J. SCI. HIROSHIMA UNIV. SER. A-I
32 (1968) 381-396

The Rank of the Incidence Matrix of Points and d-Flats in Finite Geometries

Noboru HAMADA

(Received September 26, 1968)

1. Introduction and Summary

The concept of majority decoding and, more generally, threshold decoding was introduced by Massey [3]. In order to obtain majority decodable codes such as (i) a d-th order Projective Geometry code (whose parity check matrix is the incidence matrix of points and d-flats in $\mathrm{PG}(t, p^n)$) and (ii) a d-th order Affine Geometry code (whose parity check matrix is the incidence matrix of points other than the origin and d-flats not passing through the origin in $\mathrm{EG}(t, p^n)$), it is necessary to investigate the rank of the incidence matrix of points and d-flats in $\mathrm{PG}(t, p^n)$ and in $\mathrm{EG}(t, p^n)$ over $\mathrm{GF}(p^n)$. An exact formula for the rank of the incidence matrix of points and hyperplanes ($(t-1)$-flats) has been obtained by Graham and MacWilliams [2] for the case $t=2$ and has been independently obtained by Smith [5] and by Goethals and Delsarte [1] for general t. An exact formula for the rank of the incidence matrix of points and d-flats in a special case $n=1$ has been obtained by Smith [5]. For general n, although an upper bound for the rank has been obtained by Smith, an explicit formula for the rank has not yet been obtained.*)

The purpose of this paper is to derive an explicit formula for the rank of the incidence matrix of points and d-flats in $\mathrm{PG}(t, p^n)$ and in $\mathrm{EG}(t, p^n)$ for the general case, by extending the methods used by Smith.

The main results are as follows.

(i) In the case of $\mathrm{PG}(t, p^n)$, we have the

THEOREM 1. *Over* $\mathrm{GF}(p^n)$, *the rank of the incidence matrix of points and d-flats in* $\mathrm{PG}(t, p^n)$ *is equal to*

$$R_d(t, p^n) = \sum_{s_0} \cdots \sum_{s_{n-1}} \prod_{j=0}^{n-1} \sum_{i=0}^{L(s_{j+1}, s_j)} (-1)^i \binom{t+1}{i} \binom{t+s_{j+1}p-s_j-ip}{t} \tag{1.1}$$

where $s_n=s_0$ *and summations are taken over all integers* s_j $(j=0, 1, \cdots, n-1)$ *such that*

$$d+1 \leqq s_j \leqq t+1 \quad and \quad 0 \leqq s_{j+1}p-s_j \leqq (t+1)(p-1) \tag{1.2}$$

*) This problem was suggested by Professor R. C. Bose during his visit to Hiroshima, May 1968.

and $L(s_{j+1}, s_j)$ *is the greatest integer not exceeding* $(s_{j+1}p - s_j)/p$, *i.e.*,

$$L(s_{j+1}, s_j) = \left[\frac{s_{j+1}p - s_j}{p}\right]. \tag{1.3}$$

(ii) In the case of $\mathrm{EG}(t, p^n)$, we have the

THEOREM 2. *Over* $\mathrm{GF}(p^n)$, *the rank of the incidence matrix of* $(p^n)^t - 1$ *points other than the origin and d-flats not passing through the origin in* $\mathrm{EG}(t, p^n)$ *is equal to* $R_d(t, p^n) - R_d(t-1, p^n) - 1$.

The process of deriving our explicit formulas and our results given in [6] may be useful to obtain majority decodable codes such as d-th order Projective Geometry codes and d-th order Affine Geometry codes. In section 2 and section 3, we shall prove Theorem 1 and Theorem 2, respectively.

2. Rank of the incidence matrix of points and d-flats in $\mathrm{PG}(t, p^n)$.

In this section, we investigate the rank of the incidence matrix of points and d-flats in $\mathrm{PG}(t, p^n)$ and prove Theorem 1.

With the help of the Galois field $\mathrm{GF}(q)$, where q is an integer of the form p^n (p being a prime), we can define a finite projective geometry $\mathrm{PG}(t, q)$ of t dimensions as a set of points satisfying the following conditions (a), (b) and (c):

(a) A point in $\mathrm{PG}(t, q)$ is represented by (ν) where ν is a non-zero element of $\mathrm{GF}(q^{t+1})$.

(b) Two points (ν) and (μ) represent the same point when and only when there exists a non-zero element σ of $\mathrm{GF}(q)$ such that $\mu = \sigma\nu$.

(c) A d-flat, $0 \leqq d \leqq t$, in $\mathrm{PG}(t, q)$ is defined as a set of points

$$\{(a_0\nu_0 + a_1\nu_1 + \cdots + a_d\nu_d)\} \tag{2.1}$$

where a's run independently over the elements of $\mathrm{GF}(q)$ and are not all simultaneously zero and $(\nu_0), (\nu_1), \cdots, (\nu_d)$ are linearly independent over the coefficient field $\mathrm{GF}(q)$, in other words, they do not lie on a $(d-1)$-flat.

It is well known that the number, v, of points in $\mathrm{PG}(t, q)$ is equal to

$$v = (q^{t+1} - 1)/(q-1) \tag{2.2}$$

and the number, b, of d-flats in $\mathrm{PG}(t, q)$ is equal to

$$b = \phi(t, d, q) = \frac{(q^{t+1}-1)(q^t-1)\cdots(q^{t-d+1}-1)}{(q^{d+1}-1)(q^d-1)\cdots(q-1)}. \tag{2.3}$$

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

$$N=\|n_{ij}\|; \quad i=1, 2, \cdots, b \quad \text{and} \quad j=1, 2, \cdots, v \tag{2.4}$$

where

$$n_{ij}=\begin{cases} 1, & \text{if the } j\text{-th point is incident with the } i\text{-th } d\text{-flat,} \\ 0, & \text{otherwise.} \end{cases}$$

In order to obtain an explicit formula for the rank of the incidence matrix N over GF(q), we start with the following proposition summarizing the essential results due to Smith [5].

