

代数曲線上の 2 点についての gap 集合と それらの点を支持台に持つ代数曲線符号

本間 正明*

神奈川大学工学部

homma@cc.kanagawa-u.ac.jp

1 代数曲線符号

有限体 \mathbb{F}_q の上で定義された代数曲線 X 上の Goppa 符号は、その曲線上の相異なる \mathbb{F}_q -有理点 P_1, \dots, P_n からなる正因子 $D = \sum_{i=1}^n P_i$ とこれらの点をその support には含まない \mathbb{F}_q -有理な因子 F とから構成される。さらに、理論的には必要はないが、煩雑さを避けるために、 F は正因子であると仮定する。

この D と F から線形符号をつくる標準的方法として X の関数加群を用いる方法と、微分加群を用いる方法とがある。前者は L -構成法、後者は Ω -構成法とよばれる。

ここで、この小論を通して用いるいくつかの記号を用意するが、概ね Stichtenoth [9] に従う。 \mathbb{F} を完全体とし¹、 X を \mathbb{F} 上定義された絶対既約な完備非特異代数曲線²とし、 X の \mathbb{F} -有理関数全体を $\mathbb{F}(X)$ で表す。また \mathbb{F} -有理微分全体のなす $\mathbb{F}(X)$ ベクトル空間を $\Omega_{\mathbb{F}(X)}$ で表す。またこの曲線 X の \mathbb{F} -有理点全体を $X(\mathbb{F})$ で表す。この曲線の種数を g で表す。

*ここで述べる事柄は、Seon Jeong Kim (Gyeongsang National University) との共同研究の一部である。証明を含めた完全版は、遠くない将来、どこかに発表する予定である。

¹符号について考えるときは、当然 \mathbb{F} は有限体 \mathbb{F}_q とする。

²以下、これを単に \mathbb{F} 上の代数曲線 (あるいは、単に、曲線) とよぶことにする。

$f \in \mathbb{F}$ について, $(f)_0$ で f の零点のなす因子を, $(f)_\infty$ で f の極のなす因子を表し, さらに, $(f) := (f)_0 - (f)_\infty$ と記す. $\Omega_{\mathbb{F}(X)}$ の元についても同様な記法を用いる. $(f)_0, (f)_\infty, (f)$ 等は \mathbb{F} 上定義された因子である³. \mathbb{F} 上定義された因子のことを \mathbb{F} -有理因子とよぶことにする.

\mathbb{F} -有理因子 E について,

$$\mathcal{L}(E) := \{f \in \mathbb{F}(X) \setminus \{0\} \mid (f) + E \succ 0\} \cup \{0\},$$

$$\Omega(E) := \{\omega \in \Omega_{\mathbb{F}(X)} \setminus \{0\} \mid (\omega) \succ E\} \cup \{0\},$$

として, これらの \mathbb{F} ベクトル空間としての次元を $\ell(E) := \dim_{\mathbb{F}} \mathcal{L}(E)$, $i(E) := \dim_{\mathbb{F}} \Omega(E)$ で表す.

さて, 冒頭のパラグラフの状況に戻ろう.

L -構成法 \mathbb{F}_q -線形写像

$$\mathcal{L}(F) \ni f \longmapsto (f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n$$

を考え, この像である符号を $C_L(D, F)$ で表す. 明らかに $\dim C_L(D, F) = \ell(F) - \ell(F - D)$ である.

Ω -構成法 \mathbb{F}_q -線形写像

$$\Omega(F - D) \ni \eta \longmapsto (\text{res}_{P_1} \eta, \dots, \text{res}_{P_n} \eta) \in \mathbb{F}_q^n,$$

を考え, この像である符号を $C_\Omega(D, F)$ で表す. 明らかに, $\dim C_\Omega(D, F) = i(F - D) - i(F)$ である.

Riemann-Roch の定理と留数定理より, 容易にわかるように, $C_L(D, F)$ と $C_\Omega(D, F)$ は互いに双対符号の関係にある.

