九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Zeros of extended zeta polynomials for coding theory

Ono, Katsuhiko
Kyushu University

https://hdl.handle.net/2324/21933

出版情報：Journal of Math-for-Industry (JMI). 4 (A), pp.35-39, 2012-04-08. 九州大学大学院数理学研究院
バージョン：
権利関係：

Journal of Math-for-Industry, Vol. 4 (2012A-5), pp. 35–39

Zeros of extended zeta polynomials for coding theory

Katsuhiko Ono

Received on November 21, 2011 / Revised on January 10, 2012

Abstract. In 1999, Iwan Duursma defined the zeta polynomial for coding theory and formulated an analogue of the Riemann hypothesis for coding theory. In this paper, we consider certain self-reciprocal polynomials which generalize some zeta polynomials, and investigate whether the analogue of the Riemann hypothesis holds for this generalization. We show that in some cases the analogue of the Riemann hypothesis holds true, and conjecture that this is always the case.

Keywords. zeros, zeta polynomials for coding theory

1. Introduction

A linear code of length n over a finite field $\mathbb{F}_q$ of q elements is a subspace of $\mathbb{F}_q^n$ (the space of n-letter words) over $\mathbb{F}_q$. The minimum distance is denoted by d. The zeta functions and zeta polynomials for linear codes were introduced by Duursma [1] in 1999. The zeta function of a linear code is defined as the function

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

with a polynomial $P(T)$ of degree at least $n-d$. The polynomial $P(T)$ is called the zeta polynomial of $\mathscr{C}$. These were defined as an analogue of congruence zeta functions of algebraic curves and have many similar properties to those of algebraic curves. The code $\mathscr{C}$ is said to be self-dual if $\mathscr{C}$ is equal to $\mathscr{C}^{\perp}$, the orthogonal complement of $\mathscr{C}$ in $\mathbb{F}_q^n$. For zeta polynomials $P(T)$ of self-dual codes, it is well known that the following functional equation holds:

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

where $2g = n+2-2d$. This is analogous to the congruence zeta functions of algebraic curves over finite fields. Weil [11] moreover proved that all roots of the congruence zeta functions have the absolute value $1/\sqrt{q}$. This fact is called the Riemann hypothesis analogue in the theory of algebraic curves. Duursma conjectured in [4] that all zeta polynomials of extremal self-dual codes would satisfy the Riemann hypothesis analogue. Also, he has shown in [4] that all extremal Type IV codes of length which is a multiple of 6 satisfy the Riemann hypothesis analogue. For extremal Type I to III codes, the conjecture is still open. We explain the types of codes and the notion "extremal" in Section 2.

In this paper, we first show that zeta polynomials of all extremal Type I (respectively Type III) codes whose length is a multiple of 8 (respectively 12) can explicitly be written as follows (the proof will be given in Section 3):

(Type I)

$$P(T) = C\sum_{k=0}^{2m}\frac{(3m-k)!(m+k)!}{(3m)!}\sum_{j=0}^{\lfloor k/2\rfloor}\frac{2^j 3^{k-2j}}{j!(k-2j)!(m-k+j)!}T^k,$$

(Type III)

$$(1+3T^2)P(T) = C'\sum_{k=0}^{2m}\frac{(3m-k)!(m+k)!}{(3m)!}\sum_{j=0}^{\lfloor k/2\rfloor}\frac{3^{k-j}}{j!(k-2j)!(m-k+j)!}T^k,$$

with some explicit constants C and C'. With these expressions in mind, we consider more generally, for a non-zero real number α, the polynomial

$$P_\alpha^{(m)}(T) := \sum_{k=0}^{2m}\frac{(3m-k)!(m+k)!}{(3m)!}\sum_{j=0}^{\lfloor k/2\rfloor}\frac{\alpha^j 3^{k-2j}}{j!(k-2j)!(m-k+j)!}T^k.$$

For this, we conjecture the following.

Conjecture 1.1. *If $2 \le |\alpha| < \infty$, all zeros of $P_\alpha^{(m)}(T)$ have absolute value $1/\sqrt{\alpha}$.*

Our main theorem proves this conjecture in a special case.

Theorem 1.1. *When $\alpha = \frac{9}{4}$, the conjecture is true.*

We prove this by showing that $P_\alpha^{(m)}(T)$ can be written in terms of a classical orthogonal polynomial.

2. Definition

2.1. Zeta polynomials for coding theory

We give definitions of some terminologies associated with zeta polynomials for coding theory.