Proposition 1 (Smith). *Over* GF(q), *the rank of the incidence matrix N of v points and b d-flats in* PG(t, q) *is equal to the number of integers m such that* (i) $1 \leqq m \leqq v$ *and* (ii) *there exists a set of $d+1$ positive integers m_k $(k=0, 1, \cdots, d)$ which satisfies*

$$m=\sum_{k=0}^{d} m_k \quad \textit{and} \quad D_p[m(q-1)]=\sum_{k=0}^{d} D_p[m_k(q-1)] \tag{2.5}$$

where $D_p[M]$ is defined for a non-negative integer M having the p-adic representation

$$M=c_0+c_1p+\cdots+c_up^u \qquad (0 \leqq c_i<p, \quad \textit{for all} \quad i=0, 1, \cdots, u) \tag{2.6}$$

by

$$D_p[M]=c_0+c_1+\cdots+c_u. \tag{2.7}$$

The following two theorems play an important role in proving Theorem 1.

Theorem 2.1. *Let m be a positive integer such that $1 \leqq m \leqq v$ and let the p-adic representation of $m(q-1)$ be*

$$m(q-1)=\sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij}p^{in+j} \tag{2.8}$$

where c_{ij}'s are non-negative integers less than p.

If there exists a set of $d+1$ positive integers m_k $(k=0, 1, \cdots, d)$ which satisfies

$$m=\sum_{k=0}^{d} m_k \quad \textit{and} \quad D_p[m(q-1)]=\sum_{k=0}^{d} D_p[m_k(q-1)], \tag{2.9}$$

then there exists a unique set of $n+1$ positive integers s_l $(l=0, 1, \cdots, n)$ such that

$$s_n=s_0, \; d+1 \leqq s_j \leqq t+1 \quad \textit{and} \quad \sum_{i=0}^{t} c_{ij}=s_{j+1}p-s_j \tag{2.10}$$

for each $j=0, 1, \cdots, n-1$.

Note that $0 \leqq s_{j+1}p - s_j \leqq (t+1)(p-1)$ must hold for each $j=0, 1, \cdots, n-1$, since $0 \leqq c_{ij} \leqq p-1$ for all i and j.

THEOREM 2.2. *Let* s_l $(l=0, 1, \cdots, n)$ *be a set of* $n+1$ *positive integers such that*

$$s_n = s_0, \quad d+1 \leqq s_j \leqq t+1 \quad \text{and} \quad 0 \leqq s_{j+1}p - s_j \leqq (t+1)(p-1) \tag{2.11}$$

for each $j=0, 1, \cdots, n-1$. *Let* c_{ij} $(i=0, 1, \cdots, t,\ j=0, 1, \cdots, n-1)$ *be a set of non-negative integers less than* p *satisfying*

$$\sum_{i=0}^{t} c_{ij} = s_{j+1}p - s_j \tag{2.12}$$

for each $j=0, 1, \cdots, n-1$. *Then,*

(i) $\sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} p^{in+j}$ *is a multiple of* $p^n - 1$, *that is, there exists an integer* m, $1 \leqq m \leqq v$, *such that*

$$\sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} p^{in+j} = m(p^n - 1). \tag{2.13}$$

(ii) *There exists a set of* $d+1$ *positive integers* m_k $(k=0, 1, \cdots, d)$ *which satisfies* (2.9) *for the integer* m.

At first, we prove the following two lemmas.

LEMMA 2.1. *Let* m *be a positive integer such that* $1 \leqq m \leqq v$ *and let the* p*-adic representation of* $m(q-1)$ *be*

$$m(q-1) = \sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} p^{in+j}, \tag{2.13$'$}$$

then there exists a unique set of $n+1$ *positive integers* s_l $(l=0, 1, \cdots, n)$ *such that*

$$s_n = s_0, \quad 1 \leqq s_j \leqq t+1 \quad \text{and} \quad \sum_{i=0}^{t} c_{ij} = s_{j+1}p - s_j \tag{2.14}$$

for each $j=0, 1, \cdots, n-1$.

PROOF. Since

$$\sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} p^j = \sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} p^{in+j} - \sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij}(p^{in}-1)p^j \tag{2.15}$$

and $(p^{in}-1)$ is a multiple of $p^n - 1$, $\sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} p^j$ is a multiple of $p^n - 1$ by assumption (2.13′), that is, there exists a positive integer r, $1 \leqq r \leqq t+1$, such that

$$\sum_{i=0}^{t}\sum_{j=0}^{n-1} c_{ij}p^j = r(p^n-1). \tag{2.16}$$

The equation (2.16) can be expressed as

$$r+\sum_{i=0}^{t}\sum_{j=0}^{j_0-1} c_{ij}p^j = rp^n-\sum_{i=0}^{t}\sum_{j=j_0}^{n-1} c_{ij}p^j \tag{2.17}$$

for any integer j_0 $(1\leqq j_0\leqq n-1)$. Since the right hand side of equation (2.17) is a multiple of p^{j_0}, its left hand side must be a multiple of p^{j_0}, that is, there exist $n-1$ positive integers s_{j_0}, $1\leqq s_{j_0}\leqq t+1$, $(j_0=1, 2, \cdots, n-1)$ such that

$$r+\sum_{i=0}^{t}\sum_{j=0}^{j_0-1} c_{ij}p^j = s_{j_0}p^{j_0} \tag{2.18}$$

for each $j_0=1, 2, \cdots, n-1$. Solving $n-1$ equations (2.18), we obtain

$$\sum_{i=0}^{t} c_{ij} = s_{j+1}p-s_j \tag{2.19}$$

for each $j=0, 1, \cdots, n-1$ where $s_n=s_0$ and $s_0=r$.

