

## Chapter 4

# The Riemann Hypothesis and Coding Theory

If the ring of integers  $\mathbb{Z}$  is analogous with the polynomial ring  $GF(p)[x]$ , then we have the following comparisons:

$$\begin{array}{ccc} \mathbb{Z} & \leftrightarrow & GF(p)[x] \\ \text{prime numbers} & \leftrightarrow & \text{irreducible polynomials in } GF(p)[x], \end{array}$$

where  $p$  is a prime,

$$\begin{array}{ccc} \zeta(s) & \leftrightarrow & Z_{\mathbb{P}^1}(s) \\ \text{(Riemann zeta function)} & & \text{(Hasse–Weil zeta fcn of } \mathbb{P}^1/GF(p)). \end{array}$$

This analogy extends (no pun intended) to finite algebraic extensions, leading to analogies between the Dedekind zeta function  $\zeta_K(s)$  of a number field  $K$  and the Hasse–Weil zeta function of a smooth projective curve defined over a finite field. If the ring of integers  $\mathcal{O}$  of a number field  $K$  are analogous with the coordinate ring  $GF(q)(X)$  of a smooth projective curve  $X/GF(q)$ , then we have the following comparisons:

$$\begin{array}{ccc} \mathcal{O} & \leftrightarrow & GF(q)(X) \\ \text{prime ideals in } \mathcal{O} & \leftrightarrow & \text{prime ideals in } GF(q)(X), \end{array}$$

where  $q$  is a prime power (discussed briefly using SAGE in Sect. 4.4.4 below),

$$\begin{array}{ccc} \zeta_K(s) & \leftrightarrow & Z_X(s) \\ \text{(Dedekind zeta function)} & & \text{(Hasse–Weil zeta fcn of } X/GF(q)). \end{array}$$

The basic idea behind this is that if we believe that the Riemann hypothesis holds for the Riemann zeta function, and its analogs for Dedekind zeta functions, then we should also believe in its truth for the Hasse–Weil zeta function for curves. (The Riemann hypothesis for curves was settled by A. Weil in the 1940s.)

I. Duursma [D1, D2, D3, D4, D5, D6] has defined a zeta function for linear codes and has extended this analogy to linear codes,<sup>1</sup> so that in some vague sense:

Hasse-Weil zeta function of a curve  $\Leftrightarrow$  Duursma zeta function of a code.

In particular, there is an analog of the well-known Riemann hypothesis in coding theory. This chapter is devoted to explaining the fascinating details surrounding this open question.

## 4.1 Introduction to the Riemann Zeta Function

The *Riemann hypothesis*, first formulated by Bernhard Riemann in 1859, is one of the most famous and important unsolved problems in mathematics. The Riemann hypothesis is a conjecture about the distribution of the zeros of the Riemann zeta-function  $\zeta(s)$ . The Riemann zeta-function  $\zeta(s)$  is the function of a complex variable  $s$  initially defined by the following infinite series:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for values of  $s$  with real part greater than one. A globally convergent series for the zeta function, valid for all complex numbers  $s$  except  $s = 1$ , was conjectured by Konrad Knopp and proved by Helmut Hasse in 1930:

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^n (-1)^k \binom{n}{k} (k+1)^{-s}. \quad (4.1.1)$$

Another interesting property that the Riemann zeta function has is its so-called functional equation:

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s).$$

If we let

$$\xi(s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s),$$

then we can rewrite this as

$$\xi(1-s) = \xi(s).$$

Because of (4.1.1), the Riemann zeta-function is defined for all complex numbers  $s \neq 1$ . It has zeros at the negative even integers (i.e., at  $s = -2, -4, -6, \dots$ ). These

---

<sup>1</sup>In fact, this analogy can be extended to an analogy between curves and matroids. The analogy with curves and codes is discussed in more detail in Sect. 4.4.4 below.

are called the *trivial zeros*. The Riemann hypothesis is concerned with the *nontrivial zeros* and states that:

The real part of any nontrivial zero of the Riemann zeta function is  $\frac{1}{2}$ .

It has been an open question for almost 150 years, despite attracting concentrated efforts from many outstanding mathematicians.

## 4.2 Introduction to the Duursma Zeta Function

Let  $C$  be an  $[n, k, d]_q$  code, i.e., a linear code over  $GF(q)$  of length  $n$ , dimension  $k$ , and minimum distance  $d$ . Recall that the Singleton bound states that  $d + k \leq n + 1$  and that codes which satisfy equality in this bound are called MDS (maximum distance separable) codes.

Motivated by analogies with local class field theory, in [D1] Iwan Duursma introduced the *zeta function*  $Z = Z_C$  associated to a linear code  $C$  over a finite field,

$$Z(T) = \frac{P(T)}{(1-T)(1-qT)}, \quad (4.2.1)$$

where  $P(T) = P_C(T)$  is a polynomial of degree  $n + 2 - d - d^\perp$ , called the *zeta polynomial*.<sup>2</sup> If  $C$  is self-dual (i.e.,  $C = C^\perp$ ), it satisfies a functional equation of the form

$$P(t) = q^g t^{2g} P\left(\frac{1}{qt}\right).$$

This does not look too much like the functional equation for the Riemann zeta function (yet).

If  $\gamma = \gamma(C) = n + 1 - k - d$  (the *genus* of  $C$ ) and if

$$z_C(T) = Z_C(T)T^{1-\gamma},$$

then the functional equation can be written in the form

$$z_{C^\perp}(T) = z_C(1/qT).$$

If we let

$$\zeta_C(s) = Z_C(q^{-s})$$

and

$$\xi_C(s) = z_C(q^{-s}),$$

---

<sup>2</sup>In general, if  $C$  is an  $[n, k, d]$ -code, then we use  $[n, k^\perp, d^\perp]$  for the parameters of the dual code,  $C^\perp$ . It is a consequence of Singleton's bound that  $n + 2 - d - d^\perp \geq 0$ , with equality when  $C$  is an MDS code.

then  $\zeta_C$  and  $\xi_C$  have the same zeros, but  $\xi_C$  is “more symmetric” since the functional equation expressed in terms of it becomes<sup>3</sup>

$$\xi_{C^\perp}(s) = \xi_C(1 - s).$$

Abusing terminology, we call both  $Z_C$  and  $\zeta_C$  the *Duursma zeta function* of  $C$ .

### 4.3 Introduction

Recall that a linear code  $C$  is called an  $[n, k, d]_q$ -code if it is a  $k$ -dimensional subspace of  $GF(q)^n$  having minimum distance  $d$ ,

$$d = \min_{c \in C, c \neq 0} \text{wt}(c),$$

where  $\text{wt}$  is the Hamming weight of a codeword. The dual code of  $C$ , denoted  $C^\perp$ , has parameters  $[n, n - k, d^\perp]$  for some  $d^\perp \geq 1$ . The *genus* of an  $[n, k, d]_q$ -code  $C$  is defined by

$$\gamma(C) = n + 1 - k - d.$$

This measures how “far away the code is from being MDS.” If  $C$  is an algebraic-geometric code constructed from the Riemann–Roch space of an algebraic curve over  $GF(q)$ , then it is often equal to the genus of the curve (see [TV] for details).

Note that if  $C$  is a self-dual code, then its genus satisfies  $\gamma = n/2 + 1 - d$ .

#### 4.3.1 Virtual Weight Enumerators

The following definition generalizes the notion introduced in Sect. 2.1 above.

**Definition 88** A homogeneous polynomial  $F(x, y) = x^n + \sum_{i=1}^n f_i x^{n-i} y^i$  of degree  $n$  with complex coefficients is called a *virtual weight enumerator* with *support*  $\text{supp}(F) = \{0\} \cup \{i \mid f_i \neq 0\}$ . If  $F(x, y) = x^n + \sum_{i=d}^n A_i x^{n-i} y^i$  with  $A_d \neq 0$ , then we call  $n$  the *length* of  $F$  and  $d$  the *minimum distance* of  $F$ . Such an  $F$  of even degree satisfying (2.2.1) is called a *virtually self-dual weight enumerator over  $GF(q)$*  having *genus*

$$\gamma(F) = n/2 + 1 - d.$$

If  $b > 1$  is an integer and  $\text{supp}(F) \subset b\mathbb{Z}$ , then the virtual weight enumerator  $F$  is called  *$b$ -divisible*.

---

<sup>3</sup>This notation is inspired by analogous notation used for functions associated with the classical Riemann zeta function. See any book on the Riemann zeta function or [http://en.wikipedia.org/wiki/Riemann\\_zeta\\_function](http://en.wikipedia.org/wiki/Riemann_zeta_function).

The classification of nontrivial formally self-dual divisible codes into the four Types (as defined in Chap. 2) has a virtually self-dual weight enumerator analog. In other words, the Gleason–Pierce theorem has a strengthening where the hypothesis does not require the existence of a code, only a form which certain invariance properties.

**Theorem 89** (Gleason–Pierce–Assmus–Mattson) *Let  $F$  be a  $b$ -divisible virtually self-dual weight enumerator over  $GF(q)$ .*

*Then either*

- I.  $q = b = 2$ ,
- II.  $q = 2, b = 4$ ,
- III.  $q = b = 3$ ,
- IV.  $q = 4, b = 2$ ,
- V.  $q$  is arbitrary,  $b = 2$ , and  $F(x, y) = (x^2 + (q - 1)y^2)^{n/2}$ .

*Proof* The proof (or proofs—there are now two of them) is due to Assmus and Mattson. The easiest place to access the argument is in the excellent survey paper by Sloane [Sl]. The rough idea is as follows (for details, please see Sect. 6.1 in Sloane’s paper).

Let  $G$  denote the subgroup of  $GL(2, \mathbb{C})$  generated by the matrix of the “MacWilliams transform”

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

together with the diagonal matrices having  $b$ th roots of unity on the diagonal (since  $F(x, y) \mapsto F(\zeta x, y)$  and  $F(x, y) \mapsto F(x, \zeta y)$  both fix  $F$  if  $\zeta \in F$  is any  $b$ th root of unity). Let  $G'$  denote its image in  $PGL(2, \mathbb{C})$ . Think of  $F(x, y)$  as a function  $f(z)$  of  $z = x/y$  on  $\mathbb{P}^1$ . Let  $m$  denote the number of zeros of  $f$  (not counting multiplicity). By the invariance properties,  $m = 1$  is impossible. If  $m = 2$ , then the invariance property implies (V). If  $m \geq 3$ , then  $G'$  must be finite. The classification of finite subgroups of  $PGL(2, \mathbb{C})$  results in the remaining possibilities (I), ..., (IV).  $\square$

Next we give the virtual weight enumerator analog of Definition 39 above.

### Definition 90

- Let  $F(x, y)$  be a virtually self-dual weight enumerator. If  $b > 1$  is an integer and  $\text{supp}(F) \subset b\mathbb{Z}$ , then  $F$  is called  $b$ -divisible.
- If  $F$  is a  $b$ -divisible virtually self-dual weight enumerator over  $GF(q)$ , then  $F$  is called

$$\left\{ \begin{array}{ll} \text{Type I} & \text{if } q = b = 2, 2|n, \\ \text{Type II} & \text{if } q = 2, b = 4, 8|n, \\ \text{Type III} & \text{if } q = b = 3, 4|n, \\ \text{Type IV} & \text{if } q = 4, b = 2, 2|n. \end{array} \right.$$

**Theorem 91** (Sloane–Mallows–Duursma) *If  $F$  is a  $b$ -divisible virtually self-dual weight enumerator with length  $n$  and minimum distance  $d$ , then*

$$d \leq \begin{cases} b\lceil \frac{n}{b(b+1)} \rceil + b & \text{if } F \text{ is Type 1,} \\ b\lceil \frac{n}{b(b+2)} \rceil + b & \text{if } F \text{ is Type 2.} \end{cases} \quad (4.3.1)$$

*In particular,*

$$d \leq \begin{cases} 2\lfloor n/8 \rfloor + 2 & \text{if } F \text{ is Type I,} \\ 4\lfloor n/24 \rfloor + 4 & \text{if } F \text{ is Type II,} \\ 3\lfloor n/12 \rfloor + 3 & \text{if } F \text{ is Type III,} \\ 2\lfloor n/6 \rfloor + 2 & \text{if } F \text{ is Type IV.} \end{cases}$$

*Proof* This is only stated for self-dual codes, but the proof of Theorem 1 and the argument in Sect. 1.1 of Duursma [D3] hold more generally for virtually self-dual weight enumerators. A complete proof is given in Appendix 7.4 below.  $\square$

**Definition 92** A virtually self-dual weight enumerator  $F$  is called *extremal* if the bound in Theorem 91 holds with equality.

*Remark 8*

- Here is a more general definition. Let  $G$  be a subgroup of  $GL(2, \mathbb{C})$  containing  $\sigma = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 0 & -1 \end{pmatrix}$ , acting on  $\mathbb{C}[x, y]$  by  $\sigma : F(x, y) \mapsto F(\sigma(x, y)^t)$ , and  $\chi : G \rightarrow \mathbb{C}^\times$  a character. Call a virtual weight enumerator  $F$  of length  $n$  a *formally  $\chi$ -self-dual weight enumerator*, or a *virtually self-dual weight enumerator twisted by  $\chi$* , if<sup>4</sup>

$$F(x, y) = \chi(\sigma) F\left(\frac{x + (q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right).$$

The virtually self-dual weight enumerator definition above is the special case where  $\chi$  is a trivial. This “twisted” definition also covers, for example, the case of Ozeki’s “formal weight enumerators” in [O]. For brevity, we call  $F$  a *twisted virtually self-dual weight enumerator* if it satisfies

$$F(x, y) = -F\left(\frac{x + (q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}}\right). \quad (4.3.2)$$

Much of the theory of zeta functions for virtually self-dual weight enumerators also applies to twisted virtually self-dual weight enumerators. See Chinen [Ch1, Ch2] and Sect. 4.8 below.

---

<sup>4</sup>This “twisted” terminology is motivated by terminology in automorphic forms and arithmetical algebraic geometry for analogous objects.

- Note that a virtual weight enumerator does not depend on a prime power  $q$  but a virtually self-dual weight enumerator does depend on  $q$  through (2.2.1).

**Definition 93** A virtual weight enumerator  $F$  is formally identified with an object we call a *virtual code*  $C$  subject only to the following condition: we formally extend the definition of  $C \mapsto A_C$  to all virtual codes by  $A_C = F$ . Of course, if  $F$  is the weight enumerator of an actual code, say  $C'$ , then we have  $A_C = F = A_{C'}$ . In other words, a virtual code is only well defined up to formal equivalence. If  $C_1$  and  $C_2$  are virtual codes, then we define  $C_1 + C_2$  to be the virtual code associated to the virtual weight enumerator  $A_{C_1}(x, y) + A_{C_2}(x, y)$ .

The following question is really more a question of the classification of self-dual codes than of virtually self-dual weight enumerators. An excellent reference is the book [NRS].

**Open Problem 18** Given a virtually self-dual weight enumerator  $F$ , find necessary and sufficient conditions (short of enumeration) which determine whether or not  $F$  arises as the weight enumerator of some self-dual code  $C$ .

## 4.4 The Zeta Polynomial

We shall give three definitions of the zeta polynomial, all due to Duursma.

### 4.4.1 First Definition

**Definition 94** A polynomial  $P(T)$  for which

$$\frac{(xT + (1-T)y)^n}{(1-T)(1-qT)} P(T) = \dots + \frac{A_C(x, y) - x^n}{q-1} T^{n-d} + \dots$$

is called a *Duursma zeta polynomial* of  $C$ .

The *Duursma zeta function* is defined in terms of the zeta polynomial by means of (4.2.1) above.

