楕円曲線から得られる代数幾何符号のゼータ関数について

名古屋工業大学大学院 工学専攻 情報工学系プログラム 情報数理分野
金子 尚弥 (Naoya KANEKO)

1 導入

数学では様々な分野でゼータ関数が考えられているが,1999 年に [1] において Iwan Duursma によって符号に対してもゼータ関数が定義され,[2] では (自己双対符号に対して) リーマン予想の類似も定式化された. また,1980 年代に Goppa は有限体上の代数曲線とその有理点から代数幾何符号と言われる符号を作った. 本講演では楕円曲線から得られる代数幾何符号のゼータ関数の性質, 特にリーマン予想についてわかったことを紹介する. 構成としては 2 節で符号理論の簡単な説明と符号のゼータ関数を定義してリーマン予想の類似を定式化し, 3 節では代数幾何符号を定義して一般的に成り立つ性質をみる. そしてメインの 4 節では楕円曲線から得られる代数幾何符号のゼータ関数を計算機を用いて具体的な計算をした結果やその考察を述べる.

2 符号のゼータ関数とリーマン予想

符号理論とは情報工学における 1 つの分野であり, コンピュータで通信する際に生じる情報の欠落や誤りなどを検出して修正する機能を持つ符号というものを研究する. ここでは, 符号理論に関する必要最低限のことをまとめる. 主な参考文献は [6],[7],[8] である. 以下では q は素数のべき乗とする.

定義 2.1. 有限体 $\mathbb{F}_q$ 上の n 次元ベクトル空間 $\mathbb{F}_q^n$ の部分空間 C を ($\mathbb{F}_q$上の) **線形符号**あるいは単に**符号**といい, C の元のことを符号語という. C の基底を $x_1, \cdots, x_k$ とするとき, それらを並べた $k \times n$ 行列を C の**生成行列**という. このとき C は生成行列 G を用いて

$$C = \{(a_1, \cdots, a_k)G \mid a_i \in \mathbb{F}_q\}$$

と表せる.

一般に符号 C が大きいほどより多くの情報を伝えることができ,$\mathbb{F}_q^n \setminus C$ が大きいほど誤り訂正の能力が高くなる. 符号理論では相反するこの 2 つの条件を満たすような効率のよい符号を作ることが目標である. 次に $\mathbb{F}_q^n$ に距離を定義する.

定義 2.2. $x = (x_1, x_2, \cdots, x_n), y = (y_1, y_2, \cdots, y_n) \in \mathbb{F}_q^n$ に対して

$$d(x, y) := \#\{1 \leq i \leq n \mid x_i \neq y_i\}$$

とする. ここで有限集合 S に対して $\#S$ は S の元の個数を表す. このとき $d(x, y)$ は $\mathbb{F}_q^n$ 上の距離と

なり, ハミング距離という. 符号 C の**最小距離** d を

$$d := \min\{d(x,y) \mid x,y \in C, x \neq y\}$$

で定める.

定義 2.3. $x \in \mathbb{F}_q^n$ に対して

$$\mathrm{wt}(x) := d(x,0) = \{1 \leq i \leq n \mid x_i \neq 0\}$$

を x の重さという. また, 符号 C の最小重み w を

$$w := \min\{\mathrm{wt}(x) \mid x \in C, x \neq 0\}$$

とする. $d(x,y) = d(x-y,0) = \mathrm{wt}(x-y)$ であることから符号の**最小距離と最小重みは一致している**ことに注意する.

定義 2.4. $\mathbb{F}_q^n$ の符号 C が k 次元で最小距離が d のとき $[n,k,d]$ 符号と表す. 符号理論での意味は k が大きいほど多くの情報を送信でき,d が大きいほど多くの誤りを訂正できる. また

$$C^{\perp} = \{x = (x_1, \cdots, x_n) \in \mathbb{F}_q^n \mid x^t y = x_1 y_1 + \cdots + x_n y_n = 0 \ (\forall y = (y_1, \cdots, y_n) \in C)\}$$

は $[n, n-k, d^{\perp}]$ 符号であり C の**双対符号**という.

n,k,d の間には様々な制限が知られており, ここでは 1 つだけ紹介する.

定理 2.5. $[n,k,d]$ 符号 C は

$$d \leq n - k + 1$$

を満たす. これをシングルトン限界式という. また, この不等式が等号となる符号のことを MDS (***maximum distance separable***) **符号**という.

