数理解析研究所講究録 1476 巻 2006 年 233-239



# Formal weight enumerator のゼータ関数とその Riemann 予想

大阪工業大学　工学部　知念 宏司　(Koji Chinen)
Department of Mathematics, Faculty of Engineering,
Osaka Institute of Technology.

**概 要**

1999 年, 論文 [4] において Iwan Duusma は初めて線型符号の zeta 関数を定義した. それは符号の重み多項式から構成されるが, 筆者らは [1], [8] において, 実在の符号の重み多項式でなくてもその zeta 関数が定義できることを指摘した. さらに, 知念 [2] においてはこの考えをさらに進め, formal weight enumerator と呼ばれる不変多項式に対してその zeta 関数を定義し, Duursma と同様の議論が展開できることを示した ([3] も参照). 本稿では, $x$ のみの項をもたない不変式に対して zeta 関数を定義し, その性質を調べる.

*Summary*

In 1999, Iwan Duursma defined the zeta functions for linear codes. They are constructed from the weight enumerators of codes. The author first exdended Duursma's theory to so-called "formal weight enumerators" in [2]. In this article, we define zeta functions for invariant homogeneous polynomials which do not have the term of $x$ only, and study some properties of them.

## 1 導 入

まず, 符号の zeta 関数についての Duursma の理論を概観する. $p$ を素数, $q=p^r$ $(r\geq 1)$ とし, $C$ を有限体 $\mathbf{F}_q$ 上の $[n,k,d]$ 符号とする. また $c\in C$ の Hamming 重さを $\mathrm{wt}(c)$ で表す. $A_i:=\sharp\{c\in C\,;\,\mathrm{wt}(c)=i\}$ とおくとき,

$$W_C(x,y):=\sum_{i=0}^{n}A_i x^{n-i}y^i$$

を $C$ の重み多項式と呼ぶ. これは $x,y$ の斉次 $n$ 次式である. 1999 年, 論文 [4] において Iwan Duusma は「符号の zeta 関数」を, 重み多項式の一種の母関数として定義した:

**定 義 1.1** $C$ に対して, 次数 $n-d$ 以下のある多項式 $P(T)\in\mathbf{Q}[T]$ がただ 1 つ存在して,

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n=\cdots+\frac{W_C(x,y)-x^n}{q-1}T^{n-d}+\cdots$$

が成立する. $P(T)$ を $C$ の **zeta 多項式**, $Z(T):=P(T)/\{(1-T)(1-qT)\}$ を $C$ の **zeta 関数**と呼ぶ.

多項式 $P(T)$ の存在と一意性に関しては, Duursma の論文に詳しく書かれていないが, 初等的証明が筆者らの総合報告 [1, pp.92-93], [8, p.44], および [2, pp.32-33] にある.

この定義にいう「符号の zeta 関数」に関して詳しいことは Duursma の論文 [5], [6] あるいは [1], [8] などをご参照いただきたいが, 彼の一連の結果のうち筆者にとって特に興味深いのは自己双対符号の zeta 多項式に対する関数等式

$$P(T) = P\Big(\frac{1}{qT}\Big)q^g T^{2g} \tag{1.1}$$

である ($g = n/2 + 1 - d$). これは代数曲線の zeta 多項式 (いわゆる合同 zeta 関数の分子) がもつ関数等式と全く同じ形であり, したがって「符号の Riemann 予想」を次のように定式化できる:

**定 義 1.2** $C$ を自己双対符号, その zeta 多項式を $P(T)$ とする. $P(T)$ の任意の根 $\alpha$ に対して,

$$|\alpha| = \frac{1}{\sqrt{q}}$$

が成り立つとき, $C$ は Riemann 予想を満たすという.

符号の Riemann 予想はすべての自己双対符号によって満たされるわけではなく, その必要十分条件を求めることはまだ未解決であるが, Duursma は

**問 題 1.3** 「Extremal な自己双対符号は Riemann 予想を満たす」は正しいか.

という問題を提出している ([6]). ここで, $\mathbf{F}_q$ 上の同じ符号長の自己双対符号のうち, 最小距離が最大のものを extremal という. そしていわゆる Type IV 自己双対符号に関してはこれを肯定的に解決している ([7]).

