エルミート曲線を用いた線形符号について

著者	藤川 大輔
出版者	法政大学大学院理工学研究科
雑誌名	法政大学大学院紀要．理工学・工学研究科編
巻	60
ページ	1-4
発行年	2019-03-31
URL	http://doi.org/10.15002/00022096

エルミート曲線を用いた線形符号について

ON LINEAR CODES CONSTRUCTED BY AN HERMITE CURVE

藤川大輔
Daisuke FUJIKAWA

指導教員 桂　利行

法政大学大学院理工学研究科システム理工学専攻修士課程

Society has changed from analog era to the digital age. Telecommunications are carried out by using bit strings of 0 and 1, but the bit inversion (replacement of 0 and 1) may occur by noises, etc. We call it an error. Such an error often occurs in the digital technology, and how to correct the errors is a problem of much practical interest. The theory of code plays a big role here. Coding theory is an indispensable technology in modern telecommunication. As one of the theories of codes, we have the theory of algebraic geometric code, which is based on the theory of algebraic curve. The features of algebraic geometric codes are that the code parameters are estimated with inequalities and that any linear codes are realized by algebraic geometric codes. In this research, we use algebraic curves and finite fields to construct linear codes with specific parameters.

Key Words *: Algebraic geometric code, Algebraic curve, Hermite curve*

1. はじめに

時代の流れとともにアナログからデジタルの時代へと推移してきた. 情報通信は 0 と 1 のビット列を用いて行われるが, ノイズなどによりビットの反転 (0 と 1 の入れ替え) が起こる. これを誤りという. デジタル技術には誤りがつきものであり, いかに誤りを訂正するかが問題である. ここで符号理論が大きな役割を担っている.

CD や DVD, 携帯電話をはじめとする様々な電子機器にはリード・ソロモン符号や BCH 符号が組み込まれているなど, 符号理論は現代の情報通信において必要不可欠な技術である. 符号理論の一分野に代数幾何符号がある. これは代数曲線論を取り入れたものである. 代数幾何符号の特徴として, 符号のパラメータが不等式で評価できる点やすべての線形符号は代数幾何符号で実現可能である点などが挙げられる.

本研究では, 有限体 $\mathbb{F}_{2^4}$ 上のエルミート曲線を用いて, 特定のパラメータをもつ符号の構成法を発見する.

2. 代数曲線論

平面アフィン代数曲線とは, 2 変数多項式の方程式 $f(x, y) = 0$ の解の集合のことである. 本研究においては代数曲線 $f(x, y) = 0$ が任意の点で非特異であるとする. つまり任意の点 (x_0, y_0) において $\frac{\partial f}{\partial x} \neq 0$ または $\frac{\partial f}{\partial y} \neq 0$ である. このような代数曲線を非特異代数曲線という. また代数曲線を分類する上で重要な離散的不変量である種数 g は, X が n 次の非特異射影代数曲線であるとき

$$g = \frac{(n-1)(n-2)}{2}, \tag{1}$$

で求めることができる.

代数曲線において因子という重要な概念がある. X を非特異射影代数曲線とする. X の有限個の点の形式的な整数環 $\mathbb{Z}$ の元を係数とする一次結合

$$D := \sum_P n_P P,$$

$$(P \in X, n_P \in \mathbb{Z}, \text{有限個の点を除き } n_P = 0)$$

を X 上の因子という. また, $\deg D = \sum_P n_P$ と定義し, D の次数という. これにより, 主因子と標準因子を定義する. 関数 $f \in k(X)\backslash 0$ に対し, f の零点のなす因子を $(f)_0$, f の極のなす因子を $(f)_\infty$ と表したとき,

$$(f) := (f)_0 - (f)_\infty,$$

を主因子という. X には標準因子 K_X が線形同値を除いて定義され, $\deg K_X = 2g - 2$ となる.

因子 D に対し,

$$L(D) = \{f \in k(X)\backslash\{0\} \mid (f) + D \succ 0\} \cup \{0\},$$

とおく. 次に $\dim L(D)$ を計算する上で重要となる, Riemann-Roch の定理と呼ばれる定理がある.

