Europ. J. Combinatorics (1985) **6**, 183–187

Intersection Theorems for Vector Spaces

P. FRANKL AND R. L. GRAHAM

We prove that if b is an arbitrary positive integer, $\mathcal{F}=\{F_1,\dots,F_m\}$ is a collection of k-dimensional subspaces of an n-dimensional vector space over a finite field K, and there exist numbers $\mu_1,\dots,\mu_s$ such that $k\not\equiv\mu_t \pmod b$, $1\leq t\leq s$, but for all $1\leq i<j\leq m$, $\dim|F_i\cap F_j|\equiv\mu_t \pmod b$ for some t, then $|\mathcal{F}|\leq\begin{bmatrix}n\\s\end{bmatrix}_K$ holds.

1. INTRODUCTION

Let K be a finite field, $|K|=q$, and let V be an n-dimensional vector space over K. The number of t-dimensional subspaces of V is given by

$$\begin{bmatrix}n\\t\end{bmatrix}_q=\prod_{0\leq i<t}\frac{q^{n-i}-1}{q^{t-i}-1}.$$

Since we always refer to the same K, we will write this simply as $\begin{bmatrix}n\\t\end{bmatrix}$.

If A, B are subspaces of V, $A<B$, then B/A denotes the factor space of B by A. If $A\cap B=\langle 0\rangle$—the zero-space, then AB/A is the canonical projection of B into V/A. Suppose $1\leq k<n$ and $\mathcal{F}=\{F_1,\dots,F_m\}$ is a family of distinct k-dimensional subspaces of V. For $0\leq s\leq k$, let $\mathcal{F}^{(s)}$ be the collection of s-dimensional subspaces contained in some $F\in\mathcal{F}$.

Next we introduce the containment matrices $\mathbf{M}_{\mathcal{F}}(i,j)$. For $0\leq i\leq j\leq k$, let $\mathbf{M}_{\mathcal{F}}(i,j)$ denote the $|\mathcal{F}^{(i)}|\times|\mathcal{F}^{(j)}|$ matrix whose rows (columns) are indexed by the members of $\mathcal{F}^{(i)}(\mathcal{F}^{(j)})$, respectively, and where the entry in row U and column V is 1 if $U\subseteq V$ and 0 otherwise. When it causes no confusion we write simply $M(i,j)$ for $\mathbf{M}_{\mathcal{F}}(i,j)$; also $\mathbf{M}(i,\mathcal{F})$ will denote $\mathbf{M}_{\mathcal{F}}(i,k)$.

THEOREM 1.1. *Suppose $b,\mu_1,\dots,\mu_s$ are integers with $0\leq\mu_1<\cdots<\mu_s<b$ such that*

$$k\not\equiv\mu_t(\mathrm{mod}\ b),\qquad t=1,\dots,s,\tag{1.1}$$

and for all $1\leq i<j\leq m$,

$$\dim(F_i\cap F_j)\equiv\mu_t(\mathrm{mod}\ b)\quad\textit{for some } t.\tag{1.2}$$

Then $\mathbf{M}(s,\mathcal{F})$ has full (column) rank; in particular,

$$|\mathcal{F}|\leq|\mathcal{F}^{(s)}|\leq\begin{bmatrix}n\\s\end{bmatrix}.\tag{1.3}$$

holds except possibly for $q=2$, $b=6$, $s=3$ or 4.

THEOREM 1.2. *Suppose $\mathbf{M}(s,\mathcal{F})$ has full column rank. Then for all l such that $0\leq s\leq l<k$ we have*

$$|\mathcal{F}^{(l)}|\geq|\mathcal{F}|\frac{\begin{bmatrix}k+s\\l\end{bmatrix}}{\begin{bmatrix}k+s\\k\end{bmatrix}}.\tag{1.4}$$

0195-6698/85/020183+05 $02.00/0

The following proposition can be checked directly.

PROPOSITION 1.3. *For all $0 \leq i \leq j \leq k$ we have*

$$\mathbf{M}(i,j)\mathbf{M}(j,\mathscr{F}) = \begin{bmatrix} k-i \\ j-i \end{bmatrix} \mathbf{M}(i,\mathscr{F}), \tag{1.5}$$

$$\mathbf{M}(j,\mathscr{F})^{\mathrm{T}}\mathbf{M}(j,\mathscr{F}) = \left(\begin{bmatrix} \dim(F_r \cap F_s) \\ j \end{bmatrix} \right)_{1 \leq r,s \leq m} := \mathbf{N}_j.$$

COROLLARY 1.4. *The row space over the rationals of $\mathbf{M}(i,\mathscr{F})$ and of $\mathbf{N}_i$ is contained in the row space of $\mathbf{M}(j,\mathscr{F})$.*

Note also:

$$\operatorname{rank} \mathbf{M}(j,\mathscr{F}) \leq |\mathscr{F}^{(j)}| \leq \begin{bmatrix} n \\ j \end{bmatrix}. \tag{1.6}$$

REMARK 1.5. Theorems 1.1 and 1.2 are the vector space analogues of a theorem for subsets of a set of Frankl and Wilson [3], and Frankl and Füredi [4], respectively. Note, however, that in [3] b is required to be a prime.

