数理解析研究所講究録 1440 巻 2005 年 97-101

Zeta function of a linear code and its Riemann hypothesis property

北海道大学・理学研究科　吉田瞳 (Hitomi Yoshida)
Graduate school of Mathematics,
Hokkaido University

1 Introduction

Duursma defined zata function of code first in 1999. After that, the definition of it was expanded even general linear code. Furtheremore, a Riemann hypothesis analogue for self-dual linear code was formulated. In this paper, we introduce Duursma's theory.

2 Preliminaries

Let C be a linear code of length n and minimum distance d over the finite field of q elements. Let A_i be the number of words of weight i in C. The weight distribution may be represented by a polynomial

$$W_{\mathrm{C}}(x, y)=\sum_{i}^{n} \mathrm{A}_i x^{n-i} y^{i}$$

called the weight enumerator.

Difinition 2.1 *The zeta polynomial $P(T)$ of C is the unique polynomial of degree at most $n-d$ such that generating function*

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T)+xT)^{n}$$

has expansion

$$\cdots+\frac{W_{C}(x, y)-x^{n}}{q-1} T^{n-d}+\cdots .$$

The quotient $Z(T)=P(T)/((1-T)(1-qT))$ is called the zeta function of the linear code.

Difinition 2.2 *Let C be a linear code over the field F_q of q elements has as main parameters its length n, dimension k, and minimum distance d. Then dual code of C is defined by*

$$C^{\perp} = \{u \in F_q \mid u \cdot v = 0 \ \forall v \in C\},$$

where for all $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ in F_q, inner product $u \cdot v$ is defined by

$$u \cdot v = u_1 v_1 + \cdots + u_n v_n.$$

Dimension and minimum distance of $C^{\perp}$ is denoted by $k^{\perp}$ and $d^{\perp}$ respectively.

Difinition 2.3 *If C is equal to its dual code $C^{\perp}$, then the code is called self-dual code.*

Theorem 2.1 *For zeta polynomial $P(T)$, the following holds.*

(i) $\deg P(T) = n + 2 - d - d^{\perp}$

(ii) *Let zeta polynomial and zeta function of $C^{\perp}$ be $P^{\perp}(T)$ and $Z^{\perp}(T)$ respectively. Then*

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

$$Z^{\perp}(T) = Z(\frac{1}{qT}) q^{g-1} T^{g+g^{\perp}-2},$$

where $g = n + 1 - k - d$, $g^{\perp} = n + 1 - k^{\perp} - d^{\perp}$.

In particular, if C is self-dual code, since $P(T) = P^{\perp}(T)$, the following hold.

(i)' $\deg P(T) = 2g$

(ii)'

$$P(T) = P(\frac{1}{qT}) q^{g} T^{2g}$$

$$Z(T) = Z(\frac{1}{qT}) q^{g-1} T^{2g-2}$$

Proof. [2, p59].

By the way, like these equations, there are some equations for weight enumerator.

Theorem 2.2 *For weight enumerator of C, the following hold.*

(i) $\widetilde{W_C}(x,y) := W_C(x+y,y) \Rightarrow \widetilde{W_{C^\perp}}(x,y) = \dfrac{1}{|C|}\widetilde{W_C}(qy,x)$

(ii) $\widetilde{W_C}(z) := \widetilde{W_C}(1,z) \Rightarrow \widetilde{W_{C^\perp}}(z) = \dfrac{(qz)^n}{|C|}\widetilde{W_C}\left(\frac{1}{qz}\right)$

(iii) $W_C^{\dim}(x,y) := \sum_{R\subseteq N} \dim C(R) x^{n-|R|}y^{|R|}$

$\Rightarrow W_{C^\perp}^{\dim}(x,y) = (x+y)^{n-1}\{(n-k)y - kx\} + W_C^{\dim}(y,x)$

3 A Riemann hypothesis analogue for self-dual codes

Difinition 3.1 [3, p119 Def4.1] Let C be self-dual code , $P(T)$ be its zeta polynomial. C is called that C has the Riemann hypothesis prperty, when for all zeros α of $P(T)$, $|\alpha| = \dfrac{1}{\sqrt{q}}$.

Difinition 3.2 *Let C be a self-dual code. C is called extremal when equality holds inthe following upper bounds.*

(Type I) $d \leq 2\lfloor n/8 \rfloor + 2$

(Type II) $d \leq 4\lfloor n/24 \rfloor + 4$

(Type III) $d \leq 3\lfloor n/12 \rfloor + 3$

(Type IV) $d \leq 2\lfloor n/6 \rfloor + 2$

Four type is a classification of a non-trivial divisible self-dual code defined over F_q. A code is said to be divisible when all weights are divisible by an integer c greater than one. Type I, II, III and IV means $(q, c) = (2,2)$, $(2,4)$, $(3,3)$ and $(4,2)$ respectively.

Problem [3, p119 open problem4.2] Do all extremal weight enumerators hane the Riemann hypothesis property?

Example 3.1 [8,4,4] *extended hamming code C_8 is a self-dual binary extremal doubly even code. It's weight enumerators is*

$$W_{C_8}(x,y) = x^8 + 14x^4y^4 + y^8.$$

Hence, it's zeta polynomial is

$$P(T) = \frac{1}{5}(1 + 2T + 2T^2).$$

Since $\alpha = \dfrac{1 \pm i}{2}$, *so* $|\alpha| = \dfrac{1}{\sqrt{2}} = \dfrac{1}{\sqrt{q}}$. *So C_8 has the Riemann hypothesis property.*

Example 3.2 [72,36,16] *code*
If such a code exists, then the zeros all have same absolete value $\frac{1}{\sqrt{2}}$.

Example 3.3 $C_8 \oplus C_8 \oplus C_8$ *is the set of words $(a|b|c)$ where a, b, c are arbitrary words of C_8. This code is type II and not extremal. This code is not satisfy the Riemann hypothesis property.*

Theorem 3.1 *Extremal self-dual code of type IV has the Riemann hypothesis property.*

In [4], Duursma obtained this theorem. But, it seems that it can't be proved as for three other types yet. Like this, the necessary and sufficient condition for zeta function of code to satisfy Riemann hypothesis property doesn't get clear yet.

References

[1] Duursma, I, Weight distribution of geomrteic Goppa codes, Trans. Amer. Math. Soc. 351, No.9 (1999), 3609-3639.

[2] Duursma, I, From weight enumerators to zeta functions, Discrete Appl. Math. 111 (2001), 55-73.

[3] Duursma, I, A Riemann hypothesis analogue for self-dual codes, DIMACS series in Discrete Math. and Theoretical Computer Science 56 (2001), 115-124

[4] Duursma, I, Extremal weight enumerators and ultraspherical polynomials, Discrete Math. 268, No.1-3 (2003), 103-127

[5] MacWilliams, F. J. and Sloane, N. L. A, *The Theory of Error-Correcting Codes*, North-Holland, 1997