また, Pellikaan - Shen - van Wee [8] によって, 全ての線形符号は適当な曲線 X とその上の因子の組 (D, F) から L -構成法によって得られることが証明されている. 従って, 全ての線形符号は Ω -構成法によって得られると言っても良い.

以下, 小論では Ω -構成法で得られた符号について考察する. 符号 $C_\Omega(D, F)$ の設計距離は F, D に何の制限も設けなければ Riemann - Roch の定理により,

$$(1) \quad \deg F - (2g - 2)$$

³これは, その因子にあらわれる点自身が $X(\mathbb{F})$ の点であることを意味しない.

で与えられる.

われわれは, $C_\Omega(D, F)$ の最小距離について議論したいので, それを $d_\Omega(D, F)$ なる記号で表す.

2 Garcia - Lax および Garcia - Kim - Lax による評価

Garcia と Lax は 1991 年に, F が \mathbb{F}_q -有理点 Q の何倍かになっている状況では, ある場合に (1) より良い評価が得られることを示した. すなわち, α, β が Q での空隙⁴であるとき, $F = (\alpha + \beta - 1)Q$ とすれば,

$$(2) \quad d_\Omega(D, F) \geq \deg F - (2g - 2) + 1;$$

である.

翌年, Garcia - Kim - Lax の 3 人によって, 以下のような場合には評価 (2) が改良されることが示された. この状況はエルミート曲線⁵の場合に良く適合する⁶.

t を自然数として, $\alpha + t \leq \beta$ とする. さらに, $\alpha, \alpha + 1, \dots, \alpha + t$ をひき続く $t + 1$ 個の Q での空隙の列, $\beta - (t - 1), \dots, \beta - 1, \beta$ をひき続く t 個の Q での空隙の列とすると, $F = (\alpha + \beta - 1)Q$ とすれば,

$$(3) \quad d_\Omega(D, F) \geq \deg F - (2g - 2) + t + 1.$$

なる評価を得る.

上に述べたような, 代数曲線符号の支持因子 F の台が 1 点からなる, いわゆる 1 点符号は比較的取り扱い易いため, 好まれているが, 理論上は支持因子の台⁷が例えば, 2 点であるような符号も興味があると思われる.

⁴関数 $f \in \mathbb{F}_q(X)$ で f の極因子 $(f)_\infty$ がちょうど αQ となるものが存在するとき, α を Q での非空隙 (nongap) といい, そうでないとき, 空隙 (gap) という. 与えられた点での空隙の個数は曲線の種数 g に一致する.

⁵平面非特異曲線 $y^q + y = x^{q+1}$ を \mathbb{F}_{q^2} 上で考えた曲線.

⁶エルミート曲線上で \mathbb{F}_{q^2} -有理点 Q について $F = mQ$ とし, D として残余の有理点すべてとした符号 $C_L(D, F)$, $C_\Omega(D, F)$ の真の最小距離は Yang-Kumar [11] によって知られている.

⁷この言葉を省略して, 支持台と呼ぶことにする.

実際, G. L. Matthews [7] は, 特にエルミート曲線上の, 2点を支持台とする曲線を調べ, パラメータの意味で1点を支持台とするものより良い符号が存在することを具体的構成によって明らかにした.

われわれは, 2点を支持台とする代数曲線符号を, 彼女の取り扱いよりは少しばかり理論的に, 扱う.

3 曲線上の2点についての空隙集合

前節の Garcia-Lax および Garcia-Kim-Lax のような定理を2点を支持台に持つような符号について定式化しようとすれば, 1点の場合の空隙列に相当する事柄について調べる必要がある.

これについては Kim [6] および著者 [5] によって基本的事柄が調べられている. ここでは, それらの中から必要となる部分を復習し, さらに, われわれの定理を定式化するために必要な概念について述べる. この節では基礎体 \mathbb{F} は, 単に完全体であるとする. さらに曲線 X の種数 g は2以上とする.

