数理解析研究所講究録
第95巻 1970年 12-22

12

Polynomial codeの構造について

愛媛大学 理 浜田昇

§1. 序

前回，有限射影幾何 $PG(t,P^n)$ における点と d-flats からなる incidence matrix N_P や $EG(t,P^n)$ における点と d-flats からなる incidence matrix N_E の $GF(P^n)$ 上での rank を求め，incidence matrix N_P を parity check matrix とする d-th order Projective Geometry code や incidence matrix N_E を parity check matrix とする d-th order Affine Geometry code の構造を明らかにした[3]。

今回は，前回と同様な方法を用いて，これらの geometry codes を特別な場合として含む polynomial code の構造を明らかにする。

§2. Polynomial codeの定義とその構造

$X_1, X_2, \cdots, X_m$ を $GF(q^\Delta)$ 上の値を取る m 個の変数とし，次の2条件をみたす $X_1, X_2, \cdots, X_m$ の多項式：

$$f(X_1, X_2, \cdots, X_m) = \sum_{\nu_1, \cdots, \nu_m} c_{\nu_1 \nu_2 \cdots \nu_m} X_1^{\nu_1} X_2^{\nu_2} \cdots X_m^{\nu_m} \quad (2.1)$$

の全体を $P(m, \Delta, \mu, b)$ で表わす。 すなわち，

$$P(m, \Delta, \mu, b) = \left\{ f(X_1, X_2, \cdots, X_m) \;\middle|\; \begin{array}{l} (2.1) \text{ のタイプで，(条1)，} \\ (\text{条2}) \text{ をみたすもの} \end{array} \right\}$$

(条件1) 係数 $c_{\nu_1 \nu_2 \cdots \nu_m}$ はすべて $GF(q^\Delta)$ の元である。

(条件2) 各項のベキ：$\nu_1, \nu_2, \cdots, \nu_m$ の和はすべて b の倍数で，かつ，μb より大きくならないこと。

i.e., $$\sum_{i=1}^{m} \nu_i = jb \quad (j = 0, 1, \cdots, \mu-1 \text{ or } \mu) \quad (2.2)$$

ここに，μ は非負の与えられた整数で，b は $(q^\Delta - 1)$ の約数である。 以下，

$$Z = (q^\Delta - 1)/b \;, \quad n = (q^{\Delta m} - 1)/b \quad (2.3)$$

とおく。 $X_i^{q^\Delta} = X_i$ $(i = 1, 2, \cdots, m)$ であるから，以下，ν_i $(i = 1, 2, \cdots, m)$，μ は

$$0 \leqq \nu_i \leqq q^\Delta - 1 \;, \quad 0 \leqq \mu < mZ \quad (2.4)$$

をみたす整数とする。

$P(m, \Delta, \mu, b)$ に属する多項式 $f(X_1, X_2, \cdots, X_m)$ (以下, $f(\bar{X})$ と略記する) に対して, $GF(q^\Delta)$ の元を要素とする n 次元ベクトル空間 $W(n; q^\Delta)$ のベクトル $\underline{v} = (v_0, v_1, \cdots, v_{n-1})$ を次のように対応させる。

$$\sigma : f(\bar{X}) \in P(m, \Delta, \mu, b) \longrightarrow \underline{v} \in W(n; q^\Delta) \quad (2.5)$$

ここに, $\underline{v} = (v_0, v_1, \cdots, v_{n-1})$ の j 番目の要素 v_j は

$$v_j = f(a_{1j}, a_{2j}, \cdots, a_{mj}) \quad (j = 0, 1, \cdots, n-1) \quad (2.6)$$

で与えられ, $(a_{1j}, a_{2j}, \cdots, a_{mj})$ は, α を $GF(q^{\Delta m})$ の原始元とする時, $GF(q^{\Delta m})$ の元 α^j $(j = 0, 1, \cdots, n-1)$ の座標表現である。 すなわち, α^j を $\alpha^0, \alpha^1, \cdots, \alpha^{m-1}$ で表わした時の係数文,

$$\alpha^j = \sum_{i=1}^{m} a_{ij}\, \alpha^{i-1} \quad (j = 0, 1, \cdots, n-1) \quad (2.7)$$

である。 (もちろん, $a_{1j}, a_{2j}, \cdots, a_{mj}$ は $GF(q^\Delta)$ の元である。)

σ による $f(\bar{X})$ の像を $\underline{v}(f)$ で表わし,

$$W_0 = \left\{ \underline{v}(f) \;\middle|\; f(\bar{X}) \in P(m, \Delta, \mu, b) \right\} \quad (2.8)$$

とおくと, σ は $P(m, \Delta, \mu, b)$ から W_0 の上への1対1対応

である。

特に，$W(n;q^s)$ではなくて，$W(n;q)$のベクトルに対応する$P(m,s,\mu,b)$の多項式$f(\bar{x})$の全体を$Q(m,s,\mu,b,q)$で表わす。すなわち，

$$Q(m,s,\mu,b,q)=\left\{ f(\bar{x})\in P(m,s,\mu,b) \;\middle|\; \begin{array}{l} f(a_{1j},\cdots,a_{mj})\in GF(q) \\ \text{for } j=0,1,\cdots,n-1 \end{array} \right\}$$