【Riemann-Roch の定理】種数が g である非特異射影代数曲線を X とおき, その標準因子を K_X とおく. このとき, X 上の任意の因子 D に対し,

$$\dim L(D) - \dim L(K_X - D) = \deg D - g + 1, \tag{2}$$

が成り立つ. ただし, $\deg D$ は因子 D の次数を表す.

X を $\mathbb{F}_q$ 上定義された代数曲線とするとき, X の $\mathbb{F}_q$ 上定義された点を有理点といい, 有理点の個数の限界式が色々と知られている. 特にその中でも Hasse-Weil-Serre 限界式は重要な限界式である.

【Hasse-Weil-Serre 限界式】X における有理点の個数を $\sharp X(\mathbb{F}_q)$ とし, g を X の種数とする. このとき,

$$\sharp X(\mathbb{F}_q) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor, \tag{3}$$

が成り立つ. ただし $\lfloor\ \rfloor$ はガウス記号である.

Hasse-Weil-Serre 限界式において等号を満たすような $\mathbb{F}_q$ 上の代数曲線を最大曲線と呼ぶこととする.

3. 符号理論

$\mathbb{F}_q$ を, $q(q = p^a, p$ は素数, a は自然数) 個の元をもつ有限体とし, $\mathbb{F}_q^n$ を $\mathbb{F}_q$ 上の n 次元横数ベクトル空間とする. $\mathbb{F}_q^n$ の元 $(x_1, x_2, \ldots, x_n)$ を符号語とよぶ. $\mathbb{F}_q^n$ の部分空間 C を考え, C の元を情報として送信する. この C を線形符号といい, n を C の符号長, C の次元 k を情報長という.

C の 2 つの符号語として

$$x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n),$$

とおく. このとき,

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

としたとき, $d(x, y)$ をハミング距離または単に距離という. 特に C のすべての符号語間を比較した際に最も最小となる距離を最小距離といい, d と表すこととする. また, としたとき, $w(x)$ をハミング重みまたは単に重みという. 特に C の成分が全て 0 の符号語を除く, すべての符号語に対して最小となる重みを最小重みと呼び, w と表す. 線形符号の場合, d と w が一致する性質がある.

符号長が n であり, 情報長が k, 最小距離が d である線形符号を $[n, k, d]$-(線形) 符号という. また, 符号長 n, 情報長 k, 最小距離 d を総称してパラメータという.

$[n, k, d]$-符号 C において, C の基底となるベクトルを行に持つ $k \times n$ 行列を生成行列といい, G で表す. 長さが k の情報ベクトルを i としたとき, 符号語 c は $c = iG$ で生成することが出来る. これにより生成された符号語の重みを全て調べることで, その符号の最小重み, つまり最小距離が求まる.

線形符号においては $\lfloor (d - 1)/2 \rfloor$ 個の誤りを訂正することが出来る.

【Singleton 限界式】符号長を n とし, 情報長を k, 最小距離を d とする. このとき,

$$d \leq n - k + 1, \tag{4}$$

が成り立つ.

このことから情報長 k と最小距離 d は共に大きくすることは不可能となる.

4. 代数幾何符号

以下, 有限体 $\mathbb{F}_q$ 上の代数曲線を X と表すこととする. また, X における有理点を $P_1, P_2, \ldots, P_n, Q_1, Q_2, \ldots, Q_l$(ただし n と l は自然数) とし, $m_1, m_2, \ldots, m_l$ は整数とする. このとき, 形式的な有限和として

$$D = P_1 + P_2 + \cdots + P_n,$$

を定義する. また, $\mathrm{supp}D \cap \mathrm{supp}G = \emptyset$ となる因子 $G = m_1Q_1 + m_2Q_2 + \cdots + m_lQ_l$ を選ぶことで,

$$L(G) = \{f \in \mathbb{F}_q(X)\backslash\{0\} \mid (f) + G \succ 0\} \cup \{0\},$$

となる関数空間の部分空間を定義することが出来る. これによって写像

$$\begin{array}{ccc} L(G) & \xrightarrow{\varphi} & \mathbb{F}_q^n \\ \cup & & \cup \\ f & \longmapsto & (f(P_1), f(P_2), \ldots, f(P_n)), \end{array}$$

を構成することが可能となる. $C(X, D, G) = \mathrm{Im}\varphi$ とおき, $C(X, D, G)$ を代数幾何符号という.