次に符号のゼータ関数を定義するために符号の重さの分布を表した重さ多項式 (weight enumerator) を定義する.

定義 2.6. 符号 C に対して

$$A_i := \#\{w \in C \mid \mathrm{wt}(w) = i\}$$

とするとき,n 次斉次多項式

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

を C の重さ多項式という.

定義 2.7. $[n,k,d]$ 符号 C に対して

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

を満たす高々 $n-d$ 次の多項式 $P(T) \in \mathbb{Q}[T]$ が一意的に存在する. この $P(T)$ を C の**ゼータ多項式**といい $Z(T) = P(T)/((1-T)(1-qT))$ を C のゼータ関数という.

この定義が表しているのは $P(T)$ をうまくとることで左辺を級数展開したときに T^{n-d} の係数に重さ多項式が現れるようにできるということである. 証明の概略としては $P(T) = a_0 + a_1T + \cdots + a_{n-d}T^{n-d}$ とすると定義の条件から $a_0, \cdots, a_{n-d}$ を未知数とする連立方程式が得られてその解が一意的に定まるという流れである (より詳しい証明として [4] を参照). ゼータ多項式 $P(T)$ の性質として次が知られている (証明は [3] を参照).

命題 2.8. $[n, k, d]$ 符号 C のゼータ多項式を $P(T)$ とし,C の双対符号である $[n, n-k, d^\perp]$ 符号 $C^\perp$ のゼータ多項式を $P^\perp(T)$ とする. $d^\perp \geq 2$ のとき
(1) $\deg P(T) = n + 2 - d - d^\perp$.
(2) $P(1) = 1$.
(3) $P^\perp(T) = q^g T^{g+g^\perp} P(1/qT)$.
ここで $g = n + 1 - k - d, g^\perp = n + 1 - k^\perp - d^\perp$ であり g を C の種数という (この名の由来は合同ゼータ関数の関数等式の類似からである).
(4) MDS 符号のゼータ多項式は 1 であり, その逆も成り立つ.

$C = C^\perp$ となるとき C を自己双対符号というが, このとき $P(T) = P^\perp(T)$ だから命題の (3) よりゼータ多項式は関数等式

$$P(T) = q^g T^{2g} P(1/qT)$$

を満たす. これは合同ゼータ関数の関数等式と同じ形である (合同ゼータ関数については 3 節で詳しく述べる). そこで Duursma は自己双対符号に対してリーマン予想の類似を合同ゼータ関数のリーマン予想に沿って定義したが, ここでは自己双対とは限らない一般の符号に対して次のようにリーマン予想の類似を定式化する.

定義 2.9. $\mathbb{F}_q$ 上の符号 C が**リーマン予想を満たす**とは,C のゼータ多項式の根の大きさが $1/\sqrt{q}$ となることである. つまり

$$P(\alpha) = 0 \implies |\alpha| = \frac{1}{\sqrt{q}}$$

となることである.

4 節でみるようにリーマン予想を満たす符号も, 満たさない符号もどちらも存在する. このように符号によってリーマン予想の成立の可否が変わるが, リーマン予想を満たす符号の特徴づけはいまだにわかっていない. また, 符号のリーマン予想を考える意味としては次のように符号の最小距離の評価が得られることである (証明は [2]).

定理 2.10. $\mathbb{F}_q$ 上の $[n, k, d]$ 符号のゼータ多項式を $P(T) = a_0(1 + aT + \cdots)$ の形で表したとき

$$d \leq q + a$$

が成り立つ.

ここで $P(T)$ の根を $\alpha_1, \cdots, \alpha_r$ とすると

$$|a| = \left| \sum_{i=1}^{r} \frac{1}{\alpha_i} \right|$$

だから根の大きさの評価は C の最小距離 d の評価を与えていることがわかる (先にも述べた通り, 符号理論において d は重要な量の 1 つであった). このように符号のリーマン予想は単なる類似だけではなくて, それ自身の意味ももっているのである.

