ON THE RANK OF INCIDENCE MATRICES
IN FINITE GEOMETRIES

by

K. J. C. Smith

University of North Carolina

Institute of Statistics Mimeo Series No. 555

November 1967

Abstract

The incidence matrix N of points and d-flats in PG(t,q) is a (0,1)-matrix which may be considered a matrix with entries from the field GF(q), where q is a prime power, $q = p^n$. Let $r_d(t,q)$ denote thr rank of N over GF (q). In this paper, a formula for $r_{t-1}(t,q)$ and an upper bound for $r_d(t,q)$, $1 \leq d \leq t-1$, are given. In the case q = p, the bound on $r_d(t,p)$ is attained. Similar results are given for the rank of the incidence matrix of points and d-flats not passing through the origin in EG(t,q). Proofs of the results stated in this paper are omitted and are given in the author's Ph. D. dissertation.

This research was supported by the National Science Foundation Grant No. GP-5790 and by the U. S. Army Research Office - Durham Grant No. DA-ARD-D-31-124-G910

DEPARTMENT OF STATISTICS

UNIVERSITY OF NORTH CAROLINA

Chapel Hill, N. C.

On the Rank of Incidence Matrices in Finite Geometries

by

K. J. C. Smith
University of North Carolina
Chapel Hill, N. C.

1. Introduction

Much attention has been given recently to the application of incidence matrices of incomplete block designs to the construction of q-ary linear error-correcting codes. Of particular importance in this connection is the determination of the rank of the incidence matrix of the design over the field GF(q). In this paper, we shall state some results on the rank of the incidence matrix of a configuration of points and d-flats in the finite projective and affine geometries PG(t,q) and EG(t,q). The proofs of these results and their applications to the theory of error-correcting codes are given in [5].

2. Points and d-flats in PG(t,q)

The $v = (q^{t+1}-1)/(q-1)$ points in PG(t,q) may be represented by the non-zero elements of $GF(q^{t+1})$. Here, q is a prime power, say $q=p^n$. Let γ be a primitive element of $GF(q^{t+1})$. The elements γ^{u_1} and γ^{u_2} represent the same point if and only if $u_1 \equiv u_2 \bmod v$. We denote the point represented by γ^u by P_u, $u=0,1,\ldots,v-1$.

For $1 \leq d \leq t-1$, let $\gamma^{e_o}, \gamma^{e_1}, \ldots, \gamma^{e_d}$ be linearly independent over GF(q). A d-flat consists of those points represented by the elements

This research was supported by the National Science Foundation Grant No. GP-5790 and by the U. S. Army Research Office - Durham Grant No. DA-ARD-D-31-124-G910.

γ^u, where

$$\gamma^u = a_0\gamma^{e_0} + a_1\gamma^{e_1} + \dots + a_d\gamma^{e_d},$$

and where $a_0, a_1, \dots, a_d$ run independently over the elements of $GF(q)$ and are not simultaneously zero. Regarding $GF(q^{t+1})$ as a $(t+1)$-dimensional vector space over $GF(q)$, a d-flat corresponds to a $(d+1)$- dimensional subspace of $GF(q^{t+1})$ with the null vector omitted. There are $k = \phi\,(d,0,q)$ points on a d-flat and the number of d-flats in $PG(t,q)$ is $b = \phi\,(t,d,q)$, where

(2.2) $$\phi\,(N,m,q) = \frac{(q^{N+1}-1)\,(q^{N}-1)\dots(q^{N-m+1}-1)}{(q^{m+1}-1)\,(q^{m}-1)\dots(q-1)}\,.$$

For $d=t-1$, each t-dimensional subspace of $GF(q^{t+1})$ is the kernel of a non-zero linear functional from $GF(q^{t+1})$ onto $GF(q)$, which we may express in terms of the trace from $GF(q^{t+1})$ to $GF(q)$. To each $(t-1)$-flat there corresponds a non-zero element μ of $GF(q^{t+1})$ such that the $(t-1)$-flat is the set of points represented by those elements γ^u such that

(2.3) $$T(\mu\gamma^u) = 0,$$

where

(2.4) $$T(x) = x + x^q + \dots + x^{q^t}.$$

Let Σ be a given d-flat, where $1 \leq d \leq t-1$. Suppose the k points on Σ are $P_{u_1}, P_{u_2}, \dots, P_{u_k}$. We may assume $0 \leq u_1 < u_2 < \dots < u_k \leq v-1$. We define the incidence polynomial of the d-flat Σ as the polynomial $I_\Sigma(x)$, given by

(2.5) $$I_\Sigma(x) = x^{u_1} + x^{u_2} + \dots + x^{u_k}.$$

Suppose we order the d-flats in some manner and denote them by $\Sigma_0, \Sigma_1, \dots, \Sigma_{b-1}$. We define the incidence matrix N of points and d-flats in $PG(t,q)$ as the bxv matrix given by $N = (n_{ij})$, where

(2.6) $$n_{ij} = \begin{cases} 1, & \text{if the point } P_j \text{ is incident with the flat } \Sigma_i; \\ 0, & \text{otherwise}, \quad i=0,1,\dots,b-1;\ j=0,1,\dots,v-1. \end{cases}$$

We may regard N as a $(0,1)$-matrix with entries in $GF(q)$.

