Contemporary Mathematics

Self-inversive polynomials, curves, and codes

D. Joyner and T. Shaska

Abstract. We study connections between self-inversive and self-reciprocal polynomials, reduction theory of binary forms, minimal models of curves, and formally self-dual codes. We prove that if $\mathcal{X}$ is a superelliptic curve defined over $\mathbb{C}$ and its reduced automorphism group is nontrivial or not isomorphic to a cyclic group, then we can write its equation as $y^n = f(x)$ or $y^n = xf(x)$, where $f(x)$ is a self-inversive or self-reciprocal polynomial. Moreover, we state a conjecture on the coefficients of the zeta polynomial of extremal formally self-dual codes.

1. Introduction

Self-inversive and self-reciprocal polynomials have been studied extensively in the last few decades due to their connections to complex functions and number theory. In this paper we explore the connections between such polynomials to algebraic curves, reduction theory of binary forms, and coding theory. While connections to coding theory have been explored by many authors before we are not aware of any previous work that explores the connections of self-inversive and self-reciprocal polynomials to superelliptic curves and reduction theory.

In Section 2, we give a geometric introduction to inversive and reciprocal polynomials of a given polynomial. We motivate such definitions via the transformations of the complex plane which is the original motivation to study such polynomials. It is unclear who coined the names inversive, reciprocal, palindromic, and antipalindromic, but it is obvious that inversive come from the inversion $z \mapsto \frac{1}{\bar{z}}$ and reciprocal from the reciprocal map $z \mapsto \frac{1}{z}$ of the complex plane.

We take the point of view of the reduction theory of binary forms. While this is an elegant and beautiful theory for binary quadratics, it is rather technical for higher degree forms. However, the inversion plays an important role on reduction as can be seen from section 2 and from [5] and [2]. We are not aware of other authors have explored the connection between reduction theory and self-inversive and self-reciprocal polynomials before even though the overlap is quite obvious.

We state some of the main results of self-inversive polynomials including the *middle coefficient conjecture* (2.3) and results on the location of the roots of such polynomials. Self-inversive polynomials over $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are discussed and a few recent results on the height of such polynomials. The normal references here are

2000 *Mathematics Subject Classification.* Primary 14Hxx; 11Gxx.

[7, 13, 16–20, 22, 25]. Further, we discuss the roots of the self-inversive polynomials. There is a huge amount of literature on this topic including several conjectures. It is the location of such roots that makes self-inversive polynomials interesting in reduction theory, coding theory, and other areas of mathematics. An attempt at a converse to this conjecture is discussed in §2.2.

In Section 3 it is given an account of how self-inversive polynomials can be used to determine minimal polynomials of superelliptic curves with extra automorphisms. This is a new idea spurred by Beshaj's thesis [2] and [1] and has some interesting relations between two different areas of mathematics, namely the theory of algebraic curves and the theory of self-inversive polynomials. Further details in this direction are planned in [5]. In this section we prove that for any superelliptic curve with reduced automorphism group not trivial and not isomorphic to a cyclic group we can write the equation of the curve as $y^n = f(x)$ or $y^n = xf(x)$, where $f(x)$ is a palindromic, antipalindromic, or self-inversive polynomial. Indeed, we can say more since in each case when the automorphism group of the curve we can determine the polynomial $f(x)$ specifically.

In Section 4 we explore connections of self-inversive and self-reciprocal polynomials to reduction theory of binary forms. We show that self-inversive polynomials which have all roots on the unit circle correspond to the totally real forms. The reduction theory for such forms is simpler than for other forms since the Julia quadratic of any degree n form $f(x, y)$ is a factor of a degree $(n-1)(n-2)$ covariant $G_f(x, y)$ given in terms of the partial derivatives of f; see [1]. We prove that for f palindromic, G_f is self-inversive and if f is palindromic of odd degree then G_f is palindromic. Moreover, we determine explicitly which self-inversive polynomials f with all roots on the unit circle are reduced.

In Section 5 we discuss the Riemann hypothesis for formal weight enumerators of codes and its relation to the self-inversive polynomials. We state several open problems which relate to Riemann hypotheses for extremal formal weight enumerators of codes.

Most of the results obtained here, with the necessary adjustments, can be extended to curves defined over fields of positive characteristic. In [21] equations of superelliptic curves are also determined over such fields. The main question that comes from the connection between self-inversive and self-reciprocal polynomials and reduction theory is whether such polynomials are actually reduced. In other words, if $f(x, y)$ is a primitive form which is self-reciprocal or self-inversive, is it true that $f(x, y)$ is reduced? This question is addressed in [5].

Acknowledgments: We would like to thank Lubjana Beshaj for helpful conversations and explaining to us the reduction theory of self-inversive and self-reciprocal forms.

2. Self-inversive polynomials

Let $\mathbb{P}^1$ be the Riemann sphere and $\mathrm{GL}_2(\mathbb{C})$ the group of 2×2 matrices with entries in $\mathbb{C}$. Then $\mathrm{GL}_2(\mathbb{C})$ acts on $\mathbb{P}^1$ by linear fractional transformations. This action is a transitive action, i.e. has only one orbit. Consider now the action of $\mathrm{SL}_2(\mathbb{R})$ on the Riemann sphere. This action is not transitive, because for $M =$

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ we have

$$\text{Img } (Mz) = \frac{(\alpha\delta - \beta\gamma)}{|\gamma z + \delta|^2} \text{Img } z.$$

Hence, z and Mz have the same sign of imaginary part when $\det(M) = 1$. 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. Let $\mathcal{H}_2$ be the complex upper half plane, i.e.

$$\mathcal{H}_2 = \left\{ z = x + iy \in \mathbb{C} \;\middle|\; \text{Img } (z) > 0 \right\} \subset \mathbb{C}.$$

The group $\mathrm{SL}_2(\mathbb{R})$ preserves $\mathcal{H}_2$ and acts transitively on it, since for $g \in \mathrm{SL}_2(\mathbb{R})$ and $z \in \mathcal{H}_2$ we have

$$\text{Img } (gz) = \frac{\text{Img } z}{|\gamma z + \delta|^2} > 0$$

The modular group $\Gamma = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ also acts on $\mathcal{H}_2$. This action has a fundamental domain $\mathcal{F}$

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

Consider now all binary quadratic forms with real coefficients. A quadratic form $f \in \mathbb{R}[x, y]$ has two complex roots (conjugate of each other) if f is positive definite. Hence, we have a one to one correspondence between positive definite quadratic forms and points of $\mathcal{H}_2$. For a given $f \in \mathbb{R}[x, y]$, let $\xi(f)$ denote the zero of f in $\mathcal{H}_2$. This is called *zero map*. The positive definite binary form f has minimal coefficients if and only if $\xi(f) \in \mathcal{F}$; see [1] for details.

The group $SL_2(\mathbb{R})$ acts on the set of positive definite quadratic forms by linear changes of coordinates. Moreover, the zero map $f \mapsto \xi(f)$ is equivariant under this action. In other words, $\xi(f^M) = \xi(f)^M$, for any $M \in \mathrm{SL}_2(\mathbb{R})$. Hence, to *reduce* a binary quadratic f with integer coefficients we simply compute $\xi(f)$ and then determine $M \in \Gamma$ such that $\xi(f)^M \in \mathcal{F}$. Then, the quadratic f^M has minimal coefficients.

