HIROSHIMA MATH. J.
3 (1973), 153–226

On the p-Rank of the Incidence Matrix of a Balanced or Partially Balanced Incomplete Block Design and its Applications to Error Correcting Codes

Noboru HAMADA

(Received January 26, 1973)

CONTENTS

0. Introduction and Summary

In this paper, we shall investigate the ranks over the Galois field GF(q), i.e., q-ranks, of the incidence matrices of balanced incomplete block (*BIB*) designs and partially balanced incomplete block (*PBIB*) designs where q is a prime or a prime power, say $q=p^n$.

These q-ranks, especially the p-ranks of the incidence matrices of *BIB* designs derived from finite geometries, have been investigated in relation to majority decodable codes. The p-rank of the incidence matrix $N(p^m; t, \mu)$ of points and μ-flats in a finite projective geometry PG (t, p^m) has been investigated by several authors [10, 11, 12, 30, 31, 32] and a general formula for the p-rank of $N(p^m; t, \mu)$ has been obtained by the present author [12]. An explicit formula for the p-rank of the incidence matrix $M_1(p^m; t, \mu)$ of points other than the origin and μ-flats not passing through the origin in an affine geometry EG(t, p^m) has been obtained by Smith [31] for the case $m=1$ and by the present author [12] for general m. In this paper, another formula for the p-rank of $N(p^m; t, \mu)$ and an explicit formula for the p-rank of the incidence matrix $M^*(p^m; t, \mu)$ of all points and μ-flats in EG(t, p^m) will be given. Tables for the p-ranks of $N(p^m; t, \mu)$ and $M^*(p^m; t, \mu)$ will also be given. The above mentioned incidence matrices are those of *BIB* designs or *PBIB* designs. If the transpose of incidence matrix N of a *BIB* design or a *PBIB* design is used as a parity check matrix of a linear code C, the code C has a merit in that a relatively simple decoding procedure, called majority decoding [18], is applicable. It is desirable to obtain, in an error correcting code, a linear code having a relatively large number of information symbols. The number of information symbols of a q-ary linear code C with length v is equal to v–Rank$_q(N)$ where Rank$_q(N)$ denotes the q-rank of N. It is, therefore, necessary to obtain, in *BIB* designs and *PBIB* designs, the value of q and the incidence matrix N having a relatively small q-rank.

This paper is divided into four parts. In Part I, the value of q and the incidence matrix N having a relatively small q-rank in *BIB* designs and *PBIB* designs are investigated. It will be shown that the q-rank of the incidence matrix of a *BIB* design with parameters v, b, r, k, λ is never less than $v-1$ unless q is a factor of $r-\lambda$ and that, for q being a factor of $r-\lambda$, its q-rank depends on the block structure of the design. A lower bound, from which we can obtain the value of q such that the q-rank of N is relatively small, for the q-rank of the incidence matrix N of a *PBIB* design is given. From this lower bound and the results in [35], we can obtain lower bounds for q-ranks of the incidence matrices of T_m type *PBIB* designs and N_m type *PBIB* designs. To obtain the incidence matrix of a *BIB* design with a relatively small p-rank for a prime p which is a factor of $r-\lambda$, we shall enumerate nonisomorphic solutions for a *BIB* design with parameters satisfying either the condition (i) $1\leqq\lambda\leqq 3$, $3\leqq k\leqq 5$ and $6\leqq v\leqq b\leqq 30$ or (ii) $1\leqq\lambda\leqq 3$

and $7 \leqq v = b \leqq 20$ and investigate their p-ranks. As far as we concern with *BIB* designs discussed above, the p-rank of the incidence matrix of a *BIB* design derived from a finite geometry is minimum among *BIB* designs with the same parameters. In Table 6.2, if two *BIB* designs D_1 and D_2 are nonisomorphic, their p-ranks are different for some prime p except for the designs of Nos. 6, 8, 12 and 13. This shows that p-rank is useful as a criterion of isomorphism.

In Part II, the p-ranks of the incidence matrices of *BIB* designs derived from finite geometries are investigated. Another formula for the p-rank of $N(p^m; t, \mu)$ and tables for the p-rank are given. A formula for the p-rank of the incidence matrix of points and certain sets in PG(t, p^m) is also given. As a special case, the p-rank of the complement matrix of $N(p^m; t, \mu)$ can be obtained from the formula. In Section 9, an explicit formula for the p-rank of the incidence matrix $M^*(p^m; t, \mu)$ of all points and all μ-flats in EG(t, p^m) and tables for the p-rank are given.

In Part III, the p-ranks of the incidence matrices of *PBIB* designs derived from finite geometries are investigated. An explicit formula for the p-rank of the incidence matrix of points and μ-flats with a cycle θ in PG(t, p^m) is obtained by using the cyclic structure of μ-flats in PG(t, p^m) [36]. It is shown that the dual of any *BIB* design PG(t, p^m): μ is a *PBIB* design and its p-rank is given.

In Part IV, we shall apply these results and technique to error correcting codes, especially to geometry codes and polynomial codes. In Section 13, the results in Parts I, II and III are applied to *BIBD* codes and *PBIBD* codes. In Section 14, the number of information symbols of the Projective Geometry code, the Affine Geometry code and the Euclidean Geometry code and their generator polynomials are given. In Section 15, a formula for the number of information symbols of a polynomial code is given.

Part I. The p-ranks of the incidence matrices of a *BIB* design and a *PBIB* design

1. The incidence matrices of a *BIB* design and a *PBIB* design

A balanced incomplete block (*BIB*) design [37] with parameters v, b, r, k, λ is an arrangement of v objects (treatments) into b sets (blocks) such that:

(i) Each block contains exactly k distinct treatments.

(ii) Each treatment occurs in exactly r different blocks.

(iii) Every pair of treatments occur in λ blocks.

Among parameters v, b, r, k, λ, there are the following relations:

$$(1.1) \qquad vr = bk, \quad \lambda(v-1) = r(k-1) \quad \text{and} \quad b \geqq v.$$

The last inequality is due to Fisher [9].

A partially balanced incomplete block (*PBIB*) design [6, 20] with m associate classes and parameters v, b, r, k, λ_i, n_i, p^i_{jk} (i, j, $k=0, 1, \ldots, m$) is an arrangement of v treatments into b blocks such that:

(i) Each block contains exactly k distinct treatments.

(ii) Each treatment occurs in exactly r different blocks.

(iii) There exists a relationship of association, called an association scheme with m associate classes [7], between every pair of the v treatments satisfying the following three conditions:

(a) Any two treatments are either 1st, 2nd, ..., or mth associates, the relation of association being symmetrical. Each treatment is the zero-th associate of itself.

(b) Each treatment α has n_i ith associates, the number n_i being independent of α.

(c) If any two treatments α and β are ith associates, then the number of treatments which are jth associates of α and kth associates of β is p^i_{jk} and is independent of the pair of ith associates α and β.

(iv) Any pair of treatments which are ith associates occur together in exactly λ_i blocks.

After numbering v treatments and b blocks in some way, respectively, we define the incidence matrix of a *BIB* design or a *PBIB* design to be the matrix:

$$N = \|n_{ij}\|; \quad i=1, 2, \ldots, v \quad \text{and} \quad j=1, 2, \ldots, b$$

where $n_{ij}=1$ or 0 according as the ith treatment occurs in the jth block or not. In the special case where N is the incidence matrix of a *BIB* design, the following relations hold:

$$\sum_{j=1}^{b} n_{ij} = r \quad \text{for each } i=1, 2, \ldots, v. \tag{1.2}$$

$$\sum_{i=1}^{v} n_{ij} = k \quad \text{for each } j=1, 2, \ldots, b. \tag{1.3}$$

$$\sum_{j=1}^{b} n_{\alpha j} n_{\beta j} = \lambda \quad \text{for each pair of } \alpha \text{ and } \beta. \tag{1.4}$$

Since each entry of the incidence matrix N is 0 or 1, the rank of N over GF(p^n) is equal to its rank over GF(p) for any prime p and any positive integer n. We shall deal with only the rank of N over GF(p) or the p-rank of N in Part I.

2. A lower bound for the p-rank of the incidence matrix of a *BIB* design

To obtain the value of a prime p such that the p-rank of the incidence matrix N of a *BIB* design with parameters v, b, r, k, λ is relatively small, we prepare the following theorem:

THEOREM 2.1. (i) *If p is a prime which is not a factor of $r(r-\lambda)$, the p-rank of N is equal to v.*

(ii) *If p is a prime which is a factor of r but not a factor of $r-\lambda$, the p-rank of N is equal to $v-1$ or v. If p is a common factor of r and k but not a factor of $r-\lambda$, the p-rank of N is equal to $v-1$.*

PROOF. Let p be any prime and let $\mathscr{R}_p(N)$ be the vector space over GF(p) generated by the column vectors of the incidence matrix N of a *BIB* design with parameters v, b, r, k, λ. Then it follows from (1.2) and (1.4) that there exist column vectors $\boldsymbol{a}$ and $\boldsymbol{b}_i$ ($i=1, 2, \ldots, v$) in $\mathscr{R}_p(N)$ such that

$$\boldsymbol{a}^T=(r_1, r_1, \ldots, r_1) \quad \text{and} \quad \boldsymbol{b}_i^T=(\lambda_1, \ldots, \lambda_1, \overset{\underset{\smile}{i}}{r_1}, \lambda_1, \ldots, \lambda_1)$$

where r_1 and λ_1 are non-negative integers less than p such that $r_1 \equiv r$ and $\lambda_1 \equiv \lambda$ mod p, and $\boldsymbol{x}^T$ denotes the transpose of the vector $\boldsymbol{x}$. Since

$$r_1\boldsymbol{b}_i^T-\lambda_1\boldsymbol{a}^T \equiv (0, 0, \ldots, 0, r_1(r_1-\lambda_1), 0, \ldots, 0) \bmod p$$

for $i=1, 2, \ldots, v$ and $r(r-\lambda)\equiv r_1(r_1-\lambda_1)$ mod p, we can see that (i) holds. Similarly, we can see from the linear combinations $\boldsymbol{b}_1-\boldsymbol{b}_j$ ($j=2, 3, \ldots, v$) that the p-rank of N is greater than or equal to $v-1$. If p is a factor of k, it follows from (1.3) that the p-rank of N is less than or equal to $v-1$. We have therefore the required result.

Theorem 2.1 shows that the p-rank of N is never less than $v-1$ unless p is a factor of $r-\lambda$. For a prime p being a factor of $r-\lambda$, the p-rank of N may be less than $v-1$. In general, it depends on the block structure of the design.

EXAMPLE 2.1. Consider a *BIB* design with parameters

$$v=8,\ b=14,\ r=7,\ k=4,\ \lambda=3.$$

It is known [21, 33] that there are four nonisomorphic designs D_i ($i=1, 2, 3, 4$) in all as follows:

$$D_1 = \left\{ \begin{matrix} 1248, 2358, 3468, 4578, 5618, 6728, 7138 \\ 3567, 4671, 5712, 6123, 7234, 1345, 2456 \end{matrix} \right\}$$

$$D_2 = \left\{ \begin{matrix} 1234, 1256, 1278, 5678, 3478, 3456, 1357 \\ 2457, 2458, 1358, 1467, 1468, 2367, 2368 \end{matrix} \right\}$$

$$D_3 = \left\{ \begin{matrix} 1234, 5678, 1256, 1456, 1278, 1478, 1357 \\ 3457, 1368, 3468, 2358, 2458, 2367, 2467 \end{matrix} \right\}$$

$$D_4 = \left\{ \begin{matrix} 1248, 2358, 3468, 4578, 5618, 6728, 7138 \\ 2357, 6731, 5174, 3412, 7246, 1625, 4563 \end{matrix} \right\}$$

where each of the numbers 1, 2, ..., 8 represents each of the eight treatments and each set of four numbers $c_1c_2c_3c_4$ represents a block which contains four treatments c_1, c_2, c_3 and c_4. Let N_i be the incidence matrix of the *BIB* design D_i, then it can be shown easily that $\mathrm{Rank}_2(N_1)=4$, $\mathrm{Rank}_2(N_2)=5$, $\mathrm{Rank}_2(N_3)=6$ and $\mathrm{Rank}_2(N_4)=7(=v-1)$ where $\mathrm{Rank}_p(N)$ denotes the rank of N over $GF(p)$. This shows that for a prime p which is a factor of $r-\lambda$, the p-rank of the incidence matrix of a *BIB* design with parameters v, b, r, k, λ depends on the block structure of the design. In Section 6 and Part II, the p-rank of N for a prime p being a factor of $r-\lambda$ will be investigated in detail.

3. A lower bound for the p-rank of the incidence matrix of a *PBIB* design

Let N be the incidence matrix of a *PBIB* design with m associate classes and parameters v, b, r, k, λ_i, n_i, p^i_{jk} $(i, j, k=0, 1, \dots, m)$ and we define association matrices A_i $(i=0, 1, \dots, m)$ to be the matrices:

$$A_i=\|a^\beta_{\alpha i}\|;\ \alpha=1, 2, \dots, v \quad \text{and } \beta=1, 2, \dots, v$$

where $a^\beta_{\alpha i}=1$ or 0 according as the treatments α and β are ith associates or not. These association matrices A_0, A_1, $\dots$, A_m are symmetric, linearly independent and satisfy the following relations:

$$A_0=I_v,\ \sum_{i=0}^m A_i=G_v,\ A_iA_j=A_jA_i=\sum_{k=0}^m p^k_{ij}A_k, \tag{3.1}$$

$$NN^T=\lambda_0A_0+\lambda_1A_1+\cdots+\lambda_mA_m \tag{3.2}$$

where I_v is the unit matrix of order v, G_v is the vxv matrix whose elements are all unity and $\lambda_0=r$.

The linear closure of the association matrices A_0, A_1, $\dots$, A_m over the real field is a linear associative and commutative algebra, which is called the association algebra [5], [24] of the given association and denoted by $\mathfrak{A}_m$ or $[A_i;\ i=0, 1, \dots, m]$. It is completely reducible and its minimum two sided ideals are linear. We define $\mathscr{P}_k$ $(k=0, 1, \dots, m)$ by

$$\mathscr{P}_k=\|p^i_{jk}\|;\ j=0, 1, \dots, m \quad \text{and } i=0, 1, \dots, m$$

and let z_{jk} $(j=0, 1, \dots, m)$ be the characteristic roots of $\mathscr{P}_k$, then it is known that the principal idempotents $A^\#_0$, $A^\#_1$, $\dots$, $A^\#_m$ of those $m+1$ ideals and the association matrices A_0, A_1, $\dots$, A_m are mutually linked by the linear combinations of the others, that is,

$$A_k=\sum_{j=0}^m z_{jk}A^\#_j \quad \text{and} \quad A^\#_j=\sum_{k=0}^m z^{jk}A_k \tag{3.3}$$

where $z^{jk}=\alpha_jz_{jk}/vn_k$ and α_j is the rank of $A^\#_j$ over the real field.
From (3.2) and (3.3), it follows that

$$NN^T=\rho_0A^\#_0+\rho_1A^\#_1+\cdots+\rho_mA^\#_m \tag{3.4}$$

where $\rho_i = \sum_{j=0}^{m} \lambda_j z_{ij}$ for $i=0, 1, \ldots, m$ and ρ_i's are the characteristic roots of NN^T with multiplicities α_i. If z_{jk}'s are all rational, ρ_j's and all of the idempotent matrices $A_i^\#$ $(i=0, 1, \ldots, m)$ are rational.

The following theorem which gives a lower bound for the p-rank of the incidence matrix of a *PBIB* design may be useful in constructing a better *PBIBD* code (see Section 13).

THEOREM 3.1. *Suppose that z_{ij}'s are all rational and let c_1 and c_2 be the minimum positive integers such that $c_1\alpha_i z_{ij}/vn_j$'s and $c_2 z_{ij}$'s are all integers (i.e., entries of $c_1 A_i^\#$'s and $c_2\rho_i$'s are all integers). Then the p-rank of N is greater than or equal to $\sum_{i=0}^{m} \varepsilon_i\alpha_i$ provided p is not a factor of c_1c_2, where $\varepsilon_i=0$ or 1 according as $c_2\rho_i$ is zero* mod *p or not. In the special case $\rho_i \neq 0$ for all $i=0, 1, \ldots, m$, the p-rank of N is equal to v unless p is a factor of $c_1 \prod_{i=0}^{m} c_2\rho_i$.*

PROOF. As $\text{Rank}_p(N) \geqq \text{Rank}_p(NN^T)$ for any prime p, it is sufficient to prove that $\text{Rank}_p(NN^T) = \sum_{i=0}^{m} \varepsilon_i\alpha_i$ for any prime p which is not a factor of c_1c_2. Let $A_i^* = c_1 A_i^\#$ and $\rho_i^* = c_2\rho_i$ for $i=0, 1, \ldots, m$. ρ_i^*'s and entries of A_i^*'s are all integers. Since

$$\sum_{i=0}^{m} A_i^\# = I_v,\ A_i^\# A_j^\# = \delta_{ij} A_i^\# \qquad (i, j=0, 1, \ldots, m)$$

and

$$\text{Rank}_p(B) \leqq \text{Rank}(B)$$

for any prime p and for any matrix B whose elements are all integers, where Rank(B) denotes the rank of B over the real field, we have

$$\text{Rank}_p(c_1 I_v) = \text{Rank}_p\Big(\sum_{i=0}^{m} A_i^*\Big) \leqq \text{Rank}_p[A_0^* : A_1^* : \ldots : A_m^*]$$

$$\leqq \sum_{i=0}^{m} \text{Rank}_p(A_i^*) \leqq \sum_{i=0}^{m} \text{Rank}(A_i^*) = \sum_{i=0}^{m} \alpha_i = v.$$

From the above inequalities, it follows that if p is a prime which is not a factor of c_1,

$$\text{Rank}_p[A_0^* : A_1^* : \ldots : A_m^*] = v \quad \text{and} \quad \text{Rank}_p(A_i^*) = \alpha_i$$

for $i=0, 1, \ldots, m$. Let $\boldsymbol{a}_1^{(i)}, \boldsymbol{a}_2^{(i)}, \ldots, \boldsymbol{a}_{\alpha_i}^{(i)}$ $(i=0, 1, \ldots, m)$ be linearly independent column vectors of A_i^* and let

$$P = [\boldsymbol{a}_1^{(0)}, \ldots, \boldsymbol{a}_{\alpha_0}^{(0)} : \ldots : \boldsymbol{a}_1^{(m)}, \ldots, \boldsymbol{a}_{\alpha_m}^{(m)}].$$

Then P is a non-singular matrix over GF(p). Since A_i^*'s are all symmetric and $A_i^* A_j^* = c_1 \delta_{ij} A_i^*$, using (3.4), we have

$$\mathrm{Rank}_p(c_1 c_2 N N^T) = \mathrm{Rank}_p\Big(\sum_{i=0}^{m} \rho_i^* A_i^*\Big) = \mathrm{Rank}_p\Big[P^T\Big(\sum_{i=0}^{m} \rho_i^* A_i^*\Big)P\Big]$$

and

$$\mathrm{Rank}_p\Big[c_1 P^T\Big(\sum_{i=0}^{m} \rho_i^* A_i^*\Big)P\Big] = \mathrm{Rank}_p\Big[\sum_{i=0}^{m} \rho_i^* (A_i^* P)^T (A_i^* P)\Big] = \sum_{i=0}^{m} \varepsilon_i \alpha_i.$$

Therefore, we have the required result.

Since $\rho_i = \sum_{j=0}^{m} \lambda_j z_{ij}$ $(i=0, 1, \ldots, m)$, it is sufficient to obtain only the values of α_i's and z_{ij}'s except for parameters v, n_i's and λ_i's to obtain such a lower bound.

4. A lower bound for the p-rank of the incidence matrix of a T_m type *PBIB* design

Suppose that there are $v = \binom{s}{m}$ treatments $\phi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ indexed by the combinations or subsets of m integers $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ out of the set of s integers $(1, 2, \ldots, s)$ where m and s are any integers such that $4 \leqq 2m \leqq s$. Among those v treatments, an association of triangular type or T_m type with m associate classes is defined as follows:

DEFINITION 4.1. Two treatments $\phi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $\phi(\beta_1, \beta_2, \ldots, \beta_m)$ are ith associates if their indices $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $(\beta_1, \beta_2, \ldots, \beta_m)$ have $m-i$ integers in common. Each treatment is the 0th associate of itself.

The association defined above satisfies three conditions of the association scheme with m associate classes and this scheme is called a triangular type association scheme with m associate classes, or briefly, a T_m type association scheme [23, 35]. In this case, it has been shown by Yamamoto, Fujii and Hamada [35] that

$$n_i = \binom{m}{i}\binom{s-m}{i}, \qquad \alpha_i = \binom{s}{i} - \binom{s}{i-1}, \tag{4.1}$$

$$z_{ij} = \frac{\binom{s-m}{j}}{\binom{s-m}{i}} \sum_{a=0}^{i} (-1)^{i-a} \binom{m-a}{j}\binom{m-a}{m-i}\binom{s-i+1}{a} \tag{4.2}$$

or

$$z_{ij} = \sum_{a=0}^{j} (-1)^{j-a} \binom{m-i}{a}\binom{m-a}{m-j}\binom{s-m-i+a}{a} \tag{4.2'}$$

for $i, j=0, 1, \ldots, m$. The last equation is due to Ogasawara [23]. From Theorem 3.1 and the above equations, we can obtain a lower bound for the p-rank of the incidence matrix of a T_m type *PBIB* design.

In the special case $m=2$, we have

$$
\begin{aligned}
&v=\binom{s}{2}, \quad n_0=1, \quad n_1=2(s-2), \quad n_2=\binom{s-2}{2},\\
&z_{00}=1, \quad z_{01}=n_1, \quad z_{02}=n_2,\\
&z_{10}=1, \quad z_{11}=s-4, \quad z_{12}=-(s-3),\\
&z_{20}=1, \quad z_{21}=-2, \quad z_{22}=1,\\
&\alpha_0=1, \quad \alpha_1=s-1, \quad \alpha_2=s(s-3)/2,\\
&\rho_0=rk, \quad \rho_1=r+\lambda_1(s-4)-\lambda_2(s-3), \quad \rho_2=r-2\lambda_1+\lambda_2,\\
&c_1=s(s-1)(s-2) \quad \text{and} \quad c_2=1
\end{aligned}
$$

where s is an integer not less than four.

THEOREM 4.1. *Let N be the incidence matrix of a T_2 type PBIB design with parameters $v=\binom{s}{2}$, b, r, k, λ_i, n_i, p^i_{jk} $(i, j, k=0, 1, 2)$.*

(A) *In the case when $\rho_1\neq 0$ and $\rho_2\neq 0$.*

(i) *The p-rank of N is equal to v unless p is a factor of $rk\rho_1\rho_2\, s(s-1)\cdot(s-2)$.*

(ii) *If p is a prime which is a factor of ρ_1 but not a factor of $\rho_2 s(s-1)\cdot(s-2)$, the p-rank of N is greater than or equal to $s(s-3)/2$.*

(iii) *If p is a prime which is a factor of ρ_2 but not a factor of $\rho_1 s(s-1)\cdot(s-2)$, the p-rank of N is greater than or equal to $s-1$.*

(B) *In the case when $\rho_1=0$ and $\rho_2\neq 0$, $\mathrm{Rank}_p(N)\leqq s(s-3)/2+1$ for any prime p and the p-rank of N is never less than $s(s-3)/2$ unless p is a factor of $\rho_2 s(s-1)(s-2)$.*

(C) *In the case when $\rho_1\neq 0$ and $\rho_2=0$, $\mathrm{Rank}_p(N)\leqq s$ for any prime p and the p-rank of N is never less than $s-1$ unless p is a factor of $\rho_1 s(s-1)(s-2)$.*

5. A lower bound for the p-rank of the incidence matrix of an N_m type *PBIB* design

Suppose that there are $v=s_1 s_2\ldots s_m$ treatments $\phi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ indexed by m-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ where $\alpha_i=1, 2, \ldots, (s_i-1)$ or s_i for $i=1, 2, \ldots, m$. Among these treatments, we define a relation of m-fold nested type or N_m type association as follows:

DEFINITION 5.1. A pair of treatments $\phi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $\phi(\beta_1, \beta_2, \ldots, \beta_m)$ are ith associates if $\alpha_j=\beta_j$ for all $j=1, 2, \ldots, m-i$ and $\alpha_{m-i+1}\neq\beta_{m-i+1}$. Each treatment is 0th associate of itself.

The association defined above satisfies three conditions of the association scheme with m associate classes and it is called an m-fold nested type association scheme or an N_m type association scheme [35]. For the special case $m=2$, it is called a group divisible (GD) type association scheme [7]. After numbering v treatments in dictionary-wise, we can express the association matrices as follows:

$$
\begin{aligned}
&A_0=I_v,\ A_1=I_{s_1}\otimes\cdots\otimes I_{s_{m-1}}\otimes(G_{s_m}-I_{s_m}),\\
(5.1)\qquad &A_i=I_{v_{m-i}}\otimes(G_{s_{m-i+1}}-I_{s_{m-i+1}})\otimes G_{s_{m-i+2}}\otimes\cdots\otimes G_{s_m},\\
&A_m=(G_{s_1}-I_{s_1})\otimes G_{s_2}\otimes\cdots\otimes G_{s_m}
\end{aligned}
$$

for $i=2, 3, \ldots, m-1$ where $v_j=s_1s_2\ldots s_j$ and $A\otimes B$ denotes Kronecker product of the matrices $A=\|a_{ij}\|$ and B, i.e., $A\otimes B=\|a_{ij}B\|$.

The linear closure of the association matrices A_i $(i=0, 1, \ldots, m)$ over the real field is called an m-fold nested type association algebra or an N_m type association algebra and denoted by $\mathfrak{A}(N_m)$. It is known [35] that the mutually orthogonal idempotents of $\mathfrak{A}(N_m)$ are expressed as follows:

$$
\begin{aligned}
&A_0^{\#}=\frac{1}{v}G_v,\ A_1^{\#}=(I_{s_1}-\frac{1}{s_1}G_{s_1})\otimes\frac{1}{s_2}G_{s_2}\otimes\cdots\otimes\frac{1}{s_m}G_{s_m},\\
(5.2)\qquad &A_i^{\#}=I_{v_{i-1}}\otimes(I_{s_i}-\frac{1}{s_i}G_{s_i})\otimes\frac{1}{s_{i+1}}G_{s_{i+1}}\otimes\cdots\otimes\frac{1}{s_m}G_{s_m},\\
&A_m^{\#}=I_{s_1}\otimes I_{s_2}\otimes\cdots\otimes I_{s_{m-1}}\otimes(I_{s_m}-\frac{1}{s_m}G_{s_m})
\end{aligned}
$$

for $i=2, 3, \ldots, m-1$. From (5.1) and (5.2), we have

$$
\begin{aligned}
&\alpha_0=1,\ \alpha_1=s_1-1,\ \alpha_j=s_1s_2\ldots s_{j-1}(s_j-1),\\
&n_0=1,\ n_1=s_m-1,\ n_j=(s_{m-j+1}-1)s_{m-j+2}\cdots s_m,\\
&z_{00}=z_{10}=\cdots=z_{m0}=1,\ z_{01}=z_{11}=\cdots=z_{m-11}=n_1,\\
(5.3)\qquad &z_{m1}=-1,\ z_{0j}=z_{1j}=\cdots=z_{m-jj}=n_j,\\
&z_{m-j+1j}=-s_{m-j+2}s_{m-j+3}\cdots s_m,\\
&z_{m-j+2,j}=z_{m-j+3,j}=\cdots=z_{mj}=0
\end{aligned}
$$

for $j=2, 3, \ldots, m$. Theorem 3.1 and the above equations give a lower bound for the p-rank of the incidence matrix of an N_m type $PBIB$ design. As a special case $m=2$, we have

$$
\begin{aligned}
&v=s_1s_2,\ n_0=1,\ n_1=s_2-1,\ n_2=(s_1-1)s_2,\\
&z_{00}=1,\ z_{01}=n_1,\ z_{02}=n_2,\\
&z_{10}=1,\ z_{11}=n_1,\ z_{12}=-s_2,\\
&z_{20}=1,\ z_{21}=-1,\ z_{22}=0, \qquad (5.4)\\
&\alpha_0=1,\ \alpha_1=s_1-1,\ \alpha_2=s_1(s_2-1),\\
&\rho_0=rk,\ \rho_1=rk-v\lambda_2,\ \rho_2=r-\lambda_1,\\
&c_1=s_1s_2 \quad \text{and} \quad c_2=1.
\end{aligned}
$$

From Theorem 3.1, we have therefore the following theorem:

THEOREM 5.1. *Let N be the incidence matrix of an N_2 (GD) type PBIB design with parameters $v=s_1s_2$, b, r, k, λ_i, n_i, p^i_{jk} (i, j, $k=0$, 1, 2).*

(A) *In the case $\rho_1\neq 0$ and $\rho_2\neq 0$ (regular GD design).*

(i) *The p-rank of N is equal to v unless p is a factor of $rk\rho_1\rho_2s_1s_2$.*

(ii) *If p is a prime which is a factor of ρ_1 but not a factor of $\rho_2s_1s_2$, the p-rank of N is greater than or equal to $s_1(s_2-1)$.*

(iii) *If p is a prime which is a factor of ρ_2 but not a factor of $\rho_1s_1s_2$, the p-rank of N is greater than or equal to s_1-1.*

(B) *In the case $\rho_1=0$ and $\rho_2\neq 0$ (semi-regular GD design),* $\mathrm{Rank}_p(N)\leqq s_1(s_2-1)+1$ *for any prime p and the p-rank of N is never less than $s_1(s_2-1)$ unless p is a factor of $\rho_2s_1s_2$.*

(C) *In the case $\rho_1\neq 0$ and $\rho_2=0$ (singular GD design),* $\mathrm{Rank}_p(N)\leqq s_1$ *for any prime p and the p-rank of N is never less than s_1-1 unless p is a factor of $\rho_1s_1s_2$.*

In Part III, the p-rank of N for a prime p which is a factor of $\rho_1\rho_2$ will be investigated. Applying Theorem 3.1 to an F_p type *PBIB* design and an OL_r type *PBIB* design [35] etc., we can obtain similar results.