$\deg(K_X - G) < 0$ の場合は $\dim L(K_X - D) = 0$ である. これと (4) 式により, $2g - 2 < \deg G < n$ ならば,

$$k = \deg G - g + 1, \tag{5}$$

$$n - \deg G \leq d \leq n - \deg G + g, \tag{6}$$

となる. これにより実現可能な符号のパラメータの範囲を明らかにすることが可能となる.

5. C_{ab} 曲線

三浦 [4] によって発見された C_{ab} と呼ばれる曲線上で定義される線形符号 (C_{ab} 符号と略す) は, フェルマー曲線, 楕円曲線や超楕円曲線などの有用な多くの曲線上の符号を包含している. そして, Feng-Rao 設計距離 δ_{FR} の下界として, Goppa 限界として知られる最小距離の下界が得られ, その結果, Feng-Rao 復号アルゴリズムによって Goppa 限界以上の誤りが訂正できるという優れた特徴を備えている. また実際に, 従来の BCH 符号などでは達成されなかった優れた符号パラメータを有する符号が, C_{ab} 符号として構成できることが示されている [5].

【定義】$a, b(a < b)$ を $\gcd(a, b) = 1$ である正整数とする. このとき,

$$h(x, y) = x^b + \alpha y^a + g(x, y) = 0$$

で定義される曲線を C_{ab} 曲線と呼ぶ. ただし, $\alpha \in \mathbb{F}_q^\times = \mathbb{F}\backslash\{0\}, g(x, y) = \sum_{\substack{i,j \geq 0 \\ ai+bj<ab}} \alpha_{ij}x^iy^j, \alpha_{ij} \in \mathbb{F}_q$ である.

【定義】q を素数のべきとして, $\mathbb{F}_{q^2}$ 上の曲線を

$$x^{q+1} - y^q - y = 0, \quad x, y \in \mathbb{F}_{q^2} \tag{7}$$

で定義する. この曲線はエルミート曲線と呼ばれ, C_{ab} 曲線の定義式において $a = q, b = q + 1, \alpha = -1, g(x, y) = -y$ といたものになっている.

6. 代数幾何符号の構成

有限体 $\mathbb{F}_{2^4}$ 上のエルミート曲線 $x^5 - y^4 - y = 0$ を用いて, 具体的な符号の構成を試みた.

まずはじめに, 有限体 $\mathbb{F}_{2^4}$ の元を生成するために既約多項式 $x^4 + x^3 + 1$ の根を α とし, べき表現と多項式表現, ベクトル表現をまとめた表 1 を作成した.

(1) 式より, $x^5 - y^4 - y = 0$ の種数 g は $g = 6$ である. したがって, Hasse-Weil-Serre 限界式を用いると,

$$\sharp X(\mathbb{F}_{2^4}) \leq 2^4 + 1 + \lfloor 2\sqrt{2^4} \rfloor = 65$$

となる. それをもとに, この代数曲線における $\mathbb{F}_{2^4}$ 有理点がいくつあるかすべて調べた. その結果, 65 個の $\mathbb{F}_{2^4}$ 有理点を持つことが確認できた. そして各有理点を $P_0.P_1, \ldots, P_{64}$ とおき, 表 2 としてまとめた. これより, 次のことがわかる.

表 1 有限体 $\mathbb{F}_{2^4}$

べき表現	多項式表現	ベクトル表現
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	α^3+1	1001
α^5	$\alpha^3+\alpha+1$	1011
α^6	$\alpha^3+\alpha^2+\alpha+1$	1111
α^7	$\alpha^2+\alpha+1$	0111
α^8	$\alpha^3+\alpha^2+\alpha$	1110
α^9	α^2+1	0101
α^{10}	$\alpha^3+\alpha$	1010
α^{11}	$\alpha^3+\alpha^2+1$	1101
α^{12}	$\alpha+1$	0011
α^{13}	$\alpha^2+\alpha$	0110
α^{14}	$\alpha^3+\alpha^2$	1100

【命題】有限体 $\mathbb{F}_{2^4}$ 上において $x^5-y^4-y=0$ は最大曲線である.

