

代数系と符号理論 第15回板書プリント

植松友彦 2007.7.6

1 有限幾何入門

有限の点（「つぶつぶ」）からなる幾何学について説明し、有限幾何が符号の構成に利用できることを説明する。

1.1 点と線

ここでは、 F_{2^s} 上の m 次元ベクトル空間からなる $\text{EG}(m, 2^s)$ と呼ばれる有限ユークリッド幾何について説明する。

- 点： $F_{2^s}^m$ の元 $a = (a_0, a_1, \dots, a_{m-1})$ のことを $\text{EG}(m, 2^s)$ の点という。とくに、 $(0, 0, \dots, 0)$ のことを原点という。
- 直線：2点 a_0 と a が線形独立であるとき（すなわち $\beta_0 a_0 + \beta a = 0$ となるのは $\beta_0 = \beta = 0$ に限るとき）、 2^s 個の点の集合

$$\{a_0 + \beta a\} \triangleq \{a_0 + \beta a : \beta \in F_{2^s}\}$$

を直線または1-フラットという。

通常の幾何学とは異なり、直線は有限個の点の集合でしかなく、全ての直線が等しい個数 2^s の要素を有することに注意する。

以下に、直線の幾つかの性質を示す。

性質1 (平行な直線) a_0 と a が線形独立であるとき、直線 $\{\beta a\}$ と $\{a_0 + \beta a\}$ は共通の点を持たない。なぜなら、もし共通の点を有したとすれば、ある $\beta', \beta'' \in F_{2^s}$ が存在して、

$$\beta' a = a_0 + \beta'' a$$

が成り立つ。この式は、

$$a_0 + (\beta'' - \beta')a = 0$$

を意味し、これは a_0 と a が線形独立であることに矛盾する。

以下では、 $\{\beta a\}$ と $\{a_0 + \beta a\}$ は「平行」であるという。これは、通常のユークリッド幾何学における直線の方程式において y 切片が異なり傾きが等しい直線が平行であることに対応している。 b_0 を直線 $\{\beta a\}$ にも直線 $\{a_0 + \beta a\}$ にも含まれない点とする。このとき、直線 $\{b_0 + \beta a\}$ は、点 b_0 を通り、2直線 $\{\beta a\}$ と $\{a_0 + \beta a\}$ に平行な直線である。

各々の直線は 2^s 個の点を有しているので、 $\text{EG}(m, 2^s)$ では、原点を通る直線 $\{\beta a\}$ に平行な直線は $2^{(m-1)s} - 1$ 本ある。これらの $2^{(m-1)s}$ 本の平行直線を平行束 (parallel bundle) をなすという。

性質 2 (交わる直線) $EG(m, s)$ において、 a_1 と a_2 を線形独立な点とする。このとき、直線 $\{a_0 + \beta a_1\}$ と $\{a_0 + \beta a_2\}$ は唯一の点 a_0 を共通に有する。なぜならば、もし a_0 以外に共通の点があったとすれば、 $\beta' \neq 0$ および $\beta'' \neq 0$ が存在して、

$$a_0 + \beta' a_1 = a_0 + \beta'' a_2$$

が成り立ち、この式は、 $\beta' a_1 - \beta'' a_2 = 0$ を意味し、これは a_1, a_2 が線形独立であったことに矛盾する。従って、直線 $\{a_0 + \beta a_1\}$ と $\{a_0 + \beta a_2\}$ は唯一の点を共有し、共に a_0 を通過する。

以下では、このような場合、直線 $\{a_0 + \beta a_1\}$ と直線 $\{a_0 + \beta a_2\}$ は点 a_0 で交わるという。これは、ユークリッド幾何学における y 切片が等しい直線が y 軸上の一点で交わることに対応している。

