数理解析研究所講究録
第 1593 巻 2008 年 145-153

不変式環上のリーマン仮説類似について

九州大学・理学部数学科 奥田 隆幸 (Takayuki Okuda)
(Department of Mathematics, Faculty of Science,
Kyushu University.)

1 概要

線形符号が self-dual であるとき、weight enumerator(x, y の 2 変数斉次多項式) は、MacWilliams 変換で不変であるが、x, y の 2 変数斉次多項式で MacWilliams 変換で不変なものを、formally self-dual な formal weight enumerator(以下、self-dual な f.w.e.) と呼ぶ。Iwan M.Duursma は、self-dual な f.w.e. に対して、zeta 多項式と呼ばれる 1 変数多項式を定義した。

この zeta 多項式は、ある関数等式を満たすことが分かっており、特に zeta 多項式が実係数になるとき、その零点は、ある原点中心の円周に対して対称に存在する。更に、さまざまな self-dual な f.w.e. に対して、zeta 多項式の零点が全て、円周上に存在することが知られている。このとき、この f.w.e. はリーマン仮説類似を満たす、という。

しかし数値計算上、ある self-dual な f.w.e. の無限列がリーマン仮説類似を満たす (全ての zeta 多項式の全ての零点が、同一円周上に乗る) であろうと予想されながら、まだ証明されていない例がいくつかある。

TypeIV extremal で $length \equiv 0(mod6)$ の場合には、全ての零点が同一円周上に乗るという事が証明されている (Duursma 2003[4]) が、$length \equiv 2, 4(mod6)$ の場合は未解決であった。この報告では、TypeIV extremal で $length \equiv 4(mod6)$ の場合に、zeta 多項式の零点の振る舞いが、$length \equiv 0(mod6)$ の場合と対応している事を示し、特に、$length \equiv 4(mod6)$ の場合にも、全ての zeta 多項式の零点が、同一円周上に乗るということを紹介したい。

2 リーマン仮説類似の定義

線形符号に対して weight enumerator を定義すると、線形符号の性質に応じて weight enumerator もいろいろな性質を持つ。特に、self-dual な線形符号の weight enumerator は、MacWilliams 変換で不変である。

weight enumerator の形式的な一般化として、次の定義を導入する。

formal weight enumerator

$\mathbb{C}_n[x,y]$ を x,y の 2 変数 n 次斉次多項式全体のベクトル空間とする。
$\mathbb{C}_n[x,y]$ の元 $F(x,y)$ を $length = n$ の formal weight enumerator (以下 f.w.e.) といい、$F(x,y) = a_0x^n + a_dx^{n-d}y^d + a_{d+1}x^{n-d-1}y^{d+1} + \cdots$ (ただし $a_d \neq 0$ とし, a_0 はどのような数であってもよいとする) と書ける場合に、最小距離 d_F を $d_F = d$ と定義する。
更に $F(x,y)$ が $q \in \mathbb{N}$ に対する MacWilliams 変換で不変、つまり

$$\sigma_q := \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}$$

に対し、$\sigma_q \cdot F(x,y) = F(x,y)$ となるとき、$F(x,y)$ は q で formally self-dual な f.w.e という。(以下、 q で self-dual な f.w.e.)
ただし $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot F(x,y) := F(ax+by, cx+dy)$ とする。

この q で self-dual な f.w.e. に対して、zeta 多項式と呼ばれる 1 変数多項式を次の様に定義する。

zeta 多項式

q で self-dual な f.w.e. である $F(x,y)$ に対し、zeta 多項式と呼ばれる 1 変数多項式 $P_F(T)$ を、以下の性質を持つものとして定める

- $degP_F(T) \leq n - d_F$
- $\frac{F(x,y) - A_0x^n}{q-1} = [T^{n-d_F}]\frac{P_F(T)}{(1-T)(1-qT)}(xT + y(1-T))^n$

