ISRAEL JOURNAL OF MATHEMATICS, Vol. 71, No. 3, 1990

RANK OF INCLUSION MATRICES AND MODULAR REPRESENTATION THEORY

BY

AVITAL FRUMKIN AND ARIEH YAKIR

Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel

ABSTRACT

We use results from the modular representation theory of the groups S_n and $GL_n(\mathbf{F}_q)$ to determine the rank of inclusion matrices.

§0. Introduction

In this paper we shall compute the rank of the incidence matrix of the lattice of subsets of a finite set or the lattice of subspaces of a finite dimensional vector space over the finite field $\mathbf{F}_q$ ($q = p^d$, p a prime number). The computation of the rank will be carried out over any field K except:

(a) $\mathrm{char}(K) = 2$ for the incidence matrix of subsets.

(b) $\mathrm{char}(K) = p$ ($q = p^d$) for the incidence matrix of subspaces.

The argument will rely upon the representation theory of the groups S_n and $GL_n(\mathbf{F}_q)$ over the field K or over an extension of K, as they are developed in G. James's books [4], [5]. It is well known that if $\mathrm{char}(K) = 0$ then the incidence matrix of subsets and the incidence matrix of subspaces have full rank (see [2], [3], [6]). The rank of the incidence matrix of subsets was determined by Linial and Rothschild [7] for a field K of characteristic 2 and for arbitrary K by Wilson [8]. An independent proof for arbitrary K appears in Frankl [1]. We believe that the result concerning the rank of the incidence matrix of subspaces is new. We shall examine subsets and subspaces simultaneously. (The case of subsets becomes a "special" case of subspaces by taking $q = 1$.) Let n be a fixed natural number. Let q be either 1 or a positive power of a prime p. For $2 \le q$ define

$$\Delta_{i,q} := \left\{ U \le \mathbf{F}_q^{(n)} \,\middle|\, \dim U = i \right\}$$

($\mathbf{F}_q^{(n)}$ is an n-dimensional vector space over $\mathbf{F}_q$);

Received November 22, 1989

$$\Delta_{i,1} := \left\{ x \subseteq \{1,2,3,\ldots,n\} \,\middle|\, |X| = i \right\},$$

$$\begin{bmatrix} n \\ i \end{bmatrix}_q := |\Delta_{i,q}|.$$

We shall sometimes suppress the q and write $\left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right]$ or Δ_i.

$A^{l,k}$ is a matrix over the field K with $\left[\begin{smallmatrix} n \\ l \end{smallmatrix}\right]$ rows and $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ columns. $A^{l,k}$ rows correspond to the elements of Δ_l and its columns to the elements of Δ_k.

For $x \in \Delta_k$, $y \in \Delta_l$

$$A^{l,k}_{y,x} = \begin{cases} 1, & y \subseteq x; \\ 0, & \text{otherwise.} \end{cases}$$

In this paper we shall prove:

THEOREM. *Let* $l \le k$, $l + k \le n$.
If $q = 1$ *assume* $\mathrm{char}(K) \neq 2$.
If $q \ge 2$, $q = p^d$, *p a prime, assume* $\mathrm{char}(K) \neq p$.
Put $Y = \left\{ i \,\middle|\, 0 \le i \le l, \left[\begin{smallmatrix} k-i \\ l-i \end{smallmatrix}\right] \neq 0 \right\}$. *Then*

$$\mathrm{rank}_K(A^{l,k}) = \sum_{i \in Y} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}.$$

(*We assume* $\left[\begin{smallmatrix} n \\ -1 \end{smallmatrix}\right] = 0$.)