This approach can be generalized to higher degree forms $f \in \mathbb{R}[x, y]$. Then $f(x, y)$ is a product of linear and quadratic factors over $\mathbb{R}$. In studying roots of $f(x, y)$ we are simply concerned with roots in the upper half plane $\mathcal{H}_2$. The zero map can also be defined in this case, but its definition is much more technical. The interested reader can check [1] or [2] for details.

Hence the problem of finding a form equivalent to f with minimal coefficients becomes equivalent to determine a matrix $M \in \Gamma$ such that $\xi(f)^M \in \mathcal{F}$. The generators of the modular group Γ are the matrices

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

which correspond to transformations $z \to -\frac{1}{z}$ and $z \to z + 1$. Next, we will see the geometry of some of these transformations which play an important role in this process.

Let $\sigma(z) = \frac{1}{z}$ be the **reciprocal map** of the complex plane. Then,

$$\sigma(a + bi) = \frac{1}{|z|^2} (a - bi)$$

Hence, on the unit circle $U = \{z \in \mathbb{C},\ |z| = 1\}$ the reciprocal map becomes simply the complex conjugation. From this we see that to the geometric inversion of the unit circle corresponds the **inversion map**

$$\tau : z \to \frac{1}{\bar{z}}$$

which sends points $z \in \mathcal{H}_2$ inside the unit circle U to points in $z' \in \mathcal{H}_2$ with the same argument as z and $|z| \cdot |z'| = 1$. It fixes points on the unit circle U. It is exactly this transformation together with $z \mapsto z + 1$ which we use to "move" points within $\mathcal{H}_2$ and bring them in the fundamental domain. We are interested in forms $f(x, y)$ which are fixed by this transformation. Hence, we are interested in polynomials $f(z, 1)$ whose set of roots is fixed by $\tau(z)$.

For a degree n polynomial $f(z) \in \mathbb{C}[z]$, the **inversive** of f is called the function $f^\star(z) = z^n f\left(\frac{1}{\bar{z}}\right)$. A polynomial f will be called **self-inversive** if $f = f^\star$. We can make this definition more precise.

Let $p(z) \in \mathbb{C}[z]$ such that

$$p(z) = \sum_{i=0}^{n} a_i z^i. \tag{2.1}$$

Then, $p(z)$ is called **self-inversive** if its set of zeroes is fixed by the inversion map $\tau(z) = 1/\bar{z}$. Thus, the set of roots is

$$\left\{\alpha_1, \ldots, \alpha_n, \frac{1}{\bar{\alpha}_1}, \ldots, \frac{1}{\bar{\alpha}_n}\right\}$$

and then $p(z)$ is given by

$$p(z) = a_n \prod_{i=1}^{s} \left(z^2 - \left(\alpha_i + \frac{1}{\bar{\alpha}_i}\right) z + \frac{\alpha_i}{\bar{\alpha}_i}\right), \tag{2.2}$$

Let us denote by $\bar{p}(z)$ the *conjugate polynomial* of $p(z)$, namely

$$\bar{p}(z) := \sum_{i=0}^{n} \bar{a}_i z^i.$$

Then, we have the following; see [20].

LEMMA 1. *If $p(z)$ be given as in Eq. (2.1). The following are equivalent:*

(1) *$p(z)$ is self-inversive*
(2) *For every $z \in \mathbb{C} \setminus \{0\}$,*

$$\bar{a}_n\, p(z) = a_0\, z^n\, \bar{p}\left(\frac{1}{z}\right)$$

(3) *For every $z \in \mathbb{C} \setminus \{0\}$*

$$p(z) = w \cdot z^n \cdot \bar{p}\left(\frac{1}{z}\right),$$

where $|w| = 1$.
(4) *For $j = 0, 1, \ldots, n$,*

$$a_0 \bar{a}_j = \bar{a}_n a_{n-j}$$

Moreover, if $p(z)$ is self inversive then

(1) *$|a_i| = |a_{n-i}|$ for all $i = 0, \ldots, n$.*

(2) $\bar{a}_n \left[n\, p(z) - z\, p'(z)\right] = a_0\, z^{n-1}\, \bar{p}'\left(\frac{1}{z}\right)$, *for each* $z \in \mathbb{C}$
(3) $\left|n \cdot \frac{p(z)}{z \cdot p'(z)} - 1\right| = 1$, *for each* $z \in U$.

Studying roots of the self-inversive polynomials is an old problem which has been studied by many authors. A classical result due to Cohn states that a self-inversive polynomial has all its zeros on the unit circle if and only if all the zeros of its derivative lie in the closed unit disk.

For $p(z) \in \mathbb{C}[z]$ we let $||p||$ denote the *maximum modulus* of $p(z)$ on the unit circle. In [20] it is proved the following

THEOREM 1. *If* $p(z) = \sum_{i=0}^{n} a_i z^j$, $a_n \neq 0$, *is a self-inversive polynomial which has all the zeroes on* $|z| = 1$, *then*

$$|a_i| \leq \frac{||p||}{2}$$

for each $i \neq \frac{n}{2}$ *and* $|a_{n/2}| \leq \frac{\sqrt{2}}{2}||p||$.

From the above theorem we can see that the middle coefficient is special. The *middle coefficient conjecture* says that for $p(z)$ as in the above theorem, it is conjectured that

$$|a_{n/2}| \leq ||p|| \tag{2.3}$$

If n is even then the middle coefficient conjecture is true when $|a_{n/2}| \leq 2|a_n|$; see [20, pg. 334] for details.

The following theorem holds; see [25], [16] for details.

THEOREM 2. *Let* $p \in \mathbb{C}[x]$ *be a degree* n *self-inversive polynomial. If*

$$|a_{n-\lambda}| > \frac{1}{2}\, \frac{n}{n-2\lambda} \sum_{k=0, k\neq\lambda, k\neq n-\lambda}^{n} |a_k|$$

for some $\lambda < \frac{n}{2}$, *then* $p(z)$ *has exactly* $n - 2\lambda$ *non-real roots on the unit circle.*

If n *is even and* $\lambda = \frac{n}{2}$, *then* $p(z)$ *has no roots on the unit circle if*

$$|a_{n/2}| > 2 \sum_{k=0, k\neq n/2}^{n} |a_k|$$

For a proof see [25]. If $\lambda = 0$ this correspond to a result of Lakatos and Losonczi [16] which says that a self-inversive polynomial with non-zero discriminant has all roots on the unit circle if

$$|a_n| \geq \frac{1}{2} \sum_{k=1}^{n} |a_k|\,.$$

There is a huge amount of literature on bounding the roots or the coefficients of polynomials or finding polynomials which have bounded coefficients. Most of that work relates to Mahler measure and related works. There was another approach by Julia [15] which did not gain the attention it deserved. Lately there are works of Cremona and Stoll in [24], Beshaj [1, 2], and others who have extended Julia's method and provide an algorithm of finding the polynomial (up to a coordinate change) with the smallest coefficients. The first paragraph of this section eludes to that approach.

2.1. Reciprocal polynomials. For a degree n polynomial $f(z) \in \mathbb{C}[z]$, its **reciprocal** is called the polynomial $f^{\times}(z) = z^n f\left(\frac{1}{z}\right)$. A polynomial is called **self-reciprocal** or **palindromic** if $f = f^{\times}$ and it is called **anti-palindromic** if $f = -f^{\times}$.

