

有限体上の代数曲線を用いた符号について

森田, 洋平 / MORITA, Yohei

(出版者 / Publisher)

法政大学大学院理工学・工学研究科

(雑誌名 / Journal or Publication Title)

法政大学大学院紀要. 理工学・工学研究科編

(巻 / Volume)

56

(開始ページ / Start Page)

1

(終了ページ / End Page)

4

(発行年 / Year)

2015-03-24

(URL)

<https://doi.org/10.15002/00011353>

有限体上の代数曲線を用いた符号について

ON CODES CONSTRUCTED BY AN ALGEBRAIC CURVES OVER A FINITE FIELD

森田 洋平

Yohei MORITA

指導教員 桂 利行

法政大学大学院理工学研究科システム工学専攻修士課程

The coding theory plays an important role in improving the reliability in information and communication. In particular, the error correcting code is applied to the field such as acoustic equipments and satellite communications. In the beginning of 1980's, V.D.Goppa, a mathematician, discovered the algebraic geometry code. This code is the error correcting code based on algebraic geometry. It is possible to generate algebraic geometry code by using algebraic curves over a finite field. We can estimate the information length and the minimum distance of these codes. However, there are many codes that are not constructed concretely. In this paper, we construct some concrete algebraic geometry codes by using an algebraic curve over a finite field.

Key Words : Algebraic curve, Error correcting code, Algebraic geometry code, Finite field

1. はじめに

昨今、符号理論は CD や DVD、Blue-ray Disc などの光ディスクや通信衛星にも応用されており、情報通信において誤り訂正符号は工学的において必要不可欠な技術となっている。

誤り訂正符号には数学的な側面も多く潜んでいる。1980 年代初頭に数学者 Valery Denisovich Goppa によって明らかとなった代数幾何符号は特に顕著である。Valery Denisovich Goppa は符号理論に代数幾何における性質を応用することで、当時不可能とされていた訂正能力の高い強力な符号が存在することを数学的に証明した。これにより、代数多様体を用いた符号が発見された。しかしながら具体的な構成が明らかになっていない代数幾何符号も今もなお多く存在する。本論文では代数曲線を用いて代数幾何符号を具体的に生成することを試みた。

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点であるとする。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 $\frac{\partial f}{\partial y} \neq 0$ となる。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を表す**種数**を g とする。

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 Z の元を係数とする一次結合

$$D := \sum_P n_P P$$

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

を X 上の因子という。

これより、 $\deg D = \sum_P n_P$ 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 $f \in k(X) \setminus \{0\}$ 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。

種数 g を用いて $\dim K_X = 2g - 2$ となる因子 K_X を**標準因子**という。

因子 D に対し、

$$L(D) = \{f \in k(X) \setminus \{0\} \mid (f) + D \succeq 0\} \cup \{0\}$$

とおき、 $l(D) = \dim L(D)$ とする。

次に $l(D)$ 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 である非特異で完備である代数曲線を 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、

$$l(D) - l(K_X - D) = \deg D + 1 - g$$

が成り立つ。ただし、 $\deg D$ は因子 D の次数を表す。■

C を F_q 上定義された代数曲線とすると、有理点の個数の限界式が色々知られている。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】 C における有理点の個数を $\sharp C(F_q)$ とし、 g を C の種数とする。このとき、

$$\sharp C(F_q) \leq q + 1 + g[2\sqrt{q}]$$

が成り立つ。ただし $[\]$ 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 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

(1) 線形符号

元の数が q 個の有限体を F_q とし、その上の n 次元行数ベクトル空間を F_q^n と表すこととする。ただし $q = p^m$ で、 p は素数であり m は自然数である。 F_q^n の元 $(x_1, x_2, \dots, x_n)$ を符号語またはアルファベットという。さらに n を符号長という。また $F_q^n \supset C$ が部分空間であるとき、 C を線形符号といい、 C の次元 k を情報長という。

C の 2 つの符号語として

$$\begin{aligned} x &= (x_1, x_2, \dots, x_n) \\ y &= (y_1, y_2, \dots, y_n) \end{aligned}$$

をおく。このとき、

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

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、

$$w(x) = \#\{i \mid x_i \neq 0, 1 \leq i \leq n\}$$

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 の符号を除く、すべての符号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。