6. Enumeration of nonisomorphic solutions of *BIB* designs and their *p*-ranks

In Section 2, it has been shown that the p-rank of the incidence matrix N of a *BIB* design with parameters v, b, r, k, λ is never less than $v-1$ unless p is a factor of $r-\lambda$ and that, for a prime p which is a factor of $r-\lambda$, the p-rank of N depends, in general, on the block structure of the design. In this section, to investigate in detail the p-rank of the incidence matrix of a *BIB* design, we shall enumerate all possible nonisomorphic solutions of a certain restricted class of *BIB* designs and investigate their p-ranks.

DEFINITION 6.1. Two *BIB* designs D_1 and D_2 with the same parameters are isomorphic if there exist two permutation matrices P and Q such that $N_1 = PN_2Q$ for their incidence matrices N_1 and N_2. Otherwise they are nonisomorphic.

Let N_1 and N_2 be the incidence matrices of two *BIB* designs D_1 and D_2 with the same parameters, respectively. Then if two designs D_1 and D_2 are isomorphic, the p-rank of N_1 is equal to the p-rank of N_2 for any prime p.

Since it is very difficult, in general, to enumerate all possible nonisomorphic solutions, taking into account the results in Section 13, we shall confine ourselves to *BIB* designs with parameters satisfying either the condition (i) $1 \leqq \lambda \leqq 3$, $3 \leqq k \leqq 5$ and $6 \leqq v \leqq b \leqq 30$ or (ii) $1 \leqq \lambda \leqq 3$ and $7 \leqq v = b \leqq 20$. All parameter combinations satisfying the above conditions, the number of nonisomorphic solutions and their p-ranks are given in Table 6.1. The symbol — in Table 6.1 denotes the case where the number of nonisomorphic solutions has not yet been obtained. The symbols PG(t, q): μ and EG(t, q): μ denote the *BIB* design derived from finite projective geometry PG(t, q) and Affine geometry EG(t, q), respectively, by identifying the points of the geometry with the v treatments and identifying the μ-flats of the geometry with the b blocks (see Sections 7 and 9). The number a^* with asterisk (*) denotes that the p-rank of the design PG(t, q): μ or EG(t, q): μ which is written on the right hand side of a^* is equal to a and $\delta = [r/2\lambda]$. It is easy to see that *BIB* designs Nos. 2, 3, 5 and 11 in Table 6.1 are all unique (i.e., all designs are isomorphic) and their p-ranks are equal to 4, 3, 6 and 7, respectively where $p = r - \lambda$. Hussain [14, 15] showed that the *BIB* design No. 9 has only one solution while the design No. 15 has three nonisomorphic solutions and the design No. 14 does not exist. Nandi [21, 22] showed that *BIB* designs Nos. 1, 4, 7 and 13 have one, four, three and five nonisomorphic solutions, respectively. Pasquale [25] showed that the *BIB* design No. 12 has two nonisomorphic solutions. Since the design No. 10 is the complementary design of No. 9, it follows from the uniqueness of the design No. 9 that the design No. 10 is also unique. Thus, the designs which have not yet been solved in Table 6.1 are five designs Nos. 6, 8, 16, 17 and 18.

TABLE 6.1.
NUMBER OF NONISOMORPHIC SOLUTIONS AND THEIR P-RANKS

No.	v	b	r	k	λ	δ	$r-\lambda$	no. of noniso.	p	p-rank	Geometrical design
1	6	10	5	3	2	1	3	1	3	5	
2	7	7	3	3	1	1	2	1	2	4*	PG(2, 2):1
3	7	7	4	4	2	1	2	1	2	3	complement
4	8	14	7	4	3	1	4	4	2	4*, 5, 6, 7	EG(3, 2):2
5	9	12	4	3	1	2	3	1	3	6*	EG(2, 3):1
6	9	18	8	4	3	1	5	—	5	—	
7	10	15	6	4	2	1	4	3	2	5, 6, 7	
8	10	30	9	3	2	2	7	—	7	—	
9	11	11	5	5	2	1	3	1	3	6	
10	11	11	6	6	3	1	3	1	3	5	
11	13	13	4	4	1	2	3	1	3	7*	PG(2, 3):1
12	13	26	6	3	1	3	5	2	5	13, 13	
13	15	15	7	7	3	1	4	5	2	5*,6,8,8,8	PG(3, 2):2
14	15	21	7	5	2	1	5	non-existence			
15	16	16	6	6	2	1	4	3	2	6, 7, 8	
16	16	20	5	4	1	2	4	1	2	9*	EG(2, 4):1
17	21	21	5	5	1	2	4	2	2	10*, 12	PG(2, 4):1
18	25	30	6	5	1	3	5	1	5	15*	EG(2, 5):1

(a) Enumeration of nonisomorphic solutions of the design No. 17

THEOREM 6.1. *The BIB design with parameters* (21, 21, 5, 5, 1) *has two nonisomorphic solutions and their* 2*-ranks are equal to* 10 *and* 12.

PROOF.. Let us denote twenty-one treatments by $\infty, 0_1, 0_2, 0_3, 0_4, 1_1, 1_2, \ldots, 4_3, 4_4$ and twenty-one blocks by $B_i (i=0, 1, 2, 3, 4)$ and $B_{jk} (j, k=1, 2, 3, 4)$. Without loss of generality, we can assume that

$$B_0 = (\infty, 0_1, 0_2, 0_3, 0_4), \quad B_1 = (\infty, 1_1, 1_2, 1_3, 1_4), \quad B_2 = (\infty, 2_1, 2_2, 2_3, 2_4),$$

$$B_3 = (\infty, 3_1, 3_2, 3_3, 3_4), \quad B_4 = (\infty, 4_1, 4_2, 4_3, 4_4), \quad B_{11} = (0_1, 1_1, 2_1, 3_1, 4_1),$$

$$B_{12} = (0_1, 1_2, 2_2, 3_2, 4_2), \quad B_{13} = (0_1, 1_3, 2_3, 3_3, 4_3), \quad B_{14} = (0_1, 1_4, 2_4, 3_4, 4_4)$$

and B_{jk} contains two treatments 0_j and 1_k for $j=2, 3, 4$ and $k=1, 2, 3, 4$. It suffices therefore to consider an arrangement of 12 treatments $(l+1)_i (l=1, 2, 3; i=1, 2, 3, 4)$ into 12 blocks B_{jk} $(j=2, 3, 4; k=1, 2, 3, 4)$.

Since each treatment $(l+1)_i$ must be contained in only one block of four blocks $B_{j1}, B_{j2}, B_{j3}, B_{j4}$ for each $j=1, 2, 3, 4$, we can define 4×4 matrices A_l $(l=1, 2, 3)$ as follows:

$$A_l = \|a_{ij}^{(l)}\|: \qquad i=1, 2, 3, 4 \text{ and } j=1, 2, 3, 4$$

where $a_{ij}^{(l)}=k$ if treatment $(l+1)_i$ is contained in a block B_{jk} of four blocks B_{j1}, B_{j2}, B_{j3}, B_{j4}. Then it is easy to see that (i) the above twenty-one blocks constitute a *BIB* design with parameters (21, 21, 5, 5, 1) if and only if A_1, A_2 and A_3 are 4×4 mutually orthogonal Latin squares and that (ii) two *BIB* designs D_1 and D_2 are isomorphic if and only if the corresponding 4×4 mutually orthogonal Latin squares $\{A_1^{(1)}, A_2^{(1)}, A_3^{(1)}\}$ and $\{A_1^{(2)}, A_2^{(2)}, A_3^{(2)}\}$ are isomorphic, that is, the set $\{A_1^{(2)}, A_2^{(2)}, A_3^{(2)}\}$ can be obtained from the set $\{A_1^{(1)}, A_2^{(1)}, A_3^{(1)}\}$ by permuting the elements 1, 2, 3, 4 in the matrices $A_l^{(1)}$ $(l=1, 2, 3)$ and permuting rows and columns suitably of the matrices $A_l^{(1)}$. It is easy to see that there exist only two nonisomorphic complete sets of 4×4 mutually orthogonal Latin squares as follows:

$$A_1^{(1)} = \begin{bmatrix} 1&2&3&4 \\ 2&1&4&3 \\ 3&4&1&2 \\ 4&3&2&1 \end{bmatrix}, \quad A_2^{(1)} = \begin{bmatrix} 1&3&4&2 \\ 2&4&3&1 \\ 3&1&2&4 \\ 4&2&1&3 \end{bmatrix}, \quad A_3^{(1)} = \begin{bmatrix} 1&4&2&3 \\ 2&3&1&4 \\ 3&2&4&1 \\ 4&1&3&2 \end{bmatrix}$$

and

$$A_1^{(2)} = \begin{bmatrix} 1&2&3&4 \\ 2&3&4&1 \\ 3&4&1&2 \\ 4&1&2&3 \end{bmatrix}, \quad A_2^{(2)} = \begin{bmatrix} 1&3&4&2 \\ 2&4&1&3 \\ 3&1&2&4 \\ 4&2&3&1 \end{bmatrix}, \quad A_3^{(2)} = \begin{bmatrix} 1&4&2&3 \\ 2&1&3&4 \\ 3&2&4&1 \\ 4&3&1&2 \end{bmatrix}$$

The blocks corresponding to the above Latin squares are

$B_{21}^{(1)}=(0_2, 1_1, 2_2, 3_3, 4_4)$, $B_{22}^{(1)}=(0_2, 1_2, 2_1, 3_4, 4_3)$, $B_{23}^{(1)}=(0_2, 1_3, 2_4, 3_1, 4_2)$,

$B_{24}^{(1)}=(0_2, 1_4, 2_3, 3_2, 4_1)$, $B_{31}^{(1)}=(0_3, 1_1, 2_3, 3_4, 4_2)$, $B_{32}^{(1)}=(0_3, 1_2, 2_4, 3_3, 4_1)$,

$B_{33}^{(1)}=(0_3, 1_3, 2_1, 3_2, 4_4)$, $B_{34}^{(1)}=(0_3, 1_4, 2_2, 3_1, 4_3)$, $B_{41}^{(1)}=(0_4, 1_1, 2_4, 3_2, 4_3)$,

$B_{42}^{(1)}=(0_4, 1_2, 2_3, 3_1, 4_4)$, $B_{43}^{(1)}=(0_4, 1_3, 2_2, 3_4, 4_1)$, $B_{44}^{(1)}=(0_4, 1_4, 2_1, 3_3, 4_2)$

and

$B_{21}^{(2)}=(0_2, 1_1, 2_4, 3_3, 4_2)$, $B_{22}^{(2)}=(0_2, 1_2, 2_1, 3_4, 4_3)$, $B_{23}^{(2)}=(0_2, 1_3, 2_2, 3_1, 4_4)$,

$B_{24}^{(2)}=(0_2, 1_4, 2_3, 3_2, 4_1)$, $B_{31}^{(2)}=(0_3, 1_1, 2_3, 3_2, 4_4)$, $B_{32}^{(2)}=(0_3, 1_2, 2_4, 3_3, 4_1)$,

$B_{33}^{(2)}=(0_3, 1_3, 2_1, 3_4, 4_2)$, $B_{34}^{(2)}=(0_3, 1_4, 2_2, 3_1, 4_3)$, $B_{41}^{(2)}=(0_4, 1_1, 2_2, 3_4, 4_3)$,

$B_{42}^{(2)}=(0_4, 1_2, 2_3, 3_1, 4_4)$, $B_{43}^{(2)}=(0_4, 1_3, 2_4, 3_2, 4_1)$, $B_{44}^{(2)}=(0_4, 1_4, 2_1, 3_3, 4_2)$.

Let N_1 and N_2 be the incidence matrices of the above two designs D_1 and D_2, respectively. Then it is easy to see that $\mathrm{Rank}_2(N_1)=10$ and $\mathrm{Rank}_2(N_2)=12$. This completes the proof.

In Section 7, it will be shown that the design D_1 is isomorphic with the *BIB* design PG(2, 4): 1.

(b) Enumeration of nonisomorphic solutions of the design No. 16

THEOREM 6.2. *The BIB design with parameters* (16, 20, 5, 4, 1) *is unique and its 2-rank is equal to* 9.

PROOF. Let us denote sixteen treatments by 0, 1, 2, ..., 15 and twenty blocks by B_0, B_1, ..., B_{19}. Without loss of generality, we can assume that

$$B_0=(0,\ 1,\ 2,\ 3),\quad B_1=(0,\ 4,\ 5,\ 6),\quad B_2=(0, 7,\ 8,\ 9),$$
$$B_3=(0, 10, 11, 12),\quad B_4=(0, 13, 14, 15),\quad B_5=(1, 4,\ 7, 10),$$
$$B_6=(1,\ 5,\ 8, 13),\quad B_7=(1,\ 6, 11, 14),\quad B_8=(1, 9, 12, 15)$$

and B_9, B_{10}, ..., B_{19} contain $\{2, 4\}$, $\{2, 5\}$, $\{2, 6\}$, $\{2\}$, $\{3, 4\}$, $\{3, 5\}$, $\{3, 6\}$, $\{3\}$, $\{4\}$, $\{5\}$, $\{6\}$, respectively. It suffices therefore to consider an arrangement of 9 treatments 7, 8, ..., 15 into 11 blocks $B_i (i=9, 10, ..., 19)$. Let x_i $(i=9, 10, ..., 19)$ be integers such that $x_i=1$ or 0 according as the treatment 7 (or 10) is contained in the block B_i or not. Then, since $\lambda=1$ and $r=5$, x_i's must satisfy the following conditions:

$$\begin{array}{lllllll}
 & x_9+x_{10}+x_{11}+x_{12} & & & & & =1\\
 & & x_{13}+x_{14}+x_{15}+x_{16} & & & & =1\\
(6.1)\quad & x_9 & +x_{13} & & +x_{17} & & =0\\
 & \quad x_{10} & \quad +x_{14} & & & +x_{18} & =1\\
 & \qquad x_{11} & \qquad +x_{15} & & & \qquad +x_{19} & =1\\
 & \multicolumn{6}{l}{x_9+x_{10}+x_{11}+x_{12}+x_{13}+x_{14}+x_{15}+x_{16}+x_{17}+x_{18}+x_{19}=3.}
\end{array}$$

From the above equations, we have the following four solutions:

$$(6.2)\quad \begin{array}{ll}
\boldsymbol{z}_1=(0, 1, 0, 0; 0, 0, 0, 1; 0, 0, 1), & \boldsymbol{z}_3=(0, 0, 0, 1; 0, 1, 0, 0; 0, 0, 1),\\
\boldsymbol{z}_2=(0, 0, 1, 0; 0, 0, 0, 1; 0, 1, 0), & \boldsymbol{z}_4=(0, 0, 0, 1; 0, 0, 1, 0; 0, 1, 0)
\end{array}$$

where $\boldsymbol{z}=(x_9, x_{10}, ..., x_{19})$. It is easy to see that by renaming sixteen treatments and twenty blocks, we can obtain the solutions z_3 and z_4 from the solutions z_1 and z_2, respectively. It suffices therefore to consider two cases z_1 and z_2.

(i) In the case z_1, that is, treatment 7 is contained in blocks B_{10}, B_{16} and B_{19}.

In this case, it follows from (6.1), (6.2) and $x_{10}=x_{16}=x_{19}=0$ that treatment 10 must be contained in blocks B_{12}, B_{15} and B_{18}. Using a similar method, it is shown that treatment 8 must be contained in blocks B_{12}, B_{15} and B_{17}. This contradicts $\lambda=1$, since there exist two blocks B_{12} and B_{15} which contain two treatments 8 and 10. Hence, there does not exist such a design.

(ii) In the case z_2, that is, treatment 7 is contained in blocks B_{11}, B_{16} and B_{18}.

In this case, it follows from (6.1), (6.2) and $x_{11}=x_{16}=x_{18}=0$ that treatment 10 must be contained in blocks B_{12}, B_{14} and B_{19}.

Let y_j $(j=9, 10, \dots, 19)$ be integers such that $y_j=1$ or 0 according as the treatment 8 is contained in the block B_j or not. Then y_j's must satisfy the following conditions:

$$
\begin{array}{lllllllllllll}
y_9+y_{10}+y_{11}+y_{12} & & & & & & & & & & &=1\\
& & & & y_{13}+y_{14}+y_{15}+y_{16} & & & & & & &=1\\
y_9 & & & & +y_{13} & & & & +y_{17} & & &=1\\
& y_{10} & & & & +y_{14} & & & & +y_{18} & &=0\\
& & y_{11} & & & & +y_{15} & & & & +y_{19}&=1\\
& & y_{11} & & & & & +y_{16} & & +y_{18} & &=0\\
& & & y_{12} & & +y_{14} & & & & & +y_{19}&=1\\
\multicolumn{12}{l}{y_9+y_{10}+y_{11}+y_{12}+y_{13}+y_{14}+y_{15}+y_{16}+y_{17}+y_{18}+y_{19}=3.}
\end{array}
\tag{6.3}
$$

From the above equations, we have the following unique solution:

$$(y_9, y_{10}, \dots, y_{19})=(0, 0, 0, 1; 0, 0, 1, 0; 1, 0, 0).$$

This implies that treatment 8 must be contained in blocks B_{12}, B_{15} and B_{17}. Similarly, we can construct the design, step by step, and we have the following unique solution:

$$
\begin{array}{lll}
B_9 =(2, 4, 12, 13), & B_{10}=(2, 5, 9, 11), & B_{11}=(2, 6, 7, 15),\\
B_{12}=(2, 8, 10, 14), & B_{13}=(3, 4, 9, 14), & B_{14}=(3, 5, 10, 15),\\
B_{15}=(3, 6, 8, 12), & B_{16}=(3, 7, 11, 13), & B_{17}=(4, 8, 11, 15),\\
B_{18}=(5, 7, 12, 14), & B_{19}=(6, 9, 10, 13). &
\end{array}
$$

Since the design EG(2, 4): 1 is a *BIB* design with parameters (16, 20, 5, 4, 1), it follows from the uniqueness of the design that any *BIB* design with parameters (16, 20, 5, 4, 1) is isomorphic with the design EG(2, 4): 1. In Section 9, it is shown that the 2-rank of the incidence matrix of the design EG(2, 4): 1 is equal to 9. Hence, we have the required result.

Using a similar method, it can be shown that the *BIB* design No. 18 is also unique and any *BIB* design with parameters (25, 30, 6, 5, 1) is isomorphic with the design EG(2, 5): 1.

(c) Table of nonisomorphic solutions and their p-ranks

Nonisomorphic solutions of *BIB* designs in Table 6.1 and their p-ranks are given in Table 6.2. The notations used are coincident with those generally used for cyclic solutions. For noncyclic solutions, treatments are represented by a, b, c, ..., and so on. In Table 6.2 (or Table 6.1), if designs D_1 and D_2 are nonisomorphic, their p-ranks are different except for designs Nos. 6, 8, 12 and 13. In Sections 7 and 9, it will be shown that the designs D_1 of Nos. 4, 13 and 17 are isomorphic with EG(3, 2): 2, PG(3, 2): 2 and PG(2, 4): 1, respectively. These designs have the minimum p-ranks. This suggests that the p-rank of the *BIB* design PG(t, q): μ or EG(t, q): μ might be, in general, minimum in *BIB* designs with the same parameters.

In Part II, we shall investigate the p-ranks of the incidence matrices of the *BIB* designs PG(t, q): μ and EG(t, q): μ.

TABLE 6.2.

NONISOMORPHIC SOLUTIONS AND THEIR P–RANKS

No.	v r λ	no. of noniso.	p	rank	nonisomorphic solutions
1	6 5 2	1	3	5	(∞, 1, 4), (0, 1, 4) mod 5
2	7 3 1	1	2	4	(0, 1, 3) mod 7
3	7 4 2	1	2	3	(2, 4, 5, 6) mod 7
4	8 7 3	4	2	4	D_1: abdh, bceh, cdfh, degh, efah, fgbh, gach, cefg, dfga, egab, fabc, gbcd, acde, bdef
				5	D_2: abcd, abef, abgh, efgh, cdgh, cdef, aceg, bdeg, bdeh, aceh, adfg, adfh, bcfg, bcfh
				6	D_3: abcd, efgh, abef, adef, abgh, adgh, aceg, cdeg, acfh, cdfh, bceh, bdeh, bcfg, bdfg

TABLE 6.2. (continued)

No.	v r λ	no. of noniso.	p	rank	nonisomorphic solutions
				7	D_4: abdh, bceh, cdfh, degh, efah, fgbh, gach, bceg, fgca, eagd, cdab, gbdf, afbe, defc
5	9 4 1	1	3	6	(∞, 0, 4) $PC(4)$, (0, 2, 7) mod 8
6	9 8 3	—	5	—	—
7	10 6 2	3	2	5	D_1: abcd, abef, acgh, adij, bcij, bdgh, cdef, aegi, afhj, behj, bfgi, cehi, cfgj, degj, dfhi
				6	D_2: abcd, abef, aceg, adhi, bchi, bdgj, cdfj, afhj, agij, behj, bfgi, ceij, cfgh, defi, degh
				7	D_3: abcd, abef, aceg, adhi, bcij, bdgh, cdfj, afhj, agij, behj, bfgi, cehi, cfgh, defi, degj
8	10 9 2	—	7	—	—
9	11 5 2	1	3	6	(0, 1, 2, 4, 7) mod 11
10	11 6 3	1	3	5	(3, 5, 6, 8, 9, 10) mod 11
11	13 4 1	1	3	7	(0, 1, 5, 11) mod 13
12	13 6 1	2	5	13	D_1: (0, 2, 8), (1, 4, 5) mod 13
				13	D_2: abc, ade, afg, ahi, ajk, alm, bdf, beg, bhj, bil, bkm, cdh, cei, cfj, cgm, ckl, dgk, dim, djl, efl, ehk, ejm, fhm, fik, ghl, gij
13	15 7 3	5	2	5	D_1: abcdijk, abefilm, abghino, acegjln, acfhjmo, adehklo, adfgkmn, bcehkmn, bcfgklo, bdegjmo, bdfhjln, cdefino, cdghilm, efghijk, ijklmno
				6	D_2: abcdijk, abcelmn, abfgjmo, acfhklo, adefino, adghilm, aeghjkn, bcghino, bdegklo, bdfhkmn, befhijl, cdehjmo, cdfgjln, cefgikm, ijklmno
				8	D_3: abcdijk, abcelmn, abfgjmo, acghilo, adefklo, adfhimn, aeghjkn, bcfhkno, bdegino, bdghklm, befhijl, cdehjmo, cdfgjln, cefgikm, ijklmno

TABLE 6.2. (continued)

No.	v r λ	no. of noniso.	p	rank		nonisomorphic solutions
				8	D_4:	abcdijk, abcelmn, abfgjmo, acghkno, adefklo, adfhimn, aeghijl, bcfhilo, bdegino, bdghklm, befhjkn, cdehjmo, cdfgjln, cefgikm, ijklmno
				8	D_5:	abcdijk, abcelmn, abfgimo, acghkno, adefklo, adfhjmn, aeghijl, bcfhjlo, bdehino, bdghklm, befgjkn, cdegjmo, cdfgiln, cefhikm, ijklmno
14	15 7 2	0	5	—		non-existence
15	16 6 2	3	2	6	D_1:	abcdef, abghij, acgklm, adhkno, aeilnp, afjmop, bcgnop, bdhlmp, beikmo, bfjkln, cdijkp, cehjlo, cfhimn, degjmn, dfgilo, efghkp
				7	D_2:	abcdef, abghij, achklm, adilno, aejknp, afgmop, bcgkno, bdikmp, bejlmo, bfhlnp, cdgjlp, cehiop, cfijmn, deghmn, dfhjko, efgikl
				8	D_3:	abcdef, abghij, achklm, adikno, aejlop, afgmnp, bcgkop, bdilmp, bejkmn, bfhlno, cdgjln, cehinp, cfijmo, deghmo, dfhjkp, efgikl
16	16 5 1	1	2	9		$(\infty, 0, 5, 10)$ $PC(5)$,$(0, 4, 12, 13)$ mod 15
17	21 5 1	2	2	10	D_1:	abcde, afghi, ajklm, anopq, arstu, bfjnr, bgkos, bhlpt, bimqu, cfkpu, cgjqt, chmns, cilor, dflqs, dgmpr, dhjou, diknt, efmot, eglnu, ehkqr, eijps
				12	D_2:	abcde, afghi, ajklm, anopq, arstu, bfjnr, bgkos, bhlpt, bimqu, cfmps, cgjqt, chknu, cilor, dflou, dgmpr, dhjqs, diknt, efkqt, eglnu, ehmor, eijps
18	25 6 1	1	5	15		$(\infty, 0, 6, 12, 18)$ $PC(6)$, $(0, 8, 17, 21, 22)$ mod 24

Part II. The p-rank of the incidence matrix of a *BIB* design derived from a finite geometry

7. The p-rank of the incidence matrix of points and μ-flats in PG(t, q)

With the help of the Galois field GF(q), where q is an integer of the form p^m (p being a prime), we can define a finite projective geometry PG(t, q) of t dimensions as a set of points satisfying the following conditions:

(i) A point in PG(t, q) is represented by (v) where v is a nonzero element of GF(q^{t+1}).

(ii) Two points (v_1) and (v_2) represent the same point when and only when there exists a nonzero element σ of GF(q) such that $v_1=\sigma v_2$.

(iii) A μ-flat, $0\leqq\mu\leqq t$, in PG(t, q) is defined as a set of points

$$\{(a_0v_0+a_1v_1+\cdots+a_\mu v_\mu)\}$$

where a's run independently over the elements of GF(q) and are not all simultaneously zero and (v_0), (v_1), ..., (v_μ) are linearly independent over the coefficient field GF(q), in other words, they do not lie on a $(\mu-1)$-flat. In GF(q^{t+1}), there exists an element α called primitive such that every nonzero element of GF(q^{t+1}) can be represented by α^u ($u=0, 1, ..., q^{t+1}-2$). It satisfies an irreducible equation of degree $t+1$ with coefficients from GF(q):

$$\alpha^{t+1}+a_t^*\alpha^t+\cdots+a_1^*\alpha+a_0^*=0 \tag{7.1}$$

and $\alpha^{q^{t+1}-1}=1$. Using (7.1), every nonzero element α^u $(0\leqq u\leqq q^{t+1}-2)$ of GF(q^{t+1}) can also be represented uniquely by a polynomial in α, of degree at most t, with coefficients from GF(q). Thus, every nonzero element of GF(q^{t+1}) may be represented either as a power of the primitive element α or as a polynomial in α, of a degree at most t, with coefficients from GF(q). If

$$\alpha^u=b_t\alpha^t+b_{t-1}\alpha^{t-1}+\cdots+b_1\alpha+b_0, \tag{7.2}$$

then the correspondence

$$\alpha^u\leftrightarrow(b_t, b_{t-1}, ..., b_0) \quad \text{and} \quad 0\leftrightarrow(0, 0, ..., 0) \tag{7.3}$$

induces a vector space structure on GF(q^{t+1}) over GF(q) and the elements α^0 $(=1)$, α^1, α^2, ..., α^t form a basis for GF(q^{t+1}).