If $p(z) \in \mathbb{C}[z]$ be a polynomial such that its set of roots is fixed by reciprocal map $\sigma(z)$, say

$$S = \left\{\alpha_1, \ldots, \alpha_s, \frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_s}\right\},$$

then $f(z)$ is palindromic or antipalindromic polynomial. Due to the properties of the binomial coefficients the polynomials $P(x) = (x+1)^n$ are palindromic for all positive integers n, while the polynomials $Q(x) = (x-1)^n$ are palindromic when n is even and anti-palindromic when n is odd. Also, cyclotomic polynomials are palindromic.

What if we would like some kind of invariant of the reciprocal map $z \mapsto 1/z$? Consider the transformation

$$\alpha(z) = z + \frac{1}{z}$$

Obviously, $\alpha(1/z) = z$. When considered as a function $\alpha : \mathbb{C} \to \mathbb{C}$ this is a 2 to 1 map since both z and $1/z$ go to the same point. Considered on each one of the three orbits of $SL_2(\mathbb{R})$ in $\mathbb{C}$ we have the following: α sends the upper half-plane $\mathcal{H}_2$ onto the complex plane $\mathbb{C}$ except for $(-\infty, 2]$ and $[2, \infty)$ which are doubly covered by $\mathbb{R} \setminus \{0\}$. We organize such actions in the following Lemma:

LEMMA 2. *For any polynomial $p(z) = \sum_{i=0}^{n} a_i z^i$ of degree $n = 2s$ the following are equivalent:*

(1) *The coefficients of $p(z)$ satisfy*

$$a_i = a_{n-i}, \quad \text{for all } i = 0, \ldots n.$$

(2) *There exists a polynomial $q(z)$ such that*

$$p(z) = z^s \, q\left(\frac{1}{z}\right)$$

(3) *There exists some polynomial $g(z)$ of degree $m \geq 1$ such that*

$$p(z) = z^m \cdot g\left(z + \frac{1}{z}\right)$$

For a proof see [13] among other papers. Hence, any polynomial $f(z)$ satisfying any of the properties of the Lemma is self-reciprocal.

Next we list some properties of palindromic and antipalindromic polynomials. Their proofs are elementary and we skip the details.

REMARK 1. *Here are some general properties of palindromic and anti-palindromic polynomials:*

(1) *For any antipalindromic polynomial $p(z) = \sum_{i=0}^{n} a_i z^i$*

$$a_i = -a_{n-i}, \quad \text{for all } i = 0, \ldots n.$$

(2) *For any polynomial f, the polynomial $f + f^{\times}$ is palindromic and the polynomial $f - f^{\times}$ is antipalindromic.*
(3) *The product of two palindromic or antipalindromic polynomials is palindromic.*

(4) *The product of a palindromic polynomial and an antipalindromic polynomial is antipalindromic.*
(5) *A palindromic polynomial of odd degree is a multiple of $x+1$ (it has -1 as a root) and its quotient by $x+1$ is also palindromic.*
(6) *An antipalindromic polynomial is a multiple of $x-1$ (it has 1 as a root) and its quotient by $x-1$ is palindromic.*
(7) *An antipalindromic polynomial of even degree is a multiple of x^2-1 (it has -1 and 1 as a roots) and its quotient by x^2-1 is palindromic.*

The following lemma shows an important correspondence among the pairs of roots $\left(\alpha, \frac{1}{\alpha}\right)$ of $f(z)$ and real roots of $g\left(z+\frac{1}{z}\right)$. Polynomials $f(z)$ which have all roots on the units circle correspond to $g\left(z+\frac{1}{z}\right)$ which have all real roots. When homogenized the corresponding forms are called *totally real forms* (cf. Section 4).

LEMMA 3. *Let $f(z)=\sum_{i=0}^{n} a_i z^i$ be a palindromic polynomial and $g(z)\in\mathbb{C}[z]$ such that $f(z)=z^m g(z+1/z)$. Denote by S_f the set of pairs of roots of $f(z)$ on U,*

$$S_f=\left\{\left(\alpha,\frac{1}{\alpha}\right),\ \textit{such that}\ |\alpha|=1\ \textit{and}\ f(\alpha)=0\right\}$$

and by S_g the set of roots of $g(z)$ in $[-2,2]$. There is a one-to-one correspondence between S_f and S_g.

PROOF. The proof is rather elementary. If $|z|=1$ then $z=\cos\theta+i\sin\theta$, for some θ. Then, $\alpha(z)=2\cos\theta$ is in the interval $[-2,2]$. Conversely, if $t\in[-2,2]$ then $t=2\cos\theta$ for some θ. Hence, $t=z+1/z$, where $z=\cos\theta\pm i\sin\theta$. □

Notice that the inversion $z\mapsto 1/z$ induces an involution on the group of symmetries of a palindromic polynomial. Hence, the Galois group of such polynomials is non-trivial. We will see in the next section how such involution among the roots of $f(x)$ induces automorphisms for algebraic curves with affine equation $y^n=f(x)$.

A polynomial $f(z)=\sum_{i=0}^{n} a_i z^i$ is called **quasi-palindromic** if

$$|a_i|=|a_{n-i}|,$$

for all $i=0,\ldots,n$.

The following Lemma will be used in the next section.

LEMMA 4. *Let $f,g\in\mathbb{C}[x]$ with no common factor. If f and g are self-inversive then fg is a self-inversive. If f and g are quasi-palindromic, then fg is quasi-palindromic.*

PROOF. The proof is an immediate consequence of the definitions. Since the set of roots of f and g contain all z and $\frac{1}{\bar{z}}$ (resp. z and $\pm\frac{1}{z}$), then so would contain their union, which is the set of roots of fg. □

REMARK 2. *A polynomial with real coefficients all of whose complex roots lie on the unit circle in the complex plane (all the roots are unimodular) is either palindromic or antipalindromic*

2.2. Self-reciprocal polynomials over the reals. Here is a basic fact about even degree self-reciprocal polynomials; see [8], §2.1; see also [18]. The degree $d=2n$ polynomial $p(z)$ is self-reciprocal if and only if it can be written

$$p(z)=z^n\cdot(a_n+a_{n+1}\cdot(z+z^{-1})+\cdots+a_{2n}\cdot(z^n+z^{-n})),$$

if and only if it can be written

$$p(z) = a_{2n} \cdot \prod_{k=1}^{n} (1 - \alpha_k z + z^2), \tag{2.4}$$

for some real $\alpha_k \in \mathbb{R}$.

Note that $g(z) = 1 - \alpha z + z^2$ has roots on the unit circle if and only if the roots are of the form $e^{\pm i\theta}$, for some θ, in which case, $\alpha = 2\cos(\theta)$.

For the rest of this section we denote by $p(z) = \sum_{i=0}^{n} a_i z^i$ a degree n self-reciprocal polynomial, where $n = 2d$ or $n = 2d+1$. The answer to the following question is unknown at this time: for which increasing sequences $a_0 < a_1 < \ldots a_d$ do the roots of the corresponding self-reciprocal polynomial, $p(z) = 0$, lie on the unit circle $|z| = 1$?