とする。

$$V_0=\{\, \underline{v}(f) \mid f(\bar{x})\in Q(m,s,\mu,b,q)\,\} \qquad (2.9)$$

とおくと，V_0は$W(n;q)$のベクトル部分空間を作る。

（定義）$W(n;q)$のベクトルのうちで，V_0に属するベクトル$\underline{v}(f)$だけを符号とする線形符号（linear code）のことを(n,m,s,μ,q)-多項式符号（polynomial code）という。

これについては，嵩，Shu Lin，Peterson [1] による次の定理が成り立つ。

（定理 2.1）(a) (n,m,s,μ,q)-多項式符号はcyclic codeである。

(b) αを$GF(q^{sm})$の原始元とすれば，(n,m,s,μ,q)-

多項式符号を生成する生成多項式 $g(x)$ の根は，α^h のタイプのものに限る。　ここに，h は $0 \leqq h < q^{sm}-1$ なる整数である。

(c)　α^h $(0 \leqq h < q^{sm}-1)$ が (n, m, s, μ, q)-多項式符号の生成多項式 $g(x)$ の根であるための必要かつ十分条件は h が次の2条件をみたす整数であることである。

(条件1)　h は b の倍数であること。

(条件2)　h は s 個の整数値 $W_{q^s}(h)$, $W_{q^s}(hq)$, $\cdots$, $W_{q^s}(hq^{s-1})$ のうちの最小値が b の倍数で，かつ，0より大きく，$(mz-\mu)b$ より小さくなるような整数であること。i.e., h は

$$\min_{0 \leqq l < s} W_{q^s}(hq^l) = jb \quad (\text{但し}, 0 < j < mz-\mu) \qquad (2.10)$$

をみたす整数 j が存在するような整数であること。

ここに，$W_{q^s}(H)$ は，(イ)　$0 \leqq H < q^{sm}-1$ なる整数 H に対しては，H の q^s 進数表示を

$$H = \delta_1 + \delta_2 q^s + \cdots + \delta_m q^{(m-1)s} \quad (0 \leqq \delta_i < q^s)$$

とするとき，

$$W_{q^s}(H) = \delta_1 + \delta_2 + \cdots + \delta_m \qquad (2.11)$$

を意味し，(ロ)　$H \geqq q^{sm}-1$ なる整数 H に対しては，H を $(q^{sm}-1)$ で割った時の余りを H_0 とするとき，$W_{q^s}(H) = W_{q^s}(H_0)$

を意味する。

(系 2.1) (a) (n, m, s, μ, q)-多項式符号の dual code も cyclic code である。

(b) α^h $(0 \leqq h < q^{sm}-1)$ が (n, m, s, μ, q)-多項式符号の生成多項式 $g_0(x)$ の根であるための必要かつ十分条件は, h が次の条件をみたす整数であることである。

(条件1) h は b の倍数であること.

(条件2) h は

$$\max_{0 \leqq l < s} W_{q^s}(hq^l) = jb \quad (0 \leqq j \leqq \mu) \qquad (2.12)$$

をみたす整数 j が存在するような整数であること.

この note の目的は, これらの定理と前回の方法を用いて, (n, m, s, μ, q)-多項式符号の information symbol の数を求めることである。

まず, 次の補題が成り立つ。 (詳しくは論文[2]参照)

(補題 2.1) h を $0 \leqq h < q^{sm}-1$ なる整数とし, h の q 進表示を

$$h = \sum_{i=0}^{m-1} \sum_{j=0}^{s-1} c_{ij} q^{is+j} \qquad (0 \leqq c_{ij} < q) \quad (2.13)$$

とする。　このとき，h が b の倍数，すなわち，$(q^{\Delta}-1)/Z$ の倍数であるならば，次の条件をみたす整数の組 $(f_0, f_1, \cdots, f_{\Delta})$ がただ一組存在する。 i.e., $j = 0, 1, \cdots, \Delta-1$ に対して，

$$\text{(条件)} \quad \begin{cases} f_{\Delta} = f_0, \quad 0 \leqq f_j < mZ & (2.14) \\ Z \sum_{i=0}^{m-1} c_{ij} = f_{j+1} q - f_j & (2.14') \end{cases}$$

をみたす整数の組 $(f_0, f_1, \cdots, f_{\Delta})$ がただ一組存在する。

c_{ij} は $0 \leqq c_{ij} \leqq q-1$ なる整数であるから，(2.14′) は $(f_{j+1} q - f_j)/Z$ $(j = 0, 1, \cdots, \Delta-1)$ が

$$0 \leqq (f_{j+1} q - f_j)/Z \leqq m(q-1) \qquad (2.15)$$

をみたす整数であることを示す。

(補題 2.2)　逆に，$(f_0, f_1, \cdots, f_{\Delta})$ を次の条件：

$$\text{(条件)} \quad \begin{cases} f_{\Delta} = f_0, \quad 0 \leqq f_j < mZ \\ (f_{j+1} q - f_j)/Z \text{ は整数，かつ，} \\ 0 \leqq (f_{j+1} q - f_j)/Z \leqq m(q-1) \end{cases} \qquad (2.16)$$

