

## 不変式環の Riemann 仮説類似に対する考察

九州大学・数理学研究院 田上 真 (Makoto Tagami)  
 Faculty of Mathematics,  
 Kyushu University

### 1 序論

コード理論に対するゼータ関数及びゼータ多項式は Duursma[3] により 1999 年に導入された。これは代数曲線上の合同ゼータ関数の類似として定義されており、代数曲線上のものと多くの似た性質を持っている。例えば  $C$  を  $q$  元からなる有限体上の種数  $g$  の特異点のない射影的代数曲線とし、その合同ゼータ関数を  $Z(T)$  とする。  $Z(T)$  は有理関数になり、

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

と書ける、ここで  $P(T)$  は次数  $2g$  の多項式で、ゼータ多項式という。この時

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

なる関数等式が成り立つことは良く知られているが、自己双対コードに対するゼータ多項式もこの関数等式を満たしている。

ゼータ多項式の全ての零点は絶対値  $1/\sqrt{q}$  をもつという Riemann 仮説類似は代数曲線上のゼータ多項式に対して Weil[13] により証明された。これに反して自己双対コードのゼータ多項式は常に Riemann 仮説を満たすわけではない。例えば  $H_8$  を binary extended Hamming code とすると、 $H_8$  の 3 つの直和は self-dual コードであるが Riemann 仮説は満たしていない (小路 [8] を参照)。Duursma は [5] で extremal な自己双対コードに対するゼータ多項式は Riemann 仮説を満たすという予想を提起し、[6] で extremal Type IV コードに対して予想を証明した。Type I ~ III に対してはまだ未解決である。ここで注意すべきことは Riemann 仮説の成立不成立はコードの存在とはあまり関係ないということである。実際に extremal Type IV コードは長さが 136 を超えると存在しないが (Zhang[15] を参照)、Riemann 仮説は常に成り立っている。Type I ~ IV コードにはそれぞれ  $GL(2, \mathbb{C})$  の有限群が付随しており、その weight enumerator はその群に対する不変式になっている。これらのことから Duursma の提起したコード理論の Riemann 仮説は不変式環の枠組みで考えることが自然であると思われる (このことを示唆している文献として知念 [2] がある)。この報告ではどのような群に対する不変式環の “extremal” 多項式 (3 節, 定義 3.1 を参照のこと) が Riemann 仮説を満たすかを調べる。特に Type IV に関係した不変式環のある部分環で群の不変式環ではなく、全ての長さに対する extremal 多項式が Riemann 仮説を満たしているものが存在することを示す。

### 2 ゼータ多項式とそのいくつかの性質

$\mathbb{C}[x, y]$  を複素数体上の 2 変数多項式環とする。コード理論の類似として、 $n$  次の斉次多項式  $f(x, y) \in \mathbb{C}[x, y]$  で  $x^n$  の係数が 1 であるものを  $n$  次の formal weight enumerator とすることにする。また

$$f(x, y) = x^n + A_d x^{n-d} y^d + (y \text{ について } d+1 \text{ 次以上の項}), (A_d \neq 0)$$

とした時,  $d$  を  $f$  の最小距離という.  $R$  を可換環とした時,  $R[[T]]$  で  $R$  上の形式的冪級数環を表す.  $Z(T) = \sum_{i=0}^{\infty} a_n T^n \in R[[T]]$  に対して,  $[T^k] Z(T)$  で  $k$  次の係数  $a_k$  を表す. この時次の補題が成り立つ. この補題は Duursma[3] による.

**補題 2.1.**  $f$  を  $n$  次の formal weight enumerator, その最小距離を  $d$ ,  $q$  を 1 と異なる任意の正の実数とする. この時高々  $n-d$  次の多項式  $P(T) \in \mathbb{C}[T]$  で次を満たすものが一意的に存在する.

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

**定義 2.1 (ゼータ多項式).** formal weight enumerator  $f$  に対して, 補題 2.1 で定まる多項式  $P(T)$  を  $f$  の ( $q$  に関する) ゼータ多項式という.

第 1 節で述べたように, 有限体  $\mathbb{F}_q$  上の代数曲線に対するゼータ多項式は関数等式を満たし, その根はすべて絶対値  $1/\sqrt{q}$  を持っている. 定義 2.1 のゼータ多項式に対して, その根が全て絶対値  $1/\sqrt{q}$  を持つならば, formal weight enumerator  $f$  は Riemann 仮説類似 (又は単に Riemann 仮説) を満たすと言う.

