数理解析研究所講究録 1465 巻 2006 年 17-23

Formal weight enumerator のゼータ関数と Mallows-Sloane bound の類似

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. そこでも本来の Duursma の理論と同様 extremal という性質が重要な役割を果たしていることが観察された. 本稿では formal weight enumerator の extremal 性について, 定量的な特徴づけを行なう. 具体的には, Mallows-Sloane bound と類似の限界式を Duursma [7] の方法を応用することにより導出する.

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 introduce the notion of "extremal formal weight enumerators" and deduce a certain bound similar to the Mallows-Sloane bound. The method is an application of that of Duursma [7].

1 導 入

まず, 符号の zeta 関数についての Duursma の理論を概観しよう. 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. よく知られているように,

$$A_i := \sharp\{c \in C\ ;\ \mathrm{wt}(c) = i\}$$

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 は初めて符号の zeta 関数を定義した:

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.

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] あるいは筆者らの総合報告 [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 α 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]).

注意. よく知られているように, extremal 自己双対符号で実在するものは有限個である. したがって上記の問題も, 数値計算により解決可能であるという見方をされる読者もあるだろう. しかし, このあと述べるように, この問題はむしろ重み多項式自体の問題 (対応する符号の存在, 非存在に関係なく), さらに言えば重み多項式型の斉次多項式の問題と考えるべきであろう, というのが筆者の印象である.

さて, 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. しかし筆者はこのことに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]). 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 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

$$W^{\perp}(x,y) := W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = -W(x,y)$$

によって区別される (*cf.* 定義 2.1). 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

$$\begin{aligned} &\text{Formal weight enumerator } W(x,y) \text{ が Riemann 予想を満たす} \\ \underset{\text{def.}}{\Leftrightarrow}\ &P(T) \text{ のすべての根 } \alpha \text{ が } |\alpha| = \frac{1}{\sqrt{2}} \text{ を満たす} \end{aligned}$$

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]).

本稿では, 符号の重み多項式でない不変多項式の実例である formal weight enumerator に対して, その extremal 性を定義し, その「仮想的最小距離」すなわち (1.2) における d の評価を得ること (Duursma の方法の応用による直接証明) を目標とする.

2 Formal weight enumerators

まず formal weight enumerator を定義しよう:

定義 2.1 多項式 $W(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i \in \mathbf{C}[x,y]$ $(4|n)$ が次の (i), (ii) を満たすとき, $W(x,y)$ を formal weight enumerator という:

(i) $A_i \neq 0 \ \Rightarrow\ 4|i$,

(ii) $W^{\perp}(x,y) := W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = -W(x,y)$.

不変式論の立場からいうと, formal weight enumerator は不変式環 $\mathbf{C}[x,y]^{G_8}$ の元である. ここで, G_8 は Shephard-Todd による複素鏡映群の分類において No.8 と名づけられている群である ([14]):

$$G_8 := \left\langle \frac{1-i}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

$\mathbf{C}[x,y]^{G_8}$ の生成元は拡大 Hamming 符号の重み多項式 $W_8(x,y) = x^8 + 14x^4y^4 + y^8$ と $W_{12}(x,y) = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}$ であることが知られている. なお, formal weight enumerator という命名は小関道夫氏による ([12]). $W_{12}(x,y)$ は [12] において, Broué-Enguehard 写像により Eisenstein 級数 $E_6(z)$ を構成するのに用いられた. また, formal weight enumerator の一般形は

$$W_8(x,y)^l W_{12}(x,y)^{2m+1} \quad (l,m \geq 0), \tag{2.1}$$

およびそれらの適当な 1 次結合である.

次に extremal formal weight enumerator を定義しよう.

定 義 2.2 すべての n 次 formal weight enumerators のうち, 式 (1.2) における d が最大であるものを, extremal formal weight enumerator と呼ぶ.

上に述べたことから, formal weight enumerator の次数 n は $n \equiv 4 \pmod 8$ を満たす. $n = 12, 20, 28$ に対してはそれぞれ $W_{12}(x,y)$, $W_8(x,y)W_{12}(x,y)$, $W_8(x,y)^2W_{12}(x,y)$ が extremal となるが, $n \geq 36$ のときは, 同じ次数で形の違う formal weight enumerator が必ず複数存在するため, それらを組み合わせて y 低次の項を消去し, d がより大きなものを構成することができる:

例 2.3 $\deg W = 36$. 式 (2.1) の形の formal weight enumerator には次の 2 つがある:

$$\begin{aligned} W_8(x,y)^3 W_{12}(x,y) &= x^{36} + 9x^{32}y^4 - 828x^{28}y^8 - \cdots \\ W_{12}(x,y)^3 &= x^{36} - 99x^{32}y^4 + 3168x^{28}y^8 - \cdots. \end{aligned}$$

この場合,

$$\frac{11}{12} W_8(x,y)^3 W_{12}(x,y) + \frac{1}{12} W_{12}(x,y)^3 = x^{36} - 495x^{28}y^8 - 19005x^{24}y^{12} - \cdots$$

が extremal となる.

一般に, (2.1) の形の formal weight enumerator で同じ次数のものが m 個あれば, y^4, y^8, $\cdots$, $y^{4(m-1)}$ までが消去でき, $d = 4m$ となる. しかし, この計算は一種の連立 1 次方程式だから, ひょっとすると運よく y^{4m} も消えることがあるかも知れない. しかし実際にはそういうことは起きない, というのが次節で述べる限界式である.