Every point in PG(t, q) is represented by (α^0), (α^1), (α^2), ..., (α^{v-1}) and a μ-flat may be defined as the set of points

$$\{(a_0\alpha^{e_0}+a_1\alpha^{e_1}+\cdots+a_\mu\alpha^{e_\mu})\}$$

where $v=(q^{t+1}-1)/(q-1)$ and α^{e_0}, α^{e_1}, ..., α^{e_μ} are $\mu+1$ linearly independent elements of $\mathrm{GF}(q^{t+1})$ over $\mathrm{GF}(q)$ and $a_0, a_1, \dots, a_\mu$ run independently over the elements of $\mathrm{GF}(q)$, not all zero. In the following, we shall call such a set of points $(\alpha^{e_0}), (\alpha^{e_1}), \dots, (\alpha^{e_\mu})$ the defining points of the μ-flat and denote the empty set by (-1)-flat for convenience' sake. It is well known [8] that the number, b, of μ-flats in $\mathrm{PG}(t, q)$ is equal to $\phi(t, \mu, q)$ where

$$\phi(t, \mu, q) = \frac{(q^{t+1}-1)\ (q^t-1)\cdots(q^{t-\mu+1}-1)}{(q^{\mu+1}-1)\ (q^\mu-1)\cdots(q-1)} \tag{7.4}$$

for any integers t and μ such that $0 \leqq \mu \leqq t$. For convenience' sake, we make a promise that $\phi(t, -1, q)=1$ for $t \geqq -1$ and $\phi(t, \mu, q)=0$ for t and μ such that $t<\mu$ or $\mu \leqq -2$.

After numbering b μ-flats in $\mathrm{PG}(t, q)$ in some way, we define the incidence matrix of v points and b μ-flats in $\mathrm{PG}(t, q)$ to be the matrix:

$$N(q;\, t, \mu) = \|n_{ij}(q;\, t, \mu)\|;\ i=0, 1, \dots, v-1 \text{ and } j=1, 2, \dots, b$$

where $n_{ij}(q;\, t, \mu)=1$ or 0 according as the ith point (α^i) is incident with the jth μ-flat or not. In the following, $N(q;\, t, \mu)$ may also be denoted by $N(p^m;\, t, \mu)$ where $q=p^m$. It is known [2] that $N(q;\, t, \mu)$ is the incidence matrix of a *BIB* design, denoted by $\mathrm{PG}(t, q)$: μ, with parameters:

$$\begin{gathered} v=(q^{t+1}-1)/(q-1), \quad b=\phi(t, \mu, q), \quad r=\phi(t-1, \mu-1, q), \\ k=(q^{\mu+1}-1)/(q-1) \quad \text{and} \quad \lambda=\phi(t-2, \mu-2, q). \end{gathered} \tag{7.5}$$

In this case, we have

$$r-\lambda = q^\mu \phi(t-2, \mu-1, q) \text{ and } \delta=[r/2\lambda]=[(q^t-1)/2(q^\mu-1)]. \tag{7.6}$$

It is therefore necessary to investigate the q-rank and the p^*-rank of $N(q;\, t, \mu)$ where p^* is a prime which is a factor of $\phi(t-2, \mu-1, q)$.

The q-rank of $N(q;\, t, \mu)$ has been investigated by many authors [10], [11], [30], [31], [32] and the complete solution for this problem has been obtained by the present author [12]. The result is as follows:

THEOREM 7.1. *The q-rank of the incidence matrix $N(q;\, t, \mu)$ of v points and b μ-flats in $\mathrm{PG}(t, q)$ is equal to*

$$R_\mu(t, p^m) = \sum_{(s_0^*, \dots, s_m^*)} \prod_{j=0}^{m-1} \sum_{i=0}^{L(s_{j+1}^*, s_j^*)} (-1)^i \binom{t+1}{i} \binom{t+s_{j+1}^* p - s_j^* - ip}{t} \tag{7.7}$$

where $q=p^m$ and summation is taken over all ordered sets $(s_0^*, s_1^*, \dots, s_m^*)$, denoted by $S_{t,\mu}^*(p^m)$, of $m+1$ integers s_l^* $(l=0, 1, \dots, m)$ such that

$$s_m^* = s_0^*,\ \mu+1 \leqq s_j^* \leqq t+1 \ \textit{and}\ 0 \leqq s_{j+1}^* p - s_j^* \leqq (t+1)\,(p-1) \tag{7.8}$$

for each $j=0, 1, \ldots, m-1$ *and* $L(s^*_{j+1}, s^*_j)=[(s^*_{j+1}p-s^*_j)/p]$, *that is,* $L(s^*_{j+1}, s^*_j)$ *is the greatest integer not exceeding* $(s^*_{j+1}p-s^*_j)/p$.

From Theorem 7.1, we have the following theorem which may be useful in calculating the value of $R_\mu(t, p^m)$.

THEOREM 7.2. *The q-rank of* $N(q; t, \mu)$ *is also equal to*

$$R_\mu(t, p^m)=\sum_{(s_0,\ldots,s_m)}\prod_{j=0}^{m-1}\sum_{i=0}^{L(s_{j+1},s_j)}(-1)^i\binom{t+1}{i}\binom{t+s_{j+1}p-s_j-ip}{t} \tag{7.9}$$

where $q=p^m$ *and summation is taken over all ordered sets* $(s_0, s_1, \ldots, s_m)$, *denoted by* $S_{t,\mu}(p^m)$, *of* $m+1$ *integers* s_l $(l=0, 1, \ldots, m)$ *such that*

$$s_m=s_0,\ 0\leqq s_j\leqq t-\mu \text{ and } 0\leqq s_{j+1}p-s_j\leqq(t+1)(p-1) \tag{7.10}$$

for each $j=0, 1, \ldots, m-1$.

PROOF. Let s_l and s^*_l $(l=0, 1, \ldots, m)$ be any non-negative integers such that $s_l+s^*_l=t+1$. Then we can see that the ordered set $(s^*_0, s^*_1, \ldots, s^*_m)$ belongs to $S^*_{t,\mu}(p^m)$ if and only if the corresponding ordered set $(s_0, s_1, \ldots, s_m)$ belongs to $S_{t,\mu}(p^m)$. Since both the coefficients of x^u and $x^{(p-1)(t+1)-u}$ of the (real) expansion of $(1+x+x^2+\cdots+x^{p-1})^{t+1}$ are equal to $\sum_{i=0}^{[u/p]}(-1)^i\binom{t+1}{i}\binom{t+u-ip}{t}$ and $s^*_{j+1}p-s^*_j=(p-1)(t+1)-(s_{j+1}p-s_j)$ for $j=0, 1, \ldots, m-1$, it follows that

$$\sum_{i=0}^{L(s^*_{j+1},s^*_j)}(-1)^i\binom{t+1}{i}\binom{t+s^*_{j+1}p-s^*_j-ip}{t}$$
$$=\sum_{i=0}^{L(s_{j+1},s_j)}(-1)^i\binom{t+1}{i}\binom{t+s_{j+1}p-s_j-ip}{t}$$

for each $j=0, 1, \ldots, m-1$. Hence, we get the required result from Theorem 7.1.

COROLLARY 7.3. *For any positive integer n, the rank of* $N(p^m; t, \mu)$ *over* GF(p^n) is equal to $R_\mu(t, p^m)$.

PROOF. It is well known that if each entry of a matrix N is an element of GF(p), the rank of N over GF(p^n) is equal to its rank over GF(p) for any positive integer n. Since each entry of the matrix $N(q; t, \mu)$ is 0 or 1, it follows that the p-rank of $N(q; t, \mu)$ is equal to the q-rank where $q=p^m$. Hence, we have the required result.

In the special case $\mu=t-1$, since $S_{t,t-1}(p^m)=\{(0, 0, \ldots, 0), (1, 1, \ldots, 1)\}$, we have the following corollary:

COROLLARY 7.4. *The p-rank of the incidence matrix* $N(p^m; t, t-1)$ *of v points and v hyperplanes* ($(t-1)$*-flats*) *in* PG(t, p^m) *is equal to*

$$R_{t-1}(t, p^m)=\binom{t+p-1}{t}^m+1. \tag{7.11}$$

In the case $t=2$, this result has been obtained by Graham and MacWilliams [11] and, for general t, was conjectured by Rudolph [30] to be true and has been independently obtained by Smith [31, 32] and by Goethals and Delsarte [10].

COROLLARY 7.5. *In the special case $q=p$ (i.e., $m=1$), the p-rank of the incidence matrix $N(p; t, \mu)$ of v points and b μ-flats in* PG(t, p) *is equal to*

$$R_\mu(t, p)=\sum_{s=0}^{t-\mu}\sum_{i=0}^{L(s,s)}(-1)^i\binom{t+1}{i}\binom{t+s(p-1)-ip}{t} \tag{7.12}$$

where $L(s, s)$ is the greatest integer not exceeding $s(p-1)/p$.

This result has been obtained by Smith [31].

COROLLARY 7.6. *In the special case $q=2$, the 2-rank of the incidence matrix $N(2; t, \mu)$ is equal to $R_\mu(t, 2)=\sum_{s=0}^{t-\mu}\binom{t+1}{s}$.*

Table 7.1 gives all solutions for *BIB* designs PG(t, p^m): μ with $7\leqq v\leqq 50$ and their p-ranks where $v=(p^{m(t+1)}-1)/(p^m-1)$. These solutions are obtained by using the cyclic structure of μ-flats [27, 36] and tables due to Alanen and Knuth [1].

In the case $\phi(t-2, \mu-1, q)\geqq 2$, it is also necessary to investigate the p^*-rank of $N(p^m; t, \mu)$ for a prime p^* which is a factor of $\phi(t-2, \mu-1, q)$. In Table 7.1, there are four designs (Nos. 4, 8, 9, 11) satisfying the above condition and their p^*-ranks are given in Table 7.2 which suggests that the p^*-rank of $N(p^m; t, \mu)$ might, in general, be equal to $v-1$ or v. Their p^*-ranks are computed by the usual method.

Table 7.3 gives the p-ranks of the incidence matrices $N(p^m; t, \mu)$ for all *BIB* designs PG(t, p^m): μ with parameters satisfying the following conditions:

$$p=2, 3, 5, 7;\ 1\leqq m\leqq 5,\ \ 1\leqq\mu<t \ \text{ and } \ 50<v<10000$$

where

$$v=(p^{m(t+1)}-1)/(p^m-1) \ \text{ and } \ \delta=[r/2\lambda]=[(q^t-1)/2(q^\mu-1)].$$

Comparing the p-ranks of designs Nos. 13 and 17 in Table 6.2 and the p-ranks of designs Nos. 3 and 5 in Table 7.1, respectively, we can see that the design D_1 of No. 13 in Table 6.2 is isomorphic with the design PG(3, 2): 2 and the design D_1 of No. 17 in Table 6.2 is isomorphic with the design PG(2, 4): 1.

TABLE 7.1.
BIB DESIGNS PG(t, p^m): μ AND THEIR P–RANKS

No.	v	b	r	k	λ	p-rank	δ	p^m	t	μ	PG(t, p^m):μ
1	7	7	3	3	1	4	1	2	2	1	(0, 1, 5) mod 7
2	13	13	4	4	1	7	2	3	2	1	(0, 1, 5, 11) mod 13
3	15	15	7	7	3	5	1	2	3	2	(0, 1, 2, 7, 9, 12, 13) mod 5
4	15	35	7	3	1	11	3	2	3	1	(0, 1, 12), (0, 2, 9) mod 15 (0, 5, 10) PC(5)
5	21	21	5	5	1	10	2	4	2	1	(0, 1, 4, 14, 16) mod 21
6	31	31	6	6	1	16	3	5	2	1	(0, 1, 6, 18, 22, 29) mod 31
7	31	31	15	15	7	6	1	2	4	3	(0, 1, 2, 3, 5, 7, 11, 14, 15, 16, 22, 23, 26, 28, 29) mod 31
8	31	155	35	7	7	16	2	2	4	2	(0, 1, 2, 14, 15, 22, 28), (0, 1, 3, 5, 14, 26, 29), (0, 1, 4, 6, 10, 14, 25), (0, 4, 7, 9, 16, 24, 25), (0, 8, 11, 13, 19, 23, 30) mod 31
9	31	155	15	3	1	26	7	2	4	1	(0, 1, 14), (0, 2, 28), (0, 4, 25), (0, 7, 16), (0, 8, 19) mod 31
10	40	40	13	13	4	11	1	3	3	2	(0, 1, 2, 8, 16, 18, 23, 25, 28, 29, 34, 37, 38) mod 40
11	40	130	13	4	1	30	6	3	3	1	(0, 1, 28, 37), (0, 2, 18, 25), (0, 5, 11, 19) mod 40 (0, 10, 20, 30) PC(10)

TABLE 7.2.
THE p^*-RANK OF BIB DESINGS PG(t, p^m):μ

No.	v	b	r	k	λ	p^*	p^*-rank	No.	v	b	r	k	λ	p^*	p^*-rank
4	15	35	7	3	1	3	14	9	31	155	15	3	1	7	31
8	31	155	35	7	7	7	30	11	40	130	13	4	1	2	39

TABLE 7.3.

THE P–RANK OF BIB DESINGS PG(t, p^m):μ

No.	v	p-rank	δ	p^m	t	μ	No.	v	p-rank	δ	p^m	t	μ
12	57	29	4	7	2	1	43	364	253	15	3	5	2
13	63	7	1	2	5	4	44	364	343	60	3	5	1
14	63	22	2	2	5	3	45	400	85	3	7	3	2
15	63	42	5	2	5	2	46	400	316	28	7	3	1
16	63	57	15	2	5	1	47	511	10	1	2	8	7
17	73	28	4	8	2	1	48	511	46	2	2	8	6
18	85	17	2	4	3	2	49	511	130	4	2	8	5
19	85	61	10	4	3	1	50	511	256	8	2	8	4
20	91	37	5	9	2	1	51	511	382	18	2	8	3
21	121	16	1	3	4	3	52	511	466	42	2	8	2
22	121	61	5	3	4	2	53	511	502	127	2	8	1
23	121	106	20	3	4	1	54	585	65	4	8	3	2
24	127	8	1	2	6	5	55	585	401	36	8	3	1
25	127	29	2	2	6	4	56	651	226	13	25	2	1
26	127	64	4	2	6	3	57	757	217	14	27	2	1
27	127	99	10	2	6	2	58	781	71	2	5	4	3
28	127	120	31	2	6	1	59	781	391	13	5	4	2
29	156	36	2	5	3	2	60	781	711	78	5	4	1
30	156	121	15	5	3	1	61	820	101	4	9	3	2
31	255	9	1	2	7	6	62	820	590	45	9	3	1
32	255	37	2	2	7	5	63	1023	11	1	2	9	8
33	255	93	4	2	7	4	64	1023	56	2	2	9	7
34	255	163	9	2	7	3	65	1023	176	4	2	9	6
35	255	219	21	2	7	2	66	1023	386	8	2	9	5
36	255	247	63	2	7	1	67	1023	638	17	2	9	4
37	273	82	8	16	2	1	68	1023	848	36	2	9	3
38	341	26	2	4	4	3	69	1023	968	85	2	9	2
39	341	146	8	4	4	2	70	1023	1013	255	2	9	1
40	341	296	42	4	4	1	71	1057	244	16	32	2	1
41	364	22	1	3	5	4	72	1093	29	1	3	6	5
42	364	112	4	3	5	3	73	1093	190	4	3	6	4

TABLE 7.3. (continued)

No.	v	p-rank	δ	p^m	t	μ	No.	v	p-rank	δ	p^m	t	μ
74	1093	547	14	3	6	3	106	4095	299	4	2	11	8
75	1093	904	45	3	6	2	107	4095	794	8	2	11	7
76	1093	1065	182	3	6	1	108	4095	1586	16	2	11	6
77	1365	37	2	4	5	4	109	4095	2510	33	2	11	5
78	1365	302	8	4	5	3	110	4095	3302	68	2	11	4
79	1365	882	34	4	5	2	111	4095	3797	146	2	11	3
80	1365	1289	170	4	5	1	112	4095	4017	341	2	11	2
81	2047	12	1	2	10	9	113	4095	4083	1023	2	11	1
82	2047	67	2	2	10	8	114	4369	257	8	16	3	2
83	2047	232	4	2	10	7	115	4369	2801	136	16	3	1
84	2047	562	8	2	10	6	116	4681	126	4	8	4	3
85	2047	1024	16	2	10	5	117	4681	1576	32	8	4	2
86	2047	1486	34	2	10	4	118	4681	4091	292	8	4	1
87	2047	1816	73	2	10	3	119	5461	50	2	4	6	5
88	2047	1981	170	2	10	2	120	5461	561	8	4	6	4
89	2047	2036	511	2	10	1	121	5461	2276	32	4	6	3
90	2451	785	25	49	2	1	122	5461	4397	136	4	6	2
91	2801	211	3	7	4	3	123	5461	5342	682	4	6	1
92	2801	1401	25	7	4	2	124	6643	1297	41	81	2	1
93	2801	2591	200	7	4	1	125	7381	226	4	9	4	3
94	3280	37	1	3	7	6	126	7381	2761	41	9	4	2
95	3280	303	4	3	7	5	127	7381	6616	410	9	4	1
96	3280	1087	13	3	7	4	128	8191	14	1	2	12	11
97	3280	2194	42	3	7	3	129	8191	92	2	2	12	10
98	3280	2978	136	3	7	2	130	8191	378	4	2	12	9
99	3280	3244	546	3	7	1	131	8191	1093	8	2	12	8
100	3906	127	2	5	5	4	132	8191	2380	16	2	12	7
101	3906	1078	12	5	5	3	133	8191	4096	32	2	12	6
102	3906	2829	65	5	5	2	134	8191	5812	66	2	12	5
103	3906	3780	390	5	5	1	135	8191	7099	136	2	12	4
104	4095	13	1	2	11	10	136	8191	7814	292	2	12	3
105	4095	79	2	2	11	9	137	8191	8100	682	2	12	2

TABLE 7.3. (continued)

No.	v	p-rank	δ	p^m	t	μ	No.	v	p-rank	δ	p^m	t	μ
138	8191	8178	2047	2	12	1	142	9841	4921	41	3	8	4
139	9841	46	1	3	8	7	143	9841	7828	126	3	8	3
140	9841	460	4	3	8	6	144	9841	9382	410	3	8	2
141	9841	2014	13	3	8	5	145	9841	9796	1640	3	8	1

8. The p-rank of the incidence matrix of points and certain sets in PG(t, q)

Let us denote $\phi(t, \mu, q)$ μ-flats in PG(t, q) by $V_l(t, \mu)$ $(l=0, 1, \dots, \phi(t, \mu, q)-1)$ and let $W_{\eta l+k}(t, \mu, \nu)$ $(k=0, 1, \dots, \eta-1)$ be $\eta=\phi(\mu, \nu, q)$ ν-flats contained in the μ-flat $V_l(t, \mu)$ where t, μ and ν are any integers such that $0<\nu<\mu\leqq t$ and $q=p^m$. Let $U_{\eta l+k}(t, \mu, \nu)$ be the set of points obtained from the μ-flat $V_l(t, \mu)$ by deleting all points which are contained in the ν-flat $W_{\eta l+k}(t, \mu, \nu)$ and we define the incidence matrix of $v=(q^{t+1}-1)/(q-1)$ points (α^i) and $b=\phi(t, \mu, q)\phi(\mu, \nu, q)$ sets $U_j(t, \mu, \nu)$ in PG(t, q) to be the matrix:

$$N(q;\, t, \mu, \nu)=\|n_{ij}(q;\, t, \mu, \nu)\|;\ i=0, 1, \dots, v-1 \text{ and } j=0, 1, \dots, b-1$$

where $n_{ij}(q;\, t, \mu, \nu)=1$ or 0 according as the ith point (α^i) is contained in the jth set $U_j(t, \mu, \nu)$ or not, and α is a primitive element of GF(q^{t+1}). It is easy to see that $N(q;\, t, \mu, \nu)$ is the incidence matrix of a *BIB* design with the following parameters:

$$(8.1)\quad \begin{aligned} &v=(q^{t+1}-1)/(q-1), \qquad b=\phi(t, \mu, q)\phi(\mu, \nu, q),\\ &r=\phi(t-1, \mu-1, q)\{\phi(\mu, \nu, q)-\phi(\mu-1, \nu-1, q)\},\\ &k=(q^{\mu+1}-q^{\nu+1})/(q-1),\\ &\lambda=\phi(t-2, \mu-2, q)\ \{\phi(\mu, \nu, q)-2\phi(\mu-1, \nu-1, q)+\phi(\mu-2, \nu-2, q)\}. \end{aligned}$$

In this case, we have

$$(8.2)\qquad \delta=[r/2\lambda]=[(q^{t+1}-q)/2(q^{\mu+1}-q^{\nu+1}-q+1)]$$

and

$$(8.3)\qquad \begin{aligned} r-\lambda=q^{\nu}\{&q^{\mu+1}\phi(t-2, \mu-1, q)\phi(\mu-1, \nu, q)\\ &+\phi(t-2, \mu-2, q)\phi(\mu-2, \nu-1, q)\}. \end{aligned}$$

So, it is necessary to investigate the p-rank and the p^*-rank of the incidence matrix of $N(p^m;\ t,\ \mu,\ \nu)$ where p^* is a prime which is a factor of $\{q^{\mu+1}\phi(t-2,\ \mu-1,\ q)\phi(\mu-1,\ \nu,\ q)+\phi(t-2,\ \mu-2,\ q)\phi(\mu-2,\ \nu-1,\ q)\}$.

In the special case $\mu=t$, $N(q;\ t,\ t,\ \nu)$ is the incidence matrix of a *BIB* design with parameters:

$$
\begin{aligned}
&v=(q^{t+1}-1)/(q-1), \qquad b=\phi(t,\ \nu,\ q),\\
(8.4)\qquad &r=b-\phi(t-1,\ \nu-1,\ q), \qquad k=v-(q^{\nu+1}-1)/(q-1),\\
&\lambda=b-2\phi(t-1,\ \nu-1,\ q)+\phi(t-2,\ \nu-2,\ q)
\end{aligned}
$$

and it is the complement matrix of $N(q;\ t,\ \nu)$.

To obtain the p-rank of $N(q;\ t,\ \mu,\ \nu)$, we prepare the

LEMMA 8.1. *Let $\mathscr{R}_p(N)$ be the vector space over* GF(p) *which is generated by column vectors of the matrix N. Then,*

$$\text{(i)}\qquad J_v\in\mathscr{R}_p(N(q;\ t,\ \mu)),\qquad J_v\notin\mathscr{R}_p(N(q;\ t,\ \mu,\ \nu))$$

and

$$\text{(ii)}\qquad \mathscr{R}_p([J_v\colon N(q;\ t,\ \mu,\ \nu)])=\mathscr{R}_p(N(q;\ t,\ \nu))$$

for any integers t, μ and ν such that $0<\nu<\mu\leqq t$ where $q=p^m$ and J_v is the column vector of order v whose elements are all unity.

PROOF. (i) Since $N(q;\ t,\ \nu)$ is the incidence matrix of a *BIB* design with parameter $r=\phi(t-1,\ \nu-1,\ q)$ and $\phi(t-1,\ \nu-1,\ q)$ is not a multiple of p, it follows from $\sum_{j=1}^{b} n_{ij}(q;\ t,\ \nu)=r\ (i=0,\ 1,\ \ldots,\ v-1)$ that $J_v\in\mathscr{R}_p(N(q;\ t,\ \nu))$.

Since $N(q;\ t,\ \mu,\ \nu)$ is the incidence matrix of a *BIB* design with parameter $k=q^{\nu+1}(q^{\mu-\nu}-1)/(q-1)$, it follows from $\sum_{i=0}^{v-1} n_{ij}(q;\ t,\ \mu,\ \nu)=k\ (j=1,\ 2,\ \ldots,\ b)$ that $N(q;\ t,\ \mu,\ \nu)^TJ_v\equiv 0 \bmod p$. This implies that any vector which belongs to $\mathscr{R}_p(N(q;\ t,\ \mu,\ \nu))$ is orthogonal to J_v. On the other hand, it follows from $v=(q^{t+1}-1)/(q-1)$ that

$$J_v^TJ_v=(q^{t+1}-1)/(q-1)\not\equiv 0 \bmod p.$$

This implies that $J_v\notin\mathscr{R}_p(N(q;\ t,\ \mu,\ \nu))$.

(ii) At first, we shall prove that

$$\text{(8.5)}\qquad \mathscr{R}_p([J_v\colon N(q;\ t,\ \mu,\ \nu)])\subset\mathscr{R}_p(N(q;\ t,\ \nu)).$$

Since $J_v\in\mathscr{R}_p(N(q;\ t,\ \nu))$, it suffices to show that any column vector of $N(q;\ t,\ \mu,\ \nu)$ belongs to $\mathscr{R}_p(N(q;\ t,\ \nu))$. Let $\boldsymbol{x}$ be any column vector of $N(q;\ t,\ \mu,\ \nu)$ where $\boldsymbol{x}^T=(x_0,\ x_1,\ \ldots,\ x_{v-1})$. Then, there exist a unique μ-flat V and a unique ν-flat W_1 contained in the μ-flat V such that $x_i=1$ or 0 according as the ith point (α^i)

is contained in $V-W_1$ or not. Let us denote $\eta=\phi(\mu, \nu, q)$ ν-flats contained in the μ-flat V by W_j $(j=1, 2, \ldots, \eta)$ and let z_j $(j=1, 2, \ldots, \eta)$ be column vectors of $N(q; t, \nu)$ such that $z_{ij}=1$ or 0 according as the ith point (α^i) is incident with the ν-flat W_j or not, where $\boldsymbol{z}_j^T=(z_{0j}, z_{1j}, \ldots, z_{v-1j})$. Then it follows that

$$\boldsymbol{x}\equiv c_1 \sum_{j=1}^{\eta} \boldsymbol{z}_j-\boldsymbol{z}_1 \mod p$$

where c_1 is a positive integer less than p such that

$$c_1\phi(\mu-1, \nu-1, p^m)\equiv 1 \mod p.$$

This implies that (8.5) holds.

Next, we shall prove that

$$\mathscr{R}_p([J_v\colon N(q; t, \mu, \nu)])\supset\mathscr{R}_p(N(q; t, \nu)). \tag{8.6}$$

Let $\boldsymbol{z}$ be any column vector of $N(q; t, \nu)$ where $\boldsymbol{z}^T=(z_0, z_1, \ldots, z_{v-1})$. Then there exists a unique ν-flat W such that $z_i=1$ or 0 according as the ith point (α^i) is incident with W or not. Let us denote $b_0=\phi(t-\nu-1, \mu-\nu-1, q)$ μ-flats containing the ν-flat W by V_j $(j=1, 2, \ldots, b_0)$ and let $\boldsymbol{x}_j$ $(j=1, 2, \ldots, b_0)$ be column vectors of $N(q; t, \mu, \nu)$ such that $x_{ij}=1$ or 0 according as the ith point (α^i) is contained in V_j-W or not. Then it follows that

$$\boldsymbol{z}\equiv J_v-c_2 \sum_{j=1}^{b_0} \boldsymbol{x}_j \mod p$$

where c_2 is a positive integer less than p such that

$$c_2\phi(t-\nu-2, \mu-\nu-2, p^m)\equiv 1 \mod p.$$

This implies that (8.6) holds. This completes the proof.

From Lemma 8.1 and Theorem 7.2, we have the following theorem:

THEOREM 8.2. *For any integer μ such that $0<\nu<\mu\leqq t$, the p-rank of $N(q; t, \mu, \nu)$ is equal to $R_\nu(t, p^m)-1$ where $q=p^m$ and $R_\nu(t, p^m)$ is given by* (7.7) *or* (7.9).

Since each entry of $N(q; t, \mu, \nu)$ is 0 or 1, we have the

COROLLARY 8.3. *For any positive integer n, the rank of $N(p^m; t, \mu, \nu)$ over* GF(p^n) *is equal to $R_\nu(t, p^m)-1$.*

Since $N(q; t, t, \nu)$ is the complement matrix of $N(q; t, \nu)$, we have the

COROLLARY 8.4. *The p-rank of the complement matrix of the incidence matrix $N(q; t, \nu)$ of points and ν-flats in* PG(t, q) *is equal to $R_\nu(t, p^m)-1$.*

This corollary shows that the p-rank of the complement matrix of $N(q; t, \nu)$ is less than the p-rank of $N(q; t, \nu)$.