3 代数幾何符号

ここでは有限体上の代数曲線とその有理点から符号が作れることを説明する. さらに, 合同ゼータ関数についても簡単に触れる. 2 節でみたように, 符号とは $\mathbb{F}_q^n$ の部分空間として抽象的に定義したので次のように簡単に作ることができる. $\mathbb{F}_q$ 上のベクトル空間 V と V から $\mathbb{F}_q^n$ への線形写像 $f : V \to \mathbb{F}_q^n$ があるときに $\mathrm{Im}(f)$ は符号となる. このとき f が単射ならば符号 $\mathrm{Im}(f)$ を V と同一視でき,V についてよく理解できているならそれを符号の性質として理解することもできる. 代数幾何符号とは V としてリーマン・ロッホ空間をとり f として有理点の代入写像とするものである. 代数曲線に関する基本的な定義などは紙面の都合により省略するが主な参考文献は [8] であるからそちらを参照されたい.

X を $\mathbb{F}_q$ 上の種数 g の非特異代数曲線として $P_1, \cdots, P_n$ を X の相異なる $\mathbb{F}_q$ 有理点とし, $D = P_1 + \cdots + P_n$ を因子とする. G を $\mathbb{F}_q$ 上で定義された因子として $D \cap G = \emptyset$ ($:\Leftrightarrow$ 代数閉包 $\bar{\mathbb{F}}_q$ 上で $\mathrm{Supp}\, D \cap \mathrm{Supp}\, G = \emptyset$) とする. このとき F_q 上のベクトル空間

$$L(G) := \{f \in \mathbb{F}_q(X)^\times \mid (f) + G > 0\} \cup \{0\}$$

を考える. ここで $\mathbb{F}_q(X)$ は X の $\mathbb{F}_q$ 上の有理関数体である. このとき線形写像 Φ_L を

$$\begin{array}{rccc} \Phi_L \colon & L(G) & \longrightarrow & \mathbb{F}_q^n \\ & \cup & & \cup \\ & f & \longmapsto & (f(P_1), \cdots, f(P_n)) \end{array}$$

のように定義する.$C_L = C_L(X, D, G) := \mathrm{Im}\ \Phi_L$ は符号となり**弱代数幾何符号**という. $\mathrm{Ker}\ \Phi_L = L(G - D)$ であるから, 特に $\deg G < \deg D = n$ なら Φ_L は単射となる. 代数幾何符号の性質として, 符号の次元と最小距離がある程度わかることが挙げられる.

定理 3.1. 上記の設定において $G > 0$ とする.C_L が $[n, k, d]$ 符号であるとき次が成り立つ.
(1) $\deg G < n$ ならば

$$k \geq \deg G - g + 1$$

$$n - \deg G \leq d \leq n - \deg G + g$$

となる.
(2) $2g - 2 < \deg G < n$ ならば

$$k = \deg G - g + 1$$

となる.

この定理の証明の概略は, 仮定から Φ_L が単射だから符号 C_L と $L(G)$ を同一視することができ, リーマン・ロッホの定理

$$\dim L(G) - \dim L(K_X - G) = \deg G + 1 - g$$

より $\dim L(G)$, したがって k がわかるということである (詳しい証明は [8] を参照). 定理 3.1 の (1) の仮定を満たすとき C_L を**代数幾何符号**といい,(2) の仮定を満たすとき**強代数幾何符号**という.

次に代数曲線に対して合同ゼータ関数を定義する. X を $\mathbb{F}_q$ 上で定義された代数曲線とし,N_ν を X の $\mathbb{F}_{q^\nu}$ 有理点の個数とする ($\nu = 1, 2, \cdots$). このとき

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{\nu=1}^{\infty} \frac{N_\nu}{\nu} T^\nu\right)$$

を X の**合同ゼータ関数**という. 合同ゼータ関数は様々な性質が知られており, 関数等式やリーマン予想の類似を満たすことも証明されている (ヴェイユ予想という). 以下では特別な場合のみの主張を述べる.

定理 3.2. X を $\mathbb{F}_q$ 上の非特異完備代数曲線で種数が 1 であるとき

$$\begin{aligned} Z(X/\mathbb{F}_q, T) &= \frac{P(T)}{(1-T)(1-qT)} \\ P(T) &= (1-\alpha_1 T)(1-\alpha_2 T) = 1 + (N_1 - (1+q))T + qT^2 \\ Z(X/\mathbb{F}_q, T) &= Z(X/\mathbb{F}_q, 1/qT) \end{aligned}$$

が成り立つ. さらに $P(T)$ の根の大きさは $1/\sqrt{q}$ である.

