no. 4, 131–160.
[19] Shaska, T. *Determining the automorphism group of a hyperelliptic curve.* Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 248–254, ACM, New York, 2003.
[20] Singerman, D. *Subgroups of Fuchsian groups and finite permutation groups* Bull. London Math. Soc., **2** (1970), 319–323.
[21] Wootton, A. *Multiple prime covers of the Riemann sphere* Cent. Eur. J. Math. **3** (2005), no. 2, 260–272.
[22] Wootton, A. *The full automorphism group of a cyclic p-gonal surface.* J. Algebra **312** (2007), no. 1, 377–396.

Department of Mathematics, Rose-Hulman Institute of Technology, 5500 Wabash Avenue Terre Haute, IN 47803
E-mail address: brought@rose-hulman.edu

Department of Mathematics, Oregon State University, Kidder Hall 368, Corvallis, OR 97331-4605
E-mail address: camachoc@math.oregonstate.edu

Department of Mathematics, Grinnell College, 1115 8th Avenue, Grinnell, IA 50112
E-mail address: paulhus@math.grinnell.edu

Department of Mathematics, University of Michigan, 2074 East Hall 530 Church Street, Ann Arbor, MI 48109-1043
E-mail address: rebecca.winarski@gmail.com

Department of Mathematics, University of Portland, 5000 N. Willamette Blvd., Portland, OR 97203
E-mail address: wootton@up.edu

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 131–136
ISSN: 1930-1235; (**2018**)

ON THE CONNECTEDNESS OF THE BRANCH LOCUS OF THE SCHOTTKY SPACE

RUBÉN A. HIDALGO

Departamento de Matemática y Etadística,
Universidad de La Frontera,
Temuco, Chile

MILAGROS IZQUIERDO

Mathematiska Institutionen,
Linköpings Universitet,
581 83 Linköpings, Sweden

Dedicated to the memory of Kay Magaard

Abstract. Schottky space $\mathcal{S}_g$ is the space that parametrizes $\mathrm{PSL}_2(\mathbb{C})$-conjugacy classes of Schottky groups of rank $g \geq 2$. The branch locus $\mathcal{B}_g$ consists of the conjugacy classes of those Schottky groups which are a finite index proper subgroup of some Kleinian group. In a previous paper we observed that $\mathcal{B}_g$ was connected for $g \geq 3$ odd and that it has at most two components for $g \geq 4$ even. In this short note, we observe that $\mathcal{B}_g$ is always connected.

MSC 2010: Primary: 30F10, 30F40
Keywords: Schottky, branch locus

1. Introduction

A Schottky group of rank $g \geq 2$ is a purely loxodromic Kleinian group, with non-empty region of discontinuity, isomorphic to the free group of rank g. Geometrically, these groups are constructed as follows. Let C_k, C_k', $k = 1, \cdots, g$, be $2g$ Jordan curves on the Riemann sphere $\widehat{\mathbb{C}}$ such that they are mutually disjoint and bound a $2g$-connected domain $\mathcal{D}$. Suppose that for each k there exists a fractional linear

E-mail addresses: ruben.hidalgo@ufrontera.cl, milagros.izquierdo@liu.se.
Partially supported by project Fondecyt 1150003, Anillo ACT 1415 PIA-CONICYT and Redes Etapa Inicial Grant 2017-170071.

transformation $A_k \in \mathrm{PSL}_2(\mathbb{C})$ so that (i) $A_k(C_k)=C'_k$ and (ii) $A_k(\mathcal{D}) \cap \mathcal{D} = \emptyset$. Then the group Γ, generated by all these transformations, is a Schottky group of rank g. Every Schottky group is constructed in that way [1]. If Ω is the region of discontinuity of the Schottky group Γ, then Ω is connected and Ω/Γ is a closed Riemann surface of genus g (by the retrosection theorem, every closed Riemann surface of genus g is obtained in that way). Schottky groups are exactly those Kleinian groups providing the lowest regular planar coverings of closed Riemann surfaces. See [8, 9].

The *Schottky space of rank* $g \geq 2$, which we denote as $\mathcal{S}_g$, is the one that parametrizes $\mathrm{PSL}_2(\mathbb{C})$-conjugacy classes of Schottky groups of rank g. ($\mathcal{S}_g$ can be identified with the space of classes of conformally equivalent Kleinian structures on an oriented handlebody.) If Γ is a Schottky group, then we denote by $[\Gamma] \in \mathcal{S}_g$ its conjugacy class. The *branch locus* $\mathcal{B}_g \subset \mathcal{S}_g$ consists of the conjugacy classes of those Schottky groups which are a finite index proper subgroup of some Kleinian group.

A marked Schottky group of rank $g \geq 2$ is a tuple $(\Gamma, A_1, \ldots, A_g)$, where Γ is a Schottky group of rank g and $A_1, \ldots, A_g$ is a set of generators for it. Two marked Schottky groups of rank g, say $(\Gamma, A_1, \ldots, A_g)$ and $(\widehat{\Gamma}, \widehat{A}_1, \ldots, \widehat{A}_g)$, are said to be equivalent if there is a Möbius transformation B so that $BA_jB^{-1} = \widehat{A}_j$, for every $j = 1, \ldots, g$. The *marked Schottky space of rank* g, denoted by $\mathcal{MS}_g$, parametrizes equivalence classes of marked Schottky groups of rank g. This space can be identified with the quasiconformal deformation space of a Schottky group of rank g, so it carries a complex manifold of dimension $3(g-1)$ [2, 13]. (It can also be identified with the Teichmüller space of classes of marked Kleinian structures of an orientable handlebody of genus g.)

The group of holomorphic automorphisms of $\mathcal{MS}_g$ is isomorphic to the outer automorphism group $\mathrm{Out}(F_g)$, where F_g is the free group of rank g, and the *forgetful map* $\pi : \mathcal{MS}_g \to \mathcal{S}_g$ is a (regular) orbifold-covering whose deck group is $\mathrm{Out}(F_g)$ [4, 8, 9, 13]. In this setting, the branch locus $\mathcal{B}_g$ is the projection under π of the points in $\mathcal{MS}_g$ with non-trivial $\mathrm{Out}(F_g)$-stabilizer.