If $n = 2d$, which $p(z)$ with $a_0 < a_1 < \ldots a_d$, can be written as a product $\prod_{k=1}^{d}(1 - 2\cos(\theta_k)z + z^2)$?

It is clear that, in a product such as (2.4), with all its roots on the unit circle so $-2 \leq \alpha_k \leq 2$, we have

$$0 < a_0 \leq a_1 \leq \cdots \leq a_n, \quad a_{n-i} = a_{n+i}, \tag{2.5}$$

for all $i \in \{0, 1, 2, \ldots, n\}$, provided the collection α_js satisfy

$$\alpha_k \leq -1. \tag{2.6}$$

A self-reciprocal polynomial satisfying (2.5) is called *symmetric increasing*. Motivated by Problem 3 below, we look for a bound which is more general than (2.6) and which also implies the polynomial is symmetric increasing. For instance, we observe that the following result can be used inductively to establish a generalization of (2.6).

LEMMA 5. *Let $p(z)$ be as above. To multiply $p(z)$ by $1 - \alpha x + x^2$ $(-2 \leq \alpha \leq 2)$, and still have the new coefficients satisfy a symmetric increasing condition such as in (2.5), we require*

$$(a_i, a_{i+1}, a_{i+2}, a_{i+3}) \cdot (1, -1 - \alpha, 1 + \alpha, -1) \leq 0, \tag{2.7}$$

for all $i \leq d$. In particular, if $a_i = a$, $a_{i+1} = a + \epsilon_1$, $a_{i+2} = a + \epsilon_2$, $a_{i+3} = a + \epsilon_3$ then (2.7) holds if

$$\epsilon_2 \leq \frac{\epsilon_1 + \epsilon_3}{2}.$$

PROOF. This is verified simply by multiplying out $p(z)(1 - \alpha x + x^2)$, so omitted. □

The examples below illustrate how sensitive (2.5) is to the size of the α_js.

EXAMPLE 1. *We have*

$$(1+1.05x+x^2)(1-0.28x+x^2)(1+1.25x+x^2) = x^6+2.02x^5+3.6685x^4+3.67250x^3+3.6685x^2+2.02x+1,$$

which satisfies (2.5), but change the 0.28 *to* 0.3 *and*

$$(1+1.05x+x^2)(1-0.30x+x^2)(1+1.25x+x^2) = x^6+2x^5+3.6225x^4+3.60625x^3+3.6225x^2+2x+1,$$

does not. Similarly, we have

$$(1 + 1.05x + x^2)(1 - 0.3x + x^2)(1 + 1.25x + x^2)(1 - 0.6x + x^2) =$$
$$x^8 + 1.4x^7 + 3.4225x^6 + 3.43275x^5 + 5.08125x^4 + 3.43275x^3 + 3.4225x^2 + 1.4x + 1,$$

which satisfies (2.5), but change the 0.6 *to* 0.7 *and*

$$(1+1.05x+x^2)(1-0.3x+x^2)(1+1.25x+x^2)(1-0.7x+x^2)=$$

$$x^8+1.3x^7+3.2225x^6+3.0705x^5+4.720625x^4+3.0705x^3+3.2225x^2+1.3x+1,$$

does not.

The polynomial

$$(1+1.5x+x^2)(1+0.2x+x^2)(1+0.1x+x^2)=x^6+1.8x^5+3.47x^4+3.63x^3+3.47x^2+1.8x+1$$

satisfies (2.5), as does

$$(1+1.5x+x^2)(1+0.2x+x^2)(1+0.1x+x^2)(1-0.5x+x^2)=$$

$$x^8+1.3x^7+3.57x^6+3.695x^5+5.125x^4+3.695x^3+3.57x^2+1.3x+1$$

but change the 0.5 *to* 0.6 *and the product*

$$(1+1.5x+x^2)(1+0.2x+x^2)(1+0.1x+x^2)(1-0.6x+x^2)=$$

$$x^8+1.2x^7+3.39x^6+3.348x^5+4.762x^4+3.348x^3+3.39x^2+1.2x+1$$

does not.

The polynomial

$$(1+0.1x+x^2)(1+0.2x+x^2)(1+0.3x+x^2)(1+0.92x+x^2)=$$

$$x^8+1.52x^7+4.662x^6+4.6672x^5+7.32952x^4+4.6672x^3+4.662x^2+1.52x+1$$

satisfies (2.5), but change the 0.92 *to* 0.91 *and*

$$(1+0.1x+x^2)(1+0.2x+x^2)(1+0.3x+x^2)(1+0.91x+x^2)=$$

$$x^8+1.51x^7+4.656x^6+4.6361x^5+7.31746x^4+4.6361x^3+4.656x^2+1.51x+1$$

does not.

The above lemma holds, namely the condition (2.7), because

$$(1+0.1x+x^2)(1+0.2x+x^2)(1+0.3x+x^2)(1+0.92x+x^2)(1+0.999x+x^2)=$$

$$x^{10}+2.519x^9+7.18048x^8+10.844538x^7+16.6540528x^6+$$

$$+16.65659048x^5+16.6540528x^4+10.844538x^3+7.18048x^2+2.519x+1$$

satisfies (2.5), but change the 0.999 *to* 0.99 *and*

$$(1+0.1x+x^2)(1+0.2x+x^2)(1+0.3x+x^2)(1+0.92x+x^2)(1+0.99x+x^2)=$$

$$x^{10}+2.51x^9+7.1668x^8+10.80258x^7+16.612048x^6+$$

$$+16.5906248x^5+16.612048x^4+10.80258x^3+7.1668x^2+2.51x+1$$

does not.

3. Superelliptic curves and self-inversive polynomials

The following theorem connects self-reciprocal polynomials with a very special class of algebraic curves, namely superelliptic curves. We follow the definitions and notation as in [4].

Fix an integer $g \geq 2$. Let $\mathcal{X}_g$ denote a genus g generic planar curve defined over an algebraically closed field k of characteristic $p \geq 0$. We denote by G the full automorphism group of $\mathcal{X}_g$. Hence, G is a finite group. Denote by K the function field of $\mathcal{X}_g$ and assume that the affine equation of $\mathcal{X}_g$ is given by some polynomial in terms of x and y.

Let $H = \langle \tau \rangle$ be a cyclic subgroup of G such that $|H| = n$ and H is in the center of G, where $n \geq 2$. Moreover, we assume that the quotient curve $\mathcal{X}_g/H$ has genus zero. The **reduced automorphism group of $\mathcal{X}_g$ with respect to H** is called the group $\bar{G} := G/H$, see [4].

Assume $k(x)$ is the genus zero subfield of K fixed by H. Hence, $[K : k(x)] = n$. Then, the group $\bar{G}$ is a subgroup of the group of automorphisms of a genus zero field. Hence, $\bar{G} < PGL_2(k)$ and $\bar{G}$ is finite. It is a classical result that every finite subgroup of $PGL_2(k)$ is isomorphic to one of the following: C_m, D_m, A_4, S_4, A_5, *semidirect product of an elementary Abelian group with cyclic group*, $PSL(2,q)$ and $PGL(2,q)$.

The group $\bar{G}$ acts on $k(x)$ via the natural way. The fixed field of this action is a genus 0 field, say $k(z)$. Thus, z is a degree $|\bar{G}| := m$ rational function in x, say $z = \phi(x)$.