$[n, k, d]$ 符号 C において、 C の基底となるベクトルを行に持つ (k, n) 行列を生成行列といい、 G で表す。長さ 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。また Singleton 限界式により、情報長 k を長くすると誤り訂正可能な個数は少なくなり、一方で誤り訂正可能な個数を多くしようとすると情報長 k は短くなってしまふ。

【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、

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

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。

(2) 代数幾何符号

以下、有限体 F_q 上の代数曲線を C と表すこととする。また、 C における有理点を $P_1, P_2, \dots, P_n, Q_1, Q_2, \dots, Q_l$ (ただし n と l は自然数) とし、 $m_1, m_2, \dots, m_l$ は整数とする。このとき、形式的な和として

$$D = P_1 + P_2 + \dots + P_n$$

を定義することができる。また、 $D \cap G = \emptyset$ となる因子 $G = m_1 Q_1 + m_2 Q_2 + \dots + m_l Q_l$ を選ぶことで、

$$L(G) = \{f \in F_q(C) \setminus \{0\} \mid (f) + G \succ 0\} \cup \{0\}$$

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

$$\begin{array}{ccc} L(G) & \xrightarrow{\phi_L} & F_q^n \\ \psi & & \psi \\ f & \mapsto & (f(P_1), f(P_2), \dots, f(P_n)) \end{array}$$

を構成することが可能となる。 $C_L(C, D, G) = \text{Im } \phi_L$ とおき、 $C_L(C, D, G)$ を弱い意味の代数幾何符号という。

$\deg(K_C - G) < 0$ の場合は $l(K_C - D) = 0$ である。

これと Singleton 限界式により、

(1) $\deg G < n$ の場合

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

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

(2) $2g - 2 < \deg G < n$ の場合

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

となる。これにより実現可能な $[n, k, d]$ 符号の範囲を明らかにすることが可能となる。

$G \succ 0$ かつ $\deg G < n$ のとき、 C_L を代数幾何符号という。さらに $G \succ 0$ かつ $2g - 2 < \deg G < n$ のとき、 C_L を強い意味の代数幾何符号ということが多い。

これにより $L(G)$ から F_q^n への写像 ϕ_L が構成可能となる。

4. 結果

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ を用いて、具体的な符号の生成を試みた。

まずはじめに、有限体 F_{2^4} の元を生成するために既約多項式 $x^4 + x^3 + 1 = 0$ の根を α とし、冪表現と多項式表現、ベクトル表現をまとめた表が以下である。

冪表現	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	$\alpha^3 + 1$	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	$\alpha^2 + 1$	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

それをもとに、この代数曲線における 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 F_{2^4} 有理点を持つことが確認できた。この際、 $x^5 + y^5 = 1$ の代数曲線は射影空間においては $x^5 + y^5 = z^5$ と表されることより斉次座標 (x, y, z) で求めた。そして各有理点を $P_0, \dots, P_{64}$ 表として以下にまとめた。

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

これより、以下のことが分かる。

【命題】

有限体 F_{2^4} 上において代数曲線 $x^5 + y^5 = 1$ は最大曲線である。■

実際にこの有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ から代数幾何符号を生成する。

a を自然数として $G = aP_0$ とおく。すると、

$$\begin{array}{ccc} L(aP_0) & \xrightarrow{\phi_L} & F_{2^4}^{64} \\ \cup & & \cup \\ f & \longmapsto & (f(P_1), f(P_2), \dots, f(P_{64})) \end{array}$$