For the proof of Theorem 1.1 we use the following old number-theoretical result. Recall that a Mersenne prime is a prime of the form $q = 2^d - 1$.

THEOREM 1.6 (Bang [1]). *If q and b are integers, $q \geq 2$, $b \geq 3$, and $(q,k) \neq (2,6)$ then $q^b - 1$ has a prime divisor p which does not divide $q^l - 1$ for $1 \leq l < b$. Also if $b = 2$, then the same holds unless q is a Mersenne prime.*

2. THE PROOF OF THEOREM 1.1

Since $\begin{bmatrix} x \\ i \end{bmatrix}$ is a polynomial of degree i in q^x for $0 \leq i \leq s$, every polynomial of degree s can be uniquely written as a linear combination of the $\begin{bmatrix} x \\ i \end{bmatrix}$. Take $p(x) = \prod_{1 \leq i \leq s} (q^{x-\mu_i} - 1)$ and write

$$p(x) = \sum_{0 \leq i \leq s} \alpha_i \begin{bmatrix} x \\ i \end{bmatrix} \tag{2.1}$$

where all α_i are rational.

Define the matrix $\mathbf{N} := \sum_{0 \leq i \leq s} \alpha_i \mathbf{N}_i$. Then $\mathbf{N}$ is an $m \times m$ matrix with general entry

$$n_{r,t} = \prod_{i=1}^{s} (q^{\dim(F_r \cap F_t) - \mu_i} - 1).$$

Suppose first $(q,b) \neq (2,6)$; moreover, if $b = 2$ then q is not a Mersenne prime. Let p be a prime dividing $q^b - 1$ but none of $q-1, q^2-1, \ldots, q^{b-1}-1$ (such p exists in view of Theorem 1.6). Then $n_{r,t}$ is divisible by p if and only if $r \neq t$. Hence $\det \mathbf{N} \not\equiv 0 \pmod{p}$.

In the case q, a Mersenne prime, $b = 2$, we must have $s = 1$, $p(x) = q^{x-\mu_1} - 1$. The off-diagonal entries of $\mathbf{N}$ are all divisible by 2^3 but $n_{r,r}$ is only divisible by 2. Hence $\det \mathbf{N} \not\equiv 0 \pmod{2^{m+1}}$.

In the case $q = 2$, $b = 6$ we distinguish the subcases $s = 1, 2, 5$:
if $s = 1$ then $n_{r,t}$ is divisible by 3^2 iff $r \neq t$;
if $s = 5$ then $n_{r,t}$ is divisible by 3^3 iff $r \neq t$;
if $s = 2$ then one can argue in the same way either with 3^2 or 7.

In all cases we proved that rank $\mathbf{N} = m$. Since the row space of $\mathbf{N}$ is contained in that of $\mathbf{M}(s, \mathcal{F})$, we infer that the latter has rank m, too. This proves the first part of the theorem. Now the second part follows from

$$\text{rank } \mathbf{M}(s, \mathcal{F}) \leq |\mathcal{F}^{(s)}| \leq \begin{bmatrix} n \\ s \end{bmatrix}.$$

3. The Proof of Theorem 1.2

First note that the statement is obvious for $l = s$, and thus for $k = 1$, as well. We apply induction on k. Suppose we know already that the statement of the Theorem holds for $k-1$. Choose an arbitrary one-dimensional subspace A from $\mathcal{F}^{(1)}$. Define

$$\mathcal{F}(A) = \{F/A: A \subseteq F \in \mathcal{F}\}.$$

Then $\mathcal{F}(A)$ is a family of $(k-1)$-dimensional subspaces of V/A.

Proposition 3.1. $\mathbf{M}(s, \mathcal{F}(A))$ *has full column rank.*

Proof. Suppose on the contrary that for some nonzero vector $\boldsymbol{\nu}$ of length $|\mathcal{F}(A)|$ we have

$$\mathbf{M}(s, \mathcal{F}(A))\boldsymbol{\nu}^{\mathrm{T}} = 0. \tag{3.1}$$

Let us denote by $\tilde{\mathbf{M}}$ the submatrix of $\mathbf{M}(s, \mathcal{F})$ spanned by the columns F, so that $A < F \in \mathcal{F}$. It will be enough to show that $\tilde{\mathbf{M}}\boldsymbol{\nu}^{\mathrm{T}} = 0$, i.e., the scalar product of $\boldsymbol{\nu}$ with each row of $\tilde{\mathbf{M}}$ is zero. Let us check this for an arbitrary row $\mathbf{r}_B$ corresponding to some s-dimensional subspace B.

