線型符号の zeta 関数とその Riemann 予想

知念 宏司 (近畿大学 理工学部 理学科)

JANT 17 (東京理科大学)
2007.7.7

「線型符号の zeta 関数」
— Iwan Duursma が初めて定義 (1999 年)

当初の動機 — Goppa 符号の重み分布を知りたい
⇒ 有理関数体の場合の考察から一般の線型符号へ

自己双対符号の zeta 関数 — 代数曲線の場合と似るが...

Riemann 予想 — 満たす符号とそうでないものがある.

今日の内容

- 線型符号の zeta 関数 (Duursma の理論) 紹介 (前半 40 分ぐらい)
- 最近の結果の紹介

1. Zeta 関数の定義

p : 素数, $q = p^r$ $(r \geq 1)$, $\mathbf{F}_q$: 有限体 $(\sharp \mathbf{F}_q = q)$.

C : $\mathbf{F}_q$ 上の $[n, k, d]$ 符号.

$W_C(x, y) := x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i$: C の重み多項式.

— x, y の斉次 n 次式であることに注意.

以下 $d, d^\perp \geq 2$ とする $(d^\perp$: 後出$)$.

定 義 1. C に対し, $n - d$ 次以下の多項式 $P(T) \in \mathbf{Q}[T]$ がただ 1 つ存在し,

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

となる.

$P(T)$: C の zeta 多項式,
$Z(T) = \frac{P(T)}{(1-T)(1-qT)}$: C の zeta 関数と呼ぶ.

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

この式の見方

左辺は T **の有理式** $\Rightarrow$ $\frac{1}{1-T} = 1+T+T^2+\cdots,$
$\frac{1}{1-qT} = 1+qT+q^2T^2+\cdots$

i.e. (左辺)=

$$P(T)(1+T+T^2+\cdots)(1+qT+q^2T^2+\cdots)(y(1-T)+xT)^n$$

さらに展開 $\Rightarrow$ T^{n-d} **の係数に** C **の重み多項式が現れる.**

$\downarrow$

符号の zeta = 重み多項式の母関数.

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

$P(T)$ はなぜ一意に決まる ?

まず,

$$f(T) := \frac{(y(1-T)+xT)^n}{(1-T)(1-qT)}$$

を考える ($P(T)=1$ **とした場合). これの展開を**

$$c_0 + c_1T + c_2T^2 + c_3T^3\cdots$$

とするとき, 係数 $c_0, \cdots, c_{n-d}$ **は** x, y **の斉次式.**
詳しくは ...

$$f(T)=\frac{(y(1-T)+xT)^n}{(1-T)(1-qT)}=c_0+c_1T+c_2T^2+\cdots+c_{n-d}T^{n-d}+\cdots$$

$\exists b_{ij}\in\mathbf{Z}$ **があり,**

$$\begin{aligned}
c_0 &= && && y^n\\
c_1 &= && b_{10}\,xy^{n-1} && +b_{11}\,y^n\\
&\cdots && \cdots\cdots\cdots &&\\
c_i &= && b_{i0}x^iy^{n-i}+\cdots+b_{i,i-1}\,xy^{n-1} && +b_{ii}\,y^n\\
&\cdots && \cdots\cdots\cdots &&\\
c_{n-d} &= && b_{n-d,0}x^{n-d}y^d+\cdots+b_{n-d,n-d-1}\,xy^{n-1} && +b_{n-d,n-d}\,y^n
\end{aligned}$$

実は $b_{i0}\neq 0\Rightarrow$ **組合わせて** $W_C(x,y)-x^n$ **が作れる！**

$$W_C(x,y):=x^n+\sum_{i=d}^{n}A_ix^{n-i}y^i$$

$$f(T)=y^n+\{b_{10}xy^{n-1}+b_{11}y^n\}T+\cdots+\{b_{n-d,0}x^{n-d}y^d+\cdots+b_{n-d,n-d}y^n\}T^{n-d}+\cdots$$

$a_0,\ a_1,\ \cdots,\ a_{n-d}$**: given として,**
$(a_0+a_1T+\cdots+a_{n-d-1}T^{n-d-1}+a_{n-d}T^{n-d})f(T)$ **の** T^{n-d} **の係数は**

$$\begin{aligned}
& && && a_{n-d}y^n\\
& && && +a_{n-d-1}\{b_{10}xy^{n-1}+b_{11}y^n\}\\
& && && \cdots\cdots\cdots\\
& && +a_i\{b_{i0}x^iy^{n-i}+\cdots && +b_{ii}y^n\}\\
& && && \cdots\cdots\cdots\\
& +a_0\{b_{n-d,0}x^{n-d}y^d+\cdots && && +b_{n-d,n-d}y^n\}
\end{aligned}$$

これが $\frac{W_C(x,y)-x^n}{q-1}$ **に一致するように** $a_0,\ a_1,\ \cdots,\ a_{n-d}$ **を決めたのが** $P(T)$**.**

$$W_C(x,y):=x^n+\sum_{i=d}^{n}A_ix^{n-i}y^i$$

注 意. この証明の本質

$\cdots$ $W_C(x,y)$ が x, y の斉次 n 次式であること

(符号 C が実在することではなく).