$(j = 0, 1, \cdots, \Delta-1)$ をみたす整数の組とすると，

(i)　$0 \leqq c_{ij} < q$　$(i = 0, 1, \cdots, m-1,\ j = 0, 1, \cdots, \Delta-1)$ で，かつ，

$$\sum_{i=0}^{m-1} c_{ij} = (f_{j+1} q - f_j)/Z \qquad (2.17)$$

$(j = 0, 1, \cdots, s-1)$ をみたす整数の組 $\{c_{ij}\}$ が少なくとも一組存在する。

(ii) (2.17) をみたす任意の整数の組 $\{c_{ij}\}$ に対して,

$$h = \sum_{i=0}^{m-1} \sum_{j=0}^{s-1} c_{ij} q^{is+j} \qquad (2.18)$$

とおくと, h は b の倍数で, かつ, $0 \leq h < q^{sm} - 1$ なる整数である。

(iii) このとき, $l = 0, 1, \cdots, s-1$ に対して,

$$W_{q^s}(h q^l) = \rho_{s-l} b \qquad (2.19)$$

が成り立つ。

従って, 定理 2.1 の条件は

$$0 < \min(\rho_1, \rho_2, \cdots, \rho_s) < mz - \mu \qquad (2.20)$$

を意味する。 従って, 次の定理が成り立つ。

(定理 2.2) $(\rho_0, \rho_1, \cdots, \rho_s)$ を (2.16) と (2.20) の条件をみたす任意の整数の組とする。 このとき, $\{c_{ij} : i = 0, 1, \cdots, m-1, j = 0, 1, \cdots, s-1\}$ を (2.17) をみたす任意の整数の組とし, (2.18) で h を定義すると, α^h は (n, m, s, μ, q)-多項式符号の生成多項式 $g(x)$ の根である。 逆に,

$g(x)$ の根は上のタイプのものに限る。

$$0 \leqq \max\{\rho_1, \rho_2, \cdots, \rho_\delta\} \leqq \mu \qquad (2.21)$$

とおくと，(系 2.1) より，次の系が成り立つ。

(系 2.2) $(\rho_0, \rho_1, \cdots, \rho_\delta)$ を (2.16) と (2.21) の条件をみたす任意の整数の組とする。このとき，$\{c_{ij}\}$ を (2.17) をみたす任意の整数の組とし，(2.18) で h を定義すると，α^h は (n, m, δ, μ, q)-多項式符号の dual code の生成多項式 $g_D(x)$ の根である。逆に，$g_D(x)$ の根は上のタイプのものに限る。

一般に，cyclic な linear code の information symbol の数はその dual code を生成する生成多項式の根の数に等しい。

従って，(n, m, δ, μ, q)-多項式符号の information symbol の数は (n, m, δ, μ, q)-多項式符号の dual code を生成する生成多項式 $g_D(x)$ の根の数に等しい。以下，$g_D(x)$ の根の数を求める。

条件 (2.16) と (2.21) は合せて次のようにかける。

$$\text{(条件)} \begin{cases} \rho_\delta = \rho_0, \quad 0 \leqq \rho_j \leqq \mu \\ (\rho_{j+1} q - \rho_j)/n \text{ は整数，かつ，} \\ 0 \leqq (\rho_{j+1} q - \rho_j)/n \leqq m(q-1) \end{cases} \qquad (2.22)$$

前回と同様な方法（[2], [3] 参照）を用いて，系 2.2 より次の結果をうる。

（定理 2.3） (n, m, s, μ, q)-多項式符号の information symbol の数は次式によって与えられる。

$$\sum_{\rho_0} \cdots \sum_{\rho_{s-1}} \prod_{j=0}^{s-1} \sum_{i=0}^{L(\rho_{j+1}, \rho_j)} (-1)^i \binom{m}{i} \binom{m-1+(\rho_{j+1}q-\rho_j)/q - iq}{m-1} \quad (2.23)$$

ここに，$\rho_s = \rho_0$ で，$\sum_{\rho_0} \cdots \sum_{\rho_{s-1}}$ は (2.22) の条件をみたすすべての整数の組 $(\rho_0, \rho_1, \cdots, \rho_{s-1})$ にわたる和を表わし，$L(\rho_{j+1}, \rho_j)$ は $(\rho_{j+1}q - \rho_j)/q$ を越えない最大の整数を表わす。

参考文献

[1] Kasami, T., Shu Lin and Peterson, W. W. (1968). Polynomial codes. IEEE Transactions on information theory IT-14 807-814.

[2] Hamada, N. (1968). The rank of the incidence matrix of points and d-flats in finite geometries.

J. Sci. Hiroshima Univ. Ser. A-I 32 381-396.

[3] 浜田昇 (1970). 有限幾何における点とd-flatoからなるincidence matrixのrankとmajority decodable codeについて.

数理解析研究所講究録 82.