**Lemma 95** If we expand  $\frac{(xT+y(1-T))^n}{(1-T)(1-qT)}$  in powers of  $T$ , we find that it is equal to

$$\begin{aligned} & b_{0,0}y^n T^0 + (b_{1,1}xy^{n-1} + b_{1,0}y^n)T^1 + (b_{2,2}x^2y^{n-2} + b_{2,1}xy^{n-1} + b_{2,0}y^n)T^2 \\ & + \dots + (b_{n-d,n-d}x^{n-d}y^d + b_{n-d,n-d-1}x^{n-d-1}y^{d+1} + \dots + b_{n-d,0}y^n)T^{n-d} \\ & + \dots, \end{aligned}$$

where  $b_{i,j}$  are the coefficients given by

$$b_{k,\ell} = \sum_{i=\ell}^k \frac{q^{k-i+1} - 1}{q - 1} \binom{n}{i} \binom{i}{\ell}$$

for  $0 \leq \ell \leq k \leq n - d$  and  $b_{k,\ell} = 0$  otherwise.

*Proof* Use (4.4.2) below and compare the coefficients.  $\square$

**Proposition 96** *The Duursma zeta polynomial  $P = P_C$  exists and is unique, provided that  $d^\perp \geq 2$ .*

*Proof* This is proven in the appendix to Chinen [Ch2]. Here is the rough idea. Expand  $\frac{(xT + y(1-T))^n}{(1-T)(1-qT)}$  in powers of  $T$ , as in Lemma 95 above. The Duursma polynomial is a polynomial of degree  $n + 2 - d - d^\perp$ . Provided that  $d^\perp \geq 2$ , the Duursma polynomial can be written as  $P(T) = a_0 + a_1T + \dots + a_{n-d}T^{n-d}$ . Now, use

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

to express the coefficients by means of the matrix equation  $B \cdot \vec{a} = \vec{A}$  given by

$$\begin{pmatrix} b_{0,0} & b_{1,0} & \dots & b_{n-d,0} \\ 0 & b_{1,1} & \dots & b_{n-d,1} \\ 0 & 0 & b_{2,2} & \dots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & b_{n-d,n-d} \end{pmatrix} \begin{pmatrix} a_{n-d} \\ a_{n-d-1} \\ \vdots \\ a_0 \end{pmatrix} = \begin{pmatrix} A_n/(q-1) \\ A_{n-1}/(q-1) \\ \vdots \\ A_d/(q-1) \end{pmatrix}. \quad (4.4.1)$$

Thanks to Lemma 95 above, we know that the diagonal entries of this matrix are binomial coefficients,  $b_{i,i} = \binom{n}{i}$ , hence are nonzero. Therefore the matrix is invertible, and the existence is established.  $\square$

Here is a corollary of the proof. (These identities are given in [D5] as (5) and (6); see also (4.1) of [D4].)

**Corollary 97** (Duursma) *If  $d^\perp \geq 2$ , then  $P(0) = (q-1)^{-1} \binom{n}{d}^{-1} A_d$ , and*

$$\frac{A_{d+1}}{q-1} = \binom{n}{d+1} (P(0)(q-d) + P'(0)).$$

In particular,  $P$  always has a nonzero positive constant coefficient.

*Proof* By the above proof,  $b_{n-i,n-i}$  is the  $i$ th binomial coefficient, and so the first equation follows from the system of equations in (4.4.1).

The second equation follows similarly, so its proof is omitted.  $\square$



**Example 98** Consider the self-dual code  $C$  of length  $n = 6$ , dimension  $k = 3$ , and minimum distance  $d = 2$ . This is unique up to equivalence and has weight enumerator  $W(x, y) = x^6 + 3x^4y^2 + 3x^2y^4 + y^6$ . The SAGE commands

SAGE

```
sage: q,T,x,y = var("q,T,x,y")
sage: f1 = lambda q,T,N:
    sum([ sum([q^i for i in range(k+1)])*T^k for k in range(N)])
sage: f2 = lambda x,y,T,n:
    sum([ binomial(n,j)*(x-y)^j*y^(n-j)*T^j for j in range(n+1)])
sage: a0,a1,a2,a3,a4 = var("a0,a1,a2,a3,a4")
sage: F = expand(f1(2,T,6)*f2(x,y,T,6)*(a0+a1*T+a2*T^2+a3*T^3+a4*T^4))
```

compute the first 6 terms (as a power series in  $T$ ) of the series  $\frac{(xT+y(1-T))^n}{(1-T)(1-qT)}P(T)$  when  $q = 2$ ,  $n = 6$ ,  $k = 3$ , and  $d = 2$ . Next, we compute the coefficients and read off the matrix  $B$ :

SAGE

```
sage: aa = (F.coeff("T^4")).coeffs("x")
sage: v = [expand(aa[i][0]/y^(6-i)) for i in range(5)]
sage: B0 = [v[0].coeff("a%s"%str(i)) for i in range(5)]
sage: B1 = [v[1].coeff("a%s"%str(i)) for i in range(5)]
sage: B2 = [v[2].coeff("a%s"%str(i)) for i in range(5)]
sage: B3 = [v[3].coeff("a%s"%str(i)) for i in range(5)]
sage: B4 = [v[4].coeff("a%s"%str(i)) for i in range(5)]
sage: B0.reverse(); B1.reverse(); B2.reverse(); B3.reverse(); B4.reverse()
sage: B = matrix([B0,B1,B2,B3,B4])
sage: B

[ 1 -3 4 -2 1]
[ 0 6 -12 12 0]
[ 0 0 15 -15 15]
[ 0 0 0 20 0]
[ 0 0 0 0 15]
```

Note that the diagonal entries are binomial coefficients.

Finally, we compute the vector  $\vec{A}$  and solve the equation  $B \cdot \vec{a} = \vec{A}$ :

SAGE

```
sage: Wmx6 = 3*x^4*y^2+3*x^2*y^4+y^6
sage: c = [Wmx6(1,y).coeff("y%s"%str(i)) for i in range(2,7)]
sage: c.reverse()
sage: A = vector(c)
sage: (B^(-1)*A).list()
[4/5, 0, 0, 0, 1/5]
```

This implies that the zeta function of  $C$  is given by  $P(T) = \frac{1}{5} + \frac{4}{5}T^4$ .

Duursma has given several definitions (all equivalent of course) of  $P(T)$ . Before stating another one, we need the following definition and lemma.

**Definition 99** Define  $c_j$  by

$$\frac{(xT + (1-T)y)^n}{(1-T)(1-qT)} = \sum_{k=0}^{\infty} c_k(x, y) T^k.$$

Define  $M_{n,\delta}$  by

$$M_{n,\delta}(x, y) = x^n + (q - 1)c_{n-\delta}(x, y).$$

This is called the *MDS virtual weight enumerator of length  $n$  and distance  $\delta$* .

It is not hard to see that

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

and of course

$$(xT + (1-T)y)^n = \sum_{i=0}^n \binom{n}{i} y^{n-i} (x-y)^i T^i.$$

Therefore,

$$c_k(x, y) = \sum_{i+j=k} \frac{q^{j+1}-1}{q-1} \binom{n}{i} y^{n-i} (x-y)^i. \quad (4.4.2)$$

A version of the following result is stated in Duursma [D5] (see his (9)).

**Lemma 100** *If  $F$  is a virtual weight enumerator of length  $n$  and minimum distance  $d$ , then there are coefficients  $c \in \mathbb{Q}$  and  $a_i = a_j(F) \in \mathbb{Q}$  such that*

$$F(x, y) = cx^n + a_0 M_{n,d}(x, y) + a_1 M_{n,d+1}(x, y) + \cdots + a_r M_{n,d+r}(x, y) \quad (4.4.3)$$

for some  $r$ ,  $0 \leq r \leq n - d$ . In fact,  $c = 1 - a_0 - \cdots - a_r$ .

*Proof* The functions  $M_{n,d+i}(x, y) - x^n$  form a basis for the vector space  $V = \{\sum_{i=d}^n b_i x^{n-i} y^i \mid b_i \in \mathbb{Q}\}$ .

Consider the equation

$$\begin{aligned} F(x, y) - x^n &= a_0(M_{n,d}(x, y) - x^n) + a_1(M_{n,d+1}(x, y) - x^n) \\ &\quad + \cdots + a_r(M_{n,d+r}(x, y) - x^n). \end{aligned}$$

If  $r = \dim(V) - 1$ , then one can solve for the  $a_0, \dots, a_r$ . Without loss of generality, we may take  $r \geq 0$  to be as small as possible. We have then

$$\begin{aligned} F(x, y) &= (1 - a_0 - \cdots - a_r)x^n + a_0 M_{n,d}(x, y) + a_1 M_{n,d+1}(x, y) + \cdots \\ &\quad + a_r M_{n,d+r}(x, y). \end{aligned} \quad \square$$

*Example 101* We use SAGE [S] to compute examples.

When  $q = 2$ ,

$$M_{10,5}(x, y) = -34y^{10} + 220xy^9 - 585x^2y^8 + 840x^3y^7 - 630x^4y^6 + 252x^5y^5 + x^{10},$$

and when  $q = 3$ ,

$$M_{12,5}(x, y) = -48y^{12} + 1152xy^{11} - 2376x^2y^{10} + 8360x^3y^9 - 7920x^4y^8 \\ + 9504x^5y^7 - 3696x^6y^6 + 1584x^7y^5 + x^{12}.$$

The negative coefficients in these polynomials are consistent with the fact that for codes of dimension greater than 1, the length of an MDS code satisfies the bound  $n \leq q + k - 1$  (see, for example, pages 12–13 in [TV]). In the first example, a  $[10, 6, 5]_2$  code must satisfy  $10 \leq 2 + 6 - 1$  (so it does not exist), and, in the second example, a  $[12, 8, 5]_3$  code must satisfy  $12 \leq 3 + 8 - 1$  (so it does not exist).

On the other hand, when  $q = 13$ ,

$$M_{12,5}(x, y) = 312177312y^{12} + 312178752xy^{11} + 143076384x^2y^{10} \\ + 39755760x^3y^9 + 7436880x^4y^8 + 1007424x^5y^7 \\ + 88704x^6y^6 + 9504x^7y^5 + x^{12}.$$

Indeed, according to SAGE's `ReedSolomonCode` command, there is an MDS code  $C$  having parameters  $[12, 8, 5]_{13}$ :

SAGE

```
sage: C = ReedSolomonCode(12, 8, GF(13))
sage: C.spectrum()

[1,
 0,
 0,
 0,
 0,
 9504,
 88704,
 1007424,
 7436880,
 39755760,
 143076384,
 312178752,
 312177312]
```

This SAGE session tells us that

$$\text{spec}(C) = [1, 0, 0, 0, 0, 9504, 88704, 1007424, 7436880, 39755760, 143076384, \\ 312178752, 312177312],$$

as the above (independently obtained) computation implies.

These virtual weight enumerators are computed using the following SAGE code:

SAGE

```

sage: R = PolynomialRing(QQ, 2, "xy")
sage: x, y = R.gens()
sage: f = lambda q, n, m : \
    (x*T+y*(1-T))^(n)*sum([T^i for i in range(m)]) \
    *sum([(q*T)^i for i in range(m)])
sage: M = lambda q, n, d, m : (f(q, n, m).list())[d]*(q-1)+x^n

```

As long as  $m$  is taken to be sufficiently large, this code will return the correct value of  $M_{n,d}$ .

*Example 102* The Duursma zeta function of the  $[2^r - 1, 2^r - r - 1, 3]$ -Hamming code,  $\text{Ham}(r, GF(2))$ , can be computed using the following SAGE commands:

SAGE

```

sage: C = HammingCode(3, GF(2))
sage: C.zeta_function()
(2/5*T^2 + 2/5*T + 1/5)/(2*T^2 - 3*T + 1)
sage: C = HammingCode(4, GF(2))
sage: C.zeta_function()
(16/429*T^6 + 16/143*T^5 + 80/429*T^4 + 32/143*T^3 \
+ 30/143*T^2 + 2/13*T + 1/13)/(2*T^2 - 3*T + 1)

```

In other words,

$$Z_{\text{Ham}(3, GF(2))}(T) = \frac{\frac{1}{5}(2T^2 + 2T + 1)}{2T^2 - 3T + 1},$$

and

$$Z_{\text{Ham}(4, GF(2))}(T) = \frac{\frac{1}{429}(16T^6 + 48T^5 + 80T^4 + 96T^3 + 90T^2 + 66T + 33)}{2T^2 - 3T + 1}.$$

*Example 103* The Duursma zeta function of the maximal binary linear self-dual doubly even code of length 8 can be computed using the following different SAGE commands:

SAGE

```

sage: MS = MatrixSpace(GF(2), 4, 8)
sage: G =
MS([[1,1,1,1,0,0,0,0],[0,0,1,1,1,1,0,0],[0,0,0,0,1,1,1,1],
    [1,0,1,0,1,0,1,0]])
sage: C = LinearCode(G)
sage: C
Linear code of length 8, dimension 4 over Finite Field of size 2
sage: C.zeta_function()

```

```
(2/5*T^2 + 2/5*T + 1/5) / (2*T^2 - 3*T + 1)
sage: C.sd_zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: C == C.dual_code()
True
```

In other words,

$$P_C(T) = (2T^2 + 2T + 1)/5.$$

### 4.4.2 Second Definition

Here is Duursma's second definition of the zeta polynomial.

**Definition 104** Let  $F = A_C$  denote the weight enumerator of a  $[n, k, d]_q$ -code  $C$ . Using the coefficients  $a_j = a_j(F)$  of (4.4.3), define

$$P(T) = P_C(T) = a_0 + a_1T + \cdots + a_rT^r.$$

This  $P(T)$  is the *Duursma zeta polynomial* of  $C$ .

More generally, if  $F$  is an virtual weight enumerator and the coefficients  $a_j = a_j(F)$  are as in (4.4.3), define  $P(T) = P_F(T) = a_0 + a_1T + \cdots + a_rT^r$ .

Note that by comparing coefficients of  $x^n$  on both sides of (4.4.3), we see that  $a_0 + \cdots + a_r = 1$  is equivalent to  $P(1) = 1$ .

*Example 105* Note that if  $C$  is an MDS code of length  $n$  and minimum distance  $d$  over  $GF(q)$ , then  $A_C = M_{n,d}$  (this is proven as part of the discussion in Sect. 2 of Duursma [D2]). This forces  $c = 0$ ,  $a_0 = 1$  in (4.4.3), so<sup>5</sup>  $P(t) = 1$ .

*Remark 9* Note that  $[n, k, d]$  makes sense as parameters of a virtual weight enumerator when  $F$  is a weight enumerator of an actual code  $C$  (so  $F = A_C$ ) or when  $F$  is a virtually self-dual weight enumerator (so  $\gamma = n/2 - d + 1$ , where  $n$  and  $d$  are as in Definition 88) or a virtual MDS code (so  $k = n + 1 - d$ ).

**Lemma 106** *The Duursma zeta function of Definition 94 is the same as the Duursma zeta function of Definition 104.*

*Proof* By Definition 99, the zeta polynomial of Definition 94 associated to  $F = A_C$  is  $T^r$  if you replace  $F = A_C$  by  $F = M_{n,d+j}$ :

$$\frac{(xT + (1-T)y)^n}{(1-T)(1-qT)} T^j = \cdots + \frac{M_{n,d+j}(x, y) - x^n}{q-1} T^{n-d} + \cdots.$$

---

<sup>5</sup>See also Duursma's Proposition 1 in [D5] and Chinen's Theorem 3.2 in [Ch3].

Multiply by  $a_j$  and sum both sides over  $j \in \{0, \dots, r\}$  to obtain Definition 104. Therefore,  $P(T)$  satisfying Definition 94 also satisfies Definition 104.  $\square$

### 4.4.3 Third Definition

In preparation for the third definition, which originated in Sect. 7 of Duursma [D1], we introduce some notation.

Let  $C$  be an  $[n, k, d]_q$  code, let  $S \subset \{1, 2, \dots, n\}$  be a subset, let  $C_S$  denote the subcode of  $C$  of codewords with support contained in  $S$ , and let  $k_S = k_S(C)$  denote the dimension of  $C_S$ .