REMARK (i). The theorem remains true for the case $q = 1$ and $\mathrm{char}(K) = 2$ (see [1], [7], and [8] for proofs) but our method fails in this case. The theorem is false for the case $q \ge 2$, $q = p^d$, p a prime, $\mathrm{char}(K) = p$: It is easy to see that for $x, y \in \Delta_k$

$$(A^{k,k+1} \circ {}^{t}A^{k,k+1})_{x,y} = \begin{cases} 0, & \dim(x+y) > k+1, \\ 1, & \dim(x+y) = k+1, \\ \left[\begin{smallmatrix} n-k \\ 1 \end{smallmatrix}\right], & x = y; \end{cases}$$

$$({}^{t}A^{k-1,k} \circ A^{k-1,k})_{x,y} = \begin{cases} 0, & \dim(x \cap y) < k-1, \\ 1, & \dim(x \cap y) = k-1, \\ \left[\begin{smallmatrix} k \\ 1 \end{smallmatrix}\right], & x = y. \end{cases}$$

Hence

$$A^{k,k+1} \circ {}^{t}A^{k,k+1} - {}^{t}A^{k-1,k} \circ A^{k-1,k} = \left(\begin{bmatrix} n-k \\ 1 \end{bmatrix} - \begin{bmatrix} k \\ 1 \end{bmatrix} \right) I_k$$

where I_k is the $\begin{bmatrix} n \\ k \end{bmatrix} \times \begin{bmatrix} n \\ k \end{bmatrix}$ identity matrix. But

$$\begin{bmatrix} n-k \\ 1 \end{bmatrix} - \begin{bmatrix} k \\ 1 \end{bmatrix} \equiv 0 (\operatorname{mod} q).$$

Therefore, if $q = p^d$, $\operatorname{char}(K) = p$ then

$$A^{k,k+1} \circ {}^{t}A^{k,k+1} = {}^{t}A^{k-1,k} \circ A^{k-1,k}.$$

Now take n to be any odd number (≥ 3). Put $k = (n-1)/2$. Obviously

$$\operatorname{rank}_K({}^{t}A^{k-1,k} \circ A^{k-1,k}) \leq \operatorname{rank}_K(A^{k-1,k}) \leq \begin{bmatrix} n \\ k-1 \end{bmatrix} = \begin{bmatrix} n \\ \frac{n-3}{2} \end{bmatrix}.$$

But $A^{k,k+1}$ is a square matrix. If it is regular, so is $A^{k,k+1} \circ {}^{t}A^{k,k+1}$. Thus $A^{k,k+1}$ is not regular.

So

$$\operatorname{rank}_K(A^{k,k+1}) < \begin{bmatrix} n \\ k \end{bmatrix}.$$

Put

$$Y = \left\{ i \middle| 0 \leq i \leq k, \begin{bmatrix} k+1-i \\ k-i \end{bmatrix} \neq 0 \right\}.$$

If $\operatorname{char}(K) = p$ $(q = p^d)$ then $Y = \left\{ i \middle| 0 \leq i \leq k \right\}$. Therefore

$$\sum_{i \in Y} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix} = \begin{bmatrix} n \\ k \end{bmatrix}.$$

So our theorem does not hold in this case.

Remark (ii). If $l + k > n$ then $(n-k) + (n-l) < n$. By passing to the dual space of $\mathbf{F}_q^{(n)}$ and replacing each $U \in \Delta_{i,q}$ by its annihilator, one can easily see that

$$\operatorname{rank}_K(A^{l,k}) = \operatorname{rank}_K(A^{n-k,n-l}).$$

(If $q = 1$ replace each $x \in \Delta_{i,1}$ by its complement in $\{1, \ldots, n\}$.)

A modification of [5, Th. 13.3] (if true) can be used to obtain a short proof of our theorem. Without the modification, however, this short proof applies only to the case $l \leq k \leq n/2$. We shall not pursue this point of view here.

The Symmetric Group S_n acts as a permutation group on the set $\Delta_{i,1}$. For $2 \leq q$ the General Linear Group $\mathrm{GL}_n(\mathbf{F}_q)$ acts as a permutation group on the set $\Delta_{i,q}$.

If Δ is a finite set and K is a field, we define $K\Delta$ to be the K-vector-space of formal K-linear combinations of elements of Δ. Δ is a basis of $K\Delta$ over K.

If a group G acts as a permutation group on the set Δ, then under the definition

$$g \cdot \sum_{x\in\Delta} a_x x := \sum_{x\in\Delta} a_x gx \qquad (g \in G,\ a_x \in K)$$

$K\Delta$ is a module over the group-ring KG. In our argument G will be either S_n (if $q = 1$) or $\mathrm{GL}_n(\mathbf{F}_q)$ (if $q \geq 2$).