If (Γ, A_1, A_2) is a marked Schottky group of rank $g = 2$, then $E = A_1A_2 - A_2A_1$ is an elliptic transformation of order two such that $E_1 = EA_1$ and $E_2 = EA_2$ are also elliptic transformations of order two. In this case, the Kleinian group $K = \langle E, E_1, E_2 \rangle \cong \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$ (called a Whittaker group) contains Γ as an index two subgroup [7]. It follows that $\mathcal{B}_2$ is connected. In the paper [6] we observed that the sublocus of $\mathcal{B}_2$ consisting of the conjugacy classes of rank two Schottky groups which are finite index proper subgroups of Kleinian groups different from the Whittaker ones, has exactly two connected components. For $g \geq 3$ odd, we proved in [6] that $\mathcal{B}_g$ is connected and, for $g \geq 4$ even, that $\mathcal{B}_g$ has at most two connected components. In this short note we complete the above results as follows:

Theorem 1. *The branch locus $\mathcal{B}_g$ is connected for every $g \geq 2$.*

As observed in the previous lines, we only need to prove the connectedness of $\mathcal{B}_g$ for the case $g \geq 4$ even.

2. Proof of Theorem 1

2.1. **Cyclic extension of Schottky groups.** First of all, we will see an interpretation of $\mathcal{MS}_g$ and $\mathcal{S}_g$ in terms of quasiconformal deformation spaces: If Γ is

a Schottky group of rank $g \geq 2$, then by [2] its quasiconformal deformation space $\mathcal{Q}(\Gamma)$ turns out to be a connected complex manifold of dimension $3g-3$. As any two Schottky groups of the same rank g are quasiconformally equivalent, their respective quasiconformal deformation spaces are complex analytically equivalent. It can be seen that if Γ is a Schottky group of rank g, then $\mathcal{Q}(\Gamma)$ is isomorphic to $\mathcal{MS}_g$; that is $\mathcal{Q}(\Gamma)$ is a model of the marked Schottky space $\mathcal{MS}_g$. To obtain a model of $\mathcal{S}_g$, one has to consider the following equivalence relation on $\mathcal{Q}(\Gamma)$: two deformations ω_1 and ω_2 are equivalent if there is a Möbius transformations A so that $\omega_1\Gamma\omega_1^{-1} = A\omega_2\Gamma\omega_2^{-1}A^{-1}$. Then, the set of equivalence classes is a model for $\mathcal{S}_g$. Details can be found, for instance, in [2, 13].

Assume that there is a Kleinian group K containing Γ as a finite index normal subgroup (in particular, K is finitely generated). As each Beltrami coefficient for K is also a Beltrami differential for Γ and both K and Γ have the same limit set, there is a natural holomorphic embedding $\iota : \mathcal{Q}(K) \to \mathcal{Q}(\Gamma)$ centered at Γ. In general, if there is some $[\mu] \in \mathcal{Q}(\Gamma)$ so that the Schottky group Γ_u is contained in some Kleinian group K as a finite index normal subgroup, then it provides a holomorphic embedding $j : \mathcal{Q}(K) \to \mathcal{Q}(\Gamma)$ centered at Γ_u.

A Kleinian group K, containing a Schottky group Γ of rank $g \geq 2$ as a finite index normal subgroup so that K/Γ is a cyclic group, is called a cyclic extension Schottky group or *cyclic-Schottky group*. A geometrical picture of these Kleinian groups is provided in [5]. In the case that K/Γ is a cyclic group of rank a prime integer p, the group K is a free product, in the sense of the Klein-Maskit combination theorems, of t cyclic groups generated by loxodromic transformations, r cyclic groups generated by elliptic transformations of order p and s Abelian groups, each one generated by a loxodromic transformation and an elliptic transformation of order p both of them commuting, so that $g = 1 + p(t + r + s - 1) - r$. In particular

$$K \cong \mathbb{Z} * \overset{t}{\cdots} * \mathbb{Z} * \mathbb{Z}_p * \overset{r}{\cdots} * \mathbb{Z}_p * (\mathbb{Z} \times \mathbb{Z}_p) * \overset{s}{\cdots} * (\mathbb{Z} \times \mathbb{Z}_p). \tag{1}$$

We say that a cyclic-Schottky group K as above is of type $(g, p; t, r, s)$. In this case, the region of discontinuity Ω of K coincides with the region of discontinuity of the Schottky group Γ, and $S = \Omega/\Gamma$ is a closed Riemann surface of genus g admitting a conformal automorphism ϕ of order p with $S/\langle\phi\rangle$ of signature $(\gamma; p, \overset{2r}{\ldots}, p)$, where $\gamma = t + s$ [8, 13].

The above description permits also to see that any two cyclic-Schottky groups of the same type are quasiconformally conjugated. In particular, the quasiconformal deformation space of a cyclic-Schottky groups of a fixed type (which is connected from the measurable Riemann mapping's theorem) contains all cyclic-Schottky groups of such a type.

2.2. **A cyclic decomposition of $\mathcal{B}_g$, for $g \geq 3$.** Now, let $F(g, p; t, r, s)$ be the subset of $\mathcal{B}_g$ consisting of those points $[\Gamma] \in \mathcal{S}_g$ for which there exists some $\Gamma_0 \in [\Gamma]$ and a cyclic-Schottky group K, of type $(g, p; t, r, s)$, containing Γ_0 as an index p normal subgroup.

First of all it is easy to see that $\mathcal{B}_g$ is the union of the subsets $F(g, p; t, r, s)$, where p is prime, t, r, s are non-negative integers so that $g - 1 = p(t + r + s - 1) - r$ [6]: Let W be a Kleinian group containing a Schottky group Γ as a non-trivial finite index normal subgroup and consider the natural epimorphism $\theta : W \to W/\Gamma$. Let $\phi \in W/\Gamma$ an element of prime order p. The group $K = \theta^{-1}(\langle\phi\rangle)$ is a Kleinian group containing Γ as a normal subgroup of index p. In [6] it was observed that, for $p \geq 3$,

$F(g,p;t,r,s)$ is not necessarily connected (this it might happen since K may contain different Schottky groups of rank g). However, for $p=2$, it was proved in [3] that $F(g,2;t,r,s)$ is always connected. Moreover,it can be seen that $F(g,2;t,r,s)$ is an orbifold of complex dimension$(3g-3+r)/2$. Finally, in [6] it was proved that, for $p\geq 3$, every connected component of $F(g,p;t,r,s)$ intersects some $F(g,2;t',r',s')$ (this since the orbifold $\mathcal{O}=M/\langle\phi\rangle$, where M is the handlebody uniformized by Γ and K uniformizes $\mathcal{O}$, admits an orientation-preserving self-homeomorphism τ of order two keeping Γ).