Definition 2.1. If $\mathscr{C}$ is a code of length n, let A_k be the number of codewords of weight k in $\mathscr{C}$. The numbers A_0, A_1, $\ldots$, A_n, are called the weight distribution of $\mathscr{C}$, and the polynomial

$$\sum_{k=0}^{n} A_k x^{n-k} y^k$$

is called the weight enumerator of $\mathscr{C}$, which is denoted by $W(x,y)$. Here x and y are variables, and $W(x,y)$ is a homogeneous polynomial of degree n in x and y.

For a polynomial $Z(T) = \sum_{k=0}^{\infty} a_k T^k$, we denote by $[T^k]Z(T)$ the coefficient a_k. In 1999, Duursma [1] defined the zeta function for a linear code as follows.

Definition 2.2 (Duursma [1])**.** For any linear code $\mathscr{C}$ over the field $\mathbb{F}_q$ of length n and the minimum distance d, there exists a unique polynomial $P(T)$ of degree at most $n-d$ such that

$$[T^{n-d}]\frac{P(T)}{(1-T)(1-qT)}(xT+y(1-T))^n = \frac{W(x,y)-x^n}{q-1}.$$

We call $P(T)$ the zeta polynomial of the linear code $\mathscr{C}$, and $Z(T) = P(T)/((1-T)(1-qT))$ the zeta function of $\mathscr{C}$. When $\mathscr{C}$ is self-dual, $P(T)$ satisfies the function equation described in the introduction.

We can formulate an analogue of the Riemann hypothesis as follows.

Definition 2.3. The code $\mathscr{C}$ satisfies the Riemann hypothesis analogue if all zeros of $P(T)$ have the same absolute value $1/\sqrt{q}$.

2.2. Extremal codes

A linear code over the field $\mathbb{F}_q$ of q elements has as main parameters its length n, dimension k, and minimum distance d. The dual code $\mathscr{C}^\perp$ has length n, dimension $n-k$, and we write its minimum distance $d^\perp$. The code $\mathscr{C}$ is said to self-dual code if $\mathscr{C}$ is equal to $\mathscr{C}^\perp$. A code is said to be a divisible code if the Hamming distance between any two words is divisible by an integer c greater than 1. The Gleason-Prange theorem [5, 6] classifies the non-trivial self-dual divisible codes into four cases

$$\begin{array}{lll} \text{(Type I)} & (q,c)=(2,2) & 2 \mid n, \\ \text{(Type II)} & (q,c)=(2,4) & 8 \mid n, \\ \text{(Type III)} & (q,c)=(3,3) & 4 \mid n, \\ \text{(Type IV)} & (q,c)=(4,2) & 2 \mid n. \end{array}$$

In each case, the parameters are bounded by the Mallows-Sloane upper bounds [7]

$$\begin{array}{ll} \text{(Type I)} & d \le 2\lfloor n/8 \rfloor + 2, \\ \text{(Type II)} & d \le 4\lfloor n/24 \rfloor + 4, \\ \text{(Type III)} & d \le 3\lfloor n/12 \rfloor + 3, \\ \text{(Type IV)} & d \le 2\lfloor n/6 \rfloor + 2. \end{array}$$

A code of each type is called extremal if it attains the respective Mallows-Sloane bound. For a homogeneous polynomial p over the complex numbers, let $p(D)$ be the differential operator defined by replacing each occurrence of variables x_j in p by $\partial/\partial x_j$. For a code with homogeneous weight enumerator $W(x,y)$, we seek pairs of polynomials $a(x,y)$ and $p(x,y)$ such that $a(x,y)$ divides $(p(x,y)(D))W(x,y)$.

Lemma 2.1 (Duursma [4])**.** *For a self-dual divisible code with weight enumerator $W(x,y)$, let*

$$\begin{array}{ll} \text{(Type I)} & a(x,y) = (x^3y - xy^3)^{d-3}, \\ & p(x,y) = (x^3y - xy^3), \\ \text{(Type II)} & a(x,y) = (x^5y - xy^5)^{d-5}, \\ & p(x,y) = (x^5y - xy^5), \\ \text{(Type III)} & a(x,y) = (x^3y - y^4)^{d-4}, \\ & p(x,y) = (8x^3y - y^4), \\ \text{(Type IV)} & a(x,y) = (x^2y - y^3)^{d-3}, \\ & p(x,y) = (9x^2y - y^3). \end{array}$$

Then $a(x,y) \mid (p(x,y)(D))W(x,y)$.