必ずしも実在しない符号も理論の核心部分で使われている.

それは ...

---

2. MDS 符号と Zeta 関数

定 義 2. $[n,k,d]$ 符号が MDS 符号 (最大距離分離符号)

$\underset{\text{def.}}{\Leftrightarrow}$ $d = n-k+1$

● 「Singleton の限界式」 $d \le n-k+1$ で等号成立の場合. 必ずしも実在しない).

e.g., $\mathbf{F}_2$ 上 の MDS 符号は $[n,1,n]$, $[n,n-1,2]$, $[n,n,1]$ のみ (自明な MDS 符号).

● 重み多項式はつねに (形式的に) 作れる:

例. $M_{n,d}(x,y) = M_{5,3}(x,y) = x^5 + 10x^2y^3 - 5xy^4 + 2y^5$.

↑ n,d のみで決まる ($k = n-d+1$)　　負の係数 ↑ ($\Rightarrow$ 符号は実在しない)

● MDS 符号は符号の zeta でも重要な役割を果たす:

定 理 2. C が MDS $\Leftrightarrow$ $P(T) = 1$.

定 理 3. C の zeta 多項式が $P(T) = a_0 + a_1T + \cdots + a_rT^r$

$\Leftrightarrow$ $W_C(x,y) = a_0M_{n,d}(x,y) + a_1M_{n,d+1}(x,y) + \cdots + a_rM_{n,d+r}(x,y)$.

符号の zeta $\Leftrightarrow$ $W_C(x,y)$ の MDS 符号による表示.

3. 関数等式

C : $[n,k,d]$ 符号 $/\mathbf{F}_q$,
$C^\perp$: C の双対符号 ($[n,k^\perp(=n-k),d^\perp]$ 符号とする).

$P(T)$: C の zeta 多項式, $P^\perp(T)$: $C^\perp$ の zeta 多項式.

定 理 4.

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

$$\begin{aligned} g &:= n+1-k-d \ (C \text{ の種数}), \\ g^\perp &:= n+1-k^\perp-d^\perp(=k+1-d^\perp). \end{aligned}$$

関数等式

$C^\perp = C$ (自己双対) なら $P(T) = P^\perp(T)$, $g^\perp = g$ より

系.

$$P(T) = P\left(\frac{1}{qT}\right) q^g T^{2g} \ (\text{関数等式}).$$

Zeta 関数 $Z(T) = P(T)/(1-T)(1-qT)$ で表せば

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

関数等式は $C^\perp = C$ $(W_{C^\perp}(x,y) = W_C(x,y))$ の帰結

合同 zeta と 符号の zeta, 関数等式は全く同じ !

4. Riemann 予想

C: 自己双対 $[n, \frac{n}{2}, d]$ 符号 /$\mathbf{F}_q$, $P(T)$: その zeta 多項式.

代数曲線の場合と全く同様に,

定 義 3. C が Riemann 予想を満たす

$$\underset{\text{def.}}{\Leftrightarrow} P(T) \text{ の} \forall \text{根 } \alpha \text{ に対し } |\alpha| = \frac{1}{\sqrt{q}}.$$

問 題 1. Riemann 予想を満たす自己双対符号を特徴づけよ. $\cdots$ 重要な未解決問題

「よい符号は Riemann 予想を満たす」であってほしいが ...

Duursma の観察と extremal codes

Duursma の問題:

問 題 2.「extremal 自己双対符号は Riemann 予想を満たす」は正しいか ?

定 義 4. 符号長 n の自己双対符号で, 最大の最小距離を持つものを extremal code という (確かによい性質だ).

● 重み多項式でいえば, $W_C(x, y) := x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i$ の d が (同じ n の中で) 最大のもの.

● とくに「I 型」$\sim$「IV 型」自己双対符号に対して言うことが多い.

注 意. Extremal code の存在，非存在の問題．例えば $[72, 36, 16]$ extremal code $/\mathbf{F}_2$ が存在するか？ — 30 年来の未解決問題.