Consequentently, to prove the connectedness of $\mathcal{B}_g$ we only need to look at the possible intersections of the connected families $F(g,2;t,r,s)$. To show that two families $F(g,2;t,r,s)$, $F(g,2;t',r',s')$ intersect, we need to construct a Kleinian group K containing two cyclic-Schottky groups K_1,K_2, of type $(g,2;t,r,s)$, $(g,2;t',r',s')$ and both of them containing the same Schottky group Γ of rank g as index two subgroup.

The following intersections were obtained in [6]:

Theorem 2 ([6])**.** *Consider connected components $F(g,2;t,r,s)$ of $\mathcal{B}_g$. Then the following hold:*

(1) *If $g\geq 3$ is odd:*
   (a) $F(g,2;t,r,s)\cap F(g,2;(g-1)/2,2,0)\neq\emptyset$, *if t is even.*
   (b) $F(g,2;t,r,s)\cap F(g,2;(g-3)/2,4,0)\neq\emptyset$, *if t is odd.*
   (c) $F(g,2;(g-1)/2,2,0)\cap F(g,2;(g-3)/2,4,0)\neq\emptyset$.

(2) *If $g\geq 4$ is even:*
   (a) $F(g,2;t,r,s)\cap F(g,2;g/2,1,0)\neq\emptyset$, *if s and t are even.*
   (b) $F(g,2;t,r,s)\cap F(g,2;(g-2)/2,3,0)\neq\emptyset$, *if s is even and t is odd.*
   (c) $F(g,2;t,r,s)\cap F(g,2;(g-2)/2,1,1)\neq\emptyset$, *if s is odd and t is even.*
   (d) $F(g,2;t,r,s)\cap F(g,2;(g-4)/2,3,1)\neq\emptyset$, *if s and t are odd.*
   (e) $F(g,2;g/2,1,0)\cap F(g,2;(g-2)/2,3,0)\neq\emptyset$.
   (f) $F(g,2;(g-2)/2,1,1)\cap F(g,2;(g-4)/2,3,1)\neq\emptyset$.

The above asserts, for $g\geq 3$ odd, that $\mathcal{B}_g$ is connected. In the case $g\geq 4$ is even, Theorem 2 permits to observe that the connectivity of $\mathcal{B}_g$ will be obtained if $F(g,2;0,g+1,0)\cap F(g,2;(g-2)/2,1,1)\neq\emptyset$.

2.3. **The connectedness of $\mathcal{B}_g$, for $g\geq 4$ even.** In order to obtain the connectedness of $\mathcal{B}_g$, for $g\geq 4$ even, we will construct two cyclic-Schottky groups K_1 and K_2, of respective types $(g,2;0,g+1,0)$ and $(g,2;(g-2)/2,1,1)$, each one containing the same Schottky group Γ as an index two normal subgroup. To do it, we consider the Kleinian group K constructed from the Klein-Maskit combination theorems [8,10,11] by using $(g-2)/2+4$ elliptic transformations of order two, say $E_1,\ldots,E_{(g-2)/2},F_1,F_2,F_3,F_4$, such that $(F_2F_1)^2=(F_3F_2)^2=(F_4F_3)^2=1$, as shown in Figure 1.

The Kleinian group K has a Cantor as a limit set, and if its (connected) region of discontinuity is Ω, then the 2-orbifold Ω/K is the Riemann sphere (genus zero) with exactly $(g-2)+5$ cone points, each one of order two. Let us consider the surjective homomorphism $\theta: K\to\langle a,b\rangle\cong\mathbb{Z}_2^2$ defined by $\theta(E_1)=\cdots=\theta(E_{(g-2)/2})=\theta(F_1)=\theta(F_4)=b$, $\theta(F_2)=a$, $\theta(F_3)=ab$.

The kernel Γ of θ is a index 4, torsion free subgroup of the Kleinian group K. The Kleinian group Γ is geometrically finite purely loxodromic Kleinian group

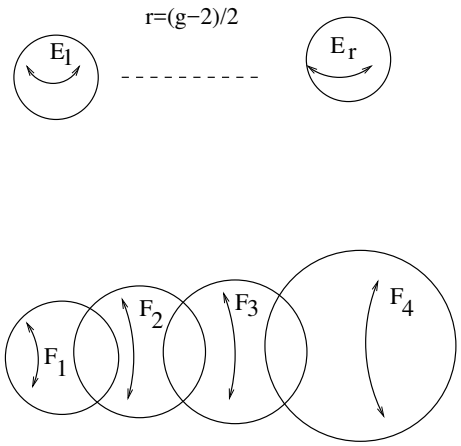

FIGURE 1. The Kleinian group K

with connected region of discontinuity. It follows from the classification of function groups [12] that Γ is necessarily a Schottky group.

Let $K_1 = \theta^{-1}(\langle a \rangle)$ and $K_2 = \theta^{-1}(\langle b \rangle)$. Both of these are index two subgroups of K and $\Gamma = K_1 \cap K_2$ has index two in each of K_1 and K_2. It can be seen that

$$K_1 = \langle F_1E_1, \ldots, F_1E_{(g-2)/2}, F_4F_3, F_2, F_3F_1 \rangle,$$
$$K_2 = \langle E_1, \ldots, E_{(g-2)/2}, F_2E_1F_2, \ldots, F_2E_{(g-2)/2}F_2, F_1, F_4, F_3F_2 \rangle.$$

The group K_1 is a cyclic-Schottky group of type $(g, 2; (g-2)/2, 1, 1)$. It induces an involution ϕ_1 in the handlebody M uniformized by Γ whose branch locus in $M/\langle \phi_1 \rangle$ consists of 1 loop and one arc of fixed points. Similarly, K_2 is a cyclic-Schottky group of type $(g, 2; 0, g+1, 0)$ inducing an involution ϕ_2 in the same handlebody M uniformized by Γ whose branch locus in $M/\langle \phi_2 \rangle$ consists of $g+1$ arcs of fixed points.

The groups K, Γ, K_1 and K_2 as above are as desired ones.