For each i $(0 \leq i \leq n)$ $M^{i,q}$ will be $K\Delta_{i,q}$ (again, we shall suppress the q and write M^i). M^i is a module over the group-ring KG. We shall always assume that $l \leq k$ and $l + k \leq n$.

$\varphi^{l,k} : M^k \to M^l$ will be the linear transformation whose matrix with respect to the bases Δ_k of M^k and Δ_l of M^l is $A^{l,k}$. That is:

$$(\forall x \in \Delta_k) \qquad \varphi^{l,k}(x) = \sum_{\substack{y\in\Delta_l \\ y\subseteq x}} 1 \cdot y.$$

Since $\forall g \in G$, $A^{l,k}_{gy,gx} = A^{l,k}_{y,x}$ it follows $\varphi^{l,k} \in \hom_{KG}(M^k, M^l)$.

Definition.

(a) $M^{\leq l} = \bigoplus_{i=0}^{l} M^i$.

(b) $\varphi^{\leq l,k} = \bigoplus_{i=0}^{l} \varphi^{i,k}$, $\varphi^{\leq l,k} : M^k \to M^{\leq l}$.

It is obvious that the set $\bigcup_{i=0}^{l} \Delta_i$ is a basis for $M^{\leq l}$ over K. The matrix of $\varphi^{\leq l,k}$ with respect to the bases Δ_k of M^k and $\bigcup_{i=0}^{l} \Delta_i$ of $M^{\leq l}$ is obtained by stacking the rows of

$$A^{0,k}, A^{1,k}, A^{2,k}, \ldots, A^{l,k}$$

as follows:

$$\begin{matrix} A^{l,k} \\ \vdots \\ \vdots \\ A^{1,k} \\ A^{0,k}. \end{matrix}$$

We shall call this matrix $A^{\leq l,k}$.

In Frankl [1], the rank of the matrix $A^{l,k}$ is determined by using the rank of matrices of the type $A^{\leq j,h}$. We show in §3 how this is done. In §2 we compute $\mathrm{rank}_K(A^{\leq l,k})$.

§1. Background from the representation theory of the group S_n and the group $\mathrm{GL}_n(\mathbf{F}_q)$ over the field K

In the case $q = 1$ ($G = S_n$) we shall have to assume at some point that $\mathrm{char}(K) \neq 2$. In the case $q \geq 2$ ($G = \mathrm{GL}_n(\mathbf{F}_q)$) we shall have to assume that $\mathrm{char}(K) \neq p$ where $q = p^d$ (p a prime). Moreover, we have to assume also that K contains a primitive p-th root of unity. If K does not contain a primitive p-th root of unity, we can of course (if $\mathrm{char}(K) \neq p$) extend K to a larger field. Obviously, extension of the field does not change the rank of $A^{l,k}$ or $A^{\leq l,k}$.

A symmetric linear form $\langle\ ,\ \rangle$ is defined over M^i. The definition of $\langle\ ,\ \rangle$ is carried out by stating that Δ_i is an orthonormal basis of M^i.

The module M^i has a submodule S^i (which is called Specht-Module). Below are known facts about S^i:

(a) If $i \leq n/2$ then $\dim S^i = \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}$. (Actually, what we need is $\dim S^i \geq \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}$, which is easier to prove and appears implicitly in [5, Chapter 12].) See [4, Ex. 14.4] and [5, Th. 13.3].

(b) THE SUBMODULE THEOREM. *If W is a submodule of M^i then either $S^i \subseteq W$ or $W \subseteq (S^i)^\perp$ ($\perp$ with respect to $\langle\ ,\ \rangle$).*

See [4, 4.8] and [5, 11.12 (ii)].

(c) There is $\alpha \in M^i$ and there is an idempotent $r \in KG$ such that:

(i) $S^i = \mathrm{Span}_{KG}(r \cdot \alpha)$, and

(ii) if $j < i \leq n/2$ then $\forall \delta \in M^j\ r \cdot \delta = 0$.

See [4, 4.5 & 4.6] and [5, 11.7 & 11.11].

