On Duursma Zeta Functions of Type IV Virtual Codes

S. Catalano[1]

[1]Department of Mathematics
United States Naval Academy

Honors Presentation

Outline

Outline

Topic

This talk will survey some of the properties of the zeta function of a linear code and give examples using the software package SAGE ,

http://www.sagemath.org

The analog of the Riemann hypothesis will be discussed.

Notation and Definitions

- linear code = subspace of $\mathbb{F}^n$, $\mathbb{F} = GF(q)$.
- C = linear code of length n / $\mathbb{F}$.
- $q = 2 \implies$ binary .
- $q = 3 \implies$ ternary .
- $q = 4 \implies$ quaternary .
- standard basis: $\mathbf{e}_1 = (1, 0, ..., 0) \in \mathbb{F}^n$, $\mathbf{e}_2 = (0, 1, 0, ..., 0) \in \mathbb{F}^n$, ..., $\mathbf{e}_n = (0, 0, ..., 0, 1) \in \mathbb{F}^n$.
- dimension $(C) = k$, so $|C| = q^k$.
- dual code $= C^\perp = \{v \in \mathbb{F}^n \mid v \cdot c = 0,\ \forall c \in C\}$.
- C is self-dual if $C = C^\perp$.

Hamming metric = $d(\mathbf{x}, \mathbf{y})$ = number of coordinates where these two vectors differ:

$$d(\mathbf{x}, \mathbf{y}) = |\{0 \leq i \leq n \mid x_i \neq y_i\}|. \tag{1}$$

weight $\mathrm{wt}(\mathbf{v})$ = number of non-zero entries of $\mathbf{v}$.

The smallest distance between distinct codewords in a linear code C is the minimum distance of C:

$$d = d(C) = min_{\mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}} d(\mathbf{0}, \mathbf{c}). \tag{2}$$

The Basic Problem

- C is an $[n, k, d]_q$ code
- $C^\perp$ is an $[n, k^\perp, d^\perp]_q$ code
- Iwan Duursma introduced the zeta function $Z = Z_C$ associated to C:

$$Z(T) = \frac{P(T)}{(1-T)(1-qT)}, \tag{3}$$

where $P(T)$ is a polynomial of degree $n + 2 - d - d^\perp$, called the zeta polynomial.

Outline

Examples

Basis vectors of C arranged as rows in a matrix = generator matrix G.

Example

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

is the gen mat of a self dual code parameters $[8, 4, 4]$ over $GF(2)$.
$|C| = 2^4 = 16$ and Duursma Zeta Fcn

$$Z(T) = \frac{2T^2 + 2T + 1}{5(1 - 2T)(1 - T)}$$

(Hamming) weight enumerator polynomial :

$$A_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = x^n + A_d x^{n-d} y^d + \cdots + A_n y^n,$$

where

$$A_i = |\{c \in C \mid \mathrm{wt}(c) = i\}|$$

MacWilliams identity:

$$A_{C^\perp}(x,y) = |C|^{-1} A_C(x + (q-1)y, x - y).$$

If $A_C(x,y) = A_{C^\perp}(x,y)$ then C is called a formally self-dual code .

virtual weight enumerator polynomial :

$$F(x,y) = \sum_{i=0}^{n} f_i x^{n-i} y^i = x^n + f_d x^{n-d} y^d + \cdots + f_n y^n,$$

for some integer d, $1 < d < n$. We call this polynomial virtually self-dual if it satisfies

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

If $F = A_C$ and C is a self-dual code then the above identity is a special case of the MacWilliams identity.

A polynomial $P(T)$ for which

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

is called a Duursma zeta polynomial of C.

The functional equation holds:

$$P^{\perp}(T) = P(\frac{1}{qT})q^g T^{g+g^{\perp}}, \tag{4}$$

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

The Riemann hypothesis is the statement that all zeros of $P(T)$ lie on the circle $|T| = 1/\sqrt{q}$ (in the self-dual case).

A polynomial $P(T)$ for which

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

is called a Duursma zeta polynomial of F, where F is a virtual weight enumerator.

If F is a virtually self-dual weight enumerator, then the Riemann hypothesis is the statement that all zeros of $P(T)$ lie on the circle $|T| = 1/\sqrt{q}$.

Honors Project Work

There exists extremal Type I, II, III, IV virtual self-dual weight enumerators. The definition will be skipped.

It's conjectured that the Duursma zeta function of all such weight enumerators satisfies the Riemann hypothesis.

My honors project varifies this for all extremal Type IV virtual self-dual weight enumerators with length divisible by 3.

For details, see Section 3 of my honors paper.

Outline

Riemann Hypothesis Example

SAGE has some functionality for linear codes. Here are a few examples to show the syntax.

SAGE can compute with the self-dual $[8, 4, 4]$ extended Hamming code:

Example

```
sage: C=self_dual_codes_binary(8)["8"]["1"]["code"]
sage: R.<T> = PolynomialRing(CC,"T")
sage: f = R(C.zeta_polynomial())
sage: print [z[0] for z in f.roots()]
[-0.500000000000000 + 0.500000000000000*I,
 -0.500000000000000 - 0.500000000000000*I]
```

This code satisfies the Riemann Hypothesis

Example Define the finite field of four elements as follows. Let z denote a root of the quadratic polynomial $x^2 + x + 1 \in GF(2)[x]$, where $GF(2)[x]$ denotes the polynomial ring in the indeterminate x. Let $GF(4) = \{0, 1, z, z+1\}$. This set is a field of characteristic 2. Let

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

be the generator matrix of a code C. This is a quaternary self-dual $[6, 3, 4]$ code and is referred to as the **hexacode**. In fact, this is an extremal Type IV code. Note that this code is MDS.