それでも重み多項式は (形式的に) 作れて Riemann 予想を満たす.

符号の zeta の Riemann 予想は (実在の符号ではなく) 斉次多項式の問題と見るべき ？

$[72, 36, 16]$ **extremal/$\mathbf{F}_2$:** $W_{72}(x, y) = x^{72} + 249849x^{56}y^{16} + 18106704x^{52}y^{20} + 462962955x^{48}y^{24} + 4397342400x^{44}y^{28} + 16602715899x^{40}y^{32} + 25756721120x^{36}y^{36} + 16602715899x^{32}y^{40} + 4397342400x^{28}y^{44} + 462962955x^{24}y^{48} + 18106704x^{20}y^{52} + 249849x^{16}y^{56} + y^{72}$.

Duursma の結果

定 理 5 (Duursma, 2003). IV 型 extremal code はすべて Riemann 予想を満たす.

● IV 型 extremal code で実在するのは有限個 (I∼III も).

しかし重み多項式は形式的に無限個作れて，そのすべてが Riemann 予想を満たす.

● I ∼ III 型については未解決.

いくつかの例 ($\mathbf{F}_2$ 上)

n	符号	パラメータ	重み多項式	$P(T)$	RH	コメント
2	$C_2 = \{00, 11\}$	$[2, 1, 2]$	$x^2 + y^2$	**1**	–	trivial MDS
4	$C_2 \oplus C_2$	$[4, 2, 2]$	$(x^2 + y^2)^2$	$\frac{1}{3}(1 + 2T^2)$	○	extremal
6	$C_2 \oplus C_2 \oplus C_2$	$[6, 3, 2]$	$(x^2 + y^2)^3$	$\frac{1}{5}(1 + 4T^4)$	○	extremal
8	C_8 (拡大 Hamming)	$[8, 4, 4]$	$x^8 + 14x^4y^4 + y^8$	$\frac{1}{5}(1 + 2T + 2T^2)$	○	extremal type II
8	$C_2 \oplus C_2 \oplus C_2 \oplus C_2$	$[8, 4, 2]$	$(x^2 + y^2)^4$	$\frac{1}{35}(5 - 2T^2 - 4T^3 - 4T^4 + 40T^6)$	○	!
10	$C_8 \oplus C_2$	$[10, 5, 2]$	$(x^8 + 14x^4y^4 + y^8) \cdot (x^2 + y^2)$	$\frac{1}{45}(1 + 2T^2 + 4T^3 + 6T^4 + 8T^5 + 8T^6 + 16T^8)$	×	
10	${C_2}^5$	$[10, 5, 2]$	$(x^2 + y^2)^5$	$\frac{1}{63}(7 - 4T^2 - 8T^3 - 12T^4 - 16T^5 - 16T^6 + 112T^8)$	○	!
10	(存在しない)	$[10, 5, 4]$	$x^{10} + 15x^6y^4 + 15x^4y^6 + y^{10}$	$\frac{1}{14}(1 + 2T + 3T^2 + 4T^3 + 4T^4)$	○	extremal
24	$C_8 \oplus C_8 \oplus C_8$	$[24, 12, 4]$	略	略	×	type II
72	(存在は不明)	$[72, 36, 16]$	略	略	○	extremal type II

「Riemann 予想成立 $\Rightarrow$ extremal」でないことは確か.

例 (Komichi, 九州大学修士論文 2005). 実在する II 型 $[32, 16, 4]$ code で Riemann 予想を満たすものがある.

$n = 32$ の II 型 extremal は $d = 8$. 上の符号は extremal ではない.

Riemann 予想成立のための必要十分条件はまだわからない

5. 最近の結果

再掲:

> **符号の zeta の Riemann 予想は (実在の符号ではなく) 斉次多項式の問題と見るべき ?**

⇒ 符号から離れて, Riemann 予想を満たす不変式 (仮想的符号の重み多項式) をたくさん見つけたい.

こうした方向での結果がいくつかある.