これにより, 有限体 $\mathbb{F}_{2^4}$ 上の代数曲線 $x^5-y^4-y=0$ は代数幾何符号を構成する上でよい代数曲線であることが証明された.

a を自然数として, 因子 G および D を

$$G = aP_0$$
$$D = P_1 + P_2 + \cdots + P_{64},$$

と定めると, $\mathrm{supp}G \cap \mathrm{supp}D = \emptyset$ となる. そこで, 写像 φ を

$$\begin{array}{ccc} L(G) & \xrightarrow{\varphi} & \mathbb{F}_{2^4}^{64} \\ \cup & & \cup \\ f & \longmapsto & (f(P_1), f(P_2), \ldots, f(P_{64})), \end{array}$$

としたとき, 符号 C は $C = \mathrm{Im}\varphi$ である.

$10 < a < 64$ のとき, (5) 式, (6) 式より

$$k = \deg(aP_0) - g + 1 = a - 5,$$

$$64 - a \le d \le 70 - a$$

が成り立つ. したがって, この符号 C は $[64, a-5, d]$-線形符号である. ただし, $64-a \le d \le 70-a$ である.

実際にこの有限体 $\mathbb{F}_{2^4}$ 上の代数曲線 $x^5-y^4-y=0$ から代数幾何符号を生成する.

(1) $a = 11$ のとき

符号 C は $[64, 6, d]$-線形符号であり, $53 \le d \le 59$ である. $L(G)$ の基底を表 3 に示す. ここで, 以下の命題が成り立つ.

【命題】$L(10P_0) = L(11P_0)$.