この定理の関数等式から $P(T) = qT^2 P(1/qT)$ を得るがこれは符号のゼータ多項式の関数等式と類似していることがわかる. これまでのことから代数幾何符号を考えると, 合同ゼータ関数と符号のゼータ関数 (多項式) の 2 つのゼータが登場する. このとき 2 つのゼータ関数に何か関係があるのかと疑問に思ったのがこの研究を始めたきっかけである. 次の節ではこの問題を考えるために具体的な計算をした結果や考察を述べる.

4 楕円曲線から得られる代数幾何符号のゼータ関数

ここでは楕円曲線とその $\mathbb{F}_q$ 有理点を用いて代数幾何符号をつくる. このときにできる符号のゼータ関数 (多項式) は様々な性質をもつことがわかった. $\mathrm{char}(\mathbb{F}_q) \neq 2, 3$ とするとき $\mathbb{F}_q$ 上の楕円曲線は

$$E_{a,b} : y^2 = x^3 + ax + b \ (a, b \in \mathbb{F}_q, 4a^3 + 27b^2 \neq 0)$$

の形となる. 今回の実験では, 楕円曲線の有理点が $\{P_1, \cdots, P_n, P_\infty\}$ (P_∞は無限遠点) のとき代数幾何符号の定義で現れた D と G はそれぞれ

$$\begin{aligned} D &= P_1 + \cdots + P_n \\ G &= 2P_\infty \end{aligned}$$

とする. このときにできる $[n, k, d]$ 代数幾何符号のパラメータは定理 3.1 から

$$n > 2 \text{ ならば } k = 2, n-2 \leq d \leq n-1$$

となる. よって**代数幾何符号を作る際は無限遠点も含めて 4 つ以上の有理点が必要となる**. また D, G をこのようにしたのは $L(G)$ の基底が $\{1, x\}$(x は x 座標を返す関数) のように単純なものがとれるからである. G の係数を大きくしたり D, G を全く別のものにすると他の例も考えることができる.

まずは $E_{a,b}$ の有理点の個数, さらには群構造を決定しておく. 具体的には計算機を用いて有理点を全て求め, 各有理点の位数を調べることで群の構造を決定する. $\mathbb{Z}/d\mathbb{Z}$ や $\mathbb{Z}/d_1\mathbb{Z}\times\mathbb{Z}/d_2\mathbb{Z}$ をそれぞれ $[d]$ や $[d_1,d_2]$ と表すことにすると $q=5,7$ のときそれぞれ表 1, 表 2 のようになる.

a \ b	0	1	2	3	4
0		[6]	[6]	[6]	[6]
1	[2,2]	[9]	[4]	[4]	[9]
2	[2]	[7]			[7]
3	[10]		[5]	[5]	
4	[2,4]	[8]	[3]	[3]	[8]

表 1　$E_{a,b}(\mathbb{F}_5)$ の群構造

a \ b	0	1	2	3	4	5	6
0		[2,6]	[3,3]	[13]	[3]	[7]	[2,2]
1	[8]	[5]		[6]	[10]		[11]
2	[8]	[5]		[6]	[10]		[11]
3	[2,4]	[12]	[9]	[6]	[10]	[7]	[4]
4	[8]	[5]		[6]	[10]		[11]
5	[2,4]	[12]	[9]	[6]	[10]	[7]	[4]
6	[2,4]	[12]	[9]	[6]	[10]	[7]	[4]

表 2　$E_{a,b}(\mathbb{F}_7)$ の群構造

各楕円曲線に対して重さ多項式 $A(x,y)$, ゼータ多項式 $P(T)$, リーマン予想の可否, 合同ゼータ多項式 (合同ゼータ関数の分子のこと) を求めるプログラムを作成したところ結果は $q=5,7$ のときそれぞれ表 3, 表 4 のようになった. 実は, 群構造が同じ楕円曲線からは同値な符号が得られる. ここで符号 C と C' が同値であるとは C の成分を入れ替えたり, スカラー倍することで C' にできることをいう. 符号が同値なとき, 符号の性質 (最小距離や重さ多項式, ゼータ多項式など) は同じになる.

これらの結果から次のようなことに気がつく.