もちろんどんな斉次多項式に対しても Riemann 仮説が成り立つわけではない. 以下 Riemann 仮説が成り立つための斉次多項式に関する必要条件を求める. もし  $f(x,y)$  が実数係数多項式ならば, そのゼータ多項式も実数係数多項式になる.

**定義 2.2 (MDS weight enumerator).**  $1 \leq d \leq n+1$  に対して, MDS (Maximal Distance Separable) weight enumerator  $M_{n,d}(x,y)$  を次のように定義する.  $M_{n,d} = M_{n,d,q} = x^n + \sum_{w=d}^n A_w x^{n-w} y^w$ , ここで  $A_w$  は次で定義される:

$$A_w = \sum_{i=d}^w (-1)^{i-w} \binom{n-i}{n-w} \binom{n}{i} (q^{i-d+1} - 1) = \binom{n}{w} (q-1) \sum_{j=0}^{w-d} (-1)^j \binom{w-1}{j} q^{w-d-j} \quad (2)$$

**注意 1.** 2 元体上の MDS code は自明なもの, すなわちパラメーターが  $[n, 1, n]$ ,  $[n, n-1, 2]$ ,  $[n, n, 1]$  の時しか存在しない. 一般に任意の  $n, d$  に対して MDS code が存在するとは限らないが上記のようにして weight enumerator は考えられる. 特に  $q$  は素数冪と限らず, 任意の正数に対して定義される.

次の補題は [4, Prop.1] による.

**補題 2.2.**  $1 \leq d \leq n$  に対して次が成り立つ:

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

$\{M_{n,1}, M_{n,2}, \dots, M_{n,n}, M_{n,n+1}\}$  は一次独立で  $\mathbb{C}[x,y]$  の  $n$  次斉次多項式のなす部分空間の基底をなしている. よって任意の  $n$  次 formal weight enumerator  $f$  は  $\{M_{n,i}\}$  の一次結合で書ける.  $f = \sum_{i=d}^{n+1} p_i M_{n,i}$  ( $p_d \neq 0$ ) とすると,  $f$  の最小距離は  $d$  で, 補題 2.2 より  $f$  のゼータ多項式  $P(T)$  は  $P(T) = p_d + p_{d+1}T + \dots + p_n T^{n-d}$  となるのが解る.

$\tau \in \text{GL}(2, \mathbb{C})$ ,  $f \in \mathbb{C}[x,y]$  に対して,  $(\tau \cdot f)(x,y) := f((x,y)\tau)$  と定義する. また  $\sigma = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 \\ q-1 & -1 \end{pmatrix}$  で

MacWilliams 変換を表す.

**補題 2.3.**  $1 \leq d \leq n+1$  に対して

$$\sigma \cdot M_{n,d} = q^{\frac{n}{2}-d+1} M_{n,n-d+2}.$$

**補題 2.4.**  $f \in \mathbb{C}[x,y]$  を最小距離  $d$  の formal weight enumerator, そのゼータ多項式を  $P(T)$ , その次数を  $r = 2g$  とする. また  $d \geq 2$  と仮定する. この時次は同値である (複号同順).

(i)  $\sigma \cdot f = \pm f$ ,

$$(ii) P(T) = \pm q^g P\left(\frac{1}{qT}\right) T^r.$$

さらにこの時ゼータ多項式の次数は  $r = n - 2d + 2$  となる.

系 2.1. formal weight enumerator  $f$  は実数係数で最小距離 2 以上とする. この時  $f$  が Riemann 仮説を満たすには  $\sigma \cdot f = \pm f$  が成り立つことが必要である.

### 3 不変式環に対する Riemann 仮説類似と判定アルゴリズム

Duursma は [5] において, 全ての extremal self-dual divisible code に対して Riemann 仮説類似が成り立つことを予想している. self-dual divisible code は Type I から IV のものがあるが, それぞれの Type に  $GL(2, \mathbb{C})$  の有限部分群が付随しており, コードの weight enumerator はその群に対する不変式になっている. この節では Duursma の予想をもっと広く一般の不変式環に対して考え, いくつかの具体的な不変式環の extremal 多項式に対して, Riemann 仮説類似の成否を調べる.