不変式について

$W_{C^\perp}(x,y) = W_C(x,y)$ **とは** $\cdots$ $\sigma_q := \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}$ **のとき**

$$W_C{}^{\sigma_q}(x,y) = W_C(x,y)$$

であること ($W \mapsto W^{\sigma_q}$: **MacWilliams 変換**). **ただし,**

$$f^\sigma(x,y) = f(ax+by, cx+dy)$$

$$(f(x,y) \in \mathbf{C}[x,y],\ \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}).$$

● $W^{\sigma_q}(x,y) = W(x,y)$ **となる** W

$$\in \mathbf{C}[x,y]^{\langle\sigma_q\rangle} = \mathbf{C}[xy(x-y), x+(\sqrt{q}-1)y]$$

$\cdots$ **不変式環の例.**

Formal weight enumerators

Formal weight enumerator (以下 FWE) とは $\mathbf{C}[x,y]^{G_8}$ $(G_8 := \left\langle \frac{1-i}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix} \right\rangle)$ **の元で,**

$$W(\tfrac{x+y}{\sqrt{2}}, \tfrac{x-y}{\sqrt{2}}) = -W(x,y)$$

となるもの.

- **II 型符号の重み多項式なら** $W(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}) = W(x,y)$**.**
- $\mathbf{C}[x,y]^{G_8} = \mathbf{C}[W_{12}(x,y), W_{C_8}(x,y)]$**.**
  $\cdots$ $\mathbf{F}_2$ **上の符号と関連.**
- $W_{12}(x,y) = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}$ **は FWE の例.**

FWE $W(x,y) = x^n + \sum_{i=d}^{n} A_i x^{n-i}y^i$ **を** $\mathbf{F}_2$ **上の仮想的** $[n, \frac{n}{2}, d]$ **符号の重み多項式と見よう.**

- **関数等式は**

$$P(T) = -P\left(\frac{1}{2T}\right) 2^g T^{2g} \quad (g = \frac{n}{2} + 1 - d)$$

Riemann 予想を

「$P(T)$ **のすべての根が** $|T| = 1/\sqrt{2}$ **上」**

と定義.

例. $W_{12}(x,y) = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12} \Rightarrow$

$$P(T) = \frac{1}{15}(2T^2-1)(2T^2+1)(2T^2+2T+1)$$

$\cdots$ **Riemann 予想成立！**

数値実験では, 実在の符号の場合と同様

「extremal FWE $\Rightarrow$ Riemann 予想成立 ?」

らしい.

→ **KC, Proc. Japan Acad. 81 Ser. A. (2005), 168 - 173.**

この方向で $\cdots$

Tagami, 数理研講究録 1476(2006), 96 − 104:

● $|T| = 1/\sqrt{q}$ **上にある** $P(T)$ **の根の個数を数えるアルゴリズム提案 (Sturm の定理利用. 根の近似計算ではない).**

● **種々の不変式環 (or その部分環) の考察, e.g.,**

定 理 6. $R = \mathbf{C}[x+y, y(x^2-y^2)]$ **の extremal 多項式 (次数** $\equiv 5 (\mathrm{mod}\ 6)$**) は** $q = 4$ **で Riemann 予想を満たす (証明: Duursma と同様の手法).**

など

※ R **自身は不変式環ではなく,** $\mathbf{C}[x,y]^{\langle \sigma_4 \rangle}$ **の部分環.**

種数 1 の場合

自己双対 $[n, \frac{n}{2}, d]$ **符号** C **の種数：** $g = \frac{n}{2} + 1 - d$.

● **zeta 多項式** $P(T)$ **について** $\deg P = 2g$.

$$g = 1 \Leftrightarrow P(T) \text{ は 2 次式 (そして } n = 2d)$$

定 理 7 (Nishimura). C: **種数 1, 自己双対** $/\mathbf{F}_q$, $W_C(x, y) = x^n + A_d x^{n-d} y^d + \cdots$ **：その重み多項式のとき,**

$$\boxed{\begin{array}{l} C \text{ が Riemann 予想を満たす} \\ \Leftrightarrow \frac{\sqrt{q}-1}{\sqrt{q}+1}\binom{2d}{d} \le A_d \le \frac{\sqrt{q}+1}{\sqrt{q}-1}\binom{2d}{d}. \end{array}}$$

→ **学会アブストラクト (西村 - 斎藤 - 平松, 2005 年 9 月, 岡山大, 代数分科会), p.26**

$$\boxed{\frac{\sqrt{q}-1}{\sqrt{q}+1}\binom{2d}{d} \le A_d \le \frac{\sqrt{q}+1}{\sqrt{q}-1}\binom{2d}{d}}$$

例. $n = 8$, $d = 4$, $q = 2$. **このとき**

$$\frac{\sqrt{2}-1}{\sqrt{2}+1}\binom{8}{4} \approx 12.0101, \quad \frac{\sqrt{2}+1}{\sqrt{2}-1}\binom{8}{4} \approx 407.9898$$

$W_{C_8}(x, y) = x^8 + 14x^4y^4 + y^8$ **(拡大 Hamming) は確かに条件を満たし** $(A_d = A_4 = 14)$**,**

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

(限定的とはいえ) Riemann 予想成立のための必要十分条件を与えた初めての結果.