REMARK. In [4], James establishes the existence of an element $s \in KG$ satisfying $s \cdot s = 2^i s$ rather than an idempotent. We assume, when $q = 1$, that $\mathrm{char}(K) \neq 2$ so we can define

$$r := 2^{-i} s.$$

It is easily seen that $r^2 = r$. For $q \geq 2$ ($q = p^d$, p a prime), the construction of the idempotent r is possible if K contains a primitive p-th root of unity (which is possible only if $\mathrm{char}(K) \neq p$).

The cumbersome fact which follows is necessary only for the proof of Theorem 1.2 below.

(d) (i) For $i \le n/2$ define

$$\Gamma := \left\{ x \in \Delta_{i,1} \middle| \forall j[(1 \le j \le i) \Rightarrow (j \in x \text{ or } n-j+1 \in x)] \right\},$$

$$(\forall x \in \Gamma) \qquad s_x = \#\left\{ j \middle| 1 \le j \le i,\ j \notin x \right\}.$$

Define $\beta \in M^{i,1}$ by

$$\beta := \sum_{x \in \Gamma} (-1)^{s_x} x;$$

then $\beta \in S^i$.

See [4, Def. 4.3].

(ii) Let $q \ge 2$. Let $\epsilon_1, \ldots, \epsilon_n$ be a basis of $\mathbf{F}_q^{(n)}$ over $\mathbf{F}_q$. Assume $i \le n/2$. For each j $(1 \le j \le i)$ define

$$\Phi_j := \left\{ \sum_{t=1}^{2j} a_t \epsilon_t \middle| a_t \in \mathbf{F}_q,\ a_{2j} = 1,\ a_{2j-1} \in \{0,1\},\ \forall t < j,\ a_{2t} = 0 \right\}.$$

For $v \in \Phi_j$, $v = \sum_{t=1}^{2j} a_t \epsilon_t$, define

$$s(v) = \begin{cases} 1, & a_{2j-1} = 1, \\ 0, & a_{2j-1} = 0; \end{cases}$$

$$\Gamma := \left\{ U \in \Delta_{i,q} \middle| (\exists v_1 \in \Phi_1, v_2 \in \Phi_2, \ldots, v_i \in \Phi_i) U = \mathrm{Span}_{\mathbf{F}_q}(v_1, \ldots, v_i) \right\}.$$

If $U \in \Gamma$ and if $U = \mathrm{Span}_{\mathbf{F}_q}(v_1, \ldots, v_i)$ $(v_t \in \Phi_t)$ then, for each t, v_t is uniquely determined so we can define $s(U) = \sum_{t=1}^{i} s(v_t)$.

Now define $\beta \in M^{i,q}$ by

$$\beta := \sum_{U \in \Gamma} (-1)^{s(U)} U;$$

then $\beta \in S^i$.

See [5, Ex. 11.17 (v)].

Using the above facts we shall now prove three theorems.

1.1. Theorem. *If $q = 1$ assume* $\mathrm{char}(K) \ne 2$, *and if $q \ge 2$, $q = p^d$, p prime, assume K contains a p-th primitive root of unity* (*so of course* $\mathrm{char}(K) \ne p$). *Assume also that $i \le n/2$. Then there exists a basis B^i of S^i and for each $\beta \in B^i$ there exists an idempotent $r_\beta \in KG$ s.t.*

(i) $r_\beta \cdot \beta = \beta$;

(ii) *if $j < i$ then*, $\forall \delta \in M^j$, $r_\beta \cdot \delta = 0$.

PROOF. Take $\alpha \in M^i$ and $r \in KG$ whose existence is assured by Fact (c) above. Since $S^i = \mathrm{Span}_{KG}(r\alpha)$ it follows that $S^i = \mathrm{Span}_K\{gr\alpha \mid g \in G\}$. Let B^i then be any subset of $\{gr\alpha \mid g \in G\}$ which is a basis of S^i over the field K. Take $\beta \in B^i$. There is $g \in G$ s.t. $\beta = gr\alpha$. Define $r_\beta := grg^{-1}$. $r_\beta \in KG$ is an idempotent $(r_\beta^2 = grg^{-1}\cdot grg^{-1} = gr^2g^{-1} = grg^{-1})$.