定義 1.1 を詳しく見てみると, $P(T)$ の存在と一意性の証明においては, $W_C(x,y)$ が実在する符号の重み多項式であることよりも, それが $x$, $y$ **の斉次 $n$ 次式であることがより本質的**であることがわかる (*cf.* [1, p.93], [2, p.33], [8, p.45]). この事実はすでに MDS 符号 (最大距離分離符号) の zeta 関数の考察において Duursma 自身によっても用いられている. しかしこのことに筆者はより積極的に注目し, 必ずしも符号と関連をもたない複素数係数の斉次多項式

$$W(x,y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \quad (A_d \neq 0) \tag{1.2}$$

に対してその zeta 多項式 $P(T)$ を, 全く同様に定義できることを指摘した ([2, p.40], このことは前述の [1], [2], [8] にある初等的証明を見れば明らかにわかる). さらにそこでは, そのような斉次多項式の実例として, 小関氏の formal weight enumerator (*cf.* [11]) を考えた. それは (1.2) の形の斉次式で, Type II 自己双対符号の重み多項式にきわめて似るが, 性質

$$W^{\perp}(x,y) := W^{\sigma_2}(x,y) = -W(x,y)$$

によって区別される. ただし,

$$\sigma_q = \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \tag{1.3}$$

であり, 1 次変換 $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の多項式 $f(x,y)$ への作用は $f^\sigma(x,y) = f(ax+by, cx+dy)$ とする.

式 (1.2) の formal weight enumerator に対して, $q=2$ とおいて zeta 多項式 $P(T)$ を定義すると, それは関数等式

$$P(T) = -P\Big(\frac{1}{2T}\Big)2^g T^{2g}$$

($g = n/2+1-d$) を満たし, Riemann 予想も本来の Duursma の理論と同様に

Formal weight enumerator $W(x,y)$ が Riemann 予想を満たす

$\underset{\text{def.}}{\Leftrightarrow}$ $P(T)$ のすべての根 $\alpha$ が $|\alpha| = \dfrac{1}{\sqrt{2}}$ を満たす

と定式化できることがわかった ([2, p.42]). さらに "extremal formal weight enumerator" という概念を導入すれば, Riemann 予想の成立, 不成立に関しても, 「extremal formal weight enumerator は Riemann 予想を満たす」ということが推測される実験結果が得られ ([2, p.42-43]), 「符号の zeta 関数」の理論において本質的役割を果たしているのは, 実在する符号ではなく, 重み多項式と同じタイプの斉次多項式自体が内在している何らかの性質であるらしいことがわかってきたのである ([2, p.43]).

なお, [2, §5] で述べた通り, formal weight enumerators と Type II 自己双対符号の重み多項式は, ともに不変式環 $\mathbf{C}[x,y]^{G_8}$ に含まれる ($G_8$ は Shephard-Todd [12] で分類された複素鏡映群の 1 つ). したがって, われわれは $\mathbf{C}[x,y]^{G_8}$ に含まれる (1.2) の形のすべての元に関して, 「extremal ならば Riemann 予想を満たす」という予想に到達することになる.

もちろん, $q=2$ 以外でも, $W^{\sigma_q}(x,y) = -W(x,y)$ を満たすような (1.2) の形の $W(x,y)$ があれば, その zeta 多項式が $P(T) = -P(\frac{1}{qT})q^g T^{2g}$ という関数等式を満たすのは明らかである. 筆者はそのような具体例として $q=3$ の場合を [3, §4] で扱っており, やはり「extremal なら Riemann 予想成立 ?」という数値的観察を行なっている.

本稿では, これまでとは違った形の斉次多項式を扱い, その zeta 関数の性質を調べることを目標とする. 具体的には,

$$f(x,y) = \sum_{i=d}^{n} A_i x^{n-i} y^i \quad (A_i \in \mathbf{C}, A_d \neq 0) \tag{1.4}$$

という形のものである. 主として, ある $q \in \mathbf{N}$ ($q \geq 2$) に対して, $f^{\sigma_q} = f$ を満たすものが考察の対象である (Duursma の理論からわかるように, この不変性があれば, zeta 関数は関数等式をもつ).

このような多項式を考える動機としては, まず Duursma の定義 (定義 1.1) においても必ず $x^n$ の項を取り除いていること (したがって, この形の多項式に対しても, zeta 多項式の定義が可能である), さらに (1.4) の形の不変式はさまざまな不変式環に実際に含まれていること, しかも同じ式が複数の不変式環に含まれることがしばしばあり, したがって, このような多項式を考えることで, 不変式環に依存しない, 何か「普遍的な」性質がわかるのではないか, という期待を持っていることである.

## 2 主結果

多項式 $f(x,y)$ は (1.4) の形で $d \geq 2$ (これはかなり本質的), また $q \in \mathbf{N}$, $q \geq 2$ とする. まず

**定 義 2.1** 多項式 $f(x,y)$ に対して次数 $n-d$ 以下のある多項式 $P_{f,q}(T) \in \mathbf{C}[T]$ がただ 1 つ存在して,

$$\frac{P_{f,q}(T)}{(1-T)(1-qT)}(y(1-T)+xT)^n = \cdots + \frac{f(x,y)}{q-1}T^{n-d} + \cdots$$

が成立する. $P_{f,q}(T)$ を $f(x,y)$ の zeta 多項式, $Z_{f,q}(T) := P_{f,q}(T)/\{(1-T)(1-qT)\}$ を $f(x,y)$ の zeta 関数と呼ぼう.