Suppose the length is a multiple of 8, 24, 12, 6 respectively in Type I, II, III, IV cases. Then we have by [4]

$$\begin{array}{ll} \text{(Type I)} & (x^3y - xy^3)(D)W(x,y) \\ & = -(d-2)_3(n-d)A_d(x^3y - xy^3)^{d-3}, \\ \text{(Type II)} & (x^5y - xy^5)(D)W(x,y) \\ & = -(d-4)_5(n-d)A_d(x^5y - xy^5)^{d-5}, \\ \text{(Type III)} & (8x^3y - y^4)(D)W(x,y) \\ & = (-1)^{d-3}(d-3)_4 A_d(x^3y - y^4)^{d-4}, \\ \text{(Type IV)} & (9x^2y - y^3)(D)W(x,y) \\ & = (-1)^{d-2}(d-2)_3 A_d(x^2y - y^3)^{d-3}, \end{array}$$

where the symbol $(a)_n$ means $(a)_n = a(a+1)\cdots(a+n-1)$, and A_d is the number of words which have exactly minimum distance d components. Let $P(T)$ be the zeta polynomial for the code and put

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

Theorem 2.1 (Duursma [4])**.** *Write $Q(T) = \sum_k q_k T^k$.*

Then we have

$$\text{(Type I)}\quad \sum_{k=0}^{2m} q_k \binom{4m}{m+k} T^k = \frac{(n-d)(d-2)_3}{(n-3)_4} A_d (1+3T+2T^2)^m,$$

$$\text{(Type II)}\quad \sum_{k=0}^{4m} q_k \binom{6m}{m+k} T^k = \frac{(n-d)(d-4)_5}{(n-5)_6} A_d ((1+3T+2T^2)(1+2T+2T^2))^m,$$

$$\text{(Type III)}\quad \sum_{k=0}^{2m} q_k \binom{4m}{m+k} T^k = \frac{(d-3)_4}{2(n-3)_4} A_d (1+3T+3T^2)^m,$$

$$\text{(Type IV)}\quad \sum_{k=0}^{m} q_k \binom{3m}{m+k} T^k = \frac{(d-2)_3}{3(n-2)_3} A_d (1+2T)^m.$$

3. Proof of theorem

3.1. Auxiliary polynomials

Let $R(T) = \sum_{k=0}^{2m} r_k T^k$ be the monic polynomial such that $P(\frac{T}{\sqrt{q}}) = CR(T)$ with a constant C. In the case of Type I and the length being a multiple of 8, we obtain from Theorem 2.1

$$\sum_{k=0}^{2m} \binom{4m}{m+k} r_k T^k = \binom{4m}{m} (1 + \frac{3}{\sqrt{2}} T + T^2)^m.$$

By multinomial theorem, the coefficient on the left is given by

$$\binom{4m}{m+k} r_k = \binom{4m}{m} \sum_{j=0}^{\lfloor i/2 \rfloor} \frac{m!(\frac{3}{\sqrt{2}})^{k-2j}}{j!(k-2j)!(m-k+j)!}.$$

Therefore, we obtain

$$r_k = \frac{(3m-k)!(m+k)!}{(3m)!} \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{(\frac{3}{\sqrt{2}})^{k-2j}}{j!(k-2j)!(m-k+j)!}.$$

Similarly, in the case of Type III length being a multiple of 12, we obtain

$$r_k = \frac{(3m-k)!(m+k)!}{(3m)!} \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{(\sqrt{3})^{k-2j}}{j!(k-2j)!(m-k+j)!}.$$

We are thus naturally led to define the following polynomial $R_a^{(m)}(T)$ which simultaneously generalizes the above two.

Definition 3.1. Let a be a non-zero real number, we define $R_a^{(m)}(T)$ as

$$R_a^{(m)}(T) := \sum_{k=0}^{2m} \frac{(3m-k)!(m+k)!}{(3m)!} \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{a^{k-2j}}{j!(k-2j)!(m-k+j)!} T^k.$$

The polynomial $P_\alpha^{(m)}(T)$ in the introduction and $R_a^{(m)}(T)$ are related with each other by

$$P_\alpha^{(m)}(\frac{T}{\sqrt{\alpha}}) = R_{\frac{3}{\sqrt{\alpha}}}^{(m)}(T). \tag{1}$$

By numerical experiments, we conjecture the following:

Suppose $0 < |a| \le \frac{3}{\sqrt{2}}$. Then, all zeros of $R_a^{(m)}(T)$ lie on the unit circle for all m.

