数理解析研究所講究録
第82巻 1970年 108-126

有限幾何における点と d-flats からなる incidence matrix の rank と majority decodable code について

愛媛大学 理. 浜田 昇

§1. 序

最近，人工衛星や宇宙船の開発がさかんに行なわれているが，これにともなって，データを伝送する際に生ずる誤りを検出，修正するための誤り訂正符号（error correcting code）の研究，特に，誤りを簡単に検出，修正出来る majority decodable code の研究がさかんに行なわれている。

有限射影幾何 $PG(t, p^n)$ における点と d-flats からなる incidence matrix を parity check matrix とする d-th order Projective Geometry code や $EG(t, p^n)$ における点と d-flats からなる incidence matrix を parity check matrix とする d-th order affine Geometry code のような有限幾何から作られる majority decodable code を作る為めには $PG(t, p^n)$ や $EG(t, p^n)$ における incidence matrix の $GF(p^n)$ 上での rank を求める必要があるが，一般の正整

数n, dに対するrankはまだ求まっていない。 現在知られているのは次の通り。

(1) $n=1$の場合

Smith[4]によって, すべてのt, d ($0<d<t$)に対するrankが求められた。

(2) $n \geqq 2$の場合

(イ) $d=t-1$ (hyperplane)のとき

• $t=2$に対して, Graham と MacWilliams [2] が求めた。

• $t \geqq 2$に対して, Smith[4], 独立に, Goethals と Delsarte[1]が求めた。

(ロ) $1 \leqq d < t-1$のとき

Smith[4] によって, rank の upper bound は求められたが, rank そのものはまだ求められていない。*)

このpaperの目的は任意の素数pと任意の正整数n, t, d ($0<d<t$)に対する$PG(t,p^n)$や$EG(t,p^n)$における点とd-flatsからなるincidence matrixの$GF(p^n)$上でのrank

---

*) この問題はNorth Carolina大学のR.C.Bose教授が広島大学にこられたとき示されたものである。

を求め，d-th order Projective Geometry code や d-th order affine Geometry code を構成することである。

§2. PG(t, P^n) における点と d-flats からなる incidence matrix の rank

$q = p^n$（P は素数，n は正整数とする。t 次元射影幾何 PG(t, q) における $v = (q^{t+1}-1)/(q-1)$ 個の点と

$$b = \phi(t, d, q) = \frac{(q^{t+1}-1)(q^{t}-1)\cdots(q^{t-d+1}-1)}{(q^{d+1}-1)(q^{d}-1)\cdots(q-1)} \quad (2.1)$$

個の d-flats $(0 \leqq d \leqq t)$ にそれぞれ適当に番号をつけ，これら v 個の点と b 個の d-flats からなる incidence matrix を次のように定義する。

$$N = \| n_{ij} \| : i = 1, 2, \cdots b, \; j = 1, 2, \cdots v \quad (2.2)$$

ここに，

$$n_{ij} = \begin{cases} 1, & j \text{ 番目の点が } i \text{ 番目の d-flat にのっているとき,} \\ 0, & \text{そうでないとき。} \end{cases}$$

この incidence matrix N の rank および d-th order Projective Geometry code を生成する generator polynomial を求めるのに次の Smith[4] による Proposition は重要である。

Proposition 1 (i) $PG(t,q)$におけるv個の点とb個のd-flatsからなるincidence matrix Nの$GF(q)$上でのrankは$\{\theta_1(\beta^m), \theta_2(\beta^m), \cdots, \theta_b(\beta^m)\}$の中に$\theta_i(\beta^m) \neq 0$となる$d$-flat Σ_i $(1 \leqq i \leqq b)$が少なくとも一つ存在するような整数m $(1 \leqq m \leqq v)$の数に等しい。ここに、

$$\theta_i(x) = \sum_{j=1}^{v} n_{ij} x^j, \qquad \beta = \alpha^{q-1} \qquad (2.3)$$

