THE p-RANK OF THE INCIDENCE MATRIX OF INTERSECTING LINEAR SUBSPACES.

Peter Sin

University of Florida

Abstract. Let V be a vector space of dimension $n+1$ over a field of p^t elements. A d-dimensional subspace and an e-dimensional subspace are considered to be incident if their intersection is not the zero subspace. The rank of these incidence matrices, modulo p, are computed for all n, d, e and t. This result generalizes the well known formula of Hamada for the incidence matrices between points and subspaces of given dimensions in a finite projective space. A generating function for these ranks as t varies, keeping n, d and e fixed, is also given. In the special case where the dimensions are complementary, i.e. $d+e=n+1$, our formula improves previous upper bounds on the size of partial m-systems (as defined by Shult and Thas).

§1. Incidence geometry of linear subspaces

Let V be an $(n+1)$-dimensional vector space over $\mathbb{F}_q$, where $q=p^t$. For $1 \le i \le n$ let $\mathcal{L}_i$ denote the set of i-dimensional subspaces of V (i-subspaces for short). Then $\mathcal{L}_1$ is the set of points of the projective space $\mathbb{P}(V)$ and $\mathcal{L}_n$ the set of hyperplanes. Aside from trivialities, there is just one natural incidence relation between points and hyperplanes, that for which a point is incident to a hyperplane if it lies in the hyperplane. When we seek to generalize by replacing points and hyperplanes with subspaces of V of a fixed dimensions e and d respectively, there are several incidence relations which might be considered. One is *inclusion*, in which two subspaces are taken to be incident if the smaller is contained in the larger. Another natural notion of incidence is *non-zero intersection*, in which an d-dimensional subspace and an e-dimensional subspace are considered to be incident if their intersection is not the zero subspace. It is the latter incidence relation which we study in this note.

The number of i-dimensional subspaces in V is equal to

$$\begin{bmatrix} n+1 \\ i \end{bmatrix}_q = \frac{(q^{n+1}-1)\cdots(q^{n-i+2}-1)}{(q-1)\cdots(q^i-1)}. \tag{1}$$

Supported by NSF grant DMS0071060

In particular, this number is congruent to 1 modulo p. Let $A(d,e)$ be the incidence matrix of the incidence relation of non-zero intersection between $\mathcal{L}_d$ and $\mathcal{L}_e$ (ordered in some arbitrary but fixed fashion), considered as a matrix with integer entries. Then $A(d,e)$ is a $\begin{bmatrix} n+1 \\ e \end{bmatrix}_q \times \begin{bmatrix} n+1 \\ d \end{bmatrix}_q$ matrix, all the entries of which are 0 or 1. By its p-rank, we mean the rank of $A(d,e)$ when considered as a matrix with entries in a field of characteristic p.

Before we can give the formula for the p-rank of $A(d,e)$ we must introduce some further notation. Let $m(n+1,r,p-1)$ be the number of monomials in $n+1$ variables of total degree r and with (partial) degree at most $p-1$ in each variable. This number is equal to the coefficient of x^r in $(1+x+\cdots+x^{p-1})^{n+1}$, or, more explicitly,

$$m(n+1,r,p-1) = \sum_{i=0}^{\lfloor \frac{r}{p} \rfloor} (-1)^i \binom{n+1}{i} \binom{n+r-ip}{n}. \tag{2}$$

Here $\lfloor y \rfloor$ stands for the integer part of the number y.

Let $\mathcal{H}$ denote the set of t-tuples $\mathbf{s} = (s_0, \ldots, s_{t-1})$ of integers satisfying (for $j = 0, \ldots, t-1$)

(1) $1 \le s_j \le n$;

(2) $0 \le ps_{j+1} - s_j \le (p-1)(n+1)$. (Subscripts mod t.)

We give $\mathcal{H}$ its natural partial order: $\mathbf{s}' \le \mathbf{s}$ if and only if $s'_j \le s_j$ for all j. For $1 \le r \le n$, we will also denote the tuple $(r, r, \ldots, r)$ by $(\underline{r})$.

Theorem 1. *The p-rank of $A(d,e)$ is given by the formula*

$$\operatorname{rank}_p A(d,e) = 1 + \sum_{\substack{\mathbf{s} \in \mathcal{H} \\ (\underline{e}) \le \mathbf{s} \le (\underline{n-d+1})}} \prod_{j=0}^{t-1} m(n+1, ps_{j+1} - s_j, p-1)$$

The well known case $d = 1$ of this theorem is due to N. Hamada [3]. (See also [1].)