(a) $A \not< B$. Then BA/A is an s-dimensional subspace of V/A and $B \subset F$ is equivalent to $BA/A \subseteq F/A$ for $F \in \mathcal{F}(A)$, i.e., the row corresponding to BA/A of $\mathbf{M}(s, \mathcal{F}(A))$ is the same as that of $\tilde{\mathbf{M}}$ corresponding to B.

(b) $A < B$. Now $BA/A = B/A$ is $(s-1)$-dimensional and $(\boldsymbol{\nu}, \mathbf{r}_B) = 0$ follows from

$$0 = \mathbf{M}(s-1, s)\mathbf{M}(s, \mathcal{F}(A)\boldsymbol{\nu}^{\mathrm{T}} = \begin{bmatrix} k-s+1 \\ k-s \end{bmatrix}\mathbf{M}(s-1, \mathcal{F}(A))\boldsymbol{\nu}^{\mathrm{T}},$$

i.e., $\mathbf{M}(s-1, \mathcal{F}(A))\boldsymbol{\nu}^{\mathrm{T}} = 0$.

Now we apply the induction hypothesis to $\mathcal{F}(A)$ and infer

$$|\mathcal{F}(A)^{(l-1)}| \geq |\mathcal{F}(A)| \frac{\begin{bmatrix} k-1+s \\ l-1 \end{bmatrix}}{\begin{bmatrix} k-1+s \\ k-1 \end{bmatrix}}. \tag{3.2}$$

Note that $B \to B/A$ gives a 1-1 correspondence between members of $\mathcal{F}^{(l)}$ containing A and members of $\mathcal{F}(A)^{(l-1)}$.

Summing up (3.2) for all $A < V$, dim $A = 1$, gives

$$\begin{bmatrix} l \\ 1 \end{bmatrix}|\mathcal{F}^{(l)}| \geq \begin{bmatrix} k \\ 1 \end{bmatrix}|\mathcal{F}| \frac{\begin{bmatrix} k+s-1 \\ l-1 \end{bmatrix}}{\begin{bmatrix} k+s-1 \\ k-1 \end{bmatrix}},$$

or equivalently,

$$|\mathcal{F}^{(l)}| \geq |\mathcal{F}| \frac{\begin{bmatrix} k \\ 1 \end{bmatrix}\begin{bmatrix} k+s-1 \\ l-1 \end{bmatrix}}{\begin{bmatrix} l \\ 1 \end{bmatrix}\begin{bmatrix} k+s-1 \\ k-1 \end{bmatrix}} = \frac{\begin{bmatrix} k+s \\ l \end{bmatrix}}{\begin{bmatrix} k+s \\ k \end{bmatrix}} |\mathcal{F}|.$$

REMARK 3.2. To see that Theorem 1.2 is best possible, take as $\mathcal{F}$ all the k-dimensional subspaces of a $(k+s)$-dimensional space. Actually one should prove that for this $\mathcal{F}$, $\mathbf{M}(s, \mathcal{F})$ has full column rank. However, for $F, F' \in \mathcal{F}$ we have $\dim(F \cap F') \geq \dim W - \dim F - \dim F' = k - s$. Thus, choosing $\mu = k - i$ for $i = 1, \ldots, s$ and $b > s$, $\mathcal{F}$ satisfies the hypothesis of Theorem 1.1. Hence $\mathbf{M}(s, \mathcal{F})$ has full column rank.

4. APPLICATIONS

In [3] the subset version of Theorem 1.1 was applied to give a constructive lower bound for the Ramsey number $R(k, k)$. Recall that $R(k, k)$ is the minimum number m such that for every graph on m vertices, either the graph or its complement contains a complete subgraph on k vertices. It is known (cf. [6]):

$$\frac{k2^{k/2}}{e2^{1/2}} \leq R(k, k) \leq \binom{2k-2}{k-1}.$$

However the lower bound is non-constructive. Apart from graphs constructed via set intersections no graphs are known to show that $R(k, k)$ is non-polynomial.

We give another such construction now. Suppose $k = b^2 - 1$, and let the vertex set of the graph $V(G)$ be the family of all k-dimensional subspaces of V. Let $F, F' \in V(G)$ form an edge if $\dim(F \cap F') \equiv -1 \pmod{b}$. Then $|V(G)| = [{}_{b^2}{}^n_1]$ while Theorem 1.1 implies that both the maximal complete and the maximal empty subgraph of G have at most $[{}_{b}{}^n_1]$ vertices.

5. CONCLUDING REMARKS

All our statements remain true with exactly the same proofs if we replace vector space by projective space and dimension by rank.