Table 8.1 gives all solutions for BIB designs $N(q;\ t,\ \mu,\ v)$ with $7 \leqq v \leqq 50$ and $b < 1000$ and their p-ranks. The symbol C(No. i in Table 7.1) means that this design is the complement of the design No. i in Table 7.1. The symbol $CT(\ldots)$ denotes that the rest of the initial blocks are generated by a cyclical transformation indicated by $CT(\ldots)$ after; for example, symbol (0, 7, 9, 12) mod 15 CT(0, 1, 2, 9, 7, 12, 13) of No. 5 in Table 8.1 denotes that all initial blocks may be generated cyclically from the initial block (0, 7, 9, 12) by the cyclical transformation CT(0, 1, 2, 9, 7, 12, 13), that is, all initial blocks are

(0, 7, 9, 12), (1, 12, 7, 13), (2, 13, 12, 0), (9, 0, 13, 1),

(7, 1, 0, 2), (12, 2, 1, 9), (13, 9, 2, 7).

TABLE 8.1.

SOLUTIONS FOR BIB DESIGNS $N(p^m;\ t,\ \mu,\ v)$ AND THEIR P-RANKS

No.	v	b	r	k	λ	rank	δ	p^m	t	μ	v	Solution
1	7	7	4	4	2	3	1	2	2	2	1	C(No. 1 in Table 7.1)
2	13	13	9	9	6	6	0	3	2	2	1	C(No. 2 in Table 7.1)
3	15	15	8	8	4	4	1	2	3	3	2	C(No. 3 in Table 7.1)
4	15	35	28	12	22	10	0	2	3	3	1	C(No. 4 in Table 7.1)
5	15	105	28	4	6	10	2	2	3	2	1	(0, 7, 9, 12) mod 15, CT(0, 1, 2, 9, 7, 12, 13)
6	21	21	16	16	12	9	0	4	2	2	1	C(No. 5 in Table 7.1)
7	31	31	25	25	20	15	0	5	2	2	1	C(No. 6 in Table 7.1)
8	31	31	16	16	8	5	1	2	4	4	3	C(No. 7 in Table 7.1)
9	31	155	120	24	92	15	0	2	4	4	2	C(No. 8 in Table 7.1)
10	31	465	120	8	28	15	2	2	4	3	2	(0, 5, 7, 11, 14, 22, 26, 28) mod 31, CT(0, 1, 2, 3, 5, 26, 11, 22, 23, 28, 29, 7, 14, 15, 16)
11	31	155	140	28	126	25	0	2	4	4	1	C(No. 9 in Table 7.1)
12	40	40	27	27	15	10	0	3	3	3	2	C(No. 10 in Table 7.1)
13	40	130	117	36	105	29	0	3	3	3	1	C(No. 11 in Table 7.1)
14	40	520	117	9	24	29	2	3	3	2	1	(0, 8, 16, 18, 23, 25, 28, 34, 37) mod 40, CT(0, 1, 2, 25, 8, 37, 38, 18, 23, 16, 34, 28, 29)

9. The p-rank of the incidence matrix of all points and all μ-flats in EG(t, q)

(a) The incidence matrix of all points and all μ-flats in EG(t, q)

The affine geometry of t dimensions, denoted by EG(t, q), is a set of points which satisfy the following conditions:

(i) A point is represented by (v) where v is an element of the Galois field GF(q^t) and each element represents a unique point.

(ii) A μ-flat, $0<\mu\leqq t$, passing through the origin, denoted by (0), is defined as a set of points:

$$\{(a_1v_1+a_2v_2+\cdots+a_\mu v_\mu)\}$$

where a's run independently over the elements of GF(q) and $v_1, v_2, \ldots, v_\mu$ are linearly independent elements of GF(q^t) over GF(q).

(iii) A μ-flat not passing through the origin is defined as a set of points:

$$\{(v_0+a_1v_1+\cdots+a_\mu v_\mu)\}$$

where a's run independently over the elements of GF(q) and $v_0, v_1, \ldots, v_\mu$ are linearly independent elements of GF(q^t).

Let α be a primitive element of GF(q^t). Then every non-zero element of GF(q^t) can be represented by $\alpha^0, \alpha^1, \ldots, \alpha^{q^t-2}$ and every point in EG(t, q) can be expressed by (0), (α^0), (α^1), ..., (α^{q^t-2}). It is well known that the number, b_0, of μ-flats passing through the origin in EG(t, q) is equal to $b_0=\phi(t-1, \mu-1, q)$ and the number, b_1, of μ-flats not passing through the origin is equal to

$$b_1=\phi(t, \mu, q)-\phi(t-1, \mu, q)-\phi(t-1, \mu-1, q) \tag{9.1}$$

where $\phi(t, \mu, q)$ is given by (7.4). In order to define the incidence matrix of all points and all μ-flats in EG(t, q), we shall denote the origin (0) in EG(t, q) by P_0 and the point (α^u) by P_{u+1} $(u=0, 1, \ldots, q^t-2)$.

After numbering b_0 μ-flats passing through the origin in EG(t, q) and b_1 μ-flats not passing through the origin in EG(t, q) in some way, respectively, we define the incidence matrix, $M_0^*(q; t, \mu)$, of all points and b_0 μ-flats passing through the origin in EG(t, q) and the incidence matrix, $M_1^*(q; t, \mu)$, of all points and b_1 μ-flats not passing through the origin in EG(t, q), to be the matrices:

$$M_l^*(q; t, \mu)=\|m_{ij}^{(l)*}(q; t, \mu)\| ; \; i=0, 1, \ldots, q^t-1 \text{ and } j=1, 2, \ldots, b_l$$

where $m_{ij}^{(l)*}(q; t, \mu)=1$ or 0 according as the ith point P_i is incident with the jth μ-flat or not. Let

$$M^*(q; t, \mu)=[M_0^*(q; t, \mu): M_1^*(q; t, \mu)]. \tag{9.2}$$

Then, $M^*(q; t, \mu)$ is the incidence matrix of all points and all μ-flats in EG(t, q). It is known [2] that $M^*(q; t, \mu)$ is the incidence matrix of a *BIB* design, denoted by EG(t, q): μ, with parameters:

$$v=q^t, \quad b=\phi(t, \mu, q)-\phi(t-1, \mu, q), \quad r=\phi(t-1, \mu-1, q), \tag{9.3}$$
$$k=q^\mu \quad \text{and} \quad \lambda=\phi(t-2, \mu-2, q).$$

In this case, we have

$$r-\lambda=q^\mu\phi(t-2, \mu-1, q) \quad \text{and} \quad \delta=[r/2\lambda]=[(q^t-1)/2(q^\mu-1)]. \tag{9.4}$$

It is therefore necessary to investigate the p-rank and the p^*-rank of $M^*(q; t, \mu)$ where $q=p^m$ and p^* is a prime which is a factor of $\phi(t-2, \mu-1, q)$. But they have not yet been obtained. So, in this section, we shall investigate the p-rank of $M^*(q; t, \mu)$.

(b) Main theorems for the p-ranks of $M(q; t, \mu)$ and $M^*(q; t, \mu)$

Let $M_l(q; t, \mu)$ $(l=0, 1)$ be the matrix which is obtained from $M_l^*(q; t, \mu)$ by deleting its first row (correspoinding to the origin) and let

$$M(q; t, \mu)=[M_0(q; t, \mu): M_1(q; t, \mu)]. \tag{9.5}$$

Then we have the following main theorems:

THEOREM 9.1. *The p-rank of the incidence matrix $M(q; t, \mu)$ of q^t-1 points other than the origin and all μ-flats in* EG(t, q) *is equal to $R_\mu(t, p^m)-R_\mu(t-1, p^m)$ where $q=p^m$ and $R_\mu(t, p^m)$ is given by* (7.9).

THEOREM 9.2. *The p-rank of the incidence matrix $M^*(q; t, \mu)$ of all points and all μ-flats in* EG(t, q) *is also equal to $R_\mu(t, p^m)-R_\mu(t-1, p^m)$.*

COROLLARY 9.3. *For any positive integer n, the rank of $M(p^m; t, \mu)$ (or $M^*(p^m; t, \mu)$) over* GF(p^n) *is equal to $R_\mu(t, p^m)-R_\mu(t-1, p^m)$.*

COROLLARY 9.4. *In the special case $\mu=t-1$, the p-rank of the incidence matrix $M^*(p^m; t, t-1)$ of all points and all hyperplane in* EG(t, p^m) *is equal to* $\binom{t+p-1}{t}^m$.

COROLLARY 9.5. *In the special case $m=1$, the p-rank of the incidence matrix $M^*(p; t, \mu)$ of all points and all μ-*flats *in* EG(t, p) *is equal to $R_\mu(t, p)-R_\mu(t-1, p)$ where $R_\mu(t, p)$ is given by* (7.12).

COROLLARY 9.6. *In the special case $q=2$, the 2-rank of the incidence matrix $M^*(2; t, \mu)$ of 2^t points and $\phi(t, \mu, 2)-\phi(t-1, \mu, 2)$ μ-flats in* EG$(t, 2)$ *is equal to* $\sum_{s=0}^{t-\mu}\binom{t}{s}$.

(c) Preliminary result for the proof of main theorems

To obtain an explicit formula for the p-rank of the incidence matrix $M(q; t, \mu)$, we shall use the following properties, called the cyclic structure, of μ-flats in EG(t, q).

THEOREM 9.7 (Rao). (i) *Let*

$$V(0)=\{(0), (\alpha^{c_2}), (\alpha^{c_3}), \ldots, (\alpha^{c_n})\} \qquad (n=q^{\mu})$$

be any μ-flat passing through the origin in EG(t, q), *then the set*

$$V(r)=\{(0), (\alpha^{c_2+r}), (\alpha^{c_3+r}), \ldots, (\alpha^{c_n+r})\}$$

is also some μ-flat passing through the origin for any positive integer r.

(ii) *Let*

$$V^*(0)=\{(\alpha^{c_1^*}), (\alpha^{c_2^*}), \ldots, (\alpha^{c_n^*})\} \qquad (n=q^{\mu})$$

be any μ-flat not passing through the origin in EG(t, q), *then the set*

$$V^*(r)=\{(\alpha^{c_1^*+r}), (\alpha^{c_2^*+r}), \ldots, (\alpha^{c_n^*+r})\}$$

is also some μ-flat not passing through the origin for any positive integer r.

For some positive integer θ, $V(\theta)$ coincides with $V(0)$. Such an integer θ is called a cycle of the (initial) flat $V(0)$ and the minimum value of these cycles is called the minimum cycle (*m.c.*) of $V(0)$. Since $V(q^t-1)=V(0)$ and $V^*(q^t-1)=V^*(0)$, any μ-flat in EG(t, q) has q^t-1 as a cycle.

THEOREM 9.8 (Rao). (i) *Any μ-flat passing through the origin in* EG(t, q) *has some factor of $(q^t-1)/(q-1)$ as the minimum cycle.*

(ii) *Any μ-flat not passing through the origin in* EG(t, q) *has q^t-1 as the minimum cycle.*

From the above two theorems, it follows that (i) all μ-flats passing through the origin may be generated cyclically from a set of initial μ-flats, say $V_{00}(0)$, $V_{01}(0)$, $\ldots$, $V_{0\pi_0-1}(0)$, passing through the origin by the transformation:

$$(0)\rightarrow(0) \quad \text{and} \quad (\alpha^u)\rightarrow(\alpha^{u+1}) \tag{9.6}$$

for $u=0, 1, \ldots, q^t-2$, that is, all μ-flats passing through the origin are represented by $V_{0k}(r)$ $(k=0, 1, \ldots, \pi_0-1;\ r=0, 1, \ldots, \theta_k-1)$ where θ_k is the minimum cycle of the initial μ-flat $V_{0k}(0)$ and π_0 is an integer such that $\sum_{i=0}^{\pi_0} \theta_i=b_0$ and (ii) all μ-flats not passing through the origin may be generated cyclically from a set of initial μ-flats, say $V_{10}(0)$, $V_{11}(0)$, $\ldots$, $V_{1\pi_1-1}(0)$, not passing through the origin by the transformation (9.6), that is, all μ-flats not passing through the origin are represented by $V_{1k}(r)$ ($k=0, 1, \ldots, \pi_1-1$; $r=0, 1, \ldots, q^t-2$) where $\pi_1=b_1/(q^t-1)$. Since any multiple of the minimum cycle of a μ-flat is also a cycle of the μ-flat, any μ-flat in EG(t, q) has $v^*=q^t-1$ as a cycle.

Let $V_{0k}(u\theta_k+r_0)=V_{0k}(r_0)$ for all integers k, u and r_0 such that

$$0\leqq k<\pi_0,\ 1\leqq u<v^*/\theta_k \quad \text{and} \quad 0\leqq r_0<\theta_k$$

and we define the incidence matrix of v^* points other than the origin and $\pi_l v^*$ μ-flats $V_{lk}(r)$ ($k=0, 1, \ldots, \pi_l-1$; $r=0, 1, \ldots, v^*-1$) to be the matrix:

$$\tilde{M}_l=\|\tilde{m}_{ij}^{(l)}\| \ ; \quad i=0, 1, \ldots, \pi_l v^*-1 \quad \text{and} \quad j=0, 1, \ldots, v^*-1$$

where $\tilde{m}_{kv^*+r,j}^{(l)}=1$ or 0 according as the jth point (α^j) is incident with the μ-flat $V_{lk}(r)$ or not. Let

$$\tilde{M} = \begin{bmatrix} \tilde{M}_0 \\ \tilde{M}_1 \end{bmatrix}. \tag{9.7}$$

Since $M(q;\ t,\ \mu)$ can be obtained from $\tilde{M}^T$ by deleting duplicates of rows of $\tilde{M}$ and by permuting rows suitably, the rank of $M(q;\ t,\ \mu)$ is equal to the rank of $\tilde{M}$. Hence, it suffices to obtain an explicit formula for the rank of $\tilde{M}$ over GF(q).

(d) The proof of main theorems

In the following, we shall use an extension of the methods used by Smith [31]. From the definition of $\tilde{M}_0$ and $\tilde{M}_1$, we can see that

$$\tilde{m}_{kv^*+r+1,j+1}^{(l)} = \tilde{m}_{kv^*+r,j}^{(l)} \tag{9.8}$$

for any integers l, k, r and j such that

$$0\leqq l\leqq 1,\quad 0\leqq k<\pi_l,\quad 0\leqq r<v^* \quad \text{and} \quad 0\leqq j<v^* \tag{9.9}$$

where the subscripts $r+1$ and $j+1$ are taken mod v^*. We define the incidence polynomial of the μ-flat $V_{lk}(r)$ by

$$\tilde{\theta}_{k,r}^{(l)}(x)=\sum_{j=0}^{v^*-1} \tilde{m}_{kv^*+r,j}^{(l)}\, x^j. \tag{9.10}$$

Then it follows from (9.8) and (9.10) that

$$\tilde{\theta}_{k,r}^{(l)}(x)\equiv x^r\tilde{\theta}_{k,0}^{(l)}(x) \quad \bmod x^{v^*}-1 \tag{9.11}$$

for any integers l, k and r satisfying the condition (9.9). Let

$$(9.12)\qquad V=\begin{pmatrix}\alpha^0 & (\alpha^2)^0 & \cdots & (\alpha^{v^*})^0\\ \alpha^1 & (\alpha^2)^1 & \cdots & (\alpha^{v^*})^1\\ \vdots & \vdots & \cdots & \vdots\\ \alpha^{v^*-1} & (\alpha^2)^{v^*-1} & \cdots & (\alpha^{v^*})^{v^*-1}\end{pmatrix}.$$

Then the matrix V is a non-singular Vandermonde matrix over $\mathrm{GF}(q^t)$ of order v^*. From (9.10) and (9.11), we have the following equation:

$$(9.13)\qquad \tilde{M}V=\begin{pmatrix}V & & & & & \\ & \ddots & & & 0 & \\ & & V & & & \\ & & & V & & \\ & 0 & & & \ddots & \\ & & & & & V\end{pmatrix}\begin{pmatrix}D_{00}\\ \vdots\\ D_{0\pi_0-1}\\ D_{10}\\ \vdots\\ D_{1\pi_1-1}\end{pmatrix}$$

where

$$(9.13')\qquad D_{lk}=\begin{pmatrix}\tilde{\theta}^{(l)}_{k0}(\alpha^1) & & & \\ & \tilde{\theta}^{(l)}_{k0}(\alpha^2) & & 0\\ & & \ddots & \\ 0 & & & \tilde{\theta}^{(l)}_{k0}(\alpha^{v^*})\end{pmatrix}$$

for $l=0$, 1 and $k=0, 1, \ldots, \pi_l-1$. Since both V and the composite matrix of V's on the right hand side of (9.13) are non-singular matrices over $\mathrm{GF}(q^t)$, the rank of $\tilde{M}$ over $\mathrm{GF}(q^t)$ is equal to the rank of the second matrix on the right hand side of (9.13). Hence, the rank of $\tilde{M}$ over $\mathrm{GF}(q^t)$ is equal to the number of integers h, $1\leqq h\leqq v^*$, such that $\tilde{\theta}^{(l)}_{k0}(\alpha^h)\neq 0$ for some integers l and k. Since the entries of $\tilde{M}$ are elements of subfield $\mathrm{GF}(p)$ of $\mathrm{GF}(q^t)$, the rank of $\tilde{M}$ over $\mathrm{GF}(q^t)$ is equal to its rank over $\mathrm{GF}(p)$. Thus we have the following theorem:

THEOREM 9.9. *The p-rank of the incidence matrix $M(q;\ t,\ \mu)$ of q^t-1 points other than the origin and all μ-flats in* $\mathrm{EG}(t,\ q)$ *is equal to the number of integers h, $1\leqq h\leqq q^t-1$, such that $\tilde{\theta}^{(l)}_{k0}(\alpha^h)\neq 0$ for some integers l and k.*

Let

$$\begin{aligned}\textstyle\sum&=\{(a_1\alpha^{e_1}+a_2\alpha^{e_2}+\cdots+a_\mu\alpha^{e_\mu})\}\\ &=\{(0),\ (\alpha^{c_2}),\ (\alpha^{c_3}),\ \ldots,\ (\alpha^{c_n})\}\qquad (n=q^\mu)\end{aligned}$$

be any μ-flat passing through the origin in $\mathrm{EG}(t,\ q)$ and let

$$\sum^* = \{(\alpha^{e_0^*} + a_1\alpha^{e_1^*} + \cdots + a_\mu\alpha^{e_\mu^*})\}$$
$$= \{(\alpha^{c_1^*}), (\alpha^{c_2^*}), \ldots, (\alpha^{c_n^*})\} \qquad (n = q^\mu)$$

be any μ-flat not passing through the origin in EG(t, q) where a's run independently over the elements of GF(q), $\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_\mu}$ are linearly independent elements of GF(q^t) and $\alpha^{e_0^*}, \alpha^{e_1^*}, \ldots, \alpha^{e_\mu^*}$ are also linearly independent elements of GF(q^t). We define the incidence polynomial of the μ-flat $\sum$ and the μ-flat $\sum^*$ as the polynomials

(9.14) $$\theta_\Sigma(x) = x^{c_2} + x^{c_3} + \cdots + x^{c_n} \qquad (n = q^\mu)$$

and

(9.15) $$\theta_{\Sigma^*}(x) = x^{c_1^*} + x^{c_2^*} + \cdots + x^{c_n^*} \qquad (n = q^\mu),$$

respectively. Then it follows that

(9.16) $$\theta_\Sigma(\alpha^h) = \sum_{a_1} \cdots \sum_{a_\mu} (a_1\alpha^{e_1} + a_2\alpha^{e_2} + \cdots + a_\mu\alpha^{e_\mu})^h$$

and

(9.17) $$\theta_{\Sigma^*}(\alpha^h) = \sum_{a_1} \cdots \sum_{a_\mu} (\alpha^{e_0^*} + a_1\alpha^{e_1^*} + \cdots + a_\mu\alpha^{e_\mu^*})^h$$

where each summation is taken over all elements of GF(q). Expanding each term of (9.16) and (9.17) and using the following equation:

(9.18) $$\sum_{a \in GF(q)} a^j = \begin{cases} -1, & \text{if } j = k(q-1),\ k > 0 \\ 0, & \text{otherwise,} \end{cases}$$

we have

(9.19) $$\theta_\Sigma(\alpha^h) = (-1)^\mu \sum_k \binom{h}{k_1(q-1), \ldots, k_\mu(q-1)} \alpha^{e_1k_1(q-1) + \cdots + e_\mu k_\mu(q-1)}$$

and

(9.20) $$\theta_{\Sigma^*}(\alpha^h) = (-1)^\mu \sum_l \binom{h}{l_0, l_1(q-1), \ldots, l_\mu(q-1)} \alpha^{e_0^* l_0 + g}$$
$$\left(g = \sum_{i=1}^{\mu} e_i^* l_i(q-1)\right)$$

where the summation in (9.19) is taken over all choices of positive integers $k_1, k_2, \ldots, k_\mu$ such that $\sum_{i=1}^{\mu} k_i(q-1) = h$ and the summation in (9.20) is taken over all choices of a non-negative integer l_0 and positive integers $l_1, l_2, \ldots, l_\mu$ such that $l_0 + \sum_{i=1}^{\mu} l_i(q-1) = h$.

Let $V_{0k}(0)$ be a μ-flat passing through the origin in EG(t, q) from which the μ-flat $\sum$ can be generated and let $V_{1l}^*(0)$ be a μ-flat not passing through the origin in EG(t, q) from which the μ-flat $\sum^*$ can be generated. Then it follows from (9.11) that (i) $\tilde{\theta}_{k0}^{(0)}(\alpha^h)\neq 0$ if and only if $\theta_\Sigma(\alpha^h)\neq 0$ and (ii) $\tilde{\theta}_{l0}^{(1)}(\alpha^h)\neq 0$ if and only if $\theta_{\Sigma^*}(\alpha^h)\neq 0$. Hence, from Theorem 9.9, we have the following theorem:

THEOREM 9.10. *The p-rank of the incidence matrix* $M(q;\ t,\ \mu)$ *of* q^t-1 *points other than the origin and all* μ*-flats in* EG(t, q) *is equal to the number of integers* h, $1\leqq h\leqq q^t-1$, *such that* $\theta_{\Sigma_0}(\alpha^h)\neq 0$ *for some* μ*-flat* $\sum_0$ *(passing through the origin or not passing through the origin) in* EG(t, q).

In order to obtain the number of integers h satisfying the above condition, we shall use the following two theorems summarizing the essential results due to Smith [31].

THEOREM 9.11. *Let h be an integer such that* $1\leqq h\leqq q^t-1$. *Then a necessary and sufficient condition for the integer h that there exists a* μ*-flat* $\sum$ *passing through the origin in* EG(t, q) *such that* $\theta_\Sigma(\alpha^h)\neq 0$ *is that h is an integer such that there exists a set of* μ *positive integers* k_i ($i=1, 2, \ldots, \mu$) *satisfying the following conditions*:

$$(9.21)\qquad h=\sum_{i=1}^{\mu} k_i(q-1) \quad \text{and} \quad D_p[h]=\sum_{i=1}^{\mu} D_p[k_i(q-1)]$$

where $D_p[n]$ *is defined by*

$$(9.22)\qquad D_p[n]=c_0+c_1+\cdots+c_u$$

for a non-negative integer n having the p-adic representation:

$$n=c_0+c_1p+\cdots+c_up^u \qquad (0\leqq c_i<p).$$

THEOREM 9.12. *Let h be an integer such that* $1\leqq h\leqq q^t-1$. *Then a necessary and sufficient condition for the integer h that there exists a* μ*-flat* $\sum^*$ *not passing through the origin in* EG(t, q) *such that* $\theta_{\Sigma^*}(\alpha^h)\neq 0$ *is that h is an integer such that* $h\neq q^t-1$ *and that there exists a set of one non-negative integer* l_0 *and* μ *positive integers* l_i ($i=1, 2, \ldots, \mu$) *satisfying the following conditions*:

$$(9.23)\qquad h=l_0+\sum_{i=1}^{\mu} l_i(q-1) \quad \text{and} \quad D_p[h]=D_p[l_0]+\sum_{i=1}^{\mu} D_p[l_i(q-1)].$$

If h is an integer which satisfies the condition (9.21), it is an integer which satisfies the condition (9.23). In the special case $h=q^t-1$, it satisfies the conditions (9.21) and (9.23). Hence, from Theorems 9.10, 9.11 and 9.12, we have the following theorem:

THEOREM 9.13. *The p-rank of the incidence matrix* $M(q;\ t,\ \mu)$ *of* q^t-1

points other than the origin and all μ-flats in EG(t, q) *is equal to the number of integers h, $1 \leqq h \leqq q^t - 1$, such that there exists a set of one non-negative integer l_0 and μ positive integers l_i $(i=1, 2, \ldots, \mu)$ satisfying the condition* (9.23).

The following theorem due to the present author [12] plays an important role in enumerating the number of integers h satisfying the above condition.

THEOREM 9.14. *Let h be an integer such that $1 \leqq h \leqq q^t - 1$ and let the p-adic representation of h be*

$$h = \sum_{i=0}^{t-1} \sum_{j=0}^{m-1} c_{ij} p^{im+j} \tag{9.24}$$

where $q = p^m$ and c_{ij}'s are non-negative integers less than p. Then a necessary and sufficient condition for the integer h that there exists a set of one non-negative integer l_0 and μ positive integers l_i $(i=1, 2, \ldots, \mu)$ satisfying the condition (9.23), is that there exists a set of $m+1$ positive integers s_l $(l=0, 1, \ldots, m)$ satisfying the following conditions:

$$s_m = s_0, \quad \mu \leqq s_j \leqq t, \quad 0 \leqq s_{j+1} p - s_j \leqq t(p-1) \tag{9.25}$$

and

$$\sum_{i=0}^{t-1} c_{ij} \geqq s_{j+1} p - s_j \tag{9.26}$$

for each $j = 0, 1, \ldots, m-1$.

Using the above theorems, we now prove Theorems 9.1 and 9.2.

(Proof of Theorem 9.1) In [12], the present author showed that the number of integers h satisfying the conditions (9.25) and (9.26) was equal to $R_\mu(t, p^m) - R_\mu(t-1, p^m)$. Hence, we have the required result from Theorems 9.13 and 9.14.

(Proof of Theorem 9.2) Since $M^*(q; t, \mu)$ is the incidence matrix of a *BIB* design with parameters (9.3), it follows from the definition of $M^*(q; t, \mu)$ that

$$m_{0j}^{(0)*} = 1, \quad \sum_{i=1}^{q^t-1} m_{ij}^{(0)*} = q^\mu - 1 \qquad \text{for } j = 1, 2, \ldots, b_0$$

and

$$m_{0j}^{(1)*} = 0, \quad \sum_{i=1}^{q^t-1} m_{ij}^{(1)*} = q^\mu \qquad \text{for } j = 1, 2, \ldots, b_1.$$

This implies that the first row of $M^*(q; t, \mu)$ can be expressed as a linear combination of the other rows of $M^*(q; t, \mu)$ with coefficient from GF(p). Since $M(q; t, \mu)$ is the matrix obtained from $M^*(q; t, \mu)$ by deleting its first row, the p-rank of $M^*(q; t, \mu)$ is equal to the p-rank of $M(q; t, \mu)$. Hence, we have the required result from Theorem 9.1.

(e) Tables of the p-ranks of *BIB* designs EG(t, p^m) : μ

Table 9.1 gives solutions for *BIB* designs EG(t, p^m): μ with $7 \leqq v \leqq 50$ and their p-ranks where $v = p^{mt}$. Solutions for designs Nos. 12, 13 and 14 are omitted here, for values of b are large. Comparing the p-ranks of designs D_i $(i=1, 2, 3, 4)$ of No. 4 in Table 6.2 and the p-rank of the design of No. 1 in Table 9.1, we can see that the design D_1 of No. 4 in Table 6.2 is isomorphic with the design EG(3, 2): 2.

Table 9.2 gives the p-ranks of the incidence matrices $M^*(p^m;\ t,\ \mu)$ of all *BIB* designs EG(t, p^m): μ with parameters satisfying either the condition:

(i) $p=2$; $2 \leqq m \leqq 5$, $1 \leqq \mu < t$ and $50 < v < 10000$

or

(ii) $p=3, 5, 7$; $1 \leqq m \leqq 5$, $1 \leqq \mu < t$ and $50 < v < 10000$.

In the special case $q=2$, we can see from Corollaries 7.6 and 9.6 that the 2-rank of $M^*(2;\ t,\ \mu)$ is equal to the 2-rank of $N(2;\ t-1,\ \mu-1)$. So, these designs EG$(t, 2)$: μ and their 2-ranks are omitted from Table 9.2.

TABLE 9.1.