LEMMA 6. *Let $\mathcal{X}_g$ be a superelliptic curve of level n with $|Aut\ (\mathcal{X}_g)| > n$. Then, $\mathcal{X}_g$ can be written as*

$$y^n = f(x^s), \quad or \quad y^n = xf(x^s)$$

for some $s > 1$.

The proof goes similar as for the hyperelliptic curves as in [23]. Since below we display all equations of such curves in such form then the Lemma is obviously true.

Next we focus on studying the nature of the polynomial $f(x)$ and its connections to self-inversive polynomials. We are assuming that the curves are of characteristic zero, so the reduced automorphism group is cyclic, dihedral, A_4, S_4, or A_5. The list of equations, including the full group of automorphisms, the dimension of the loci, and the ramification of the corresponding covers can be taken from [21].

THEOREM 3. *If the reduced automorphism group of a superelliptic curve $\mathcal{X}$ is nontrivial or not isomorphic to a cyclic group, then $\mathcal{X}$ can be written with the affine equation*

$$y^n = f(x) \quad or \quad y^n = x \cdot f(x)$$

where $f(x)$ is a palindromic or antipalindromic polynomial. If the reduced automorphism group is isomorphic to A_5, then $f(x)$ is a quasi-palindromic plynomial.

PROOF. If $\overline{\mathrm{Aut}}\ (\mathcal{X})$ is isomorphic to a dihedral group D_{2m}, then the equation of $\mathcal{X}_g$ can be written as in one of the following cases

$$\begin{aligned}
y^n &= F(x) := \prod_{i=1}^{\delta}(x^{2m} + \lambda_i x^m + 1)\\
y^n &= (x^m - 1)\cdot F(x),\\
y^n &= x \cdot F(x),\\
y^n &= (x^{2m} - 1)\cdot F(x),\\
y^n &= x(x^m - 1)\cdot F(x),\\
y^n &= x(x^{2m} - 1)\cdot F(x),
\end{aligned}$$

The polynomial $F(x)$ is palindromic from Lemma 2. The polynomials $x^m - 1$ and $x^{2m} - 1$ are antipalindromic. From Lemma 4 the products $(x^m - 1)F(x)$ and $(x^{2m} - 1)F(x)$ are antipalindromic. Hence, if the reduced automorphism group of a superelliptic curve is isomorphic to a dihedral group then the equation of the curve can be written as $y^2 = f(x)$ or $y^2 = xf(x)$, where $f(x)$ can be chosen to be a palindromic or antipalindromic polynomial.

If $\overline{\mathrm{Aut}}\ (\mathcal{X})$ is isomorphic to A_4, then the equation of $\mathcal{X}_g$ can be written as in one of the following cases

$$\begin{aligned}
y^n &= G(x)\\
y^n &= (x^4 + 2i\sqrt{3}x^2 + 1)\cdot G(x),\\
y^n &= (x^8 + 14x^4 + 1)\cdot G(x),\\
y^n &= x(x^4 - 1)\cdot G(x),\\
y^n &= x(x^4 - 1)(x^4 + 2i\sqrt{3}x^2 + 1)\cdot G(x),\\
y^n &= x(x^4 - 1)(x^8 + 14x^4 + 1)\cdot G(x),
\end{aligned}$$

where

$$G(x) := \prod_{i=1}^{\delta}(x^{12} - \lambda_i x^{10} - 33x^8 + 2\lambda_i x^6 - 33x^4 - \lambda_i x^2 + 1)$$

Notice that every factor of $G(x)$ is palindromic, hence $G(x)$ is also palindromic from Lemma 4. The polynomials $x^4 + 2i\sqrt{3}x^2 + 1$ and $x^8 + 14x^4 + 1$ are palindromic and therefore $(x^4 + 2i\sqrt{3}x^2 + 1)\,G(x)$ and $(x^8 + 14x^4 + 1)\,G(x)$ are palindromic. When multiplied by $x^4 - 1$ such polynomials become antipalindromic since $x^4 - 1$ is antipalindromic. So the equation of the curve can be written as $y^2 = f(x)$ or $y^2 = xf(x)$, where $f(x)$ can be chosen to be a palindromic or antipalindromic polynomial.

If $\overline{\mathrm{Aut}}\ (\mathcal{X})$ is isomorphic to S_4, then the equation of $\mathcal{X}_g$ can be written as in one of the following cases

$$\begin{aligned}
y^n &= M(x)\\
y^n &= \left(x^8+14x^4+1\right)\cdot M(x)\\
y^n &= x(x^4-1)\cdot M(x)\\
y^n &= \left(x^8+14x^4+1\right)\cdot x(x^4-1)\cdot M(x)\\
y^n &= \left(x^{12}-33x^8-33x^4+1\right)\cdot M(x)\\
y^n &= \left(x^{12}-33x^8-33x^4+1\right)\cdot\left(x^8+14x^4+1\right)\cdot M(x)\\
y^n &= \left(x^{12}-33x^8-33x^4+1\right)\cdot x(x^4-1)\cdot M(x)\\
y^n &= \left(x^{12}-33x^8-33x^4+1\right)\cdot\left(x^8+14x^4+1\right)\cdot x(x^4-1)M(x)
\end{aligned}$$

where

$$M(x)=\prod_{i=1}^{\delta}\left(x^{24}+\lambda_i x^{20}+(759-4\lambda_i)x^{16}+2(3\lambda_i+1228)x^{12}+(759-4\lambda_i)x^8 +\lambda_i x^4+1\right)$$

Since every factor of $M(x)$ is palindromic, then $M(x)$ is palindromic. By Lemma 4 we have that the equation of the curve can be written as $y^2=f(x)$ or $y^2=xf(x)$, where $f(x)$ can be chosen to be a palindromic or antipalindromic polynomial. The antipalindromic cases correspond exactly to the cases when x^4-1 appears as a factor.

Let $\overline{\mathrm{Aut}}\ (\mathcal{X})$ is isomorphic to A_5. This case is slightly different from the other cases due to the fact that now the reduced group has an element of order 5 and $f(x)$ will be written as a decomposition of x^5. So the change of coordinates $x\mapsto -x$ will preserve the sign for odd powers and change it for even powers of x.