(αは$GF(q^{t+1})$の原始元)である。

(ii) $\{\theta_1(\beta^m), \theta_2(\beta^m), \cdots, \theta_b(\beta^m)\}$の中に$\theta_i(\beta^m) \neq 0$となる$d$-flat Σ_iが少なくとも一つ存在するための整数m $(1 \leqq m \leqq v)$に対する必要かつ十分条件は

$$m = \sum_{k=0}^{d} m_k \text{ かつ } D_p[m(q-1)] = \sum_{k=0}^{d} D_p[m_k(q-1)] \quad (2.4)$$

をみたす$d+1$個の正整数m_k $(k=0,1,\cdots,d)$が存在することである。ここに、$D_p[M]$は正整数Mのp進表示が

$$M = c_0 + c_1 p + \cdots + c_u p^u \quad (0 \leqq c_i < p) \qquad (2.5)$$

であるとき、

$$D_p[M] = c_0 + c_1 + \cdots + c_u \qquad (2.6)$$

でもって定義される。

Smithは Proposition 1を用いて、$n=1$の場合のincidence matrix Nのrankおよび、$n \geqq 2$の場合のNのrankのupper boundを求めたが($n \geqq 2$の場合の)Nのrankそ

のものは求めることが出来なかった。　§2の目的は Proposition 1 をさらに進めて，$n \geqq 1$ の場合の N の rank を求めることである。以下，その方法を簡単に記述する。（詳しくは論文[3]を参照）

Proposition 1 から incidence matrix N の rank を求めるためには正整数 m $(1 \leqq m \leqq v)$ に対して，(2.4) をみたす $d+1$ 個の正整数 m_k $(k=0, 1, \cdots d)$ が存在するような m の個数が計算出来ればよい。従って，このような m の個数が簡単に計算出来る方法（必要十分条件）を示せばよい。

［定理 2.1］ m を $1 \leqq m \leqq v$ なる整数とし，$m(q-1)$ の P 進表示を

$$m(q-1) = \sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} P^{in+j} \quad (0 \leqq c_{ij} < P) \qquad (2.7)$$

とする。このとき，この m に対して (2.4) をみたす $d+1$ 個の正整数 m_k $(k=0, 1 \cdots, d)$ が存在するならば，

$$s_n = s_0, \quad d+1 \leqq s_j \leqq t+1 \qquad (2.8)$$

かつ，$\sum_{i=0}^{t} c_{ij} = s_{j+1} P - s_j \quad (j=0, 1, \cdots, n-1) \qquad (2.8)'$

となる $n+1$ 個の正整数 s_l $(l=0, 1, \cdots n)$ が存在し，かつ，各 s_l は m によって一意的に定まる。

（注）　このとき，$0 \leqq c_{ij} \leqq P-1$ であるから，$(2.8)'$ より

$0 \leqq s_{j+1} P - s_j \leqq (t+1)(P-1)$ である。

[定理 2.2] 逆に, s_l ($l = 0, 1, \cdots n$) を

$$s_n = s_0, \quad d+1 \leqq s_j \leqq t+1$$

かつ, $0 \leqq s_{j+1} P - s_j \leqq (t+1)(p-1)$ (2.9)

($j = 0, 1, \cdots, n-1$) なる $n+1$ 個の整数とし, C_{ij} ($i = 0, 1, \cdots, t$, $j = 0, 1, \cdots, n-1$) を (2.8)′をみたす任意の整数(但し $0 \leqq C_{ij} < P$) とすると,