REFERENCES

[1] V. Chuckrow. On Schottky groups with applications to Kleinian groups. Annals of Math. **88**, (1968) 47-61.
[2] L. Bers. Automorphic forms for Schottky groups. *Adv. in Math.*, 16:332–361, 1975.
[3] R. Díaz, I. Garijo, G. Gromadzki and R.A. Hidalgo. Structure of Whittaker groups and application to conformal involutions on handlebodies. *Topology and its Applications* **157** (2010), 2347–2361.
[4] C. J. Earle. The group of biholomorphic self-mappings of Schottky space. *Ann. Acad. Sci. Fenn. Ser. A I Math.* **16** (1991), no. 2, 399–410.
[5] R. A. Hidalgo. Cyclic extensions of Schottky uniformizations. *Ann. Acad. Scie. Fenn.* **29** (2004), 329–344.
[6] R. A. Hidalgo and M. Izquierdo. On the connectivity of the branch locus of the Schottky space. *Annales Academiae Scientiarum Fennicae* **39** (2014), 635–654.
[7] L. Keen. On hyperelliptic Schottky groups. *Annales Academiae Scientiarum Fennicae. Series A.I. Mathematica* **5**, (1980), 165–174.
[8] B. Maskit. *Kleinian Groups*. G.M.W. **287**, Springer-Verlag, (1988).
[9] B. Maskit. Self-maps of Kleinian groups. *Amer. J. Math.* **93** (1971), 840–856.
[10] B. Maskit. On Klein's combination theorem III. *Ann. of Math. Studies* **66** (1971), Princeton Univ. Press, 297–316.

[11] B. Maskit. On Klein's combination theorem. IV. *Trans. Amer. Math. Soc.* **336** (1993), 265–294.
[12] B. Maskit. On the classification of Kleinian Groups II-Signatures. *Acta Mathematica* **138** (1977), 17–42.
[13] S. Nag. *The complex analytic theory of Teichmüller spaces.* A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York 1988.

ALBANIAN JOURNAL OF MATHEMATICS
Volume 12, Number 1, Pages 137–145
ISSN: 1930-1235; (**2018**)

THE SYLOW STRUCTURE OF TRANSITIVE PERMUTATION GROUPS ACTING WITH FIXITY 4

BARBARA BAUMEISTER, KAY MAGAARD, AND REBECCA WALDECKER

Dedicated to the memory of Kay Magaard.

Abstract. We study finite permutation groups with special properties, motivated from the theory of Riemann surfaces. In this article we focus on groups acting with fixity 4 and analyse their Sylow structure and possible orbit lengths of Sylow subgroups.

MSC 2010: 20B10, 20B25.
Keywords: Sylow structure, transitive permutation group

1. Introduction

The nature of the fixed point sets of group actions continues to play a central role in group theory. This paper continues our investigation of transitive permutation groups in which all nonidentity elements fix at most four points, with a focus on the Sylow structure of such groups. We decided to summarize basic results about orbit sizes of Sylow subgroups in this article, in particular some information for the primes 2 and 3, because this information is much more intricate and complex than it was in previous work on groups acting with fixity 2 or 3.

Building on this work, subsequent papers will give more details of the Sylow structure analysis and consequences for the group structure in general, along with a classification of finite simple groups acting with fixity 4. While our class of permutation groups is of purely group theoretic interest, our initial interest in this topic stems from the study of Weierstraß points of Riemann surfaces, and we refer the reader to [6] for more background.

Acknowledgments. The project on permutation groups with low fixity started with support by the DFG. It was initiated by Kay Magaard and most of the work in this paper has been completed during his visits at the Martin-Luther-Universität Halle-Wittenberg in 2016 and 2017. Work on the project has continued after his passing in July 2018 and will continue until his initial goal has been reached.

2. Notation and examples

Let $k \in \mathbb{N}_0$ and suppose that the group G acts on the finite set Ω. We say that G has fixity k on Ω if and only if there is some element of G that fixes exactly k distinct points on Ω and if no element of G fixes more than k distinct points.

Hypothesis 1. *Suppose that (G, Ω) is such that G acts faithfully and transitively on Ω and that G has fixity 4 in this action.*

We begin with natural and well-known examples.

Example 1 (Classical examples)**.** *Suppose that the group G acts sharply 5-transitively on a set Ω of size at least 6. Then for all pair-wise distinct elements $\omega_1, \omega_2, \omega_3, \omega_4 \in \Omega$, we find α, β in $\Omega \setminus \{\omega_1, \omega_2, \omega_3, \omega_4\}$ that are distinct, and then the 5-transitivity gives an element $g \in G$ such that $\omega_1, \omega_2, \omega_3, \omega_4$ are fixed and α is mapped to β. In particular every four point stabilizer is non-trivial, but every five point stabilizer is trivial because of the sharp 5-transitivity. Therefore (G, Ω) satisfies Hypothesis 1.*

Now Jordan's result (see for example p. 327 in [5]) this gives the well-known examples $\mathcal{S}_5$, $\mathcal{S}_6$, $\mathcal{A}_7$, M_{12}, in their natural action. The transitive subgroup $M_{11} \leq M_{12}$ also gives rise to an example, with point stabilizers of order $2^2 \cdot 3 \cdot 5 \cdot 11$.

Calculations in GAP ([8]) show that the groups $\mathcal{S}_5$, $\mathcal{A}_6$ and $\mathcal{S}_6$ also give rise to several (very small) examples, respectively.

Example 2 (Frobenius group extensions)**.** *Suppose that F is a Frobenius group with Frobenius kernel K and complement H and suppose that G is a group with a subgroup U of order 4 such that $G = F \rtimes U$.*

Consider the action of G on G/H by right multiplication. As all conjugates of H are contained in F, it follows that $|N_G(H)| = 4 \cdot |H|$. If $g \in G$ is such that $g \in N_G(H) \setminus H$, then all elements of H fix the coset Hg. This gives four fixed points on the set G/H, and it follows that $(G, G/H)$ satisfies Hypothesis 1 in the special case where all elements have 0 or 4 fixed points.

A similar construction works based on pairs (G, Ω) that satisfy the main hypothesis of [6].

Example 3. *Suppose that G is a finite group, that $U \leq G$ has order 2 and that $H, M \leq G$ are such that the following hold: $H \leq M$, $G = M \rtimes U$ and with respect to the action by right multiplication, the group M has fixity 2 on M/H. In particular $|N_M(H) : H| = 2$. As M has index 2 in G, all conjugates of H in G are contained in M and $|N_G(H) : H| = 4$. It follows that $(G, G/H)$ satisfies Hypothesis 1 with the action of G on G/H by right multiplication.*

3. General properties

By "group" we always mean a finite group, and by "permutation group" we always mean a group that acts faithfully. Throughout this paper Ω denotes a finite set and G denotes a permutation group on Ω. We also use the notion of fixity introduced in the previous section.