BIB DESIGNS EG$(t,\ p^m)$: μ AND THEIR P-RANKS

No.	v	b	r	k	λ	rank	δ	p^m	t	μ	EG$(t,\ p^m)$: μ
1	8	14	7	4	3	4	1	2	3	2	$(\infty, 0, 1, 5), (0, 3, 4, 5)$ mod 7
2	8	28	7	2	1	7	3	2	3	1	$(\infty, 0), (0, 1), (0, 3), (0,5)$ mod 7
3	9	12	4	3	1	6	2	3	2	1	$(\infty, 0, 4)$ $PC(4)$, $(0, 2, 7)$ mod 8
4	16	30	15	8	7	5	1	2	4	3	$(\infty, 0, 1, 2, 7, 9, 12, 13)$, $(0, 4, 5, 6, 7, 9, 11, 12)$ mod 15
5	16	140	35	4	7	11	2	2	4	2	$(\infty, 0, 1, 12), (\infty, 0, 2, 9)$ mod 15, $(\infty, 0, 5, 10)$ $PC(5)$, $(0, 7, 9, 12)$, $(0, 4, 5, 12), (0, 4, 9, 11)$, $(0, 1, 2, 7), (0, 1, 3, 5)$, $(0, 6, 11, 12), (0, 1, 9, 13)$ mod 15
6	16	120	15	2	1	15	7	2	4	1	$(\infty, 0), (0, 1), (0, 2), (0, 3), (0, 4)$, $(0, 5)$ $(0, 6), (0, 7)$ mod 15
7	16	20	5	4	1	9	2	4	2	1	$(\infty, 0, 5, 10)$ $PC(5)$, $(0, 8, 12, 14)$ mod 15
8	25	30	6	5	1	15	3	5	2	1	$(\infty, 0, 6, 12, 18)$ $PC(6)$, $(0, 8, 17, 21, 22)$ mod 24

TABLE 9.1. (continued)

No.	v	b	r	k	λ	rank	δ	p^m	t	μ	EG(t, p^m): μ
9	27	39	13	9	4	10	1	3	3	2	$(\infty, 0, 1, 5, 11, 13, 14, 18, 24)$ $PC(13)$ $(0, 7, 10, 16, 17, 18, 21, 22, 24)$ mod 26
10	27	117	13	3	1	23	6	3	3	1	$(\infty, 0, 13)$ $PC(13)$, $(0, 18, 24)$, $(0, 1, 5)$, $(0, 3, 15)$, $(0, 7, 16)$ mod 26
11	32	62	31	16	15	6	1	2	5	4	$(\infty, 0, 1, 2, 3, 5, 7, 11, 14, 15, 16, 22, 23, 26, 28, 29)$, $(0, 5, 7, 9, 10, 11, 13, 14, 18, 19, 20, 21, 22, 25, 26, 28)$ mod 31
12	32	620	155	8	35	16	2	2	5	3	—
13	32	—	155	4	15	26	5	2	5	2	—
14	32	496	31	2	1	31	15	2	5	1	—
15	49	56	8	7	1	28	4	7	2	1	$(\infty, 0, 8, 16, 24, 32, 40)$ $PC(8)$, $(0, 18, 22, 28, 29, 31, 43)$mod 48

TABLE 9. 2.
THE P-RANK OF BIB DESINGS EG(t, p^m): μ

No.	v	p-rank	δ	p^m	t	μ	No.	v	p-rank	δ	p^m	t	μ
16	64	16	2	4	3	2	29	256	25	2	4	4	3
17	64	51	10	4	3	1	30	256	129	8	4	4	2
18	64	27	4	8	2	1	31	256	235	42	4	4	1
19	81	15	1	3	4	3	32	256	81	8	16	2	1
20	81	50	5	3	4	2	33	343	84	3	7	3	2
21	81	76	20	3	4	1	34	343	287	28	7	3	1
22	81	36	5	9	2	1	35	512	64	4	8	3	2
23	125	35	2	5	3	2	36	512	373	36	8	3	1
24	125	105	15	5	3	1	37	625	70	2	5	4	3
25	243	21	1	3	5	4	38	625	355	13	5	4	2
26	243	96	4	3	5	3	39	625	590	78	5	4	1
27	243	192	15	3	5	2	40	625	225	13	25	2	1
28	243	237	60	3	5	1	41	729	28	1	3	6	5

TABLE 9.2. (continued)

No.	v	p-rank	δ	p^m	t	μ	No.	v	p-rank	δ	p^m	t	μ
42	729	168	4	3	6	4	66	3125	2438	65	5	5	2
43	729	435	14	3	6	3	67	3125	3069	390	5	5	1
44	729	651	45	3	6	2	68	4096	49	2	4	6	5
45	729	722	182	3	6	1	69	4096	524	8	4	6	4
46	729	100	4	9	3	2	70	4096	1974	32	4	6	3
47	729	553	45	9	3	1	71	4096	3515	136	4	6	2
48	729	216	14	27	2	1	72	4096	4053	682	4	6	1
49	1024	36	2	4	5	4	73	4096	125	4	8	4	3
50	1024	276	8	4	5	3	74	4096	1511	32	8	4	2
51	1024	736	34	4	5	2	75	4096	3690	292	8	4	1
52	1024	993	170	4	5	1	76	4096	256	8	16	3	2
53	1024	243	16	32	2	1	77	4096	2719	136	16	3	1
54	2187	36	1	3	7	6	78	6561	45	1	3	8	7
55	2187	274	4	3	7	5	79	6561	423	4	3	8	6
56	2187	897	13	3	7	4	80	6561	1711	13	3	8	5
57	2187	1647	42	3	7	3	81	6561	3834	41	3	8	4
58	2187	2074	136	3	7	2	82	6561	5634	126	3	8	3
59	2187	2179	546	3	7	1	83	6561	6404	410	3	8	2
60	2401	210	3	7	4	3	84	6561	6552	1640	3	8	1
61	2401	1316	25	7	4	2	85	6561	225	4	9	4	3
62	2401	2275	200	7	4	1	86	6561	2660	41	9	4	2
63	2401	784	25	49	2	1	87	6561	6026	410	9	4	1
64	3125	126	2	5	5	4	88	6561	1296	41	81	2	1
65	3125	1007	12	5	5	3							

Part III. The p-rank of the incidence matrix of a *PBIB* design derived from a finite geometry

10. The p-rank of the incidence matrix of points and μ-flats with a cycle θ in PG(t, q)

In this section, we shall investigate the p-rank of the incidence matrix of points and μ-flats with a cycle θ less than v in PG(t, q) where $v=(q^{t+1}-1)/(q-1)$.

(a) **Preliminary results**

Let q be a prime power, say $q=p^m$ and consider a μ-flat $V(0)$ in PG(t, q) with the defining points $(\alpha^{e_0}), (\alpha^{e_1}), \dots, (\alpha^{e_\mu})$:

$$V(0)=\{(a_0\alpha^{e_0}+a_1\alpha^{e_1}+\cdots+a_\mu\alpha^{e_\mu})\}$$

and a μ-flat $V(r)$ with the defining points $(\alpha^{e_0+r}), (\alpha^{e_1+r}), \dots, (\alpha^{e_\mu+r})$:

$$V(r)=\{(a_0\alpha^{e_0+r}+a_1\alpha^{e_1+r_1}+\cdots+a_\mu\alpha^{e_\mu+r})\}$$

where r is a positive integer. For some positive integer θ, $V(\theta)$ coincides with $V(0)$. Such an integer θ is called a cycle of the initial flat $V(0)$ and the minimum value of these cycles is called the minimum cycle (*m.c.*) of the initial flat $V(0)$. Since $V(v)=V(0)$, v is a cycle of any μ-flat $V(0)$. To obtain the p-rank of the incidence matrix of points and μ-flats with a cycle θ less than v in PG(t, q), we shall use the following properties, called the cyclic structure, of μ-flats in PG(t, q).

THEOREM 10.1 (Rao). (i) *Let*

$$V(0)=\{(\alpha^{c_1}), (\alpha^{c_2}), \dots, (\alpha^{c_k})\}$$

be a μ-flat in PG(t, q), *where* $k=(q^{\mu+1}-1)/(q-1)$, *then the set*

$$V(r)=\{(\alpha^{c_1+r}), (\alpha^{c_2+r}), \dots, (\alpha^{c_k+r})\}$$

is also some μ-flat in PG(t, q) *for any positive integer r.*

(ii) *Any μ-flat in* PG(t, q) *has some factor of v as the minimum cycle.*

This theorem shows that all μ-flats in PG(t, q) may be generated cyclically from a set of initial μ-flats, say $V_0(0), V_1(0), \dots, V_{\pi-1}(0)$, by the transformation:

$$(10.1) \qquad (\alpha^u)\longrightarrow(\alpha^{u+1}) \qquad (u=0, 1, \dots, v-1),$$

where $(\alpha^v)=(\alpha^0)$, that is, all μ-flats in PG(t, q) can be represented by $V_i(r)$ ($i=0, 1, \dots, \pi-1$; $r=0, 1, \dots, \theta_i-1$) where θ_i is the *m.c.* of the initial μ-flat $V_i(0)$ and π is an integer such that $\sum_{i=0}^{\pi-1}\theta_i=\phi(t, \mu, q)$.

The following theorems due to Yamamoto, Fukuda and Hamada [36] play an important role in obtaining the p-rank of the incidence matrix of points and μ-flats with a cycle θ in PG(t, q).

THEOREM 10.2. *If a μ-flat V has a cycle less than v, then there exists a positive integer l such that $l+1$ is a common factor of $t+1$ and $\mu+1$, and that $\theta_l=(q^{t+1}-1)/(q^{l+1}-1)$ is the m.c. of the μ-flat V. In this case, the flat V is composed of $(q^{\mu+1}-1)/(q^{l+1}-1)$ flats each of which belongs to a set of θ_l l-flats $V(0)$, $V(1)$, $\dots$, $V(\theta_l-1)$ generated from the initial l-flat $V(0)=\{(a_0\alpha^0+a_1\alpha^{\theta_l}+\cdots+a_l\alpha^{l\theta_l})\}$ of the m.c. θ_l.*

Note that this theorem shows that (i) if a μ-flat V has a cycle θ less than v, then θ must be an integer of the form $(q^{t+1}-1)/(q^{l+1}-1)$, where l is some positive integer such that $l+1$ is a common factor of $t+1$ and $\mu+1$, and (ii) the μ-flat V can be also expressed as follows:

$$V=\{(b_0\alpha^{f_0}+b_1\alpha^{f_1}+\cdots+b_{\mu_l}\alpha^{f_{\mu_l}})\}$$

where μ_l is an integer such that $\mu_l+1=(\mu+1)/(l+1)$ and b's run independently over the elements of $\mathrm{GF}(q^{l+1})$, not all zero, and $\alpha^{f_0}, \alpha^{f_1}, \ldots, \alpha^{f_{\mu_l}}$ are μ_l+1 linearly independent elements of $\mathrm{GF}(q^{t+1})$ over $\mathrm{GF}(q^{l+1})$.

In the following, we shall denote a μ-flat having the cycle $\theta_l=(q^{t+1}-1)/(q^{l+1}-1)$ by a $\mu(l)$-flat where l is an integer such that $l+1$ is a common factor of $t+1$ and $\mu+1$.

THEOREM 10.3. (i) *If $t+1$ and $\mu+1$ are relatively prime, then all μ-flats in* PG(t, q) *have the minimum cycle $v=(q^{t+1}-1)/(q-1)$ and can be generated from $\pi=\phi(t, \mu, q)/v$ initial μ-flats where $\phi(t, \mu, q)$ is given by* (7.4). *If $(t+1, \mu+1)=p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_u^{\gamma_u}$ (>1, p's are primes such that $p_i<p_{i+1}$) is the highest common factor of $t+1$ and $\mu+1$, then the number of different minimum cycles is* $\prod_{i=1}^{u}(1+\gamma_i)$.

(ii) Let

$$\begin{aligned}
&\theta[x_1, \ldots, x_u]=(q^{t+1}-1)/(q^h-1),\\
&t[x_1, \ldots, x_u]=(t+1)/h-1,\\
&\mu[x_1, \ldots, x_u]=(\mu+1)/h-1,\\
&q[x_1, \ldots, x_u]=q^h, \qquad h=p_1^{x_1}\ldots p_u^{x_u}.
\end{aligned}\tag{10.2}$$

Then the numbers of $\mu(p_1^{x_1}p_2^{x_2}\ldots p_u^{x_u}-1)$-flats having the cycle $\theta[x_1, \ldots, x_u]$ and the m.c. $\theta[x_1, \ldots, x_u]$ are respectively

$$\begin{aligned}
&n(x_1, \ldots, x_u)=\phi(t[x_1, \ldots, x_u], \mu[x_1, \ldots, x_u], q[x_1, \ldots, x_u]),\\
&n^*(\gamma_1, \ldots, \gamma_u)=n(\gamma_1, \ldots, \gamma_u),\\
&n^*(x_1, \ldots, x_u)=n(x_1, \ldots, x_u)-\sum_{x_j\leqq y_j\leqq\gamma_j;\,\exists j,\,x_j<y_j} n^*(y_1, \ldots, y_u)
\end{aligned}\tag{10.3}$$

and the number of initial μ-flats of the m.c. $\theta[x_1, \ldots, x_u]$ is

$$\pi(x_1, \ldots, x_u)=n^*(x_1, \ldots, x_u)/\theta[x_1, \ldots, x_u]\tag{10.4}$$

from which the totality of μ-flats having the m.c. $\theta[x_1, \ldots, x_u]$ can be generated.

COROLLARY 10.4. *Let l be any integer such that $l+1$ is a common factor* *of $t+1$ and $\mu+1$, and let θ_l, t_l and μ_l be integers such that*

$$\theta_l=(q^{t+1}-1)/(q^{l+1}-1),\quad t_l+1=(t+1)/(l+1), \tag{10.5}$$
$$\mu_l+1=(\mu+1)/(l+1).$$

Then the number of $\mu(l)$-flats is equal to $n=\phi(t_l, \mu_l, q^{l+1})$.

Note that since any μ-flat has a cycle v, it is also $\mu(0)$-flat.

(b) The main theorems for the p-ranks of $N(\theta_l)$ and $N(\theta[x_1, \dots, x_u])$

After numbering $n_l\,\mu(l)$-flats in some way, we define the incidence matrix of v points and $n_l\,\mu(l)$-flats in PG(t, q) to be the matrix:

$$N(\theta_l)=\|n_{ij}(\theta_l)\| \quad ; \qquad i=0, 1, \dots, v-1 \text{ and } j=1, 2, \dots, n_l$$

where $n_{ij}(\theta_l)=1$ or 0 according as the ith point (α^i) in PG(t, q) is incident with the jth $\mu(l)$-flat or not. It is known [36] that when $l>0$, $N(\theta_l)$ is the incidence matrix of a *PBIB* design of N_2 type (*GD*) with parameters:

$$\begin{aligned} &v=\phi(t, 0, q),\quad b=\phi(t_l, \mu_l, q^{l+1}),\quad r=\phi(t_l-1, \mu_l-1, q^{l+1}),\\ &k=\phi(\mu, 0, q),\quad \lambda_1=\phi(t_l-1, \mu_l-1, q^{l+1}),\quad \lambda_2=\phi(t_l-2, \mu_l-2, q^{l+1}),\\ &n_1=(v/\theta_l-1),\quad n_2=(v/\theta_l)(\theta_l-1),\quad p^1_{11}=v/\theta_l-2 \text{ and } p^2_{11}=0. \end{aligned} \tag{10.6}$$

In this case, we have

$$\rho_1=rk-v\lambda_2=q^{(l+1)\mu_l}\phi(t_l-2, \mu_l-1, q^{l+1})\,(q^{l+1}-1)/(q-1) \tag{10.7}$$

and

$$\rho_2=r-\lambda_1=0.$$

Hence, this design is a singular *GD* design. Since

$$\mathrm{Rank}_{p_0}(N(\theta_l))\leqq \mathrm{Rank}(N(\theta_l))=\alpha_0+\alpha_1$$

for any prime p_0, it follows from $\alpha_0=1$ and $\alpha_1=(q^{t+1}-1)/(q^{l+1}-1)-1$ that $\mathrm{Rank}_{p_0}(N(\theta_l))\leqq(q^{t+1}-1)/(q^{l+1}-1)$. On the other hand, it follows from Theorem 5.1 that the p_0-rank of $N(\theta_l)$ is never less than $(q^{t+1}-1)/(q^{l+1}-1)-1$ unless p_0 is a factor of $v\rho_1$. It is therefore necessary to investigate the p-rank and the p^*-rank of $N(\theta_l)$ where $q=p^m$ and p^* is a prime which is a factor of $v\phi(t_l-2, \mu_l-1, q^{l+1})(q^{l+1}-1)/(q-1)$. As a solution for this problem, we have the following main theorem which is a generalization of Theorem 7.2.

THEOREM 10.5. *The p-rank of the incidence matrix $N(\theta_l)$ of points and μ-flats having the cycle θ_l in* PG(t, q) *is equal to $R_{\mu_l}(t_l, p^{m(l+1)})$ where $q=p^m$ and $R_\mu(t, p^m)$ is given by* (7.9).

Since any μ-flat in PG(t, q) is a $\mu(0)$-flat, we have the

COROLLARY 10.6. *The p-rank of the incidence matrix of points and μ-flats in* PG(t, q) *is equal to* $R_\mu(t, p^m)$.

More generally, consider $n(x_1, \ldots, x_u)$ μ-flats having a cycle $\theta[x_1, \ldots, x_u]$. After numbering these $n(x_1, \ldots, x_u)$ μ-flats in some way, we define the incidence matrix of v points and $n(x_1, \ldots, x_u)$ μ-flats having the cycle $\theta[x_1, \ldots, x_u]$ to be the matrix:

$$N(\theta[x_1, \ldots, x_u]) = \|n_{ij}(\theta[x_1, \ldots, x_u])\|; \; i=0, 1, \ldots, v-1, j=1, 2, \ldots, \eta$$

where $\eta = n(x_1, \ldots, x_u)$ and $n_{ij}(\theta[x_1, \ldots, x_u]) = 1$ or 0 according as the ith point (α^i) is incident with the jth μ-flat having the cycle $\theta[x_1, \ldots, x_u]$ or not. It is known [36] that when $\theta[x_1, \ldots, x_u] < v$, $N(\theta[x_1, \ldots, x_u])$ is the incidence matrix of a *PBIB* design of N_2 type with parameters:

$$\begin{aligned} &v = \phi(t, 0, q), \quad b = \phi(t[x_1, \ldots, x_u], \mu[x_1, \ldots, x_u], q[x_1, \ldots, x_u]), \\ &k = \phi(\mu, 0, q), \quad r = \lambda_1 = \lambda_1(x_1, \ldots, x_u), \quad \lambda_2 = \lambda_2(x_1, \ldots, x_u), \\ &n_1 = v/\theta[x_1, \ldots, x_u] - 1, \quad n_2 = \{\theta[x_1, \ldots, x_u] - 1\} v/\theta[x_1, \ldots, x_u], \\ &p_{11}^1 = v/\theta[x_1, \ldots, x_u] - 2 \qquad \text{and} \quad p_{11}^2 = 0 \end{aligned}$$

where

$$\begin{aligned} \lambda_1(x_1, \ldots, x_u) &= \phi(t[x_1, \ldots, x_u] - 1, \mu[x_1, \ldots, x_u] - 1, q[x_1, \ldots, x_u]), \\ \lambda_2(x_1, \ldots, x_u) &= \phi(t[x_1, \ldots, x_u] - 2, \mu[x_1, \ldots, x_u] - 2, q[x_1, \ldots, x_u]). \end{aligned}$$

From theorems 10.3 and 10.5, we have the following theorem:

THEOREM 10.7. *The p-rank of the incidence matrix $N(\theta[x_1, \ldots, x_u])$ of all points and all μ-flats having the cycle $\theta[x_1, \ldots, x_u]$ in* PG(t, q) *is equal to*

$$R_{\mu[x_1, \ldots, x_u]}(t[x_1, \ldots, x_u], p^{m p_1^{x_1} \cdots p_u^{x_u}})$$

where $q = p^m$ and $\mu[x_1, \ldots, x_u]$, $t[x_1, \ldots, x_u]$ and $\theta[x_1, \ldots, x_u]$ are given by (10.2) *and $R_\mu(t, p^m)$ is given by* (7.7) *or* (7.9).

(c) The proof of Theorem 10.5

From Theorems 10.1 and 10.2, it follows that all $\mu(l)$-flats in PG(t, q) can be generated cyclically from a set of initial $\mu(l)$-flats, say $V_0(0), V_1(0), \ldots, V_{\pi_l - 1}(0)$, by the transformation (10.1), that is, all $\mu(l)$-flats in PG(t, q) can be represented by $V_k(r)$ $(k=0, 1, \dots, \pi_l-1;\ r=0, 1, \dots, c_k-1)$ where c_k is the *m.c.* of the initial $\mu(l)$-flat $V_k(0)$ and π_l is an integer such tha $\sum_{k=0}^{\pi_l-1} c_k=n_l$. Let

$$(10.8) \qquad v^*=q^{t+1}-1 \quad \text{and} \quad V_k(r_1c_k+r_2)=V_k(r_2)$$

for $k=0, 1, \dots, \pi_l-1$, $r_1=1, 2, \dots, v^*/c_k-1$ and $r_2=0, 1, \dots, c_k-1$. We define the incidence matrix of $v^*\pi_l\mu(l)$-flats $V_k(r)$ $(k=0, 1, \dots, \pi_l-1;\ r=0, 1, \dots, v^*-1)$ and v^* points (α^j) $(j=0, 1, \dots, v^*-1)$ in PG(t, q) to be the matrix:

$$\tilde{N}(\theta_l)=\|\tilde{n}_{ij}(\theta_l)\|; \quad i=0, 1, \dots, v^*\pi_l-1 \quad \text{and} \quad j=0, 1, \dots, v^*-1$$

where $\tilde{n}_{kv^*+r,j}(\theta_l)=1$ or 0 according as the jth point (α^j) in PG(t, q) is incident with the $\mu(l)$-flat $V_k(r)$ or not. Since $(\alpha^{j_1v+j_2})=(\alpha^{j_2})$ and $V_k(r_1c_k+r_2)=V_k(r_2)$, the following relations hold:

$$(10.9) \qquad \begin{aligned} &\tilde{n}_{i,j_1v+j_2}(\theta_l)=\tilde{n}_{i,j_2}(\theta_l) \\ &\tilde{n}_{kv^*+r_1c_k+r_2,j}(\theta_l)=\tilde{n}_{kv^*+r_2,j}(\theta_l) \end{aligned}$$

for any integers i, j_1, j_2, j, k, r_1 and r_2 such that

$$0\leqq i<v^*\pi_l, \quad 0\leqq j_1<q-1, \quad 0\leqq j_2<v, \quad 0\leqq j<v^*,$$
$$0\leqq k<\pi_l, \quad 1\leqq r_1<v^*/c_k \quad \text{and} \quad 0\leqq r_2<c_k.$$

From (10.9) and the definition of $\tilde{N}(\theta_l)$, we have

$$(10.10) \qquad \tilde{n}_{kv^*+r+1,j+1}(\theta_l)=\tilde{n}_{kv^*+r,j}(\theta_l)$$

for $r, j=0, 1, \dots, v^*-1$ and $k=0, 1, \dots, \pi_l-1$ where the subscripts $r+1$ and $j+1$ are taken mod v^*. Since $N(\theta_l)$ can be obtained from $\tilde{N}(\theta_l)^T$ by deleting duplicates of columns and rows of $\tilde{N}(\theta_l)$ and by permuting rows suitably, the rank of $N(\theta_l)$ is equal to the rank of $\tilde{N}(\theta_l)$. It suffices therefore to obtain the p-rank of $\tilde{N}(\theta_l)$. In the following, we shall use a similar method used in Section 9.

We define the polynomial $\tilde{\theta}_{kr}(x)$ of the $\mu(l)$-flat $V_k(r)$ by

$$(10.11) \qquad \tilde{\theta}_{kr}(x)=\sum_{j=0}^{v^*-1}\tilde{n}_{kv^*+r,j}(\theta_l)x^j.$$

From (10.10) and (10.11), we have

$$(10.12) \qquad x^r\tilde{\theta}_{k0}(x)\equiv\tilde{\theta}_{kr}(x) \quad \mod x^{v^*}-1$$

for $r=0, 1, \dots, v^*-1$ and $k=0, 1, \dots, \pi_l-1$. Using (10.11) and (10.12), it can be shown that the following equation holds.

(10.13)
$$\tilde{N}(\theta_l)V=\begin{pmatrix} V & & & \\ & V & 0 & \\ & & \ddots & \\ 0 & & & V \end{pmatrix}\begin{pmatrix} D_1 \\ D_2 \\ \vdots \\ D_{\pi_l} \end{pmatrix}$$

where

(10.14)
$$D_k=\begin{pmatrix} \tilde{\theta}_{k0}(\alpha^1) & & & \\ & \tilde{\theta}_{k0}(\alpha^2) & & 0 \\ & & \ddots & \\ 0 & & & \tilde{\theta}_{k0}(\alpha^{v^*}) \end{pmatrix}$$

and V is a Vandermonde matrix of order $v^*=q^{t+1}-1$ defined by (9.12). Since both V and the composite matrix of V's on the right hand side of (10.13) are non-singular matrices over $\mathrm{GF}(q^{t+1})$, the rank of $\tilde{N}(\theta_l)$ over $\mathrm{GF}(q^{t+1})$ is equal to the rank of the second matrix on the right hand side of (10.13). Hence, the rank of $\tilde{N}(\theta_l)$ over $\mathrm{GF}(q^{t+1})$ is equal to the number of integers h, $1\leqq h\leqq v^*$, such that $\tilde{\theta}_{k0}(\alpha^h)\neq 0$ for some integer k. Since the rank of $\tilde{N}(\theta_l)$ over $\mathrm{GF}(q^{t+1})$ is equal to the rank of $\tilde{N}(\theta_l)$ over $\mathrm{GF}(p)$ and that the rank of $N(\theta_l)$ is equal to the rank of $\tilde{N}(\theta_l)$, we have the following theorem:

THEOREM 10.8. *The p-rank of the incidence matrix $N(\theta_l)$ of points and $\mu(l)$-flats in* PG(t, q) *is equal to the number of integers h, $1\leqq h\leqq v^*$, such that $\tilde{\theta}_{k0}(\alpha^h)\neq 0$ for some integer k.*

Let

$$\Sigma=\{(a_0\alpha^{e_0}+a_1\alpha^{e_1}+\cdots+a_\mu\alpha^{e_\mu})\}$$

be any $\mu(l)$-flat and we define the polynomial $S_\Sigma(x)$ of the $\mu(l)$-flat Σ by

(10.15)
$$S_\Sigma(x)=\sum_u x^u$$

where the summation is taken over all integer u such that

(10.16)
$$\alpha^u=a_0\alpha^{e_0}+a_1\alpha^{e_1}+\cdots+a_\mu\alpha^{e_\mu}$$

for some elements a_0, a_1, $\ldots$, a_μ of $\mathrm{GF}(q)$. Suppose Σ is a $\mu(l)$-flat generated from an initial $\mu(l)$-flat $V_k(0)$. Then we have

(10.17)
$$S_\Sigma(x)\equiv x^h\tilde{\theta}_{k0}(x) \qquad \mathrm{mod}\ x^{v^*}-1$$

for some integer h. This implies that $S_\Sigma(\alpha^h)\neq 0$ if and only if $\tilde{\theta}_{k0}(\alpha^h)\neq 0$, for any integer h. Hence, we have the

THEOREM 10.9. *The p-rank of $N(\theta_l)$ is equal to the number of integers h, $1 \leqq h \leqq v^*$, such that $S_\Sigma(\alpha^h) \neq 0$ for some $\mu(l)$-flat Σ in* PG(t, q).

From (10.15) and the note of Theorem 10.2, it follows that the polynomial $S_\Sigma(x)$ of the $\mu(l)$-flat Σ can be expressed as follows:

$$S_\Sigma(\alpha^h) = \sum_{b_0} \cdots \sum_{b_{\mu_l}} (b_0 \alpha^{f_0} + b_1 \alpha^{f_1} + \cdots + b_{\mu_l} \alpha^{f_{\mu_l}})^h \tag{10.18}$$

where the summations are taken over all elements of GF(q^{l+1}). Expanding (10.18) and using (9.18), we can see that (i) if h is not a multiple of $q^{l+1}-1$, $S_\Sigma(\alpha^h)=0$ for every $\mu(l)$-flat Σ and (ii) if h is a multiple of $q^{l+1}-1$, $S_\Sigma(\alpha^h)$ can be expressed as follows:

$$S_\Sigma(\alpha^h) = (-1)^{\mu_l+1} \sum_k \binom{h}{k_0(q^{l+1}-1), \ldots, k_{\mu_l}(q^{l+1}-1)} \alpha^g$$

$$\left(g = \sum_{i=1}^{\mu_l} f_i k_i (q^{l+1}-1) \right)$$

where the summation is taken over all choices of μ_l+1 positive integers k_0, k_1, ..., k_{μ_l} such that $\sum_{i=0}^{\mu_l} k_i(q^{l+1}-1) = h$. Comparing (9.19) and the above equation, we have the following theorem from Theorem 9.11.