となる代数幾何符号の生成が可能である。

この場合、定理より、

(1) $a = \deg(aP_0) < 64$ ならば

$$k_L \geq \deg(aP_0) - 6 + 1 = a - 5$$

$$64 - a = 64 - \deg(aP_0) \leq d_L \leq 64 - \deg(aP_0) + 6 = 70 - a$$

(2) $10 = 2\delta - 2 < a = \deg(aP_0) < 64$ ならば

$$k_L = \deg(aP_0) - 6 + 1 = a - 5$$

が成り立つ。

(2) より $a > 10$ の場合、強い意味の代数幾何符号となるため情報長が定まり、符号として扱いやすくなる。

(1) $L(11P_0)$ の場合

$$k_L = \deg(11P_0) - 6 + 1 = 11 - 5 = 6$$

$$53 = 64 - \deg(11P_0) \leq d_L \leq 64 - \deg(11P_0) + 6 = 59$$

となるが、 $L(11P_0)$ の場合は次の命題が成り立つ。

【命題】

$$L(10P_0) = L(11P_0) \quad \blacksquare$$

このことから、

$$54 = 64 - \deg(11P_0) \leq d_L \leq 64 - \deg(11P_0) + 6 = 60$$

となる。

すると、 P_0 で極を持ち、それ以外の有理点において正則となるような関数を見つけることで、それらが基底となる。

関数	位数
f_1	1
f_2	$\frac{x}{(y+1)}$
f_3	$\frac{1}{(y+1)}$
f_4	$\frac{x^2}{(y+1)^2}$
f_5	$\frac{x}{(y+1)^2}$
f_6	$\frac{1}{(y+1)^2}$

が得られる。

これらより、線形写像

$$\begin{array}{ccc} L(11P_0) & \xrightarrow{\phi_L} & F_{2^4}^{64} \\ \cup & & \cup \\ f & \longmapsto & (f(P_1), f(P_2), \dots, f(P_{64})) \end{array}$$

によって強い意味の代数幾何符号の生成行列が得られる。

実際に、これらの基底を

$$f_3 + f_6 = \frac{1}{(y+1)} + \frac{1}{(y+1)^2}$$

と組み合わせることにより、重みが 54 となる。

これより、以下の定理を導いたことになる。

【定理】

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ において因子 $G = 11P_0$ を用いると、 M_1 代数幾何符号として $[64, 6, 54]$ 符号を生成することができる。

(2) $L(15P_0)$ の場合

$$k_L = \deg(15P_0) - 6 + 1 = 15 - 5 = 10$$

$$49 = 64 - \deg(15P_0) \leq d_L \leq 64 - \deg(15P_0) + 6 = 55$$

関数 $f_1, f_2, \dots, f_6$ にさらに以下の関数も加える。

関数	位数
f_7	$\frac{x^3}{(y+1)^3}$
f_8	$\frac{x^2}{(y+1)^3}$
f_9	$\frac{x}{(y+1)^3}$
f_{10}	$\frac{1}{(y+1)^3}$

これらから、 $f_5 + f_6 + f_9 + f_{10}$ と組み合わせることにより、重みが 49 となる。

【定理】

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ において因子 $G = 15P_0$ を用いると、 M_2 代数幾何符号として $[64, 10, 49]$ 符号を生成することができる。

(3) $L(20P_0)$ の場合

$$k_L = \deg(20P_0) - 6 + 1 = 20 - 5 = 15$$

$$44 = 64 - \deg(20P_0) \leq d_L \leq 64 - \deg(20P_0) + 6 = 50$$

関数 $f_1, f_2, \dots, f_{10}$ にさらに以下の関数も加える.

	関数	位数
f_{11}	$\frac{x^4}{(y+1)^4}$	-16
f_{12}	$\frac{x^3}{(y+1)^4}$	-17
f_{13}	$\frac{x^2}{(y+1)^4}$	-18
f_{14}	$\frac{x}{(y+1)^4}$	-19
f_{15}	$\frac{1}{(y+1)^4}$	-20

これらから、 $f_5 + f_6 + f_9 + f_{11} + \alpha^{12}f_{14} + \alpha^{12}f_{15}$ と組み合わせることにより、重みが 44 となる.

【定理】

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ において因子 $G = 20P_0$ を用いると、 M_3 代数幾何符号として [64, 15, 44] 符号を生成することができる.

(4) $L(25P_0)$ の場合

$$k_L = \deg(25P_0) - 6 + 1 = 25 - 5 = 20$$

$$39 = 64 - \deg(25P_0) \leq d_L \leq 64 - \deg(25P_0) + 6 = 45$$

関数 $f_1, f_2, \dots, f_{15}$ にさらに以下の関数も加える.