まずは extremal 多項式を定義する.

定義 3.1 (extremal 多項式).  $A$  を  $\mathbb{C}[x, y]$  の部分空間とする. 任意の次数  $n$  に対して,

$$A_n = \{f \in A \mid f \text{ は } n \text{ 次斉次多項式}\}$$

とおく.  $h \in A_n$  が  $A_n$  の中で最小距離が最大である時  $h$  を次数  $n$  の extremal 多項式という.

例 1.  $f = x^8 + 14x^4y^4 + y^8$ ,  $g = x^4y^4(x^4 - y^4)^4$  とすると,  $\mathbb{C}[f, g]$  の次数 48 の extremal 多項式は一意的に決まり

$$\begin{aligned} & x^{48} + 17296x^{36}y^{12} + 535095x^{32}y^{16} + 3995376x^{28}y^{20} + 7681680x^{24}y^{24} \\ & + 3995376x^{20}y^{28} + 535095x^{16}y^{32} + 17296x^{12}y^{36} + y^{48} \end{aligned}$$

となる.

例 2.  $f = x + y$ ,  $g = y(x^2 - y^2)$  とすると,  $\mathbb{C}[f, g]$  の次数 11 の extremal 多項式は一意的に決まり

$$x^{11} + 66x^6y^5 + 198x^5y^6 + 330x^4y^7 + 495x^3y^8 + 550x^2y^9 + 330xy^{10} + 78y^{11}$$

となる.

まずは一番簡単な不変式環から考える.

命題 3.1.  $G = \langle \sigma \rangle$ ,  $\chi$  を  $\chi(\sigma) = -1$  なる  $G$  の linear character とする. この時次が成り立つ.

$$(i) \mathbb{C}[x, y]^G = \mathbb{C}[x + (\sqrt{q} - 1)y, y(x - y)].$$

$$(ii) \mathbb{C}[x, y]_\chi^G = (x - (\sqrt{q} + 1)y) \mathbb{C}[x, y]^G.$$

(iii)  $\mathbb{C}[x, y]^G$  の  $n = 2m + l$  ( $l = 0, 1$ ) 次の extremal 多項式の最小距離は  $m + 1$  である.

(iv)  $\mathbb{C}[x, y]_\chi^G$  の  $n$  次の extremal 多項式の最小距離を  $d$  とする. この時もし  $n = 2m + 1$  とすると,  $d = m + 1$ .  $n = 2m + 2$  の時  $m + 1 \leq d \leq m + 2$  である.

(v)  $\mathbb{C}[x, y]^G$  の  $n$  次の extremal 多項式を  $h$  とすると,

$$h = \begin{cases} M_{n, m+1} & \text{if } n = 2m, \\ \frac{1}{\sqrt{q} + q} (\sqrt{q} M_{n, m+1} + q M_{n, m+2}) & \text{if } n = 2m + 1. \end{cases}$$

特に extremal 多項式は Riemann 仮説類似を満たす.

(vi)  $\mathbb{C}[x, y]_x^G$  の  $n$  次の extremal 多項式を  $h$ , その最小距離を  $d$  とすると,

$$h = \begin{cases} \frac{1}{\sqrt{q}-q}(\sqrt{q}M_{n,m+1} - qM_{n,m+2}) & \text{if } n = 2m + 1, d = m + 1, \\ \frac{1}{1-q}(M_{n,m+1} - qM_{n,m+3}) & \text{if } n = 2m + 2, d = m + 1, \\ M_{n,m+2} & \text{if } n = 2m + 2, d = m + 2. \end{cases}$$

特に extremal 多項式は Riemann 仮説類似を満たす.

以下  $q$  を整数に制限し, 有理数係数のゼータ多項式が与えられた時その全ての根が絶対値  $1/\sqrt{q}$  を持つことを調べるこの論文で用いたアルゴリズムを述べる.