THEOREM 10.10. *Let h be an integer such that $1 \leqq h \leqq q^{t+1}-1$. Then a necessary and sufficient condition for the integer h that there exists a $\mu(l)$-flat Σ in* PG(t, q) *such that $S_\Sigma(\alpha_h) \neq 0$ is that h is an integer such that there exists a set of μ_l+1 positive integers k_i ($i=0, 1, \ldots, \mu_l$) satisfying the following conditions*:

$$h = \sum_{i=0}^{\mu_l} k_i(q^{l+1}-1) \quad \textit{and} \quad D_p[h] = \sum_{i=0}^{\mu_l} D_p[k_i(q^{l+1}-1)] \tag{10.19}$$

where $D_p[n]$ is defined by (9.22).

The following theorem due to the present author [12] plays an important role in enumerating the number of integers h satisfying the consition (10.19).

THEOREM 10.11. *Let h be an integer such that $1 \leqq h \leqq q^{t+1}-1$ and let the p-adic representation of h be*

$$h = \sum_{i=0}^{t_l} \sum_{j=0}^{m_l-1} c_{ij} p^{m_l i + j} \tag{10.20}$$

where $q=p^m$, $m_l=(l+1)m$ and c_{ij}'s are non-negative integers less than p. Then there exists a set of μ_l+1 positive integers k_i ($i=0, 1, \ldots, \mu_l$) satisfying the condition (10.19) *for the integer h if and only if there exists an ordered set $(s_0, s_1, \ldots, s_{m_l})$ in $S^*_{t_l, \mu_l}(p^{m_l})$ such that*

(10.21) $$\sum_{i=0}^{t_l} c_{ij}=s_{j+1}p-s_j$$

for each $j=0, 1, \ldots, m_l-1$ *where* $S^*_{t,\mu}(p^m)$ *is a set of ordered sets* $(s^*_0, s^*_1, \ldots, s^*_m)$ *satisfying the condition* (7.8).

Using the foregoing theorems, we can prove Theorem 10.5.

(Proof of Theorem 10.5) From Theorems 10.9, 10.10 and 10.11, it follows that the p-rank of $N(\theta_l)$ is equal to the number of integers h, $1\leqq h\leqq q^{t+1}$, such that there exists an ordered set $(s_0, s_1, \ldots, s_{m_l})$ satisfying the condition (10.21) in $S_{t_l,\mu_l}(p^{m_l})$. From Theorem 2.3, (2.56) and Lemma 2.6 in [12] due to the present author, we can see that the number of integers h satisfying the above condition is equal to $R_{\mu_l}(t_l, p^{m_l})$ where $R_\mu(t, p^m)$ is given by (7.7) or (7.9). We have therefore the required result.

11. The p-rank of the incidence matrix of points and μ-flats not passing through the origin in EG(t, q)

Let $M_1(q; t, \mu)$ be the incidence matrix of q^t-1 points other than the origin and b_1 μ-flats not passing through the origin in EG(t, q) where $q=p^m$ and b_1 is given by (9.1). Then if $q\neq 2$, $M_1(q; t, \mu)$ is the incidence matrix of an N_2 type *PBIB* design with parameters:

$$v=q^t-1,\quad b=b_1,\quad r=\phi(t-1, \mu-1, q)-\phi(t-2, \mu-2, q),\quad k=q^\mu,$$

$$\lambda_1=0,\quad \lambda_2=\phi(t-2, \mu-2, q)-\phi(t-3, \mu-3, q),\quad n_1=q-2,\ n_2=q^t-q,$$

$$p^1_{11}=q-3,\quad p^2_{11}=0,\quad \alpha_1=(q^t-q)/(q-1),\quad \alpha_2=(q-2)(q^t-1)/(q-1),$$

$$\rho_1=q^{\mu-1}\{q^{\mu+1}\phi(t-2, \mu-1, q)-(q^t-1)\phi(t-3, \mu-2, q)\},$$

$$\rho_2=q^\mu\phi(t-2, \mu-1, q)\qquad\text{and}\quad \delta=[r/2\max\{\lambda_1, \lambda_2\}].$$

In the special case $q=2$, $M_1(2; t, \mu)$ is the incidence matrix of a *BIB* design with parameters:

(11.1) $$v=2^t-1,\quad b=(2^t-1)\phi(t-2, \mu-1, 2),\quad r=2^\mu\phi(t-2, \mu-1, 2),$$
$$k=2^\mu\qquad\text{and}\quad \lambda=2^{\mu-1}\phi(t-3, \mu-2, 2).$$

Since $M_1(2; t, \mu)$ is isomorphic with $N(2; t-1, \mu, \mu-1)$,

$$\mathrm{Rank}_{p_0}(M_1(2; t, \mu))=\mathrm{Rank}_{p_0}(N(2; t-1, \mu, \mu-1))$$

for any prime p_0. We shall therefore consider only the case $q\neq 2$ in the following. Since $\rho_1\rho_2\neq 0$ and $\mathrm{Rank}_{p_0}(M_1(q; t, \mu))\leqq v$ for any prime p_0, it follows from Theorem 5.1 that the p_0-rank of $M_1(q; t, \mu)$ is equal to v unless p_0 is a factor of

$vrk\rho_1\rho_2$. It is therefore necessary to investigate the p-rank and the p^*-rank of $M_1(q; t, \mu)$ where $q=p^m$ and p^* is a prime which is a factor of $vrk\rho_1\rho_2$ except for p.

The p-rank of $M_1(q; t, \mu)$ for the special case $q=p$ (i.e., $m=1$) has been obtained by Smith [31] and its p-rank for general case $q=p^m$ has been obtained by the present author [12]. The result is as follows:

THEOREM 11.1. *The p-rank of the incidence matrix $M_1(q; t, \mu)$ of q^t-1 points other than the origin and b_1 μ-flats not passing through the origin in* EG(t, q) *is equal to $R_\mu(t, p^m)-R_\mu(t-1, p^m)-1$ where $q=p^m$ and $R_\mu(t, p^m)$ is given by* (7.7) *or* (7.9).

In the special case $q=2$, we have the following corollary:

COROLLARY 11.2. *The 2-rank of $M_1(2; t, \mu)$ is equal to* $\sum_{s=1}^{t-\mu}\binom{t}{s}$.

Table 11.1 gives solutions for *GD* type *PBIB* designs $M_1(p^m; t, \mu)$ with $7\leqq v\leqq 50$ and their p-ranks. The p-rank of $M_1(p^m; t, \mu)$ with $50<v<10000$ can be obtained at once from Table 9.2. The p^*-rank of $M_1(p^m; t, \mu)$ has not yet been obtained in general. But I dare say its p^*-rank is equal to $v-1$ or v.

TABLE 11.1.
SOLUTIONS FOR *GD* TYPE *PBIB* DESIGNS $M_1(p^m; t, \mu)$
AND THEIR *P*-RANKS

No.	v	b	r	k	λ_1	λ_2	n_1	ρ_1	ρ_2	rank	δ	p^m	t	μ	*PBIB* design
1	8	8	3	3	0	1	1	1	3	5	1	3	2	1	(0, 2, 7) mod 8
2	15	15	4	4	0	1	2	1	4	8	2	4	2	1	(0, 8, 12, 14) mod 15
3	24	24	5	5	0	1	3	1	5	14	2	5	2	1	(0, 8, 17, 21, 22) mod 24
4	26	26	9	9	0	3	1	3	9	9	1	3	3	2	(0, 7, 10, 16, 17, 18, 21, 22, 24) mod 26
5	26	104	12	3	0	1	1	10	12	22	6	3	3	1	(0, 18, 24), (0, 1, 5), (0, 3, 15), (0, 7, 16) mod 26
6	48	48	7	7	0	1	5	1	7	27	3	7	2	1	(0, 18, 22, 28, 29, 31, 43) mod 48

12. The dual of the *BIB* design PG$(t, q):\mu$ and its p-rank

Let q be a prime power, say $q=p^m$ and let α be a primitive element of $GF(q^{t+1})$. After numbering $v^*=\phi(t, \mu, q)$ μ-flats in PG(t, q) in some way, we define the incidence matrix of v^* μ-flats and $b^*=(q^{t+1}-1)/(q-1)$ points in PG(t, q) to be the matrix:

$$N^*(q;\, t,\, \mu)=\|n^*_{ij}(q;\, t,\, \mu)\| \quad ;\ i=1, 2, \dots, v^* \ \text{ and } \ j=0, 1, \dots, b^*-1$$

where $n^*_{ij}(q;\, t,\, \mu)=1$ or 0 according as the jth points (α^j) is incident with the ith μ-flat V_i or not. Then we have the following theorem:

THEOREM 12.1. *$N^*(q;\, t,\, \mu)$ is the incidence matrix of a PBIB design with $m^*=\min\{\mu+1,\, t-\mu\}$ associate classes and parameters:*

$$v^*=\phi(t,\, \mu,\, q),\ b^*=(q^{t+1}-1)/(q-1),\ r^*=(q^{\mu+1}-1)/(q-1),$$

$$k^*=\phi(t-1,\, \mu-1,\, q), \qquad \lambda_i=(q^{\mu-i+1}-1)/(q-1),$$

$$n_i=q^{i^2}\phi(t-\mu-1,\, i-1,\, q)\phi(\mu,\, \mu-i,\, q), \tag{12.1}$$

$$p^i_{jk}=\sum_{v=m_0}^{m_1}\sum_{l=0}^{m_2} q^{e_{vl}}\phi(\mu-i,\, v,\, q)\phi(i-1,\, \mu-j-v,\, q)\phi(i-1, \mu-k-v,\, q)$$

$$\cdot\phi(t-\mu-i-1,\, v+j+k-\mu-l-1,\, q)\chi(\omega_1,\, \omega_2,\, l:\, q)$$

$$(\omega_1=v+i+j-\mu,\ \omega_2=v+i+k-\mu)$$

for $i, j, k=1, 2, \dots, m^*$ where m_0, m_1, m_2 and e_{vl} are integers such that

$$m_0=\max\{-1,\, \mu-i-j,\, \mu-i-k,\, \mu-j-k\},$$

$$m_1=\min\{\mu-i,\, \mu-j,\, \mu-k\},$$

$$m_2=v+j+k-\mu, \tag{12.2}$$

$$e_{vl}=(\mu-i-v)(2\mu-2v-j-k+l)+(v+i+j+k-\mu-l)$$

$$\cdot(v+j+k-\mu-l)$$

and $\chi(\omega_1,\, \omega_2,\, l;\, q)$ is defined by

$$\chi(\omega_1,\, \omega_2,\, l;\, q)=\frac{\prod_{i=0}^{l-1}(q^{\omega_1}-q^i)(q^{\omega_2}-q^i)}{\prod_{i=0}^{l-1}(q^l-q^i)} \tag{12.3}$$

for any positive intergers ω_1, ω_2, l and $\chi(\omega_1,\, \omega_2,\, 0;\, q)=1$ for $\omega_1,\, \omega_2\geqq 0$.

In order to prove the above theorem, we prepare the following lemma:

LEMMA 12.2. *Let t, π, μ and v be any integers such that*

$$0\leqq v\leqq \pi<t \quad \text{and} \quad \pi+\mu-t\leqq v\leqq \mu<t \tag{12.4}$$

and let W be a π-flat in PG$(t,\, q)$. *Then the number, $\eta(t,\, \pi,\, \mu,\, v;\, q)$, of μ-flats V such that $V\cap W$ coincides with the given v-flat U in W is equal to*

(12.5) $$\eta(t, \pi, \mu, \nu; q)=q^{(\pi-\nu)(\mu-\nu)}\phi(t-\pi-1, \mu-\nu-1, q)$$

and the number, $\eta(t, \pi, \mu, -1; q)$, of μ-flats V such that $V \cap W$ is empty is equal to

(12.5′) $$\eta(t, \pi, \mu, -1; q)=q^{(\pi+1)(\mu+1)}\phi(t-\pi-1, \mu, q).$$

PROOF. Let $(\alpha^{d_0}), (\alpha^{d_1}), \ldots, (\alpha^{d_\nu})$ be the defining points of the ν-flat U and let $(\alpha^{d_0}), (\alpha^{d_1}), \ldots, (\alpha^{d_\nu}), (\alpha^{e_1}), \ldots, (\alpha^{e_{\mu-\nu}})$ be the defining points of a μ-flat V such that $V \cap W=U$. Then the first points (α^{e_1}) can be chosen in $b^*-(q^{\pi+1}-1)/(q-1)$ ways, the second in $b^*-(q^{\pi+2}-1)/(q-1)$ ways, the third in $b^*-(q^{\pi+3}-1)/(q-1)$ ways and so on. The total number of ways of choosing $\mu-\nu$ linearly independent points $(\alpha^{e_1}), (\alpha^{e_2}), \ldots, (\alpha^{e_{\mu-\nu}})$ such that $V \cap W=U$ is

$$(q^{t+1}-q^{\pi+1})(q^{t+1}-q^{\pi+2})\ldots(q^{t+1}-q^{\pi+\mu-\nu})/(q-1)^{\mu-\nu}.$$

While, each μ-flat V which contains the given ν-flat U can be generated by any one of $(q^{\mu+1}-q^{\nu+1})(q^{\mu+1}-q^{\nu+2})\ldots(q^{\mu+1}-q^{\nu+\mu-\nu})/(q-1)^{\mu-\nu}$ sets of $\mu-\nu$ independent points $(\alpha^{e_1}), (\alpha^{e_2}), \ldots, (\alpha^{e_{\mu-\nu}})$. Hence, the number of μ-flats V such that $V \cap W=U$ is equal to $q^{(\pi-\nu)(\mu-\nu)}\phi(t-\pi-1, \mu-\nu-1, q)$ when $\nu \geqq 0$. Since the number of μ-flats in PG(t, q) is equal to $\phi(t, \mu, q)$ and the number of ν-flats U in W is equal to $\phi(\pi, \nu, q)$, the number of μ-flats V such that $V \cap W$ is empty is equal to

$$\phi(t, \mu, q)-\sum_{\nu=n_0}^{n_1} q^{(\pi-\nu)(\mu-\nu)}\phi(t-\pi-1, \mu-\nu-1, q)\phi(\pi, \nu, q)$$

i.e., $q^{(\pi+1)(\mu+1)}\phi(t-\pi-1, \mu, q)$ where $n_0=\max\{0, \pi+\mu-t\}$ and $n_1=\min\{\pi, \mu\}$. Hence, we have the required result.

Note that this lemma shows that if we denote the empty set by (-1)-flat, the number of μ-flats V such that $V \cap W$ coincides with a given ν-flat U in W is given by $q^{(\pi-\nu)(\mu-\nu)}\phi(t-\pi-1, \mu-\nu-1, q)$ for any integer ν such that $-1 \leqq \nu \leqq \min\{\mu, \pi\}$ where $\phi(t, \mu, q)=0$ in the case $t<\mu$ or $\mu<-1$.

(Proof of Theorem 12.1) Since $N^*(q; t, \mu)$ is dual of the design $N(q; t, \mu)$, it follows that parameters v^*, b^*, r^* and k^* are given by (12.1). To prove that parameters λ_i, n_i and p^i_{jk} are given by (12.1), we define a relationship of association between every pair of $v^*=\phi(t, \mu, q)$ treatments, $\phi_1, \phi_2, \ldots, \phi_{v^*}$, as follows: Two treatments ϕ_{l_1} and ϕ_{l_2} are ith associates $(i=0, 1, \ldots, m^*)$ if $V_{l_1} \cap V_{l_2}$ is a $(\mu-i)$-flat. From this definition and Lemma 12.2, it is easy to see that the number, $n_i(l_1)$, of treatments ϕ_{l_2} being ith associates of a treatment ϕ_{l_1} is equal to $q^{i^2}\cdot \phi(t-\mu-1, i-1, q)\phi(\mu, \mu-i, q)$ and the number, $\lambda_i(l_1, l_2)$, of blocks which contain both treatments ϕ_{l_2} and ϕ_{l_1} being ith associates is equal to $(q^{\mu-i+1}-1)/(q-1)$. Hence, it suffices to show that parameters p^i_{jk}'s are given by (12.1).

To calculate the number $p_{j_1 j_2}^{i}$, let us consider any μ-flats V_{l_1} and V_{l_2} in

PG(t, q) such that $V_{l_1} \cap V_{l_2}$ is a $(\mu-i)$-flat, and a μ-flat V_{l_3} such that $V_{l_1} \cap V_{l_3}$ is a $(\mu-j_1)$-flat and $V_{l_2} \cap V_{l_3}$ is a $(\mu-j_2)$-flat. Since $V_{l_1} \cap V_{l_2} \cap V_{l_3}$ is a flat or the empty set, we can assume, without loss of generality, that $V_{l_1} \cap V_{l_2} \cap V_{l_3}$ is a ν-flat $(-1 \leqq \nu \leqq \mu-i)$ and that

$$W_{123} = V_{l_1} \cap V_{l_2} \cap V_{l_3} = W[d_0, d_1, \ldots, d_\nu],$$

$$W_{12} = V_{l_1} \cap V_{l_2} = W[d_0, d_1, \ldots, d_\nu; e_1, e_2, \ldots, e_{\mu-i-\nu}],$$

$$W_{k3} = V_{l_k} \cap V_{l_3} = W[d_0, d_1, \ldots, d_\nu; e_1^{(k)}, e_2^{(k)}, \ldots, e_{\mu-j_k-\nu}^{(k)}],$$

$$V_{l_k} = W[d_0, d_1, \ldots, d_\nu; e_1, \ldots, e_{\mu-i-\nu}; e_1^{(k)}, \ldots, e_{\mu-j_k-\nu}^{(k)}; h_1^{(k)}, \ldots, h_{\nu+i+j_k-\mu}^{(k)}],$$

$$V_{l_3} = W[d_0, d_1, \ldots, d_\nu; e_1^{(1)}, \ldots, e_{\mu-j_1-\nu}^{(1)}; e_1^{(2)}, \ldots, e_{\mu-j_2-\nu}^{(2)}; f_1, \ldots, f_{\nu+j_1+j_2-\mu}]$$

for $k=1, 2$, where $W[c_0, c_1, \ldots, c_\pi]$ denotes the π-flat generated by $\pi+1$ linearly independent points $(\alpha^{c_0}), (\alpha^{c_1}), \ldots, (\alpha^{c_\pi})$. Moreover, we can assume that the first l points $(\alpha^{f_1}), (\alpha^{f_2}), \ldots, (\alpha^{f_l})$ belong to the $(\mu+i)$-flat $T(V_{l_1}, V_{l_2})$ and the other points $(\alpha^{f_{l+1}}), (\alpha^{f_{l+2}}), \ldots, (\alpha^{f_{\nu+j_1+j_2-\mu}})$ do not belong to $T(V_{l_1}, V_{l_2})$ where l is an integer such that $0 \leqq l \leqq \nu+j_1+j_2-\mu$ and $T(V_1, V_2)$ denotes the minimum flat of flats which contain both V_1 and V_2. For a moment, we shall fix points $(\alpha^{d_0}), (\alpha^{d_1}), \ldots, (\alpha^{d_\nu}), (\alpha^{e_1}), \ldots, (\alpha^{e_{\mu-i-\nu}}), (\alpha^{e_1^{(k)}}), \ldots, (\alpha^{e_{\mu-j_k-\nu}^{(k)}}), (\alpha^{h_1^{(k)}}), \ldots, (\alpha^{h_{\nu+i+j_k-\mu}^{(k)}})$ $(k=1, 2)$ and investigate the number of μ-flats V_{l_3} satisfying the above conditions. Since points $(\alpha^{e_1^{(1)}}), (\alpha^{e_2^{(1)}}), \ldots, (\alpha^{e_{\mu-j_1-\nu}^{(1)}}), (\alpha^{f_1})$ and $\mu+1$ defining points of V_{l_2} must be linearly independent, and points $(\alpha^{e_1^{(2)}}), (\alpha^{e_2^{(2)}}), \ldots, (\alpha^{e_{\mu-j_2-\nu}^{(2)}})$, (α^{f_1}) and $\mu+1$ defining points of V_{l_1} must be linearly independent, point (α^{f_1}) can not belong to $W_0^{(1)}$ and $W_0^{(2)}$ where $W_0^{(k)}$ is a flat generated by the defining points $(\alpha^{d_0}), \ldots, (\alpha^{d_\nu}), (\alpha^{e_1^{(1)}}), \ldots, (\alpha^{e_{\mu-j_1-\nu}^{(1)}}), (\alpha^{e_1^{(2)}}), \ldots, (\alpha^{e_{\mu-j_2-\nu}^{(2)}}), (\alpha^{h_1^{(k)}}), \ldots,$ $(\alpha^{h_{\nu+i+j_k-\mu}^{(k)}}), (\alpha^{e_1}), \ldots, (\alpha^{e_{\mu-i-\nu}})$. Hence, the number of ways of choosing a point (α^{f_1}) in $T(V_{l_1}, V_{l_2})$ is equal to

$$\frac{q^{\mu+i+1}-1}{q-1} - \left\{\frac{q^{2\mu-j_1-\nu+1}-1}{q-1} + \frac{q^{2\mu-j_2-\nu+1}-1}{q-1} - \frac{q^{3\mu-2\nu-i-j_1-j_2+1}}{q-1}\right\},$$

i.e., $q^{\mu+i+1}(q^{\mu-\nu-i-j_1}-1)(q^{\mu-\nu-i-j_2}-1)/(q-1)$. Since (α^{f_1}) is a point in the $(\mu+i)$-flat $T(V_{l_1}, V_{l_2})$, α^{f_1} can be expressed as

$$\alpha^{f_1} = \sum_i a_i^{(1)} \alpha^{d_i} + \sum_i a_i^{(2)} \alpha^{e_i} + \sum_{k=1}^{2} \sum_i b_i^{(k)} \alpha^{e_i^{(k)}} + \sum_{k=1}^{2} \sum_i c_i^{(k)} \alpha^{h_i^{(k)}} \tag{12.8}$$

using elements $a_i^{(1)}, a_i^{(2)}, b_i^{(k)}, c_i^{(k)}$ of GF(q) such that $c_1^{(k)}, c_2^{(k)}, \ldots, c_{\nu+i+j_k-\mu}^{(k)}$ are not all simultaneously zero for each $k=1, 2$. Let $W_1^{(k)}$ be the flat generated by a point (α^{f_1}) and defining points of $W_0^{(k)}$. Then it follows from (12.8) that $W_1^{(1)} \cap W_1^{(2)}$ is a $(3\mu-2\nu-i-j_1-j_2+2)$-flat. Since a point (α^{f_2}) in $T(V_{l_1}, V_{l_2})$ can not belong to $W_1^{(1)}$ and $W_1^{(2)}$, the number of ways of choosing a point (α^{f_2}) in $T(V_{l_1}, V_{l_2})$ is equal to $q^{\mu+i+1}(q^{\mu-\nu-i-j_1+1}-1)(q^{\mu-\nu-i-j_2+1}-1)/(q-1)$. Similarly, we can see that the number of ways of choosing a point (α^{f_r}) $(1 \leqq r \leqq l)$ in $T(V_{l_1}, V_{l_2})$ is equal to $q^{\mu+i+1}(q^{\mu-\nu-i-j_1+r-1}-1)(q^{\mu-\nu-i-j_2+r-1}-1)/(q-1)$. Hence, the total number of ways of choosing l linearly independent points (α^{f_1}), (α^{f_2}), ..., (α^{f_l}) is

$$q^{(\mu+i+1)l}\prod_{r=1}^{l}\{(q^{\mu-\nu-i-j_1+r-1}-1)(q^{\mu-\nu-i-j_2+r-1}-1)/(q-1)\}$$

While each flat $W[d_0, d_1, \ldots, d_\nu; e_1^{(1)}, \ldots, e_{\mu-j_1-\nu}^{(1)}; e_1^{(2)}, \ldots, e_{\mu-j_2-\nu}^{(2)}; f_1, \ldots, f_l]$ can be generated by any one of $\prod_{r=1}^{l}\{(q^{2\mu-\nu-j_1-j_2+l+1}-q^{2\mu-\nu-j_1-j_2+r})/(q-1)\}$ sets of l independent points $(\alpha^{f_1}), (\alpha^{f_2}), \ldots, (\alpha^{f_l})$. Hence, the number of flats $W[d_0, d_1, \ldots, d_\nu; e_1^{(1)}, \ldots, e_{\mu-j_1-\nu}^{(1)}; e_1^{(2)}, \ldots, e_{\mu-j_2-\nu}^{(2)}; f_1, \ldots, f_l]$ passing through the fixed points $(\alpha^{d_0}), (\alpha^{d_1}), \ldots, (\alpha^{d_\nu}), (\alpha^{e^{(1)}_1}), \ldots, (\alpha^{e^{(1)}_{\mu-j_1-\nu}}), (\alpha^{e^{(2)}_1}), \ldots, (\alpha^{e^{(2)}_{\mu-j_2-\nu}})$ is equal to $q^{(\mu-\nu-i)l}\chi(\nu+i+j_1-\mu, \nu+i+j_2-\mu, l; q)$ and it does not depend on the fixed points. From Lemma 12.2, it follows that the number of μ-flats V_{l_3} in PG(t, q) such that

$$V_{l_3}\cap T(V_{l_1}, V_{l_2})=W[d_0, \ldots, d_\nu; e_1^{(1)}, \ldots, e_{\mu-j_1-\nu}^{(1)}; e_1^{(2)}, \ldots, e_{\mu-j_2-\nu}^{(2)}; f_1, \ldots, f_l]$$

is equal to $\eta(t, \mu+i, \mu, 2\mu+l-\nu-j_1-j_2; q)$ and it does not depend on the fixed points. Since the number of ν-flats W_{123} in W_{12} is equal to $\phi(\mu-i, \nu, q)$ and the number of $(\mu-j_k)$-flats V in V_{l_k} such that $V\cap W_{12}=W_{123}$ is equal to $\eta(\mu, \mu-i, \mu-j_k, \nu; q)$ for $k=1, 2$, it follows that $p^i_{j_1j_2}(l_1, l_2)$ is equal to

$$p^i_{j_1j_2}(l_1, l_2)=\sum_{\nu=m_0}^{m_1}\sum_{l=0}^{m_2}\phi(\mu-i, \nu, q)\eta(\mu, \mu-i, \mu-j_1, \nu; q)\eta(\mu, \mu-i, \mu-j_2, \nu; q)$$
$$\cdot q^{(\mu-\nu-i)l}\chi(\nu+i+j_1-\mu, \nu+i+j_2-\mu, l; q)\eta(t, \mu+i, \mu, 2\mu+l-\nu-j_1-j_2; q)$$

and it does not depend on μ-flats V_{l_1} and V_{l_2} such that $V_{l_1}\cap V_{l_2}$ is a $(\mu-i)$-flat. This completes the proof.

Since $N^*(q; t, \mu)^T$ is isomorphic with $N(q; t, \mu)$, we have the following theorem from Theorem 7.2.

THEOREM 12.3. *The p-rank of the incidence matrix $N^*(q; t, \mu)$ of a PBIB design with parameters* (12.1) *is equal to $R_\mu(t, p^m)$ where $q=p^m$ and $R_\mu(t, p^m)$ is given by* (7.9).

Part IV. Applications to error correcting codes

13. Applications to *BIBD* codes and *PBIBD* codes

Consider a channel which is capable of transmitting any one of q distinct symbols. Such a channel is called a q-ary channel. In this paper, we shall confine ourselves to the case when q is a prime or a prime power, say $q=p^m$. The symbols can then be put into a one-to-one correspondence with the elements of the Galois field GF(q). Given a set of $s(<q^n)$ distinct messages, we can set up a one-to-one correspondence between the massages and a set C of s distinct n-vectors with elements of GF(q). The elements of C may be called code vectors or code words. Thus each message corresponds to a unique code vector. If C is a subspace of the vector space $W_n(q)$ of all n-vectors with elements of GF(q), the code is said to be a q-ary linear code with length n. The dimension, k, of the subspace C is called the number of information symbols of the code C. The orthogonal or null space C_D of C is also a linear subspace of $W_n(q)$ and it is called the dual code of C. A matrix H whose row vectors span the dual code C_D is called a parity check matrix of the code C. To transmit a message over the channel, the n elements of the code vector $(c_1, c_2, \dots, c_n)$ corresponding to the message are presented in succession to the channel. Due to the presence of noise a transmitted symbol may be received as one of the other $q-1$ symbols. In this case, we say that an error has occurred in transmitting the symbol and, at the receiver, a decision is made, based on the information in the received vector, which specifies a unique vector of C, from which the corresponding message is interpolated. The process of specifying a code vector, based on the received vector, is called decoding. If the decoding procedure necessarily gives a correct result, provided at most δ errors have occurred in transmitting the code vector, we say that the code is capable of correcting up to δ errors. The ratio k/n is called the transmisson rate of information. A problem of error correcting codes is how to construct a linear code such that

(i) it is capable of correcting a relatively large number of errors,

(ii) it has a relatively high transmission rate of information and that

(iii) the encoding and decoding procedures are simple and economical to implement. If we use the transpose matrix of the incidence matrix N of a *BIB* design or a *PBIB* design as a parity check matrix, a relatively simple decoding procedure, called majority decoding [18], is applicable. So, we call such a code C a *BIBD* code and a *PBIBD* code, respectively and we shall investigate them in this and next sections.

