

Computational aspects of Duursma zeta functions using SAGE

D. Joyner

Computational aspects of Duursma zeta functions using
SAGE

7-21-2007

C is an $[n, k, d]_q$ code

C^\perp is an $[n, k^\perp, d^\perp]_q$ code

Motivated by local CFT, Iwan Duursma introduced the **zeta function** $Z = Z_C$ associated to C :

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

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

This talk will survey some of the properties of the zeta function and give examples using the software package **SAGE** .

The *genus* of an $[n, k, d]_q$ -code C is defined by

$$\begin{aligned}\gamma(C) &= n + 1 - k - d \\ &= \text{"distance code is from being MDS"}.\end{aligned}$$

For AG codes, it often is equal to the genus of the associated curve

Note that if C is a self-dual code then its genus satisfies

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

SAGE has some native Python commands, and GAP- and GUAVA-wrappers, for linear codes. Here are a few examples to show the syntax.

SAGE can compute Hamming codes:

Example

```
sage: C = HammingCode(3,GF(3))
sage: C
      Linear code of length 13, dimension 10
      over Finite field of size 3
sage: C.minimum_distance()
      3
```

SAGE can compute the Golay codes

Example

```
sage: C = ExtendedTernaryGolayCode(); C
      Linear code of length 11, dimension 6 over
          Finite field of size 3
sage: C.minimum_distance()
      6
```

More with Golay codes:

Example

```
sage: C.gen_mat()
```

```
[1 0 2 1 2 2 0 0 0 0 0 1]
[0 1 0 2 1 2 2 0 0 0 0 1]
[0 0 1 0 2 1 2 2 0 0 0 1]
[0 0 0 1 0 2 1 2 2 0 0 1]
[0 0 0 0 1 0 2 1 2 2 0 1]
[0 0 0 0 0 1 0 2 1 2 2 1]
```

```
sage: C.spectrum()
```

```
[1, 0, 6, 12, 42, 96, 126, 222, 168, 50, 6, 0, 0]
```

This calls a C program written by Steve Linton in the kernel of GAP.

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

$$A_i = |\{c \in C \mid \text{wt}(c) = i\}| = \# \text{ of codewds wt } i.$$

$A_C(x, y) = A_{C^\perp}(x, y)$ iff C is *formally self-dual code*

There exist a SD MDS code $[10, 5, 6]_{41}$ (due to J.-L. Kim, Y. Lee).

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 Duusma zeta polynomial $P = P_C$ exists and is unique.)

The *functional equation* holds:

$$P^\perp(T) = P\left(\frac{1}{qT}\right) q^g T^{g+g^\perp}, \quad (2)$$

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 $|T| = 1/\sqrt{q}$.

Let C be a b -divisible code. If C and C^\perp both contain the all-ones codeword then C is said to be *Type 2 divisible*. We say C is *Type 1 divisible* if C is not of Type 2.

Lemma: If C is Type 1 divisible then

$$d + bd^\perp \leq n + b(b + 1).$$

If C is Type 2 divisible then

$$2d + bd^\perp \leq n + b(b + 2).$$

Let C be a fsd b -divisible $[n, k, d]_q$ -code.

We say C is *Type I* if $q = b = 2$, and n is even.

We say C is *Type II* if $q = 2$, $b = 4$, and $8|n$.

We say C is *Type III* if $q = b = 3$, and $4|n$.

If $q = 4$, $b = 2$, and n is even then C is said to be *Type IV*.

Lemma (*Mallows-Sloane bounds*) If C is SD then

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

Virtual weight enumerator - 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.

If $F(x, y) = x^n + \sum_{i=d}^n f_i x^{n-i} y^i$ with $f_d \neq 0$ then we say that the *length* of F is n and the *minimum distance* of F is d .

Formally self-dual weight enumerator - Such an F of even degree invariant under $\sigma = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}$

Genus of a FSDWE: $\gamma(F) = n/2 + 1 - d$.

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 $A_C = F$.

Extremal FSDWEs

Define Type I, II, III, IV analogously for FSDWEs. (Analog of Gleason-Pierce thrm for FSDWEs?)

Theorem (Duursma): If F is a FSDWE with length n and minimum distance d then

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

A FSDWE F (ie, a virtual SD code) of one of these Types is called **extremal** if this bound holds with equality.

A code is called *optimal* if its minimum distance is maximal among all linear codes of that length and dimension.

It is known that any two extremal codes (if they exist) have the same weight enumerator polynomial.

Duursma conjectures the RH holds for $Z(T)$ for all extremal virtual codes.

Define c_j by

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

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 δ** .

The zeta polynomial P of these MDS FWE's satisfies $P(T) = 1$.
In particular, the RH is false.

We use SAGE 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 $q = 3$,

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

Note: $n \leq q + k - 1$, so $[10, 6, 5]_2 \implies 10 \leq 2 + 6 - 1$ and $[12, 8, 5]_3 \implies 12 \leq 3 + 8 - 1$

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

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

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

These virtual weight enumerators are computed using the following SAGE code

Example

```
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
```

(All on one line)

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

Example

```
sage: C = HammingCode(3,GF(2))
sage: C.zeta_function()
(1/5 + 2/5*T + 2/5*T^2)/(1 - 3*T + 2*T^2)
sage: C = ExtendedTernaryGolayCode()
sage: C.zeta_function()
(1/7 + 3/7*T + 3/7*T^2)/(1 - 4*T + 3*T^2)
```

These satisfy the RH.

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 an optimal formally self-dual binary code C .

C has 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 $\sqrt{2}$.

Duursma has “explicitly” computed all zeta functions of extremal virtual SD codes. For all low values of the parameters, computations using **SAGE** have shown that the RH holds.

SAGE: www.sagemath.org

guava 3.0: <http://linear-ecc.googlecode.com/>