Conics with a Hermitian curve

神奈川大学工学部 本間正明 (Masaaki HOMMA) *

A Hermitian curve X is a plane curve of degree $q+1$ which is projectively equivalent to the plane curve with the inhomogeneous equation $y^q+y=x^{q+1}$ over the finite field $\mathbb{F}_{q^2}$ of q^2 elements, which has q^3+1 $\mathbb{F}_{q^2}$-rational points. The geometry of lines over $\mathbb{F}_{q^2}$ harmonizes with those points, that is to say, a line over $\mathbb{F}_{q^2}$ either tangents to X at an $\mathbb{F}_{q^2}$-rational point with multiplicity $q+1$ or meets X in exactly $q+1$ $\mathbb{F}_{q^2}$-rational points. For the conics over $\mathbb{F}_{q^2}$, we can not expect them to behave well with the $\mathbb{F}_{q^2}$-rational points of X, however, in the joint research with Seon Jeong Kim on the two-point codes on X, we met a certain family of conics over $\mathbb{F}_{q^2}$ whose behavior on the $\mathbb{F}_{q^2}$-rational points of X seemed interesting.

1 誤り訂正符号

有限体 $\mathbb{F}$ 上の座標空間 $\mathbb{F}^n$ の部分ベクトル空間 $C \subseteq \mathbb{F}^n$ のことを (線形) **符号**とよぶ. これはノイズがあるようなチャンネルを通して情報伝達をするとき，いかにノイズの影響を軽減するかという課題に対する「しかけ」に由来する．簡単の為，$\mathbb{F}$ を 2 元体 $\mathbb{F}_2$ とすれば，n ビットの情報は，$\mathbb{F}^n$ のある元に対応すると考えられる．チャンネルを通して伝達したい，いくつかのメッセージがあるとき，それらの情報を C の元に対応させておく．その n ビットのメッセージをチャンネルを通して伝達したとき，ノイズの影響でいわゆる「文字化け」が n ビットの列のうちのどこかで起こるかもしれない．文字化けを起してしまった n ビットの列は，多くの場合，もはや C の元ではないだろう．その，C の元ではない n ビットの列を眺めて，C の元を次のようにして回復（推測）する．$\mathbb{F}^n$ の元 $\mathbf{x}=(x_1,x_2,\ldots,x_n)$, $\mathbf{y}=(y_1,y_2,\ldots,y_n)$ に対し，

$$d(\mathbf{x},\mathbf{y}) = {}^{\#}\{\, i \,|\, x_i \neq y_i \,(1 \leq i \leq n)\,\}$$

によって（Hamming 距離とよばれる）距離を定め，(「文字化け」はそうしばしばは起こらないということで,）この距離で最も近い C の元がオリジナルメッセージに対応する元であろうと考える.

符号 C が $[n,k,d]$-符号であるとは，$C \subseteq \mathbb{F}^n$ であり，

$$\begin{aligned} k = k(C) &= \dim_{\mathbb{F}} C, \\ d = d(C) &= \min\{d(\mathbf{x},\mathbf{y}) | \mathbf{x},\mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\} \end{aligned}$$

*この研究は日本学術振興会科学研究費補助金 (基盤 C) (15500017) の援助を受けた.

となることを意味する．$d(C)$ は文字通り**最小距離**とよばれるが，C が線形空間であるので，

$$d(C) = \min\{d(\mathbf{x}, \mathbf{0}) | \mathbf{x} \in C,\ \mathbf{x} \neq \mathbf{0}\}$$

である．$d(\mathbf{x}, \mathbf{0})$ は $\mathbf{x}$ の重みとよばれ，$d(C)$ は C の**最小重み**とよばれることもある．