- ($P(T)=1$ を除き) ゼータ多項式の係数に規則性がみられ (定数項):(T^2 の係数)$=1:q$ となっている. これは合同ゼータ多項式と同じ性質である.
- 同じ楕円曲線から作られるゼータ多項式と合同ゼータ多項式は一致してしない. しかし, ある楕円曲線のゼータ多項式を定数倍すると, 他の楕円曲線の合同ゼータ多項式になっているものがある.
- [4] と [5], [6] と [7] のようにゼータ多項式が一致するペアがある.
- ほとんどのゼータ多項式がリーマン予想を満たしている. 楕円曲線 $[2,4]$ から符号を作ったと

楕円曲線	$A(x,y)$	$P(T)$	RH の可否	合同ゼータ多項式
[2,2]	$x^3+12xy^2+12y^3$	1	○	$1-2T+5T^2$
[4]	$x^3+4x^2y+4xy^2+16y^3$	$\frac{1}{3}(1-3T+5T^2)$	○	$1-2T+5T^2$
[5]	$x^4+8x^2y^2+16y^4$	$\frac{1}{3}(1-3T+5T^2)$	○	$1-T+5T^2$
[6]	$x^5+8x^2y^3+4xy^4+12y^5$	$\frac{1}{5}(1-T+5T^2)$	○	$1+5T^2$
[7]	$x^6+12x^2y^4+12y^6$	$\frac{1}{5}(1-T+5T^2)$	○	$1+T+5T^2$
[2,4]	$x^7+8x^2y^5+12xy^6+4y^7$	$\frac{2}{21}(1+\frac{9}{2}T+5T^2)$	×	$1+2T+5T^2$
[8]	$x^7+12x^2y^5+4xy^6+8y^7$	$\frac{1}{7}(1+T+5T^2)$	○	$1+2T+5T^2$
[9]	$x^8+16x^2y^6+8y^8$	$\frac{1}{7}(1+T+5T^2)$	○	$1+3T+5T^2$
[10]	$x^9+16x^2y^7+4xy^8+4y^9$	$\frac{1}{9}(1+3T+5T^2)$	○	$1+4T+5T^2$

表 3

楕円曲線	$A(x,y)$	$P(T)$	RH の可否	合同ゼータ多項式
[2,2]	$x^3+18xy^2+30y^3$	1	○	$1-4T+7T^2$
[4]	$x^3+6x^2y+6xy^2+36y^3$	$\frac{1}{3}(1-5T+7T^2)$	○	$1-4T+7T^2$
[5]	$x^4+12x^2y^2+36y^4$	$\frac{1}{3}(1-5T+7T^2)$	○	$1-3T+7T^2$
[6]	$x^5+12x^2y^3+6xy^4+30y^5$	$\frac{1}{5}(1-3T+7T^2)$	○	$1-2T+7T^2$
[7]	$x^6+18x^2y^4+30y^6$	$\frac{1}{5}(1-3T+7T^2)$	○	$1-T+7T^2$
[2,4]	$x^7+12x^2y^5+18xy^6+18y^7$	$\frac{2}{21}(1+\frac{5}{2}T+7T^2)$	○	$1+7T^2$
[8]	$x^7+18x^2y^5+6xy^6+24y^7$	$\frac{1}{7}(1-T+7T^2)$	○	$1+7T^2$
[3,3]	$x^8+24x^2y^6+24y^8$	$\frac{1}{7}(1-T+7T^2)$	○	$1+T+7T^2$
[9]	$x^8+24x^2y^6+24y^8$	$\frac{1}{7}(1-T+7T^2)$	○	$1+T+7T^2$
[10]	$x^9+24x^2y^7+6xy^8+18y^9$	$\frac{1}{9}(1+T+7T^2)$	○	$1+2T+7T^2$
[11]	$x^{10}+30x^2y^8+18y^{10}$	$\frac{1}{9}(1+T+7T^2)$	○	$1+3T+7T^2$
[2,6]	$x^{11}+24x^2y^9+18xy^{10}+6y^{11}$	$\frac{4}{55}(1+\frac{23}{4}T+7T^2)$	×	$1+4T+7T^2$
[12]	$x^{11}+30x^2y^9+6xy^{10}+12y^{11}$	$\frac{1}{11}(1+3T+7T^2)$	○	$1+4T+7T^2$
[13]	$x^{12}+36x^2y^{10}+12y^{12}$	$\frac{1}{11}(1+3T+7T^2)$	○	$1+5T+7T^2$

表 4

きのゼータ多項式が $q=5$ のときはリーマン予想を満たしていないが $q=7$ のときには満たしている.