$P_{f,q}(T)$ の存在と一意性は定義 1.1 の場合と全く同様に証明できる. さらに (1.3) の $\sigma_q$ による不変性を導入すれば $P_{f,q}(T)$, $Z_{f,q}(T)$ はいろいろな性質をもつことがわかる:

**定 理 2.2** ある $q \in \mathbf{N}$, $q \geq 2$ に対して $f^{\sigma_q}(x,y) = f(x,y)$ とすると, 次が成り立つ:

(i) $\deg P_{f,q} = 2g \quad (g = n/2+1-d)$.

(ii) $P_{f,q}(T) = P_{f,q}(\frac{1}{qT})q^gT^{2g}$ (関数等式).

(iii) $(1-T)(1-qT) | P_{f,q}(T)$.

上の (iii) はなかなか不思議で, 定義 2.1 を見れば, 結局 $Z_{f,q}(T)$ の極が消えて多項式になってしまうということである. さらに

**定 理 2.3** ある $q \in \mathbf{N}$, $q \geq 2$ に対して $f^{\sigma_q}(x,y) = f(x,y)$ とすると, 任意の $q' \in \mathbf{N}$, $q' \geq 2$ に対して $(1-T)(1-q'T) | P_{f,q'}(T)$ であり,

$$(q-1)Z_{f,q}(T) = (q'-1)Z_{f,q'}(T)$$

が成り立つ.

つまり,

$$Z_f(T) := (q-1)Z_{f,q}(T) \tag{2.1}$$

は, $q$ に依存せず, $f(x,y)$ のみによって決まるということである (これはある意味,「不変式環によらない性質」と言えるかも知れない).

このように, 新しいタイプの zeta 関数が定義できたので, 次は Riemann 予想がどうなるかを調べよう. 上に述べたことから, $P_{f,q}(T)$ よりもむしろ (2.1) の $Z_f(T)$ の零点分布を調べるのが適当であろう. そこで次の定義をおく:

**定 義 2.4** ある $R > 0$ が存在して, $Z_f(T)$ のすべての根 $\alpha$ が $|\alpha| = R$ を満たすとき, $f(x,y)$ は Riemann 予想を満たすという.

つまり, $Z_f(T)$ の根がすべてある一定の半径の円周上に並んでいるときに $f(x,y)$ は Riemann 予想を満たすということにするのである.

実は, 数値実験から Riemann 予想を満たすと見られる $f(x,y)$ の無限系列がいくつか見つかっており, そのうちのある系列については, 実際に Riemann 予想を満たすことが証明できる. これを節を改めて見ていこう.

## 3 いくつかの具体例

ここでは次のような多項式の系列を考え, Riemann 予想について調べる:

$$\begin{aligned} f_m(x,y) &= \{xy(x^2-y^2)\}^m \quad (\deg f_m = 4m), \\ g_m(x,y) &= \{xy(x^4-y^4)\}^m \quad (\deg g_m = 6m), \\ h_m(x,y) &= \{y(x^3-y^3)\}^m \quad (\deg g_m = 4m), \\ t_m(x,y) &= \{y(x^2-y^2)\}^m \quad (\deg g_m = 3m), \\ u_m(x,y) &= \{y(x-y)\}^m \quad (\deg g_m = 2m), \end{aligned} \tag{3.1}$$

ただし, いずれも $m \geq 2$ とする. これらはいずれも, 実在の符号とのつながりを持っている. まず, いわゆる Type I 自己双対符号の重み多項式が含まれる不変式環は $\mathbf{C}[x^2+y^2, f_2(x,y)]$, 同様に Type II は $\mathbf{C}[x^8+14x^4y^4+y^8, g_4(x,y)]$, Type III は $\mathbf{C}[x^4+8xy^3, h_3(x,y)]$, Type IV は $\mathbf{C}[x^2+3y^2, t_2(x,y)]$, 最後に, $q$ を一般として, $\mathbf{F}_q$ 上の自己双対符号の重み多項式が含まれる不変式環は $\mathbf{C}[x^2+(q-1)y^2, u_1(x,y)]$ である (*cf.* [9, Chap.19], ここだけ $m=1$ が出てきてしまうが).

最も簡単なのは $u_m(x,y)$ で, 次が成り立つ:

**命 題 3.1** 任意の $m \geq 2$ に対し, $Z_{u_m}(T)$ は定数.

つまりこの場合は Riemann 予想を考えること自体できないことになる. 次に

**定 理 3.2** 任意の $m \geq 2$ に対し, $t_m(x,y)$ は $R = 1/2 (= 1/\sqrt{4})$ に対する Riemann 予想を満たす. つまり, $Z_{t_m}(T)$ のすべての根 $\alpha$ は $|\alpha| = 1/2$ を満たす.