The uniqueness of the set of integers s_l $(l=0, 1, \cdots, n)$ can be proved as follows.

Let s_l^* $(l=0, 1, \cdots, n)$ be another set of $n+1$ positive integers such that

$$s_n^* = s_0^* \quad \textit{and} \quad \sum_{i=0}^{t} c_{ij} = s_{j+1}^*p-s_j^* \tag{2.20}$$

for $j=0, 1, \cdots, n-1$. Then, from (2.19) and (2.20), we have $s_{j+1}p-s_j=s_{j+1}^*p-s_j^*$ $(j=0, 1, \cdots, n-1)$ and $\sum_{j=0}^{n-1}\sum_{i=0}^{t} c_{ij}p^j=s_0(p^n-1)=s_0^*(p^n-1)$. This implies that $s_l^*=s_l$ for all $l=0, 1, \cdots, n$. This completes the proof.

LEMMA 2.2. *Let M and M_k $(k=0, 1, \cdots, d)$ be positive integers and let the p-adic representations of M and M_k be*

$$M=\sum_{l=0}^{u} c_lp^l \quad \textit{and} \quad M_k=\sum_{l=0}^{u} c_l^{(k)}p^l. \tag{2.21}$$

Then, $M=\sum_{k=0}^{d} M_k$ and $D_p[M]=\sum_{k=0}^{d} D_p[M_k]$ if and only if $c_l=\sum_{k=0}^{d} c_l^{(k)}$ for each $l=0, 1, \cdots, u$.

PROOF. If $M=\sum_{k=0}^{d} M_k$ and $D_p[M]=\sum_{k=0}^{d} D_p[M_k]$, then,

$$\sum_{l=0}^{u} c_lp^l = \sum_{k=0}^{d}\sum_{l=0}^{u} c_l^{(k)}p^l \tag{2.22}$$

and

$$\sum_{l=0}^{u} c_l = \sum_{k=0}^{d}\sum_{l=0}^{u} c_l^{(k)}. \tag{2.22'}$$

Since c_l's are non-negative integers less than p, it follows from (2.22) that c_l $(l=0, 1, \cdots, u)$ must be expressed as

$$c_l = \sum_{k=0}^{d} c_l^{(k)} + \alpha_{l-1} - \alpha_l p \tag{2.23}$$

for some non-negative integers α_l $(l=-1, 0, \cdots, u)$ where $\alpha_{-1}=\alpha_u=0$. Taking summation of (2.23) over l, we have

$$\sum_{l=0}^{u} c_l = \sum_{l=0}^{u} \sum_{k=0}^{d} c_l^{(k)} - (p-1)\sum_{l=0}^{u-1} \alpha_l. \tag{2.24}$$

The equations (2.22′) and (2.24) show that $(p-1)\sum_{l=0}^{u-1}\alpha_l=0$. This implies that all integers α_l must be zero since they are non-negative integers and $p \geqq 2$. Thus we have $c_l = \sum_{k=0}^{d} c_l^{(k)}$ for each $l=0, 1, \cdots, u$.

The converse is obvious.

(Proof of Theorem 2.1) Let the p-adic representation of $m_k(q-1)$ be

$$m_k(q-1) = \sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij}^{(k)} p^{in+j} \qquad (k=0, 1, \cdots, d), \tag{2.25}$$

then from lemma 2.2, we have

$$c_{ij} = \sum_{k=0}^{d} c_{ij}^{(k)} \tag{2.26}$$

for all $i=0, 1, \cdots, t$ and $j=0, 1, \cdots, n-1$. Since m_k is a positive integer such that $1 \leqq m_k \leqq v$, it follows from lemma 2.1 that for each $k=0, 1, \cdots, d$, there exists a unique set of $n+1$ positive integers $s_l^{(k)}$ $(l=0, 1, \cdots, n)$ such that

$$s_n^{(k)} = s_0^{(k)},\ 1 \leqq s_j^{(k)} \leqq t+1 \quad \text{and} \quad \sum_{i=0}^{t} c_{ij}^{(k)} = s_{j+1}^{(k)} p - s_j^{(k)} \tag{2.27}$$

for each $j=0, 1, \cdots, n-1$. From (2.26) and (2.27), we have

$$\sum_{i=0}^{t} c_{ij} = \Big(\sum_{k=0}^{d} s_{j+1}^{(k)}\Big)p - \Big(\sum_{k=0}^{d} s_j^{(k)}\Big). \tag{2.28}$$

Let $s_l = \sum_{k=0}^{d} s_l^{(k)}$ for each $l=0, 1, \cdots, n$, then it holds that

$$s_n = s_0 \quad \text{and} \quad \sum_{i=0}^{t} c_{ij} = s_{j+1}p - s_j \tag{2.29}$$

for $j=0, 1, \cdots, n-1$. Since the set of integers s_l $(l=0, 1, \cdots, n)$ for m is unique and all $s_l^{(k)}$'s are positive, it follows that $d+1 \leqq s_j \leqq t+1$ for each $j=0, 1, \cdots, n-1$. This completes the proof.

For the proof of Theorem 2.2, we shall prove the following three lemmas.