上に述べた「しかけ」は $d(C)$ が大きければ大きいほど，誤りを訂正する能力が向上する[1]．一方 $(^{\#}\mathbb{F})^n - (^{\#}\mathbb{F})^k$ は意味を担わないビット列の数だから，この値が小さいほど，すなわち k が大きいほど経済的な符号と考えられる．要するに d も k も大きければ大きいほど望ましい符号である．しかし n を固定したとき，d と k の望ましさはトレードオフの関係にある．実際，

$$k + d \leq n + 1 \tag{1}$$

となる[2]．したがって，この等号を到達するような符号[3]はある意味では最も望ましい符号であるが，基礎体 $\mathbb{F}$ の大きさで制限を受けてしまう[4]：

$$\begin{aligned} ^{\#}\mathbb{F} &\geq n - k + 1 \qquad \text{if } \ k \geq 2; \\ ^{\#}\mathbb{F} &\geq k + 1 \qquad \text{if } \ n - 2 \geq k. \end{aligned}$$

例 1.1 α を q 元体の乗法群 $\mathbb{F}_q^{\times}$ の生成元とする．すなわち，

$$\mathbb{F}_q = \{0, 1, \alpha, \ldots, \alpha^{q-2}\}$$

である．$k < q$ について，

$$\mathbb{F}_q{}^q \supset \mathcal{R}S_k \stackrel{\text{def}}{=} \{(f(0), f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \mid f(x) \in \mathbb{F}_q[x]_{<k}\}$$

とする．ただし，$\mathbb{F}_q[x]_{<k}$ は次数が k に満たない多項式全体である．明かに，$\dim_{\mathbb{F}_q} \mathcal{R}S_k = k$ である．また，

$$\begin{aligned} (f(0), f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \text{の重み} &= q - ^{\#}(\{f = 0 \text{ の根}\} \cap \{0, 1, \alpha, \ldots, \alpha^{q-2}\}) \\ &\geq q - \deg f \geq q - (k-1) \end{aligned}$$

であるから $d \geq q - (k-1)$ であり，(1) より $d = q - (k-1)$ となり，$\mathcal{R}S_k$ は MDS 符号である．この符号は**拡張された Reed-Solomon 符号**とよばれる．

---

[1]容易に確かめられるように，n ビット中 $[(d-1)/2]$ 個までの「文字化け」は正しく訂正される．

[2]これは Singlton 限界式とよばれる．証明は以下の通り：$\mathbb{F}^n \xrightarrow{\pi} \mathbb{F}^{n-d+1}$ を 1 番目の座標から $d-1$ 番目の座標を無視する射影 $\pi(x_1, \ldots, x_n) = (x_d, \ldots, x_n)$ とする．これを C に制限した写像 $\pi_{|C}$ は C の最小重みが d であることより，単射．よって $k \leq n - d + 1$ を得る．

[3]それらは，**MDS**(Maximum Distance Separable) **符号**とよばれる．

[4]証明は例えば [3, Ch. 11, §3, Cor. 7] 参照.

2 Goppa符号

拡張されたReed-Solomon符号（例 1.1）の構成は幾何学的に次のように解釈できる．$\mathbb{F}_q$ 上の射影直線 $\mathbb{P}^1$ 上の点 $P_\infty \stackrel{\text{def}}{=} (1:0)$, $P_\beta \stackrel{\text{def}}{=} (\beta, 1)$ $(\beta \in \mathbb{F}_q)$ を考えれば，明かに

$$\mathcal{R}S_k = \{(f(P_\beta))_{\beta\in\mathbb{F}_q} \mid f \in L((k-1)P_\infty)\}$$

となる．ここで，$L((k-1)P_\infty)$ は $\mathbb{P}^1$ の $\mathbb{F}_q$ 上定義された有理関数で P_∞ にだけ高々 $k-1$ 位の極を持つようなもののなす $\mathbb{F}_q$ ベクトル空間である．

このような見方を有限体 $\mathbb{F}$ 上定義された曲線 X に適用すれば，**Goppa符号**[5]の定義に達する．

定義 2.1 $\mathbb{F}$ 上定義された非特異曲線 X 上の $\mathbb{F}$ 有理点全体を $X(\mathbb{F})$ で表す．$P_1, \ldots, P_n \in X(\mathbb{F})$ とし，形式的に因子と見て $D = P_1 + \cdots + P_n$ とかく．さらに $\mathbb{F}$ 上定義された因子[6] G でその support に $P_1, \ldots, P_n$ を含まないようなものを考える．この状況で自然な写像