$EG(m, 2^s)$ の点 a_0 が与えられたとき、 a_0 で交わる直線の数、

$$\frac{2^{ms} - 1}{2^s - 1}$$

個ある。この性質は後によく用いる。

性質 3 (2 点を通る直線) $EG(m, 2^s)$ 上の 2 点 a_1 と a_2 が与えられたとする。これらの 2 点が線形従属であるならば、 $a_2 = \beta a_1$ となる元 $\beta \in F_{2^s}$ が存在し、2 点 a_1, a_2 は直線 $\{\beta a_1\}$ で結ばれている。他方、2 点 a_1 と a_2 が線形独立であるならば、 $a_3 = a_1 + a_2$ とすることで、2 点 a_1, a_2 は直線 $\{a_1 + \beta a_3\}$ で結ばれている。これから、 $EG(m, 2^s)$ における直線の総数は、

$$\frac{2^{(m-1)s}(2^{ms} - 1)}{2^s - 1}$$

になる。

例 1 $m = 3, s = 1$ として得られる有限ユークリッド幾何 $EG(3, 2)$ を考えよう。 $EG(3, 2)$ の点は $2^3 = 8$ 個ある。また、直線は

$$\frac{2^{(3-1) \cdot 1}(2^{3 \cdot 1} - 1)}{2^1 - 1} = 4 \times 7 = 28$$

個ある。点と線を次の表にまとめておく。

EG(3,2) の点			
$a_0 = (000)$	$a_1 = (001)$	$a_2 = (010)$	$a_3 = (011)$
$a_4 = (100)$	$a_5 = (101)$	$a_6 = (110)$	$a_7 = (111)$
EG(3,2) の直線			
$\{a_0, a_1\}$	$\{a_1, a_2\}$	$\{a_2, a_4\}$	$\{a_3, a_7\}$
$\{a_0, a_2\}$	$\{a_1, a_3\}$	$\{a_2, a_5\}$	$\{a_4, a_5\}$
$\{a_0, a_3\}$	$\{a_1, a_4\}$	$\{a_2, a_6\}$	$\{a_4, a_6\}$
$\{a_0, a_4\}$	$\{a_1, a_5\}$	$\{a_2, a_7\}$	$\{a_4, a_7\}$
$\{a_0, a_5\}$	$\{a_1, a_6\}$	$\{a_3, a_4\}$	$\{a_5, a_6\}$
$\{a_0, a_6\}$	$\{a_1, a_7\}$	$\{a_3, a_5\}$	$\{a_5, a_7\}$
$\{a_0, a_7\}$	$\{a_2, a_3\}$	$\{a_3, a_6\}$	$\{a_6, a_7\}$

1.2 平面と μ -フラット

有限ユークリッド幾何 $\text{EG}(m, 2^s)$ の直線概念を平面まで拡張しよう。 $\text{EG}(m, 2^s)$ において、 $a_0, a_1, \dots, a_\mu$ を $\mu + 1$ 個の線形独立な点とする。但し、 $\mu < m$ とする。このとき、 $2^{\mu s}$ 個の点の集合

$$\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu\} \triangleq \{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu : \beta_i \in F_{2^s}, 1 \leq i \leq \mu\}$$

を μ -フラットあるいは、 μ 次元の超平面と呼ぶ。明らかに、 μ -フラット

$$\{\beta_1 a_1 + \dots + \beta_\mu a_\mu\}$$

は、原点を含む $2^{\mu s}$ 個の点を有する。直線のとときと同様に、2つの μ -フラット $\{\beta_1 a_1 + \dots + \beta_\mu a_\mu\}$ と $\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu\}$ は共通の点をもたず、平行であると呼ばれる。 $\text{EG}(m, 2^s)$ で原点を通る任意の μ -フラットは、それに平行な $2^{(m-\mu)s} - 1$ 個の μ -フラットを持ち、これらの平行な $2^{(m-\mu)s}$ 個の μ -フラットは平行束をなす。

$a_{\mu+1}$ が μ -フラット $\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu\}$ の点でないとき、 $(\mu + 1)$ フラット

$$\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu + \beta_{\mu+1} a_{\mu+1}\}$$

は μ -フラット $\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu\}$ を含んでいる。いま、 $b_{\mu+1}$ を $\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu + \beta_{\mu+1} a_{\mu+1}\}$ に含まれていない点とする。このとき、2つの $(\mu + 1)$ -フラット

$$\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu + \beta_{\mu+1} a_{\mu+1}\}, \quad \{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu + \beta_{\mu+1} b_{\mu+1}\}$$

は、 μ -フラット $\{a_0 + \beta_1 a_1 + \dots + \beta_\mu a_\mu\}$ で交わる (すなわち、これらの点を共有する) という。