We shall first make some brief comments about the statement, followed by an alternative statement of Theorem 1 (due to G. E. Moorhouse) using the "transfer matrix method" [7, 4.7, p. 241].

Remarks.

1. Note that when $d + e > n + 1$ the sum is zero, yielding a rank of 1 as expected.
2. We observe that if $\mathbf{s} = (s_0, \ldots, s_{t-1})$ satisfies $e \le s_j \le n-d+1$ for all j but does not belong to $\mathcal{H}$ then there is some j' for which $m(n+1, ps_{j'+1} - s_{j'}, p-1) = 0$. Therefore, in Theorem 1, one could as well sum over all tuples $\mathbf{s}$ with $e \le s_j \le n - d + 1$ instead of just those belonging to $\mathcal{H}$.
3. At first sight, the symmetry between d and e which is clear in the incidence relation may not appear to be reflected in the formula of Theorem 1. In fact there is a symmetry present in the formula, as we shall indicate briefly. For each choice

of d and e we shall associate a module for $\mathrm{GL}(V)$ with the matrix $A(e,d)$ in such way that the module for $A(e,d)$ is the dual (contragredient) module of the module for $A(d,e)$. Elementary properties of duality [2, Lemma 2.5] imply that the tuples correpsonding to the composition factors for $A(e,d)$ are obtained from those for $A(d,e)$ by replacing each entry s_j by $n-s_j+1$. This interchanges the roles of d and e in the outer sum of Theorem 1. Finally, since $m(n+1, ps_{j+1}-s_j, p-1) = m(n+1, (p-1)(n+1)-(ps_{j+1}-s_j), p-1)$ the inner sum is unchanged by replacing every s_j by $n-s_j+1$.

A generating function for Theorem 1. Eric Moorhouse has pointed out the following useful reformulation of Theorem 1 in a way which allows more rapid evaluation of $\operatorname{rank}_p A(d,e)$. Let $D = D(n,p,d,e)$ be the matrix with rows and columns indexed by $\{e, e+1, \ldots, n-d+1\}$ given by $D_{s,s'} = m(n+1, ps'-s, p-1)$. Then Theorem 1 can be rewritten as

$$\operatorname{rank}_p A(d,e) = 1 + \operatorname{trace} D^t = 1 + (\text{coefficient of } x^t \text{ in } \operatorname{trace}[(I-xD)^{-1}]) \quad (3)$$

This version of Theorem 1 is easily implemented in symbolic computational software. It also allows us to consider the asymptotic behaviour of $\operatorname{rank}_p A(d,e)$ with respect to t. The matrix D, which is independent of t, is easily seen to be a primitive matrix in the sense of the Perron-Frobenius Theorem, which tells us that D has a positive real eigenvalue λ with multiplicity one which has greater absolute value than all other eigenvalues of D. We conclude that $\operatorname{rank}_p A(d,e) \sim \lambda^t$ as $t \to \infty$.

Theorem 1 will be proved using the modular representation theory of $\mathrm{GL}(V)$ and in particular the description in terms of $\mathcal{H}$ of the submodule lattice of the permutation module on $\mathbb{P}(V)$ of V given in [2]. The connection between this result and the topic at hand is established in §2.1. There we show that the matrix $A(d,e)$ represents a homomorphism of permutation modules for $\mathrm{GL}(V)$ which can be factored through the permutation module on $\mathbb{P}(V)$, hence its image is isomorphic to a subquotient of this permutation module. Finally in §2.2 this subquotient is characterized in terms of the partially ordered set $\mathcal{H}$ (Theorem 2). By the results of [2], this description yields the compositon factors and their characters and, in particular, Theorem 1.

In §3, as an applicaton of Theorem 1, we explain how the special case $d+e = n+1$ yields improved bounds on the size of partial m-systems, defined in [5].

§2. Permutation modules for GL(V)

2.1. Incidence maps.

Let $F^{\mathcal{L}_i}$ denote the F-vector space with basis $\mathcal{L}_i$. Since $\mathrm{GL}(V)$ permutes the basis, the module $F^{\mathcal{L}_i}$ is an $F\,\mathrm{GL}(V)$-permutation module.