**Lemma 107** *The dimension  $k_S$  satisfies*

$$k_S = \begin{cases} 0 & \text{for } 0 \leq |S| < d, \\ k - (n - |S|) & \text{for } n - d^\perp < |S| \leq n. \end{cases}$$

When  $d \leq |S| \leq n - d^\perp$ , then  $k_S$  depends on  $S$  and  $C$  in a more subtle way.

*Proof* It follows from the definition of the minimum distance  $d$  that  $k_S = 0$  if  $0 \leq |S| < d$ . If  $C$  is  $[n, k, d]$ , then the dual code  $C^\perp$  is  $[n, n - k, d^\perp]$ , so  $n - k + d^\perp \leq n + 1$ , or  $d^\perp \leq k + 1$ . If  $S^c = \{j \mid 1 \leq j \leq n, j \notin S\}$ , then  $C_S$  is isomorphic to the code “shortened on  $S^c$ .” The dimensions of such shortened codes are given in Theorem 1.5.7 in [HP1]. In particular, if  $|S^c| < d^\perp$ , then we find  $k_S = n - |S^c| - (n - k) = k - |S^c|$ , as desired.  $\square$

The *binomial moments* of  $C$  are the integers  $B_0^1, B_1^1, B_2^1, \dots$  defined by

$$B_i^1 = B_i^1(C) = \sum_{|S|=i} \frac{q^{k_S} - 1}{q - 1}.$$

**Lemma 108** *The binomial moments satisfy*

$$B_i^1 = \begin{cases} 0 & \text{for } 0 \leq i < d, \\ \binom{n}{i} \frac{q^{i+k-n-1}}{q-1} & \text{for } n - d^\perp < i \leq n. \end{cases}$$

*Proof* This is an easy corollary of the above lemma.  $\square$

The numbers

$$b_i = b_i(C) = B_{d+i}^1 / \binom{n}{d+i} \quad (4.4.4)$$

are called the *normalized binomial moments* of  $C$  ( $0 \leq i \leq n - d$ ). We extend this to all  $i \in \mathbb{Z}$  by

$$b_i = b_i(C) = \begin{cases} 0 & \text{for } i < 0, \\ \frac{q^{i+d+k-n}-1}{q-1} & \text{for } n-d^\perp - d < i. \end{cases}$$

Finally, we can give Duursma's third definition.

**Definition 109** Define the *zeta function* of  $C$  to be the generating function of the normalized binomial moments of the code:

$$Z(T) = \sum_{i=0}^{\infty} b_i T^i.$$

This is a rational function (see Duursma [D1], Sect. 7),

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

where

$$P(T) = a_0 + a_1 T + \cdots + a_{n+2-d-d^\perp} T^{n+2-d-d^\perp}$$

is the zeta polynomial, and

$$a_i = b_i - (q+1)b_{i-1} + qb_{i-2}. \quad (4.4.5)$$

**Lemma 110** *The Duursma zeta function of Definition 109 is the same as the Duursma zeta function of Definition 94.*

*Proof* If

$$B^1(x, y) = \sum_{j=0}^n B_j^1 x^{n-j} y^j$$

and  $A_C(x, y) = x^n + (q-1)A^1(x, y)$ , then it is known<sup>6</sup> that  $B^1(x, y) = A^1(x + y, y)$ . Therefore,  $\frac{A_C(x, y) - x^n}{q-1} = B^1(x - y, y)$  and

$$(zT + y)^n Z(T) = \cdots + B^1(z, y)T^{n-d} + \cdots$$

(where  $z = x - y$ ) defines the Duursma zeta polynomial of  $C$  in the sense of Definition 94. Let us compare coefficients of  $z^\ell T^{n-d}$  on both sides. On the right-hand side, it is  $B_{n-\ell}^1$ , and on the other side, it is  $\binom{n}{\ell} b_{n-d-\ell}$ . We must verify that these are

---

<sup>6</sup>This is proven in Sect. 9 of [D5]. See Theorem 1.1.26 and Exercise 1.1.27 in [TV] for a closely related result.

the same. However, this is the formula for the normalized binomial moment and so is, by definition, true.  $\square$

As a corollary, we find that if the weight enumerator  $A_C$  is known, then

$$B^1(x, y) = \frac{A_C(x + y, y) - (x + y)^n}{q - 1} = \sum_{j=0}^n B_j^1 x^{n-j} y^j$$

is easy to compute, and the coefficients of the zeta polynomial are given by (4.4.4) and (4.4.5). (In fact, this is what the SAGE command `zeta_polynomial` computes.)

SAGE

```
sage: C = HammingCode(3, GF(2))
sage: C.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: C = best_known_linear_code(6, 3, GF(2))
sage: C.minimum_distance()
3
sage: C.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
```

#### 4.4.4 Analogies with Curves

Let  $X$  be a smooth projective curve of genus<sup>7</sup>  $g$  over a finite field  $GF(q)$ . Suppose that  $X$  is defined by a polynomial equation  $F(x, y) = 0$ , where  $F$  is a polynomial with coefficients in  $GF(q)$ . Let  $N_k$  denote the number of solutions in  $GF(q^k)$  and create the generating function

$$G(t) = N_1 t + N_2 t^2 / 2 + N_3 t^3 / 3 + \cdots.$$

Define the zeta function of  $X$  by the formal power series

$$\zeta(t) = \zeta_X(t) = \exp(G(t)), \quad (4.4.6)$$

so  $Z(0) = 1$ . In particular, the logarithmic derivative of  $\zeta(t)$  has integral coefficients. It is known that<sup>8</sup>

$$\zeta_X(t) = \frac{p(t)}{(1-t)(1-qt)}$$

<sup>7</sup>These terms will not be defined precisely here. Please see Tsafman and Vladut [TV], Sect. 2.3.2, or Schmidt [Sc] for a rigorous treatment.

<sup>8</sup>This was first proved by Dwork using  $p$ -adic methods [Dw].



with  $p = p_X$  a polynomial of degree  $2g$ , where  $g$  is the genus of  $X$ . This has a “functional equation” of the form

$$p(t) = q^g t^{2g} p\left(\frac{1}{qt}\right).$$

The logarithmic derivative of  $\zeta_X$  is the generating function of the sequence of counting numbers  $\{N_1, N_2, \dots\}$ . The Riemann hypothesis for curves over finite fields states that the roots of  $P$  have absolute value  $q^{-1/2}$ . It is well known that the Riemann hypothesis holds for  $\zeta_X$  (so the roots of zeta function of a curve all have absolute value  $1/\sqrt{q}$ ; this is a theorem of André Weil from the 1940s). Therefore, by a suitable change-of-variable (replacing  $t$  by  $t/\sqrt{q}$ ), we see that curves over finite fields give rise to a large class of example of polynomials having roots on the unit circle. The paper of Kedlaya discusses approaches to finding such polynomials whose coefficients satisfy some arithmetic conditions.

These roots can be interpreted in terms of the eigenvalues of a linear transformation<sup>9</sup> on a vector space. In fact, there is a unitary symplectic  $2g \times 2g$  matrix  $\Theta = \Theta_X$  such that<sup>10</sup>

$$p(t) = \det(I - tq^{1/2}\Theta).$$

When  $C$  is a formally self-dual AG code (associated to a smooth projective curve  $X$  of genus  $g$  over a finite field, a divisor  $D$  on  $X$  and points  $\{P_i\}$  on  $X$  disjoint from  $D$ ; see, for example, [TV, TVN]) of genus  $g$  (as a code), the Duursma polynomial  $P = P_C$  “often” has the same degree as  $p = p_X$  and satisfies the same functional equation. One can see using Theorem 4.1.28 in [TVN] that such codes are rather easy to construct, so this situation is not too unusual. This motivates the following question.

**Open Problem 19** Let  $C$  be a formally self-dual code over  $GF(q)$ . When is there a curve  $X/GF(q)$  for which the zeta function of the curve  $\zeta_X$  is equal (up to a constant factor, if necessary) to the zeta function  $Z_C$  of the code?

Since the Riemann hypothesis holds for  $\zeta_X$ , a necessary condition for Open Question 19 to hold is that the Duursma zeta function of the code must satisfy the Riemann hypothesis. Generally, the Duursma zeta function of a self-dual code does not satisfy the Riemann hypothesis, but see Example 9.7 in [D6] for two (self-dual) codes for which this holds. Here is a SAGE computation which verifies this:<sup>11</sup>

<sup>9</sup>In fact, it is possible to interpret  $P(t)$  in terms of the characteristic function of “the Frobenius operator” acting on a cohomology space, though we shall omit details here.

<sup>10</sup>See Faifman and Rudnick [FR] for an interesting analysis of the “statistics” of the eigenvalues of  $\Theta$  in the case where  $X$  is “hyperelliptic.”

<sup>11</sup>The reciprocal of the numerator of the  $\zeta$ -function of a curve is the characteristic polynomial of the Frobenius endomorphism of the Jacobian, i.e., the Frobenius polynomial.

SAGE

```

sage: K = GF(2)
sage: E = EllipticCurve(K, [0,1,1,-2,0]); E
Elliptic Curve defined by y^2 + y = x^3 + x^2 over Finite Field
of size 2
sage: E.trace_of_frobenius()
-2
sage: E.frobenius_polynomial()
x^2 + 2*x + 2

```

*Remark 10* However, there are other reasons to question that these zeta functions agree except in unusual circumstances. For example, using Sect. 3.1.1 (especially, Corollary 3.1.13) in [TVN], one sees that  $p(1)/p(0) = q/h$ , where  $h$  is the so-called class number of  $X$  (which is the number of  $GF(q)$ -rational points on the Jacobian of  $X$ , [TVN], p. 135). On the other hand,  $P(0)/P(1)$  is given in Corollary 97 above. It is possible that  $q/h = (q-1)^{-1} \binom{n}{d}^{-1} A_d$ , but, if true, this is highly nonintuitive.

Alain Connes and others have worked on a natural spectral interpretation of the zeros of the Riemann zeta function. In other words, one wants to construct a self-adjoint operator on a Hilbert space whose spectrum is the set of nontrivial zeros of the Riemann zeta function. In the analogy between the Riemann zeta function and the Hasse–Weil zeta function of a curve  $X$ , the analog of this self-adjoint operator is the Frobenius operator on a certain cohomology space. The next open question asks is there an analog for Duursma zeta functions as well?

**Open Problem 20** Let  $C$  be a self-dual code over  $GF(q)$ . When is there a linear operator  $\Phi$  on a “natural” rational vector space for which the zeta polynomial  $P = P_C$  can be interpreted in terms of the characteristic function of  $\Phi$ ?

The coefficients of the logarithmic derivative of the Hasse–Weil zeta function of a curve  $X/GF(q)$  are integers—they count the number of points of  $X$  over a certain extension field of  $GF(q)$ . Is there an analog for the Duursma zeta function?

**Open Problem 21** Let  $C$  be a self-dual code over  $GF(q)$ . Is there a “natural” interpretation of the coefficients of the logarithmic derivative of  $Z_C$ ? Does the logarithmic derivative of  $Z_C(T)$  have integral coefficients?

There is a “natural” interpretation of the coefficients of  $P_C$ —see the construction in Sect. 4.4.3 above.

## 4.5 Properties

We survey some of the most remarkable properties, both conjectured and proven, of these zeta functions.

### 4.5.1 The Functional Equation

If  $\gamma = \gamma(C)$  is the genus of  $C$  and if

$$z_C(T) = Z_C(T)T^{1-\gamma},$$

then the functional equation in [D1] can be written in the form

$$z_{C^\perp}(T) = z_C(1/qT).$$

If we let

$$\zeta_C(s) = Z_C(q^{-s})$$

and

$$\xi_C(s) = z_C(q^{-s}),$$

then  $\zeta_C$  and  $\xi_C$  have the same zeros, but  $\xi_C$  is “more symmetric” since the functional equation expressed in terms of it becomes<sup>12</sup>

$$\xi_{C^\perp}(s) = \xi_C(1-s).$$

Abusing terminology, we call both  $Z_C$  and  $\zeta_C$  the *Duursma zeta function* of  $C$ .

The analog of this for a virtually self-dual weight enumerator is as follows: let  $F$  denote a virtually self-dual weight enumerator with degree  $n$  and minimum distance  $d$ , so  $\gamma = n + 1 - k - d = n/2 + 1 - d$  is the genus.

In fact, since Duursma’s zeta function *only* depends on  $C$  via its weight enumerator  $A_C(x, y)$  of  $C$ , for any virtual weight enumerator  $F(x, y)$ , there is an associated *zeta function*  $Z = Z_F$  and *zeta polynomial*  $P = P_F$ . If we define  $F^\perp$  by  $F^\perp = F \circ \sigma$ , where

$$\sigma = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix},$$

then there is a functional equation relating  $Z$  and  $Z^\perp = Z_{F^\perp}$  (and hence also  $P$  and  $P^\perp = P_{F^\perp}$ ). Note that even though  $F$  may not depend on  $q$ ,  $F^\perp$  (and hence  $Z^\perp$ ) does.

**Proposition 111** *For any virtual weight enumerator  $F$  satisfying*

$$F(x, y) = a_0 M_{n,d}(x, y) + a_1 M_{n,d+1}(x, y) + \cdots + a_r M_{n,d+r}(x, y)$$

*and for any  $q$ , the zeta function  $Z = Z_F$  satisfies the functional equation*

$$Z^\perp(T)T^{1-g^\perp} = Z\left(\frac{1}{qT}\right)\left(\frac{1}{qT}\right)^{1-g}. \quad (4.5.1)$$

---

<sup>12</sup>This notation is inspired by analogous notation used for functions associated with the classical Riemann zeta function. See any book on the Riemann zeta function or [http://en.wikipedia.org/wiki/Riemann\\_zeta\\_function](http://en.wikipedia.org/wiki/Riemann_zeta_function).

Analogously, the zeta polynomial  $P = P_F$  satisfies the functional equation

$$P^\perp(T) = P\left(\frac{1}{qT}\right) q^g T^{g+g^\perp}, \quad (4.5.2)$$

where  $g = n/2 + 1 - d$  and  $g^\perp = n/2 + 1 - d^\perp$ .

*Remark 11* (1) Note that both  $P^\perp$  and  $P$  are polynomials of degree  $n + 2 - d - d^\perp = g + g^\perp$  and  $g$  is the genus if  $F = A_C$  is an actual weight enumerator.

(2) This proof is essentially the same as that of Proposition 9.2 in [D6]. This hypothesis here is slightly more general.

*Proof* This is a consequence of Definition 104 and the MacWilliams identity.

By hypothesis, the coefficients  $a_j = a_j(F)$  of (4.4.3) satisfy  $a_0 + \dots + a_r = 1$ . Therefore,  $F^\perp = F \circ \sigma$  satisfies

$$F^\perp = a_0 M_{n,d} \circ \sigma + a_1 M_{n,d+1} \circ \sigma + \dots + a_r M_{n,d+r} \circ \sigma. \quad (4.5.3)$$

Recall that the dual of the MDS code with parameters  $[n, k, \delta]$  is the MDS code with parameters  $[n, k^\perp, \delta^\perp]$ . By this and MacWilliams' identity, we have  $M_{n,\delta} \circ \sigma = q^{n/2+1-\delta} M_{n,\delta^\perp} = q^{k-n/2} M_{n,\delta^\perp}$ , where  $k^\perp + \delta^\perp = n + 1$ , and  $k = n - \delta + 1$  is the dimension of the (virtual) MDS code of length  $n$  and minimum distance  $\delta$  (for a proof of this, see Appendix A in Duursma [D5]). Thus,  $M_{n,\delta} \circ \sigma = q^{n/2+1-\delta} M_{n,n-\delta+2}$ , and it follows that

$$\begin{aligned} F^\perp &= \sum_{d \leq \delta \leq d+r} a_{\delta-d} q^{n/2+1-\delta} M_{n,n-\delta+2} \\ &= \sum_{n-d-r+2 \leq \delta' \leq n-d+2} a_{n-\delta'+2-d} q^{\delta'-1-n/2} M_{n,\delta'} \\ &= \sum_{0 \leq \delta'' \leq r} a_{r-\delta''} q^{n/2-d-r+1+\delta''} M_{n,n-d-r+2+\delta''}. \end{aligned}$$

This implies

$$\begin{aligned} P^\perp(T) &= a_0^\perp + a_1^\perp T + \dots + a_r^\perp T^r \\ &= a_r q^{n/2-r-d+1} + a_{r-1} q^{n/2-r-d+2} T + \dots + a_0 q^{n/2-d+1} T^r \\ &= a_r q^{n/2-r-d+1} + a_{r-1} q^{n/2-r-d+1} (Tq) + \dots + a_0 q^{n/2-r-d+1} (Tq)^r \\ &= q^{n/2-r-d+1} (a_r + a_{r-1} (Tq) + \dots + a_0 (Tq)^r) \\ &= q^{n/2-r-d+1} (Tq)^r (a_0 + a_1 (Tq)^{-1} + \dots + a_r (Tq)^{-r}) \\ &= q^{n/2-d+1} T^r P(1/qT). \end{aligned}$$

□

### 4.5.2 Puncturing Preserves $P$

Suppose that  $C$  is an  $[n, k, d]$  code over  $GF(q)$  and  $i$  is any integer satisfying  $1 \leq i \leq n$ . The *punctured code*  $P_i(C)$  at the coordinate  $i$  is the code having length  $n - 1$  obtained by projecting  $C$  onto the remaining coordinates. The *shortened code*  $S_i(C)$  at the coordinate  $i$  is the code having length  $n - 1$  obtained by projecting the subcode

$$\{c = (c_1, \dots, c_n) \in C \mid c_i = 0\}$$

onto the remaining coordinates.