Also, $r_\beta\beta = grg^{-1}\cdot gr\alpha = gr^2\alpha = gr\alpha = \beta$. If $j < i$ and $\delta \in M^j$ then $r_\beta\cdot\delta = (grg^{-1})\delta = g(r(g^{-1}\delta)) = g\cdot 0 = 0$.

1.2. THEOREM. *If $i \leq k$ and $i + k \leq n$ then there exists $\alpha \in M^k$, $\beta \in S^i$ s.t.*

$$\langle \beta, \varphi^{i,k}\alpha\rangle = 1.$$

PROOF. $2i = i + i \leq i + k \leq n$. Therefore we can exploit Fact (d) above. We shall examine the cases $q = 1$ and $q \geq 2$ separately.

(i) $q = 1$. Take $\alpha = 1\cdot\{1,2,3,\ldots,k\} \in M^k$. Let β be the same β which appears in Fact (d)(i). β is supported by 2^i elements of Δ_i. One of them is $\{1,2,\ldots,i\}$. For each element x of Δ_i which supports β, except $\{1,2,\ldots,i\}$, there exists j, $1 \leq j \leq i$, s.t. $n - j + 1 \in x$. But $i + k \leq n$. Therefore $j + k \leq n$, $k \leq n - j$, $k < n - j + 1$. So $x \not\subseteq \{1,2,\ldots,k\}$. Hence of all 2^i elements supporting β, only one, namely $\{1,2,\ldots,i\}$, is contained in $\{1,2,\ldots,k\}$. The coefficient of $\{1,2,\ldots,i\}$ in β is 1 and therefore $\langle\beta,\varphi^{i,k}\alpha\rangle = 1$.

(ii) $q \geq 2$. We follow the beginning of the proof of Th. 13.3 in [5]. Let $\epsilon_1,\ldots,\epsilon_n$ be a basis of $\mathbf{F}_q^{(n)}$ over $\mathbf{F}_q$. Take $\alpha = 1\cdot\mathrm{Span}_{\mathbf{F}_q}(\epsilon_2,\epsilon_4,\epsilon_6,\ldots,\epsilon_{2i},\epsilon_{2i+1},\epsilon_{2i+2},\ldots,\epsilon_{k+i}) \in M^k$. (This is possible if $i \leq k$ and $i + k \leq n$.) Let β be the same β which appears in Fact (d)(ii). Let U be an i-dimensional subspace of $\mathrm{Span}_{\mathbf{F}_q}(\epsilon_2,\epsilon_4,\ldots,\epsilon_{2i},\epsilon_{2i+1},\ldots,\epsilon_{k+i})$. If the support of U (with respect to the basis $\epsilon_1,\ldots,\epsilon_n$ of $\mathbf{F}_q^{(n)}$) contains one of $\epsilon_{2i+1},\epsilon_{2i+2},\ldots,\epsilon_{k+i}$ then obviously $U \notin \Gamma$ (the Γ defined in Fact (d)(ii)). Therefore, if $U \in \Gamma$ then the support of U (with respect to $\epsilon_1,\ldots,\epsilon_n$) is contained in $\{\epsilon_2,\epsilon_4,\epsilon_6,\ldots,\epsilon_{2i}\}$. Since $\dim U = i$ it follows that

$$U = \mathrm{Span}_{\mathbf{F}_q}(\epsilon_2,\epsilon_4,\ldots,\epsilon_{2i}).$$

So the only element of Γ which is contained in $\mathrm{Span}_{\mathbf{F}_q}(\epsilon_2,\epsilon_4,\ldots,\epsilon_{2i},\epsilon_{2i+1},\ldots,\epsilon_{i+k})$ is $\mathrm{Span}_{\mathbf{F}_q}(\epsilon_2,\ldots,\epsilon_{2i})$. The coefficient of $\mathrm{Span}_{\mathbf{F}_q}(\epsilon_2,\ldots,\epsilon_{2i})$ in β is 1. Therefore

$$\langle\beta,\varphi^{i,k}\alpha\rangle = 1.$$

1.3. THEOREM. *If $i \leq k$ and $i + k \leq n$ then*

$$S^i \subseteq \mathrm{im}\varphi^{i,k}.$$

PROOF. Theorem 1.2 shows that

$$\operatorname{im}\varphi^{i,k} \not\subseteq (S^i)^\perp.$$

Therefore, according to the Submodule Theorem (Fact (b)), it follows that

$$S^i \subseteq \operatorname{im}\varphi^{i,k}.$$

§2. Computation of $\operatorname{rank}_K(A^{\le l,k})$

In this section we shall prove:

2.1. THEOREM. *Let* $l \le k$, $l + k \le n$.
If $q = 1$ *assume* $\operatorname{char}(K) \ne 2$.
If $q \ge 2$, $q = p^d$, p *prime, assume* $\operatorname{char}(K) \ne p$.
Then $\operatorname{rank}_K(A^{\le l,k}) = \begin{bmatrix} n \\ l \end{bmatrix}$.

PROOF.

$$\operatorname{rank}(A^{\le l,k}) = \dim\operatorname{im}(\varphi^{\le l,k}).$$

At first we shall find $\begin{bmatrix} n \\ l \end{bmatrix}$ linearly independent vectors in $\operatorname{im}(\varphi^{\le l,k})$. For each i ($0 \le i \le l$) let B^i be the basis of S^i constructed in Theorem 1.1. (If $\operatorname{char}(K) \ne p$ we can extend K to contain a primitive p-th root of unity.) For each $\beta \in B^i$ choose $\epsilon_\beta \in M^k$ s.t. $\varphi^{i,k}(\epsilon_\beta) = \beta$. (This is possible by Theorem 1.3.)

Set

$$H^i := \left\{ \varphi^{\le l,k}(r_\beta \epsilon_\beta) \,\middle|\, \beta \in B^i \right\}.$$

Fix i ($0 \le i \le l$). Let $\beta \in B^i$.

$$\begin{aligned} \varphi^{\le l,k}(r_\beta\epsilon_\beta) &= \bigoplus_{j=0}^{l} \varphi^{j,k}(r_\beta\epsilon_\beta) \\ &= \bigoplus_{j=0}^{i-1} \varphi^{j,k}(r_\beta\epsilon_\beta) \oplus \varphi^{i,k}(r_\beta\epsilon_\beta) \oplus \bigoplus_{j=i+1}^{l} \varphi^{j,k}(r_\beta\epsilon_\beta) \\ &= \bigoplus_{j=0}^{i-1} 0 \oplus \beta \oplus \bigoplus_{j=i+1}^{l} \varphi^{j,k}(r_\beta\epsilon_\beta). \end{aligned}$$

(*Explanation*: $\varphi^{j,k}(r_\beta\epsilon_\beta) = r_\beta\varphi^{j,k}(\epsilon_\beta)$. If $j < i$ then, since $\varphi^{j,k}(\epsilon_\beta) \in M^j$, it follows that $r_\beta \cdot \varphi^{j,k}(\epsilon_\beta) = 0$. $\varphi^{i,k}(r_\beta\epsilon_\beta) = r_\beta\varphi^{i,k}(\epsilon_\beta) = r_\beta\beta = \beta$.)

"Picture" of $\varphi^{\leq l,k}(\beta)$:

$$\varphi^{\leq l,k}(\beta) = \begin{array}{lll} \star & : l & \textit{component} \\ \star & : l-1 & \text{"} \\ \vdots & & \\ \vdots & & \\ \star & : i+1 & \text{"} \\ \beta & : i & \text{"} \\ 0 & : i-1 & \text{"} \\ 0 & : i-2 & \text{"} \\ \vdots & & \\ 0 & : 0 & \text{"} \end{array}$$

CLAIM. For each $\gamma \in H^i$

$$\gamma \notin \operatorname{Span}_K\left((H^i \setminus \{\gamma\}) \cup \bigcup_{j=i+1}^{l} H^j\right).$$

PROOF OF THE CLAIM. The i component of γ is some β, $\beta \in B^i$. B^i is linearly independent (being a basis of S^i). The i component of elements of $\bigcup_{j=i+1}^{l} H^j$ is zero.