LEMMA 2.3. *For any set of $n+1$ positive integers s_l $(l=0, 1, \cdots, n)$ which satisfies the conditions:*

$$s_n = s_0,\quad 1 \leqq s_j \leqq t+1 \quad \text{and} \quad 0 \leqq s_{j+1}p - s_j \leqq (t+1)(p-1) \tag{2.30}$$

for all $j=0, 1, \cdots, n-1$, there exists a set of non-negative integers c_{ij}, $0 \leqq c_{ij} \leqq p-1$, $(i=0, 1, \cdots, t,\ j=0, 1, \cdots, n-1)$ satisfying

$$\sum_{i=0}^{t} c_{ij} = s_{j+1}p - s_j \tag{2.31}$$

for $j=0, 1, \cdots, n-1$, and $\sum_{i=0}^{t}\sum_{j=0}^{n-1} c_{ij}p^{in+j}$ is a multiple of p^n-1, i.e.,

$$\sum_{i=0}^{t}\sum_{j=0}^{n-1} c_{ij}p^{in+j} = m(p^n-1) \quad \text{and} \quad 1 \leqq m \leqq v. \tag{2.32}$$

PROOF. The existence of non-negative integers c_{ij} less than p is obvious since $0 \leqq s_{j+1}p - s_j \leqq (t+1)(p-1)$.

From (2.31), we have

$$\sum_{j=0}^{n-1}\sum_{i=0}^{t} c_{ij}p^j = \sum_{j=0}^{n-1}(s_{j+1}p - s_j)p^j = s_n p^n - s_0 = s_0(p^n-1). \tag{2.33}$$

Thus, we get the required result from (2.15) and (2.33).

LEMMA 2.4. *Let s_l $(l=0, 1, \cdots, n)$ be $n+1$ positive integers which satisfies the conditions:*

$$s_n = s_0,\quad d+1 \leqq s_j \leqq t+1 \quad \text{and} \quad 0 \leqq s_{j+1}p - s_j \leqq (t+1)(p-1) \tag{2.34}$$

for all $j=0, 1, \cdots, n-1$, then there exist $d+1$ sets of $n+1$ positive integers $s_l^{(k)}$ $(k=0, 1, \cdots, d,\ l=0, 1, \cdots, n)$ such that

$$\sum_{k=0}^{d} s_l^{(k)} = s_l \qquad (l=0, 1, \cdots, n) \tag{2.35}$$

$$s_n^{(k)} = s_0^{(k)},\quad 1 \leqq s_j^{(k)} \leqq t+1 \quad \text{and} \quad 0 \leqq s_{j+1}^{(k)}p - s_j^{(k)} \leqq (t+1)(p-1) \tag{2.36}$$

for all $j=0, 1, \cdots, n-1$ and $k=0, 1, \cdots, d$.

PROOF. The case $d=0$ is trivial. We, therefore, assume that $1 \leqq d \leqq t$ and give a step by step method of constructing a series of positive integers $s_{j_0+1}^{(k)}, s_{j_0}^{(k)}, \cdots, s_0^{(k)} = s_n^{(k)}, s_{n-1}^{(k)}, \cdots, s_{j_0+2}^{(k)}$ $(k=0, 1, \cdots, d)$ having required properties by starting with the decomposition of s_{j_0+1} into $d+1$ positive integers $s_{j_0+1}^{(k)}$, where s_{j_0+1} is one of the least integers among $s_1, s_2, \cdots, s_n$.

(i) Construction of $s_{j_0+1}^{(k)}$ $(k=0, 1, \cdots, d)$

Since $s_{j_0+1} \geqq d+1$, we can define $s_{j_0+1}^{(k)}$ $(k=0, 1, \cdots, d)$ satisfying the following conditions:

$$1 \leqq s_{j_0+1}^{(k)} \leqq t+1 \quad \text{and} \quad \sum_{k=0}^{d} s_{j_0+1}^{(k)} = s_{j_0+1}. \tag{2.37}$$

(ii) Construction of $s_{j_0}^{(k)}$ by using $s_{j_0+1}^{(k)}$ $(k=0, 1, \cdots, d)$

Since $s_{j_0} \geqq s_{j_0+1}$, there exist a positive integer Q_{j_0} and a non-negative integer R_{j_0} less than s_{j_0+1} such that

$$s_{j_0} = Q_{j_0} s_{j_0+1} + R_{j_0} \tag{2.38}$$

Thus if we define $s_{j_0}^{(k)}$ by the sum of $s_{j_0+1}^{(k)} Q_{j_0}$ and a non-negative integer $\alpha_k s_{j_0+1}^{(k)}$ not greater than $s_{j_0+1}^{(k)}$, i.e.,

$$s_{j_0}^{(k)} = s_{j_0+1}^{(k)} Q_{j_0} + \alpha_k s_{j_0+1}^{(k)} \qquad (0 \leqq \alpha_k \leqq 1) \tag{2.39}$$

such that $\sum_{k=0}^{d} \alpha_k s_{j_0+1}^{(k)} = R_{j_0}$, then we have

$$\sum_{k=0}^{d} s_{j_0}^{(k)} = s_{j_0} \quad \text{and} \quad 1 \leqq s_{j_0+1}^{(k)} \leqq s_{j_0}^{(k)} \leqq t+1. \tag{2.40}$$

Since $s_{j_0+1} p - s_{j_0} \geqq 0$, we have $Q_{j_0} \leqq p$. Whenever s_{j_0} is not a multiple of s_{j_0+1}, the equality does not hold, i.e., $Q_{j_0} < p$. When s_{j_0} is a multiple of s_{j_0+1}, the equality may holds but we have $\alpha_0 = \alpha_1 = \cdots = \alpha_d = 0$. Anyway, we have

$$s_{j_0+1}^{(k)} p - s_{j_0}^{(k)} = s_{j_0+1}^{(k)} (p - Q_{j_0} - \alpha_k) \geqq 0. \tag{2.41}$$

Combining the results with $s_{j_0+1} p - s_{j_0} \leqq (t+1)(p-1)$, $\sum_{k=0}^{d} s_{j_0+1}^{(k)} = s_{j_0+1}$ and (2.40), we have

$$s_{j_0+1}^{(k)} p - s_{j_0}^{(k)} \leqq (t+1)(p-1). \tag{2.41$'$}$$

(iii) Construction of $s_l^{(k)}$ by using $s_{l+1}^{(k)}$ (general case)

In general, two cases can occur, i.e., (a) $s_l < s_{l+1}$ and (b) $s_l \geqq s_{l+1}$.