$$L(G) \ni f \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}^n \tag{2}$$

の像は線形符号であるが，これを $C_L(D, G)$ であらわす．

Goppa符号 $C_L(D, G)$ について，Singlton限界式 (1) の限界からどの程度後退するのかを見ておく．すなわち，$C_L(D, G)$ について $n + 1 - (k + d)$ を評価する．X の種数を g とする．線形写像 (2) の Kernel は $L(G - D)$ であるから，

$$k = \dim\ L(G) - \dim\ L(G - D).$$

一方

$$\begin{aligned} (f(P_1), \ldots, f(P_n)) \text{の重み} &= n - {}^{\#}\{P_i \mid f(P_i) = 0\} \\ &\geq n - \deg\ G \end{aligned}$$

であるから，

$$d \geq n - \deg\ G \tag{3}$$

である．従って n が大きいとき，すなわち $L(G - D) = (0)$ のとき，Riemann-Roch により，

$$n + 1 - (k + d) \leq \deg\ G - \dim\ L(G) + 1 = g - h^1(G)$$

なる評価式を得る．

---

[5] ここに述べるのは，L 構成法とよばれるものである．Goppa符号には Ω 構成法とよばれれる構成の仕方もあるが，ここでは省略する．

[6] この因子の support 個々の点は $\mathbb{F}$ 有理点でなくとも構わない．

定義 2.2 (3) の右辺を $C_L(D,G)$ の**設計距離**[7]とよぶ.

多くの場合 G は正因子ととることが多い．以下，われわれも $G \succ 0$ と仮定する.

注意 2.3 $C_L(D,G)$ の最小距離が設計距離に一致する必要十分条件は X 上の $\mathbb{F}$-有理関数 f であって

$$(f)_\infty = G, \quad (f)_0 \subset D$$

となるものが存在することである．ただし，$(f)_\infty$ は f の極因子を $(f)_0$ は零因子をあらわす.

定義 2.4 ある $Q \in X(\mathbb{F})$ と自然数 m について，$G = mQ$ で $D = \sum_{P \in X(\mathbb{F}) \setminus \{Q\}} P$ であるとき，$C_L(D,G)$ を**1 点符号**とよぶ．同様に， $Q_1, Q_2 \in X(\mathbb{F})$ と自然数 m_1, m_2 について

$$C_L\left(\sum_{P \in X(\mathbb{F}) \setminus \{Q_1, Q_2\}} P\,, \quad m_1 Q_1 + m_2 Q_2 \right)$$

を**2 点符号**とよぶ.

3 Hermitian 曲線

q を素数 p の正冪とする．非斉次多項式

$$y^q + y = x^{q+1} \tag{4}$$

で定義された射影平面曲線 $X \subset \mathbb{P}^2$ を $\mathbb{F}_{q^2}$ 上で考えたものを **Hermitian 曲線**とよぶ.

この曲線は非特異平面曲線であるから，種数は $g = q(q-1)/2$ である.

注意 3.1 2 次拡大 $\mathbb{F}_{q^2}/\mathbb{F}_q$ の trace Tr と norm Nm を用いると (4) は $Tr(y) = Nm(x)$ とかける.

$X(\mathbb{F}_{q^2})$ は q^3+1 個の点からなる．$q^3+1 = q^2+1+2g\sqrt{q^2}$ であるから，$X/\mathbb{F}_{q^2}$ は Weil の上限式を到達する曲線になっている.

X は無限遠直線上には唯一の点を持ち，これは $\mathbb{F}_{q^2}$-有理点である．この点を P_∞ で表す．また原点 $(0,0)$ も X の ($\mathbb{F}_{q^2}$-有理) 点であるが，この点を P_0 で表す.

この曲線の自己同型は全て$\mathbb{F}_{q^2}$ 上定義され，$X(\mathbb{F}_{q^2})$ に 2 重推移的に働く．従って，この曲線上の 1 点符号を考えるときは，定義 2.4 で $Q = P_\infty$， 2 点符号を考えるときは，$Q_1 = P_\infty$，$Q_2 = P_0$ として一般性を失わない.