**Lemma 112** *If  $C$  is a linear code of length  $n$  and  $i$  is an integer,  $1 \leq i \leq n$ , then*

$$P_i(C)^\perp = S_i(C^\perp).$$

A *check-bit extension*  $\hat{C}$  is a code of length  $n + 1$  of the form

$$\{(c_1, \dots, c_n, c_{n+1}) \in GF(q)^{n+1} \mid (c_1, \dots, c_n) \in C, c_{n+1} = c \cdot a\}$$

for some fixed vector  $a \in GF(q)^n$ .

To end this section, we recall that the zeta polynomial of a code  $C$ ,  $P_C$ , remains the same if we replace  $C$  by (a) the averaged puncturing  $P(C)$  of  $C$ , (b) the averaged shortening  $S(C)$  of  $C$ , or (c) a check-bit extension  $\hat{C}$  of  $C$ . These facts provide inductive formulas for computing the zeta polynomial.

**Theorem 113** (Duursma [D5]) *If  $C$  is a linear code of length  $n$ , if*

$$F_{P(C)}(x, y) = \frac{1}{n} \sum_{i=1}^n A_{P_i(C)}(x, y)$$

*denotes the averaged punctured weight enumerator, and if*

$$F_{S(C)}(x, y) = \frac{1}{n} \sum_{i=1}^n A_{S_i(C)}(x, y)$$

*denotes the averaged shortened weight enumerator, then*

$$P_C(T) = P_{F_{P(C)}}(T) = P_{F_{S(C)}}(T).$$

This is proven in Sect. 5 of Duursma [D5].

### 4.5.3 The Riemann Hypothesis

Knowledge of the zeros of  $Z(T)$  could be very useful for understanding the possible values of the minimum distance. Let  $C$  be a code which is not MDS. If  $\rho_1, \rho_2, \dots, \rho_r$

denote the zeros, counted according to multiplicity, of the Duursma zeta polynomial  $P(T)$  of a linear code  $C$ , then

$$\frac{P'(T)}{P(T)} = \sum_i \frac{1}{T - \rho_i}.$$

**Proposition 114** (Duursma) *If  $[A_0, \dots, A_n]$  denotes the spectrum of  $C$ , then*

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

*In particular,*

$$d \leq q - \sum_i \rho_i^{-1}.$$

The proof uses the assumption that  $C$  is an actual linear code, not a virtual code, and that  $P(T) \neq 1$ .

*Proof* For the first statement, see Corollary 97. The second statement follows from the first since  $\frac{A_{d+1}}{A_d} \geq 0$ .  $\square$

In particular, if  $C$  is any  $b$ -divisible code with  $b \geq 2$ , then

$$d = q - \sum_i \rho_i^{-1}. \quad (4.5.4)$$

If  $F$  is a virtually self-dual weight enumerator, then the zeros of the zeta function  $\zeta_F(s)$  (or  $\xi_F(s)$ ) occur in pairs about the “critical line”  $\operatorname{Re}(s) = \frac{1}{2}$ .

**Definition 115** We say the zeta function  $\zeta_F$  (or, by abuse of terminology, the virtually self-dual weight enumerator  $F$ ) satisfies the *Riemann hypothesis* (if all zeta zeros occur on the “critical line.”

The following result is not best possible, but illustrates the idea that for “large”  $q$ , the Riemann hypothesis is “often” false.

**Corollary 116** *Let  $C$  be an  $[n, k, d]$  code over  $GF(q)$  with  $A_{d+1} = 0$ ,  $q > n^2$ ,  $2 \leq d$ , and  $d + d^\perp < n + 2$ . If  $n > 3$ , then the Duursma zeta polynomial is not a constant and does not satisfy the Riemann hypothesis.*

This is an easy consequence<sup>13</sup> of Proposition 114, and the proof is left to the reader. The hypotheses to this corollary are probably not best possible. The point is that it should not be hard to construct codes which violate the Riemann hypothesis.

---

<sup>13</sup>Assume that the Riemann hypothesis is true and  $q > n^2$ . Then show that the hypothesis contradicts the trivial estimate  $q - d \leq |\sum_i \rho_i^{-1}| \leq r\sqrt{q} = (n + 2 - d - d^\perp)\sqrt{q}$ .

*Example 117* It is clear from Example 105 above that the Duursma zeta function may have no zeros (i.e., may be constant). Indeed, this is true for all MDS codes, including some formally self-dual ones.<sup>14</sup>

*Remark 12* Let  $F$  denote a virtually self-dual weight enumerator as in Proposition 111, and let  $r(T) = z_F(T/\sqrt{q})$ . The functional equation implies that  $r(T)$  is a self-reciprocal function:  $r(1/T) = r(T)$ . The Riemann hypothesis is the statement that all  $2\gamma$  zeros of  $r(T)$  lie on the “critical line”  $|T| = 1$ . If  $r_0(\theta) = r(e^{i\theta})$ , then the functional equation and the fact that  $r$  has rational coefficients imply

$$r_0(\theta) = r_0(-\theta) = \overline{r_0(\theta)}.$$

In other words,  $r_0(\theta)$  is real valued.

The following open question is all the more tantalizing because we actually know (thanks to Duursma [D3]) explicitly the Duursma zeta functions of all extremal virtually self-dual weight enumerators.

**Open Problem 22** (Duursma) For all extremal virtual (self-dual) weight enumerators  $F$ , the zeta function  $Z = Z_F$  satisfies the Riemann hypothesis.

This is the *Riemann hypothesis* for virtually self-dual weight enumerators.

**Lemma 118** Let  $F$  denote a virtually self-dual weight enumerator of genus  $\gamma$  as above, and let  $P = P_F$  denote the associated zeta polynomial. It is known that  $P(T^2/q) = T^{2\gamma} f(T + T^{-1})$ , where  $f \in \mathbb{R}[x]$  is a polynomial of degree  $2\gamma$  with real coefficients.

*Proof* See Duursma [D3], Theorem 7 and Lemma 10. □

## 4.6 Self-reciprocal Polynomials

Thanks to the functional equation for the Duursma zeta polynomial, the validity of the Riemann hypothesis for a self-dual code (more generally a virtual self-dual weight enumerator) can be reduced to the question of whether or not a related polynomial has all its zeros on the unit circle. This section contains some of the basic results known about zeros of self-reciprocal polynomials on the unit circle.

---

<sup>14</sup>Formally self-dual MDS codes exist—see Example 12 in [JKT], which gives a formally self-dual  $[42, 21, 22]$ -code over a very large extension of  $GF(7)$ . (In fact, this code even has  $A_5$  as its permutation automorphism group.) Even better, in Kim and Lee [KL], a self-dual MDS code with parameters  $[10, 5, 6]_{41}$  is constructed.

### 4.6.1 “Smoothness” of Roots

A natural question to ask about zeros of polynomials is how “smoothly” do they vary as functions of the coefficients of the polynomial?

To address this, suppose that the coefficients  $a_i$  of the polynomial  $p$  are functions of a real parameter  $t$ . Abusing notation slightly, identify  $p(z) = p(t, z)$  with a function of two variables ( $t \in \mathbb{R}$ ,  $z \in \mathbb{C}$ ). Let  $r = r(t)$  denote a root of this polynomial, regarded as a function of  $t$ :

$$p(t, r(t)) = 0.$$

Using the two-dimensional chain rule,

$$0 = \frac{d}{dt} p(t, r(t)) = p_t(t, r(t)) + r'(t) \cdot p_z(t, r(t)),$$

so  $r'(t) = -p_t(t, r(t))/p_z(t, r(t))$ . Since  $p_z(t, r(t)) = p'(r)$ , the denominator of this expression for  $r'(t)$  is zero if and only if  $r$  is a double root of  $p$  (i.e., a root of multiplicity 2 or more).

In answer to the above question, we have proven the following result on the “smoothness of roots.”

**Lemma 119**  *$r = r(t)$  is smooth (i.e., continuously differentiable) as a function of  $t$ , provided that  $t$  is restricted to an interval on which  $p(t, z)$  has no double roots.*

Consider the distance function

$$d(t) = |r(t)|$$

of the root  $r$ . Another natural question is: How smooth is the distance function of a root as a function of the coefficients of the polynomial  $p$ ?

The analog to Lemma 119 holds with one extra condition.

**Lemma 120**  *$d(t) = |r(t)|$  is smooth (i.e., continuously differentiable) as a function of  $t$ , provided that  $t$  is restricted to an interval one which  $p(t, z)$  has no double roots and  $r(t) \neq 0$ .*

*Proof* This is basically an immediate consequence of the above lemma and the chain rule,

$$\frac{d}{dt} |r(t)| = r'(t) \cdot \left( \frac{d|x|}{dx} \Big|_{x=r(t)} \right). \quad \square$$

### 4.6.2 Variations on a Theorem of Eneström–Kakeya

The following theorem was discovered independently by Eneström (in the late 1800s) and Kakeya (in the early 1900s).



**Theorem 121** (Eneström–Kakeya, Version 1) *Let  $f(T) = a_0 + a_1T + \cdots + a_kT^k$  satisfy  $a_0 > a_1 > \cdots > a_k > 0$ . Then  $f(T)$  has no roots in  $|T| \leq 1$ .*

*Remark 13* Replacing the polynomial by its reverse, here is “version 2” of the Eneström–Kakeya theorem: Let  $f(z) = a_0 + a_1z + \cdots + a_kz^k$  satisfy  $0 < a_0 < a_1 < \cdots < a_k$ . Then  $f(z)$  has no roots in  $|z| \geq 1$ .

An interesting discussion on the “sharpness” of this result (i.e., to what extent a converse theorem holds) can be found in Anderson, Saff, and Varga [ASV].

Below, we state Chinen’s lemma, discovered independently by W. Chen,<sup>15</sup> whose proof is sketched in the next section (see also [Ch3]).

**Corollary 122** (Chen–Chinen) *If  $f(T)$  is a degree  $m$  polynomial of “decreasing symmetric form”*

$$f(T) = a_0 + a_1T + \cdots + a_kT^k + a_kT^{m-k} + a_{k-1}T^{m-k+1} + \cdots + a_0T^m$$

*with  $a_0 > a_1 > \cdots > a_k > 0$ , then all roots of  $f(T)$  lie on the unit circle  $|T| = 1$ , provided that  $m \geq k$ .*

### 4.6.3 A Literature Survey

We recall some facts about self-reciprocal polynomials having roots on the unit circle from papers of Ancochea [An], Anderson, Saf, and Varga [ASV] Bonsall and Marden [BoM], Chen [Chen], Chinen [Ch3], DiPippo and Howe [DH], Fell [Fe], Kedlaya [Ked], S.-L. Kim [K], Kim and Park [KiP], Konvalina and Matache [KM], works of Lakatos and Losonczi [L1, L2, LL1, LL2], Petersen and Sinclair [PS], and Schiznel [Sc].

There is also a closely related body of research on Littlewood polynomials (which may have in fact motivated many of the papers listed above), for example, Drungilas [Dr] or Mercer [M]. These papers are related to the investigation of the “Littlewood problem” in connection with autocorrelation of binary sequences. However, the Littlewood polynomials are sufficiently different from the (suitably normalized) Duursma zeta polynomials that we shall have no need to refer further to those results.

For example, Lemma 2.1.1 in DiPippo and Howe [DH] provides one way of classifying those polynomials of even degree in  $\mathbb{R}[x]$  which have all its roots on the unit circle. That result is discussed below following some preliminary definitions.

A polynomial  $p$  of the form

$$p(z) = \sum_{j=0}^m a_j z^j,$$

---

<sup>15</sup>Actually, Chen found a somewhat stronger result—see Theorem 134 below for a special case.

where  $m \geq 1$ ,  $a_m \neq 0$ ,  $a_0, \dots, a_m \in \mathbb{C}$ , and  $a_j = a_{m-j}$  ( $0 \leq j \leq m/2$ ), is called a *self-reciprocal polynomial* of degree  $m$ . Define the *reciprocal* or *reverse* polynomial of  $p$  by

$$p^*(z) = z^{\deg(p)} \cdot p(1/z), \quad (4.6.1)$$

where  $p$  is a polynomial of degree  $\deg(p)$ . Denote by  $\mathbb{R}[z]_m$  the polynomials of degree  $\leq m$  with real coefficients.

$$\mathbb{R}[z]_m = \{p \in \mathbb{R}[z] \mid \deg(p) \leq m\}. \quad (4.6.2)$$

Denote by  $R_m$  the self-reciprocal polynomials of degree  $\leq m$  with real coefficients,

$$R_m = \{p \in \mathbb{R}[z]_m \mid p = p^*\}.$$

If  $p$  is a self-reciprocal polynomial of degree  $2n$ , then

$$p(z) = \sum_{j=0}^{2n} a_j z^j = z^n [a_{2n}(z^n + z^{-n}) + \dots + a_{n+1}(z + z^{-1}) + a_n].$$

This shows that if  $\beta$  is a zero of  $p$ , then so is  $1/\beta$ .

The following statement is proven in Lakatos [L2]:

**Lemma 123** *For each  $p \in R_{2n}$  of degree  $2n$  with  $a_{2n} \neq 0$ , there are  $n$  real numbers  $\alpha_1, \dots, \alpha_n$  such that*

$$p(z) = a_{2n} \prod_{k=0}^n (z^2 - \alpha_k z + 1). \quad (4.6.3)$$

The *Chebyshev transformation*  $T : R_{2n} \rightarrow \mathbb{R}[z]_n$  is defined on the subset<sup>16</sup> of polynomials of degree  $2n$  by

$$T_p(x) = a_{2n} \prod_{k=0}^n (x - \alpha_k),$$

where  $x = z + z^{-1}$ , and  $p$  and  $\alpha_i$  are as in (4.6.3).

The following statement is proven in Lakatos [L2].

**Lemma 124** *The Chebyshev transformation  $T : R_{2n} \rightarrow \mathbb{R}[z]_n$  is a vector space isomorphism.*

---

<sup>16</sup>For simplicity, in this definition, we assume that  $a_{2n} \neq 0$ ; see [L2] for the general definition of  $T$ .

For any  $X_i \in \mathbb{C}$  ( $1 \leq i \leq n$ ), let

$$\begin{aligned}
 e_0(X_1, X_2, \dots, X_n) &= 1, \\
 e_1(X_1, X_2, \dots, X_n) &= \sum_{1 \leq j \leq n} X_j, \\
 e_2(X_1, X_2, \dots, X_n) &= \sum_{1 \leq j < k \leq n} X_j X_k, \\
 e_3(X_1, X_2, \dots, X_n) &= \sum_{1 \leq j < k < l \leq n} X_j X_k X_l, \\
 &\vdots \\
 e_n(X_1, X_2, \dots, X_n) &= X_1 X_2 \cdots X_n.
 \end{aligned}$$

The following result is proven in Losonczi [Los].