$P(T)$  を次数  $n$  の有理数係数を持ったゼータ多項式とする. まず  $P(T)$ ,  $\frac{d}{dT}P(T)$  にユークリッドの互除法を適用し,  $P(T)$  が重根を持たないことを確かめる (下記注意 2 参照).  $P(\pm\frac{1}{\sqrt{q}})$  を計算し,

$$l := \#\{t | P(t) = 0, t = \pm\frac{1}{\sqrt{q}}\}$$

とおく.  $P(T)$  に  $T = x + iy$  を代入すると

$$P(x + iy) = r(x, y^2) + iys(x, y^2)$$

という形になることは簡単にわかる.  $x^2 + y^2 = 1/q$  を  $r(x, y^2)$ ,  $s(x, y^2)$  に代入し,

$$\phi(x) = r(x, \frac{1}{q} - x^2), \psi(x) = s(x, \frac{1}{q} - x^2)$$

とする. また

$$\Omega(x) := \text{GCD}(\phi(x), \psi(x))$$

と置く.  $q$  は有理数であり, ゼータ多項式の係数も全て有理数なので  $\Omega(x)$  も有理数係数多項式になることに注意する.  $\Omega(x)$  に Sturm の定理を適用し (Sturm の定理については高木貞治 [12] を参照のこと), 区間  $(-1/\sqrt{q}, 1/\sqrt{q})$  に  $(n-l)/2$  個の実根を持つかどうか調べる. 1つの根  $x$  に対して2つの  $y$  が対応しているので, もし  $(n-l)/2$  個の実根を持つならば,  $P(T)$  は原点中心, 半径  $1/\sqrt{q}$  の円周上にすべての根を持っていることが解る.

**注意 2.** Sturm の定理による根の数の計算は代数的であり, 近似計算ではないことに注意する ( $l$  の計算も代数的). このアルゴリズムはゼータ多項式が重根を持つ場合は適用できない. しかしこの論文で調べた不変式環においては具体的な計算によりゼータ多項式の根は全て単根であることがわかる.

以下上記のアルゴリズムを用いて行いたいいくつかの具体的な不変式環の extremal 多項式に対する Riemann 仮説類似の成否の計算結果を記す.

### 3.1 linear character 付不変式環

$$S_1 = S_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, S_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}, S_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 3 & -1 \end{pmatrix}, T_1 = T_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, T_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T_3 = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}, \mathfrak{G}_i = \langle S_i, T_i \rangle \ (i = 1, 2, 3) \text{ とおく.}$$

$\mathfrak{G}_1$  の linear character は  $k = 0, 1, l = 0, 1$  に対して

$$\chi_{k,l}(S) = (-1)^k, \chi_{k,l}(T_1) = (-1)^l,$$

$\mathfrak{G}_2$  の linear character は  $k = 0, 1, l = 0, 1, 2, 3$  に対して,

$$\rho_{k,l}(S) = (-1)^k, \rho_{k,l}(T_2) = i^l,$$

$\mathfrak{G}_3$  の linear character は  $k = 0, 1, l = 0, 1, 2$  に対して,

$$\mu_{k,l}\left(\frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}\right) = (-1)^k, \mu_{k,l}\left(\begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}\right) = \omega^l,$$

$\mathfrak{G}_4$  の linear character は  $k = 0, 1, l = 0, 1$  に対して,

$$\eta_{k,l}\left(\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 3 & -1 \end{pmatrix}\right) = (-1)^k, \eta_{k,l}(T_1) = (-1)^l$$

で与えられる. それぞれの  $\mathfrak{G}_i$  と linear character に対して不変式環は次のようになる.

補題 3.1. (i)  $h_2 = x^2 + y^2, h_{4,1} = xy(x^2 - y^2), h_{4,2} = x^4 - 6x^2y^2 + y^4$  とすると

$$\mathbb{C}[x, y]_{\chi_{k,l}}^{\mathfrak{G}_1} = h_{4,1}^l h_{4,2}^k \mathbb{C}[h_2, h_{4,1}^2].$$

(ii)  $\phi_8 = x^8 + 14x^4y^4 + y^8, \phi_6 = xy(x^4 - y^4), \phi_{12} = (x^4 + y^4)(x^4 - 6x^2y^2 + y^4)(x^4 + 6x^2y^2 + y^4)$  とすると

$$\mathbb{C}[x, y]_{\rho_{k,l}}^{\mathfrak{G}_2} = \phi_6^l \phi_{12}^k \mathbb{C}[\phi_8, \phi_6^4].$$