An obvious consequence from the claim is that $\bigcup_{i=0}^{l} H^i$ is a linearly independent set.

$$\left|\bigcup_{i=0}^{l} H^i\right| = \sum_{i=0}^{l} |H^i| = \sum_{i=0}^{l} |B^i| = \sum_{i=0}^{l} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix} = \begin{bmatrix} n \\ l \end{bmatrix}.$$

It is obvious that $\bigcup_{i=0}^{l} H^i \subseteq \operatorname{im}(\varphi^{\leq l,k})$. So we have $\dim \operatorname{im}(\varphi^{\leq l,k}) \geq \begin{bmatrix} n \\ l \end{bmatrix}$. In other words, $\operatorname{rank}_K(A^{\leq l,k}) \geq \begin{bmatrix} n \\ l \end{bmatrix}$. It remains to prove

$$\operatorname{rank}_K(A^{\leq l,k}) \leq \begin{bmatrix} n \\ l \end{bmatrix}.$$

It suffices to prove this inequality in the case $\operatorname{char}(K) = 0$. (If A is a matrix over $\mathbf{Z}$ then, for each field K, $\operatorname{rank}_K(A) \leq \operatorname{rank}_{\mathbf{Q}}(A)$.) An easy calculation shows: If $i \leq l \leq k$ then $A^{i,l} \circ A^{l,k} = \begin{bmatrix} k-i \\ l-i \end{bmatrix} A^{i,k}$. But if $\operatorname{char}(K) = 0$ then $\begin{bmatrix} k-i \\ l-i \end{bmatrix} \neq 0$ so the rows of the matrix $A^{i,k}$ are linear combinations of the rows of $A^{l,k}$. Therefore

$$\operatorname{rank}_K(A^{\leq l,k}) \leq \operatorname{rank}_K(A^{l,k}) \leq \begin{bmatrix} n \\ l \end{bmatrix}.$$

§3. $\mathrm{rank}_K(A^{l,k})$

In this section we shall determine $\mathrm{rank}_K(A^{l,k})$ by using the result about the rank of matrices of the type $A^{\le j,h}$. The argument follows [1] and is given here for the sake of completeness (there being no difference between the case $q \ge 2$ and the case $q = 1$ dealt with by [1]).

3.1. THEOREM. *Let $l \le k$, $l + k \le n$. If $q = 1$ assume $\mathrm{char}(K) \ne 2$. If $q \ge 2$, $q = p^d$, p a prime, assume $\mathrm{char}(K) \ne p$. Put*

$$Y = \left\{ i \,\middle|\, 0 \le i \le l,\ \begin{bmatrix} k-i \\ l-i \end{bmatrix} \ne 0 \right\}.$$

Then

$$\mathrm{rank}_K(A^{l,k}) = \sum_{i \in Y} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}.$$

PROOF. Put

$$Z = \left\{ i \,\middle|\, 0 \le i \le l,\ \begin{bmatrix} k-i \\ l-i \end{bmatrix} = 0 \right\}.$$

The vector space spanned by the rows of the matrix $A^{\le l,k}$ has a basis with the property: for all i $(0 \le i \le l)$, $\left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right] - \left[\begin{smallmatrix} n \\ i-1 \end{smallmatrix}\right]$ of the elements of the basis are taken from the rows of $A^{i,k}$. (This follows by induction on l using Theorem 2.1.) But if $i \le l \le k$ then

$$A^{i,l} \circ A^{l,k} = \begin{bmatrix} k-i \\ l-i \end{bmatrix} A^{i,k}.$$

For each $i \in Y$ the rows of $A^{i,k}$ are linear combinations of the rows of $A^{l,k}$, so in the space spanned by the rows of $A^{l,k}$ there are at least $\sum_{i \in Y} \left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right] - \left[\begin{smallmatrix} n \\ i-1 \end{smallmatrix}\right]$ linearly independent vectors.

Therefore $\mathrm{rank}_K(A^{l,k}) \ge \sum_{i \in Y} \left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right] - \left[\begin{smallmatrix} n \\ i-1 \end{smallmatrix}\right]$.