このことから,

$$54 = 64 - \deg(10P_0) \le d \le 64 - \deg(10P_0) + 6 = 60$$

表 2 代数曲線 $x^5-y^4-y=0$ における $\mathbb{F}_{2^4}$ 有理点

有理点	斉次座標	有理点	斉次座標
P_0	$(0,1,1)$		
P_1	$(0,0,1)$	P_{31}	$(1,\alpha^3,\alpha^{10})$
P_2	$(0,1,0)$	P_{32}	$(1,\alpha^{10},\alpha^3)$
P_3	$(0,1,\alpha^5)$	P_{33}	$(1,\alpha^3,\alpha^{14})$
P_4	$(0,\alpha^5,1)$	P_{34}	$(1,\alpha^{14},\alpha^3)$
P_5	$(0,1,\alpha^{10})$	P_{35}	$(1,\alpha^4,\alpha^6)$
P_6	$(0,\alpha^{10},1)$	P_{36}	$(1,\alpha^6,\alpha^4)$
P_7	$(1,1,\alpha^7)$	P_{37}	$(1,\alpha^4,\alpha^{10})$
P_8	$(1,\alpha^7,1)$	P_{38}	$(1,\alpha^{10},\alpha^4)$
P_9	$(1,1,\alpha^{11})$	P_{39}	$(1,\alpha^4,\alpha^{12})$
P_{10}	$(1,\alpha^{11},1)$	P_{40}	$(1,\alpha^{12},\alpha^4)$
P_{11}	$(1,1,\alpha^{13})$	P_{41}	$(1,\alpha^4,\alpha^{13})$
P_{12}	$(1,\alpha^{13},1)$	P_{42}	$(1,\alpha^{13},\alpha^4)$
P_{13}	$(1,1,\alpha^{14})$	P_{43}	$(1,\alpha^5,\alpha^6)$
P_{14}	$(1,\alpha^{14},1)$	P_{44}	$(1,\alpha^6,\alpha^5)$
P_{15}	$(1,\alpha,\alpha^3)$	P_{45}	$(1,\alpha^5,\alpha^8)$
P_{16}	$(1,\alpha^3,\alpha)$	P_{46}	$(1,\alpha^8,\alpha^5)$
P_{17}	$(1,\alpha,\alpha^7)$	P_{47}	$(1,\alpha^6,\alpha^{13})$
P_{18}	$(1,\alpha^7,\alpha)$	P_{48}	$(1,\alpha^{13},\alpha^6)$
P_{19}	$(1,\alpha,\alpha^9)$	P_{49}	$(1,\alpha^7,\alpha^9)$
P_{20}	$(1,\alpha^9,\alpha)$	P_{50}	$(1,\alpha^9,\alpha^7)$
P_{21}	$(1,\alpha,\alpha^{10})$	P_{51}	$(1,\alpha^7,\alpha^{13})$
P_{22}	$(1,\alpha^{10},\alpha)$	P_{52}	$(1,\alpha^{13},\alpha^7)$
P_{23}	$(1,\alpha^2,\alpha^3)$	P_{53}	$(1,\alpha^8,\alpha^9)$
P_{24}	$(1,\alpha^3,\alpha^2)$	P_{54}	$(1,\alpha^9,\alpha^8)$
P_{25}	$(1,\alpha^2,\alpha^5)$	P_{55}	$(1,\alpha^8,\alpha^{11})$
P_{26}	$(1,\alpha^5,\alpha^2)$	P_{56}	$(1,\alpha^{11},\alpha^8)$
P_{27}	$(1,\alpha^2,\alpha^6)$	P_{57}	$(1,\alpha^8,\alpha^{12})$
P_{28}	$(1,\alpha^6,\alpha^2)$	P_{58}	$(1,\alpha^{12},\alpha^8)$
P_{29}	$(1,\alpha^2,\alpha^{14})$	P_{59}	$(1,\alpha^{10},\alpha^{12})$
P_{30}	$(1,\alpha^{14},\alpha^2)$	P_{60}	$(1,\alpha^{12},\alpha^{10})$
		P_{61}	$(1,\alpha^{11},\alpha^{12})$
		P_{62}	$(1,\alpha^{12},\alpha^{11})$
		P_{63}	$(1,\alpha^{11},\alpha^{14})$
		P_{64}	$(1,\alpha^{14},\alpha^{11})$

が成り立つ. よって, 最小距離 d は

$$54 \le d \le 59$$

となる. そこで, 重みが 54 となる関数体の組合せを見つければよい. 実際, f_4+f_5 のとき重みが 54 となる. よって, 最小距離 d は $d=54$ とわかる.

【定理】有限体 $\mathbb{F}_{2^4}$ 上の代数曲線 $x^5-y^4-y=0$ において因子 $G = 11P_0$ を用いると, 代数幾何符号として $[64, 6, 54]$-線形符号を構成することができる.

(2) $a = 12$ のとき

表 3 $L(G)$ の基底 ($a = 11$ のとき)

関数体	関数	位数
f_1	1	0
f_2	$\frac{x}{y+1}$	-4
f_3	$\frac{y}{y+1}$	-5
f_4	$\frac{x^2}{(y+1)^2}$	-8
f_5	$\frac{xy}{(y+1)^2}$	-9
f_6	$\frac{y^2}{(y+1)^2}$	-10

符号 C は $[64, 7, d]$-線形符号であり, $52 \leq d \leq 58$ である. $L(G)$ の基底を表 4 に示す. そこで, 重みが 52 となる関数体

表 4 $L(G)$ の基底 ($a = 12$ のとき)

関数体	関数	位数
f_1	1	0
f_2	$\frac{x}{y+1}$	-4
f_3	$\frac{y}{y+1}$	-5
f_4	$\frac{x^2}{(y+1)^2}$	-8
f_5	$\frac{xy}{(y+1)^2}$	-9
f_6	$\frac{y^2}{(y+1)^2}$	-10
f_7	$\frac{x^3}{(y+1)^3}$	-12

の組合せを見つければよい. 実際, $\alpha^4 f_5 + f_7$ のとき重みが 52 となる. よって, 最小距離 d は $d = 52$ とわかる.