Let $\omega \in \Omega$ and $g \in G$, and moreover let $\Lambda \subseteq \Omega$ and $H \leq G$. Then $H_\omega := \{h \in H \mid \omega^h = \omega\}$ denotes the **stabilizer of ω in H**,

$$\mathrm{fix}_\Lambda(H) := \{\omega \in \Lambda \mid \omega^h = \omega\}$$

for all $h \in H\}$ denotes the **fixed point set of H in Λ** and we write $\mathrm{fix}_\Lambda(g)$ instead of $\mathrm{fix}_\Lambda(\langle g\rangle)$. We write ω^H for the H-orbit in Ω that contains ω.

Whenever $n, m \in \mathbb{N}$ and p is a prime number, then we denote by (n, m) the largest natural common divisor of n and m and by n_p the largest power of p dividing n.

Finally, a subgroup H of G is said to be a **TI-subgroup** if and only if for all $g \in G$, we have that $H^g \cap H = 1$ or $H^g = H$.

We begin with general local properties that follow from our main hypothesis. We will notice that the primes 2 and 3 behave differently from the larger primes in $\pi(G)$, motivating the extensive analysis that we begin to describe in this article.

Lemma 4. *Suppose that Hypothesis 1 holds and let $\alpha \in \Omega$. If $p \in \pi(G_\alpha)$ and $p \geq 5$, then G_α contains a Sylow p-subgroup of G.*

If moreover some non-trivial p-element fixes four points, then the corresponding four point stabilizer contains a Sylow p-subgroup of G.

Proof. Let $Q \in \mathrm{Syl}_p(G_\alpha)$ and let $Q \leq P \in \mathrm{Syl}_p(G)$. Then $Z(P)$ centralises Q and therefore stabilizes the set $\mathrm{fix}_\Omega(Q)$ of size at most 4, by hypothesis. In particular $Z(P)$ induces a subgroup of $\mathcal{S}_4$ on this set, but it has order divisible by $p \geq 5$. This implies that $Z(P)$ fixes every element of $\mathrm{fix}_\Omega(Q)$, in particular $Z(P) \leq G_\alpha$. With the same argument P fixes every fixed point of $Z(P)$, including α, and therefore $P \leq G_\alpha$.

Now let $1 \neq x \in P$ be such that x fixes four points. Let $\Delta := \mathrm{fix}_\Omega(x)$. Then we argue as above: First $Z(P)$ centralizes x and hence fixes Δ point-wise, and then P also stabilizes Δ point-wise. □

From this we obtain initial information about $F^*(G)$:

Corollary 5. *Suppose that Hypothesis 1 holds, let $\alpha \in \Omega$ and let $p \in \pi(G)$. If $P \in Syl_p(G)$ and $P \leq G_\alpha$, then $O_p(G) = 1$. In particular, if $p > 3$ and $p \in \pi(G_\alpha)$, then $O_p(G) = 1$.*

Proof. The first statement follows from the fact that G acts faithfully and transitively on Ω. Then the second claim follows form the first, together with Lemma 4. □

Lemma 6. *Suppose that Hypothesis 1 holds. Let $\alpha \in \Omega$ and suppose that $H \leq G_\alpha$ is a non-trivial 4-point stabilizer.*

(a) H is a TI-subgroup.
(b) If 3 divides $\pi(H)$, then H contains a Sylow 3-subgroup of G or $N_G(H)$ has a subgroup that induces A_4 on $fix_\Omega(H)$.
(c) If $N_G(H)$ is not transitive on $fix_\Omega(H)$, then $N_G(H)/H$ is elementary abelian of order 4 and $N_{G_\alpha}(H)/H$ of order 2.
(d) If $1 \neq X \leq G_\alpha$ is a subgroup that fixes exactly one or two points, then $|N_G(X) : N_{G_\alpha}(X)| \in \{1, 2\}$. If X fixes exactly four points, then $N_G(X) \leq N_G(H)$ and $|N_G(H) : N_{G_\alpha}(H)| \in \{2, 4\}$. In particular, if $3 \in \pi(N_G(X))$ in this case, then $3 \in \pi(G_\alpha)$.

Proof. Set $\Delta := \mathrm{fix}_\Omega(H)$ and let $g \in G$. Then $H \cap H^g$ fixes Δ and Δ^g point-wise, so $\mathrm{fix}_\Omega(H \cap H^g)$ contains Δ and Δ^g. If $H \cap H^g \neq 1$, then Hypothesis 1 forces $|\Delta \cup \Delta^g| \leq 4$ and therefore $\Delta = \Delta^g$ and $H = H^g$. This is (a).

The hypothesis in (b) implies that some nontrivial 3-element fixes four points, hence $|\Omega| \equiv 1 \mod 3$. Therefore G_α contains a Sylow 3-subgroup of G. Suppose

that H does not contain a Sylow 3-subgroup of G. Then there exists a 3-element in G_α that induces a 3-cycle on Δ. Such an element stabilizes the set Δ and therefore normalizes H. We conclude that 3 divides $|N_{G_\alpha}(H)/H|$. If $\beta \in \Delta$ and $\beta \neq \alpha$, then $H \leq G_\beta$ and we can argue in the same way to see that 3 divides $|N_{G_\beta}(H)/H|$. In particular we find two elements that induce distinct 3-cycles on Δ, hence there is a subgroup of $N_G(H)$ that induces $\mathcal{A}_4$ on Δ. Thus (b) holds.

For (c) we suppose that $N_G(H)$ is not transitive on Δ, which means that $|N_G(H) : N_{G_\alpha}(H)| \in \{1, 2, 3\}$.

We show that H is a 2-group. As a first step we prove

$(*)$ For all $r \in \pi(G)$, H does not contain a Sylow r-subgroup of G_α.