In general, it is true that the Duursma zeta function of any MDS code is $P(T) = 1$.

Here is a more interesting example. Let z denote the same element as was defined on the previous slide. Let $G =$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & z^2 & 1 & 1 & z & 1 & 1 & z^2 & z \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & z^2 & z^2 & 0 & z & 0 & 1 & z & z^2 & z^2 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & z^2 & 1 & 0 & z^2 & z^2 & z^2 & z & 0 & z \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & z^2 & 1 & 0 & z^2 & z^2 & z^2 & z & z \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & z & 1 & 1 & z^2 & z^2 & 1 & 1 & z & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & z & z^2 & z^2 & z^2 & 0 & 1 & z^2 & 0 & z \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & z & z^2 & z^2 & z^2 & 0 & 1 & z^2 & z \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & z^2 & z & 1 & 0 & z & 0 & z^2 & z^2 & z^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & z^2 & 1 & 1 & z & 1 & 1 & z^2 & 1 & z
\end{pmatrix}$$

be a generator matrix of a code C. This is an extremal Type IV code over a field with four elements.

According to SAGE , the zeta polynomial for this code is $P(T) = \frac{48}{143}T^4 + \frac{48}{143}T^3 + \frac{32}{143}T^2 + \frac{12}{143}T + \frac{3}{143}$. It can be checked directly, using SAGE , that this satisfies the RH:

Example

SAGE

```
sage: F.<z> = GF(4,"z")
sage: MS = MatrixSpace(F, 9, 18)
sage: G = MS([[1, 0, 0, 0, 0, 0, 0, 0, 0, 1, z^2, 1, 1, z, 1, 1, z^2, z],\
....: [0, 1, 0, 0, 0, 0, 0, 0, 0, z^2, z^2, 0, z, 0, 1, z, z^2, z^2],\
....: [0, 0, 1, 0, 0, 0, 0, 0, 0, z^2, 1, 0, z^2, z^2, z^2, z, 0, z],\
....: [0, 0, 0, 1, 0, 0, 0, 0, 0, 0, z^2, 1, 0, z^2, z^2, z^2, z, z],\
....: [0, 0, 0, 0, 1, 0, 0, 0, 0, z, 1, 1, z^2, z^2, 1, 1, z, 1],\
....: [0, 0, 0, 0, 0, 1, 0, 0, 0, z, z^2, z^2, z^2, 0, 1, z^2, 0, z],\
....: [0, 0, 0, 0, 0, 0, 1, 0, 0, 0, z, z^2, z^2, z^2, 0, 1, z^2, z],\
....: [0, 0, 0, 0, 0, 0, 0, 1, 0, z^2, z, 1, 0, z, 0, z^2, z^2, z^2],\
....: [0, 0, 0, 0, 0, 0, 0, 0, 1, z^2, 1, 1, z, 1, 1, z^2, 1, z]])
sage: C = LinearCode(G)
sage: print C.spectrum()
[1, 0, 0, 0, 0, 0, 0, 0, 2754, 0, 18360, 0, 77112, 0, 110160, 0, 50949, 0, 2808]
sage: R.<T> = PolynomialRing(CC,"T")
sage: P = C.sd_zeta_polynomial(4)
sage: P
48/143*T^4 + 48/143*T^3 + 32/143*T^2 + 12/143*T + 3/143
sage: rts = R(P).roots()
sage: [abs(r[0]) for r in rts]
[0.500000000000000, 0.500000000000000, 0.500000000000000, 0.500000000000000]
```

The Analog

- The Functional Equation for $Z(T)$:

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

- Define $\zeta(s) = Z(q^{-s})$, so the functional equation becomes $\zeta^{\perp}(s) = * \cdot \zeta(1-s)$, where * is a simple exponential expression.
  In the self-dual case, $\zeta = \zeta^{\perp}$:

The RH for $\zeta(s)$ is the statement that all zeros have $Re(s) = 1/2$

The Analog

- The Riemann zeta-function $\zeta(s)$ is

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

for $Re(s) > 1$

- The zeta-function satisfies the following functional equation:

$$\zeta(s) = * \cdot \zeta(1-s)$$

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

The RH for $\zeta(s)$ is the statement that all zeros have $Re(s) = 1/2$

For Further Reading I

W. C. Huffman and V. Pless, **Fundamentals of error-correcting codes**, Cambridge Univ. Press, 2003.

Duursma, *Extremal weight enumerators and ultraspherical polynomials*, Discrete Mathematics, vol. 268, no. 1-3, pp. 103-127, July 2003.

[△] The SAGE Group, SAGE : *Mathematical software*, version 2.11 `http://www.sagemath.org/`

[○] http://en.wikipedia.org/wiki/Riemann_zeta_function