(i) $\sum_{i=0}^{t}\sum_{j=0}^{n-1} C_{ij} P^{in+j}$ は $P^n - 1$ の倍数である。 すなわち,

$$\sum_{i=0}^{t}\sum_{j=0}^{n-1} C_{ij} P^{in+j} = m\,(P^n - 1) \qquad (2.10)$$

となる正整数 m ($1 \leqq m \leqq v$) が存在する。

(ii) この m に対して, (2.4) を満足する $d+1$ 個の正整数 m_k ($k = 0, 1, \cdots d$) が存在する。

定理 2.1 は (2.4) をみたす整数 m に対して, (2.8), (2.8)′ をみたす整数 s_l ($l = 0, 1, \cdots, n$) が一意的に定まることを示す。逆に, 定理 2.2 は (2.8), (2.9) をみたす任意の整数 s_l ($l = 0, 1, \cdots, n$) に対して, (2.8)′をみたす整数 C_{ij} ($0 \leqq C_{ij} < P$) の ordered set $\{C_{ij} ; i = 0, 1, \cdots, t, j = 0, 1, \cdots, n-1\}$ がいくつか存在し, その ordered set $\{C_{ij}\}$ によって定まる m

は(2.4)をみたすことを示す。 従って，次の定理を得る

〔定理 2.3〕(2.4)のように $d+1$ 個の正整数 m_k ($k=0,1,\cdots,d$) に分解可能な整数 m ($1 \leqq m \leqq v$) の個数は，

$$\sum_{s_0=d+1}^{t+1}\cdots\sum_{s_{n-1}=d+1}^{t+1} N_t(s_1P-s_0,\cdots,s_nP-s_{n-1}) \qquad (2.11)$$

($s_n=s_0$) である。 ここに，$N_t(u_0,u_1,\cdots u_{n-1})$ は正整数 u_j ($j=0,1,\cdots,n-1$) に対して，$\sum_{i=0}^{t} c_{ij}=u_j$ を満足する整数 c_{ij} ($0 \leqq c_{ij} < P$) の ordered set $\{c_{ij}: i=0,1,\cdots,t,\ \ j=0,1,\cdots,n-1\}$ の個数を表わす。

$0 \leqq u \leqq (t+1)(P-1)$ なる整数 u に対して，

$$0 \leqq x_i \leqq P-1 \text{ かつ } \sum_{i=0}^{t} x_i = u \qquad (2.12)$$

をみたす $t+1$ 個の整数 x_i からなる ordered set $(x_0,x_1,\cdots,x_t)$ の個数を $B_u(t,P)$ で表わすと，$B_u(t,P)$ は

$$B_u(t,P)=\sum_{i=0}^{L(u)}(-1)^i\binom{t+1}{i}\binom{t+u-iP}{t} \qquad (2.13)$$

で与えられる。 ここに，$L(u)=\left[\frac{u}{P}\right]$ である。

一方，$N_t(u_0,u_1,\cdots u_{n-1})$ の定義より

$$N_t(u_0,u_1,\cdots u_{n-1}) = \prod_{j=0}^{n-1} B_{u_j}(t,P) \qquad (2.14)$$

である。

以上のことをまとめて，次の結論をうる。

［定理 2.4］ $PG(t,p^n)$ における点と d-flats からなる incidence matrix N の $GF(p^n)$ 上での rank を $R_d(t,p^n)$ で表わすと，$R_d(t,p^n)$ は

$$R_d(t,p^n)=\sum_{s_0}\cdots\sum_{s_{n-1}}\prod_{j=0}^{n-1}\sum_{i=0}^{L(s_{j+1},s_j)}(-1)^i\binom{t+1}{i}\binom{t+s_{j+1}p-s_j-ip}{t} \tag{2.15}$$

によって与えられる。 ここに，$s_n=s_0$ で $\sum_{s_0}\cdots\sum_{s_{n-1}}$ は

$$d+1\leqq s_j\leqq t+1 \quad \text{かつ} \quad 0\leqq s_{j+1}p-s_j\leqq(t+1)(p-1) \tag{2.16}$$