(a) The case $s_l < s_{l+1}$

In this case, we can easily decompose s_l into $d+1$ positive integers $s_l^{(k)}$ $(k=0, 1, \cdots, d)$ such that

$$\sum_{k=0}^{d} s_l^{(k)} = s_l, \quad 1 \leqq s_{j_0+1}^{(k)} \leqq s_l^{(k)} \leqq s_{l+1}^{(k)} \leqq t+1 \tag{2.42}$$

and we can easily show that

$$0 \leqq s_{l+1}^{(k)} p - s_l^{(k)} \leqq (t+1)(p-1). \tag{2.43}$$

(b) The case $s_l \geqq s_{l+1}$

In this case, we can apply the same method described in (ii), for the construction of $s_l^{(k)}$ having required properties by using $s_{l+1}^{(k)}$.

Using these methods described in (i), (ii) and (iii), we can construct integers $s_l^{(k)}$ step by step until $s_{j_0+2}^{(k)}$ $(k=0, 1, \cdots, d)$ have been constructed. Now, we have to verify that the inequalities

$$0 \leqq s_{j_0+2}^{(k)} p - s_{j_0+1}^{(k)} \leqq (t+1)(p-1) \tag{2.44}$$

hold for all k. Since the construction process shows that $s_l^{(k)} \geqq s_{j_0+1}^{(k)}$ holds for each $l=0, 1, \cdots, n$ and $k=0, 1, \cdots, d$, we can see that the inequalities (2.44) hold. This completes the proof.

The following lemma seems to be not so trivial. But we can construct a set of non-negative integers satisfying the required conditions by an elementary method.

LEMMA 2.5. *Let* u_α $(\alpha=0, 1, \cdots, t)$ *and* w_β $(\beta=0, 1, \cdots, d)$ *be non-negative integers such that* $\sum_{\alpha=0}^{t} u_\alpha = \sum_{\beta=0}^{d} w_\beta$,

$$0 \leqq u_\alpha \leqq p-1 \quad \text{and} \quad 0 \leqq w_\beta \leqq (t+1)(p-1), \tag{2.45}$$

then there exists a set $\{x_{\alpha\beta}: \alpha=0, 1, \cdots, t, \beta=0, 1, \cdots, d\}$ *of non-negative integers less than* p *which satisfies the conditions*:

$$\sum_{\beta=0}^{d} x_{\alpha\beta} = u_\alpha \qquad (\text{for } \alpha=0, 1, \cdots, t) \tag{2.46}$$

and

$$\sum_{\alpha=0}^{t} x_{\alpha\beta} = w_\beta \qquad (\text{for } \beta=0, 1, \cdots, d). \tag{2.46$'$}$$

Using the above three lemmas, we now prove Theorem 2.2.

(Proof of Theorem 2.2) Lemma 2.3 shows that (i) holds.

Lemma 2.4 shows that each s_l $(0 \leqq l \leqq n)$ can be decomposed into $d+1$ positive integers $s_l^{(k)}$ $(k=0, 1, \cdots, d)$ such that $\sum_{k=0}^{d} s_l^{(k)} = s_l$ and that

$$s_n^{(k)} = s_0^{(k)},\ 1 \leqq s_j^{(k)} \leqq t+1 \quad \text{and} \quad 0 \leqq s_{j+1}^{(k)} p - s_j^{(k)} \leqq (t+1)(p-1) \tag{2.47}$$

for all $j=0, 1, \cdots, n-1$ and $k=0, 1, \cdots, d$.

Since for each j $(0 \leqq j \leqq n-1)$, $c_{\alpha j}$ $(\alpha=0, 1, \cdots, t)$ and $(s_{j+1}^{(\beta)} p - s_j^{(\beta)})$ $(\beta=0, 1, \cdots, d)$ satisfy the conditions of Lemma 2.5, there exists a set $\{c_{\alpha j}^{(\beta)}: \alpha=0, 1, \cdots, t, \beta=0, 1, \cdots, d\}$ of non-negative integers less than p which satisfy the conditions:

$$\sum_{\alpha=0}^{t} c_{\alpha j}^{(\beta)} = s_{j+1}^{(\beta)} p - s_j^{(\beta)} \qquad (\text{for } \beta=0, 1, \cdots, d) \tag{2.48}$$

and

$$\sum_{\beta=0}^{d} c_{\alpha j}^{(\beta)} = c_{\alpha j} \qquad (\textit{for } \alpha=0,1,\cdots,t). \tag{2.48'}$$

For each k $(0 \leqq k \leqq d)$, since $c_{ij}^{(k)}$ $(i=0,1,\cdots,t,\ j=0,1,\cdots,n-1)$ satisfy the conditions of lemma 2.3, there exists a positive integer m_k, $1 \leqq m_k \leqq v$, such that

$$\sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij}^{(k)} p^{in+j} = m_k(p^n - 1). \tag{2.49}$$

From (2.49), (2.48′) and the equation

$$\sum_{i=0}^{t} \sum_{j=0}^{n-1} c_{ij} p^{in+j} = m(p^n - 1), \tag{2.50}$$

we have

$$m = \sum_{k=0}^{d} m_k \quad \text{and} \quad D_p[m(p^n-1)] = \sum_{k=0}^{d} D_p[m_k(p^n-1)]. \tag{2.51}$$

This completes the proof.