今は具体的な q で計算をしたが q が一般の場合を考えることで上記の観察結果にいくつか説明をつけることができた. ポイントは #Ker[2] で生成行列の分類ができることである. ここで [2] は楕円曲線の群構造ではなく, 楕円曲線の 2 倍写像のことである. 先に結論を述べると次のようになる.

定理 4.1. 上記の設定においてできる $[n,2,d]$ 符号のゼータ多項式は

$$P(T)=\begin{cases}\frac{1}{n-1}(1+(n-q-2)T+qT^2) & (\#\mathrm{Ker}[2]=1)\\ \frac{1}{n}(1+(n-q-1)T+qT^2) & (\#\mathrm{Ker}[2]=2)\\ \frac{n-3}{n(n-1)}\left(1+(n-q+\frac{n-1}{n-3})T+qT^2\right) & (\#\mathrm{Ker}[2]=4, \text{楕円曲線が } [2,2] \text{ でない})\\ 1 & (\text{楕円曲線が } [2,2])\end{cases}$$

となる.

証明のポイントは $L(G)$ の基底が単純なことから生成行列に規則性がみられることである. それによって重さを数えあげることができ, ゼータ多項式を計算できる. より詳しく述べると $L(G)$ の基底は $\{1,x\}$ であるから符号 C_L は $\Phi_L(1)$ と $\Phi_L(x)$ で生成され,C_L の生成行列は

$$\begin{pmatrix}1 & 1 & \cdots & 1\\ x(P_1) & x(P_2) & \cdots & x(P_n)\end{pmatrix}$$

となる. ここで楕円曲線の有理点の x 座標について考察する. $E(\mathbb{F}_q)$ を楕円曲線の $\mathbb{F}_q$ 有理点全体のなす集合とすると楕円曲線の定義方程式より明らかに $(x_0,y_0)\in E(\mathbb{F}_q)$ ならば $(x_0,-y_0)\in E(\mathbb{F}_q)$ である. つまり $y_0\neq 0$ ならば x 座標が等しい異なる有理点が存在する. y 座標が 0 となる有理点が 2 等分点であるが, 楕円曲線の 2 等分点の個数は 0,1,3 のいずれかとなる. $\#\mathrm{Ker}[2]=1$, つまり 2 等分点をもたないとき, 無限遠点を除いた有理点の集合 $\{P_1,\cdots,P_n\}$ は適切に添字を付け替えることによって $\{P_1,P_1',P_2,P_2',\cdots,P_m,P_m'\}$ で P_i と P_i' の x 座標が等しくなるようにできる (もちろん $n=2m$ である). 有理点の添字を入れ替えて符号を作ると集合としては異なるが, 符号の性質は変わらないから, この操作をしてもよいことに注意する. 生成行列は

$$\begin{pmatrix}1 & 1 & 1 & 1 & \cdots & 1 & 1\\ a_1 & a_1 & a_2 & a_2 & \cdots & a_m & a_m\end{pmatrix}\quad (2\leq m\leq q)$$

となる. ここで $a_1,\cdots,a_n\in\mathbb{F}_q$ はどの 2 つも相異なる. よって符号語 x は $\alpha,\beta\in\mathbb{F}_q$ によって

$$x=(\alpha+\beta a_1,\alpha+\beta a_1,\alpha+\beta a_2,\alpha+\beta a_2,\cdots,\alpha+\beta a_m,\alpha+\beta a_m)$$

の形となる. 次に x の重さ $\mathrm{wt}(x)$ を考える. まず $\mathrm{wt}(x)=0$ となるのは $\alpha=\beta=0$ のときのみである. C_L の最小距離 (=最小重み) は $n-2$ だから $\mathrm{wt}(x)=n-2$ となるものを考える. つまり x の成分の中でちょうど 2 つだけ 0 になるものである. i を固定して

$$\alpha+\beta a_i=0$$

となるのは β を固定するごとに α が一意的に定まるから q 通りある. しかし $\beta=0$ とすると $\alpha=0$ となり, 先ほど数えたものになってしまうからこれは除外する必要がある. $a_1,\cdots,a_n$ はどの 2 つも相異なっていたから $j\neq i$ に対して