Let N be the incidence matrix of a *PBIB* design with m^* associate classes and parameters v, b, r, k, λ_i, n_i, p^i_{jk} $(i, j, k=1, 2, \dots, m^*)$ and let C be a q-ary *PBIBD* code with parameters v, b, r, k, λ_i, n_i, p^i_{jk}, that is, let C be the q-ary linear code with length v which has N^T as a parity check matrix.

Suppose that $\boldsymbol{x}^T=(x_1, x_2, \ldots, x_v)$ is a transmitted code vector of C and the corresponding received vector is $\boldsymbol{r}^T=(r_1, r_2, \ldots, r_v)$. Then the error vector, $\boldsymbol{e}^T=(e_1, e_2, \ldots, e_v)$, is $\boldsymbol{r}^T-\boldsymbol{x}^T$ and the syndrome, $\boldsymbol{s}^T=(s_1, s_2, \ldots, s_b)$, of $\boldsymbol{r}^T$ is $(N^T\boldsymbol{r})^T$, i.e., $\boldsymbol{s}=N^T\boldsymbol{r}$. Applying the majority decoding algorithm [18, 30, 31] to a *PBIBD* code, we can obtain a relatively simple decoding algorithm as follows:

THEOREM 13.1. *Let C be a q-ary PBIBD code with parameters $v, b, r, k, \lambda_i, n_i, p^i_{jk}$ $(i, j, k=1, 2, \ldots, m^*)$ and let $\lambda=\max\{\lambda_1, \lambda_2, \ldots, \lambda_{m^*}\}$. Provided at most $\delta=[r/2\lambda]$ errors have occurred in transmitting the code vector, e_i $(i=1, 2, \ldots, v)$ are given correctly by the following rule*:

(i) *e_i is that value of* GF(q) *which is assumed by the greatest fraction of the $\{s_{\phi_1(i)}, s_{\phi_2(i)}, \ldots, s_{\phi_r(i)}\}$, if such a most frequent value exists where $\phi_l(i)$ $(l=1, 2, \ldots, r)$ denote the r integers j such that $n_{ij}=1$ for the given integer i $(1\leqq i\leqq v)$, that is, $n_{i\phi_1(i)}=n_{i\phi_2(i)}=\ldots=n_{i\phi_r(i)}=1$.*

(ii) *In the case where no single value is assumed by a strict plurality of the $\{s_{\phi_1(i)}, s_{\phi_2(i)}, \ldots, s_{\phi_r(i)}\}$, e_i is zero.*

Theorem 13.1 shows that a *PBIBD* code with parameters $v, b, r, k, \lambda_i, n_i, p^i_{jk}$ $(i, j, k=1, 2, \ldots, m^*)$ is capable of correcting up to $\delta=[r/2\lambda]$ errors. Hence, in *PBIBD* codes with the given length v, a *PBIBD* code with parameters such that $[r/2\lambda]$ is as large as possible is desirable. In the special case of a *BIBD* code, it follows from the equation $\lambda(v-1)=r(k-1)$ that a *BIBD* code with parameters v, b, r, k, λ such that k is as small as possible is desirable. Hence, a problem in *PBIBD* codes is how to construct a q-ary *PBIBD* code which has a relatively high transmission rate of information, in other words, a relatively small q-rank in *PBIBD* codes with the given parameters $v, b, r, k, \lambda_i, n_i, p^i_{jk}$.

Theorem 2.1 shows that the transmission rate of information of a q-ary *BIBD* code with parameters v, b, r, k, λ is never greater than $1/v$ unless q is a factor of r-λ and that for q which is a factor of r-λ, the transmission rate of a q-ary *BIBD* code depends on the block structure of the design which is used as a parity check matrix. For a *PBIBD* code, it follows from Theorem 3.1 that the transmission rate of information of a q-ary *PBIBD* code with parameters $v, b, r, \lambda_i, n_i, p^i_{jk}$ $(i, j, k=0, 1, \ldots, m)$ is zero unless q is a factor of $c_1 \prod_{i=0}^{m} c_2\rho_i$, provided that z_{ij}'s are all rational and $\rho_0\rho_1 \ldots \rho_m\neq 0$. For example, the transmission rate of a q-ary *PBIBD* code which has the transpose of the incidence matrix of a regular *GD* design as a parity check matrix is zero unless q is a factor of $vrk(rk-v\lambda_2)(r-\lambda_1)$ (see Theorem 5.1).

Table 6.1 shows that in Table 6.1, a q-ary *BIBD* code derived from PG(t, q) or EG(t, q) has the maximum transmission rate of information in *BIBD* codes with the same parameters. This suggests that a q-ary *BIBD* code derived from PG(t, q) or EG$(t\ q)$ might be the most desirable code in *BIBD* codes with the same parameters. (In the special case $k=2$, a *BIB* design with parameters:

$v=r+1$, $b=\binom{r+1}{2}$, $k=2$, $\lambda=1$ is unique and its p-rank is equal to v or $v-1$ according as a prime p is odd or not. So, such a design is omitted from Table 6.1). In Section 14, we shall investigate such a geometric code in detail.

14. Applications to geometric codes

A q-ary linear code C of length n is called a cyclic code if, for every code vector $(c_0, c_1, \ldots, c_{n-1})$ of C, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also a code vector of C. A convenient representation of cyclic codes may be made through the theory of ideals in the residue class ring of polynomials over GF(q) modulo x^n-1 [26]. In the residue class ring, we correspond the polynomial $c(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$ with the vector $\boldsymbol{c}^T=(c_0, c_1, \ldots, c_{n-1})$. Under this correspondence, it may be shown that a linear code C is cyclic if and only if it is an ideal in the residue class ring. Such ideal C contains a unique monic generator polynomial, $g(x)$, of smallest degree less than n such that each element of C is a multiple of $g(x)$. Moreover, $g(x)$ is a divisor of x^n-1 in GF(q), say $x^n-1=g(x)h(x)$. The dual code of C is also cyclic and its generator polynomial, $g_D(x)$, is given by

$$g_D(x)=x^k h(x^{-1}) \tag{14.1}$$

where k is the degree of $h(x)$.

A cyclic code may be specified by the roots of its generator polynomial of an extension field of GF(q). In the case where the code length n is a divisor of q^u-1 for some positive integer $u \geqq 2$, which has been investigated by many authors, the roots of x^n-1 are simple and are expressed by $\beta^0, \beta^1, \beta^2, \ldots, \beta^{n-1}$ where $\beta=\alpha^{(q^u-1)/n}$ and α is a primitive element of GF(q^u). In such a case, every root of the generator polynomial of a cyclic code is simple and is expressed by a power of β, say β^h. A characterization of a class of cyclic codes can, therefore, be made by the type of the roots of their generator polynomials.

14.1 Projective Geometry codes

Let $N(q;\, t,\, \mu)$ be the incidence matrix of $v=(q^{t+1}-1)/(q-1)$ points and $b=\phi(t, \mu, q)$ μ-flats in PG(t, q) where q is a prime power, say $q=p^m$.

Definition 14.1.1. A q-ary μth order Projective Geometry (*PG*) code is a q-ary linear code of length v which has $N(q;\, t,\, \mu)^T$ as a parity check matrix.

It is known [31] that this code is a cyclic code and by using the generator polynomial, it may also be defined as follows:

Definition 14.1.2. A q-ary μth order Projective Geometry code is the cyclic code of length $v=(q^{t+1}-1)/(q-1)$ with symbols from GF(q) such that the generator polynomial $g_D(x)$ of the dual code has as roots those elements $\alpha^{h(q-1)}$, $1 \leqq h \leqq v$, such that

$$0 < \min_{0 \leqq l < m} D_q[p^l h(q-1)] \leqq \mu(q-1) \tag{14.1.1}$$

where α is a primitive element of $GF(q^{t+1})$ and $D_p[n]$ is defined by (9.22).

From Definition 14.1.1 and Theorem 7.2, we have the following theorem:

THEOREM 14.1.1. *The number of information symbols of a q-ary μth order Projective Geometry code of length $v=(q^{t+1}-1)/(q-1)$ is equal to $v-R_\mu(t, p^m)$ and the number of information symbols of its dual code is equal to $R_\mu(t, p^m)$ where $q=p^m$ and $R_\mu(t, p^m)$ is given by* (7.9).

In the special case $m=1$, we have the following corollary:

COROLLARY 14.1.2. *The number of information symbols of a p-ary μth order Projective Geometry code of length $v=(p^{t+1}-1)/(p-1)$ is equal to $v-R_\mu(t, p)$ and the number of information symbols of its dual code is equal to $R_\mu(t, p)$ where $R_\mu(t, p)$ is given by* (7.12).

This result has been obtained by Smith [31]. The Projective Geometry code defined by Definition 14.1.1 may also be characterized as follows:

THEOREM 14.1.3. *Let h be an integer such that $1 \leqq h \leqq v$ and let the p-adic representation of $h(q-1)$ be*

$$h(q-1) = \sum_{i=0}^{t} \sum_{j=0}^{m-1} c_{ij} p^{im+j} \tag{14.1.2}$$

where $q=p^m$ and c_{ij}'s are non-negative integer less than p. Then β^h is a root of the generator polynomial $g_D(x)$ of the dual code of the q-ary μth order PG *code if and only if h is an integer such that*

$$\sum_{i=0}^{t} c_{ij} = s_{j+1}p - s_j \qquad (j=0, 1, \dots, m-1) \tag{14.1.3}$$

for some integers $(s_0, s_1, \dots, s_m)$ in $T_{t,\mu}(p^m)$ where $\beta=\alpha^{q-1}$ and $T_{t,\mu}(p^m)$ is a set of $(m+1)$-tuples $(s_0, s_1, \dots, s_m)$ of integers s_l such that

$$s_m = s_0,\ 1 \leqq s_j \leqq t+1,\ 0 \leqq s_{j+1}p - s_j \leqq (t+1)(p-1) \tag{14.1.4}$$

for $j=0, 1, \dots, m-1$ and $1 \leqq s_k \leqq \mu$ for some integer k.

PROOF. Let Σ be a μ-flat ($\mu(0)$-flat) in $PG(t, q)$ composed of $k=(q^{\mu+1}-1)/(q-1)$ points (α^{c_1}), (α^{c_2}), $\dots$, (α^{c_k}) and we define the incidence polynomial $\theta_\Sigma(x)$ of the μ-flat Σ as the polynomial:

$$\theta_\Sigma(x) = x^{c_1} + x^{c_2} + \cdots + x^{c_k}. \tag{14.1.5}$$

Between $\theta_\Sigma(x)$ and $S_\Sigma(x)$ defined by (10.15), the following relation holds:

(14.1.6)
$$S_\Sigma(x)=\theta_\Sigma(x)+x^v\theta_\Sigma(x)+\cdots+{}^{(q-2)v}\theta_\Sigma(x)$$
$$\equiv(q-1)\theta_\Sigma(x) \qquad \mathrm{mod}\ x^v-1.$$

From Theorems 10.10, 10.11 and (14.1.6), it follows that a necessary and sufficient condition for an integer h, $1\leqq h\leqq v$, that there exists at least one μ-flat Σ in PG(t, q) such that $\theta_\Sigma(\alpha^{h(q-1)})\neq 0$ is that h is an integer such that there exists an $(m+1)$-tuple $(s_0, s_1, \ldots, s_m)$ in $S^*_{t,\mu}(p^m)$ such that $\sum_{i=0}^{t} c_{ij}=s_{j+1}p-s_j$ for $j=0, 1, \ldots, m-1$. From the above result, Lemmas 2.1 and 2.3 in [12] due to the present author, it is easy to see that a necessary and sufficient condition for an integer h that $\theta_\Sigma(\beta^h)=0$ for every μ-flat Σ is that h is an integer such that there exists an $(m+1)$-tuple $(s_0, s_1, \ldots, s_m)$ satisfying the condition (14.1.3) in $T_{t,\mu}(p^m)$. Since β^h is a root of $g_D(x)$ if and only if $\theta_\Sigma(\alpha^h)=0$ for every μ-flat Σ, we have the required result.

COROLLARY 14.1.4. *The generator polynomial $g(x)$ of the q-ary μth order* PG *code has β^h as a root if and only if h is an integer such that there exists an $(m+1)$-tuple $(s_0, s_1, \ldots, s_m)$ satisfying the condition* (14.1.3) *in $S_{t,\mu}(p^m)$ where $S_{t,\mu}(p^m)$ is the set of $(m+1)$-tuples $(s_0, s_1, \ldots, s_m)$ of integers s_l ($l=0, 1, \ldots, m$) satisfying the following conditions*:

(14.1.7)
$$s_0=s_m,\ 0\leqq s_j\leqq t-\mu,\ 0\leqq s_{j+1}p-s\leqq(t+1)(p-1)$$

for $j=0, 1, \ldots, m-1$.

PROOF. From (14.1), it follows that the generator polynomial $g(x)$ is given by

(14.1.8)
$$g(x)=x^r h_D(x^{-1})$$

where $h_D(x)$ is a polynomial of degree $r=R_\mu(t, p^m)$ such that

(14.1.9)
$$g_D(x)h_D(x)=x^v-1.$$

Since β^h $(1\leqq h\leqq v)$ is a root of $h_D(x)$ if and only if h is an integer such that there exists an $(m+1)$-tuple $(s_0, s_1, \ldots, s_m)$ satisfying the condition (14.1.3) in $S^*_{t,\mu}(p^m)$ and $\beta^{-h}=\beta^{v-h}$, we have the required result from (14.1.8).

It is known that the minimum distance of a q-ary μth order *PG* code is at least equal to $d_{BCH}=(q^{t-\mu+1}-1)/(q-1)+1$ and the minimum distance of its dual code is equal to $(q^{\mu+1}-1)/(q-1)$ where d_{BCH} denotes the designed distance of a *BCH* code [3, 4, 13]. We can therefore summarize these results as follows:

THEOREM 14.1.5. *A q-ary μth order PG code is a cyclic code with parameters*:

(14.1.10) $$n=(q^{t+1}-1)/(q-1),\ k=n-R_\mu(t,\ p^m),\ d\geqq(q^{t-\mu+1}-1)/(q-1)+1$$

and its dual code is also a cyclic code with parameters:

(14.1.11) $$n=(q^{t+1}-1)/(q-1),\ k=R_\mu(t,\ p^m),\ d=(q^{\mu+1}-1)/(q-1)$$

where n, k and d denote the code length, the number of information symbols and the minimum distance of the code, respectively.

14.2 Affine Geometry codes

Let $M_1(q;\ t,\ \mu)$ be the incidence matrix of q^t-1 points other than the origin and b_1 μ-flats not passing though the origin in EG$(t,\ q)$.

DEFINITION 14.2.1. A q-ary μth order Affine Geometry (AG) code is a q-ary linear code of length $n=q^t-1$ which has $M_1(q;\ t,\ \mu)^T$ as a parity check matrix.

The term Affine Geometry code has been introduced by Smith [31] and it is defined as follows:

DEFINITION 14.2.2. A q-ary μth order Affine Geometry code is the cyclic code of length $n=q^t-1$ with symbols from $GF(q)$ such that the generator polynomial $g_D(x)$ of the dual code has as roots those elements α^h, $0\leqq h<q^t-1$, such that

(14.2.1) $$0\leqq \min_{0\leqq l<m} D_q[p^l h]<\mu(q-1)$$

where $q=p^m$ and α is a primitive element of $GF(q^t)$.

We shall show that the above two definitions are quivalent. The q-ary μth order AG code defined by Definition 14.2.1 can be characterized as follows:

THEOREM 14.2.1. *Let h be an integer such that* $1\leqq h\leqq q^t-1$ *and let the p-adic representation of h be*

(14.2.2) $$h=\sum_{i=0}^{t-1}\sum_{j=0}^{m-1} c_{ij}p^{im+j}$$

where $q=p^m$ *and* c_{ij}*'s are non-negative integers less than p. Then* α^h *is a root of the generator polynomial* $g_D(x)$ *of the dual code of the q-ary* μ*th order AG code defined by Definition* 14.2.1 *if and only if h is* q^t-1 *or an integer such that there exists an* $(m+1)$*-tuple* $(s_0,\ s_1,\ \ldots,\ s_m)$ *in* $T_{t,\mu}(p^m)$ *such that*

(14.2.3) $$(s_{j+1}-1)p-(s_j-1)\leqq \sum_{i=0}^{t-1} c_{ij}\leqq s_{j+1}p-s_j$$

for every $j=0,\ 1,\ \ldots,\ m-1$ *and that*

$$\sum_{i=0}^{t-1} c_{ik} < s_{k+1}p - s_k \tag{14.2.4}$$

for some integer k.

To prove the above theorem, we prepare the following lemmas:

LEMMA 14.2.2. *For any set* $\{c_{ij};\ i=0, 1, \ldots, t-1,\ j=0, 1, \ldots, m-1\}$ *of nonnegative integers* c_{ij} *less than p, not all zero, there exists a unique set of integers* s_l $(l=0, 1, \ldots, m)$ *satisfying the conditions* (14.1.4), (14.2.3) *and* (14.2.4).

PROOF. Let $h=\sum_{i=0}^{t-1}\sum_{j=0}^{m-1} c_{ij}p^{im+j}$. Then h is an integer such that $1 \leqq h \leqq q^t - 1$.

(i) In the case where h is not a multiple of p^m-1; there exists a unique set $\{c_{tj};\ j=0, 1, \ldots, m-1\}$ of non-negative integers c_{tj} less than p, not all zero, such that $\sum_{i=0}^{t}\sum_{i=0}^{m-1} c_{ij}p^{im+j}$ is a multiple of p^m-1. It follows therefore from Lemma 2.1 due to Hamada [12] that there exists a unique set of $m+1$ integers s_l $(l=0, 1, \ldots, m)$ such that

$$s_m = s_0,\ 1 \leqq s_j \leqq t+1 \quad \text{and} \quad \sum_{i=0}^{t} c_{ij} = s_{j+1}p - s_j \tag{14.2.5}$$

for $j=0, 1, \ldots, m-1$. Since c_{tj}'s are non-negative integers less than p, not all zero, these integers s_l $(l=0, 1, \ldots, m)$ satisfy the conditions (14.1.4), (14.2.3) and (14.2.4). Hence, in this case, Lemma 14.2.2 holds.

(ii) In the case where h is a multiple of p^m-1; there exists a unique set of $m+1$ integers s_l^* $(l=0, 1, \ldots, m)$ such that

$$s_m^* = s_0^*,\ 1 \leqq s_j^* \leqq t \quad \text{and} \quad \sum_{i=0}^{t-1} c_{ij} = s_{j+1}^*p - s_j^* \tag{14.2.6}$$

for $j=0, 1, \ldots, m-1$. Let $s_l = s_l^*+1$ for $l=0, 1, \ldots, m$. Then s_l's satisfy the conditions (14.1.4), (14.2.3) and (14.2.4). Hence, we have the required result.

From Lemma 3.2 in [12], we have the following lemma:

LEMMA 14.2.3. *For any set* $\{c_{ij};\ i=0, 1, \ldots, t-1,\ j=0, 1, \ldots, m-1\}$ *of non-negative integers* c_{ij} *less than p such that there exists a set of integers* s_l^* $(l=0, 1, \ldots, m)$ *satisfying the following conditions*:

$$s_m^* = s_0^*,\ \mu+1 \leqq s_j^* \leqq t+1,\ 0 \leqq s_{j+1}^*p - s_j^* \leqq (t+1)(p-1) \tag{14.2.7}$$

and

$$\sum_{i=0}^{t-1} c_{ij} \geqq (s_{j+1}^*-1)p - (s_j^*-1) \tag{14.2.8}$$

for $j=0, 1, \ldots, m-1$, *there exists a unique set of integers* s_l $(l=0, 1, \ldots, m)$ *satisfying the conditions* (14.2.3), (14.2.4) *and*

$$s_m=s_0,\ \mu+1\leqq s_j\leqq t+1,\ 0\leqq s_{j+1}p-s_j\leqq(t+1)(p-1) \tag{14.2.9}$$

for $j=0, 1, \ldots, m-1$.

(Proof of Theorem 14.2.1) From Theorems 9.12 and 9.14, it follows that a necessary and sufficient condition for the integer h that there exists a μ-flat Σ^* not passing though the origin such that $\theta_{\Sigma^*}(\alpha^h)\neq 0$ is that h is an integer such that (i) $h\neq q^t-1$ and (ii) there exists a set of $m+1$ integers s_l^* $(l=0, 1, \ldots, m)$ satisfying the conditions (14.2.7) and (14.2.8). Using the above result, Lemmas 14.2.2 and 14.2.3, it can be shown that a necessary and sufficient condition for integer h that $\theta_{\Sigma^*}(\alpha^h)=0$ for every μ-flat Σ^* not passing through the origin in EG(t, q) is that h is q^t-1 or an integer such that there exists an $(m+1)$-tuple $(s_0, s_1, \ldots, s_m)$ of integers s_l $(l=0, 1, \ldots, m)$ satisfying the conditions (14.2.3) and (14.2.4) in $T_{t,\mu}(p^m)$. Since α^h is a root of $g_D(x)$ if and only if $\theta_{\Sigma^*}(\alpha^h)=0$ for every μ-flats not passing through the origin in $EG(t, q)$, we have the required result.

COROLLARY 14.2.4. *The generator polynomial $g(x)$ of the q-ary μth order AG code has α^h as a root if and only if h is a positive integer less than q^t-1 such that there exists an $(m+1)$-tuple $(s_0, s_1, \ldots, s_m)$ satisfying the conditions* (14.2.3) *and* (14.2.4) *in $S_{t,\mu}(p^m)$, provided that h is an integer such that $1\leqq h\leqq q^t-1$.*

THEOREM 14.2.5. *The q-ary μth order PG code defined by Definition* 14.2.1 *and the q-ary μth order PG code defined by Definition* 14.2.2 *are equivalent.*

PROOF. Since $\alpha^{q^t-1}=\alpha^0$, it suffices to consider only the case where $1\leqq h< q^t-1$. If h is an integer satisfying the conditions in Theorem 14.2.1, then we have

$$\begin{aligned} D_q[p^l h] &= \sum_{i=0}^{t-1}\sum_{j=0}^{m-1-l} c_{ij}p^{j+l}+\sum_{i=0}^{t-1}\sum_{j=m-l}^{m-1} c_{ij}p^{j+l-m} \\ &< \sum_{j=0}^{m-1-l}(s_{j+1}p-s_j)p^{j+l}+\sum_{j=m-l}^{m-1}(s_{j+1}p-s_j)p^{j+l-m} \\ &= s_{m-l}(p^m-1) \end{aligned} \tag{14.2.10}$$

for each $l=0, 1, \ldots, m$. Since $s_{m-k}\leqq\mu$ for some integer k, it follows that

$$D_q[p^k h]< s_{m-k}(q-1)\leqq\mu(q-1) \tag{14.2.11}$$

for some integer k. This implies that the integer h satisfies the condition (14.2.1).

Conversely, if h is positive integer satisfying the condition (14.2.1), there exists an integer $h_0=\sum_{j=0}^{m-1} c_{tj}p^{tm+j}$ such that $h^*=h_0+h$ is a multiple of p^m-1 where c_{tj} $(j=0, 1, \dots, m-1)$ are non-negative integers less than p, not all zero. Hence, it follows from Lemma 2.2 in [12] that

$$D_q[p^l h^*]=D_q[p^l h_0]+D_q[p^l h] \tag{14.2.12}$$

for each $l=0, 1, \dots, m$. Since $h^*=\sum_{i=0}^{t}\sum_{j=0}^{m-1} c_{ij}p^{im+j}$ is a multiple of p^m-1, it follows from Lemma 2.1 in [12] that there exists a unique set of $m+1$ integers s_l $(l=0, 1, \dots, m)$ satisfying the condition (14.2.5). Since c_{ij}'s are non-negative integers less that p and c_{tj}'s are not all simultaneously zero, $\sum_{i=0}^{t-1} c_{ij}$'s satisfy the conditions (14.2.3) and (14.2.4) for the integers s_l. It suffices therefore to show that there exists at least one integer s_k such that $s_k \leqq \mu$.

Using a similar method used in (14.2.10), we have

$$D_q[p^l h^*]=s_{m-l}(p^m-1)=s_{m-l}(q-1) \tag{14.2.13}$$

for $l=0, 1, \dots, m$. Since $D_q[p^{m-k}h]<\mu(q-1)$ for some integer k and

$$D\ [p^l h_0]=\sum_{j=0}^{m-1-l} c_{tj}p^{j+l}+\sum_{j=m-l}^{m-1} c_{tj}p^{j+l-m}<p^m-1,$$

it follows from (14.2.12) and (14.2.13) that $s_k<(\mu+1)$ for some integer k. This completes the proof.

From Definition 14.2.1 and Theorem 11.1, we have the

THEOREM 14.2.6. *The number of information symbols of a q-ary μth order AG code of length $n=q^t-1$ is equal to $n-\{R_\mu(t, p^m)-R_\mu(t-1, p^m)-1\}$ and the number of information symbols of its dual code is equal to $R_\mu(t, p^m)-R_\mu(t-1, p^m)-1$ where $q=p^m$ and $R_\mu(t, p^m)$ is given by (7.9).*

Since the minimum distance of a q-ary μth order AG code is at least equal to $q^{t-\mu}+pq^{t-\mu-1}-1$ and the minimum distance of its dual code is equal to q^μ, we can summarize those results as follows:

THEOREM 14.2.7. *A q-ary μth order Affine Geometry code is a cyclic code with parameters:*

$$n=q^t-1,\quad k=n-\{R_\mu(t, p^m)-R_\mu(t-1, p^m)-1\},\quad d\geqq q^{t-\mu}+pq^{t-\mu-1}-1$$

and its dual code is a cyclic code with parameters:

$$n=q^t-1,\quad k=R_\mu(t, p^m)-R_\mu(t-1, p^m)-1,\quad d=q^\mu.$$

14.3 Euclidean Geometry codes

Let $M(q;\ t,\ \mu)$ be the incidence matrix (defined by (9.5)) of q^t-1 points other than the origin and all μ-flats in EG$(t,\ q)$.

DEFINITION 14.3.1. A q-ary μth order Euclidean Geometry (*EG*) code is a q-ary linear code of length $n=q^t-1$ which has $M(q;\ t,\ \mu)^T$ as a parity check matrix.

This code is a cyclic code and can be characterized as follows:

THEOREM 14.3.1. *Let h be an integer such that $1\leqq h\leqq q^t-1$ and let the p-adic representation of h be*

$$h=\sum_{i=0}^{t-1}\sum_{j=0}^{m-1}c_{ij}q^{im+j}.$$

Then the generator polynomial $g_D(x)$ of the dual code of a q-ary μth order Euclidean Geometry code has α^h as a root if and only if h is an integer such that there exists an $(m+1)$-tuple $(s_0,\ s_1,\ \dots,\ s_m)$ satisfying the conditions (14.2.3) *and* (14.2.4) *in $T_{t,\mu}(p^m)$.*

PROOF. From Theorems 9.11 and 9.12, it follows that (i) in the case when $1\leqq h\leqq q^t-2$, a necessary and sufficient condition for an integer h that there exists a μ-flat Σ_0 (passing or not passing through the origin) in EG$(t,\ q)$ such that $\theta_{\Sigma_0}(\alpha^h)\neq 0$ is that there exists a μ-flats Σ^* not passing through the origin such that $\theta_{\Sigma^*}(\alpha^h)\neq 0$ and (ii) in the case when $h=q^t-1$, there does not exist a μ-flat Σ^* not passing through the origin such that $\theta_{\Sigma^*}(\alpha^{q^t-1})\neq 0$ but exists a μ-flat Σ passing through the origin such that $\theta_{\Sigma}(\alpha^{q^t-1})\neq 0$. This implies that (i) in the case when $1\leqq h\leqq q^t-2$, $g_{ED}(x)$ has α^h as a root if and only if $g_{AD}(x)$ has α^h as a root and (ii) q^t-1 is not a root of $g_{ED}(x)$, where $g_{ED}(x)$ and $g_{AD}(x)$ denote the generator polynomials of the dual codes of the *EG* code and the *AG* code, respectively. Since there is no $(m+1)$-tuple $(s_0, s_1, \dots, s_m)$ satisfying the conditions (14.2.3) and (14.2.4) in $T_{t,\mu}(p^m)$ for integer $h=q^t-1$, we have the required result from Theorem 14.2.1.