**Lemma 125** *For all  $n \geq 1$  and  $\alpha_i \in \mathbb{C}$ , we have*

$$\prod_{k=0}^n (z^2 - \alpha_k z + 1) = \sum_{k=1}^{2n} c_{2n,k} z^k,$$

where  $c_{2n,k} = c_{2n,2n-k}$  and

$$c_{2n,k} = (-1)^k \sum_{\ell=1}^{\lfloor k/2 \rfloor} \binom{n-k+2\ell}{\ell} e_{k-2\ell}(\alpha_1, \dots, \alpha_n)$$

for  $0 \leq k \leq n$ .

The following statement is proven in DiPippo and Howe [DH] (and found independently by Losonczi [Los]).

**Lemma 126** *A polynomial  $p \in R_{2n}$  has all its zeros on the unit circle if and only if there are  $n$  real numbers  $\alpha_1, \dots, \alpha_n$  in the interval  $[-2, 2]$  such that (4.6.3) holds.*

*Remark 14* If  $p(z) \in R_n$  is a self-reciprocal monomial polynomial having all its coefficients lying on the unit circle, then  $p$  is determined by its  $n-1$  coefficients. The topology and volume of those coefficients, regarded as a subset of  $\mathbb{R}^{n-1}$ , were recently determined by Petersen and Sinclair [PS].

Here is a different characterization, discovered by A. Cohn, of self-reciprocal polynomials having all roots on the unit circle.

**Theorem 127** (Schur–Cohn) *Let  $p(z)$  be a self-reciprocal polynomial of degree  $n$ . Suppose that  $p(z)$  has exactly  $r$  zeros on the unit circle (counted according to multiplicity) and exactly  $s$  critical points in the closed unit disc (counted according to multiplicity). Then  $r = 2(s + 1) - n$ .*

According to Chen [Chen], the above result of Cohn, published in 1922, is closely related<sup>17</sup> to a result of Schur, published in 1918. The following beautiful result is an immediate consequence.

**Corollary 128** *A self-reciprocal polynomial has all its zeros on the unit circle if and only if all the zeros of its derivative lie inside or on the unit circle.*

See also Bonsall and Marsden [BoM] and Ancochea [An] (where they reprove a result of Cohn closely related to the theorem above).

There are various results in these papers which are, roughly speaking, stated as follows: if  $p(z) \in R_{2n}$  is “near” a nonzero constant multiple of  $1 + z + \cdots + z^{2n}$ , then  $p$  has all its zeros on the unit circle. Here is an example of such a statement from Lakatos [L1].

**Theorem 129** (Lakatos) *The polynomial  $p \in R_{2n}$  given by*

$$p(z) = \ell(z^{2n} + z^{2n-1} + \cdots + z + 1) + \sum_{k=1}^n a_k(z^{2n-k} + z^k)$$

*has all its roots on the unit circle if the coefficients satisfy the following condition:*

$$|\ell| \geq 2 \sum_{k=1}^n |a_k|.$$

A similar result holds for the odd-degree case (see [LL2]).

A statement in a similar framework, also due to Lakatos, is the following.

**Theorem 130** (Lakatos) *The polynomial  $p \in R_m$  given by*

$$p(z) = \sum_{j=0}^m a_j z^j$$

*has all its roots on the unit circle if the coefficients satisfy the following condition:*

$$|a_m| \geq \sum_{j=0}^m |a_j - a_m|.$$

---

<sup>17</sup>In fact, both are exercises in Marden [Ma].

*Remark 15* (1) This result was generalized by Schiznel in 2005 [Scl] (the term  $|a_j - a_m|$  was replaced by a more general linear combination).

(2) Of course, if  $p(z)$  is very near the polynomials  $1 + z + \cdots + z^m$ , then the differences  $a_j - a_m$  are very small, and the hypothesis obviously holds. In particular, this implies that self-reciprocal polynomials that are very near the polynomials  $1 + z + \cdots + z^m$  have all their zeros on the unit circle.

*Example 131* For example, according to SAGE,  $f(z) = 1 + z + z^3 + z^4$  and  $f(z) = 1 + z + z^2 + z^2 + z^4 + z^5 + z^6$  have *all* their roots on the unit circle, but  $f(z) = 1 + z + 2z^2 + 2z^4 + z^5 + z^6$  has only *some* (2 of its 6) roots on the unit circle.

Here is a detailed simple example to try to give some intuitive insight into the unusual results in the previous two theorems.

*Example 132* Consider the polynomial

$$f_t(z) = 1 + (1 + t) \cdot z + z^2,$$

where  $t \in \mathbb{R}$  is a parameter. Let  $R(t)$  denote the set of roots of  $f_t$ , so

$$R(t) = \left\{ \frac{-1 - t \pm \sqrt{(1+t)^2 - 4}}{2} \right\},$$

and let

$$r(t) = \max_{z \in R(t)} \{|z|\}$$

be the size of the largest root. We plot this function  $r(t)$ . The claim is that  $r(t)$  is not “smooth.”

Note that if  $0 < t < 1$ , we have

$$r(t) = \left| \frac{-1 - t \pm i\sqrt{4 - (1+t)^2}}{2} \right| = \left( \frac{(1+t)^2}{4} + \frac{4 - (1+t)^2}{4} \right)^{1/2} = 1.$$

The plot<sup>18</sup> of  $r(t)$  in the range  $-5 < t < 3$  is in Fig. 4.1. This plot suggests that  $r(t)$  is not differentiable. Indeed, if  $t > 1$ , then  $r(t) = \frac{-1-t+\sqrt{(1+t)^2-4}}{2}$ , so

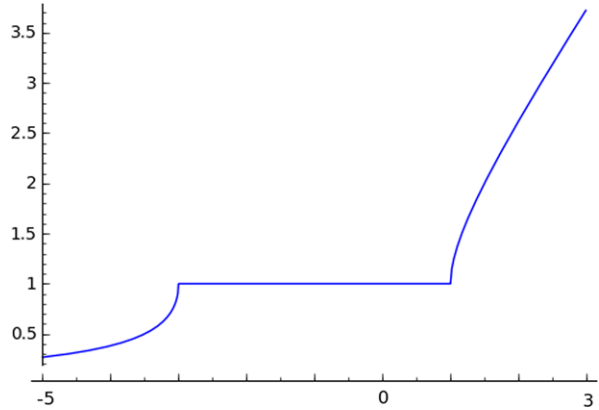
$$r'(t) = -\frac{1}{2} + \frac{1+t}{\sqrt{(1+t)^2-4}}.$$

Note that  $\lim_{t \rightarrow 1+} r'(t) = \infty$ .

---

<sup>18</sup>The plot was created using SAGE’s list\_plot command, though the axes labels were modified using GIMP for ease of reading.

**Fig. 4.1** Size of the largest root of the polynomial  $1 + (1+t)z + z^2$ ,  $-5 < t < 3$



We will return to this topic in Sect. 4.6.1.

**Corollary 133** Consider a formally self-dual code  $C$  with associated zeta polynomial  $P(T) = \sum_{i=0}^{2g} a_i T^i$  and “normalized” (self-reciprocal) zeta polynomial  $R(T) = P(T/\sqrt{q})$ . Write  $R(T) = a_0 \sum_{i=0}^{2g} c_i T^i$ . If

$$\sum_{k=1}^n |c_k - 1| \leq \frac{1}{2},$$

then  $R$  has all its roots on the unit circle.

*Remark 16* Note that  $c_0 = c_{2g} = 1$  and that  $c_i = a_i q^{-i/2} / a_0$  can in turn be related to the weights  $A_i$  via (4.4.1). Therefore, the above hypothesis implies a sort of growth condition on the coefficients  $a_i$  of  $P$  and hence also on the weights.

Recall that for a given polynomial  $g(x)$  of degree  $d$ ,  $g^*(x) = x^d g(1/x)$  denotes the reciprocal polynomial. Note that if  $f(x) = x^r g(x) + g^*(x)$ , then  $f^*(x) = f(x)$  ( $r \geq 0$ ).

The following is basically the theorem of Chen and Chinen (Corollary 122).

**Theorem 134** If  $0 < a_0 < \dots < a_{k-1} < a_d$ , then the roots of  $x^r g(x) + g^*(x)$  all lie on the unit circle,  $r \geq 0$ .

*Proof* We shall adapt some ideas from Chinen [Ch3] for our argument.

Write  $f(T)$  as in (4.6.4) as

$$f(T) = g(T) + h(T),$$

where  $g(T) = a_0 + a_1 T + \dots + a_k T^k$  and  $h(T) = a_k T^{m-k} + a_{k-1} T^{m-k+1} + \dots + a_0 T^m$ . Given a polynomial  $g(x)$ , let  $g^*(x) = x^k g(1/x)$  denote the reverse (or reciprocal) polynomial. Note that  $h(T) = T^m g(T^{-1}) = T^{m-k} g^*(T)$  and  $f^*(T) = f(T)$ .

**Claim**  $g^*(T)$  has no roots in  $|T| \leq 1$ .

*Proof* This is equivalent to the statement of the Eneström–Kakeya theorem (Theorem 121).  $\square$

**Claim**  $g(T)$  has no roots in  $|T| \geq 1$ .

*Proof* This follows from the previous claim and the observation that the roots of  $g(T)$  correspond to the inverses of the roots of  $g^*(T)$ .  $\square$

**Claim**  $|g(T)| < |g^*(T)|$  on  $|T| < 1$ .

*Proof* By the above claims, the function  $\phi(T) = g(T)/g^*(T)$  is holomorphic on  $|T| \leq 1$ . Since  $g(T^{-1}) = \overline{g^*(T)}$  on  $|T| = 1$ , we have  $|g(T)| = |g^*(T)|$  on  $|T| = 1$ . The claim follows from the maximum modulus principle.  $\square$

**Claim** The roots of  $T^r g(T) + g^*(T)$  all lie on the unit circle,  $r \geq 0$ .

*Proof* By the previous claim,  $T^r g(T) + g^*(T)$  has the same number of zeros as  $g^*(T)$  in the unit disc  $|T| < 1$  (indeed, the function  $\frac{T^r g(T) + g^*(T)}{g^*(T)} = 1 + \frac{T^r g(T)}{g^*(T)}$  has no zeros). Since  $g^*(T)$  has no roots in  $|T| < 1$ , neither does  $T^r g(T) + g^*(T)$ . But since  $T^r g(T) + g^*(T)$  is self-reciprocal (in this case), it has no zeros in  $|T| > 1$  either.  $\square$

This proves Theorem 134.  $\square$

Here is a result which shows, in some sense, how close the Duursma zeta functions of extremal virtual codes are to polynomials which have *no* roots on the unit circle.

**Lemma 135** Let  $f \in R_{2n}$ ,  $f(x) = \sum_{i=0}^d c_i z^i$ ,  $d$  even,  $c_0 < c_1 < \cdots < c_{d/2-1} < c_{d/2}$ . If  $2c_{d/2-1} < c_{d/2}$ , then  $f$  has no roots on the unit circle. Conversely, if  $f$  has no roots on the unit circle, then  $2c_0 < c_{d/2}$ .

For the converse, see Corollary 2 in Mercer [M]. For the proof of  $\implies$ , we introduce the *Chebyshev polynomials* (of the first kind)  $T_k$  defined by

$$T_k(\cos \theta) = \cos(k\theta)$$

and their normalization  $C_k(x) = 2T_k(x/2)$ . It is known that

$$C_k(z + z^{-1}) = z^k + z^{-k}, \quad k > 0,$$

and we use the convention  $C_0(x) = 1$ .

*Proof* We can write

$$\begin{aligned} \frac{f(z)}{z^{d/2}} &= z^{d/2} c_0 (z^{d/2} + z^{-d/2}) + z^{d/2} \sum_{j=1}^{d/2-1} c_j (z^j + z^{d-j}) \\ &= \sum_{j=0}^{d/2} c_j C_{d/2-j} (z + z^{-1}). \end{aligned}$$

If  $z = e^{i\theta}$ , then

$$\begin{aligned} \sum_{j=0}^{d/2} c_j C_{d/2-j} (2 \cos \theta) &= c_{d/2} + 2 \sum_{j=0}^{d/2} c_j \cos((d/2 - j)\theta) \\ &= \operatorname{Real} \left[ 2 \sum_{j=0}^{d/2} c_j \exp(i(d/2 - j)\theta) - c_{d/2} \right] \\ &= \operatorname{Real} \left[ 2 \sum_{j=0}^{d/2} c_j z^{d/2-j} - c_{d/2} \right]. \end{aligned}$$

If  $2c_{d/2-1} < c_{d/2}$ , then the Eneström–Kakeya theorem (Theorem 121) applies.  $\square$

If  $P_0(z)$  and  $P_1(z)$  are polynomials, let

$$P_a(z) = (1 - a)P_0(z) + aP_1(z)$$

for  $0 \leq a \leq 1$ .

Next, we recall an interesting characterization due to Fell [Fe] (see also Kim [K] for discussion on a similar topic).

**Theorem 136** (Fell) *Let  $P_0(z)$  and  $P_1(z)$  be real monic polynomials of degree  $n$  having zeros in  $S^1 - \{1, -1\}$ . Denote the zeros of  $P_0(z)$  by  $w_1, w_2, \dots, w_n$  and of  $P_1(z)$  by  $z_1, z_2, \dots, z_n$ . Assume that*

$$w_i \neq z_j$$

*for  $1 \leq i, j \leq n$ . Assume also that*

$$0 < \arg(w_i) \leq \arg(w_j) < 2\pi,$$

$$0 < \arg(z_i) \leq \arg(z_j) < 2\pi,$$

*for  $1 \leq i \leq j \leq n$ . Let  $A_i$  be the smaller open arc of  $S^1$  bounded by  $w_i$  and  $z_i$  for  $1 \leq i \leq n$ . Then the locus of  $P_a(z)$ ,  $0 \leq a \leq 1$ , is contained in  $S^1$  if and only if the arcs  $A_i$  are all disjoint.*



### 4.6.4 Duursma's Conjecture

We say that a polynomial satisfying the condition

$$f(T) = a_0 + a_1T + \cdots + a_kT^k + a_kT^{m-k} + a_{k-1}T^{m-k+1} + \cdots + a_0T^m \quad (4.6.4)$$

with  $a_k > a_{k-1} > \cdots > a_0 > 0$  has *increasing symmetric form*.<sup>19</sup>

If  $m = 2k$  or  $m = 2k + 1$ , then we say that  $f(T)$  has *full support*.

There is an infinite family of Duursma zeta functions for which Duursma has conjectured that the analog of the Riemann hypothesis always holds. The linear codes used to construct these zeta functions are the so-called “extremal self-dual codes” (see Definition 92 for the more general notion of an extremal self-dual weight enumerator).

Although the construction of these codes is fairly technical (see [JK2] for an expository treatment), we can give some examples. They turn out to be of increasing symmetric form.

*Example 137* Let  $r(T) = \sum_i r_i T^i$  be as in Remark 12.

Some examples of the lists of coefficients  $r_0, r_1, \dots$  computed using SAGE. We have normalized the coefficients so that they sum to 10 and represented the rational coefficients as decimal approximations to give a feeling for their relative sizes.