We next define the incidence maps α_i and β_i. Let $\alpha_i : F^{\mathcal{L}_i} \longrightarrow F^{\mathcal{L}_1}$ be the map sending an i-subspace to the (formal) sum of all 1-subspaces contained within it. Let $\beta_i : F^{\mathcal{L}_1} \longrightarrow F^{\mathcal{L}_i}$ be the map sending each 1-subspace to the (formal) sum of all i-subspaces which contain it. These are homomorphisms of $F\,\mathrm{GL}(V)$-modules since $\mathrm{GL}(V)$ preserves the incidence relations.

Let $\mathbf{1}_i \in F^{\mathcal{L}_i}$ denote the sum of all the elements of $\mathcal{L}_i$. We set

$$Y(i) = \{\sum_{w \in \mathcal{L}_i} a_w w \mid \sum_{w \in \mathcal{L}_i} a_w = 0\} \tag{4}$$

The following facts are direct consequences of the definitions and the fact that the cardinalities of the sets $\mathcal{L}_i$ are congruent to 1 modulo p.

Lemma 1.

(a) $F^{\mathcal{L}_i} = F\mathbf{1}_i \oplus Y(i)$ *as* F *GL*(V)*-modules*

(b) $\alpha_i(\mathbf{1}_i) = \mathbf{1}_1$ *and* $\beta_i(\mathbf{1}_1) = \mathbf{1}_i$.

(c) $\alpha_i(Y(i)) \subseteq Y(1)$ *and* $\beta_i(Y(1)) \subseteq Y(i)$. $\square$

The next lemma links the results of [2] with the matrix $A(d,e)$.

Lemma 2. *With respect to the bases* $\mathcal{L}_d$ *and* $\mathcal{L}_e$*, the matrix of the composite map* $\beta_e \circ \alpha_d$ *is* $A(d,e)$ *modulo* p*. In particular, the* p*-rank of* $A(d,e)$ *is equal to the dimension of the image of* $\beta_e \circ \alpha_d$.

Proof. Let $L \in \mathcal{L}_d$ and write

$$\beta_e(\alpha_d(L)) = \sum_{M \in \mathcal{L}_e} a_{L,M} M. \tag{5}$$

Then for a fixed $M \in \mathcal{L}_e$, we have the following congruences modulo p.

$$a_{L,M} \equiv |\{x \in \mathcal{L}_1 \mid x \subseteq L \cap M\}| \quad \equiv \begin{cases} 1 & \text{if } L \cap M \neq \{0\} \\ 0 & \text{if } L \cap M = \{0\} \end{cases}. \tag{6}$$

The lemma is proved. $\square$

2.2 Characterization of the image of the incidence map.

Lemma 1 (b) and (c) imply that the image of the incidence map $\beta_e \circ \alpha_d$ is the direct sum of $F\mathbf{1}_e$ and $\beta_e(\alpha_d(Y(d)))$ as $F\,\mathrm{GL}(V)$-modules. What matters to us is that $\beta_e(\alpha_d(Y(d)))$ is isomorphic to a subquotient of $Y(1)$, because the $F\,\mathrm{GL}(V)$-submodule structure of $Y(1)$ is well understood [2, Theorem A]. Here are the relevant facts. The $F\,\mathrm{GL}(V)$-composition factors are indexed by the set $\mathcal{H}$ and each composition factor $L(\mathbf{s})$, $\mathbf{s} \in \mathcal{H}$, appears just once in a composition series. It follows that the $F\,\mathrm{GL}(V)$-subquotients of $Y(1)$ are completely characterized by their composition factors. Therefore each subquotient determines and is determined by the subset of $\mathcal{H}$ which indexes its composition factors. By an *ideal* in a partially ordered set we mean a subset with the property that any element dominated by an element of that subset is itself a member of the subset; and by a *coideal* we mean an ideal of the opposite partial order. In these terms, [2, Theorem A] states that the

$F\,\mathrm{GL}(V)$- submodule lattice of $Y(1)$ is isomorphic to the lattice of ideals in $\mathcal{H}$ and in the dual sense the quotients of $Y(1)$ correspond to coideals in $\mathcal{H}$. Accordingly, a $F\,\mathrm{GL}(V)$-subquotient of $Y(1)$ determines and is determined by a subset of $\mathcal{H}$ which is the intersection of an ideal with a coideal. This is what we shall mean when we say that a subquotient of $Y(1)$ *corresponds* to a subset of $\mathcal{H}$.