Assume otherwise and let $r \in \pi(G)$, $R \in \mathrm{Syl}_r(G_\alpha)$ and $R \leq H$. Let $\beta \in \Delta$ be such that $\beta \neq \alpha$. In particular $R \leq H \leq G_\beta$ and then $R \in \mathrm{Syl}_r(G_\beta)$. As G is transitive on Ω, there is some $g \in G$ such that $\alpha^g = \beta$, and then R and R^g are Sylow r-subgroups of G_β. By Sylow's Theorem let $x \in G_\beta$ be such that $R^{gx} = R$. Then gx normalizes R and hence stabilizes the set $\mathrm{fix}_\Omega(R) = \Delta$, in particular $gx \in N_G(H)$. As $\alpha^{gx} = \beta$, we now have the contradiction that $N_G(H)$ acts transitively on Δ. This proves $(*)$.

If $p \in \pi(H)$ and $p \geq 5$, then Lemma 4 yields that H contains a Sylow p-subgroup P of G, contrary to $(*)$.

If $3 \in \pi(H)$, then we recall that H des not contain a Sylow 3-subgroup of G_α (by $(*)$ and therefore a subgroup of $N_G(H)$ induces $\mathcal{A}_4$ on Δ by (b). But this contradicts our hypothesis that $N_G(H)$ is not transitive on Δ.

We conclude that H is a 2-group.

Now $(*)$ implies that H is not a Sylow 2-subgroup of G_α. Let $H \leq S \in \mathrm{Syl}_2(G_\alpha)$ and $T := N_S(H)$. Then $H < T$ and therefore some $t \in T$ induces a transposition on Δ. It follows for all $\delta \in \Delta$ that some element of $N_{G_\delta}(H)$ induces a transposition on Δ. Together with the fact that $N_G(H)/H$ is isomorphic to a non-transitive subgroup of $\mathcal{S}_4$, by hypothesis, we deduce that (c) holds.

For (d) we let $\Lambda := \mathrm{fix}_\Omega(X)$. If $|\Lambda| \leq 2$, then the first assertion of (d) holds.

Now suppose that $|\Lambda| = 4$ and let M denote the point-wise stabilizer of Λ. As $N_G(X)$ stabilizes Λ, it normalizes M. If 3 is not in $\pi(N_G(M)/M))$, then (d) follows. So we suppose that $3 \in \pi(N_G(H)/H)$. Then $N_G(M)$ does not induce a 2-group on Γ and therefore $N_G(M)$ is transitive on Γ by (c), which shows the second assertion of (d).

Now suppose that $3 \in \pi(N_G(X))$. Then $3 \in \pi(N_G(M))$ and $3 \in \pi(M)$ or $3 \in \pi(N_G(M)/M))$ and $N_G(M)$ is transitive on Γ by the last paragraph. This shows the last assertion of (d).

□

Corollary 7. *Suppose that Hypothesis 1 holds. Then* $|Z(G)| \in \{1, 2, 4\}$.

Proof. Let $\alpha \in \Omega$. As G acts faithfully on Ω, we know that $Z := Z(G)$ intersects G_α trivially. Let $x \in G_\alpha$ be an element with exactly four fixed points. Then $Z \leq C_G(x)$ and hence Lemma 6 (d) implies our assertion. □

Lemma 8. *Suppose that Hypothesis 1 holds and let* $\alpha \in \Omega$. *Then the following hold:*

(a) If there is a 2-element in G_α *that has exactly one or three fixed points on* Ω, *then* G_α *contains a Sylow 2-subgroup of* G.

(b) If there is a 3-element in G_α that has exactly one, two or four fixed points, then G_α contains a Sylow 3-subgroup of G.

Proof. For (a) we suppose that $x \in G_\alpha$ is a 2-element with exactly one or three fixed points. As x has orbits of 2-power lengths on the set of points that are not fixed, it follows that Ω is odd. Therefore $|G : G_\alpha|$ is odd and consequently G_α contains a Sylow 2-subgroup of G.

Next suppose that $y \in G_\alpha$ is a 3-element with exactly one, two or four fixed points on Ω. We note that this implies that $|\Omega| \equiv 1$ or 2 mod 3 and hence G_α contains a Sylow 3-subgroup of G. This is (b). □

4. Orbit lengths for Sylow subgroups

We prove two basic lemmas that allow us to determine the possible orbit sizes for Sylow subgroups. After that we analyze the situation for the prime 2 in more detail.

Lemma 9. *Suppose that Hypothesis 1 holds. Let $S \in Syl_2(G)$ and $\alpha \in \Omega$. Then one of the following holds:*

(a) $S_\alpha = 1$.
(b) $|S_\alpha| = 2$ and S is dihedral or semidihedral.
(c) $1 \neq |S_\alpha| \leq 8$, $|\alpha^S| \geq 8$ and there exists some subgroup $T \leq S_\alpha$ of index at most 2 such that all $t \in T^\#$ fix exactly four points.
Moreover S_α is isomorphic to a subgroup of D_8.
(d) $|S : S_\alpha| \in \{2, 4\}$.
(e) $S \leq G_\alpha$.

Proof. We suppose that neither (a) nor (e) holds. Then $1 \neq S_\alpha \neq S$ and therefore the orbit $\Delta := \alpha^S$ is nonregular of length at least 2. If $|\Delta| \leq 4$, then (d) holds because $|\Delta| = |S : S_\alpha|$. So now we suppose that (d) does not hold.

Then $|\Delta| \geq 8$ and we consider (S, Δ). If this pair does not satisfy Hypothesis 1, then it satisfies Hypothesis 1.1 from [6]. Then it follows from Lemma 2.12 in this article that S is dihedral or semidihedral, which means that (b) holds.

So now we suppose that (S, Δ) satisfies Hypothesis 1 and we let $t \in S^\#$ be such that t fixes exactly four points on Δ. Without loss $\alpha \in \mathrm{fix}_\Delta(t)$. Next we let T denote the point-wise stabilizer of $\mathrm{fix}_\Delta(t)$ in S. Then $T \leq S_\alpha$ and, since T fixes four points, all other orbits of T on Δ are regular by Hypothesis 1.

We let $a \in \mathbb{N}_0$ be such that $|\Delta| = 4 \cdot a + |T|$. As $|\Delta|$ is a power of 2, at least 8, it follows that $|\Delta|$ is divisible by 8 and hence $a \cdot |T|$ is divisible by 4, but not by 8. This forces $|T| \leq 4$. Moreover $T \leq S_\alpha \neq S$ and hence $T < N_S(T)$. The factor group $N_S(T)/T$ is isomorphic to a 2-subgroup of $\mathcal{S}_4$ (i.e. a subgroup of D_8), and $|S_\alpha : T| \leq 2$. In particular $|S_\alpha| \leq 2 \cdot |T| \leq 8$, as in (c), and it only remains to prove that S_α is isomorphic to a subgroup of D_8.