$\text{EG}(m, 2^s)$ において、 μ -フラット F が与えられたとき、 F と交わる $(\mu + 1)$ -フラットの数は、

$$\frac{2^{(m-\mu)s} - 1}{2^s - 1}$$

である。更に、 μ -フラット F に含まれない点は、 F と交わるただ一つの $(\mu + 1)$ -フラットに含まれる。このことは、通常のユークリッド幾何における、直線と直線の外の点を含むただ一つの平面が存在することに対応している。最後に、 $\text{EG}(m, 2^s)$ の μ -フラットの個数は、

$$2^{(m-\mu)s} \prod_{i=1}^{\mu} \frac{2^{(m-i+1)s} - 1}{2^{(\mu-i+1)s} - 1}$$

である。

例 2 例 1 の有限ユークリッド幾何 $\text{EG}(3, 2)$ を考えよう。 $m = 3, s = 1$ なので、 $\text{EG}(3, 2)$ の 2-フラットは

$$2^{(3-2)1} \frac{2^{(3-1+1)1} - 1}{2^{(2-1+1)1} - 1} \cdot \frac{2^{(3-2+1)1} - 1}{2^{(2-2+1)1} - 1} = 2 \times \frac{8-1}{4-1} \times \frac{4-1}{1} = 14$$

個あり、それらを次の表に示す。直線 $\{a_1, a_3\}$ と交わる 2-フラットは、 $\{a_0, a_1, a_2, a_3\}, \{a_1, a_3, a_5, a_7\}, \{a_1, a_3, a_4, a_6\}$ の 3 つであり、2-フラット $\{a_0, a_1, a_2, a_3\}$ と $\{a_4, a_5, a_6, a_7\}$ は平行である。

$\text{EG}(3, 2)$ の 2-フラット			
$\{a_0, a_1, a_2, a_3\}$	$\{a_4, a_5, a_6, a_7\}$	$\{a_0, a_1, a_4, a_5\}$	$\{a_2, a_3, a_6, a_7\}$
$\{a_0, a_2, a_4, a_6\}$	$\{a_1, a_3, a_5, a_7\}$	$\{a_0, a_1, a_6, a_7\}$	$\{a_2, a_3, a_4, a_5\}$
$\{a_0, a_2, a_5, a_7\}$	$\{a_1, a_3, a_4, a_6\}$	$\{a_0, a_4, a_3, a_7\}$	$\{a_1, a_2, a_5, a_6\}$
$\{a_0, a_3, a_5, a_6\}$	$\{a_1, a_2, a_4, a_7\}$		

1.3 拡大体を用いた点の表示

拡大体 $F_{2^{ms}}$ を用いて、有限ユークリッド幾何 $EG(m, 2^s)$ を表現することを考えよう。 α を $F_{2^{ms}}$ の原始元とする。このとき、 2^{ms} 個の $F_{2^{ms}}$ の元は、 α のべきで次のように表される。

$$\alpha^\infty = 0, \alpha^0 = 1, \alpha^1, \alpha^2, \dots, \alpha^{2^{ms}-2} \quad (\alpha^\infty = 0 \text{ は形式的})$$

$F_{2^{ms}}$ は F_{2^s} を部分体として含んでいるので、任意の元 $\alpha^i \in F_{2^{ms}}$ は、

$$\alpha^i = a_{i0} + a_{i1}\alpha + a_{i2}\alpha^2 + \dots + a_{i,m-1}\alpha^{m-1}$$

と書くことができる。但し、 $a_{ij} \in F_{2^s}, 0 \leq j < m$ である。

この式から、 $\alpha^i \in F_{2^{ms}}$ と F_{2^s} 上の m 次元ベクトル $(a_{i0}, a_{i1}, \dots, a_{i,m-1}) \in F_{2^s}^m$ の間には一対一対応が存在することが分かる。そこで、 $F_{2^{ms}}$ の 2^{ms} 個の元を $EG(m, 2^s)$ の 2^{ms} 個の点とみなすことができ、 $F_{2^{ms}}$ を $EG(m, 2^s)$ と同一視することができる。この場合、点 α^{ℓ_0} を通る μ -フラットは、次のような $2^{\mu s}$ 点を含んでいる

$$\alpha^{\ell_0} + \beta_1 \alpha^{\ell_1} + \dots + \beta_\mu \alpha^{\ell_\mu}$$