$\mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ で起きていること

$\mathbf{C}[x,y]^{\langle\sigma_q\rangle} = \mathbf{C}[x+(\sqrt{q}-1)y, y(x-y)]$

$\cdots W^{\sigma_q} = W$ $\left(\sigma_q = \frac{1}{\sqrt{q}}\begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix}\right)$ となる $W(x,y)$ 全体の環 (自己双対/$\mathbf{F}_q$ の重み多項式全体より「少し広い」).

$P(T)$: $W(x,y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i \in \mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ の zeta 多項式.

「$W(x,y)$ が Riemann 予想を満たす
$\underset{\text{def.}}{\Leftrightarrow}$ $P(T)$ のすべての根 α が $|\alpha| = \frac{1}{\sqrt{q}}$ を満たす.」

定理 7(KC, arXiv:0704.3903). $\mathbf{C}[x,y]^{\langle\sigma_q\rangle}$ において, $2 \le d \le \frac{n+1}{2}$ となる任意の n, d に対し, Riemann 予想を満たす $W(x,y)$ が存在する.

"Extremal" $\cdots$ $W(x,y) := x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i$ の d が (同じ n の中で) 最大のもの.

条件 $2 \le d \le \frac{n+1}{2}$: 可能な n, d の組はほぼ全部カバー.

$\mathbf{C}[x,y]^{\langle\sigma_q\rangle} = \mathbf{C}[x+(\sqrt{q}-1)y, y(x-y)]$ では Riemann 予想と extremal は無関係!

証明の概略

適当な $[n, k, d]$ **符号** C **をとり,**

$$\tilde{W}_C(x, y) := \frac{1}{1 + q^{k-n/2}}\{W_C(x, y) + q^{k-n/2} W_{C^\perp}(x, y)\}$$

とすれば $\tilde{W}_C(x, y) \in \mathbf{C}[x + (\sqrt{q} - 1)y, y(x - y)]$

(W_C **と** $W_{C^\perp}$ **が「互いに移り合」い全体として不変**).

C**: MDS 符号** $\Rightarrow$ $\tilde{W}_C(x, y)$ **の zeta 多項式は**

$$(\textbf{const.})\{1 + (\sqrt{q}T)^{n+2-2d}\}.$$

すべての根は $|T| = 1/\sqrt{q}$ **上.**

他に C **として**

- **一般 Hamming 符号 (無限個, 一部の系列を除く)**
- **(自己双対でない) Golay 符号 (2 個)**

を取っても, $\tilde{W}_C(x, y)$ **は Riemann 予想を満たすことがわかった.**

(arXiv:0704.3903)

6. まとめ

● **Duursma の問題は「extremal code ⇒ Riemann 予想成立 ?」**

● **Extremal でなくて Riemann 予想成立の例もある.**

● **符号以外の不変式にも拡張可能で, 考える不変式の範囲によって様々な現象が見られる.**

問題:

「不変式の Riemann 予想」がそれなりの (妥当な) 意味をもつ枠組みは何か ?

参考文献

[D1] Duursma, I. : Weight distribution of geometric Goppa codes, Trans. Amer. Math. Soc. **351**, No.9 (1999), 3609-3639.

[D2] _____ : From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

[D3] _____ : A Riemann hypothesis analogue for self-dual codes, DIMACS series in Discrete Math. and Theoretical Computer Science **56** (2001), 115-124.

[D4] _____ : Extremal weight enumerators and ultraspherical polynomials, Discrete Math. **268**, No.1-3 (2003), 103-127.

[S1] 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.

[S2] 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.

[S3] 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, または `http://www.math.is.tohoku.ac.jp/~taya/sendaiNC/2004/program.html`.

[C1] Chinen, K. : Zeta functions for formal weight enumerators and the extremal property, Proc. Japan Acad. **81** Ser. A. (2005), 168 - 173.

[C2] _____ : An abundance of invariant polynomials satisfying the Riemann hypothesis, preprint, arXiv:0704.3903.

[NSH] 西村 滋人, 斎藤 正顕, 平松 豊一 : On a Riemann hypothesis analogue of genus 1 for the selfdual weight enumerators, 日本数学会 代数分科会 講演アブストラクト (2005.9, 岡山大学), p.26.

[T] 田上 真『不変式環の Riemann 仮説類似に対する考察』, 代数的組合せ論とその周辺, 京都大学数理解析研究所講究録 1476 (2006), 96-104.