Theorem 2.1 shows that for each m satisfying the requirement (2.9), there exists a unique set of s_l $(l=0,1,\cdots,n)$ satisfying (2.10). On the other hand, Theorem 2.2 shows that for each set of s_l satisfying (2.10), there exist a number of integers m satisfying the requirement (2.9).

In order to enumerate the number of m for each set of s_l, we introduce the following notation. For a set of non-negative integers u_j $(j=0,1,\cdots,n-1)$, we denote by $N_t(u_0, u_1, \cdots, u_{n-1})$ the number of ordered sets or vectors $\underline{c}(t, n-1) = (c_{00}, c_{10}, \cdots, c_{t0}; \cdots; c_{0n-1}, c_{1n-1}, \cdots, c_{tn-1})$ of non-negative integers less than p which satisfy

$$\sum_{i=0}^{t} c_{ij} = u_j \tag{2.52}$$

for all $j=0,1,\cdots,n-1$. It can easily be seen that, for $0 \leqq u_j \leqq (t+1)(p-1)$, there exists at least one set $\underline{c}(t, n-1)$ and, otherwise, there does not exist such an ordered set.

Using the notation, we have the following theorem.

THEOREM 2.3. *The number of integers m such that* (i) $1 \leqq m \leqq v$ *and* (ii) m *can be decomposed into $d+1$ positive integers m_k $(k=0,1,\cdots,d)$ satisfying the following conditions*:

$$m = \sum_{k=0}^{d} m_k \quad \textit{and} \quad D_p[m(q-1)] = \sum_{k=0}^{d} D_p[m_k(q-1)] \tag{2.53}$$

is equal to

$$\sum_{s_0=d+1}^{t+1} \cdots \sum_{s_{n-1}=d+1}^{t+1} N_t(s_1 p - s_0, \cdots, s_n p - s_{n-1}) \tag{2.54}$$

where $s_n = s_0$.

The following well known lemma is useful in the determination of $N_t(u_0, \cdots, u_{n-1})$.

LEMMA 2.6. *Let u be a non-negative integer such that $0 \leqq u \leqq (t+1)(p-1)$. Then the number, $B_u(t, p)$, of ordered sets $(x_0, x_1, \cdots, x_t)$ of $t+1$ non-negative integers x_i $(i=0, 1, \cdots, t)$ such that $0 \leqq x_i \leqq p-1$ and $\sum_{i=0}^{t} x_i = u$, is equal to*

$$B_u(t, p) = \sum_{i=0}^{L(u)} (-1)^i \binom{t+1}{i} \binom{t+u-ip}{t} \tag{2.55}$$

where $L(u)$ is the greatest integer not exceeding u/p, i.e. $L(u) = \left[\frac{u}{p}\right]$.

(Proof of Theorem 1) We can easily see that

$$N_t(u_0, u_1, \cdots, u_{n-1}) = \prod_{j=0}^{n-1} B_{u_j}(t, p). \tag{2.56}$$

Applying (2.56) and lemma 2.6 to Theorem 2.3, we get Theorem 1.

When $d \leqq \left[\frac{t}{2}\right]$, the following identity may be useful, i.e.,

$$R_d(t, p^n) = v - R_d^*(t, p^n) \tag{2.57}$$

where

$$R_d^*(t, p^n) = \sum_{s_0^*} \cdots \sum_{s_{n-1}^*} \prod_{j=0}^{n-1} \sum_{i=0}^{L(s_{j+1}^*, s_j^*)} (-1)^i \binom{t+1}{i} \binom{t+s_{j+1}^* p - s_j^* - ip}{t}, \tag{2.58}$$

$s_n^* = s_0^*$ and summations are taken over all integers s_j^* $(j=0, 1, \cdots, n-1)$ such that

$$1 \leqq s_j^* \leqq d \quad \text{and} \quad 0 \leqq s_{j+1}^* p - s_j^* \leqq (t+1)(p-1). \tag{2.59}$$

COROLLARY 2.1. *In the special case $q=p$, i.e., $n=1$, the rank of the incidence matrix N of v points and b d-flats in* PG(t, p) *is equal to*

$$R_d(t, p) = \sum_{s=d+1}^{t+1} \sum_{i=0}^{L(s,s)} (-1)^i \binom{t+1}{i} \binom{t+s(p-1)-ip}{t} \tag{2.60}$$

$$= v - \sum_{s=1}^{d} \sum_{i=0}^{L(s,s)} (-1)^i \binom{t+1}{i} \binom{t+s(p-1)-ip}{t} \tag{2.60'}$$

where $L(s, s) = \left[\frac{s(p-1)}{p}\right]$.

This result has been obtained by Smith [5].

COROLLARY 2.2. *In the special case $d=t-1$, the rank of the incidence* *matrix N of v points and v hyperplanes ($(t-1)$-flats) in* PG(t, q) *is equal to*

$$R_{t-1}(t, p^n)=\binom{t+p-1}{t}^n+1. \tag{2.61}$$

In the case $t=2$, this result has been obtained by Graham and MacWilliams [2] and, for general t, was conjectured by Rudolph [4] to be true and has been independently obtained by Smith [5] and by Goethals and Delsarte [1].