(iii)  $\psi_{4,1} = x^4 + 8xy^3, \psi_{4,2} = y(x^3 - y^3), \psi_6 = x^6 - 20x^3y^3 - 8y^6$  とすると

$$\mathbb{C}[x, y]_{\mu_{k,l}}^{\mathfrak{G}_3} = \psi_{4,2}^l \psi_6^k \mathbb{C}[\psi_{4,1}, \psi_{4,2}^3].$$

(iv)  $\xi_2 = x^2 + 3y^2, \xi_{3,1} = y(x^2 - y^2), \xi_{3,2} = x(x^2 - 9y^2)$  とすると

$$\mathbb{C}[x, y]_{\eta_{k,l}}^{\mathfrak{G}_4} = \xi_{3,1}^l \xi_{3,2}^k \mathbb{C}[\xi_2, \xi_{3,1}^2].$$

補題 3.1 の不変式環において formal weight enumerator が出てくるのは全て  $l = 0$  の時のみである. さらに  $k = 0$  とすると, Duursma の extremal codes の場合である.

補題 3.1 の  $\mathbb{C}[x, y]_{\chi_{k,l}}^{\mathfrak{G}_1} = h_{4,2}^k \mathbb{C}[h_2, h_{4,1}^2], \mathbb{C}[x, y]_{\rho_{k,l}}^{\mathfrak{G}_2} = \phi_{12}^k \mathbb{C}[\phi_8, \phi_6^4], \mathbb{C}[x, y]_{\mu_{k,l}}^{\mathfrak{G}_3} = \psi_6^k \mathbb{C}[\psi_{4,1}, \psi_{4,2}^3], \mathbb{C}[x, y]_{\eta_{k,l}}^{\mathfrak{G}_4} = \xi_{3,2}^k \mathbb{C}[\xi_2, \xi_{3,1}^2]$  に対して, それぞれ 288, 332, 322, 285 次までの extremal 多項式を調べたところ, 全て Riemann 仮説を満たしていた.

### 3.2 unitary 複素鏡映群

Type II コードの不変式環は Shephard-Todd[11] の unitary 複素鏡映群の分類における No. 9 の不変式環になっている (以下用いている群の番号は Shephard-Todd[11] に従う). そこで他の 2 次の unitary 複素鏡映群 No. 4 ~ 22 に対しても Riemann 仮説類似の成否を調べた. 実際には, 群は unitary 行列による共役同型があるので Klein[7] で与えられている特別な不変式環の生成多項式を用いて計算した, また MacWilliams 変換が unitary 行列になる時は  $q = 2$  の時だけなので,  $q = 2$  で計算した.

正四面体群から導かれる unitary 複素鏡映群

[11, Table IV] より次の表を引用する.

群の No.	群の位数	不変式環の生成多項式	多項式の次数
4	24	$f, t$	4, 6
5	72	$f^3, t$	12, 6
6	48	$f, t^2$	4, 12
7	144	$f^3, t^2$	12, 12

ここで  $f, t$  は

$$\begin{aligned} f &= x^4 + 2\sqrt{3}ix^2y^2 + y^4, \\ t &= xy(x^4 - y^4) \end{aligned}$$

で与えられる.  $\sigma \cdot f = e^{\frac{2\pi}{3}} \bar{f}$ ,  $\sigma \cdot t = t$  が成り立つ.

No. 4~6 に対する不変式環の extremal 多項式は Riemann 仮説類似を一般には満たしていない.

No. 7 の群  $G_7$  に対しては次数 12 の extremal 多項式が

$$f' = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}$$

となるので,  $\mathbb{C}[x, y]^{G_7} = \mathbb{C}[f', t]$  となる.  $\sigma f' = -f'$  が成り立つことは直接解る. この不変式環の次数  $n = 12(2m+1)$  ( $l = 0, 1$ ) 次の extremal 多項式  $h$  は  $f'$  が  $y$  について  $y^4$  の多項式になっているので,  $h = \sum_{i=0}^m a_{2i} f'^{2m-2i} t^{2i}$  とかける. よって  $\sigma \cdot h = (-1)^l h$  が成り立つことが解る. 次数 312 まで計算したところ,  $\mathbb{C}[x, y]^{G_7}$  の全ての extremal 多項式は Riemann 仮説類似を満たしていた.