【定理】有限体 $\mathbb{F}_{24}$ 上の代数曲線 $x^5 - y^4 - y = 0$ において因子 $G = 12P_0$ を用いると, 代数幾何符号として $[64, 7, 52]$-線形符号を構成することができる.

(3) $a = 14$ のとき

符号 C は $[64, 9, d]$-線形符号であり, $50 \leq d \leq 56$ である. $L(G)$ の基底を表 5 に示す. そこで, 重みが 50 となる関数体

表 5 $L(G)$ の基底 ($a = 14$ のとき)

関数体	関数	位数
f_1	1	0
f_2	$\frac{x}{y+1}$	-4
f_3	$\frac{y}{y+1}$	-5
f_4	$\frac{x^2}{(y+1)^2}$	-8
f_5	$\frac{xy}{(y+1)^2}$	-9
f_6	$\frac{y^2}{(y+1)^2}$	-10
f_7	$\frac{x^3}{(y+1)^3}$	-12
f_8	$\frac{x^2y}{(y+1)^3}$	-13
f_9	$\frac{xy^2}{(y+1)^3}$	-14

の組合せを見つければよい. 実際, $f_4 + f_5 + f_7 + f_9$ のとき重みが 50 となる. よって, 最小距離 d は $d = 50$ とわかる.

【定理】有限体 $\mathbb{F}_{24}$ 上の代数曲線 $x^5 - y^4 - y = 0$ において因子 $G = 14P_0$ を用いると, 代数幾何符号として $[64, 9, 50]$-線形符号を構成することができる.

(4) $a = 15$ のとき

符号 C は $[64, 10, d]$-線形符号であり, $49 \leq d \leq 55$ である. $L(G)$ の基底を表 6 に示す. そこで, 重みが 49 となる関数体

表 6 $L(G)$ の基底 ($a = 15$ のとき)

関数体	関数	位数
f_1	1	0
f_2	$\frac{x}{y+1}$	-4
f_3	$\frac{y}{y+1}$	-5
f_4	$\frac{x^2}{(y+1)^2}$	-8
f_5	$\frac{xy}{(y+1)^2}$	-9
f_6	$\frac{y^2}{(y+1)^2}$	-10
f_7	$\frac{x^3}{(y+1)^3}$	-12
f_8	$\frac{x^2y}{(y+1)^3}$	-13
f_9	$\frac{xy^2}{(y+1)^3}$	-14
f_{10}	$\frac{y^3}{(y+1)^3}$	-15

の組合せを見つければよい. $f_4 + f_5 + f_7 + f_9$ のとき重みが 50 となるが, 重みが 49 となる組合せは発見できなかった. よって, 最小距離 d は $d = 49$ または 50 とわかる.

7. おわりに

有限体 $\mathbb{F}_{24}$ 上の代数曲線 $x^5 - y^4 - y = 0$ を用いて, 代数幾何符号を構成した. そして, $a = 15$ の場合には最小距離は 49 または 50 であることがわかった. また, $a = 11, 12, 14$ の 3 つの場合には最小距離を定めることができた.

パラメータの決定に関して, 最小距離 d の決定は容易ではない. 今後の課題として, 有限体での計算を可能とするプログラムを活用した最小距離 d の決定が挙げられる. また, 今回用いたエルミート曲線は最大曲線であったが, 任意の種数に対して, その種数を持つ最大曲線が存在するかどうかはわからない. そこで, 標数や代数曲線の次数を変更して計算し, いつ最大曲線となるか推測することなどが挙げられる.

参考文献

[1] 桂利行 : 代数幾何入門, 共立出版, 1998

[2] 今井秀樹 : 符号理論, 電子情報通信学会, 1990

[3] 坂庭好一, 渋谷智治 : 代数系と符号理論入門, コロナ社, 2010

[4] 三浦晋示 : ある平面曲線上の代数幾何符号, 電子情報通信学会論文誌, vol.J75-A, no.11, pp.1735–1746, 1992

[5] 山西健司 : Fermat 符号の構成と性能について, 電子情報通信学会論文誌, vol.J72-A, no.3, pp.597-607, 1989