Q_1, Q_2 を相異なる X の \mathbb{F} -有理点とする. 点の組 (Q_1, Q_2) についてのワイエルシュトラス (Weierstrass) 半群 $H(Q_1, Q_2)$ とは

$$\{(\nu_1, \nu_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid \text{there exists } f \in \mathbb{F}(X) \text{ with } (f)_\infty = \nu_1 Q_1 + \nu_2 Q_2\},$$

によって定義される半群を意味する. ただし \mathbb{N}_0 は非負整数全体のなす半群である. さらに, この補集合

$$G(Q_1, Q_2) := \mathbb{N}_0 \times \mathbb{N}_0 \setminus H(Q_1, Q_2)$$

を, この2点組についての空隙集合とよぶ.

1点の場合の空隙列との大きな相違点は空隙集合は種数 g を固定してもこの位数は一定ではないことである. 空隙集合を調べるために, 以下の観察は重要である.

$m_1 < m_2 < \cdots < m_g$ と $n_1 < n_2 < \cdots < n_g$ とを, それぞれ Q_1, Q_2 での空隙列とする. Q_1 の各空隙 m_i に対し,

$$\min\{\beta \mid (m_i, \beta) \in H(Q_1, Q_2)\}$$

は Q_2 での空隙の1つとなる. これを $n_{\sigma(i)}$ と表すことにしよう. このとき, 対応 $m_i \mapsto n_{\sigma(i)}$ は Q_1 での空隙列 $G(Q_1)$ と Q_2 での空隙列 $G(Q_2)$

の間の1対1対応を与える。従って σ は

$$\mathbb{N}_{\leq g} := \{1, 2, \dots, g\}.$$

の上の置換となる。

さらに、この置換によって大小の順が反転されるような組の全体、すなわち

$$R(\sigma) := \{(i, j) \in \mathbb{N}_{\leq g} \times \mathbb{N}_{\leq g} \mid i < j \text{ and } \sigma(i) > \sigma(j)\}$$

を考え、 $r(\sigma) := \#R(\sigma)$ とする⁸。以上の記法の下で、空隙集合の個数は

$$\#G(Q_1, Q_2) = \sum_{i=1}^g m_i + \sum_{i=1}^g n_i - r(\sigma).$$

で与えられる。

さて、われわれの定理を定式化するため、2点組に対する「純な空隙」という概念を定義する。

定義 非負整数 (α_1, α_2) と $(Q_1, Q_2) \in X \times X$ について

$$\begin{aligned} \ell(\alpha_1 Q_1 + \alpha_2 Q_2) &= \ell((\alpha_1 - 1)Q_1 + \alpha_2 Q_2) \\ &= \ell(\alpha_1 Q_1 + (\alpha_2 - 1)Q_2). \end{aligned}$$

が成立するとき、 (α_1, α_2) は (Q_1, Q_2) における純な空隙であるという。

2点組 (Q_1, Q_2) における純な空隙全体を $G_0(Q_1, Q_2)$ で表す。明らかに、 $G_0(Q_1, Q_2)$ は $G(Q_1, Q_2)$ の部分集合である。

定理 3.1 上で説明した記法の下で、

$$G_0(Q_1, Q_2) = \{(m_i, n_j) \mid (i, \sigma^{-1}(j)) \in R(\sigma)\}.$$

である。特に、 $\#G_0(Q_1, Q_2) = r(\sigma)$ である。

この定理の系として、

系 3.2 純な空隙の個数は

$$\#G_0(Q_1, Q_2) \leq \frac{1}{2}g(g-1),$$

で与えられる。従って $G_0(Q_1, Q_2) = \emptyset$ である為の必要十分条件は曲線 X から射影直線 \mathbb{P}^1 への2次の被覆があつて、因子 $Q_1 + Q_2$ がその1点の逆像となることである。

⁸浅野啓三、永尾汎著「群論」岩波書店(1965)ではこの数を転位の数とよんでいる。

証明. 最初の主張は定理と $0 \leq r(\sigma) \leq \frac{1}{2}g(g-1)$. から明らか. 後半の主張は [5, Proposition 4] による $r(\sigma) = 0$ の場合の 2 点組の特徴づけより明らか. \square

4 2 点を支持台に持つ符号の最小距離の評価

以下, 再び基礎体 \mathbb{F} は有限体 \mathbb{F}_q であるとし, X の種数は $g \geq 2$ とする.