[7] deg G が大きければこの値は負になりうるが，設計距離を問題にするのはこの値が正となる場合だけである.

定義 3.2 (4) で定義された Hermitian 曲線 X 上で，$D = \sum_{P \in X(\mathbb{F}_{q^2}) \setminus \{P_\infty P_0\}} P$ とかき，$m, n \in \mathbb{N}_0$ について $C_m := C_L(D + P_0, mP_\infty)$，$C(m,n) := C_L(D, mP_\infty + nP_0)$ とおく．ただし $\mathbb{N}_0$ は非負整数全体をあらわす.

C_m の次元は Stichtenoth [4] で，最小距離については, [4] を経て Yang [5], Yang - Kumar [6] で決定された.

Hermitian 曲線 X の $\mathbb{F}_{q^2}$ 有理点 $X(\mathbb{F}_{q^2})$ と，$\mathbb{F}_{q^2}$ 有理直線とは整合的に振舞う．すなわち，$\mathbb{F}_{q^2}$ 有理直線は X とは相異なる $q+1$ 個の $\mathbb{F}_{q^2}$ 有理点での交わるか，$q+1$ 重に $\mathbb{F}_{q^2}$ 有理点で接する．このことが，設計距離を到達するような C_m について，具体的に関数を構成できる根拠となっている．実際,

定理 3.3 (Stichtenoth, Yang and Kumar) $m \in \mathbb{N}_0$ とし，$m = aq + b$ $(0 \le b < q)$ とかく．C_m の最小距離 $d(C_m)$ が設計距離 $q^3 - m$ に一致する為の必要十分条件は,「$b \le a \le b + (q^2 - q - 1)$」または「$b = 0$ かつ $a \le q^2 - 1$」.

であるが，十分性を示すための注意 2.3 に述べたような関数は，次の様にして得られる.

$U \stackrel{\text{def}}{=} \{\xi \in \mathbb{F}_{q^2} \,|\, \xi^{q+1} = 1\}$，$H \stackrel{\text{def}}{=} \{h \in \mathbb{F}_{q^2} \,|\, h + h^q = 0\}$ とする．$U \times H$ は各 $(\xi, h) \in U \times H$ について $\sigma_{(\xi,h)}(\alpha, \beta) \stackrel{\text{def}}{=} (\xi\alpha, \beta + h)$ とすることにより $X(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ に作用する．この作用による軌道分解を

$$X(\mathbb{F}_{q^2}) \setminus \{P_\infty\} = \square_0 + \square_1 + \cdots + \square_{q-1}$$

と表す．ただし，$\square_0 = \{(0,h) | h \in H\}$ とする．これ以外の $\square_i$ $(1 \le i \le q-1)$ は $q(q+1)$ 個の点からなり $(\alpha, \beta) \in \square_i$ とすると

$$\square_i = \coprod_{\xi \in U} \{x - \xi\alpha = 0\} \cap X = \coprod_{h \in H} \{y - (\beta + h) = 0\} \cap X$$

である．さらに,

(a) $i \ne j$ ならば $x(\square_i) \cap x(\square_j) = \emptyset$; $y(\square_i) \cap y(\square_j) = \emptyset$

(b) $\bigcup_{i=1}^{q-1} x(\square_i) = \mathbb{F}_{q^2} \setminus \{0\}$; $\bigcup_{i=1}^{q-1} y(\square_i) = \mathbb{F}_{q^2} \setminus H$

(c) $\alpha \in \mathbb{F}_{q^2}$ ならば $\operatorname{div}(x - \alpha) = \sum_{h \in H} (\alpha, \beta + h) - qP_\infty$

(d) $\beta \in \mathbb{F}_{q^2} \setminus H$ ならば $\operatorname{div}(y - \beta) = \sum_{\xi \in U} (\xi\alpha, \beta) - (q+1)P_\infty$

という性質がある．したがって，$m = aq + b$ が「$b = 0$ かつ $a \le q^2 - 1$」を満たすときは，$\mathbb{F}_{q^2} \setminus \{0\}$ から a 個の元 $\alpha_1, \ldots, \alpha_a$ をとり，関数 $\prod_{i=1}^{a} (x - \alpha_i)$ を考えればよい．ま