Let $\Lambda(x)$, $Q(x)$, $\psi(x)$ be as follows

$$\begin{aligned}
\Lambda(x)=&\prod_{i=1}^{\delta}(x^{60}+a_1x^{55}+a_2x^{50}+a_3x^{45}+a_4x^{40}+a_5x^{35}+a_6x^{30}-a_5x^{25}+a_4x^{20}\\
&-a_3x^{15}+a_2x^{10}-a_1x^5+1)\\
a_1=&\lambda_i-684\\
a_2=&55\lambda_i+157434\\
a_3=&1205\lambda_i-12527460\\
a_4=&13090\lambda_i+77460495\\
a_5=&69585\lambda_i-130689144\\
a_6=&134761\lambda_i-33211924\\
Q(x)=&x^{30}+522x^{25}-10005x^{20}-10005x^{10}-522x^5+1,\\
\psi(x)=&x^4+2i\sqrt{3}x^2+1
\end{aligned}$$

Then, the equation of $\mathcal{X}_g$ can be written as in one of the following cases

$$y^n = \Lambda(x)$$
$$y^n = x(x^{10} + 11x^5 - 1) \cdot \Lambda(x)$$
$$y^n = x(x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x^{10} + 11x^5 - 1) \cdot \Lambda(x)$$
$$y^n = (x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \Lambda(x)$$
$$y^n = Q(x) \cdot \Lambda(x)$$
$$y^n = x(x^{10} + 11x^5 - 1).\psi(x) \cdot \Lambda(x)$$
$$y^n = (x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1) \cdot \psi(x) \cdot \Lambda(x)$$
$$y^n = (x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1)(x(x^{10} + 11x^5 - 1)) \cdot \psi(x) \cdot \Lambda(x)$$

Notice that $\Lambda(x)$ is a quasi-palindromic polynomial since all its factors are so. So are $Q(x), \psi(x)$ and the other factors. By Lemma 4 we can say that in this case he equation of the curve can be written as $y^2 = f(x)$ or $y^2 = xf(x)$, where $f(x)$ can be chosen to be a quasi-palindromic polynomial.

This completes the proof of the theorem. □

In [12] it is shown that if the group H is unique in G and the reduced group G/H is not cyclic or nontrivial, then the field of moduli is a field of definition for superelliptic curves. In [3] and [5] it is explored the fact that most palindromic or self-inversive polynomials have minimal coefficients. So it is a natural question to investigate what is the relation between the minimal of definition of such curves, the minimal height as in [2], and the palindromic polynomial $f(x)$.

4. Self-reciprocal polynomials and reduction theory

Every stable binary form $f(z, y)$ of degree $n \geq 2$ correspond uniquely to a positive definite quadratic $\mathcal{J}_f$ called Julia quadratic; see [2]. Since positive definite quadratics have a unique zero in the upper half plane $\mathcal{H}_2$, then we associate the zero of $\mathcal{J}_f$ to the binary form f. This defines a map ε from the set of degree n binary forms to $\mathcal{H}_2$, which is called the zero map. A binary form $f(z, y)$ is called *reduced* if $\varepsilon(f) \in \mathcal{F}_2$. The size of the coefficients of a reduced binary form is bounded by its Julia invariant $\theta(f)$. If f is a reduced form, we say that f has *minimal coefficients*; see [2] for details.

There are no efficient ways to compute the Julia quadratic or the Julia invariant of a binary form of high degree (i.e. degree > 6). Moreover, there is no known method to express the Julia invariant $\theta(f)$ in terms of the generators of the ring of invariants of the degree n binary forms (i.e. transvections of the form). However, as discussed in [2] the case when f is totally real is much easier. A form is called *totally real* if it splits over $\mathbb{R}$.

Let $f \in \mathbb{C}[z]$ be a degree $n \geq 2$ polynomial. We denote by f_* the corresponding form (homogenization of f) in $\mathbb{C}[z, y]$. $GL_2(\mathbb{C})$ acts on the space of degree n binary forms. For a matrix $M \in GL_2(\mathbb{C})$ we denote by f_*^M the action of M on f_*. By f^M we denote $f_*^M(z, 1)$.

LEMMA 7. *Let $f \in \mathbb{C}[z]$ and $M = \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}$. Then, f_* is a totally real binary form if and only if f^M has all roots in the unit circle.*

PROOF. The proof is rather elementary. The Möbious transformation $h(z) = Mz$ maps $\mathcal{H}_2$ onto the open unit disk. Moreover, it maps bijectively $U \setminus \{1\}$ to $\mathbb{R}$. □

For reduction of totally real forms see [2] and [5].

THEOREM 4. *Let $f(z)$ be a self-inversive polynomial. Then the following are equivalent:*

i) all roots of $f(z)$ are on the unit circle

ii) all roots of its derivative $f'(z)$ are on the unit disk

iii) f_*^M is totally real form

PROOF. The equivalence of i) and iii) is the above Lemma. The equivalence of i) and ii) is a result of Cohn. □

It is interesting to see how the reduction is performed in such case. From [2] we have a polynomial G_f associated to f. The Julia quadratic J_f is the only quadratic factor of G_f when factored over $\mathbb{R}$. Moreover, Beshaj [2] has proved that G_f is very similar to a self-inversive polynomial. We describe briefly below

Let f be a generic totally real form given by

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

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

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

Define $G(x,y)$ as follows

$$G(x,y) = \frac{x \cdot f_x(-f_y(x,y), f_x(x,y)) + y \cdot f_y(-f_y(x,y), f_x(x,y))}{n\, f(x,y)}. \tag{4.1}$$

Notice that since f is totally real, then $f \in \mathbb{R}[x,y]$. Therefore, $G \in \mathbb{R}[x,y]$. Note also that, for $\sigma \in S_{n+1}$ we have an involution

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

Next result describes the properties of $G(x,y)$.

THEOREM 5 (Beshaj). *The polynomial $G(x,y)$ satisfies the following*

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 the Julia quadratic $\mathcal{J}_f$.

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 $i = 0, ..., d$.

Then we have the interesting connection between real forms and self-inversive polynomials.

THEOREM 6. *If f is a palindromic real form then $G_f(x,y)$ is self-inversive. If f is of odd degree then G_f is palindromic.*

PROOF. If f is palindromic, then from Lemma 3, i) we have that $a_i = a_{n-i}$ for all $i = 0,\dots,n$. That means that σ fixes all coefficients of f. Hence, $g_i^\sigma = (-1)^{n-1} g_i$ for all $i = 0,\dots,d$, where $d = \deg G_f$. Thus, G_f is self-inversive. If n is odd, then $g_i^\sigma = g_i$. Hence, G_f is palindromic.

□

We know that G_f has exactly two non-real roots, namely $\varepsilon(f)$ and its conjugate. Consider now G_f^M. Then all real roots of G_f will go to roots on the unit circle of G_f^M and the two non-real roots $\varepsilon(f)$ and its conjugate $\overline{\varepsilon(f)}$ go inside the unit disk as roots of G_f^M.

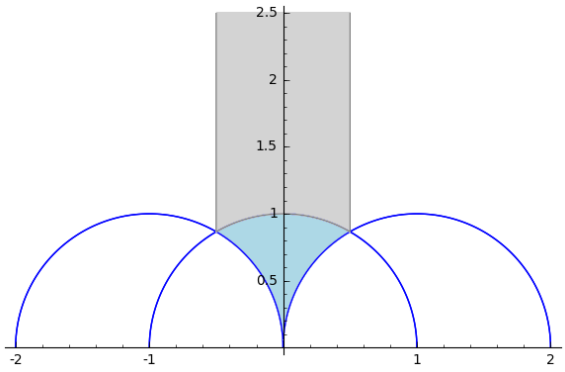

FIGURE 1. The region $\mathcal{T}$

LEMMA 8. *Let f be a self-inversive polynomial with all roots in the unit circle U, f_* its homogenization, $\mathcal{T}$ be the region in the complex plane given by*

$$\mathcal{T} = \{z = a + bi \,|\, a^2 - 2a + b^2 \geq 0,\ a^2 + 2a + b^2 \geq 0\},$$

and $M = \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}$. If $\varepsilon(f_*)^M \in \mathcal{T}$ or $\varepsilon(f_*)^M \in \mathcal{F}_2$, then f^M has minimal coefficients.