ただし 式の右辺は、T に関する形式的冪級数 $\frac{P_F(T)}{(1-T)(1-qT)}(xT + y(1-T))^n$ の、第 $n - d_F$ 次の係数 (これは x,y の n 次斉次多項式となる) を表すものとする。

この定義によって zeta 多項式は一意的に定まる事が知られている。

zeta 多項式の計算例

$F(x,y) := x^8 + 14x^4y^4 + y^8$(e8 code の weight enumerator) とすると
$length = n = 8$, $d_F = 4$, F は $q = 2$ で self-dual である。
このとき $P_F(T) = p_0 + p_1T + \cdots + p_4T^4$ としてよい。2 番目の式の左辺は $\frac{F(x,y)-x^8}{2-1} = 14x^4y^4 + y^8$ となるが、右辺に現れる形式的冪級数は

$$\begin{aligned}
\frac{P_F(T)}{(1-T)(1-2T)}&(xT+y(1-T))^8 = \\
&\cdots+\{70p_0x^4y^4 \\
&+(-112p_0+56p_1)x^3y^5 \\
&+(112p_0-84p_1+28p_2)x^2y^6 \\
&+(48p_0+56p_1-32p_2+8p_3)xy^7 \\
&+(9p_0-13p_1+11p_2-5p_3+p_4)y^8\}T^4+\cdots
\end{aligned}$$

となる。ここで x, y に対する係数比較を順にしてやると

$$p_0 = \frac{1}{5}, p_1 = \frac{2}{5}, p_2 = \frac{2}{5}, p_3 = 0, p_4 = 0$$

となる。従って

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

さて、2 変数多項式 $F(x,y)$ から 1 変数多項式 $P_F(T)$ を定義したのであるが、$F(x,y)$ には MacWilliams 変換での不変性が要請されていた。この不変性は、zeta 多項式に、次の関数等式として受け継がれる。

関数等式

$g := \frac{1}{2}(n - 2d_F + 2)$ とする。
このとき

$$deg P_F(T) = 2g = n - 2d_F + 2$$
$$P_F(T) = q^g P_F(\tfrac{1}{qT})T^{2g}$$

となる。

特に 2 番目の等式を $P_F(T)$ の関数等式と呼ぶ。
これより、α が $P_F(T)$ の零点である事と、$\frac{1}{q\alpha}$ が $P_F(T)$ の零点である事と同値であり、

更に $P_F(T)$ が実係数なら、α が $P_F(T)$ の零点である事と、$\frac{1}{q\bar{\alpha}}$ が $P_F(T)$ の零点である事と同値である。

この同値性から分かるように、zeta 多項式の零点にとって $\{z \in \mathbb{C} \mid \mid z \mid = \frac{1}{\sqrt{q}}\}$ という円は特別な意味を持つ。実は、さまざまな self-dual な f.w.e. に対して、zeta 多項式の零点が、この円周上にあることが知られている。

リーマン仮説類似

$F(x,y)$ を q で self-dual な f.w.e. とする、
$P_F(T)$ の全ての零点が $\{z \in \mathbb{C} \mid \mid z \mid = \frac{1}{\sqrt{q}}\}$ に乗るとき,
$F(x,y)$ はリーマン仮説類似を満たすという。

3 TypeIV extremal f.w.e. と、そのリーマン仮説類似

今回、特に注目するのは、TypeIV extremal と呼ばれる、$q = 4$ で self-dual な f.w.e. の無限列である。

TypeIV f.w.e.