	関数	位数
f_{16}	$\frac{x^4}{(y+1)^5}$	-21
f_{17}	$\frac{x^3}{(y+1)^5}$	-22
f_{18}	$\frac{x^2}{(y+1)^5}$	-23
f_{19}	$\frac{x}{(y+1)^5}$	-24
f_{20}	$\frac{1}{(y+1)^5}$	-25

これらから、 $f_2 + f_5 + f_6 + \alpha^{13}f_9 + \alpha^{13}f_{10} + \alpha^3f_{15} + \alpha^{11}f_{19} + \alpha^6f_{20}$ と組み合わせることにより、重みが 39 となる.

【定理】

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ において因子 $G = 25P_0$ を用いると、 M_4 代数幾何符号として [64, 20, 39] 符号を生成することができる.

(5) $L(30P_0)$ の場合

$$k_L = \deg(30P_0) - 6 + 1 = 30 - 5 = 25$$

$$34 = 64 - \deg(30P_0) \leq d_L \leq 64 - \deg(30P_0) + 6 = 40$$

関数 $f_1, f_2, \dots, f_{20}$ にさらに以下の関数も加える.

	関数	位数
f_{21}	$\frac{x^4}{(y+1)^6}$	-26
f_{22}	$\frac{x^3}{(y+1)^6}$	-27
f_{23}	$\frac{x^2}{(y+1)^6}$	-28
f_{24}	$\frac{x}{(y+1)^6}$	-29
f_{25}	$\frac{1}{(y+1)^6}$	-30

これらから、 $f_5 + f_6 + \alpha^6f_9 + \alpha^6f_{10} + \alpha^{14}f_{14} + \alpha^7f_{19} + \alpha^6f_{20} + \alpha^9f_{24} + f_{25}$ と組み合わせることにより、重みが 34 となる.

【定理】

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ において因子 $G = 30P_0$ を用いると、 M_5 代数幾何符号として [64, 25, 34] 符号を生成することができる.

(6) $L(35P_0)$ の場合

$$k_L = \deg(35P_0) - 6 + 1 = 35 - 5 = 30$$

$$29 = 64 - \deg(35P_0) \leq d_L \leq 64 - \deg(35P_0) + 6 = 35$$

関数 $f_1, f_2, \dots, f_{25}$ にさらに以下の関数も加える.

	関数	位数
f_{26}	$\frac{x^4}{(y+1)^7}$	-31
f_{27}	$\frac{x^3}{(y+1)^7}$	-32
f_{28}	$\frac{x^2}{(y+1)^7}$	-33
f_{29}	$\frac{x}{(y+1)^7}$	-34
f_{30}	$\frac{1}{(y+1)^7}$	-35

これらから、 $f_5 + f_6 + \alpha^2f_9 + \alpha^2f_{10} + f_{14} + \alpha^{11}f_{15} + \alpha^8f_{19} + \alpha^6f_{20} + \alpha^{12}f_{24} + \alpha^{11}f_{25} + \alpha^{14}f_{29} + \alpha^{10}f_{30}$ と組み合わせることにより、重みが 29 となる.

【定理】

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ において因子 $G = 35P_0$ を用いると、 M_6 代数幾何符号として [64, 30, 29] 符号を生成することができる.

5. おわりに

有限体 F_{2^4} 上の代数曲線 $x^5 + y^5 = 1$ から因子 $37P_0$ を用いて符号化率 $k/n = 1/2$ となるように $L(37P_0)$ における具体的な代数幾何符号の生成も試みたが、この場合の最小距離 27 を取るような組み合わせは発見できなかった. 一方で、 $L(35P_0)$ において最小重みが 29 に関しては保証されていることから、 $L(37P_0)$ においても最小重みが 29 までは保証されている.

現在、情報通信に用いられている符号は BCH 符号やリード・ソロモン符号である. 代数幾何符号は基底となる関数の取り方が問題となり、種数が高くなると具体的な計算が複雑になる. 今後、純粋数学の発展によって代数幾何符号が誤り訂正符号の中で大きな役割を演じることを期待している.

参考文献

- 1) 桂 利行：代数幾何入門（共立講座 21 世紀の数学），共立出版，1998
- 2) 梶原 健：代数曲線入門 はじめての代数幾何（日評数学選書），日本評論社，2004
- 3) 今井 秀樹：符号理論，コロナ社，1990
- 4) Henning Stichtenoth：Algebraic Function Fields and Codes，Springer-Verlag，1993