$$\alpha+\beta a_j\neq 0$$

である. i は 1 から m までの m 通りあるから $\mathrm{wt}(x)=n-2$ となる x は $m(q-1)$ 通りである. 次に $\mathrm{wt}(x)=n-1$ となる w は存在しないから, 残りはすべて重さ n である. よって重さ多項式は

$$A(x,y)=x^n+m(q-1)x^2y^{n-2}+(q^2-m(q-1)-1)y^n$$

となる. 重さ多項式がわかったからゼータ多項式が計算できる. その結果は

$$\begin{aligned} P(T) &= \frac{1}{2m-1}(1+(2m-2-q)T+qT^2) \\ &= \frac{1}{n-1}(1+(n-q-2)T+qT^2) \end{aligned}$$

となる. 2 等分点が 1,3 個のときも同様の考察で $P(T)$ を得られる.

この定理から計算結果の観察で気づいたことに対して説明ができる. まず, ゼータ多項式の係数の規則性で,(定数項):(T^2 の係数)$= 1 : q$ となっていることについてだが, これは定理 4.1 の $P(T)$ の形から明らかである. 次にゼータ多項式と合同ゼータ多項式が一致しないことについてだが, 定理 4.1 の設定だと合同ゼータ多項式が

$$1+(N_1-(q+1))T+qT^2 = 1+(n-q)T+qT^2$$

となるので $P(T)$ を定数倍して定数項が 1 になるようにしても T の係数が少しだけずれているから一致しないことがわかる. また, このズレがゼータ多項式と別の楕円曲線の合同ゼータ多項式が一致していることの原因であることもわかる. 次に楕円曲線が [4] と [5],[6] と [7] のようにゼータ多項式が一致するペアが存在したが, これについても定理 4.1 の $\#\mathrm{Ker}[2] = 1, \#\mathrm{Ker}[2] = 2$ のときの $P(T)$ の形をみれば等しくなっていることを確認できる. また $P(T)$ を明示的に求めることができたため, リーマン予想について考察することができる. 例えば $\#\mathrm{Ker}[2] = 1$ のとき $\mathbb{F}_q$ 有理点の個数 N_1 は $n+1$ 個だから

$$P(T) = \frac{1}{n-1}(1+(n-q-2)T+qT^2) = \frac{1}{n-1}(1+(N_1-q-3)T+qT^2)$$

であり,$P(T)$ の判別式が負であることがリーマン予想が成り立つための必要十分条件である. つまり

$$(N_1-q-3)^2 < 4q$$

であるが, これは Hasse-Weil の不等式

$$(N_1-q-1)^2 \leq 4q$$

と少しずれていることがわかる. つまり $\#\mathrm{Ker}[2] = 1$ のときにリーマン予想を満たさない例が存在する余地があるということである. 実際に $p = 23$ で $N_1 = 15$ となる楕円曲線 $y^2 = x^3 + x + 12$ を選ぶと不等式を満たさないことがわかる. 以上からリーマン予想は満たしたり満たさなかったり状況によってまちまちであることがわかった. また, 副産物として自己双対でない符号で $P(T)$ が関数等式を満たす例が作れた. 定理の $P(T)$ は

$$P(T) = qT^2P(1/qT)$$

を満たしていることが計算からわかる. 自己双対符号は n が偶数であることが必要条件であるから表 3,4 において自己双対でない符号はたくさんある.

最後に, 今回行った計算は代数幾何符号のほんの一例に過ぎず, 状況設定を変えることで他にも様々な計算ができる. もしかしたら今回の計算では見つからなかった面白い結果がまだまだ眠っているかもしれない.

参考文献

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

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

[3] Duursma, I. From weight enumerators to zeta functions, Discrete Appl. Math. **111** (2001), 55-73.

[4] 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), 数理解析研究所講究録, 1361 巻, 2004 年, 91-101.

[5] Chinen, Koji. Zeta functions for formal weight enumerators and the extremal property. Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 10, 168–173.

[6] 内田興二. 有限体と符号理論, サイエンス社, 2000.

[7] F.J. Macwilliams; N.J.A. Sloane. The Theory of Error-Correcting Codes. North-Holland Publishing Co, 1977.

[8] 桂利行. 代数幾何入門, 共立出版, 1998.