#### 正八面体群から導かれる unitary 複素鏡映群

[11, Table V] より次の表を引用する.

群の No.	群の位数	不変式環の生成多項式	多項式の次数
8	96	$h, t$	8, 12
9	192	$h, t^2$	8, 24
10	288	$h^3, t$	24, 12
11	576	$h^3, t^2$	24, 24
12	48	$f, h$	6, 8
13	96	$f^2, h$	12, 8
14	144	$f, t^2$	6, 24
15	288	$f^2, t^2$	12, 24

ここで  $f, h, t$  は

$$\begin{aligned} f &= xy(x^4 - y^4), \\ h &= x^8 + 14x^4y^4 + y^8, \\ t &= x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12} \end{aligned}$$

で与えられる.  $\sigma \cdot f = f$ ,  $\sigma \cdot h = h$ ,  $\sigma \cdot t = -t$  が成り立つ.  $h, t$  の次数の最小公倍数は 24 なので, No. 9~15 の不変式環の extremal 多項式は No. 8 の不変式環の extremal 多項式に現れることは簡単に解る. よって No. 8 のみを調べればよい. No. 8 に対して次数 292 まで調べたところ, extremal 多項式は全て Riemann 仮説類似を満たしていた.

#### 正二十面体群から導かれる unitary 複素鏡映群

No.16~22 に対しては一般に Riemann 仮説類似は成り立っていない.

### 3.3 二面体群

$D_n = \left\langle \left( \begin{array}{cc} \cos(\frac{2\pi i}{n}) & -\sin(\frac{2\pi i}{n}) \\ \sin(\frac{2\pi i}{n}) & \cos(\frac{2\pi i}{n}) \end{array} \right), \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \right\rangle$ ,  $|D_n| = 2n$  を二面体群とする. この時 Molien 級数は

$$M_{D_n}(t) = \frac{1}{(1-t^2)(1-t^n)}$$

となるので, 不変式環は代数的独立な 2 次,  $n$  次の多項式で生成される. よって

$$\begin{aligned} f &= x^2 + y^2, \\ g &= \frac{(x+iy)^n + (x-iy)^n}{2} \end{aligned}$$

とすると,  $f, g$  は代数的独立で  $\mathbb{C}[x, y]^{D_n} = \mathbb{C}[f, g]$  となる. 系 2.1 より, Riemann 仮説が成り立つには  $\sigma h = \pm h$  とならなければならないので,  $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in D_n$ , すなわち  $8|n$  という条件をつける.  $n=8$  の時は  $\mathbb{C}[x, y]^{D_n}$  は Type I コードの不変式環と一致する.  $16 \leq n \leq 96$  の時 次数 150 までの extremal 多項式を調べたところ, ゼータ多項式は高々 2 つの根を除いて, 絶対値  $1/\sqrt{2}$  を持つことが観察された.

## 4 不変式環でない環の Riemann 仮説類似

この節の目標は次の定理を示すことである.

**定理 4.1.**  $f = x+y, g = y(x^2-y^2)$  とする. また  $n \equiv 5 \pmod{6}$  と仮定する. この時  $\mathbb{C}[f, g]$  の  $n$  次の extremal 多項式は  $q=4$  に対して Riemann 仮説類似を満たす.

**注意 3.** 定理 4.1 の  $\mathbb{C}[f, g]$  は群の不変式環にはなっていない. また定理では  $n \equiv 5 \pmod{6}$  と仮定したが, 実際には任意の  $n$  に対して Riemann 仮説類似が成り立っているようである. このことは 3 節で述べたアルゴリズムを用いて, 次数が 164 まで確かめられた.

以下定理 4.1 を Duursma[6] の方法を用いて示す.  $f = x+y, g = y(x^2-y^2)$  と固定する. まず次の補題を示す.

**補題 4.1.**  $\mathbb{C}[f, g]$  の  $n = 3m+2$  次の extremal 多項式を  $h$  とする. また  $n \equiv 5 \pmod{6}$  と仮定する. この時  $h$  の最小距離は  $m+2$  以上である.