This is clear if $|S_\alpha| \leq 4$. Otherwise $|S_\alpha| = 8$ and $|T| = 4$. If we recall the equation $|\Delta| = 4 \cdot a + |T|$ from above, then we obtain that a is odd. Let $s \in S_\alpha \setminus T$. Then s stabilizes at least one of the regular T-orbits on Δ, and on such an orbit it fixes at most two points. As every element of $T^\#$ acts as a 4-cycle or a double transposition on each regular T-orbit, it follows that $S_\alpha = \langle s, T \rangle \simeq D_8$. □

Lemma 10. *Suppose that Hypothesis 1 holds and let $P \in Syl_3(G)$. Let Δ be the union of all P-orbits of Ω of size at most 3. Then one of the following holds:*

(a) *All P-orbits are regular and the point stabilizers in G are $3'$-groups.*
(b) $|\Delta| > 4$ *and* $|P| \leq 9$.
(c) $|\Delta| \leq 4$ *and P is of maximal class. There exists some nonregular P-orbit on $\Omega \setminus \Delta$ and for every such orbit Λ and all $\lambda \in \Lambda$ it is true that $|P_\lambda| = 3$ and that P_λ fixes exactly three points on Λ.*
(d) Δ *is the unique P-orbit of length 3 and all orbits of P on $\Omega \setminus \Delta$ are regular.*
(e) $1 \leq |\Delta| \leq 4$, *there is some $\delta \in \Delta$ such that $P \leq G_\delta$, and all P-orbits on $\Omega \setminus \Delta$ are regular.*

In (c), (d) and (e) we see that P possesses an orbit of length at least 9 and therefore $|P| \geq 9$.

Proof. Suppose that $|\Delta| > 4$. As P is a 3-group, all P-orbits contained in Δ are of length 1 or 3. If $\Sigma_1, \Sigma_2 \subseteq \Delta$ are distinct P-orbits of length 3, then $|\Sigma_1 \cup \Sigma_2| = 6$ and therefore Hypothesis 1 implies that P acts faithfully on $\Sigma_1 \cup \Sigma_2$. In particular P is isomorphic to a subgroup of a Sylow 3-subgroup of $\mathcal{S}_6$ and hence $|P| \leq 9$. This is (b).

If there is a unique P-orbit $\Sigma_1 \subseteq \Sigma$ of length 3, then the other P-orbits contained in Δ have length one. Consequently the kernel P_0 of the action of P on Σ_1 fixes Δ point-wise. As $|\Delta| > 4$, it follows from Hypothesis 1 that P acts faithfully on Σ_1 and therefore $|P| \leq 3$. Again this is included in (b).

Now we suppose that neither (a) nor (b) holds, and from the previous paragraphs we know that this implies that $0 \leq |\Delta| \leq 4$.

Suppose further that P acts semiregularly on $\Omega \setminus \Delta$. In particular (c) does not hold. Assume that $|\Delta| = 0$, i.e. $\Delta = \varnothing$. Then all P-orbits are regular, which implies (a) and hence a contradiction. So we know that $|\Delta| \geq 1$ and we prove that (d) or (e) holds:

If P is contained in a point stabilizer, then the size of Δ can be anything between 1 and 4 because P can fix up to four points or P has one fixed point and one orbit of length 3. These cases are covered by (e).

Otherwise all P-orbits have length at least 3. Together with our restriction $0 \leq |\Delta| \leq 4$ this implies (d).

If none of (a),(b),(d) or (e) holds, then the previous arguments show that $0 \leq |\Delta| \leq 4$ and that P has a nonregular orbit on $\Omega \setminus \Delta$. Let Λ denote such a nonregular orbit. Then Λ has size at least 9 by definition of Δ.

Let $\lambda \in \Lambda$ and let $n \in \mathbb{N}$ be such that $|\Lambda| = 3^n$. Then $n \geq 2$ and by our main hypothesis P_λ fixes at most four points in total. So it follows that P_λ fixes exactly three points on Λ and acts semi-regularly on the set of remaining points. Let $m \in \mathbb{N}$ be such that $|P_\lambda| = 3^m$ and let $a \in \mathbb{N}$ be such that $|\Lambda| = 3 + a \cdot |P_\lambda|$. Then $3^n = |\Lambda| = 3 + a \cdot |P_\lambda| = 3 + a \cdot 3^m$, so this forces $m = 1$. We deduce that $|P_\lambda| = 3$ and now Lemma 6 implies that $|N_P(P_\lambda)| \leq 9$.

This means that P has maximal class and that P_λ fixes exactly three points in Λ, as stated in (c).

Finally we argue why the concluding remark is true. In (c), with the notation introduced there, we see that $|P_\lambda| = 3$ and $|\Lambda| \geq 3$, because P_λ fixes three points on Λ. This means that $|P| = |P : P_\lambda| \cdot |P_\lambda| \geq 3 \cdot 3 = 9$.

In (d) the regular orbits of P have size at least 3 because Δ is the unique orbit of size 3. As $|\Omega| > 3$, there must be a regular P-orbit and hence $|P| \geq 9$ again.

In (e) we see that $|\Delta| \leq 4$ and $|\Omega| \geq 6$, therefore $\Omega \setminus \Delta \neq \varnothing$ and regular orbits have size strictly greater than 3. Consequently $|P| \geq 9$. □

Lemma 11. *Suppose that Hypothesis 1 holds, let $p \in \pi(G)$ and let $P \in Syl_p(G)$. Then the following hold:*

(a) *If $p = 2$, then the possible orbit sizes for P on Ω are 1, 2, 4, 8, $\frac{|P|}{8}$, $\frac{|P|}{4}$, $\frac{|P|}{2}$ and $|P|$.*
(b) *If $p = 3$, then the possible orbit sizes for P on Ω are 1, 3, $\frac{|P|}{3}$ and $|P|$.*
(c) *If $p \geq 5$, then the possible orbit sizes for P on Ω are 1 and $|P|$.*

Proof. (a) follows from Lemma 9 by inspecting the cases.

For (b) we look at Lemma 10: In addition to orbits of size $|P|$ and 1 we see in (d) that orbit size 3 is possible, and the only case where another orbit size occurs is (c), with orbits of length $|P|/3$.