た,「$b \le a \le b + (q^2 - q - 1)$」のときは $0 \le a - b \le q^2 - q - 1 = 1 + (q-2)(q+1)$ であるから，$\{0\} \cup x(\square_1) \cup \cdots \cup x(\square_{q-2})$ から $a-b$ 個の元 $\alpha_1, \ldots, \alpha_{a-b}$ をとり，残ったひとつのブロック $\square_{q-1}$ の y 座標 $y(\square_{q-1})$ から b 個の元 $\beta_1, \ldots, \beta_b$ をとって，関数 $\prod_{i=1}^{a-b}(x - \alpha_i)\prod_{j=1}^{b}(y - \beta_j)$ を考えればよい.

4 Hermitian 曲線と Conics の族

X 上の 2 点符号 $C(m,n)$ についての定理 3.3 に相当する事実は記述が煩雑になるので，ここでは省略する[8]．$d(C(m,n))$ が設計距離 $q^3 - 1 - (m+n)$ に一致するような場合に重みが $q^3 - 1 - (m+n)$ になる関数を構成するには直線から得られるものだけでは不充分である (ように思える)．そこで，2 次以上の曲線をも考慮に入れるのであるが，2 次曲線になると X との交わりが一般には直線のようにはうまく振舞わない．しかし幸いにしてある種の 2 次曲線の族と関数 $(\prod_{\alpha \in \mathbb{F}_{q^2}}(x - \alpha))/y$ を用いることによって，設計距離を到達するような $C(m,n)$ が決定できた．ここでは，その 2 次曲線の族について説明する.

各 $a \in \mathbb{F}_{q^2} \setminus \{0\}$ について，2 次曲線 $C_a : y = ax^2$ を考える．この 2 次曲線族 $\{C_a \,|\, a \in \mathbb{F}_{q^2} \setminus \{0\}\}$ は，$\mathbb{F}_{q^2}$ 上定義された既約な 2 次曲線 C で局所交点数 $i(C.X; P_0) = i(C.X; P_\infty) = 2$ となるもの全体と特徴付けができる．以下，この曲線族の，(4) で定義された Hermitian 曲線 X の $\mathbb{F}_{q^2}$ 有理点 $X(\mathbb{F}_{q^2})$ との関わりで興味深い性質について述べる.

乗法群 $\mathbb{F}_q \setminus \{0\}$ の $\mathbb{P}^2$ への作用を $c \in \mathbb{F}_q \setminus \{0\}$ に対し

$$(x, y, z) \mapsto (cx, c^2 y, z)$$

によって定める．P_0 と P_∞ はこの作用による固定点であり，$X \setminus \{P_0, P_\infty\}$ と $C_a \setminus \{P_0, P_\infty\}$ とは，この作用によって不変である．また，$\mathbb{P}^2 \setminus \{x = 0\} \cup \{P_\infty\}$ の各点の軌道は $q-1$ 個の点からなる．交点数 $(C_a.X) = 2(q+1)$ であるから，C_a と X との交わりは,

性質 1

(I) $C_a.X = 2P_\infty + 2P_0 + (P_1 + \cdots + P_{q-1}) + (P'_1 + \cdots + P'_{q-1})$

(II) $C_a.X = 2P_\infty + 2P_0 + 2(P_1 + \cdots + P_{q-1})$

のいずれかの形である．ただし (I) の $P_1, \ldots, P_{q-1}, P'_1, \ldots, P'_{q-1}$ と (II) の $P_1, \ldots, P_{q-1}$ はそれぞれが相異なる点の組である.

[8] 興味をお持ちの方は [1], [2] をご覧下さい.