- Case Type I:
  - $m = 2$ : [1.1309, 2.3990, 2.9403, 2.3990, 1.1309]
  - $m = 3$ : [0.45194, 1.2783, 2.0714, 2.3968, 2.0714, 1.2783, 0.45194]
  - $m = 4$ : [0.18262, 0.64565, 1.2866, 1.8489, 2.0724, 1.8489, 1.2866, 0.64565, 0.18262]
- Case Type II:
  - $m = 2$ : [0.43425, 0.92119, 1.3028, 1.5353, 1.6129, 1.5353, 1.3028, 0.92119, 0.43425]
  - $m = 3$ : [0.12659, 0.35805, 0.63295, 0.89512, 1.1052, 1.2394, 1.2854, 1.2394, 1.1052, 0.89512, 0.63295, 0.35805, 0.12659]
  - $m = 4$ : [0.037621, 0.13301, 0.28216, 0.46554, 0.65783, 0.83451, 0.97533, 1.0656, 1.0967, 1.0656, 0.97533, 0.83451, 0.65783, 0.46554, 0.28216, 0.13301, 0.037621]
- Case Type III:
  - $m = 2$ : [1.3397, 2.3205, 2.6795, 2.3205, 1.3397]
  - $m = 3$ : [0.58834, 1.3587, 1.9611, 2.1836, 1.9611, 1.3587, 0.58834]
  - $m = 4$ : [0.26170, 0.75545, 1.3085, 1.7307, 1.8874, 1.7307, 1.3085, 0.75545, 0.26170]

<sup>19</sup>The analogous definition of a polynomial of *decreasing symmetric form* also holds. The statement is left to the reader. The Eneström–Kakeya theorem implies (see Chinen's Theorem 122) that a polynomial of decreasing symmetric form has all its zeros on the unit circle.

- Case Type IV:  
 $m = 2$ : [2.8571, 4.2857, 2.8571]  
 $m = 3$ : [1.6667, 3.3333, 3.3333, 1.6667]  
 $m = 4$ : [0.97902, 2.4476, 3.1469, 2.4476, 0.97902]

Some remarks on the data in Example 137.

- Case Type I,  $\nu = 0$ : We conjecture that the coefficients of the (self-reciprocal) polynomial  $R(T) = \sum_i r_i T^i$ , where

$$\sum_i \binom{4m}{m+i} r_i T^i = (1 + T/\sqrt{2})^m (1 + \sqrt{2}T)^m = (1 + 3T/\sqrt{2} + T^2)^m,$$

have increasing symmetric form and full support.

- Case Type II,  $\nu = 0$ : We conjecture that the (self-reciprocal) polynomial  $R(T) = \sum_i r_i T^i$ , where

$$\sum_i \binom{6m}{m+i} r_i T^i = (1 + 2T/\sqrt{2} + T^2)^m (1 + 3T/\sqrt{2} + T^2)^m,$$

has increasing symmetric form and full support.

- Case Type III,  $\nu = 0$ : We conjecture that the (self-reciprocal) polynomial  $R(T) = \sum_i r_i T^i$ , where

$$\sum_i \binom{4m}{m+i} r_i T^i = (1 + 3T/\sqrt{3} + T^2)^m$$

has increasing symmetric form and full support.

- Case Type VI,  $\nu = 0$ : We conjecture that the (self-reciprocal) polynomial  $R(T) = \sum_i r_i T^i$ , where

$$\sum_i \binom{3m}{m+i} r_i T^i = (1 + T)^m,$$

has increasing symmetric form and full support. The right-hand side has this property by well-known properties of the binomial coefficients.

#### 4.6.5 A Conjecture on Zeros of Cosine Transforms

Are there conditions under which self-reciprocal polynomials with “increasing symmetric form” have all their zeros on  $S^1$ ?

We know that self-reciprocal polynomial with “decreasing symmetric form” have all their roots on  $S^1$  (by the Chen–Chinen theorem above). Under what conditions is the analogous statement true for functions with “increasing symmetric form?” The remainder of this section considers this question following [Jo2].

Let  $d$  be an odd integer, and let  $f(z) = f_0 + f_1z + \cdots + f_{d-1}z^{d-1} \in R_{d-1}$  be a self-reciprocal polynomial with “increasing symmetric form”

$$0 < f_0 < f_1 < \cdots < f_{\frac{d-1}{2}}.$$

For each  $c \geq f_{\frac{d-1}{2}}$ , the polynomial

$$g(z) = c \cdot (1 + z + \cdots + z^{d-1}) - f(z) = g_0 + g_1z + \cdots + g_{d-1}z^{d-1} \in R_{d-1}$$

is a self-reciprocal polynomial having nonnegative coefficients with “decreasing symmetric form.” If  $c > f_{\frac{d-1}{2}}$ , the Chen–Chinen theorem (Theorem 134) implies that all the zeros of  $g(z)$  are on  $S^1$ . Let

$$P_0(z) = g(z)/g_{d-1}, \quad P_1(z) = f(z)/f_{d-1}, \quad P_a(z) = (1-a)P_0(z) + aP_1(z),$$

for  $0 \leq a \leq 1$ . By the Chen–Chinen theorem, there is a  $t_0 \in (0, 1)$  such that all zeros of  $P_t(z)$  are on  $S^1$  for  $0 \leq t < t_0$ . In fact, if

$$t = \frac{f_{\frac{d-1}{2}} - f_{d-1}}{f_{\frac{d-1}{2}}},$$

then  $P_t(z)$  is a multiple of  $1 + z + \cdots + z^{d-1}$ .

Do any of the polynomials  $P_t(z)$  have multiple roots ( $0 < t < 1$ )? Using the notation of Sect. 4.6.1, in the case  $p(t, z) = P_t(z)$ , we have

$$r'(t) = -p_t(t, r(t))/p_z(t, r(t)) = \frac{P_1(r(t)) - P_0(r(t))}{P'_t(r(t))}.$$

If no  $P_t(z)$  has a multiple root, then by the second “smoothness-of-roots lemma” (Lemma 120), all the roots of  $f(z)$  are also on  $S^1$ .

**Conjecture 138** Let  $s : \mathbb{Z}_{>0} \rightarrow \mathbb{R}_{>0}$  be a “slowly increasing” function.

- *Odd-degree case.* If  $g(z) = a_0 + a_1z + \cdots + a_dz^d$ , where  $a_i = s(i)$ , then the roots of  $p(z) = g(z) + z^{d+1}g^*(z)$  all lie on the unit circle.
- *Even-degree case.* The roots of

$$p(z) = a_0 + a_1z + \cdots + a_{d-1}z^{d-1} + a_dz^d + a_{d-1}z^{d+1} + \cdots + a_1z^{2d-1} + a_0z^{2d}$$

all lie on the unit circle.

Using SAGE, one can guess that “logarithmic growth” might be “sufficiently slow.”

SAGE

```
sage: R.<T> = PolynomialRing(CC, "T")
sage: c = [ln(j+2+random()) for j in range(5)];
sage: p = add([c[j]*T^j for j in range(5)])
      +T^5*add([c[4-j]*T^j for j in range(5)]); p
```

```

0.867252631954867*T^9 + 1.29158950186183*T^8 + 1.40385316206528*T^7
+ 1.66723678619336*T^6 + 1.79685924871722*T^5 + 1.79685924871722*T^4
+ 1.66723678619336*T^3 + 1.40385316206528*T^2 + 1.29158950186183*T
+ 0.867252631954867
sage: [z[0].abs() for z in p.roots()]
[1.000000000000000, 1.000000000000000, 1.000000000000000, 1.000000000000000,
1.000000000000000, 1.000000000000000, 1.000000000000000, 1.000000000000000,
1.000000000000000]
sage: c = [ln(j+2+random()) for j in range(5)]; c[4] = c[4]/2;
sage: p = add([c[j]*T^j for j in range(5)])
+T^4*add([c[4-j]*T^j for j in range(5)]); p
1.07222251112144*T^8 + 1.34425116365361*T^7 + 1.55233692750212*T^6
+ 1.64078305774305*T^5 + 1.87422392028965*T^4 + 1.64078305774305*T^3
+ 1.55233692750212*T^2 + 1.34425116365361*T + 1.07222251112144
sage: [z[0].abs() for z in p.roots()]
[1.000000000000000, 1.000000000000000, 1.000000000000000, 1.000000000000000,
1.000000000000000, 1.000000000000000, 1.000000000000000, 1.000000000000000]

```

## 4.7 Examples

### 4.7.1 Komichi's Example

In [HT], the authors mention an example which occurred in the master thesis<sup>20</sup> of A. Komichi. It is claimed that the Duursma zeta function of the code  $C = H_8 \oplus H_8 \oplus H_8$ , where  $H_8$  is the self-dual extended Hamming [8, 4, 4]-code, violates the Riemann hypothesis. We verify this using SAGE.

```

SAGE
sage: MS = MatrixSpace(GF(2), 12, 24)
sage: G = MS([
....: [ 1,1,1,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ],\
....: [ 0,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ],\
....: [ 0,0,1,0,1,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ],\
....: [ 0,0,0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ],\
....: [ 0,0,0,0,0,0,0,0,1,1,1,0,0,0,0,1,0,0,0,0,0,0 ],\
....: [ 0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0,0 ],\
....: [ 0,0,0,0,0,0,0,0,0,0,1,0,1,1,0,1,0,0,0,0,0,0 ],\
....: [ 0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0 ],\
....: [ 0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,0,0,1 ],\
....: [ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0 ],\
....: [ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1 ],\
....: [ 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0 ]\
....: ])
sage: C = LinearCode(G)
sage: Cd = C.dual_code(); C == Cd
True
sage: R = PolynomialRing(CC, "T")
sage: T = R.gen()
sage: C.zeta_polynomial()
512/253*T^18 + 512/253*T^17 + 256/253*T^16 - 148736/245157*T^14
- 66048/81719*T^13 - 185536/245157*T^12 - 49408/81719*T^11
- 43088/96577*T^10 - 1808/5681*T^9 - 21544/96577*T^8 - 12352/81719*T^7
- 23192/245157*T^6 - 4128/81719*T^5 - 4648/245157*T^4 + 2/253*T^2
+ 2/253*T + 1/253

```

<sup>20</sup>This appears to be unpublished, and I have not seen it myself.

```

sage: f = R(C.zeta_polynomial())
sage: print [z[0].abs() for z in f.roots()]
[0.963950810639179, 0.707106781186546, 0.707106781186548,
0.707106781186546, 0.518698666447988, 0.707106781186548,
0.707106781186542, 0.707106781186548, 0.707106781186550,
0.707106781186551, 0.707106781186547, 0.707106781186546,
0.707106781186548, 0.707106781186544, 0.707106781186548,
0.707106781186549, 0.707106781186548, 0.707106781186549]
sage: P1 = list_plot([(z[0].real(),z[0].imag()) for z in f.roots()])
sage: t = var("t")
sage: pts = lambda t: [cos(t)/sqrt(2),sin(t)/sqrt(2)]
sage: P2 = parametric_plot(pts(t),0,2*pi,linestyle="--",rgbcolor=(1,0,0))
sage: show(P1+P2)

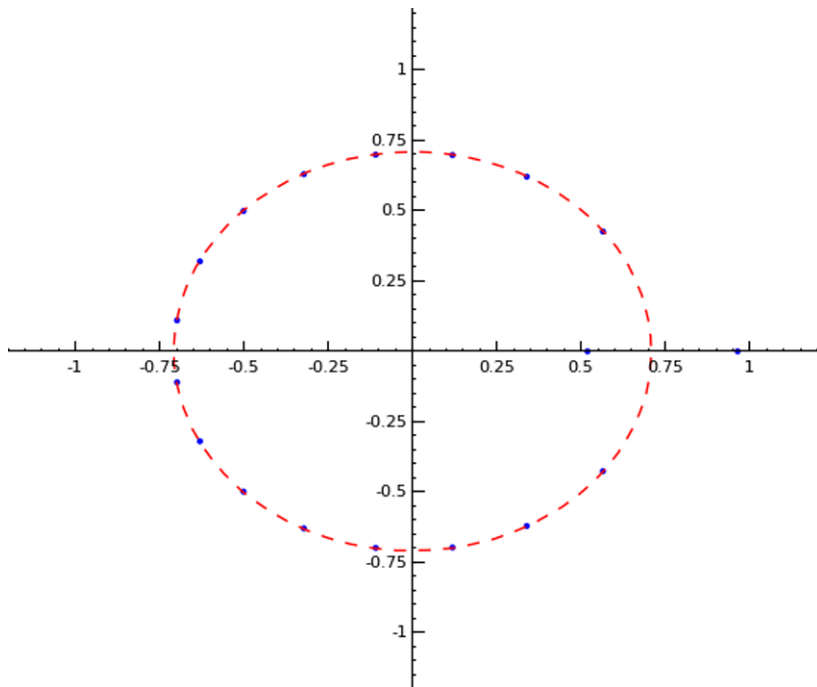
```

The plot computed in the last line is shown in Fig. 4.2.

### 4.7.2 The Extremal Case

In this section, we shall summarize some results of Duursma [D3] and Harada and Tagami [HT].

If  $F$  is an extremal virtually self-dual weight enumerator, then the zeta function  $Z = Z_F$  can be explicitly computed. First, some notation. If  $F$  is a virtually self-dual weight enumerator of minimum distance  $d$  and  $P = P_F$  is its zeta polynomial,



**Fig. 4.2** Roots of the zeta polynomial for a self-dual [24, 12, 4] binary code

then define

$$Q(T) = \begin{cases} P(T), & \text{Type I,} \\ P(T)(1 - 2T + 2T^2), & \text{Type II,} \\ P(T)(1 + 3T^2), & \text{Type III,} \\ P(T)(1 + 2T), & \text{Type IV.} \end{cases}$$

Let  $(a)_m = a(a+1) \cdots (a+m-1)$  denote the *rising generalized factorial* and write  $Q(T) = \sum_j q_j T^j$  for some  $q_j \in \mathbb{Q}$ . Let

$$\gamma_1(n, d, b) = (n-d)(d-b)_{b+1} A_d / (n-b-1)_{b+2}$$

and

$$\gamma_2(n, d, b, q) = (d-b)_{b+1} \frac{A_d}{(q-1)(n-b)_{b+1}},$$

where recall  $A_d$  denotes the coefficient of  $x^{n-d}y^d$  in the virtual weight enumerator  $F(x, y)$ .

**Theorem 139** (Duursma [D3]) *If  $F$  is an extremal virtually self-dual weight enumerator, then the coefficients of  $Q(T)$  are determined as follows.*

(a) *If  $F$  is of Type I, then*

$$\sum_{i=0}^{2m+2v} \binom{4m+2v}{m+i} q_i T^i = \gamma_1(n, d, 2) \cdot (1+T)^m (1+2T)^m (1+2T+2T^2)^v,$$

where  $m = d-3$ ,  $4m+2v = n-4$ ,  $b = q = 2$ ,  $0 \leq v \leq 3$ .

(b) *If  $F$  is of Type II, then*

$$\begin{aligned} \sum_{i=0}^{4m+8v} \binom{6m+8v}{m+i} q_i T^i \\ = \gamma_1(n, d, 2) \cdot (1+T)^m (1+2T)^m (1+2T+2T^2)^m B(T)^v, \end{aligned}$$

where  $m = d-5$ ,  $6m+8v = n-6$ ,  $b = 4$ ,  $q = 2$ ,  $0 \leq v \leq 2$ , and  $B(T) = W_5(1+T, T)$ , where  $W_5$  is as in Example 44.

(c) *If  $F$  is of Type III, then*

$$\sum_{i=0}^{2m+4v} \binom{4m+4v}{m+i} q_i T^i = \gamma_2(n, d, 3, 3) \cdot (1+3T+3T^2)^m B(T)^v,$$

where  $m = d-4$ ,  $4m+4v = n-4$ ,  $b = q = 3$ ,  $0 \leq v \leq 2$ , and  $B(T) = W_9(1+T, T)$ , where  $W_9$  is as in Example 44.

(d) If  $F$  is of Type IV, then

$$\sum_{i=0}^{m+2v} \binom{3m+2v}{m+i} q_i T^i = \gamma_2(n, d, 2, 4) \cdot (1+2T)^m (1+2T+4T^2)^v,$$

where  $m = d - 3$ ,  $3m + 2v = n - 3$ ,  $b = 2$ ,  $q = 4$ , and  $0 \leq v \leq 2$ .

It is easy to determine (especially with a computer algebra system such as SAGE) the coefficients  $q_j$  and  $p_j$  from these expressions. So, for the virtual extremal codes, Duursma has computed all the Duursma zeta functions. Yet, we *still* do not know if the Riemann hypothesis holds for them!