3. Rank of the incidence matrix of points and d-flats in EG(t, p^n)

We consider the affine case.

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

(a) A point is represented by (ν) where ν is an element of GF(q^t) and each element represents a unique point.

(b) A d-flat is defined as a set of points

$$\{(a_0\nu_0+a_1\nu_1+\cdots+a_d\nu_d)\} \tag{3.1}$$

where (ν_0), (ν_1), $\cdots$, (ν_d) are linearly independent over the coefficient field GF(q) and a's run over the elements of GF(q) subject to the restriction $\sum_{i=0}^{d} a_i=1$.

Because of difficulties arising in constructing an analytical expression for the incidence relation between the origin and d-flats in EG(t, q), we shall analyze separately the incidence matrix of points and d-flats passing through the origin and the incidence matrix of points and d-flats not passing through the origin.

(I) The case of the incidence matrix of points and d-flats passing through the origin

We define the incidence matrix of q^t points and $b_0=\phi(t-1, d-1, q)$ d-flats passing through the origin to be the matrix

$$N_0=||n_{ij}|| \ ; \ i=1, 2, \cdots, b_0 \quad \text{and} \quad j=0, 1, 2, \cdots, q^t-1. \tag{3.2}$$

where

$$n_{ij}=\begin{cases} 1, & \text{if the } j\text{-th point is incident with the } i\text{-th } d\text{-flat}, \\ 0, & \text{otherwise} \end{cases}$$

and define the incidence matrix of $v^*=q^t-1$ points other than the origin and b_0 d-flats passing through the origin to be the matrix

$$N_0^*=||n_{ij}^*|| \ ; \ i=1, 2, \cdots, b_0 \quad \text{and} \quad j=1, 2, \cdots, q^t-1. \tag{3.3}$$

Since $n_{i0}=1$ and $\sum_{j=1}^{q^t-1} n_{ij}=q^d-1$ for all $i=1, 2, \cdots, b_0$, the rank of N_0 is equal to the rank of N_0^*. It is known [6] that the structure of the matrix N_0^* is the same as the incidence matrix N of points and $(d-1)$-flats in PG$(t-1, q)$ except for ($q-1$ times) duplications of each column of N_0^*. The rank of the matrix N_0^*, therefore, is equal to the rank of the incidence matrix N.

The following theorem is an immediate consequence of Theorem 1.

THEOREM 3.1. *Over* GF(q), *the rank of the incidence matrices* N_0 *and* N_0^* *of points and d-flats passing through the origin in* EG(t, q) *is equal to* $R_{d-1}(t-1, p^n)$ *where* $R_d(t, p^n)$ *is given by equation* (1.1).

(II) The case of the incidence matrix of points and d-flats not passing through the origin

We define the incidence matrix of $v^*=q^t-1$ points other than the origin and b_1 d-flats not passing through the origin in EG(t, q) to be the matrix N_1 where b_1 is the number of d-flats not passing through the origin, i.e.,

$$b_1=\phi(t, d, q)-\phi(t-1, d, q)-\phi(t-1, d-1, q). \tag{3.4}$$

By the similar methods used in PG(t, q), Smith [5] showed the following proposition.

PROPOSITION 2 (Smith). *Over* GF(q), *the rank,* $r_d(t, p^n)$, *of the incidence matrix* N_1 *is equal to the number of integers* m *such that* (i) $1\leqq m\leqq v^*-1$ *and* (ii) *there exists a set of one non-negative integer* m_0 *and* d *positive integers* $m_k(q-1)$ $(k=1, 2, \cdots, d)$ *which satisfies the following conditions*:

$$m=m_0+\sum_{k=1}^{d} m_k(q-1) \quad \textit{and} \quad D_p[m]=D_p[m_0]+\sum_{k=1}^{d} D_p[m_k(q-1)] \tag{3.5}$$

where $0\leqq m_0\leqq m$ *and* $0<m_k(q-1)<m$ *for any* $k=1, 2, \cdots, d$.

Since in the special case $m=v^*$ $(v^*=q^t-1)$, m satisfies the condition (3.5), the rank of the incidence matrix N_1 is equal to

$$r_d(t, p^n)=r_d^*(t, p^n)-1 \tag{3.6}$$

where $r_d^*(t, p^n)$ is the number of integers m such that (i)$'$ $1\leqq m\leqq v^*$ and (ii) there exists a set of one non-negative integer m_0 and d positive integers $m_k(q-1)$ $(k=1, 2, \cdots, d)$ satisfying the condition (3.5).

From Proposition 2, lemma 2.2, Theorem 2.1 and Theorem 2.2, we have the following theorem.

THEOREM 3.2. *A necessary and sufficient condition for an integer* m *such that* $1\leqq m\leqq v^*$ *to be decomposed into one non-negative integer* m_0 *and* d *positive integers* $m_k(q-1)$ $(k=1, 2, \cdots, d)$ *satisfying the condition* (3.5) *is that there exist* $n+1$ *positive integers* s_l $(l=0, 1, \cdots, n)$ *satisfying the following conditions*:

(i) $$s_n = s_0, \quad d \leqq s_j \leqq t, \quad 0 \leqq s_{j+1}p - s_j \leqq t(p-1) \tag{3.7}$$

and

(ii) $$\sum_{i=0}^{t-1} c_{ij} \geqq s_{j+1}p - s_j \tag{3.7$'$}$$

for all $j=0, 1, \cdots, n-1$ *where* c_{ij}*'s* $(0 \leqq c_{ij} < p)$ *are coefficients of* p^{in+j} *of the* p*-adic representation for* m, *i.e.*,

$$m = \sum_{i=0}^{t-1} \sum_{j=0}^{n-1} c_{ij} p^{in+j}. \tag{3.8}$$

We prove the following lemmas, which will be used in the proof of theorem 2.