したがって C_a が (II) 型となるためには，連立方程式

$$\begin{cases} y^q + y = x^{q+1} \\ y = ax^2 \end{cases}$$

が $(0,0)$ 以外に重複解を持つことである．初等的な計算によりそれは $4a^{q+1} = 1$ ということで特徴付けられる．

性質 2

(i) q が 2 の冪であるときは (II) 型の C_a は存在しない．

(ii) q が奇素数の冪であるときは C_a が (II) 型であるための必要十分条件は $a^{q+1} = 1/4$ となることである．このとき，$P_1, \ldots, P_{q-1}$ は全て $\mathbb{F}_{q^2}$ 有理点である．

$(\alpha, \beta) \in C_a.X \setminus \{P_\infty, P_0\}$ のとき，容易に分かるように $(\frac{1}{a\alpha}, \frac{1}{\beta}) \in C_a.X \setminus \{P_\infty, P_0\}$ であり，これら 2 点が同じ軌道に含まれるための必要十分条件が $4a^{q+1} \neq 1$ である．よって，(I) 型の C_a については

性質 3 $C_a.X$ にあらわれる $2q-2$ 個の点 $P_1, \ldots, P_{q-1}, P'_1, \ldots, P'_{q-1}$ は全て $\mathbb{F}_{q^2}$ 有理点であるか，全てが $\mathbb{F}_{q^2}$ 有理点ではない．

$2q-2$ 個の点が全て $\mathbb{F}_{q^2}$ 有理点となるものを (I_0) 型とよぶことにする．

(I_0) 型あるいは (II) 型について，次の様な記法を用いる：

$$C'_a(\mathbb{F}_{q^2}) = \begin{cases} \{P_1, \ldots, P_{q-1}, P'_1, \ldots, P'_{q-1}\} & (C_a \text{ が } (\mathrm{I}_0) \text{ 型のとき}) \\ \{P_1, \ldots, P_{q-1}\} & (C_a \text{ が (II) 型のとき}) \end{cases}$$

$a, b \in \mathbb{F}_{q^2} \setminus \{0\}$ $(a \neq b)$ について，$C_a.C_b$ は $2P_\infty + 2P_0$ を含み $\deg C_a = \deg C_b = 2$ であるから，これら 2 点以外では交わらない．したがって，(I_0) 型あるいは (II) 型の C_a, C_b $(a \neq b)$ について $C'_a(\mathbb{F}_{q^2}) \cap C'_b(\mathbb{F}_{q^2}) = \emptyset$ である．また，$P \in X(\mathbb{F}_{q^2}) \setminus \{x = 0\} \cup \{P_\infty\}$ について，2 次曲線であって，それが定める X 上の因子が $2P_0 + 2P_\infty + P$ を含むものが一意的に存在するが，それは定め方よりある $a \in \mathbb{F}_{q^2} \setminus \{0\}$ に対する C_a である．性質 2, 3 より，この C_a は (I_0) 型あるいは (II) 型である．したがって，

性質 4

$$X(\mathbb{F}_{q^2}) \setminus \{x = 0\} \cup \{P_\infty\} = \coprod_{\substack{C_a \text{ は } (\mathrm{I}_0) \text{ 型} \\ \text{または (II) 型}}} C'_a(\mathbb{F}_{q^2})$$

性質 2, 4 より，それぞれの型の C_a がいくつあるか数え上げることができる．

	q が奇素数冪	q が 2 冪
(I_0) 型	$\dfrac{(q+1)(q-1)}{2}$	$\dfrac{q(q+1)}{2}$
(II) 型	$q+1$	0
(I) 型で (I_0) 型でない	$\dfrac{(q+1)(q-3)}{2}$	$\dfrac{(q+1)(q-2)}{2}$

(I_0) 型の y 座標による制御

適切な関数を構成するために (I_0) 型の 2 次曲線と 3 節で述べたような直線とを組み合せて用いる．そのため (I_0) 型についての $C'_a(\mathbb{F}_{q^2})$ 全体の配置をもう少し詳しく見る必要がある．これらは y 座標でうまく制御できる．

q を奇素数冪とする．乗法群 $\mathbb{F}_q \setminus \{0\}$ から自分自身への準同型 $c \mapsto c^2$ の像を G とする．q が奇素数だから ${}^{\#}G = (q-1)/2$ である．$(\mathbb{F}_{q^2} \setminus \{0\})/G$ は位数 $2q+2$ の巡回群であるが，生成元となる剰余類（の 1 つ）を B_1 とかき，$(\mathbb{F}_{q^2} \setminus \{0\})$ の G による剰余類への分解を

$$(\mathbb{F}_{q^2} \setminus \{0\}) = B_0 \coprod B_1 \coprod B_2 \coprod \cdots \coprod B_{2q+1}$$