$h \in \mathbb{C}[f, g]$  を extremal 多項式,  $d$  をその最小距離とする. この時明らかに

$$y^{d-1} \left| \frac{\partial}{\partial y} h(x, y) \right| \tag{3}$$

である.  $(u, v) = (x, y)\sigma$  とする. この時 (3) より

$$v^{d-1} \left| \frac{\partial}{\partial v} h(u, v) \right|.$$

$v = (x-y)/2, \frac{\partial}{\partial v} = (3\frac{\partial}{\partial x} - \frac{\partial}{\partial y}), h(u, v) = (\sigma \cdot h)(x, y) = h(x, y)$  より,

$$(x-y)^{d-1} \left| \left( 3\frac{\partial}{\partial x} - \frac{\partial}{\partial y} \right) h(x, y) \right|. \tag{4}$$

(3) と (4) より,

$$\{y(x-y)\}^{d-2} \left| \frac{\partial}{\partial y} \left( 3\frac{\partial}{\partial x} - \frac{\partial}{\partial y} \right) h(x, y) \right|$$

$n = 3m + 2$  とすると,  $h = \sum_{i=0}^m a_i f^{3(m-i)+2} g^i$  と書ける.  $f = x + y, g = y(x - y)(x + y)$  であるので,  $(x + y)^{m+2} |h(x, y)$ , よって

$$\{y(x - y)\}^{d-2} (x + y)^m \left| \frac{\partial}{\partial y} \left( 3 \frac{\partial}{\partial x} - \frac{\partial}{\partial y} \right) h(x, y) \right. \quad (5)$$

(5) の左辺は次数  $2d - 4 + m$ , 右辺は次数  $n - 2 = 3m + 1 - 2$  となる. 補題 4.1 より  $n \equiv 5 \pmod{6}$  の時  $d \geq m + 2$  であるので, 両辺は定数倍  $C$  を除いて一致する, すなわち,

$$\frac{\partial}{\partial y} \left( 3 \frac{\partial}{\partial x} - \frac{\partial}{\partial y} \right) h(x, y) = C \{y(x - y)\}^m (x + y)^m. \quad (6)$$

逆にこの式から最小距離が  $m + 2$  であることが解る. よって  $P(T)$  を  $h$  のゼータ多項式とすると,

$$[T^{n-d}] \frac{P(T)}{(1-T)(1-4T)} (xT + (1-T)y)^n = \frac{h(x, y) - x^n}{3}.$$

両辺に  $\frac{\partial}{\partial y} \left( 3 \frac{\partial}{\partial x} - \frac{\partial}{\partial y} \right)$  を作用させると,

$$[T^{n-d}] P(T) (xT + (1-T)y)^{n-2} = C \left( 3 \frac{\partial}{\partial x} - \frac{\partial}{\partial y} \right) h(x, y) = C \{y(x - y)\}^m (x + y)^m$$

をえる.  $P(T) = \sum_{i=0}^m p_i T^i$  と書くと,

$$\sum_{i=0}^m p_i \binom{3m}{m+i} y^{m+i} (x - y)^{2m-i} = C \{y(x - y)(x + y)\}^m.$$

両辺を  $y^m$  で割ってから,  $x = 1 + T, y = T$  を代入して,

$$\sum_{i=0}^m \binom{3m}{m+i} p_i T^i = C(1 + 2T)^m \quad (7)$$

を得る. 次の補題は Duursma[6] による.

補題 4.2.  $R(T) = \sum_{i=0}^{\nu} r_i T^i$  がある  $\lambda$  に対して,

$$\sum_{i=0}^{\nu} \binom{\nu + 2\lambda - 2}{\lambda - 1 + i} r_i T^i = (1 + T)^{\nu}$$

を満たすとする. この時

$$\binom{\nu + 2\lambda - 2}{\lambda - 1} R(T^2) = \frac{\nu! T^{\nu}}{(\lambda)_{\nu}} C_{\nu}^{\lambda} \binom{T + T^{-1}}{2}$$

が成り立つ. ここで  $(\lambda)_{\nu} = \lambda(\lambda + 1) \cdots (\lambda + \nu - 1)$  であり, また  $\{C_{\nu}^{\lambda}\}$  は重み関数  $(1 - x^2)^{\lambda - 1/2}$  に関する直交多項式系で,  $C_{\nu}^{\lambda}(1) = \binom{\nu + 2\lambda + 1}{\nu}$  と正規化されている.