Now let E be the matrix obtained by stacking the rows of the matrices $A^{i,l}$, $i \in Z$. Since for each $i \in Z$, $A^{i,l} \circ A^{l,k} = 0$, it follows that $E \circ A^{l,k} = 0$.

$$0 = \mathrm{rank}_K(0) \ge \mathrm{rank}_K(E) + \mathrm{rank}_K(A^{l,k}) - \begin{bmatrix} n \\ l \end{bmatrix}.$$

But the row space of $A^{\le l,l}$ has basis with the property: for all i $(0 \le i \le l)$, $\left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right] - \left[\begin{smallmatrix} n \\ i-1 \end{smallmatrix}\right]$ elements of the basis are taken from the rows of the matrix $A^{i,l}$.

Therefore

$$\operatorname{rank}_K(E) \geq \sum_{i\in Z} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}.$$

Hence

$$0 \geq \sum_{i\in Z} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix} + \operatorname{rank}_K(A^{l,k}) - \begin{bmatrix} n \\ l \end{bmatrix}.$$

$$\operatorname{rank}_K(A^{l,k}) \leq \begin{bmatrix} n \\ l \end{bmatrix} - \sum_{i\in Z} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix} = \sum_{i\in Y} \begin{bmatrix} n \\ i \end{bmatrix} - \begin{bmatrix} n \\ i-1 \end{bmatrix}.$$

§4. Affine subspaces

Let $\mathbf{F}_q$ be a field with q elements. As before, let

$$\Delta_{i,q} = \left\{ U \leq \mathbf{F}_q^{(n)} \,\middle|\, \dim U = i \right\}.$$

Put

$$\Gamma_{i,q} = \left\{ \alpha + U \,\middle|\, \alpha \in \mathbf{F}_q^{(n)},\ U \in \Delta_{i,q} \right\}.$$

Let K be any field. $A^{l,k}$ is a

$$q^{n-l} \begin{bmatrix} n \\ l \end{bmatrix} \times q^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}$$

matrix over K whose rows correspond to the elements of $\Gamma_{l,q}$ and whose columns correspond to the elements of $\Gamma_{k,q}$. For $x \in \Gamma_{k,q}$, $y \in \Gamma_{l,q}$

$$A^{l,k}_{y,x} = \begin{cases} 1, & y \subseteq x, \\ 0, & \text{otherwise}. \end{cases}$$

In a subsequent paper [9] the second author proves the following result: Assume $\operatorname{char}(K) \neq \operatorname{char}(\mathbf{F}_q)$. Let

$$l \leq k, \qquad l + k \leq n - 1.$$

Put

$$Y = \left\{ i \,\middle|\, 0 \leq i \leq l,\ \begin{bmatrix} k-i \\ l-i \end{bmatrix} \neq 0 \right\}.$$

Then

$$\operatorname{rank}_K(A^{l,k}) = \sum_{i\in Y} \left(q^{n-i} \begin{bmatrix} n \\ i \end{bmatrix} - q^{n-i+1} \begin{bmatrix} n \\ i-1 \end{bmatrix} \right).$$

References

1. P. Frankl, *Intersection theorems and* mod *p rank of inclusion matrices*, J. Comb. Theory, Ser. A **54** (1990), 85–94.

2. D. H. Gottlieb, *A certain class of incidence matrices*, Proc. Am. Math. Soc. **17** (1966), 1233–1237.

3. R. L. Graham, S.-Y.R. Li and W.-C.W. Li, *On the structure of t-designs*, SIAM J. Alg. Disc. Methods **1** (1980), 8–14.

4. G. D. James, *The representation theory of the symmetric groups*, Lecture Notes in Math., Vol. 682, Springer-Verlag, Berlin, 1978.

5. G. D. James, *Representations of general linear groups*, London Math. Soc. Lect. Note Ser., Vol. 94, Cambridge University Press, 1984.

6. W. M. Kantor, *On incidence matrices of finite projective and affine spaces*, Math. Z. **124** (1972), 315–318.

7. N. Linial and B. L. Rothschild, *Incidence matrices of subsets—a rank formula*, SIAM J. Alg. Disc. Methods **2** (1981), 333–340.

8. R. M. Wilson, *A diagonal form for the incidence matrices of t-subsets vs. k-subsets*, Eur. J. Combinatorics, to appear.

9. A. Yakir, *The permutation representation of the general affine group on the set of affine subspaces*, in preparation.