なるすべての整数 s_j（$j=0,1,\cdots,n-1$）に対する和を表わす。

［系 2.1］ 特に，$q=p$ すなわち，$n=1$ の場合には，

$$\begin{aligned}R_d(t,p)&=\sum_{s=d+1}^{t+1}\sum_{i=0}^{L(s,s)}(-1)^i\binom{t+1}{i}\binom{t+s(p-1)-ip}{t}\\&=v-\sum_{s=1}^{d}\sum_{i=0}^{L(s,s)}(-1)^i\binom{t+1}{i}\binom{t+s(p-1)-ip}{t}\end{aligned} \tag{2.17}$$

である。 ここに，$L(s,s)=\left[\dfrac{s(p-1)}{p}\right]$

これは Smith[4] によって得られた結果と一致する。

[系 2.2]　特に，$d=t-1$ の場合には

$$R_{t-1}(t, p^n) = \binom{t+p-1}{t}^n + 1 \qquad (2.18)$$

である。

これは，$t=2$ 対しては Graham と MacWilliams [2] の求めた結果と一致し，一般の $t \geqq 2$ に対しては，Smith [4] や Goethals と Delsarte [1] の求めた結果と一致する。

§ 3. $EG(t, p^n)$ における点と d-flats からなる incidence matrix の rank

(I)　$EG(t, q)$ の原点を通る d-flats の場合

$EG(t, q)$ の原点以外の $v^* = q^t - 1$ 個の点と原点を通る $b_0 = \phi(t-1, d-1, q)$ 個の d-flats からなる incidence matrix N_0 を次のように定義する。

$$N_0 = \| n_{ij} \| : i = 1, 2, \cdots b_0, \ j = 1, 2, \cdots, v^* \quad (3.1)$$

ここに

$$n_{ij} = \begin{cases} 1, & j \text{ 番目の点が } i \text{ 番目の } d\text{-flat にのっているとき}, \\ 0, & \text{そうでないとき}. \end{cases}$$

行列 N_0 の構造は N_0 の各列が $(q-1)$ 重複している点を除けば $PG(t-1, q)$ における $v = (q^t-1)/(q-1)$ 個の点と b_0 個の

$(d-1)$-flatsからなるincidence matrixと同じであることが知られている[5]。従って，次の定理をうる。

[定理3.1] $EG(t,q)$における原点以外のv^*個の点と原点を通るb_0個のd-flatsからなるincidence matrixの$GF(q)$上でのrankは$R_{d-1}(t-1,p^n)$である。

(II) $EG(t,q)$の原点を通らないd-flatsの場合

$EG(t,q)$における原点以外のv^*個の点と原点を通らないb_1個のd-flatsからなるincidence matrixをN_1とする。

ここに，

$$b_1=\phi(t,d,q)-\phi(t-1,d,q)-\phi(t-1,d-1,q) \qquad (3.2)$$

Smith[4]は$PG(t,q)$において用いたのと同様な方法を用いて，次のPropositionをえた。

Proposition 2 incidence matrix N_1の$GF(q)$上でのrank，$r_d(t,p^n)$，は次の2条件をみたす整数mの数に等しい。

(条件1) mは$1\leqq m\leqq v^*-1$なる整数であること。

(条件2) mは次のようなd個の整数$m_k(q-1)$ $(0<m_k(q-1)<m)$と整数m_0 $(0\leqq m_0\leqq m)$に分解可能であること。

$$m = m_0 + \sum_{k=1}^{d} m_k(q-1) \quad \text{かつ} \quad D_p[m] = D_p[m_0] + \sum_{k=1}^{d} D_p[m_k(q-1)] \tag{3.3}$$

これに対して次の定理が成り立つ。(詳しくは論文[3]を参照)

[定理 3.2] m を $1 \leqq m \leqq v^*$ なる整数とし，m の p 進表示を

$$m = \sum_{i=0}^{t-1} \sum_{j=0}^{n-1} c_{ij} p^{in+j} \quad (0 \leqq c_{ij} < p) \tag{3.4}$$