Actually the argument giving Theorem 1.1 works in the following more general setting: Suppose we have a finite modular lattice L which satisfies the following conditions:

(a) For $A, B \in L$, $A < B$, rank $A = i$, rank $B = j$ and $i \leq l \leq j$, the number of elements $C \in L$ with $A < C < B$, rank $C = l$, depends only on (i, l, j).

(b) For every $0 \leq i \leq s$, there exists a polynomial of degree i, $p_i(x)$ such that for every $A \in L$ with rank $A \leq k$, the number of elements $C \in L$, $C < A$, rank $C = i$, is given by p_i (rank A).

The first intersection theorem for vector spaces was proved by Hsieh.

THEOREM [8]. *Suppose $\mathcal{F}$ is a family of k-dimensional subspaces of V satisfying* $\dim(F \cap F') \geq t$ *for all $F, F' \in \mathcal{F}$. Then*

$$|\mathcal{F}| \leq \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q \quad \text{holds if } n \geq 2k+1 \qquad (t = 1 \text{ or } q \geq 3) \tag{5.1}$$

$$\text{and if } n \geq 2k+2 \qquad (t \geq 2, q = 2).$$

The corresponding statement for subsets of a set is the Erdös-Ko-Rado theorem [2]. Katona [9] gave a simple proof of it in the case $t=1$. His proof was modified by Greene and Kleitman [7] to show that (5.1) is true for $t=1$, $n=2k$ as well. Most recently Frankl and Wilson proved that (5.1) holds for arbitrary t iff $n \geq 2k$.

Recently, solving a conjecture of Erdös, Frankl and Füredi [5] proved that if $k \geq 2l+2$, $n > n_0(k)$, $\mathcal{F}$ is a family of k-element subsets of an n-set with $|A \cap A'| \neq l$ for all $A, A' \in \mathcal{F}$, then $|\mathcal{F}| \leq \binom{n-l-1}{k-l-1}$ holds. This motivates

CONJECTURE 5.2. *Suppose $\mathcal{F}$ is a family of k-dimensional subspaces of V satisfying $\dim(F \cap F') \neq l$ for all $F, F' \in \mathcal{F}$. If $k \geq 2l+2$ and $n > n_0(k)$ then we have*

$$|\mathcal{F}| \leq \begin{bmatrix} n-l-1 \\ k-l-1 \end{bmatrix}.$$

Note that Theorem 1.1 yields $|\mathcal{F}| \leq \begin{bmatrix} n \\ k-l-1 \end{bmatrix}$. For $k \leq 2l+1$ we can prove

$$|\mathcal{F}| \leq \begin{bmatrix} n \\ l \end{bmatrix} \frac{\begin{bmatrix} 2k+1-l \\ k \end{bmatrix}}{\begin{bmatrix} 2k+1-l \\ l \end{bmatrix}}$$

and this is best possible up to a factor of $1+o(1)$ for fixed k, l and n tending to infinity. We shall return to these and similar problems in a subsequent paper.

ACKNOWLEDGEMENT

The authors are indebted to Z. Füredi for pointing out an error in the original proof of Theorem 1.1 and for calling their attention to the result of Bang (Theorem 1.6).

REFERENCES

1. A. S. Bang, Talteoritiske Undersogelser, *Tideskrift for Mat.* (5) **4** (1886), 130-137.
2. P. Erdös, C. Ko and R. Rado, Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford* **12** (1961), 313-320.
3. P. Frankl and R. M. Wilson, Intersection theorems with geometric consequences. *Combinatorica* **1** (1981), 357-368.
4. P. Frankl and Z. Füredi, On hypergraphs without two edges intersecting in a given number of vertices, *J. Combin. Theory, Ser. A* **36** (1984), 230-236.
5. P. Frankl and Z. Füredi, Forbidding just one intersection, *J. Combin. Theory, Ser. A* **39** (1985), 160-176.
6. R. L. Graham, B. L. Rothschild and J. H. Spencer, *Ramsey Theory*, John Wiley, New York, 1980.
7. C. Greene and D. J. Kleitman, Proof techniques in the theory of finite sets, *MAA Studies in Mathematics* **17** (1978), 22-79.
8. W. N. Hsieh, Intersection theorems for systems of finite vector spaces, *Discrete Math.* **12** (1975), 1-16.
9. G. O. H. Katona, A simple proof of the Erdös-Ko-Rado theorem, *J. Combin. Theory, Ser. B* **13** (1972), 183-184.

Received 19 March 1984 and in revised form 15 May 1984

P. FRANKL
C.N.R.S. E.R. 175 'Combinatoire', C.M.S., 54, Boulevard Raspoil, 75270 Paris, Cedex 06, France
and

R. L. GRAHAM
AT&T Bell Laboratories, Murray Hill, N.J., U.S.A.