Define the *ultraspherical polynomial*  $C_n^m(x)$  on the interval  $(-1, 1)$  by

$$C_n^m(\cos \theta) = \sum_{\substack{0 \leq k, \ell \leq n \\ k+\ell=n}} \binom{m+k}{k} \binom{m+\ell}{\ell} \cos(k-\ell)\theta.$$

**Theorem 140** (Duursma [D3], Sect. 5.2)<sup>21</sup> If  $P$  is the Duursma zeta polynomial of an extremal Type IV virtual self-dual weight enumerator of length  $n = 3m + 3$  and minimum distance  $d = m + 3$ , then

$$Q(T^2/2) = \frac{m!^2}{(3m)!} T^m C_m^{m+1} \left( \frac{T + T^{-1}}{2} \right).$$

(Recall that, in this case,  $Q(T) = P(T)(1+2T)$ .)

It is known that all the roots of ultraspherical polynomials  $C_n^m$  lie on the interval  $(-1, 1)$ . The polynomial  $C_n^m$  is of degree  $n$ , and so there are  $n$  such roots. Replace  $T$  by  $e^{i\theta}$  in the equation displayed in the theorem above to obtain

$$Q(e^{2i\theta}/2) = \frac{m!^2}{(3m)!} e^{i\theta m} C_m^{m+1}(\cos \theta).$$

Hence, all the roots of  $Q$  and therefore also of  $P$  lie on the circle of radius  $1/\sqrt{q} = 1/2$ . Indeed, the Riemann hypothesis holds for all zeta functions associated to an extremal Type IV virtually self-dual weight enumerator (Duursma [D3]).

Let  $R(T) = P(T/\sqrt{q}) = \sum_{i=0}^{2g} r_i T^i$ . This polynomial  $R$  is self-reciprocal. Though a lot is known about self-reciprocal polynomials which have all their zeros on the unit circle, we still do not know if the  $P(T)$  satisfy the Riemann hypothesis or not! Duursma's approach is to try to describe the zeros of  $H(z)$ , where  $R(T) = T^g H(T + T^{-1})$ . By the theorem below, this function  $H$  can be explicitly described as a sum of ultraspherical polynomials. Though we know the zeros of the terms, we do not know the zeros of the sum in general. (The case of extremal codes of Type IV is different however.)

<sup>21</sup>A typo in [D3], Sect. 5.2, is corrected here.

**Theorem 141** (Duursma [D3]) *If  $\alpha_j$  ( $1 \leq j \leq g$ ) are defined by*

$$\sum_{i=0}^{2g} r_i \binom{2g+2d-4}{d-2+i} T^{2i} = T^{2g} \sum_{j=0}^g \alpha_j \binom{2j}{j}^{-1} (T + T^{-1})^{2j},$$

*then*

$$\binom{2g+2d-4}{g+d-2} \sum_{i=0}^{2g} r_i T^{2i} = T^{2g} \sum_{j=0}^g \alpha_j \binom{g+d-2}{j}^{-2} C_{2j}^{g+d-j-i} (T + T^{-1}).$$

Since  $g+d = \frac{n}{2} + 1$ , these expressions can be simplified a bit, if desired. Also, in Sect. 5.2 in [D3], Duursma explicitly computes the  $\alpha_j$ 's in each case (Type I, II, III, and IV).

Using computer computations, Harada and Tagami [HT] (among other things) showed that the Riemann hypothesis holds for all zeta functions associated to extremal Type I, II, III virtually self-dual weight enumerators of degree  $\leq 200$ .

### 4.7.3 “Random Divisible Codes”

Following Theorem 4 in Duursma [D5], we show that the Duursma zeta function of a “random divisible code” satisfies the Riemann hypothesis.

Define the (virtual) weight enumerator of the  $[n, k]_q$  random  $b$ -divisible code by

$$F(x, y) = x^n + c \sum_{i=1}^{n/b} \binom{n}{ib} (q-1)^{bi} x^{n-bi} y^{bi},$$

where  $c$  is chosen so that  $F(1, 1) = q^k$ , and  $n$  is a multiple of  $b$ . Of course, by the classification of  $b$ -divisible codes (see Theorem 89), this weight enumerator may not correspond to an actual linear code.

Duursma shows that in the following cases the zeta function  $Z_F(T)$  satisfies the Riemann hypothesis:  $n$  is even,  $k = n/2$ , and

- $q = 2, b = 4$ ,
- $q = 3, b = 3$ ,
- $q = 4, b = 2$ .

For details, see Duursma [D5], Theorem 4.

### 4.7.4 A Formally Self-dual $[26, 13, 6]_2$ -code

Moreover, in this case the Riemann hypothesis is not valid for optimal codes (which may or may not be extremal) in general, as the following example illustrates.



*Example 142* Consider the  $[26, 13, 6]_2$  code with weight distribution

$$[1, 0, 0, 0, 0, 0, 39, 0, 455, 0, 1196, 0, 2405, 0, 2405, 0, 1196, 0, 455, 0, 39, 0, 0, 0, 0, 0, 1].$$

This is (by coding theory tables, as included in SAGE [S]) an optimal formally self-dual code. This code  $C$  has the zeta polynomial

$$\begin{aligned} P(T) = & \frac{3}{17710} + \frac{6}{8855}T + \frac{611}{336490}T^2 + \frac{9}{2185}T^3 + \frac{3441}{408595}T^4 + \frac{6448}{408595}T^5 \\ & + \frac{44499}{1634380}T^6 + \frac{22539}{520030}T^7 + \frac{66303}{1040060}T^8 + \frac{22539}{260015}T^9 + \frac{44499}{408595}T^{10} \\ & + \frac{51584}{408595}T^{11} + \frac{55056}{408595}T^{12} + \frac{288}{2185}T^{13} + \frac{19552}{168245}T^{14} + \frac{768}{8855}T^{15} \\ & + \frac{384}{8855}T^{16}. \end{aligned}$$

Using SAGE, it can be checked that only 8 of the 12 zeros of this function have absolute value  $\sqrt{2}$ .

### 4.7.5 Extremal Codes of Short Length

In this section, we give some examples using SAGE.

These do not satisfy  $P(1) = 1$  but use the formulas in Theorem 139 above.

For the  $[24, 12, 8]_2$  virtually self-dual weight enumerator:

$$\begin{aligned} P(T) = & \frac{2}{969}T^{10} + \frac{2}{323}T^9 + \frac{10}{969}T^8 + \frac{4}{323}T^7 + \frac{197}{16796}T^6 + \frac{9}{988}T^5 \\ & + \frac{197}{33592}T^4 + \frac{1}{323}T^3 + \frac{5}{3876}T^2 + \frac{1}{2584}T + \frac{1}{15504}. \end{aligned}$$

For the  $[26, 13, 8]_2$  virtually self-dual weight enumerator:

$$\begin{aligned} P(T) = & \frac{32}{13167}T^{12} + \frac{32}{4389}T^{11} + \frac{4}{323}T^{10} + \frac{496}{31977}T^9 + \frac{393}{24871}T^8 + \frac{31}{2261}T^7 \\ & + \frac{281}{27132}T^6 + \frac{31}{4522}T^5 + \frac{393}{99484}T^4 + \frac{62}{31977}T^3 + \frac{1}{1292}T^2 + \frac{1}{4389}T \\ & + \frac{1}{26334}. \end{aligned}$$

For the  $[28, 14, 8]_2$  virtually self-dual weight enumerator:

$$\begin{aligned}
 P(T) = & \frac{16}{5313}T^{14} + \frac{16}{1771}T^{13} + \frac{224}{14421}T^{12} + \frac{96}{4807}T^{11} + \frac{3469}{163438}T^{10} \\
 & + \frac{291}{14858}T^9 + \frac{23}{1428}T^8 + \frac{622}{52003}T^7 + \frac{23}{2856}T^6 + \frac{291}{59432}T^5 \\
 & + \frac{3469}{1307504}T^4 + \frac{6}{4807}T^3 + \frac{7}{14421}T^2 + \frac{1}{7084}T + \frac{1}{42504}.
 \end{aligned}$$

See also Example 137.

### 4.7.6 Non-self-dual Examples

Consider the optimal binary code  $C$  having the parameters  $[6, 2, 4]$  and generator matrix

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

This has zeta polynomial  $P(T) = (2T^2 + 2T + 1)/5$ , as the following SAGE computation shows.

```

SAGE
sage: R_CC = PolynomialRing(CC, "T")
sage: n = 6; k = 2; q = 2
sage: C = best_known_linear_code(n, k, GF(q))
sage: C.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: [abs(z[0]) for z in R_CC(C.zeta_polynomial()).roots()]
[0.707106781186548, 0.707106781186548]
sage: C.weight_enumerator()
x^6 + 3*x^2*y^4
sage: Cd = C.dual_code()
sage: Cd.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: Cd.weight_enumerator()
x^6 + 3*x^4*y^2 + 8*x^3*y^3 + 3*x^2*y^4 + y^6
sage: n = 7; k = 4; q = 2
sage: C = best_known_linear_code(n, k, GF(q))
sage: C.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: C.weight_enumerator()
x^7 + 7*x^4*y^3 + 7*x^3*y^4 + y^7
sage: Cd = C.dual_code()
sage: Cd.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: Cd.weight_enumerator()
x^7 + 7*x^3*y^4

```

```

sage: n = 8; k = 4; q = 2
sage: C = best_known_linear_code(n, k, GF(q))
sage: C.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: C.weight_enumerator()
x^8 + 14*x^4*y^4 + y^8
sage: Cd = C.dual_code()
sage: Cd.zeta_polynomial()
2/5*T^2 + 2/5*T + 1/5
sage: Cd.weight_enumerator()
x^8 + 14*x^4*y^4 + y^8

```

Indeed, the optimal  $[6, 2, 4]$  code has the same zeta polynomial as the Hamming  $[7, 4, 3]$  code. This satisfies the Riemann hypothesis, although it is not formally self-dual. However, it does have the same zeta polynomial as the optimal self-dual  $[8, 4, 4]$  code.

## 4.8 Chinen Zeta Functions

In the sections above, a virtual weight enumerator  $F$  is associated with a zeta function  $Z = Z_F$ . In this section, two related zeta functions were constructed by Koji Chinen. First, he constructed a zeta function  $Z = Z_F$ , which we call a “twisted Chinen zeta function,” associated to a twisted virtually self-dual weight enumerator  $F$ . (What we call a “twisted virtually self-dual weight enumerator,” he calls a “formal weight enumerator.”) Next, he constructed a zeta function associated to any code  $C$ , which we call a “Chinen zeta function,” which is essentially defined by combining the Duursma zeta function of  $C$  with that of its dual  $C^\perp$  (some care is required to insure that the functional equation leads to an extra symmetry property).

Here is the analogous result for Chinen zeta functions of the results above.

Let  $C$  be any  $[n, k, d]$  code over  $GF(q)$ , and let  $[n, n - k, d^\perp]$  denote the parameters of the dual code  $C^\perp$ . We assume that they satisfy  $d \geq 2$  and  $d^\perp \geq 2$ . Define the *invariant weight enumerator* by

$$\tilde{A}_C(x, y) = \frac{A_C(x, y) + q^{k-n/2} A_{C^\perp}(x, y)}{1 + q^{k-n/2}}.$$

Note that  $\tilde{A}_C = \tilde{A}_{C^\perp} = \tilde{A}_C \circ \sigma_q$ , by the MacWilliams identity. The *Chinen zeta polynomial*  $\tilde{P}_C$  is the zeta polynomial  $P_F$  associated to the virtual weight enumerator  $F = \tilde{A}_C$ . The *Chinen zeta function* is defined in terms of the zeta polynomial by means of the following equation:

$$\tilde{P}_C(T) = \frac{T^{\max(0, d-d^\perp)}}{1 + q^{k-n/2}} (P_C(T) + q^{n/2-d+1} T^{n-2d+2} P_C(1/qT)). \quad (4.8.1)$$

**Theorem 143** (Chinen [Ch3]) *The Chinen zeta polynomial given by (4.8.1) above has degree  $2\tilde{g} = n + 2 - 2\min(d, d^\perp)$  and satisfies the functional equation*

$$\tilde{P}_C(T) = q^{\tilde{g}} T^{2\tilde{g}} \tilde{P}_C(1/qT).$$

By the functional equation, if  $d > d^\perp$ , then

$$\tilde{P}_C(T) = \frac{q^{k-n/2} P_{C^\perp}(T) + T^{d-d^\perp} P_C(T)}{1 + q^{k-n/2}};$$

if  $d < d^\perp$ , then

$$\tilde{P}_C(T) = \frac{P_C(T) + q^{k-n/2} T^{d^\perp-d} P_{C^\perp}(T)}{1 + q^{k-n/2}};$$

and if  $d = d^\perp$ , then

$$\tilde{P}_C(T) = \frac{P_C(T) + q^{k-n/2} P_{C^\perp}(T)}{1 + q^{k-n/2}}.$$

Note that when  $T = 1$ , we have  $P(1) = 1$  and (by the functional equation)  $P(1/q) = q^{-g} = q^{d-1-n/2}$ . This implies  $\tilde{P}_C(1) = \frac{2}{1+q^{k-n/2}}$ . It may be simpler to use the “averaged” zeta function

$$P_C^*(T) = (P_C(T) + P_{C^\perp}(T))/2,$$

but this is *not* the Chinen zeta function.

**Example 144** We use SAGE to compute the Chinen zeta polynomial of some small optimal codes. We shall normalize the Chinen zeta function so that  $\tilde{P}_C(1) = 1$ .

SAGE

```
sage: R_CC = PolynomialRing(CC, "T")
sage: n = 8; k = 2; q = 2
sage: C = best_known_linear_code(n,k,GF(q))
sage: P = C.chinen_polynomial()
sage: Cd = C.dual_code()
sage: Pd = Cd.chinen_polynomial()
sage: C.minimum_distance(); Cd.minimum_distance()
5
2
sage: P; P == Pd
2/5*t^6 + 9/35*t^5 + 4/35*t^4 + 2/35*t^3 + 2/35*t^2 + 9/140*t + 1/20
True
sage: [abs(z[0]) for z in R_CC(P*1.0).roots()]

[0.707106781186548,
0.707106781186548,
0.707106781186547,
0.707106781186547,
0.707106781186547,
0.707106781186547,
0.707106781186548]
sage: C.gen_mat()
```

```
[0 0 0 1 1 1 1 1]
[1 1 1 0 0 1 1 1]
sage: C0 = C.standard_form()[0]
sage: C0.gen_mat()
[1 0 1 1 0 1 1 1]
[0 1 0 0 1 1 1 1]
```

The Riemann hypothesis is (apparently) true since the zeros have absolute value (approximately)  $1/\sqrt{2}$ .

SAGE

```
sage: C = HammingCode(3,GF(2))
sage: C.chinen_polynomial()
(2*sqrt(2)*t^3/5 + 2*sqrt(2)*t^2/5 + 2*t^2/5
 + sqrt(2)*t/5 + 2*t/5 + 1/5)/(sqrt(2) + 1)
```

It can be easily shown that if  $C$  is formally self-dual, then  $\tilde{P}_C = P_C$ . We say that  $C$  (whether formally self-dual or not) *satisfies the Riemann hypothesis* if its Chinen zeta polynomial has all its zeros on the “critical line.”

For example, if  $C$  is an MDS code, then

$$\tilde{P}_C(T) = \frac{1}{1 + q^{k-n/2}} (1 + q^{n/2-d+1} T^{n-2d+2}).$$

If  $C$  is MDS and  $n - 2d + 2 \neq 0$ , then the Riemann hypothesis holds for the Chinen zeta function.

The following is an analog of Open Question 19 for Chinen zeta functions.

**Open Problem 23** Let  $C$  be any code over  $GF(q)$ . When is there a curve  $X/GF(q)$  for which the zeta function of the curve  $\zeta_X$  is equal to the Chinen zeta function  $Z_C$  of the code?