とする。このとき，m が Proposition 2 の 2 条件をみたすように分解可能であるための必要かつ十分条件は

$$s_n = s_0, \quad d \leqq s_j \leqq t, \quad 0 \leqq s_{j+1}p - s_j \leqq t(p-1) \tag{3.5}$$

$$\text{かつ} \quad \sum_{i=0}^{t-1} c_{ij} \geqq s_{j+1}p - s_j \quad (j = 0, 1, \cdots, n-1) \tag{3.5$'$}$$

をみたすような $n+1$ 個の整数 s_l $(l = 0, 1, \cdots, n)$ が存在することである。

従って，Proposition 2 の 2 条件をみたす整数 m の個数を計算するためには，(3.5) の条件をみたす整数 s_l $(l=0,1,\cdots,n)$ に対して，(3.5)$'$ の条件をみたす整数 c_{ij} $(0 \leqq c_{ij} < p)$ の ordered set $\{c_{ij} : i = 0, 1, 2, \cdots, t-1,\ j = 0, 1, \cdots, n-1\}$ の個数が計算出来ればよい。これに対して次の補題が成り立つ。

[補題 3.1] u_j $(j = 0, 1, \cdots, n-1)$ を $0 \leqq u_j \leqq (t-1)(p-1)$ なる整数とする。このとき，$j = 0, 1, \cdots, n-1$ に対して，

$$u_j \leqq \sum_{i=0}^{t-1} c_{ij} \leqq u_j + (p-1) \qquad (3.6)$$

かつ，あるjに対して，

$$\sum_{i=0}^{t-1} c_{ij} < u_j + (p-1) \qquad (3.6)'$$

をみたす整数c_{ij} $(0 \leqq c_{ij} < p)$ の ordered set $\{c_{ij} : i=0,1,\cdots,t-1, j=0,1,\cdots,n-1\}$ の個数は

$N_t(u_0+(p-1),\cdots,u_{n-1}+(p-1)) - N_{t-1}(u_0+(p-1),\cdots,u_{n-1}+(p-1))$

に等しい。

以上のことおよび，$m=v^*$のとき，mは(3.3)をみたすことより次の結論を得る。

[定理 3.3] EG(t,q)における原点以外のv^*個の点と原点を通らないb_1個のd-flats からなる incidence matrix N_1の GF(q)上での rank は

$$R_d(t,p^n) - R_d(t-1,p^n) - 1$$

に等しい。

[系 3.1] 特に，$d=t-1$の場合，incidence matrix N_1の rank は $\binom{t+p-1}{t}^n - 1$ である。

この結果はSmith[4]やGoethals と Delsarte[1]によって得られた。

(Ⅲ) (Ⅰ)と(Ⅱ)より次の定理をうる。

[定理 3.4] $EG(t,q)$ における q^t(または原点以外の v^*)個の点と $EG(t,q)$ におけるすべての d-flats からなる incidence matrix の $GF(q)$上での rank は

$$R_d(t,p^n)-R_d(t-1,p^n)$$

である。

§4 有限幾何を用いて作られる majority decodable code の構成と構造

最初にあとで用いる言葉の定義をかく。

q-ary linear code C (以下,略して code C と書く) とは $GF(q)$の元を要素とする N次元ベクトル空間 V_N の部分空間のことである。 V_Nの次元 N のことを code Cの長さ,部分空間 C の次元 k のことを code Cの information symbol の数という。code Cの直交補空間を C_D で表わし, C_D を code Cの dual code という。 行ベクトルが dual code を生成する行列のことを code C の parity check matrix という。 code Cに属するベクトル $\underline{C}=(c_0,c_1,\cdots,c_{N-1})$ のことを codeベクトルという。 code C のすべての code