PROOF. From Lem. 7 we have that f_*^M is a totally real form. Then $\varepsilon(f_*^M)$ is the image of the zero map in the upper half plane $\mathcal{H}_2$.

If $\varepsilon(f_*)^M \in \mathcal{F}_2$ then f_*^M is reduced and we are done. If $\varepsilon(f_*)^M \in \mathcal{T}$ then let $S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and compute $\varepsilon(f_*)^{MS}$. Let $\varepsilon(f_*)^M = a + bi$. Then

$$\varepsilon(f_*)^{MS} = \frac{1}{a+bi} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

Hence, $|\varepsilon(f_*)^{MS}| \geq 1$ and

$$-\frac{1}{2} \leq \frac{a}{a^2+b^2} \leq \frac{1}{2}$$

Hence, $\varepsilon(f_*)^M \in \mathcal{F}_2$ However, the height of f_*^M does not change under the transformation S. Hence, f_*^M has minimal coefficients. Thus, in both cases f^M has minimal coefficients. □

The region $\mathcal{T}$ is the blue colored region in Fig. 1 and the grey area is the fundamental domain.

5. Self-reciprocal polynomials and codes

The goal of this section is to show how self-reciprocal polynomials are connected to other areas of mathematics, namely whether extremal formal weight enumerators for codes satisfy the Riemann hypothesis. We will follow the setup of [11].

For $d \leq n$, denote the weight enumerator of an MDS code C over $\mathbb{F} = GF(q)$ of length n and minimum distance d by $M_{n,d}(x,y)$. The dual $C^\perp$ is also an MDS code of length n and minimum distance $d^\perp = n+2-d$. Therefore, for $d \geq 2$, the weight enumerator of $C^\perp$ is $M_{n,n+2-d}(x,y)$. Let $M_{n,n+1} = x^n$. The MDS code with weight enumerator $M_{n,1}$ has dimension $n-d+1 = n-1+1 = n$, hence $C = \mathbb{F}_q^n$. It is easy to see that $M_{n,n+1}$ is the MacWilliams transform, $(x,y) \mapsto (\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}})$, of $M_{n,1}$. We may think of $M_{n,1}$ as the weight enumerator of the zero code.

The set $\{M_{n,1}, M_{n,2}, \ldots, M_{n,n-1}, M_{n,n+1}\}$ is a basis for the vector space of homogeneous polynomials of degree n in x, y. Furthermore, this set is closed under the MacWilliams transform; see [11] for details.

If C is an $[n,k,d]_q$-code, then one can easily see that

$$A_C(x,y) = \sum_{i=d}^{n+1} a_{i-d} M_{n,i} = a_0 M_{n,d} + \ldots + a_{n+1-d} M_{n,n+1},$$

for some integers a_i as in §4.4.2 in [14]. The zeta polynomial of C is defined as

$$P(T) := a_0 + a_1 T + \cdots + a_{n-d+1} T^{n+1-d}.$$

The zeta polynomial $P(T)$ of an $[n,k,d]_q$-code C determines uniquely the weight enumerator of C. The degree of $P(T)$ is at most $n-d+1$. The quotient

$$Z(t) = \frac{P(T)}{(1-T)(1-qT)}$$

is called **the zeta function** of the linear code C. The zeta function of an MDS code

$$\frac{1}{(1-T)(1-qT)} = \sum_{j=0}^{\infty} \frac{q^{j+1}-1}{q-1} T^j$$

is the rational zeta function over $\mathbb{F}_q$; see [11, Cor. 1]. Formally self-dual codes lead to self-reciprocal polynomials. The proof of the following Proposition can be found in [11].

PROPOSITION 1. *If $P(T)$ is the zeta polynomial of a formally self-dual code, then $P(T/\sqrt{q})$ is a self-reciprocal polynomial.*

5.1. Riemann zeta function versus zeta function for self-dual codes. From [11] we have that for a self-dual code C,

$$Z(T) = q^{g-1} T^{2g-2} Z(1/qT),$$

which for $z(T) := T^{1-g} Z(T)$, may be written as

$$z(T) = z(1/qT).$$

Now let

$$\zeta_C(s) := Z(q^{-s}) \text{ and } \xi_C(s) := z(q^{-s}).$$

We obtain

$$\xi_C(s) = \xi_C(1-s),$$

which is the same symmetry equation is analogous to the functional equation for the Riemann zeta function. We note that $\zeta(s)$ and $\xi(s)$ have the same zeros.

The zeroes of the zeta function of a linear code C are useful in understanding possible values of its minimum distance d.

Let C be a linear code with weight distribution vector $(A_0, A_1, \ldots, A_n)$. Let $\alpha_1, \ldots, \alpha_r$ be the zeros of the zeta polynomial $P(T)$ of C Then

$$d = q - \sum_i \alpha_i^{-1} - \frac{A_{d+1}}{A_d}\frac{d+1}{n-d}.$$

In particular,

$$d \leq q - \sum_i \alpha_i^{-1};$$

see [11] for details.

A self-dual code C is said to satisfy *Riemann hypothesis* if the real part of any zero of $\zeta_C(s)$ is $1/2$, or equivalently, the zeros of the zeta polynomial $P_C(T)$ lie on the circle $|T| = 1/\sqrt{q}$, or equivalently, the roots of the self-reciprocal polynomial (see Proposition 1 above) $P_C(T/\sqrt{q})$ lie on the unit circle.

While Riemann hypothesis is satisfied for curves over finite fields, in general it does not hold for linear codes. A result that generates many counterexamples may be found in [14]. There is a family of self-dual codes that satisfy the Riemann hypothesis which we are about to discuss. The theory involved in this description holds in more generality than linear codes and their weight enumerators.

5.2. Virtual weight enumerators. A homogeneous polynomial

$$F(x,y) = x^n + \sum_{i=1}^{n} f_i x^{n-i} y^i$$

with complex coefficients is called a *virtual weight enumerator*. The set

$$\{0\} \cup \{i : f_i \neq 0\}$$

is called its *support*. If

$$F(x,y) = x^n + \sum_{i=d}^{n} f_i x^{n-i} y^i, \tag{5.1}$$

with $f_d \neq 0$, then n is called the *length* and d is called the *minimum distance* of $F(x,y)$.

Let C be a self-dual linear $[n,k,d]$-code. Recall that n is even, $k = n/2$ and its weight enumerator satisfies MacWilliams' Identity. A virtual generalization of $A_C(x,y)$ is straightforward. A virtual weight enumerator $F(x,y)$ of even degree that is a solution to MacWilliams' Identity

$$F(x,y) = F\left(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right), \tag{5.2}$$

is called *virtually self dual* over $\mathbb{F}_q$ with *genus* $\gamma(F) = n/2 + 1 - d$. Although a virtual weight enumerator in general does not depend on a prime power q, a virtually self-dual weight enumerator does.

PROBLEM 1. *Find the conditions under which a (self-dual) virtual weight enumerator with positive integer coefficients arises from a (self-dual) linear code.*

The zeta polynomial and the zeta function of a virtual weight enumerator are defined as in the case of codes.