1 の n 乗根 $\xi_n := exp(\frac{2\pi i}{n})$ に対し、$\tau_n := \begin{pmatrix} 1 & 0 \\ 0 & \xi_n \end{pmatrix}$ としておく。
$F(x,y)$ を $length = n$ の f.w.e. としたとき、$F(x,y)$ が $q = 4$ で self-dual というのは $\sigma_4 \cdot F(x,y) = F(x,y)$ となる事であった。
更に $F(x,y)$ が even であるというのを $\tau_2 \cdot F(x,y) = F(x,y)$ となることと定義する。つまり、$F(x,y) = F(x,-y)$ であることを even という。
そして $F(x,y)$ が Type IV であるというのを $q = 4$ で self-dual であり、尚且つ even であることと定義する。
$G_4 := <\sigma_4, \tau_2>$ として定義しておけば

$$F(x,y) \text{ が Type IV} \iff F(x,y) \in \mathbb{C}[x,y]^{G_4}$$
(ただし $\mathbb{C}[x,y]^{G_4}$ は G_4 の不変式環としている)

となる。このとき $\mathbb{C}[x,y]^{G_4} = \mathbb{C}[x^2+3y^2, (y(x^2-y^2))^2]$ となることが知られている。

この他にも TypeI,TypeII,TypeIII が次の様に定義されているが、今回は詳しく触れない。((4),(5) 参照)

$G_1 :=< \sigma_2, \tau_2 >$

Type I $\Longleftrightarrow F(x,y) \in \mathbb{C}_n[x,y]^{G_1} = \mathbb{C}[x^2+y^2, (xy(x^2-y^2))^2]$

$G_2 :=< \sigma_2, \tau_4 >$

Type II $\Longleftrightarrow F(x,y) \in \mathbb{C}_n[x,y]^{G_2} = \mathbb{C}[x^8+14x^4y^4+y^8, x^4y^4(x^4-y^4)^4]$

$G_3 :=< \sigma_3, \tau_3 >$

Type III $\Longleftrightarrow F(x,y) \in \mathbb{C}_n[x,y]^{G_3} = \mathbb{C}[x^4+8xy^3, (y(x^3-y^3))^3]$

extremal

$F(x,y)$ が $length = n$ の Type IV f.w.e. であるとき、$F(x,y)$ が extremal であるということを、F の最小距離 d_F が、$length = n$ の Type IV f.w.e. の中で最大、になるということで定義する。さらに $F_n^{IV}(x,y)$ と書いたら $length = n$ の Type IV extremal で monic な f.w.e. とする. (このようなものは一意的に存在する。従って extremal な f.w.e. の零点を調べたければ、$F_n^{IV}(x,y)$ の零点を調べればよい)

このようなものを取り扱うのは、符号理論の観点から自然なことであるが、Duursma は次のような問題を考えた。

Duursma の問題

次の命題が真であれば証明し、偽であれば反例を挙げよ。

"Type $j(j = I, II, III, IV)$ extremal f.w.e. は
全て リーマン仮説類似を満たす。"

この問題は、一般には未解決である。無限列として部分的に解決しているものでは
[Duursma 2003(4)]

$length = 6k (k \in \mathbb{N})$ の Type IV extremal f.w.e. は、リーマン仮説類似を満たす。

という結果があるが、その他は知られていなかった。(2007 年現在)

次節では、主結果として、TypeIV extremal で $length = 6k-2$ の場合にも、肯定的に解決したことを報告する。

4 主結果

主結果の主張

$F_n^{IV}(x,y)$ と書いたら $length = n$ の Type IV extremal で monic な f.w.e. のことであった。このとき任意の $k \in \mathbb{N}$ に対し

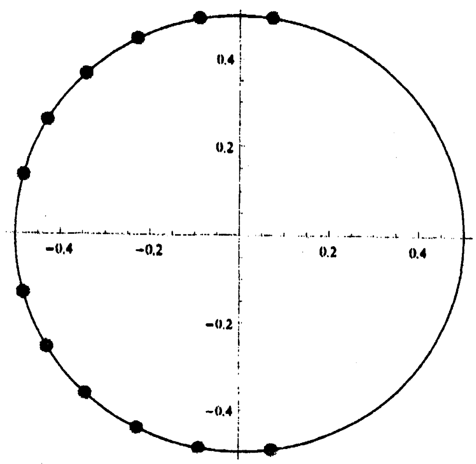
$$P_{F_{6k-2}^{IV}}(T) = \frac{4}{3}(T - \frac{1}{2}e^{i\frac{\pi}{3}})(T - \frac{1}{2}e^{-i\frac{\pi}{3}})P_{F_{6k}^{IV}}(T)$$