ベクトル$\underline{c}'=(c_0, c_1, \cdots, c_{N-1})$に対して，$(c_{N-1}, c_0, \cdots, c_{N-2})$もまたCのcodeベクトルであるとき，code Cはcyclic codeであるという。code Cのcodeベクトル$\underline{c}'=(c_0, c_1, \cdots, c_{N-1})$に対して，多項式$c(x)=c_0+c_1x+\cdots+c_{N-1}x^{N-1}$を対応させ，$c(x)$をcodeベクトル$\underline{c}$の多項式と呼ぶ。

cyclic codeに関する次のことがらはよく知られていることであるがあとの説明のために補題としてまとめておく。

[補題4.1] code Cがcyclic codeであるならば，次の2つの性質をもち，かつ，code Cを生成する生成多項式（GF(q)の元を係数とする$r=N-k$次のmonicな多項式）$g(x)$が存在する。

(i) ベクトル$\underline{c}$がcode Cに属するとき，かつ，そのときのみ，$g(x)$はcodeベクトル$\underline{c}$の多項式$c(x)$を割り切る。

(ii) $g(x)$はx^N-1の約数である。すなわち，

$$x^N-1=g(x)h(x) \tag{4.1}$$

ここに，$h(x)$はGF(q)の元を係数とするk次の多項式である。

[補題4.2] code Cがcyclic codeならば，そのdual code C_Dもcyclic codeで，その生成多項式$g_D(x)$は

$$g_D(x) = x^k h(x^{-1})$$

で与えられる。

(I) d-th order Projective Geometry code の場合

[定義] $PG(t, q)$ における v 個の点と b 個の d-flats からなる incidence matrix を parity check matrix とする code のことを d-th order Projective Geometry code と呼び，d-PG code と略記する。

以下，d-PG code および，その dual code の生成多項式 $g(x)$，$g_D(x)$ の $g(x)=0$ および $g_D(x)=0$ の根を求め，これらの code と BCH code との関係を明らかにする。

まず，d-PG code の dual code C_D を考える。定義より d-PG code の dual code C_D の任意の code ベクトル $\underline{c}'=(c_1, c_2, \cdots, c_v)$ は $PG(t, q)$ における v 個の点と b 個の d-flats からなる incidence matrix N の行ベクトルの一次結合としてかける。すなわち，c の各元 c_j $(j=1, 2, \cdots, v)$ は $GF(q)$ の元 γ_i $(i=1, 2, \cdots, b)$ を用いて，

$$c_j = \sum_{i=1}^{b} \gamma_i n_{ij} \tag{4.3}$$

とかける。従って，d-PG code の dual code C_D の長さは v であり，information symbol の数は N の $GF(q)$ 上での rank $R\,d(t, p^n)$ に等しい。また，$PG(t, q)$ における すべての d-flat はある initial d-flat から cyclical に生成出来るから，d-PG code の dual code は cyclic code である。従って，d-PG code も cyclic code である。

d-PG code の dual code における code ベクトル $\underline{c}$ の多項式を $c(x)$ とすると，

$$C(x)=\sum_{j=1}^{v} c_j x^j=\sum_{i=1}^{b} \gamma_i \left\{\sum_{j=1}^{v} n_{ij}\, x^j\right\} \qquad (4.4)$$

である。一方，

$$\theta_i(x)=\sum_{j=1}^{v} n_{ij}\, x^j \quad (i=1,2,\cdots,b) \qquad (4.5)$$

であるから，

$$C(x)=\sum_{i=1}^{b} \gamma_i\, \theta_i(x) \qquad (4.6)$$

である。

(4.6)，Proposition 1，定理 2.1，定理 2.2 および補題 4.1 より次の定理をうる。

[定理 4.1] s_l $(l=0,1,\cdots,n)$ をある k に対して，$1 \leqq s_k \leqq d$，k 以外の l に対して，$1 \leqq s_l \leqq t+1$ (4.7)

かつ，$s_n=s_0$，$0 \leqq s_{j+1}p-s_j \leqq (t+1)(p-1)$ (4.7)′

$(j=0,1,\cdots,n-1)$ をみたす任意の整数とすると，

$$0 \leqq c_{ij} < p \quad \text{かつ} \quad \sum_{i=0}^{t} c_{ij} = s_{j+1}p - s_j \qquad (4.8)$$