但し、 $\alpha^{\ell_0}, \alpha^{\ell_1}, \dots, \alpha^{\ell_\mu}$ は $F_{2^{ms}}$ における $\mu + 1$ 個の線形独立な元であり、 $\beta_i \in F_{2^s}$ である。

例 3 有限体 F_{2^4} を考えよう。この体は、 F_{2^2} を部分体として含むので、全ての元は下記の表のように $a_{i0} + a_{i1}\alpha$ の形で記述される。但し、 $\beta = \alpha^5$ とし、 $F_{2^2} = \{0, 1, \beta, \beta^2\}$ としている。

α^i	(a_{i0}, a_{i1})
$0=0$	$(0,0)$
$1=1$	$(1,0)$
$\alpha = \alpha$	$(0,1)$
$\alpha^2 = \beta + \alpha$	$(\beta, 1)$
$\alpha^3 = \beta + \beta^2\alpha$	(β, β^2)
$\alpha^4 = 1 + \alpha$	$(1, 1)$
$\alpha^5 = \beta$	$(\beta, 0)$
$\alpha^6 = \beta\alpha$	$(0, \beta)$
$\alpha^7 = \beta^2 + \beta\alpha$	(β^2, β)
$\alpha^8 = \beta^2 + \alpha$	$(\beta^2, 1)$
$\alpha^9 = \beta + \beta\alpha$	(β, β)
$\alpha^{10} = \beta^2$	$(\beta^2, 0)$
$\alpha^{11} = \beta^2\alpha$	$(0, \beta^2)$
$\alpha^{12} = 1 + \beta^2\alpha$	$(1, \beta^2)$
$\alpha^{13} = 1 + \beta\alpha$	$(1, \beta)$
$\alpha^{14} = \beta^2 + \beta^2\alpha$	(β^2, β^2)

F_{2^4} を $EG(2, 2^2)$ とみなすことで、例えば、

$$\alpha^{14} + 0 \cdot \alpha = \alpha^{14}, \alpha^{14} + 1 \cdot \alpha = \alpha^7, \alpha^{14} + \beta \cdot \alpha = \alpha^8, \alpha^{14} + \beta^2 \cdot \alpha = \alpha^{10}$$

は点 α^{14} を通る直線である。点 α^{14} を通る他の 4 つの直線は、

$$\{\alpha^{14}, \alpha^{13}, \alpha, \alpha^5\}, \quad \{\alpha^{14}, \alpha^0, \alpha^6, \alpha^2\}, \quad \{\alpha^{14}, \alpha^9, \alpha^4, 0\}, \quad \{\alpha^{14}, \alpha^{12}, \alpha^{11}, \alpha^3\}$$

である。

2 EG 符号の構成法

いま、

$$v = (v_0, v_1, \dots, v_{2^{ms}-2})$$

を F_2 上の $(2^{ms} - 1)$ 次元のベクトルとする。ここで、 i 番目の要素 v_i と $F_{2^{ms}}$ の非零元 α^i とが対応しているとし、 α^i を v_i の location number という。このとき、 F を $\text{EG}(m, 2^s)$ の μ -フラットとすると、 F^2 上のベクトル

$$v_F = (v_0, v_1, \dots, v_{2^{ms}-2})$$

を次のようにして定める。

$$v_i = \begin{cases} 1 & \alpha^i \text{が } F \text{ の点} \\ 0 & \text{elsewhere} \end{cases}$$

すなわち、 v_F の非零要素の location number が μ -フラット F の点になっている。ベクトル v_F を μ -フラット F の生成ベクトル (incidence vector) と呼ぶ。

生成ベクトルの重要な性質の一つとして、 $\text{EG}(m, 2^s)$ の原点を通らない μ -フラットの生成ベクトルを巡回シフトして得られるベクトルは原点を通らない他の μ -フラットの生成ベクトルになっていることが知られている。

例 4 $m = 2, s = 2$ として、 $\text{EG}(2, 2^2)$ の有限体 F_{2^4} による表示を考えよう。例 3 から、 α^{14} を通る 1-フラット (直線) で、原点を通らないものは、

$$L_1 = \{\alpha^{14}, \alpha^7, \alpha^8, \alpha^{10}\}, L_2 = \{\alpha^{14}, \alpha^{13}, \alpha, \alpha^5\}, L_3 = \{\alpha^{14}, \alpha^0, \alpha^6, \alpha^2\}, L_4 = \{\alpha^{14}, \alpha^{12}, \alpha^{11}, \alpha^3\}$$