The following lemma is our main tool.

Lemma 3. *Let* $1 \leq i \leq n$*.*

(a) *The* $F\,GL(V)$*-module* $\alpha_i(Y(i))$ *corresponds to the ideal* $\{\mathbf{s} \in \mathcal{H} \mid \mathbf{s} \leq (\underline{n-i+1})\}$*.*
(b) *The* $F\,GL(V)$*-module* $\beta_i(Y(1))$ *corresponds to the coideal* $\{\mathbf{s} \in \mathcal{H} \mid \mathbf{s} \geq (\underline{i})\}$*.*

Proof. Part (a) is the content of [2, 8.1]. To prove (b), we note that for each r the basis $\mathcal{L}_r$ is orthonormal for a non-singular $\mathrm{GL}(V)$-invariant symmetric bilinear form on $F^{\mathcal{L}_r}$. Using this form to identify each permutation module with its dual, we see that β_i is the dual map induced by α_i. It follows that the $\beta_i(Y(1))$ is $F\,\mathrm{GL}(V)$-isomorphic to the dual of $\alpha_i(Y(i))$. By [2, 2.5 Lemma (c)], the dual of the composition factor $L((\underline{n-i+1}))$ is $L((\underline{i}))$ and since duality reverses the partial ordering on $\mathcal{H}$, we have (b). $\square$

Setting $i = d$ in Lemma 3(a) and $i = e$ in Lemma 3(b) immediately yields the desired characterization of $\beta_e(\alpha_d(Y(d)))$.

Theorem 2. $\beta_e(\alpha_d(Y(d)))$ *corresponds to*

$$\{\mathbf{s} \in \mathcal{H} \mid \ (\underline{e}) \leq \mathbf{s} \leq (\underline{n-d+1})\}. \quad \square$$

We can now proceed to read off Theorem 1. By [2, 2.4, Corollary], the dimension of composition factor $L(\mathbf{s})$ is

$$\dim_F L(\mathbf{s}) = \prod_{j=0}^{t-1} m(n+1, ps_{j+1} - s_j, p-1). \tag{7}$$

In view of this, we see that Theorem 1 is immediate from Theorem 2.

§3. Applications to partial m-systems

We begin by stating the special case of Theorem 1 for intersecting subspaces of complementary dimensions. In this case, the submodule $\beta_e(\alpha_{n-e+1}(Y(n-e+1)))$ corresponds to the single tuple $(\underline{e})$.

Corollary 3. *The* p*-rank of* $A(n-e+1, e)$ *is given by the formula*

$$\operatorname{rank}_p A(n-e+1, e) = 1 + m(n+1, e(p-1), p-1)^t. \quad \square$$

Corollary 3 has the following application.

Corollary 4. *Suppose $\pi_1, \ldots, \pi_k$ is a set of e-subspaces of V and $\xi_1, \ldots, \xi_k$ is a set of $(n-e+1)$-subspaces of V such that $\pi_i \cap \xi_i \neq 0$ and $\pi_j \cap \xi_i = 0$ for all i, $j = 1, \ldots, k$ with $i \neq j$. Then*

$$k \leq \operatorname{rank}_p A(n-e+1, e) = 1 + m(n+1, e(p-1), p-1)^t. \tag{8}$$

Proof. These subspaces determine a $k \times k$ identity submatrix of $A(n-e+1, e)$, the rank of which is therefore an upper bound for k. □

Corollary 4 is an improvement of [6, Theorem 4] which, under the same hypothesis gives the bound

$$k \leq \binom{\binom{n+1}{e} + p - 2}{p-1}^t + 1. \tag{9}$$

The bound (9) is obtained by considering the e-dimensional vector subspaces of V as points in the projective space of $\wedge^e(V)$ under the Grassmann embedding and the $(n-e+1)$-subspaces as hyperplanes in this projective space. Under this embedding, the point corresponding to an e-subspace lies in the hyperplane corresponding to an $(n-e+1)$-subspace if and only if the two subspaces have a non-zero intersection. If H is the point-hyperplane incidence matrix of this projective space, then the points and hyperplanes corresponding to the subspaces in the hypothesis determine a $k \times k$ identity submatrix, so k is at most $\operatorname{rank} H$, which is the right hand side of (9). Since H involves all points and hyperplanes of $\mathbb{P}(\wedge^e(V))$, while $A(n-e+1, e)$ can be considered as the submatrix of H involving only those points and hyperplanes coming from e-subspaces and $(n-e+1)$-subspaces, it follows that the bound (8) is at least as good as (9). In fact it is strictly better except in the cases $e = 1$ or n, or $p = 2$, when the two bounds are equal.