Since the Riemann hypothesis holds for  $\zeta_X$  (this is a well-known theorem of André Weil), a necessary condition is that the code must satisfy the Riemann hypothesis. See Example 9.7 in [D6] for two (self-dual) codes for which this holds.

*Remark 17* For the “twisted case,” including detailed proofs and numerous examples, see Chinen [Ch2].

**Open Problem 24** Is the Chinen zeta function of a linear code  $C$  equal to the Duursma zeta function of some self-dual code  $C'$ ?

If yes, then of course the set of Chinen zeta functions would be contained in the set of Duursma zeta functions. For example, is the Chinen zeta function of a nonbinary Hamming code  $C$  (say over  $GF(q)$  with  $q > 4$ ) equal to the Duursma zeta function of some self-dual code  $C'$ ? This seems unlikely, but we do not have a proof or disproof.

*Example 145* We use SAGE to compute the Chinen zeta polynomial of some indecomposable codes.

Consider codes which are generated by the matrix  $D_m$  ( $m$  even) defined as follows.

SAGE

```
def d_matrix(m):
    if not(is_even(m)):
        raise ValueError, "%s must be even and >2"%m
    M = int(m/2)
    A = [[0]*2*i+[1]*4+[0]*(m-4-2*i) for i in range(M-1)]
    MS = MatrixSpace(GF(2), M-1, m)
    return MS(A)
```

For example,

$$D_{14} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and the binary code generated by this matrix is a  $[14, 6, 4]$  code. Using SAGE, you can see that the associated Chinen zeta function does not satisfy the Riemann hypothesis.

SAGE

```
sage: n = 14; G = d_matrix(n); C = LinearCode(G); C
Linear code of length 14, dimension 6 over Finite Field of size 2
sage: C.spectrum()
[1, 0, 0, 0, 21, 0, 0, 0, 35, 0, 0, 0, 7, 0, 0]
sage: PT = PolynomialRing(CC,"T")
sage: PC = C.chinen_polynomial(); rts = PT(PC).roots()
sage: PC
64/39*t^12 - 32/429*t^10 - 32/429*t^9 - 160/1287*t^8 - 64/429*t^7 -
160/1287*t^6 - 32/429*t^5 - 40/1287*t^4 - 4/429*t^3 - 2/429*t^2 + 1/39
sage: [z[0].abs() for z in rts]
[0.707106781186548,
0.707106781186548,
0.707106781186548,
0.707106781186547,
0.707106781186548,
0.707106781186548,
0.707106781186549,
0.707106781186548,
0.707106781186547,
0.707106781186548,
0.814795710093010,
0.613650751723920]
```

In particular, the Riemann hypothesis for the Chinen zeta function is not true for all indecomposable codes.

### 4.8.1 Hamming Codes

Chinen [Ch3] computed the zeta polynomial of the Hamming codes. Consider the Hamming code  $C = C_{r,q}$  having the parameters  $[n = \frac{q^r-1}{q-1}, n-r, 3]$  over  $GF(q)$ , with  $r \geq 3$ . (When  $r = 2$ , the Hamming code is MDS and so has already been computed.)

The Duursma zeta polynomial of the dual code is given by

$$P_{C^\perp}(T) = c \cdot \left[ 1 + \sum_{j=1}^{n-d-1} \left( \binom{j+d-1}{d-1} - q \binom{j+d-2}{d-1} \right) T^j \right],$$

where the constant  $c = c_{r,q}$  is chosen so that  $P(1) = 1$ . This is Proposition 4.4 in [Ch3].

The Chinen zeta polynomial of the Hamming codes  $C_{r,q}$  ( $r \geq 3, q \geq 2$ ) is given by

$$\tilde{P}_C(T) = \frac{c}{1 + q^{r-n/2}} (F_1(T) - q F_2(T)), \quad (4.8.2)$$

where

$$F_1(T) = \sum_{j=0}^{n-d-1} \binom{n-i-2}{d-1} q^{i+2-n/2} T^i + \sum_{j=d-3}^{n-4} \binom{i+2}{d-1} T^i$$

and

$$F_2(T) = \sum_{j=0}^{n-d-2} \binom{n-i-3}{d-1} q^{i+2-n/2} T^i + \sum_{j=d-2}^{n-4} \binom{i+1}{d-1} T^i.$$

This is Theorem 4.5 in [Ch3].

*Example 146* Here is the Chinen zeta polynomial of the Hamming  $[7, 4, 3]$  code:

SAGE

```
sage: C = HammingCode(3,GF(2))
sage: C.chinin_polynomial()
(2*T^2/5 + 2*sqrt(2)*T*(T^2/5 + T/5 + 1/10) + 2*T/5 + 1/5)/(sqrt(2) + 1)
```

**Theorem 147** (Chinen) *The Chinen zeta polynomial of the Hamming codes  $C_{r,q}$  ( $r \geq 3, q \geq 4$ ) satisfies the Riemann hypothesis.*

This theorem is also true when  $r = 2$  ( $q \geq 2$ ), as a corollary to (3.3) in [Ch3], since then  $C$  is MDS.

Chinen's proof of this theorem is beautiful and based on his result stated as Corollary 122 in Sect. 4.6.2 above. To prove Theorem 147, Chinen explicitly computes the coefficients  $a_i$  of a normalized Chinen zeta polynomial  $f$  of  $C = C_{r,q}$  and proves

that it has the above decreasing symmetric form. This implies the Riemann hypothesis, as desired. The proof of the above lemma and the explicit computation of the coefficients are carefully worked out in [Ch3], which we refer to for details.

## 4.8.2 Golay Codes

This section summarizes some of the results in Chinen [Ch3], Sect. 7.

The Chinen zeta polynomial of the [11, 6, 5] Golay code  $C$  over  $GF(3)$  is

$$\tilde{P}_C(T) = \frac{\sqrt{3}-1}{14}(\sqrt{3}T+1)(3T^2+3T+1).$$

Chinen also presents an explicit but complicated expression for the Chinen zeta polynomial of the [23, 12, 7] Golay code  $C$  over  $GF(2)$ . He also shows that both of these Chinen zeta functions satisfy the “Riemann hypothesis.” The proof is by explicitly computing zeros, verifying the Riemann hypothesis numerically.

## 4.8.3 Examples

We begin with a random example:

SAGE

```
sage: RT = PolynomialRing(CC,"T")
sage: MS = MatrixSpace(GF(2), 3, 8)
sage: G = MS([[1,0,0,1,0,1,1,0],[0,1,0,1,0,0,0,1],[0,0,1,0,1,1,0,1]])
sage: C = LinearCode(G)
sage: C.minimum_distance()
3
sage: Cd = C.dual_code(); Cd.minimum_distance()
2
sage: f = RT(C.chinen_polynomial())
sage: print [z[0].abs() for z in f.roots()]
[0.707106781186548, 0.707106781186548, 0.707106781186548,
0.707106781186548, 0.707106781186547, 0.707106781186547]
sage: C.gen_mat()
[1 0 0 1 0 1 1 0]
[0 1 0 1 0 0 0 1]
[0 0 1 0 1 1 1 0]
sage: C.spectrum()
[1, 0, 0, 1, 3, 2, 0, 1, 0]
sage: Cd.spectrum()
[1, 0, 3, 10, 7, 4, 5, 2, 0]
sage: C.chinen_polynomial()
2/7*t^6 + 4/21*t^5 + 13/70*t^4 + 17/105*t^3 + 13/140*t^2 + 1/21*t + 1/28
sage: C.zeta_polynomial()
3/7*T^5 + 3/14*T^4 + 11/70*T^3 + 17/140*T^2 + 17/280*T + 1/56
sage: f = RT(C.zeta_polynomial())
sage: print [z[0].abs() for z in f.roots()]
[0.644472635143760, 0.644472635143761, 0.458731710756610,
0.476718789722295, 0.458731710756610]
```



This next example is also random:

— SAGE —

```
sage: C = RandomLinearCode(8,3,GF(2)); C.minimum_distance()
3
sage: Cd = C.dual_code(); Cd.minimum_distance()
2
sage: C.spectrum()
[1, 0, 0, 1, 3, 2, 0, 1, 0]
sage: Cd.spectrum()
[1, 0, 3, 6, 11, 8, 1, 2, 0]
sage: C.chinen_polynomial()
2/7*t^6 + 4/21*t^5 + 13/70*t^4 + 17/105*t^3 + 13/140*t^2 + 1/21*t + 1/28
sage: C.gen_mat()
[1 0 0 1 1 0 0 1]
[0 1 0 0 0 1 1 0]
[0 0 1 1 0 0 1 1]
sage: C.zeta_polynomial()
3/7*T^5 + 3/14*T^4 + 11/70*T^3 + 17/140*T^2 + 17/280*T + 1/56
```

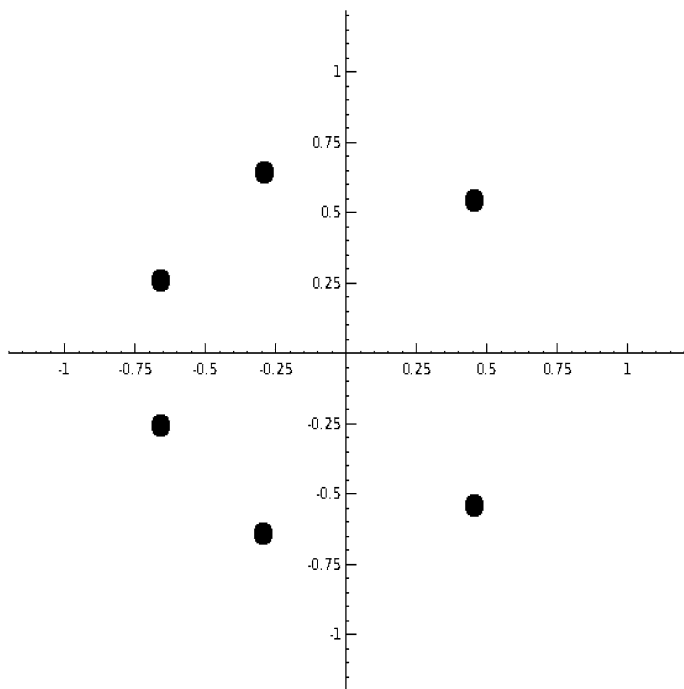
The next example concerns a code which is formally self-dual but not self-dual.

— SAGE —

```
sage: RT = PolynomialRing(CC,"T")
sage: MS = MatrixSpace(GF(2), 4, 8)
sage: G = MS([[1,0,0,0,0,1,1,0],[0,1,0,0,1,1,1,0],
               [0,0,1,0,1,1,1,1],[0,0,0,1,0,0,1,0]])
sage: C = LinearCode(G)
sage: C.minimum_distance()
2
sage: Cd = C.dual_code(); Cd.minimum_distance()
2
sage: f = RT(C.chinen_polynomial())
sage: print [z[0].abs() for z in f.roots()]
[0.707106781186549, 0.707106781186547, 0.707106781186547,
 0.707106781186546, 0.707106781186547, 0.707106781186547]
sage: C.gen_mat()
[1 0 0 0 0 1 1 0]
[0 1 0 0 1 1 1 0]
[0 0 1 0 1 1 1 1]
[0 0 0 1 0 0 1 0]
sage: C.chinen_polynomial()
2/7*t^6 + 2/7*t^5 + 11/70*t^4 + 3/35*t^3 + 11/140*t^2 + 1/14*t + 1/28
sage: C.spectrum()
[1, 0, 1, 4, 3, 4, 3, 0, 0]
sage: Cd = C.dual_code(); Cd.minimum_distance()
2
sage: Cd.spectrum()
[1, 0, 1, 4, 3, 4, 3, 0, 0]
sage: list_plot([(z[0].real(),z[0].imag()) for z in f.roots()])
```

The last command gives a plot of the roots (see Fig. 4.3).

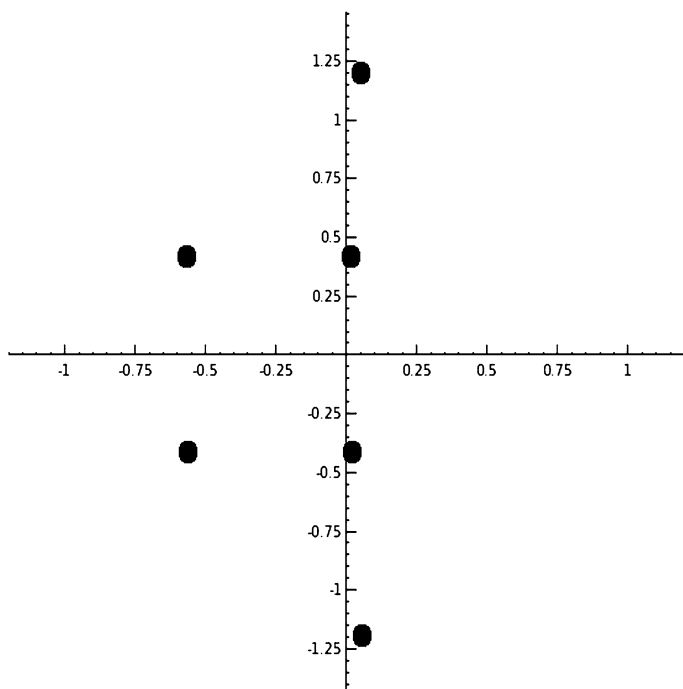
Our last example is one for which the Riemann hypothesis is false.



**Fig. 4.3** Roots of the Chinen zeta polynomial for a formally self-dual  $[8, 4, 2]$  binary code

SAGE

```
sage: RT = PolynomialRing(CC, "T")
sage: MS = MatrixSpace(GF(2), 4, 8)
sage: G = MS([[1, 1, 0, 0, 0, 0, 1, 1], [0, 0, 1, 0, 0, 1, 0, 1], [0, 0, 0, 1, 0, 1, 1, 0],
              [0, 0, 0, 0, 1, 1, 1, 1]])
sage: C = LinearCode(G)
sage: C.chinen_polynomial()
1/7*t^6 + 1/7*t^5 + 39/140*t^4 + 17/70*t^3 + 39/280*t^2 + 1/28*t + 1/56
sage: C.spectrum()
[1, 0, 0, 4, 6, 4, 0, 0, 1]
sage: Cd = C.dual_code(); Cd.minimum_distance()
2
sage: Cd.spectrum()
[1, 0, 1, 0, 11, 0, 3, 0, 0]
sage: C.minimum_distance()
3
sage: Cd = C.dual_code(); Cd.minimum_distance()
2
sage: f = RT(C.chinen_polynomial())
sage: print [z[0].abs() for z in f.roots()]
[1.19773471696883, 1.19773471696883, 0.707106781186547,
0.707106781186547, 0.417454710894058, 0.417454710894058]
sage: print [z[0] for z in f.roots()]
[0.0528116723604142 + 1.19656983895421*I,
0.0528116723604137 - 1.19656983895421*I,
-0.571218487412783 + 0.416784644196318*I,
-0.571218487412783 - 0.416784644196317*I,
0.0184068150523700 + 0.417048707955401*I,
0.0184068150523701 - 0.417048707955401*I]
```



**Fig. 4.4** Roots of the Chinen zeta polynomial for a  $[8, 4, 3]$  binary code violating the Riemann hypothesis

```
sage: C.gen_mat()
[1 1 0 0 0 0 1 1]
[0 0 1 0 0 1 0 1]
[0 0 0 1 0 1 1 0]
[0 0 0 0 1 1 1 1]
sage: C.chinen_polynomial()
1/7*t^6 + 1/7*t^5 + 39/140*t^4 + 17/70*t^3 + 39/280*t^2 + 1/28*t + 1/56
sage: list_plot([(z[0].real(),z[0].imag()) for z in f.roots()])
```

The last command gives a plot of the roots (see Fig. 4.4).

Selected Unsolved Problems in Coding Theory

Joyner, D.; Kim, J.-L.

2011, XII, 248 p. 17 illus., Hardcover

ISBN: 978-0-8176-8255-2

A product of Birkhäuser Basel