Finally, if $p \geq 5$, then we turn to Lemma 4. If P does not fix any point, then the lemma forces the point stabilizer orders to be coprime to p. This means that all P-orbits are regular. □

We remark that the group M_{12} in its natural action on 12 points provides an example for Case (b) where a 3-Sylow subgroup has one orbit of length 3 and another nonregular orbit.

For more details about the 2-structure we set up additional notation.

Hypothesis 2. *Suppose that Hypothesis 1 holds and let $S \in Syl_2(G)$. Let f denote the maximal number of points of Ω that are fixed by some involution in G, let Δ denote the union of S-orbits on Ω of length at most 4 and let*

$$F := \langle x^g \mid x, g \in G, o(x) = 2, |\, fix_\Omega(x)| = f \rangle.$$

We note that Hypothesis 2 allows for the special cases that $S = 1$ or $f = 0$.

Lemma 12. *Suppose that Hypothesis 2 holds and that the point stabilizers in G have even order. Then one of the following is true:*

(a) $|\Delta| \leq 4$, S acts semi-regularly on $\Omega \setminus \Delta$ and the stabilizer of the set Δ is strongly embedded in F.
(b) $|\Delta| > 4$ and S acts semi-regularly on $\Omega \setminus \Delta$. Moreover there exists a subset $\Delta_1 \subset$ of Δ that is S-invariant and such that $4 < |\Delta_1| \leq 8$.
(c) S does not act semi-regularly on $\Omega \setminus \Delta$ and there exists an S-orbit Λ in $\Omega \setminus \Delta$ such that $max_{s \in S^\#}\{|fix_\Lambda(s)|\} \in \{2, 4\}$.

Proof. Since G acts transitively on Ω and the maximum number of fixed points of an involution of G is 4, we see that the hypothesis of the main theorem and Proposition 3.1 of [7] are satisfied. Applied to $f = 4$, this gives exactly the statements in the three cases; it is worth mentioning that the value of k in Ronse's proposition 3.1 (ii) can only be 2 in our situation. □

Keeping the notation from Hypothesis 2 Ronse (see [7], main theorem) proves a more general result:

Theorem 13. *If G has even order and acts transitively on a set Ω such that $f \leq 4$, then one of the following holds:*

(a) The set stabilizer of Δ in F is strongly embedded in F, or
(b) $f \leq 3$ and the Sylow 2-subgroups are dihedral or semidihedral, or
(c) $f = 4$ and the Sylow 2-subgroups of G have sectional rank bounded by 4.

For later applications we need a version for simple groups.

Theorem 14. *Suppose that Hypothesis 2 holds and that G is nonabelian simple. Then one of the following is true:*

(a) The point stabilizers in G have odd order.
(b) G has a strongly embedded subgroup and is therefore isomorphic to $PSL_2(q)$, $Sz(q)$ or $PSU_3(q)$ for s suitable power q of the prime 2, where $q \geq 4$.
(c) $f \leq 3$ and G is isomorphic to $\mathcal{A}_7$, to M_{11} or to $PSL_2(q)$ for some prime power q or to $PSL_3(q)$ or $PSU_3(q)$ for some odd number q that is a prime power.
(d) $f = 4$ and G has sectional 2-rank at most 4.

Proof. Suppose that the point stabilizers have even order. Then Theorem 13 applies and $F = G$ because G is simple. So in Case (a) of the theorem, we see that G has a strongly embedded subgroup and Bender's classification gives our statement in (b). (See [2].) Case (b) of the theorem leads to dihedral or semidihedral Sylow 2-subgroups and hence to the classification results by [4] and [1], giving our list of groups in (c). Finally Case (c) in Theorem 13 directly gives our claim (d). □

If the point stabilizers have odd order, then it becomes important whether or not 3 divides their order. This connection between the primes 2 and 3 will be discussed in subsequent work. In Case (d) above, the group G is known by work of Gorenstein and Harada (see [3]).

5. Final comments

As we have discussed in the introduction, analyzing the Sylow structure of groups satisfying Hypothesis 1 is crucial when it comes to classifying these groups.

Corollary 5 shows where the differences between the primes 2 and 3 an larger primes come into play, and with its help we can prove the following:

If Hypothesis 1 holds and $\omega \in \Omega$, then all Sylow subgroups of G_ω have rank 1 or

$$F^*(G) = O_2(G)O_3(G)E(G).$$

This leads to a natural case distinction not only for primes that divide the order of point stabilizers, but also for the rank of their Sylow subgroups. Following this case distinction we will classify all finite simple groups (and some extensions) satisfying Hypothesis 1, and we are also working on general structure results.

References

[1] Alperin, J.L., Brauer, R. and Gorenstein, D.: Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups, *Transactions of the American Mathematical Society* **151** (1970), 1-261.
[2] Bender, H.: Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt, *J. Algebra* **17** (1971), 527–554 .
[3] Gorenstein, D. and Harada, K.: *Finite groups of sectional 2-rank at most 4.* Finite groups '72 (Proc. Gainesville Conf., Univ. Florida, Gainesville, Fla., 1972), pp. 57-67. North-Holland Math. Studies, Vol. 7, North-Holland, Amsterdam, 1973.
[4] Gorenstein, D. and Walter, J.H.: The Characterization of Finite Groups with Dihedral Sylow 2-Subgroups. *J. Algebra* **2** (1965), 85–151.
[5] Huppert, B. and Blackburn, N.: *Finite Groups III.* Grundlehren der mathematischen Wissenschaften, Band 243. Springer, 1982.

[6] Magaard, K. and Waldecker, R.: Transitive permutation groups where nontrivial elements have at most two fixed points, *Journal of Pure and Applied Algebra* **219**, Issue 4 (2015), 729–759.
[7] Ronse, C.: On finite permutation groups in which involutions fix at most 15 points, *Arch. Math. (Basel)* **39** (1982), no. 4, 784–788.
[8] Schönert, M. et.al. GAP – Groups, Algorithms, and Programming – version 3, release 4, patchlevel 4. Lehrstuhl D für Mathematik, RWTH Aachen, Germany, 1997.

Fakultät für Mathematik,, Universität Bielefeld, Postfach 10 01 31,, 33501 Bielefeld, Germany.
E-mail address: B.Baumeister@math.uni-bielefeld.de

Institut für Mathematik, MLU Halle-Wittenberg, Theodor-Lieser-Strasse 5, 06120 Halle, Germany.
E-mail address: rebecca.waldecker@mathematik.uni-halle.de

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.