の 4 個である。従って、これらの 1-フラットの生成ベクトルは、

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	)
$v_{L_1} =$	0	0	0	0	0	0	0	1	1	0	1	0	0	0	1	)
$v_{L_2} =$	0	1	0	0	0	1	0	0	0	0	0	0	0	1	1	)
$v_{L_3} =$	1	0	1	0	0	0	1	0	0	0	0	0	0	0	1	)
$v_{L_4} =$	0	0	0	1	0	0	0	0	0	0	0	1	1	0	1	)

となる。例えば、直線 L_2 の生成ベクトル v_{L_2} を右に巡回シフトすると、ベクトル

$$(1010001000000001)$$

が得られ、これは、直線 $\{\alpha^0, \alpha^2, \alpha^6, \alpha^{14}\}$ を意味する。他方、もし直線 L_1 の生成ベクトル v_{L_1} を巡回シフトすると、ベクトル

$$(100000001101000)$$

が得られ、これは直線 $\{\alpha^0, \alpha^8, \alpha^9, \alpha^{11}\}$ に対応している。

定義 1 符号長 $2^{ms} - 1$ の (μ, s) 次 2 元ユークリッド幾何 (EG) 符号は、 $\text{EG}(m, 2^s)$ の原点を通らない全ての $\mu + 1$ -フラットの生成ベクトルを基底とする符号に直交する最大次元の巡回符号である。

この定義から、符号長 $2^{ms} - 1$ の (μ, s) 次 EG 符号は、 $\text{EG}(m, 2^s)$ の原点を通らない全ての $(\mu + 1)$ -フラットの生成ベクトルを基底とするの線形符号の双対符号である。 $\text{EG}(m, 2^s)$ の原点を通らないフラットの生成ベクトルの巡回シフトは他の原点を通らないフラットの生成ベクトルになること

から、 $(\mu+1)$ -フラットの生成ベクトルを基底とする線形符号は巡回符号である。従って、その双対符号もまた巡回符号である。

以下では、この (μ, s) 次 EG 符号の生成多項式を求めよう。この符号の生成多項式を $F_{2^{ms}}$ に含まれる根を用いて表現することを考えよう。まず、 h によって 2^{ms} 未満の正の整数を表す。このとき、 h を 2^s 進法によって次のように表す。

$$h = \delta_0 + \delta_1 2^s + \delta_2 2^{2s} + \cdots + \delta_{m-1} 2^{(m-1)s}$$

但し、 $0 \leq \delta_i < 2^s$, $0 \leq i < m$ である。このとき、 2^s -重み $W_{2^s}(h)$ を

$$W_{2^s}(h) = \sum_{i=0}^{m-1} \delta_i \quad (\text{演算は通常の整数演算})$$

によって定義する。例えば、 $m=3, s=2$ としたとき、 $h=45$ は、

$$45 = 1 + 3 \cdot 2^2 + 2 \cdot 2^4$$

であり、 $\delta_0 = 1, \delta_1 = 3, \delta_2 = 2$ である。従って、 2^2 -重みは、

$$W_{2^2}(45) = 1 + 3 + 2 = 6$$

となる。

ここで、 $h - W_{2^s}(h)$ を考えると、

$$h - W_{2^s}(h) = \delta_1(2^s - 1) + \delta_2(2^{2s} - 1) + \cdots + \delta_{m-1}(2^{(m-1)s} - 1)$$

が成り立つ。従って、 2^s -重み $W_{2^s}(h)$ が $2^s - 1$ で割り切れるときに限り、 h が $2^s - 1$ で割り切れる。そこで、 $h^{(\ell)}$ によって、 $2^\ell h$ を $2^{ms} - 1$ で割った余り、すなわち

$$2^\ell h = q(2^{ms} - 1) + h^{(\ell)}, \quad 0 \leq h^{(\ell)} < 2^{ms} - 1$$

によって定める。明らかに h が $2^s - 1$ で割り切れるときに限り、 $h^{(\ell)}$ は $2^s - 1$ で割り切れる。特に、 $h^{(0)} = h$ であることに注意しておく。このとき、 (μ, s) 次 EG 符号の生成多項式を特徴付ける次の定理が成り立つ。