(7) において  $T' = 2T$  とすると,

$$\sum_{i=0}^m \binom{3m}{m+i} \frac{p_i}{2^i} T'^i = C(1 + T')^m.$$

よって  $R(T) = \sum_{i=0}^m \frac{p_i}{2^i} T^i = P(T/2)$ ,  $\lambda = m + 1$  に対して, 補題 4.2 を適用すると,

$$\frac{1}{C} \binom{3m}{m} R(T^2) = \frac{m! T^m}{(m+1)_m} C_m^{m+1} \binom{T + T^{-1}}{2}$$

が得られる.  $\{C_{\nu}^{\lambda}\}$  は重み関数  $(1 - x^2)^{\lambda - 1/2}$  に関する直交多項式系なので,  $C_m^{m+1}$  は区間  $[-1, 1]$  に  $m$  個の異なる根をもっている. よって  $R(T)$  は単位円周上に  $m$  個の根を持ち,  $P(T)$  は原点中心, 半径  $1/2$  の円周上に  $m$  個の根を持っていることが解る. よって定理 4.1 が証明された.



例 3.  $q = 3$  とする.  $f = x(x + 2y)$ ,  $g = y(x^3 - y^3)$  として,  $\mathbb{C}[x, y]^{\langle \sigma \rangle}$  の部分環  $\mathbb{C}[f, g]$  を考える. この環も群の不変式環ではないことはすぐにわかる. この環の extremal 多項式で次数 274 以下の Riemann 仮説類似を調べた所, 次数 2, 10 以外では全て Riemann 仮説類似を満たしていることが観察された.

**Acknowledgement** 筆者は有限複素 unitary 鏡映群や二面体群についてなど多くの有益な御助言を頂いた坂内英一先生に感謝いたします.

## 参考文献

- [1] 浅野啓三, 永尾汎, 群論, 岩波全書, 1992.
- [2] 知念 宏司, 線型符号のゼータ関数とそのリーマン予想 (Iwan Duursma の仕事の紹介, 及び 1 つの拡張), 仙台数論及び組合せ論小研究集会 2004 報告集 (2005), 31-44.
- [3] I.M. Duursma, Weight distributions of geometric Goppa codes, Trans. Amer. Math. Soc. 351(9) (1999) 3609-3639.
- [4] I.M. Duursma, From weight enumerators to zeta functions, Discrete Appl. Math. 111(1-2)(2001) 55-73.
- [5] I.M. Duursma, A Riemann hypothesis analogue for self-dual codes, Codes and Association schemes, Eds. Barg and Litsyn, AMS DIMACS Series, vol. 56, pp. 115-124, 2001.
- [6] I.M. Duursma, Extremal weight enumerators and ultraspherical polynomials, Discrete Math. 268 (2003), no. 1-3, 103-127.
- [7] F. Klein, Lectures on the icosahedron (trans. Sekiguchi), Springer Ferlark Tokyo, 1997.
- [8] 小路篤史, A Riemann hypothesis analogue for Type II codes, master thesis, Kyushu University, 2005.
- [9] C.J. Moreno, Algebraic curves over finite fields, Tracts in Mathematics, Cambridge Univ. Press, Cambridge, England, 1991.
- [10] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, North Holland, Amsterdam, 1977.
- [11] G.C. Shephard and J.A. Todd, Finite unitary reflection groups, Canadian J. Math. 6, (1954). 274-304.
- [12] 高木貞治, 代数学講義, 共立出版, 1965.
- [13] A. Weil, Courbes algébriques et variétés abéliennes, Hermann, 1971.
- [14] E.T. Whittaker and G.N. Watson, A Course of Modern Analysis, 4th ed., Cambridge University Press, Cambridge, 1963.
- [15] S. Zhang, On the nonexistence of extremal self-dual codes, Discrete Appl. Math. 91(1-3)(1999) 277-286.