状況設定を確認しておく. 相異なる X の \mathbb{F}_q -有理点 Q_1, Q_2 を固定する. さらに, $X(\mathbb{F}_q) \setminus \{Q_1, Q_2\}$ から n 個の点 P_1, \dots, P_n を選び, $D = P_1 + \dots + P_n$ とする.

F を Q_1, Q_2 を台に持つ正因子, 符号 $C_\Omega(D, F)$ の最小距離を $d_\Omega(D, F)$ で表す.

最初の主要な結果は次のとおり.

定理 4.1 自然数の組 $(\alpha_1, \alpha_2), (\beta_1, \beta_2) \in \mathbb{N} \times \mathbb{N}$, について, $t_i := \beta_i - \alpha_i$ ($i = 1, 2$) とおき, $t_i \geq 0$ ($i = 1, 2$) であると仮定する. さらに,

$$(4) \quad \{(k_1, k_2) \mid \alpha_1 \leq k_1 \leq \beta_1, \alpha_2 \leq k_2 \leq \beta_2\} \subseteq G_0(Q_1, Q_2)$$

であれば,

$$F = (\alpha_1 + \beta_1 - 1)Q_1 + (\alpha_2 + \beta_2 - 1)Q_2$$

なる F について,

$$d_\Omega(D, F) \geq \deg F - (2g - 2) + t_1 + t_2 + 2.$$

が成り立つ.

定理 4.1 で “ $t_1 = t_2 = 0$ ” の場合は, 以下の方向へ一般化できる. これは Garcia-Lax の評価式 (2) の支持台が 2 点の場合での類似である.

定理 4.2 (α_1, α_2) と (β_1, β_2) とを (Q_1, Q_2) における純な空隙とする.

$$F = (\alpha_1 + \beta_1 - 1)Q_1 + (\alpha_2 + \beta_2 - 1)Q_2,$$

とすれば,

$$d_\Omega(D, F) \geq \deg F - (2g - 2) + 2$$

である.

参考文献

- [1] A. Garcia and R. F. Lax, Goppa codes and Weierstrass gaps. in: Coding Theory and Algebraic Geometry, Lecture Note in Mathematics **1518**, 33–42, Springer, Berlin - Heidelberg 1992
- [2] A. Garcia, S. J. Kim and R. F. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes. J. Pure Appl. Algebra **84**, 199–207 (1993)
- [3] A. Garcia and P. Viana, Weierstrass points on certain non-classical curves. Arch. Math. **46**, 315–322 (1986)
- [4] V. D. Goppa, Codes on algebraic curve. Soviet Math. Dokl. **24**, 170–172 (1981)
- [5] M. Homma, The Weierstrass semigroup of a pair of points on a curve. Arch. Math. **67**, 337–348 (1996)
- [6] S. J. Kim, On the index of the Weierstrass semigroup of a pair of points on a curve. Arch. Math. **62**, 73–82 (1994)
- [7] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes. Preprint, Louisiana State University 1999
- [8] R. Pellikaan, B. Z. Shen and G. J. M. van Wee, Which linear codes are algebraic-geometric ? IEEE Trans. Inform. Theory **37**, 583–602 (1991)
- [9] H. Stichtenoth, Algebraic Function Fields and Codes. Springer, Berlin - Heidelberg 1992
- [10] M. A. Tsfasman and S. G. Vlăduț, Algebraic-Geometric Codes. Kluwer Academic Publishers, Dordrecht, 1991
- [11] K. Yang and P. V. Kumar, On the true minimum distance of Hermitian curves. Lecture Note in Mathematics **1518**, 99–107, Springer, Berlin - Heidelberg 1992