をみたす整数 c_{ij} が少なくとも一組存在する。また，(4.8) をみたす任意の整数 c_{ij} に対して，

(i) $\sum_{i=0}^{t}\sum_{j=0}^{n-1} c_{ij}\,p^{in+j}$ は $(q-1)$ の倍数である。i.e.,

$$\sum_{i=0}^{t}\sum_{j=0}^{n-1} c_{ij}\,p^{in+j} = m(q-1) \qquad (4.9)$$

となる整数 m $(1 \leqq m \leqq v)$ が存在し，かつ，

(ii) この整数 m に対する β^m は d-PG code の dual code の生成多項式 $g_D(x)$ の $g_D(x)=0$ の根である。ここに，$\beta = \alpha^{q-1}$ （α は $GF(q^{t+1})$ の原始元）である。

逆に，$g_D(x)=0$ の根は上記の β^m 以外にはない。

[系 4.1] $h_0 = (q^{d+1}-1)/(q-1)$ とすると，$\beta, \beta^2, \cdots, \beta^{h_0-1}$ は $g_D(x)=0$ の根であるが，β^{h_0} は根ではない。i.e.,

d-PG code の dual code は designed distance が h_0 である BCH code である。

d-PG code については次の定理が成り立つ。

[定理 4.2] s_l $(l = 0, 1, \cdots, n)$ を

$$s_n = s_0, \qquad 0 \leqq s_j \leqq t-d \qquad (4.10)$$

かつ，　$0 \leqq s_{j+1}p - s_j \leqq (t+1)(p-1)$　　　(4.10)′

$(j=0,1,\cdots,n-1)$ をみたす任意の整数とすると，

$$0 \leqq C_{ij} < p \quad \text{かつ} \quad \sum_{i=0}^{t} C_{ij} = s_{j+1}p - s_j \qquad (4.11)$$

をみたす整数 C_{ij} が少なくとも一組存在する。また，

(4.11)をみたす任意の整数 C_{ij} に対して，

(i) $\sum_{i=0}^{t}\sum_{j=0}^{n-1} C_{ij}p^{in+j}$ は $(g-1)$ の倍数である。i.e.,

$$\sum_{i=0}^{t}\sum_{j=0}^{n-1} C_{ij}p^{in+j} = m(g-1) \qquad (4.12)$$

となる整数 m $(1 \leqq m \leqq v)$ が存在し，かつ，

(ii) この整数 m に対する β^m は d-PG code の生成多項式 $g(x)$ の $g(x)=0$ の根である。

逆に，$g(x)=0$ の根は上記の β^m 以外にはない。

[系 4.2]　$h_1 = (g^{t-d+1}-1)/(g-1)$ とすると，$\beta^0, \beta^1, \cdots, \beta^{h_1-1}$ は $g(x)=0$ の根であるが，β^{h_1} は根ではない。すなわち，d-PG code は designed distance が h_1+1 である BCH code である。

(III) d-th order Affine Geometry code の場合

紙面の関係上省略する。

参 考 文 献

[1] Goethals, J.M. and Delsarte, P. (1967). On a class of majority logic decodable cyclic codes. presented at the San Remo International Symposium on Information Theory, September, 1967.

[2] Graham, R.L. and MacWilliams, J. (1966). On the number of information symbols in difference-set cyclic codes. Bell System Technical Journal 45 1057-1070.

[3] 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.

[4] Smith, K.J.C. (1967). Majority decodable codes derived from finite geometries. Inst. Statist. mimeo. series 561, Chapel Hill, N.C.

[5] Yamamoto, S, Fukuda, T. and Hamada, N. (1966). On finite geometries and cyclically generated incomplete block designs. J. Sci. Hiroshima Univ. Ser. A-I 30 137-149.