LEMMA 3.1. *Let* u_j $(j=0, 1, \cdots, n-1)$ *be a set of non-negative integers such that* $0 \leqq u_j \leqq (t-1)(p-1)$. *Then the number of ordered sets or vectors* $\underline{c}(t-1, n-1) = (c_{00}, c_{10}, \cdots, c_{t-10}; \cdots; c_{0n-1}, c_{1n-1}, \cdots, c_{t-1n-1})$ *of* tn *non-negative integers* c_{ij} *less than* p *such that*

$$u_j \leqq \sum_{i=0}^{t-1} c_{ij} \leqq u_j + (p-1) \qquad (j=0, 1, \cdots, n-1) \tag{3.9}$$

and that

$$\sum_{i=0}^{t-1} c_{ij} < u_j + (p-1) \tag{3.9$'$}$$

for some j, *is equal to*

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

PROOF. For any set $\{c_{\alpha j} : \alpha=0, 1, \cdots, t-1\}$ of t non-negative integers $c_{\alpha j}$ less than p such that $u_j \leqq \sum_{\alpha=0}^{t-1} c_{\alpha j} \leqq u_j + (p-1)$, there exists a non-negative integer c_{tj} $(0 \leqq j \leqq n-1)$ less than p such that

$$\sum_{\alpha=0}^{t-1} c_{\alpha j} + c_{tj} = u_j + (p-1). \tag{3.10}$$

The number of ordered sets $\underline{c}(t-1, n-1)$ of tn non-negative integers c_{ij} less than p satisfying the conditions (3.9) is, therefore, equal to the number of ordered sets $\underline{c}(t, n-1)$ of $(t+1)n$ non-negative integers less than p satisfying the equations (3.10). Thus we have lemma 3.1.

LEMMA 3.2. *For any set* $\{c_{ij} : i=0, 1, \cdots, t-1, j=0, 1, \cdots, n-1\}$ *of non-negative integers less than* p *such that there exists a set of integers* s_l $(l=0, 1, \cdots, n)$ *satisfying the condition* (3.7) *and* (3.7$'$), *there exists a unique set of integers* s_l^* $(l=0, 1, \cdots, n)$ *satisfying the following condition*:

$$s_n^* = s_0^*, \quad d \leqq s_j^* \leqq t, \quad 0 \leqq s_{j+1}^* p - s_j^* \leqq t(p-1) \tag{3.11}$$

for $j=0, 1, \cdots, n-1$ *and that*

$$s_{j+1}p - s_j \leqq s_{j+1}^* p - s_j^* \leqq \sum_{i=0}^{t-1} c_{ij} \leqq (s_{j+1}^*+1)p - (s_j^*+1) \tag{3.11'}$$

for all $j=0, 1, \cdots, n-1$ *and*

$$\sum_{i=0}^{t-1} c_{ij} < (s_{j+1}^*+1)p - (s_j^*+1) \tag{3.11''}$$

for some j.

PROOF. From $s_n^* = s_0^*$ and inequalities (3.11′) and (3.11″), we have

$$s_n^* = s_0^* = \left[\frac{\sum_{j=0}^{n-1} \sum_{i=0}^{t-1} c_{ij} p^j}{p^n - 1} \right] \quad \text{and} \quad s_{k+1}^* = \left[\frac{\sum_{i=0}^{t-1} c_{ik} + s_k^*}{p} \right] \quad (k=0, 1, \cdots, n-2)$$

and we can show that these s_l^* $(l=0, 1, \cdots, n)$ satisfy the condition (3.11).

(Proof of Theorem 2). From Theorem 3.2, lemma 3.1 and lemma 3.2, we have

$$\begin{aligned} r_d^*(t, p^n) &= \sum_{s_0=d+1}^{t} \cdots \sum_{s_{n-1}=d+1}^{t} N_t(s_1 p - s_0, \cdots, s_n p - s_{n-1}) \\ &\quad - \sum_{s_0=d+1}^{t-1} \cdots \sum_{s_{n-1}=d+1}^{t-1} N_{t-1}(s_1 p - s_0, \cdots, s_n p - s_{n-1}) \\ &= \sum_{s_0=d+1}^{t+1} \cdots \sum_{s_{n-1}=d+1}^{t+1} N_t(s_1 p - s_0, \cdots, s_n p - s_{n-1}) \\ &\quad - \sum_{s_0=d+1}^{t} \cdots \sum_{s_{n-1}=d+1}^{t} N_{t-1}(s_1 p - s_0, \cdots, s_n p - s_{n-1}) \\ &= R_d(t, p^n) - R_d(t-1, p^n). \end{aligned} \tag{3.12}$$

Combining (3.12) with (3.6), we have Theorem 2.

COROLLARY 3.1. *In the special case* $d=t-1$, *the rank of the incidence matrix* N_1 *is equal to* $\binom{t+p-1}{t}^n - 1$.

This result has been independently obtained by Smith [5] and by Goethals and Delsarte [1].

Acknowledgement. The author expresses his thanks to Prof. S. Yamamoto, Hiroshima University for his valuable advices and helpful discussions.

References

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

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

[3] Massey, J. C. (1963). *Threshold decoding*. The M. I. T. Press, Cambridge, Massachusetts.

[4] Rudolph, L. D. (1967). A class of majority logic decodable codes. *IEEE Transactions on Information Theory* **IT-13** 305-307.

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

[6] 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.

Department of Mathematics,
Faculty of Science
Hiroshima University