From equations (2.4) and (2.5), we have

$$I_{\Sigma_i}(x) = \sum_{j=0}^{v-1} n_{ij}x^j \quad , \ i=0,1,\ldots,b-1.$$

The polynomial $I_{\Sigma_i}(x)$ will be regarded as a polynomial in $GF(q)[x]$.

Let $H_d(t,q)$ be the number of integers m, $1 \le m \le v-1$, such that $I_\Sigma(\beta^m) = 0$ for every d-flat Σ, where $\beta = \gamma^{q-1}$ and γ is a primitive element of $GF(q^{t+1})$.

<u>Theorem 2.1</u> [5] Over GF (q), the rank of the incidence matrix N of points and d-flats in PG(t,q) is equal to $v - H_d(t,q)$.

For d=t-1, it is shown in [5] that for any (t-1)-flat Σ and for $1 \le m \le v-1$, $I_\Sigma(\beta^m) = 0$ if and only if $G(\gamma^{-m(q-1)}) = 0$, where

$$G(x) = \sum_{j=0}^{q^{t+1}-2} \left\{1 - [T(\gamma^j)]^{q-1}\right\} x^j.$$

Expanding $1 - [T(x)]^{q-1} = 1 - (x + x^q + \ldots + x^{q^t})^{q-1}$ as a polynomial in x of degree less than $q^{t+1}-1$, it can be shown that for $0 \le u \le q^{t+1}-2$, $G(\gamma^{-u}) \ne 0$ if and only if, in the p-adic representation of u as

$$u = c_0 + c_1 p + \ldots + c_{n-1+tn}p^{n-1+tn},$$

the equations

$$c_j + c_{j+n} + \ldots + c_{j+tn} = p-1$$

hold for each $j = 0,1,\ldots,n-1$. From this it follows that

$$H_{t-1}(t,q) = v - 1 - \binom{p+t-1}{t}^n.$$

Combining this with Theorem 2.1, we have

<u>Theorem 2.2</u> [5] The rank of the incidence matrix N of points and (t-1)-flats in PG(t,q), where $q=p^n$, is equal to

$$\binom{p+t-1}{t}^n + 1.$$

This result was proved by Graham and MacWilliams [2] in the case $t=2$. For general t, it was conjectured by Rudolph [4] and was proved independently by Goethals and Delsarte [1] and by Smith [5], each using different methods. A further proof of this result using the theory of group characters has recently appeared by MacWilliams and Mann [3].

For the case $1 \leq d \leq t-1$, it is shown in [5] that, for $1 \leq m \leq v-1$, $I_\Sigma(\beta^m) = 0$ for every d-flat Σ if and only if, for some $j=0,1,\ldots,n-1$,

$$D_q(p^j m(q-1)) = s(q-1), \quad 1 \leq s \leq d,$$

where $D_q(u)$ denoted the sum of the digits in the q-adic representation of u. That is, if $u = A_0 + A_1 q + \ldots + A_t q^t$, where $0 \leq A_i \leq q-1$, $i=0,1,\ldots,t$, then $D_q(u) = A_0 + A_1 + \ldots + A_t$. This result is obtained in [5] by an extension of the method used by Graham and MacWilliams [2] for the case $t=2$.

Define the functions $L_s(q)$, $B_s(t,q)$ [1] by

$$L_s(q) = \left[\frac{s(q-1)}{q}\right],$$

$$B_s(t,q) = \sum_{i=0}^{L_s(q)} (-1)^i \binom{t+1}{i}\binom{t+s(q-1)-iq}{t},$$

$$R_d(t,q) = \sum_{s=1}^{d} B_s(t,q).$$

It is shown that $R_d(t,q)$ is the number of integers m, $1 \leq m \leq v-1$, such that

$$D_q(m(q-1)) = s(q-1), \quad 1 \leq s \leq d.$$

Hence

$$H_d(t,q) \geq R_d(t,q),$$

and in the case $q = p$,

$$H_d(t,p) = R_d(t,p).$$

---

[1] The notation $[x]$ denotes the greatest integer less than or equal to x.

We have the following theorem.

Theorem 2.3 [5] With $R_d(t,q)$ defined as above, the rank over GF(q) of the incidence matrix N of points and d-flats in PG(t,q) is at most equal to $v - R_d(t,q)$. For $q = p$, the rank of N is equal to $v - R_d(t,p)$.

3. Points and d-flats in EG(t,q)

The q^t points in EG(t,q) may be represented by elements of $GF(q^t)$; two distinct elements represent different points. We shall refer to the point represented by the zero element as the origin. Suppose γ is a primitive element of $GF(q^t)$. Denote the point represented by γ^u by P_u, $u=0,1,\ldots,q^t-2$.