他の系列に関しては証明できていることはないが, 次のことが予想される:

**予 想 3.3** 任意の $m \geq 2$ に対し, $f_m(x,y)$, $g_m(x,y)$ は $R = 1/\sqrt{2}$ に対する Riemann 予想, $h_m(x,y)$ は $R = 1/\sqrt{3}$ に対する Riemann 予想を満たす.

このように, これらの例はある $q$ に対して $\sigma_q$ の作用で不変という性質をもつが, その zeta 関数は本質的に $q$ によらず決まる. にもかかわらず, Riemann 予想を考えると, 明らかに特定の $q$ が重要な役割を果たしているということが見て取れる. 言わば, 各系列に「固有の」Riemann 予想があるらしいのである (どんな $q$ に対しても $\sigma_q$ で不変となる $u_m(x,y)$ の Riemann 予想が考えられないというのも, こう考えると納得できる話である).

これに関連して, 導入でも述べた, 「同じ (系列の) 式が複数の不変式環に含まれる」現象について, 少し観察しておこう.

例えば, 上記 $g_2(x,y)$ は, Shephard-Todd の群 $G_{13}$, $G_{15}$ 両方の不変式環の生成元として取れる (*cf.* 小関 [10, p.104]). また, $g_4(x,y)$ は, $\mathbf{C}[x,y]^{G_8}$, $\mathbf{C}[x,y]^{G_9}$ の生成元として取れることもわかる ($G_9$ に関しては [9, p.601] にある. $G_8$ についても同様に考えればよい). そしておもしろいのは, $g_2(x,y)$ が $\mathbf{C}[x,y]^{G_6}$ の生成元にもなっていることである (*cf.* [10, p.102]). なぜこれがおもしろいかというと, $G_6$ は $GL_2(\mathbf{C})$ の中で共役をとることで, ternary self-dual codes の重み多項式を不変にする群となるからである. そういう立場か

らは, この群は $q=3$ と関係が深いはずである. ところが上で見た通り, $g_2(x,y)$ は (たとえ $q=3$ として zeta 関数を作っても) $R=1/\sqrt{2}$ (つまり $q=2$) の Riemann 予想を満たすのである.

このように, (1.4) の形の多項式がそれぞれに固有の Riemann 予想を持っていることが, 種々の不変式環における Riemann 予想の成立, 不成立に, 何らかの影響を与えている可能性もあると筆者は感じている.

なお, (1.4) の形で $\sigma_q$ の作用で不変な多項式は (3.1) に挙げたものばかりではない. これらに不変多項式 ($x$ だけの項があってもなくても) を適当に掛けたものも当てはまる. 例えば $f_m(x,y)(x^2+y^2)^v(x^8+14x^4y^4+y^8)^w$ $(v,w\geq 0)$ は $\sigma_2$ 不変であるし, $u_m(x,y)(x^2+(q-1)y^2)^v$ $(v\geq 0)$ は $\sigma_q$ 不変 $(q\geq 2)$ となる. これらも $R=1/\sqrt{q}$ の Riemann 予想を満たすことが数値実験から見て取れる. こうした多項式の Riemann 予想の意味について考えることを今後の 1 つの課題としたい.

**謝 辞.** 九州大学の坂内英一先生には, 不変式環についていろいろとご教示頂いた. ここに感謝の意を表したい.

*Submitted on December 14, 2005.*

## 参考文献

[1] 知念 宏司, 平松 豊一 : 線形符号のゼータ関数とリーマン予想の類似 (Iwan Duursma の仕事の紹介), 符号と暗号の代数的数理, 京都大学数理解析研究所講究録 1361 (2004), 91-101.

[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] Chinen, K. : Zeta functions for formal weight enumerators and the extremal property, to appear in Proc. Japan Acad. (received on August 23, 2005).

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

[5] _____ : From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

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

[7] _____ : Extremal weight enumerators and ultraspherical polynomials, Discrete Math. **268**, No.1-3 (2003), 103-127.

[8] 平松 豊一, 知念 宏司 : 線形符号のゼータ関数とそのリーマン予想, 特集「符号化理論の新時代」, 数理科学 **497** (2004), 42 - 47.

[9] MacWilliams, F. J. and Sloane, N. J. A. : The Theory of Error-Correcting Codes, North-Holland, 1977.

[10] 小関 道夫 : 符号理論と unitary reflection groups の不変式環との関連について, 第12回代数的組合わせ論シンポジウム報告集 (1996), 96-116.

[11] Ozeki, M. : On the notion of Jacobi polynomials for codes, Math. Proc. Camb. Phil. Soc. **121** (1997), 15-30.

[12] Shephard, G. C. and Todd, J. A. : Finite unitary reflection groups, Canad. J. Math. **6** (1954), 274-304.