PROPOSITION 2 ([6]). *Let $F(x,y)$ be a virtual weight enumerator of length n and minimum distance d. Then, there exists a unique function $P_F(T)$ of degree at most $n-d$ which satisfies the following*

$$\frac{(y(1-T)+xT)^n}{(1-T)(1-qT)}P_F(T) = \ldots + \frac{F(x,y)-x^n}{q-1}T^{n-d} + \ldots$$

The polynomial $P_F(T)$ and the function

$$Z_F(T) := \frac{P(T)}{(1-T)(1-qT)},$$

are called respectively *the zeta polynomial and the zeta function of the virtual weight enumerator* $F(x,y)$.

A virtual self-dual weight enumerator *satisfies the Riemann hypothesis* if the zeroes of its zeta polynomial $P_F(T)$ lie on the circle $|T| = 1/\sqrt{q}$. There is a family of virtual self-dual weight enumerators that satisfy Riemann hypothesis. It consists of enumerators that have certain divisibility properties.

Let $b > 1$ be an integer. If $\mathrm{supp}(F) \subset b\mathbb{Z}$, then F is called *b-divisible*. Let F given by Eq. (5.1) be a b-divisible, virtually self-dual weight enumerator over $\mathbb{F}_q$. Then $F(x,y)$ is called

Type I: if $q = b = 2,\ 2|n$.
Type II: if $q = 2, b = 4, 8|n$.
Type III: if $q = b = 3, 4|n$.
Type IV: if $q = 4, b = 2, 2|n$.

Then we have the following theorem:

THEOREM 7 (Mallows-Sloane-Duursma). *If $F(x,y)$ is a b-divisible self-dual virtual enumerator with length n and minimum distance d, then*

$$d \leq \begin{cases} 2\left[\frac{n}{8}\right]+2, & \text{if } F \text{ is Type I,} \\ 4\left[\frac{n}{24}\right]+4, & \text{if } F \text{ is Type II,} \\ 3\left[\frac{n}{12}\right]+3, & \text{if } F \text{ is Type III,} \\ 2\left[\frac{n}{6}\right]+2, & \text{if } F \text{ is Type IV.} \end{cases}$$

A virtually self-dual weight enumerator $F(x,y)$ is called *extremal* if the bound in Theorem 7 holds with equality. A linear code C is called b-divisible, extremal, Type I, II, II, IV if and only if its weight enumerator has the corresponding property. The zeta functions of all extremal virtually self-dual weight enumerators are known; see [10]. The following result can be found in [10].

PROPOSITION 3. *All extremal type IV virtual weight enumerators satisfy the Riemann hypothesis.*

For all other extremal enumerators, Duursma has suggested the following conjecture in [9].

PROBLEM 2. *Prove that any extremal virtual self-dual weight enumerators of type I-III satisfies the Riemann hypothesis.*

Let F denote a weight enumerator as in (5.2) and $P_F(T)$ the associated zeta polynomial. Let $p_F(T) = P_F(T/\sqrt{q})$ denote the normalized zeta polynomial. Numerous computations suggest the following result.

PROBLEM 3. *If F is an extremal weight enumerator of Type I, II, II, IV then the normalized zeta polynomial is symmetric increasing. In fact, using the notation of (2.5), if if $a_i = a$, $a_{i+1} = a + \epsilon_1$, $a_{i+2} = a + \epsilon_2$, $a_{i+3} = a + \epsilon_3$ then $\epsilon_2 \leq \frac{\epsilon_1+\epsilon_3}{2}$.*

References

[1] L. Beshaj, *Reduction theory of binary forms*, Arithmetic of superelliptic curves, 2015.

[2] ———, *Integral binary forms with minimal height*, Ph.D. Thesis, 2016.

[3] ———, *Julia quadratic of superelliptic curves with extra automorphisms*, Algebraic curves and their fibrations in mathematical physics and arithmetic geometry, 2016.

[4] L. Beshaj, V. Hoxha, and T. Shaska, *On superelliptic curves of level n and their quotients, I*, Albanian J. Math. **5** (2011), no. 3, 115–137. MR2846162

[5] L. Beshaj and T. Shaska, *Julia quadratic of self-inversive binary forms*, 2016. in preparation.

[6] Koji Chinen, *Zeta functions for formal weight enumerators and the extremal property*, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 10, 168–173 (2006). MR2196722 (2007g:11110)

[7] Keith Conrad, *Root on a circle*, 2015.

[8] Stephen A. DiPippo and Everett W. Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory **73** (1998), no. 2, 426–450. MR1657992

[9] Iwan Duursma, *A Riemann hypothesis analogue for self-dual codes*, Codes and association schemes (Piscataway, NJ, 1999), 2001, pp. 115–124. MR1816392 (2001m:94055)

[10] ———, *Extremal weight enumerators and ultraspherical polynomials*, Discrete Math. **268** (2003), no. 1-3, 103–127. MR1983272 (2005e:94295)

[11] A. Elezi and T. Shaska, *Weight distributions, zeta functions and riemann hypothesis for linear and algebraic geometry codes*, Arithmetic of superelliptic curves, 2015.

[12] R. Hidalgo and T. Shaska, *On the field of moduli of superelliptic curves*, Algebraic curves and their fibrations in mathematical physics and arithmetic geometry, 2016.

[13] David Joyner, *Zeros of some self-reciprocal polynomials*, Excursions in harmonic analysis. Volume 1, 2013, pp. 329–348. MR3050347

[14] David Joyner and Jon-Lark Kim, *Selected unsolved problems in coding theory*, Applied and Numerical Harmonic Analysis, Birkhäuser/Springer, New York, 2011. MR2838861 (2012i:94003)

[15] 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.

[16] P. Lakatos and L. Losonczi, *Self-inversive polynomials whose zeros are on the unit circle*, Publ. Math. Debrecen **65** (2004), no. 3-4, 409–420. MR2107957 (2005h:30007)

[17] Piroska Lakatos, *On polynomials having zeros on the unit circle*, C. R. Math. Acad. Sci. Soc. R. Can. **24** (2002), no. 2, 91–96. MR1902028

[18] ———, *On zeros of reciprocal polynomials*, Publ. Math. Debrecen **61** (2002), no. 3-4, 645–661. MR1943722

[19] Laszlo Losonczi and Andrzej Schinzel, *Self-inversive polynomials of odd degree*, Ramanujan J. **14** (2007), no. 2, 305–320. MR2341855 (2009b:30008)

[20] P. J. O'Hara and R. S. Rodriguez, *Some properties of self-inversive polynomials*, Proc. Amer. Math. Soc. **44** (1974), 331–335. MR0349967 (50 #2460)

[21] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)

[22] A. Schinzel, *Self-inversive polynomials with all zeros on the unit circle*, Ramanujan J. **9** (2005), no. 1-2, 19–23. MR2166374 (2006d:30008)

[23] T. Shaska, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, 2003, pp. 248–254 (electronic). MR2035219

[24] Michael Stoll and John E. Cremona, *On the reduction theory of binary forms*, J. Reine Angew. Math. **565** (2003), 79–99. MR2024647 (2005e:11091)
[25] R. S. Vieira, *On the number of roots of self-inversive polynomials on the complex unit circle* (2015).

Department of Mathematics, US Naval Academy, Annapolis, MD, 21402
E-mail address: wdjoyner@gmail.com

546 Mathematics and Science Center, Rochester, MI, 48309
E-mail address: shaska@oakland.edu