For $1 \leq d \leq t-1$, let $\gamma^{e_1}, \gamma^{e_2}, \ldots, \gamma^{e_d}$ be d elements of $GF(q^t)$ which are linearly independent over GF(q). The set of points represented by the elements

$$a_1\gamma^{e_1} + a_2\gamma^{e_2} + \ldots + a_d\gamma^{e_d}$$

as $a_1,a_2,\ldots,a_d$ run independently over the elements of GF(q) constitute a d-flat in EG(t,q) passing through the origin. Denote this d-flat by Σ. If γ^c does not represent a point on Σ, the set of points represented by the elements

$$\gamma^c + a_1\gamma^{e_1} + \ldots + a_d\gamma^{e_d}$$

constitute a d-flat passing through the point P_c and belonging to the same parallel bundle as Σ. Such a d-flat does not pass through the origin.

Because the structure of d-flats in EG(t,q) which pass through the origin is essentially that of (d-1)-flats in PG(t-1,q), we shall henceforth consider only d-flats which do not pass through the origin. Also, unless otherwise stated, we shall not consider the origin as a point. There are $b' = (q^{t-d}-1)\ \Phi\ (t-1,d-1,q)$ d-flats in EG(t,q) which do not pass through the origin; each d-flat contains $k' = q^d$ points.

As in Section 2, we may consider a (t-1)-flat in EG(t,q) as the set of points represented by those elements γ^u such that

$$T(\mu\gamma^u) = 1,$$

where μ is a non-zero element of $GF(q^t)$ and $T(x) = x + x^q = \ldots + x^{q^{t-1}}$.

For a given d-flat Σ, $1 \le d \le t-1$, suppose the k' points on Σ are $P_{u_1}, P_{u_2}, \ldots, P_{u_{k'}}$, where we may assume $0 \le u_1 < u_2 < \ldots < u_{k'} \le q^t-2$. We define the incidence polynomial of Σ as the polynomial

$$I_\Sigma(x) = x^{u_1} + x^{u_2} + \ldots + x^{u_{k'}}.$$

After ordering the b' d-flats in some manner, we define the incidence matrix N of points and d-flats as the matrix $N = (n_{ij})$, where

$$n_{ij} = \begin{cases} 1, & \text{if the point } P_j \text{ is incident with the flat } \Sigma_i; \\ 0, & \text{otherwise}, \quad i=0,1,\ldots,b'-1;\ j=0,1,\ldots,q^t-2. \end{cases}$$

Again,

$$I_{\Sigma_i}(x) = \sum_{j=0}^{q^t-2} n_{ij}x^j \quad , \ i=0,1,\ldots,b'-1.$$

Regarding N as a matrix with entries in GF(q) and $I_{\Sigma_i}(x)$ as a polynomial in GF(q) [x], let us define $K_d(t,q)$ as the number of integers u, $0 \le u \le q^t-2$ such that $I_\Sigma(\gamma^u) = 0$ for every d-flat Σ in EG(t,q) which does not pass through the origin.

<u>Theorem 3.1</u> [5] Over GF(q), the rank of the incidence matrix N of points and d-flats not passing through the origin in EG(t,q) is equal to $q^t - 1 - K_d(t,q)$.

Using methods analogous to those used in Section 2, it is shown in [5] that

$$K_{t-1}(t,q) = q^t - \binom{p+t-1}{t}^n$$

and for $1 \leq d \leq t-1$,

$$K_d(t,q) \geq R_d(t,q) - R_d(t-1,q)$$

with equality holding for $q = p$, where $R_d(t,q)$ is defined in Section 2. We state this as a theorem.

<u>Theorem 3.2</u> [5] Over $GF(q)$, $q = p^n$ the rank of the incidence matrix of points and d-flats not passing through the origin in $EG(t,q)$ is

(i) for $d = t-1$, equal to

$$\binom{p+t-1}{t}^n - 1,$$

(ii) for $1 \leq d \leq t-1$, at most equal to

$$q^t - 1 - R_d(t,q) + R_d(t-1,q),$$

with equality holding for the case $q = p$.

References

1. Goethals, J. M. and Delsarte, P. "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. "On the Number of Information Symbols in Difference-Set Cyclic Codes," Bell System Tech. J., 45 (1966), 1057-1070.

3. MacWilliams, F. J. and Mann, H. B. "On the p-rank of the Design Matrix of a Difference Set," Mathematics Research Center, University of Wisconsin, Technical Report No. 803, 1967.

4. Rudolph, L. D. "A Class of Majority Logic Decodable Codes," IEEE Trans. Information Theory, IT-13 (1967), 305-307.

5. Smith, K. J. C. "Majority Decodable Codes Derived from Finite Geometries," Institute of Statistics, University of North Carolina at Chapel Hill, Mimeo Series No.   , 1967.