である。特に、Duursma の結果を考慮すれば、

$length = 6k - 2(k \in \mathbb{N})$ の Type IV extremal f.w.e. はリーマン仮説類似を満たす。

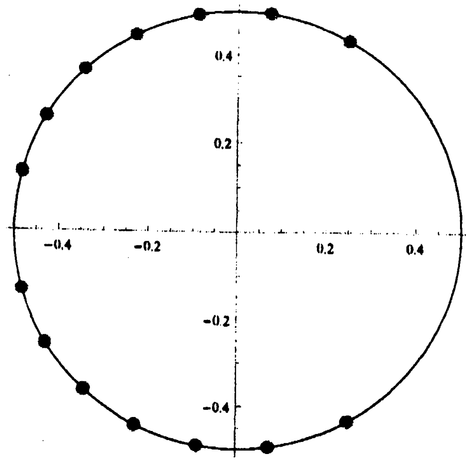
例;$P_{F_{42}^{IV}}(T)$ と $P_{F_{40}^{IV}}(T)$ の比較

$P_{F_{42}^{IV}}(T)$ の零点



(円の半径$=\frac{1}{2}$)

$P_{F_{40}^{IV}}(T)$ の零点



(円の半径$=\frac{1}{2}$)

零点の集合として、2 点 $\frac{1}{2}e^{i\frac{\pi}{3}}, \frac{1}{2}e^{-i\frac{\pi}{3}}$ 以外は完全に一致している。

主張の証明の核となるのは、次の補題である。

key lemma; F_{6k}^{IV} と F_{6k-2}^{IV} との関係

$$\frac{\partial_x^2+\frac{1}{3}\partial_y^2}{6k(6k-1)}F_{6k}^{IV}=F_{6k-2}^{IV}$$

(ただし $\partial_x := \frac{\partial}{\partial x}, \partial_y := \frac{\partial}{\partial y}$ としている)

この補題を認めれば、zeta 多項式の定義と関数等式の 1 番目の性質から、主張が得られる。

key lemma の証明の流れ

まず

(a) $F(x,y)$ が $length=n$ の TypeIV f.w.e. のとき、$(\partial_x^2+\frac{1}{3}\partial_y^2)F(x,y)$ は $length=n-2$ の TypeIV の f.w.e.

(b) $d_F \geq 2$ のとき、$d_{\partial_x^2+\frac{1}{3}\partial_y^2 F}=d_F-2$

を示す。

・(a) の証明

$x^2+\frac{1}{3}y^2$ は G_4^t の作用で不変である。ここで、よく知られた次の定理を用いる。(Duursma

2003(4) でも同じ定理を用いている)
定理「G を、$\mathbb{C}_n[x,y]$ に作用している $GL_2(\mathbb{C})$ の部分群とし、$F(x,y) \in \mathbb{C}_n[x,y]^G$ とする。
このとき $p(x,y) \in \mathbb{C}_i[x,y]^{G^t} (i \leq n)$ とすると、$p(\partial_x, \partial_y)F(x,y) \in \mathbb{C}_{n-i}[x,y]^G$ となる。」
この定理より $F(x,y)$ が $length = n$ の TypeIV f.w.e. なら $(\partial_x^2 + \frac{1}{3}\partial_y^2)F(x,y)$ は $length = n-2$ の TypeIV f.w.e. であることが分かる。

・(b) の証明
最小距離 d_F の定義より、$d_{\partial_x F} = d_F$ と、$d_F \geq 1$ なら $d_{\partial_y F} = d_F - 1$ であることが分かる。したがって $\partial_x^2 + \frac{1}{3}\partial_y^2$ は、y に関して 2 階微分であるから
$d_F \geq 2$ なら、 $d_{\partial_x^2 + \frac{1}{3}\partial_y^2 F} = d_F - 2$