定理 1 α によって $F_{2^{ms}}$ の原始元を表す。 (μ, s) 次 EG 符号の生成多項式 $g(x)$ は、 h を $2^{ms} - 1$ 以下の正の整数とするとき、条件

$$0 < \max_{0 \leq \ell < s} W_{2^s}(h^{(\ell)}) \leq (m - \mu - 1)(2^s - 1)$$

を満足するときに限り、 α^h を根として持つ。

定理の証明は省略する。証明が読みたい者は、例えば、

T. Kasami, S. Lin, and W. W. Peterson, "Polynomial codes," *IEEE Trans. on Information Theory*, vol.14, pp.807-814, 1968.

T. Kasami and S. Lin, "On majority-logic decoding for duals of primitive polynomial codes," *IEEE Trans. on Information Theory*, vol.17, no.3, pp.322-331, 1971.

などを参照されたい。(著者の一人の嵩先生は大阪大学の名誉教授であり、我が国の符号理論の先駆者であり、日本人で唯一のシャノン賞受賞者であられたが、今年亡くなられた。)

例 5 $m = 2, s = 2, \mu = 0$ として、有限体 F_{2^4} を有限ユークリッド幾何 $EG(2, 2^2)$ と見なす。 α を F_{2^4} の原始元とする。 h を 15 以下の正の整数とする。定理 1 から $(0, 2)$ 次 EG 符号の生成多項式は、

$$0 < \max_{0 \leq \ell < 2} W_{2^2}(h^{(\ell)}) \leq 3$$

を満足するときに限り α^h を根として持つ。この条件を満足する h を求めると、

$$h = 1, 2, 3, 4, 6, 8, 9, 12$$

が得られる。従って、 $g(x)$ は $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}$ を根として持つ。ここで、元 $\alpha, \alpha^2, \alpha^4, \alpha^8$ は同一の最小多項式 $x^4 + x + 1$ を持ち、元 $\alpha^4, \alpha^6, \alpha^{12}, \alpha^9$ は同一の最小多項式 $x^4 + x^3 + x^2 + x + 1$ を持つ、従って、符号長 15 の $(0, 2)$ 次 EG 符号の生成多項式は、

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1$$

が得られる。この結果から、 $(0, 2)$ 次 EG 符号は $(15, 7)$ BCH 符号と一致することが分る。

例 6 $m = 3, s = 2, \mu = 1$ とし、 F_{2^6} を $EG(3, 2^2)$ と見なす。 α を F_{2^6} の原始元とし、 h を 63 未満の正整数とする。定理 1 から符号長 63 の $(1, 2)$ 次 EG 符号の生成多項式 $g(x)$ は、

$$0 < \max_{0 \leq \ell < 2} W_{2^2}(h^{(\ell)}) \leq 3$$

を満足するときに限り、 α^h を根として持つ。この条件を満足する h は、

$$h = 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 32, 33, 48$$

であり、 $g(x)$ は根として、

$$\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}, \alpha^{16}, \alpha^{18}, \alpha^{24}, \alpha^{32}, \alpha^{33}, \alpha^{48}$$

を持つ。ここで、 $\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$ の最小多項式は $x^6 + x + 1$ であり、 $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{33}$ の最小多項式は $x^6 + x^4 + x^2 + x + 1$ であり、 $\alpha^9, \alpha^{18}, \alpha^{36}$ の最小多項式は $x^3 + x^2 + 1$ である。従って、符号長 63 の $(1, 2)$ 次 EG 符号の生成多項式は、

$$\begin{aligned} g(x) &= (x^6 + x + 1)(x^6 + x^4 + x^2 + x + 1)(x^3 + x^2 + 1) \\ &= x^{15} + x^{14} + x^{13} + x^{11} + x^4 + x^2 + 1 \end{aligned}$$

である。従って、 $(1, 2)$ 次 EG 符号は、 $(63, 48)$ 巡回符号である。

演習問題 $m = 3, s = 1$ とした $EG(3, 2)$ を考えよう。 $\mu = 1$ として得られる $(1, 1)$ 次 EG 符号の符号長ならびに生成多項式 $g(x)$ を求めよ。また、この符号の最小距離はいくつか。