By the equation (1), the above conjecture is equivalent to Conjecture 1.1. For $m = 1$, we have $R_a^{(1)}(T) = 1 + \frac{2}{3}aT + T^2$. Zeros of $R_a^{(1)}(T)$ are

$$\frac{-\frac{2}{3}a \pm \sqrt{\frac{4}{9}a^2 - 4}}{2}.$$

Thus, zeros of $R_a^{(1)}(T)$ lie on the unit circle whenever $|a| \le 3$.

We checked whether the polynomials satisfy the conjecture using Sturm's theorem [9]. And we verified that the polynomials of up to degree 100 and thousands of various randomly chosen values of a including $a = \sqrt{3}$ and $\frac{3}{\sqrt{2}}$ (which correspond to codes of Type I and III) satisfy the conjecture.

3.2. Special case of the conjecture

In the case of $a = 2$, the polynomial $R_2^{(m)}$ is written explicitly as follows.

Proposition 3.1. *When $a = 2$, the polynomial $R_2^{(m)}(T)$ is given by*

$$R_2^{(m)}(T) = \sum_{k=0}^{2m} \frac{\binom{m+k}{k}\binom{2m}{k}}{\binom{3m}{k}} T^k.$$

Proof.

$$\begin{aligned} &R_2(T) \\ &= \sum_{k=0}^{2m} \frac{(3m-k)!(m+k)!}{(3m)!} \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{a^{k-2j}}{j!(k-2j)!(m-k+j)!} T^k \\ &= \sum_{k=0}^{2m} \frac{\binom{m+k}{k}}{\binom{3m}{k}} \sum_{j=0}^{\lfloor k/2 \rfloor} 2^{k-2j} \binom{m}{k-j}\binom{k-j}{j} T^k \end{aligned}$$

We show that $\sum_{j=0}^{\lfloor k/2 \rfloor} 2^{k-2j} \binom{m}{k-j}\binom{k-j}{j} = \binom{2m}{k}$.

If k is even, then by replacing k by $2k$. We obtain

$$L.H.S. = \sum_{j=0}^{k} 2^{2k-2j}\binom{m}{2k-j}\binom{2k-j}{j}$$
$$= \sum_{j=0}^{k} 2^{2k-2j}\frac{(m)!(2k-j)!}{(2k-j)!(m-2k+j)!(j)!(2k-2j)!},$$

and hence

$$\sum_{k=0}^{m}\sum_{j=0}^{m} 2^{2k-2j}\frac{(m)!(2k-j)!}{(2k-j)!(m-2k+j)!(j)!(2k-2j)!}X^{2k}$$
$$\underset{k\to k+j}{=\!=\!=} \sum_{k=0}^{m-j}\sum_{j=0}^{m} 2^{2k}\frac{(m)!}{(m-2k-j)!(j)!(2k)!}X^{2k+2j}$$
$$= \sum_{j=0}^{m}\frac{(m)!}{(j)!(m-j)!}X^{2j}\sum_{k=0}^{m-j} 2^{2k}\frac{(m-j)!}{(2k)!(m-j-2k)!}X^{2k}$$
$$= \sum_{j=0}^{m}\binom{m}{j}(X^2)^j\sum_{k=0}^{m-j} 2^{2k}\binom{m-j}{2k}X^{2j}$$
$$= \sum_{j=0}^{m}\binom{m}{j}(X^2)^j(\frac{1}{2}(1+2X)^{m-j}+\frac{1}{2}(1-2X)^{m-j}$$
$$= \frac{1}{2}\sum_{j=0}^{m}\binom{m}{j}X^{2j}(1+2X)^{m-j}+\binom{m}{j}X^{2j}(1-2X)^{m-j}$$
$$= \frac{1}{2}((X^2+2X+1)^m+(X^2-2X+1)^m)$$
$$= \frac{1}{2}((X+1)^{2m}+(X-1)^{2m})$$
$$= \sum_{k=0}^{2m}\binom{2m}{2k}X^{2k}.$$

Similarly, if k is odd, then by replacing k by $2k+1$. We obtain

$$L.H.S. = \sum_{k=0}^{2m-1}\binom{2m}{2k+1}X^{2k+1}.$$

Therefore, we see that $\sum_{j=0}^{\lfloor k/2\rfloor} 2^{k-2j}\binom{m}{k-j}\binom{k-j}{j} = \binom{2m}{k}$. □