・key lemma の証明
$\mathbb{C}[x,y]^{G_4} = \mathbb{C}[x^2+3y^2, (y(x^2-y^2))^2]$ であることから
(1)$length = 6k-2$ のとき $d_F \geq 2k$ となる TypeIV f.w.e. は、定数倍を除き一意的に存在する
という事と
(2)$length = 6k$ のとき $d_F \geq 2k+2$ となる TypeIV f.w.e. は、定数倍を除き一意的に存在する
ということが分かる。

まず (a) より $(\partial_x^2 + \frac{1}{3}\partial_y^2)F_{6k}^{IV}$ は $length = 6k-2$ の TypeIV の f.w.e. である。
更に、(2) より F_{6k}^{IV} の最小距離は $d_{F_{6k}^{IV}} \geq 2k+2$ であるが、(b) より $d_{(\partial_x^2 + \frac{1}{3}\partial_y^2)F_{6k}^{IV}} = d_{F_{6k}^{IV}} - 2 \geq 2k$
従って $(\partial_x^2 + \frac{1}{3}\partial_y^2)F_{6k}^{IV}$ は $length = 6k-2$ の TypeIV の f.w.e. で、最小距離が $2k$ 以上のものである。
(1) よりこのようなものは定数倍を除いて一意的に存在するから、extremal の定義と合わせて考えると、これは F_{6k-2}^{IV} の定数倍である。F_{6k-2}^{IV} が monic であることを考えて調整すると

$$\frac{\partial_x^2 + \frac{1}{3}\partial_y^2}{6k(6k-1)} F_{6k}^{IV} = F_{6k-2}^{IV}$$

となる。

これで key lemma が示せた。

5 TypeI,TypeIII での類似の結果

主結果での議論は、TypeIV extremal f.w.e. の関係性を微分作用素で見つけ、それを zeta 多項式の関係に翻訳するというものであった。TypeI extremal,TypeIII extremal でも同様の議論によって、

$$
\begin{gathered}
length = 8k \text{ の Type I extremal f.w.e. は、リーマン仮説類似を満たす。} \\
\Leftrightarrow length = 8k-2 \text{ の Type I extremal f.w.e. は、リーマン仮説類似を満たす。} \\
\left(\frac{\partial_x^2+\partial_y^2}{8k(8k-1)} F_{8k}^I = F_{8k-2}^I \text{ を用いる。}\right)
\end{gathered}
$$

$$
\begin{gathered}
length = 12k \text{ の Type I extremal f.w.e. は、リーマン仮説類似を満たす。} \\
\Leftrightarrow length = 12k-4 \text{ の Type I extremal f.w.e. は、リーマン仮説類似を満たす。} \\
\left(\frac{\partial_x^4+\partial_x\partial_y^3}{12k(12k-1)(12k-2)(12k-3)} F_{12k}^{III} = F_{12k-4}^{III} \text{ を用いる。}\right)
\end{gathered}
$$

を示すことができる。しかし TypeII では、同様の関係性は成り立ちそうにない。

References

(1) Iwan M. Duursma, Weight distributions of geometric Goppa codes, Trans. Amer. Math. Soc.351 (9) (1999) 3609-3639.

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

(3) Iwan M. Duursma, A Riemann hypothesis analogue for self-dual codes, in: A. Berg, S. Litsyn (Eds.), Codes and Association Schemes (Piscataway, NJ, 1999), American Mathematical Society, Providence, RI, 2001, pp. 115-124.

(4) Iwan M. Duursma, Extremal weight enumerators and ultraspherical polynomials, Discrete Math. 268 (1-3) (2003) 103-127.

(5) T.Harada, M.Tagami, A Riemann hypothesis analogue for invariant rings, Discrete Math. 307 (2007).