3 Mallows-Sloane bound の類似

Type II 自己双対符号の場合, Mallows-Sloane bound とは次のような命題である:

定 理 3.1 (Mallows-Sloane [11]) 符号長 n の任意の Type II 自己双対符号の最小距離 d は

$$d \leq 4\left[\frac{n}{24}\right] + 4$$

を満たす. さらに, 等号が成り立つのは extremal 符号の場合, かつそのときに限る.

この定理は当初, 解析的方法で証明された (*cf.* [10, pp.624-628]). Formal weight enumerator に対しても同じ方法を適用して d の評価を得るのは計算が複雑となり困難である (がんばればできるかも知れないが). しかし, Duursma は [7] において代数的別証を与えており, その証明は formal weight enumerator に対しても通用する. したがって上の評価式は formal weight enumerator の d を次数 n で評価する式としても, 実は使える. しかし best-possible ではないのである. 実際, extremal formal weight enumerator を実際に構成してみると, d は次のようになる:

$n = \deg W$	extremal な $W(x,y)$ の d	$4\left[\frac{n}{24}\right]+4$
12	4	4
20	4	4
28	4	8
36	8	8
44	8	8
52	8	12
60	12	12
⋮	⋮	⋮

本節では, 上記の d を n で評価する best possible bound となる次の定理を示す:

定 理 3.2 Formal weight enumerator $W(x,y)$ を式 (1.2) の形に書くとき, d, n は次の式を満たす:

$$d \le 4\left[\frac{n-12}{24}\right]+4.$$

また, 等号が成り立つのは $W(x,y)$ が extremal のとき, かつそのときに限る.

以下, 証明の概略を述べる (詳しくは [3] を参照).

われわれの方法は前述の Duursma の方法を使った直接証明である. それを説明するため, 少し記号を導入する. 1 次変換 $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ に対して, 2 組の変数 (x,y), (u,v) が

$$(u,v) = (x,y)\sigma = (ax+cy, bx+dy) \tag{3.1}$$

という関係で結ばれているとする. 対応する微分作用素の関係は

$$\left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}\right) = \left(\frac{\partial}{\partial u}, \frac{\partial}{\partial v}\right)\sigma^{\mathrm{T}} = \left(a\frac{\partial}{\partial u} + b\frac{\partial}{\partial v}, c\frac{\partial}{\partial u} + d\frac{\partial}{\partial v}\right),$$

ここで, σ^{T} は σ の転置行列. さらに, 斉次多項式 $a(x,y)$, $p(x,y)$, $A(x,y)$ を取り, $p(x,y)(D)$ は作用素 $p(\partial/\partial x, \partial/\partial y)$ を表すものとする. するとまず, 次が成り立つ:

補 題 3.3

$$p((u,v)\sigma^{\mathrm{T}})(D)A(u,v) = p(x,y)(D)A((x,y)\sigma).$$

これは Duursma [7, Lemma 1] である.

基本的アイデアは, formal weight enumerator $W(x,y)$ と, 何か「よい」 $a(x,y), p(x,y)$ の間の

$$a(x,y)|p(x,y)(D)A(x,y) \tag{3.2}$$

という関係をまず見つける (よい $a(x,y), p(x,y)$ を見つけるといってもよい). これから直ちに (左辺の次数)≤(右辺の次数) という不等式が得られるが, 当然この式はパラメータ n, d を含むので, $a(x,y), p(x,y)$ が非常にうまく選んであれば, それがそのまま d を n で評価する best possible bound になる, という原理である. Duursma は $W(x,y)$ が Type II 自己双対符号の重み多項式である場合に

命 題 3.4 $d \geq 8$ のとき,

$$(xy)^{d-5}(x^4-y^4)^{d-5}|xy(x^4-y^4)(D)W(x,y).$$

を示すことで Type II 自己双対符号に対する Mallows-Sloane bound の別証明を与えている. この命題は $W(x,y)$ が formal weight enumerator の場合も成り立つ. われわれはさらに

命 題 3.5 $d \geq 8$ のとき,

$$(x^4+y^4)(x^4+6x^2y^2+y^4)|xy(x^4-y^4)(D)W(x,y).$$

を示すことで 定理 3.2 を示すことができた.

注 意. 定理 3.2 は保型形式の理論を使えば, いわゆる Siegel の定理から導くことも可能である. 例えば [9] の第 5 節を参照. 尤も, 定理 3.2 の主張をはっきりと明示してある文献はないように思われるが.

謝 辞. 筆者は, 文献 [9] をご教示頂いた坂内英一先生に, 感謝の意を表したい.

Submitted on September 30, 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 an analogue of the Mallows-Sloane bound, preprint.

[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] Ibukiyama, T : Application of modular forms to lattices (in Japanese), 第 2 回 保型形式周辺分野 スプリングコンファレンス報告集 (2004), 1-30.

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

[11] Mallows, C. L. and Sloane, N. J. A. : An upper bound for self-dual codes, Infor. and Control **22** (1973), 188-200.

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

[13] Pless, V. : Introduction to the Theory of Error-Correcting Codes, John Wiley & Sons, 1998 (Third Edition).

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

[15] Stichtenoth, H. : Algebraic Function Fields and Codes, Springer Verlag, 1993.