とする．ただし，$B_0 = G$ であり，$B_j = B_1^j$ とする．

注意 4.1 生成元となる剰余類 B_1 のとり方にかかわらず,

$$B_{\frac{q+1}{2}} \cup B_{\frac{3(q+1)}{2}} = \{\beta \in \mathbb{F}_{q^2} \setminus \{0\} \mid Tr(\beta) = 0\}$$

である．したがって，$P \in X(\mathbb{F}_{q^2}) \setminus \{P_\infty, P_0\}$ で $y(P) \in B_{\frac{q+1}{2}} \cup B_{\frac{3(q+1)}{2}}$ となる P は 直線 $x = 0$ 上にある．すなわち，どんな型の $C'_a(\mathbb{F}_{q^2})$ にも乗らない．

また，$B_j^{-1} = B_j$ となるのは，$j = 0, q+1$ であり，(II) 型の C_a について，$C'_a(\mathbb{F}_{q^2}) = B_0$ または B_{q+1} である．

定理 4.2 (I_0) 型の C_a について，ある j で $0 < j < q+1, j \neq (q+1)/2$ となるものが存在し，$y(C'_a(\mathbb{F}_{q^2})) = B_j \cup B_{2q+2-j}$ である．また，上のような各 j について,

$${}^{\#}\{C_a \mid y(C'_a(\mathbb{F}_{q^2})) = B_j \cup B_{2q+2-j}\} = \frac{q+1}{2}$$

である．

最後に q が 2 冪の場合に対応する事実を述べる．この場合 $G = \mathbb{F}_q \setminus \{0\}$ となるから $(\mathbb{F}_{q^2} \setminus \{0\})/G$ は位数 $q+1$ の巡回群となり，$\mathbb{F}_{q^2} \setminus \{0\}$ の G による剰余類への分解は

$$(\mathbb{F}_{q^2} \setminus \{0\}) = B_0 \coprod B_1 \coprod B_2 \coprod \cdots \coprod B_q$$

と書ける．ここでも，$B_0 = G = \mathbb{F}_q \setminus \{0\}$，$B_j = B_1^j$ とした．定理 4.2 に対応する事実は次の様になる．

定理 4.3 (I_0) 型の C_a について，ある $0 < j \leq q/2$ が存在して $y(C'_a(\mathbb{F}_{q^2})) = B_j \cup B_{q+1-j}$ である．また，そのような各 j について

$$^{\#}\{C_a \,|\, y(C'_a(\mathbb{F}_{q^2})) = B_j \cup B_{q+1-j}\} = q+1$$

である．

参考文献

[1] M. Homma and S. J. Kim, *Determination of the minimum distance of two-point codes on a Hermitian curve: a first step*, preprint 2003

[2] 本間正明，Hermitian 曲線上の 2 点符号 (予報),「符号と暗号の代数的数理」研究集会報告集 (平松豊一編，数理研講究録として出版予定)

[3] F. J. MacWilliams and N. J. Sloane, The theory of error-correcting codes, North-Holland, Amsterdam, 1977

[4] H. Stichtenoth, *A note on Hermitian codes*, IEEE Trans. Inform. Theory **34** (1988), 1345–1348.

[5] K. Yang, On the weight hierarchy of Hermitian and other geometric Goppa codes, Ph. D. Thesis, University of Southern California, 1992.

[6] K. Yang, P. V. Kumar, *On the true minimum distance of Hermitian codes*, in: H. Stichtenoth, M. A. Tsfasman (eds.), Coding Theory and Algebraic Geometry (Luminy, 1991), Lecture Note in Mathematics 1518, Springer - Verlag, Berlin - Heidelberg, 1992, 99–107.

Masaaki HOMMA
Department of Mathematics
Faculty of engineering, Kanagawa University
Rokkakubashi Kanagawa-ku
221-8686, Japan
homma@kanagawa-u.ac.jp