In [6, Theorem 5] the bound (9) was applied to obtain upper bounds on the size of partial m-systems. The notion of an m-system, introduced in [5], is a generalization of the classical notions of ovoids and spreads. We refer to [5] for definitions and examples. Our new bound (8) can be used in place of (9) in the formula [6, Theorem 5(i)(5)], giving a new general bound on the size k of a partial m-system. (The parameter m is $e-1$ in our notation.) In [6], the authors go on to give stronger bounds for each of the finite classical polar spaces by making use of the special features of each case. We shall compare our bound with the strongest bounds in [6] for the various types of polar space when $e = 2$ and $p = 3$, which is [6], Example(b), p.236. The expression $m(n+1, e(p-1), p-1)$ in (8) reduces in this case to

$$m(n+1, 4, 2) = \binom{n+4}{n} - (n+1)^2.$$

So for each type of geometry, there will be no 1-system when $m(n+1, 4, 2)^t + 1$ is less than the defining bound [6, Theorem 1]. We see that the polar space P admits no 1-system in the following cases:

(i) $P = W_{2r+1}(q)$, with $r \geq 6$ {8};

(ii) $P = Q(2r, q)$, with $r \geq 8$ $\{9\}$;
(iii) $P = Q^+(2r+1, q)$, with $r \geq 8$ $\{9\}$;
(iv) $P = Q^-(2r+1, q)$, with $r \geq 6$ $\{8\}$;
(v) $P = H(2r, q)$ (t even), with $r \geq 7$ $\{8\}$;
(vi) $P = H(2r+1, q)$ (t even) , with $r \geq 7$ $\{9\}$.

The bounds given in [6] for the same examples are shown in braces.

We observe that our bound (8) was obtained without reference to special features of the different types of polar space. In order to obtain sharper bounds for particular polar spaces by our methods, one would have to consider the incidence relation for totally singular subspaces and the subspaces orthogonal to them rather than for arbitrary subspaces of complementary dimensions as we have done here, so the role of $\mathrm{GL}(V)$ would be played by the appropriate classical group.

A recent paper [4] obtains even stronger restrictions on the existence of m-systems in certain polar spaces, by studying related strongly regular graphs. For example, it is shown that in cases (i), (iv) and (v) above (without assuming that $p = 3$), no 1-system exists for $r \geq 4$.

Acknowledgements. This work grew out of a discussion with J. A. Thas at the Kansas State University conference in March 2001 in honor of E. Shult. An earlier discussion with S. P. Inamdar at the Indian Statistical Institute, Bangalore, was also helpful. I am indebted to Eric Moorhouse for his alternative statement of Theorem 1 and for several other helpful comments.

References

1. E. F. Assmus, Jr., J.D. Key, *Designs and Their Codes*, Tracts in Mathematics, Vol. 102, Cambridge University Press, Cambridge, England, 1992.
2. M. Bardoe, P. Sin, *The permutation module for $GL(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and ${\mathbb{F}_q}^{n+1}$*, J. London. Math. Soc. **61** (2000), 58-80.
3. N. Hamada, *The rank of the incidence matrix of points and d-flats in finite geometries*, J. Sci. Hiroshima Univ. Ser. A-I **32** (1968), 381-396.
4. N. Hamilton, R. Mathon, *Existence and non-existence of m-systems of polar spaces*, Europ. J. Combinatorics **22** (2001), 51-61.
5. E. E. Shult, J. A. Thas, *m-systems of polar spaces*, J. Combinatorial Theory Ser. A **68** (1994), 184-204.
6. E. E. Shult, J. A. Thas, *m-systems and partial m-systems of polar spaces*, Designs, Codes and Cryptography **8** (1996), 229-238.
7. R. P. Stanley, *Enumerative Combinatorics*, Studies in Advanced Mathematics, Vol. 49, Cambridge University Press, Cambridge, England, 1992.

Department of Mathematics, University of Florida, Gainesville, FL 32611, USA
e-mail: sin@math.ufl.edu