Using this we have

$$R_2^{(m)}(T) = \sum_{k=0}^{2m}\frac{\binom{m+k}{k}\binom{2m}{k}}{\binom{3m}{k}}T^k$$
$$= \frac{m!}{3m!}\sum_{k=0}^{2m}\binom{2m}{k}(m+1)_k(m+1)_{2m-k}T^k.$$

The ultraspherical polynomial $C_n^\lambda(x)$ of degree n, which is a special case of Jacobi polynomials, is defined by

$$\sum_{n=0}^{\infty} C_n^\lambda(x)r^n = (1-2xr+r^2)^{-\lambda}.$$

For $\lambda > -\frac{1}{2}$ they are orthogonal over the interval $[-1,1]$ with respect to the weight function $(1-x^2)^{\lambda-\frac{1}{2}}$. We set $x=\cos\theta$ and obtain

$$\sum_{n=0}^{\infty} C_n^\lambda(\cos\theta)r^n = (1-2r\cos\theta+r^2)^{-\lambda}$$
$$= (1-re^{i\theta})^{-\lambda}(1-re^{-i\theta})^{-\lambda}$$
$$= \sum_{k=0}^{\infty}\frac{(\lambda)_k}{k!}r^ke^{ik\theta}\sum_{j=0}^{\infty}\frac{(\lambda)_j}{j!}r^je^{-ij\theta}$$
$$= \sum_{n=0}^{\infty}\frac{r^ne^{-in\theta}}{n!}\sum_{k=0}^{n}\binom{n}{k}(\lambda)_k(\lambda)_{n-k}e^{2ik\theta},$$

(for more details we refer the reader to [10].) and so

$$C_n^\lambda(\cos\theta) = \frac{e^{-in\theta}}{n!}\sum_{k=0}^{n}\binom{n}{k}(\lambda)_k(\lambda)_{n-k}e^{2ik\theta}.$$

By this we have

$$C_{2m}^{m+1}(\cos\theta)$$
$$= \frac{e^{-2mi\theta}}{(2m)!}\sum_{k=0}^{2m}\binom{2m}{k}(m+1)_k(m+1)_{2m-k}e^{2ik\theta},$$

and finally we obtain

$$R_2^{(m)}(e^{2i\theta}) = \frac{(m)!(2m)!}{(3m)!}e^{2mi\theta}C_{2m}^{m+1}(\cos\theta).$$

As an orthogonal polynomial, C_{2m}^{m+1} has $2m$ roots in the interval $[-1,1]$. Therefore $R_2^{(m)}(T)$ has $2m$ roots on the unit circle, and we see that $P_{9/4}^{(m)}$ has $2m$ roots on the circle with the radius $2/3$. This completes the proof of Theorem 1.1.

Acknowledgment

The author would like to thank Professor Eiichi Bannai, Professor Masanobu Kaneko and the anonymous referee for giving him helpful advice and comments.

References

[1] I. M. Duursma, Weight distributions of geometric Goppa codes, Trans. Amer. Math. Soc. 351(9)(1999)3609–3639.

[2] I. M. Duursma, From weight enumerators to zeta functions, Discrete Appl. Math. 111(1-2)(2001)55–73.

[3] I. M. Duursma, A Riemann hypothesis analogue for self-dual codes, Codes and Association schemes, pages 115–124. Amer. Math. Soc. Providence, RI, 2001.

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

[5] E. M. Rains, N. J. A. Sloane, Self-dual codes, in Handbook of Coding Theory, Vol. I, II, pages 177–294. North-Holland, Amsterdam, 1998.

[6] N. J. A. Sloane, Self-dual codes and lattices, in Relations Between Combinatorics and other parts of mathematics, pages 273–308. American Mathematical Society, Providence, RI, 1979.

[7] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, North Holland, Amsterdam, 1977.

[8] S. Zhang, On the nonexistence of extremal self-dual codes, Discrete Appl. Math. 91(1-3)(1999)277–286.

[9] T. Takagi, Lecture of Algebras (in Japanese), Kyoritsu Publication, Japan, 1965.

[10] K. Driver, P. Duren, Zeros of the hypergeometric polynomials $F(-n; b; 2b; z)$, Indag. Math. (N. S.) 11(1) (2000) 43–51.

[11] A. Weil, Courbes Algébriques et variétés abéliennes, Hermann, 1971.

Katsuhiko Ono
Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
E-mail: k-ono(at)math.kyushu-u.ac.jp