COROLLARY 14.3.2. *The generator polynomial $g(x)$ of the q-ary μth order Euclidean Geometry code has α^h as a root if and only if h is an integer such that there exists an $(m+1)$-tuple $(s_0,\ s_1,\ \dots,\ s_m)$ satisfying the conditions* (14.2.3) *and* (14.2.4) *in $S_{t,\mu}(p^m)$, provided that h is an integer such that $1\leqq h\leqq q^t-1$.*

EXAMPLE 14.3.1. Let us consider the case when $p=2$, $m=2$, $t=3$ and $\mu=1$. In this case, $q=4$ and $T_{3,1}(2^2)=\{(1,\ 1,\ 1),\ (1,\ 2,\ 1),\ (2,\ 1,\ 2)\}$. The generator polynomial $g_D(x)$ of the dual code of the 4-ary 1st order Euclidean Geometry code with length 63 can be obtain as follows:

In the case $(s_0, s_1, s_2)=(1, 1, 1)$, there are six solutions for ordered sets $(c_{00}, c_{10}, c_{20}; c_{01}, c_{11}, c_{21})$, not all zero, satisfying the conditions (14.2.3) and (14.2.4) as follows:

$$(1, 0, 0; 0, 0, 0), \quad (0, 1, 0; 0, 0, 0), \ldots, (0, 0, 0; 0, 0, 1).$$

Let $h=\sum_{i=0}^{2} \sum_{j=0}^{1} c_{ij}2^{2i+j}$. Then $h=1, 2, 4, 8, 16$ and 32. Similarly, it follows from $(s_0, s_1, s_2)=(1, 2, 1)$ and $(2, 1, 2)$ that $h=5$, 17, 20, 10, 34 and 40. Let α be a primitive element of $GF(4^3)$. For example, let α be a root of the irreducible function $f(x)=x^3+\gamma x^2+\gamma x+\gamma$ where γ is a primitive element of $GF(2^2)$ such that $\gamma^2=\gamma+1$ and $\gamma^3=1$. Then,

$$\begin{aligned} g_D(x) &= (x-\alpha^1)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})(x-\alpha^{32}) \\ &\quad \cdot(x-\alpha^5)(x-\alpha^{10})(x-\alpha^{20})(x-\alpha^{40})(x-\alpha^{17})(x-\alpha^{34}) \\ &= x^{12}+x^{10}+x^9+x^7+x^3+x^2+1. \end{aligned}$$

From Theorem 14.2.1, 14.3.1 and 14.2.5, we can see that using the generator polynomial, the *EG* code defined by Definition 14.3.1 may also be defined as follows:

DEFINITION 14.3.2. A q-ary μth order Euclidean Geometry code is the cyclic code of length $n=q^t-1$ with sumbols from $GF(q)$ such that the generator polynomial $g_D(x)$ of the dual code has as roots those elements α^h, $1 \leqq h \leqq q^t-2$, such that

$$0<\min_{0 \leqq l<m} D_q[p^l h]<\mu(q-1) \tag{14.3.2}$$

where α is a primitive element of $GF(q^t)$.

In the case $q=2^m$, this code was introduced by Weldon [34] and called a (v, m)th order Euclidean Geometry code where $v=t-\mu$.

From Theorem 9.1 and Definition 14.3.1, we have the following theorem:

THEOREM 14.3.3. *The number of information symbols of a q-ary μth order Euclidean Geometry code of length $n=q^t-1$ is equal to $n-\{R_\mu(t, p^m)-R_\mu(t-1, p^m)\}$ where $q=p^m$ and $R_\mu(t, p^m)$ is given by* (7.9).

It is known that the minimum distance of a q-ary μth order *EG* code is at least equal to $q^{t-\mu}+pq^{t-\mu-1}$ and the minimum distance of the dual code is equal to $q^\mu-1$. We can therefore summarize those results as follows:

THEOREM 14.3.4. *A q-ary μth order Euclidean Geometry code is a cyclic code with the following parameters*:

$$n=q^t-1, \quad k=n-R_\mu(t, p^m)-R_\mu(t-1, p^m), \quad d \geqq q^{t-\mu}+pq^{t-\mu-1}$$

and its dual code is a cyclic code with parameters:

$$n=q^t-1, \quad k=R_\mu(t, p^m)-R_\mu(t-1, p^m), \quad d=q^\mu-1.$$

Let $M^*(q; t, \mu)$ be the incidence matrix (defined by (9.2)) of all points and all μ-flats in $EG(t, q)$.

DEFINITION 14.3.3. A q-ary μth order extended Euclidean Geometry (EEG) code is a q-ary linear code of length $n=q^t$ which has $M^*(q; t, \mu)^T$ as a parity check matrix.

This code is not a cyclic code. From Theorem 9.2 and Definition 14.3.3, we have the following theorem:

THEOREM 14.3.5. *The number of information symbols of a q-ary μth order EEG code of length $n=q^t$ is equal to $n-\{R_\mu(t, p^m)-R_\mu(t-1, p^m)\}$.*

15. Applications to polynomial codes and Reed-Muller codes

(a) Definition and the main theorems

Let q be a prime power, say $q=p^{m_0}$ and let t and m be any positive integers. Suppose that b is a factor of q^m-1 and let

$$z=(q^m-1)/b \quad \text{and} \quad n=(q^{mt}-1)/b. \tag{15.1}$$

DEFINITION 15.1. An (n, t, m, v, q)-polynomial code is the cyclic code of length $n=(q^{mt}-1)/b$ with symbols from $GF(q)$ such that the generator polynomial $g_D(x)$ of the dual code has as roots those elements α^{hb}, $0\leqq h<n$, such that

$$\max_{0\leqq l<m} D_{q^m}[q^l hb]=jb \tag{15.2}$$

for some integer $j(0\leqq j\leqq v)$ where $D_q[n]$ is defined by (9.22) and α is a primitive element of $GF(q^{mt})$ and v is an integer such that $1\leqq v<tz$.

This code has been introduced by Kasami, Lin and Peterson [17]. An explicit formula for the number of information symbols has not yet been obtained. In this section, we shall show that using a similar method used in proving Theorem 7.1, an explicit formula for the number of information symbols of a polynomial code can be obtained.

We denote by $T(t, z, m, q)$, the set of $(m+1)$-tuples $(s_0, s_1, \ldots, s_m)$ of integers s_j such that

$$s_m=s_0, \quad 0\leqq s_j<tz \quad \text{and} \quad 0\leqq(s_{j+1}q-s_j)/z\leqq t(q-1) \tag{15.3}$$

and that $(s_{j+1}p-s_j)/z$ is an integer for each $j=0, 1, \ldots, m-1$ and by $S_v(t, z, m, q)$, the set of $(m+1)$-tuples $(s_0, s_1, \ldots, s_m)$ of integers s_j such that

$$(s_0, s_1, \ldots, s_m) \in T(t, z, m, q) \quad \text{and} \quad 0 \leqq s_l \leqq v \tag{15.4}$$

for every $l=0, 1, \ldots, m$. Then we have the following main theorem:

THEOREM 15.1. *The number of information symbols of the (n, t, m, v, q)-polynomial code is equal to*

$$I_v(t, z, m, q) = \sum_{(s_0, \ldots, s_m)} \prod_{j=0}^{m-1} \sum_{i=0}^{L_z(s_{j+1}, s_j)} (-1)^i \binom{t}{i} \binom{t-1+(s_{j+1}q-s_j)/z-iq}{t-1} \tag{15.5}$$

where the summation is taken over all $(m+1)$-tuples $(s_0, s_1, \ldots, s_m)$ in $S_v(t, z, m, q)$ and $L_z(s_{j+1}, s_j) = [(s_{j+1}q - s_j)/qz]$, i.e., $L_z(s_{j+1}, s_j)$ is the greatest integer not exceeding $(s_{j+1}q - s_j)/qz$.

In the special case $z=1$ and $q=p$, we have the

COROLLARY 15.2. *The number of information symbols of the $((p^{mt}-1)/(p^m-1), t, m, v, p)$-polynomial code is equal to*

$$I_v(t, 1, m, p) = R_{t-1-v}(t-1, p^m) \tag{15.6}$$

where $R_\mu(t, p^m)$ is given by (7.9).

In the special case $m=1$, we have the

COROLLARY 15.3. *The number of information symbols of the $(n, t, 1, v, q)$-polynomial code is equal to*

$$I_v(t, z, 1, q) = \sum_s \sum_{i=0}^{L_z(s,s)} (-1)^i \binom{t}{i} \binom{t-1+s(q-1)/z-iq}{t-1} \tag{15.7}$$

where the summation is taken over all integers s such that $0 \leqq s \leqq v$ and that $s(q-1)/z$ is an integer, and $L_z(s, s) = [s(q-1)/qz]$.

In the special case $b=1$ (i.e., $z=q^m-1$ and $n=q^{mt}-1$) and $v=v_0(q^m-1)-1$ for some positive integer v_0, we have the following theorem which may be useful in calculating $I_v(t, q^m-1, m, q)$.

THEOREM 15.4. *The number of information symbols of the $(q^{mt}-1, t, m, v_0(q^m-1)-1, q)$-polynomial code is equal to*

$$I_{v_0(q^m-1)-1}(t, q^m-1, m, q) = I_{v_0}(t+1, 1, m, q) - I_{v_0}(t, 1, m, q). \tag{15.8}$$

In the special case $q=p$, we have the following corollary:

COROLLARY 15.5. *The number of information symbols of the $(p^{mt}-1, t, m, v_0(p^m-1)-1, p)$-polynomial code is equal to*

$$I_{v_0(p^m-1)-1}(t, p^m-1, m, p) = R_{t-v_0}(t, p^m) - R_{t-1-v_0}(t-1, p^m). \tag{15.9}$$

The following generalization of the original Reed-Muller code [19, 29] to the non-binary case is due to Kasami, Lin and Peterson [16].

DEFINITION 15.2. The νth order Generalized Reed-Muller (GRM) code is the cyclic code of length $n=q^t-1$ with symbols from $GF(q)$ such that the generator polynomial $g_D(x)$ of the dual code has as roots those elements α^h, $0 \leqq h < q^t-1$, such that $D_q[h] \leqq \nu$.

From Definitions 15.1 and 15.2, it follows that the νth order GRM code is the $(q^t-1, t, 1, \nu, q)$-polynomial code with parameters:

$$n=q^t-1,\ b=1,\quad m=1\qquad \text{and}\quad z=q-1. \tag{15.10}$$

From Corollary 15.3, we have therefore the following corollary:

COROLLARY 15.6. *The number of information symbols of the νth order GRM code is equal to*

$$I_\nu(t, q-1, 1, q)=\sum_{s=0}^{\nu}\sum_{i=0}^{[s/q]}(-1)^i\binom{t}{i}\binom{t-1+s-iq}{t-1}. \tag{15.11}$$

In the special case $\nu=\nu_0(q-1)-1$ for some interger ν_0, we have the

COROLLARY 15.7. *The number of information symbols of the $(\nu_0(q-1)$ $-1)$st order GRM code is equal to*

$$I_{\nu_0(q-1)-1}(t, q-1, 1, q)=I_{\nu_0}(t+1, 1, 1, q)-I_{\nu_0}(t, 1, 1, q) \tag{15.12}$$

where

$$I_{\nu_0}(t, 1, 1, q)=\sum_{s=0}^{\nu_0}\sum_{i=0}^{[s(q-1)/q]}(-1)^i\binom{t}{i}\binom{t-1+s(q-1)-iq}{t-1}. \tag{15.13}$$

This result has been obtained by Smith [31]. In the special case $q=2$, we have the following well known result:

COROLLARY 15.8. *The number of information symbols of the νth order Reed-Muller code is equal to*

$$I_\nu(t, 1, 1, 2)=1+\binom{t}{1}+\binom{t}{2}+\cdots+\binom{t}{\nu}. \tag{15.14}$$

(b) Proof of the main theorems

In order to prove Theorem 15.1, we prepare the following lemmas:

LEMMA 15.9. *Let h be an integer such that $0 \leqq h < (q^{mt}-1)/b$ and let the q-adic representation of hb be*

$$hb=\sum_{i=0}^{t-1}\sum_{j=0}^{m-1}c_{ij}q^{im+j} \tag{15.15}$$

where c_{ij}'s are integers such that $0 \leqq c_{ij} < q$. Then there exists a unique set of $m+1$ integers s_l ($l=0, 1, \ldots, m$) such that

$$(15.16) \qquad s_m = s_0, \quad 0 \leqq s_j < zt, \quad 0 \leqq (s_{j+1}q - s_j)/z \leqq t(q-1),$$

$$(15.17) \qquad z\sum_{i=0}^{t-1} c_{ij} = s_{j+1}q - s_j \qquad \text{and} \quad D_{q^m}[q^j hb] = s_{m-j}b$$

for $j=0, 1, \ldots, m-1$.

Note that since c_{ij}'s are non-negative integers less than q, $(s_{j+1}q - s_j)/z$'s must be integers such that $0 \leqq (s_{j+1}q - s_j)/z \leqq t(q-1)$.

PROOF. Since

$$(15.18) \qquad \sum_{i=0}^{t-1}\sum_{j=0}^{m-1} c_{ij}q^j = \sum_{i=0}^{t-1}\sum_{j=0}^{m-1} c_{ij}q^{im+j} - \sum_{i=0}^{t-1}\sum_{j=0}^{m-1} c_{ij}(q^{im}-1)q^j,$$

it follows from (15.15) and (15.1) that the left hand side of (15.18) is a multiple of b. There exists therefore an integer r, $0 \leqq r < tz$, such that

$$(15.19) \qquad \sum_{t=0}^{i-1}\sum_{j=0}^{m-1} c_{ij}q^j = rb.$$

Since $b = (q^m - 1)/z$, we have

$$(15.20) \qquad z\sum_{i=0}^{t-1}\sum_{j=0}^{m-1} c_{ij}q^j = r(q^m - 1).$$

This equation can be expressed as follows:

$$(15.21) \qquad r + z\sum_{i=0}^{t-1}\sum_{j=0}^{j_0-1} c_{ij}q^j = rq^m - z\sum_{i=0}^{t-1}\sum_{j=j_0}^{m-1} c_{ij}q^j$$

for each $j_0 = 1, 2, \ldots, m-1$. Since the right hand side of (15.21) is a multiple of q^{j_0}, there exist $m-1$ integers s_{j_0}, $0 \leqq s_{j_0} < tz$, such that

$$(15.22) \qquad r + z\sum_{i=0}^{t-1}\sum_{j=0}^{j_0-1} c_{ij}q^j = s_{j_0}q^{j_0}$$

for each $j_0 = 1, 2, \ldots, m-1$. Solving $m-1$ equations (15.22), we have

$$(15.23) \qquad z\sum_{i=0}^{t-1} c_{ij} = s_{j+1}q - s_j$$

for $j=0, 1, \ldots, m-1$ where $s_m = s_0 = r$. The uniqueness of the set of intergers s_l ($l=0, 1, \ldots, m$) is obvious. From the definition of $D_q[n]$, it follows that

$$(15.24) \qquad zD_{q^m}[q^l hb] = z\sum_{i=0}^{t-1}\sum_{j=0}^{m-1-l} c_{ij}q^{j+l} + z\sum_{i=0}^{t-1}\sum_{j=m-l}^{m-1} c_{ij}q^{j+l-m}$$

$$=\sum_{j=0}^{m-1-l}(s_{j+1}q-s_j)q^{j+l}+\sum_{j=m-l}^{m-1}(s_{j+1}q-s_j)q^{j+l-m}$$

$$=s_{m-l}(q^m-1).$$

Since $b=(q^m-1)/z$, we have the required result from (15.24).

From the above lemma, we have the following lemma:

LEMMA 15.10. *If h is a non-negative integer less than $(q^{mt}-1)/b$ which satisfies the condition* (15.2), *there exists a unique set of $m+1$ integers s_l ($l=0, 1, \ldots, m$) such that*

$$(s_0, s_1, \ldots, s_m)\in S_v(t, z, m, q) \quad \textit{and} \quad z\sum_{i=0}^{t-1}c_{ij}=s_{j+1}q-s_j \tag{15.25}$$

for $j=0, 1, \ldots, m-1$ where $hb=\sum_{i=0}^{t-1}\sum_{j=0}^{m-1}c_{ij}q^{im+j}$.

Conversely, the following lemma holds:

LEMMA 15.11. *Let $(s_0, s_1, \ldots, s_m)$ be any set in S_v (t, z, m, q) and let $\{c_{ij}; i=0, 1, \ldots, t-1, j=0, 1, \ldots, m-1\}$ be any set of non-negative integers less than q such that*

$$\sum_{i=0}^{t-1}c_{ij}=(s_{j+1}q-s_j)/z \tag{15.26}$$

for each $j=0, 1, \ldots, m-1$. Then $\sum_{i=0}^{t-1}\sum_{j=0}^{m-1}c_{ij}q^{im+j}$ is a multiple of b, that is, there exists an integer h, $0\leqq h<(q^{mt}-1)/b$, such that

$$\sum_{i=0}^{t-1}\sum_{j=0}^{m-1}c_{ij}q^{im+j}=bh \tag{15.27}$$

and the above integer h satisfies the condition (15.2).

PROOF. From (15.26) and $s_m=s_0$, it follows that

$$\sum_{i=0}^{t-1}\sum_{i=0}^{m-1}c_{ij}q^j=(s_mq^m-s_0)/z=s_0b. \tag{15.28}$$

Since $(q^{im}-1)$ is a multiple of b for $i=1, 2, \ldots, t-1$, it follows from (15.18) and (15.28) that $\sum_{i=0}^{t-1}\sum_{j=0}^{m-1}c_{ij}q^{im+j}$ is a multiple of b. There exists therfore an integer h satisfying the condition (15.27).

From (15.26) and (15.24), we have

$$D_{q^m}[q^lhb]=s_{m-l}(q^m-1)/z=s_{m-l}b. \tag{15.29}$$

Since s_l's are integers such that $0 \leqq s_l \leqq v$, h satisfies the condition (15.2). This completes the proof.

(Proof of Theorem 15.1) For a set of non-negative integers u_j ($j=0, 1, \ldots, m-1$), we denote by $N_t(u_0, u_1, \ldots, u_{m-1})$ the number of ordered sets ($c_{00}, c_{10}, \ldots, c_{t0}; \ldots; c_{0m-1}, c_{1m-1}, \ldots, c_{tm-1}$) of non-negative integers c_{ij} less than q which satisfy $\sum_{i=0}^{t} c_{ij} = u_j$ for $j=0, 1, \ldots, m-1$. Then it follows from the foregoing lemmas that the number of integers h, $0 \leqq h < (q^{mt}-1)/b$, satisfying the condition (15.2) is equal to

$$\sum_{(s_0, \ldots, s_m)} N_{t-1}((s_1 q - s_0)/z, \ldots, (s_m q - s_{m-1})/z) \tag{15.30}$$

where the summation is taken over all $(m+1)$-tuples $(s_0, s_1, \ldots, s_m)$ in $S_v(t, z, m, q)$. Since the number of information symbols of a cyclic code C is equal to the number of roots of the generator polynomial $g_D(x)$ of the dual code and

$$N_t(u_0, u_1, \ldots, u_{m-1}) = \prod_{j=0}^{m-1} \sum_{i=0}^{[u_j/q]} (-1)^i \binom{t+1}{i} \binom{t+u_j-iq}{t}, \tag{15.31}$$

we have the required result from (15.30).

(Proof of Theorem 15.4) Since the number of information symbols of a cyclic code C is equal to the number of roots of the generator polynomial $g_D(x)$ of the dual code, it follows from the definition that $I_{v_0(q^m-1)-1}(t, q^m-1, m, q)$ is equal to the number of integers h, $0 \leqq h < q^{mt}-1$, such that

$$\max_{0 \leqq l < m} D_{q^m}[q^l h] = j \qquad \text{with} \quad 0 \leqq j < v_0(q^m-1). \tag{15.32}$$

Let the q-adic representation of h be

$$h = \sum_{i=0}^{t-1} \sum_{j=0}^{m-1} c_{ij} q^{im+j} \tag{15.33}$$

and let h_0 be an integer such that $h_0 = \sum_{j=0}^{m-1} c_{tj} q^{tm+j}$ and that $h+h_0$ is a multiple of q^m-1, say $h+h_0 = h^*(q^m-1)$, where c_{tj}'s are non-negative integers less than q. Then it follows from Lemma 2.2 in [12] that

$$D_{q^m}[q^l h^*(q^m-1)] = D_{q^m}[q^l h] + D_{q^m}[q^l h_0] \tag{15.34}$$

for $l=0, 1, \ldots, m-1$. Since $0 \leqq D_{q^m}[q^l h_0] \leqq q^m-1$ for $l=0, 1, \ldots, m-1$, it follows from (15.34) that h is a non-negative integer less than $q^{mt}-1$ satisfying the condition (15.32) if and only if h^* is a non-negative integer less than $(q^{m(t+1)}-1)/(q^m-1)$ such that

$$\max_{0 \leqq l < m} D_{q^m}[q^l h^*(q^m-1)] = j(q^m-1) \qquad \text{with} \quad 0 \leqq j < v_0+1. \tag{15.35}$$

If h is not a multiple of q^m-1, the correspondence h and h^* is unique. But if h is a multiple of q^m-1, the correspondence h and h^* is not unique, that is, two integers h and $h+(q^m-1)q^{tm}$ are corresponding to the integer h. Since the number of integer h^* satisfying the condition (15.35) is equal to $I_{\nu_0}(t+1, 1, m, q)$ and the number of integers h, $0\leqq h<q^{mt}-1$, such that h is a multiple of q^m-1 and satisfies the condition (15.32) is equal to $I_{\nu_0}(t, 1, m, q)$, the number of integers h satisfying the condition (15.32) is equal to $I_{\nu_0}(t+1, 1, m, q)-I_{\nu_0}(t, 1, m, q)$. This completes the proof.

Since the p^m-ary μth order Projective Geometry code is the dual code of the $((p^{m(t+1)}-1)/(p^m-1), t+1, m, t-\mu, p)$-polynomial code, we have the

COROLLARY 15.12. *The number of information symbols of the μth order PG code with length $n=(p^{m(t+1)}-1)/(p^m-1)$ is equal to $n-I_{t-\mu}(t+1, 1, m; p)$, i.e., $n-R_\mu(t, p^m)$.*

Since the p^m-ary μth order Euclidean Geometry code is the dual code of the $(p^{mt}-1, t, m, (t-\mu)(p^m-1), p)$-polynomial code, we have the

COROLLARY 16.13. *The number of information symbols of the μth order EG code with length $n=p^{mt}-1$ is equal to $n-\{I_{t-\mu}(t+1, 1, m, p)-I_{t-1-\mu}(t, 1, m, p)\}$, i.e., $n-\{R_\mu(t, p^m)-R_\mu(t-1, p^m)\}$.*

Acknowledgement.

The author expresses his thanks to Prof. S. Yamamoto, Hiroshima University for his valuable advices and encouragements during this investigation.

References

[1] Alanen, J. D. and Knuth, D. E. (1964). Tables of finite fields. Sankhya **26** 305–328.
[2] Bose, R. C. (1939). On the construction of balanced incomplete block designs. Ann. Eugen. **9** 353–399.
[3] Bose, R. C. and Chaudhuri Ray, D. K. (1960). On a class of error correcting binary group codes. Information and Control **3** 68–79.
[4] Bose, R. C. and Chaudhuri Ray, D. K. (1960). Further results on error correcting binary group codes. Information and Control **3** 279–290.
[5] Bose, R. C. and Mesner, D. M. (1959). On linear associative algebras corresponding to association schemes of partially balanced designs. Ann. Math. Statist. **30** 21–38.
[6] Bose, R. C. and Nair, K. R. (1939). Partially balanced incomplete block designs. Sankhya **4** 337–372.
[7] Bose, R. C. and Shimamoto. T. (1952). Classification and analysis of partially balanced incomplete block designs with two associate classes. J. Amer. Statist. Assoc. **47** 151–184.
[8] Carmichael, R. D. (1937). *Introduction to the theory of groups of finite order*. Ginn and Company, Boston.

[9] Fisher, R. A. (1940). An examination of the different possible solutions of a problem in incomplete blocks. Ann. Eugen. **10** 52–75.

[10] Goethals, J. M. and Delsarte, P. (1968). On a class of majority logic decodable cyclic codes. IEEE Trans. on Information Theory **IT-14** 182–188.

[11] Graham, R. L. and MacWilliams, J. (1966). On the number of parity checks in difference set cyclic codes. Bell Sys. Tech. J. **45**, 1046–1070.

[12] 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.

[13] Hocquenghem, A. (1959). Codes correcteurs d'erreurs. Chiffres **2** 147–156.

[14] Hussain, Q. M. (1945). On the totality of the solutions for the symmetrical incomplete block designs: $\lambda=2$, $k=5$ or 6. Sankhya **7** 204–208.

[15] Hussain, Q. M. (1946–48). Structure of some incomplete block designs. Sankhya **8** 381–383.

[16] Kasami, T., Shu Lin and Peterson, W. W. (1966). Some results on cyclic codes which are invariant under the affine group. University of Hawaii, Department of electrical engineering, scientific report No. 9.

[17] Kasami, T., Shu Lin and Peterson, W. W. (1968). Polynomial codes. IEEE Trans. on Information Theory **IT–14** 807–814.

[18] Massey, J. C. (1963). *Threshold decoding*. The M.I.T. Press, Cambridge, Massachusetts.

[19] Muller, D. E. (1954). Application of Boolean algebra to switching circuit design and to error detection. IEEE Trans. on Electronic Computers **EC-3** 6–12.

[20] Nair, K. R. and Rao, C. R. (1942). A note on partially balanced incomplete block designs. Science and Culture **7** 568–569.

[21] Nandi, H. K. (1946). Enumeration of nonisomorphic solutions of balanced incomplete block designs. Sankhya **7** 305–312.

[22] Nandi, H. K. (1946). A further note on nonisomorphic solutions of incomplete block designs. Sankhya **7** 313–316.

[23] Ogasawara, M. (1965). *A necessary condition for the existance of regular and symmetrical PBIB designs of T_m type*. Inst. Statist. mimeo. series **418**, Chapel Hill, N.C.

[24] Ogawa, J. (1959). *The theory of the association algebra and the relationship algebra of a partially balanced incomplete block design*. Inst. Statist. mimeo. series **224**, Chapel Hill, N.C.

[25] Pasquale, V. DE (1899). Sui sistemi ternari di 13 elementi. Rend. R. Ist. Lombardo Sci. e Lett. (2) **32** 213–221.

[26] Peterson, W. W. (1961). *Error correcting codes*. John Wiley and Sons. New York.

[27] Rao, C. R. (1945). Finite geometries and certain derived results in theory of numbers. Proc. Nat. Inst. Sci. India **11** 136–149.

[28] Rao, C. R. (1946). Difference sets and combinatorial arrangements derivable from finite geometries. Proc. Nat. Inst. Sci. India **12** 123–135.

[29] Reed, I. S. (1954). A class of multiple error correcting codes and the decoding scheme. IEEE Trans. on Information Theory **IT-4** 38–49.

[30] Rudolph, L. D. (1967). A class of majority logic decodable codes. IEEE Trans. on Information Theory **IT-13** 305–307.

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

[32] Smith, K. J. C. (1969). On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry. J. Combinatorial Theory **7** 122–129.

[33] Stanton, R. G. and Mullin, R. C. (1969). Uniqueness theorems in balanced incomplete block designs. J. Combinatorial Theory **7** 37–48.

[34] Weldon, E. J. (1967–69). *Euclidean geometry cyclic codes.* Combinatorial and its applications 377–387.

[35] Yamamoto, S., Fujii, Y. and Hamada, N. (1965). Composition of some series of association algebras. J. Sci. Hiroshima Univ. Ser. A–I **29** 181–215.

[36] 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.

[37] Yates, F. (1936). Incomplete randomised blocks. Ann. Eugen. **7** 121–140.

Department of Mathematics,
Faculty of Science,
*Ehime University**

*) The present address of the author is as follows: Mathematical institute, Faculty of Education, Hiroshima University, Shinonome, Hiroshima, Japan.