COMBINATORICA 3 (2) (1983) 193—199

AN EXTREMAL SET THEORETICAL CHARACTERIZATION OF SOME STEINER SYSTEMS

PETER FRANKL

Received 20 December 1982

Let n, k, t be integers, $n>k>t\geqq 0$, and let $m(n, k, t)$ denote the maximum number of sets, in a family of k-subsets of an n-set, no two of which intersect in exactly t elements. The problem of determining $m(n, k, t)$ was raised by Erdős in 1975. In the present paper we prove that if $k\geqq 2t+1$ and $k-t$ is a prime, then $m(n, k, t)\leqq \binom{n}{t}\binom{2k-t-1}{k}\Big/\binom{2k-t-1}{t}$. Moreover, equality holds if and only if an $(n, 2k-t-1, t)$-Steiner system exists. The proof uses a linear algebraic approach.

1. Introduction

Let X be a finite set of cardinality n. For $0<k\leqq n$, let $\binom{X}{k}$ denote the collection of all k-subsets of X. A family $\mathcal{F}$ of k-subsets of X i.e. $\mathcal{F}\subseteqq\binom{X}{k}$, is called *t-avoiding* $(0\leqq t<k)$ if the cardinality of the intersection of any two members of $\mathcal{F}$ is different from t. An easy way to construct t-avoiding families is the following: take an arbitrary $(t+1)$-element subset, T of X and let $\mathcal{F}$ consist of all the supersets of T. This gives $\binom{n-t-1}{k-t-1}$ sets. Erdős [1] conjectured that for $k>2t+1$ this is best possible.

Conjecture 1.1. (Erdős) *For* $k>2t+1$ *and* $n>n_0(k, t)$ *we have*

$$m(n, k, t) = \binom{n-t-1}{k-t-1}. \tag{1}$$

For $t=0$ the Erdős—Ko—Rado theorem [2] shows that the conjecture is valid. The same was proved for $t=1$ in [3]. The asymptotic validity, i.e. $m(n, k, t)\leqq (1+o(1))\binom{n-t-1}{k-t-1}$ was established in [4] if $k\geqq 3t+2$ and in [6] if $k-t$ is a prime power.

AMS subject classification (1980): 05 C 65; 05 B 05

From now on suppose $k \leqq 2t+1$. We first describe another construction for t-avoiding families. We need two definitions.

Definition 1.2. Let s be an integer, $s \geqq t$, and let $\mathcal{S} \subset \binom{X}{s}$ be a family. If every $T \in \binom{X}{t}$ is contained in at most one member of $\mathcal{S}$, then $\mathcal{S}$ is called an (n, s, t) *partial Steiner system* or shortly a $\mathrm{PS}(n, s, t)$. (Of course, the condition is equivalent to $|S \cap S'| < t$ for every $S, S' \in \mathcal{S}$.)

Definition 1.3. A $\mathrm{PS}(n, s, t)$ in which every $T \in \binom{X}{t}$ is contained in exactly one member of $\mathcal{S}$ is called an (n, s, t) *Steiner system* or shortly an $\mathrm{S}(n, s, t)$. (Then, of course, $|\mathcal{S}| = \binom{n}{t} \Big/ \binom{s}{t}$ holds.)

For a family of sets $\mathcal{A}$ and a positive integer h let us define $\mathcal{A}^h$, the *h'th shadow* of $\mathcal{A}$ by

$$\mathcal{A}^h = \{H : |H| = h, \text{ there exists } A \in \mathcal{A} \text{ such that } H \subseteqq A \text{ holds}\}.$$

Proposition 1.4. *If $\mathcal{S}$ is a $\mathrm{PS}(n, 2k-t-1, t)$ then $\mathcal{S}^k$ is t-avoiding.*

Proof. Take two arbitrary sets from $\mathcal{S}^k$: F, F'. Let $S, S' \in \mathcal{S}$ satisfy $F \subset S$, $F' \subset S'$. We have to show $|F \cap F'| \neq t$. If $S \neq S'$, then it follows from $|F \cap F'| \leqq \leqq |S \cap S'| < t$. If $S = S'$ then we have

$$|F \cap F| = |F| + |F'| - |F \cup F'| \geqq 2k - |S| = t+1. \quad \blacksquare$$

No Steiner system is known to exist for $t \geqq 7$ but we are helped by

Theorem 1.5. (Rödl [7]) *For fixed s, t and an arbitrary positive ε if $n > n_0(s, t, \varepsilon)$ then there exists a $\mathrm{PS}(n, s, t)$, $\mathcal{S}$ satisfying*

$$|\mathcal{S}| > (1-\varepsilon)\binom{n}{t} \Big/ \binom{s}{t}. \tag{2}$$

Corollary 1.6. *For fixed k and t we have*

$$m(n, k, t) \geqq (1 - o(1))\binom{n}{t}\binom{2k-t-1}{k} \Big/ \binom{2k-t-1}{t}. \tag{3}$$

In this paper we prove:

Theorem 1.7. *Suppose $k \leqq 2t+1$ and $k-t$ is a prime. Then*

$$m(n, k, t) \leqq \binom{n}{t}\binom{2k-t-1}{k} \Big/ \binom{2k-t-1}{t}, \tag{4}$$

and equality holds if and only if there exists an $\mathrm{S}(n, 2k-t-1, t)$.

Conjecture 1.8. The statement of Theorem 1.7. remains valid even if we drop the condition "$k-t$ is a prime".

Remark 1.9. The inequality of Theorem 1.7. was proved to be valid for $k-t$ a prime power in [6].

Suppose $\mathcal{F}=\{F_1, ..., F_m\}\subset\binom{X}{k}$ and $\mathcal{F}^h=\{G_1, ..., G_b\}$. Define a b by m matrix $M^h(\mathcal{F})$ by $m_{ij}=1$, if $G_i\subset F_j$ and $m_{ij}=0$, otherwise. Then $M^h(\mathcal{F})$ is called the h'th *containment matrix* of $\mathcal{F}$.

Our main tool in proving Theorem 1.7. is the following:

Theorem 1.10. (Frankl, Füredi [5]) *Suppose* $n>k>g\geqq h$, $\mathcal{F}\subseteqq\binom{X}{k}$, *and the columns of* $M^h(\mathcal{F})$ *are linearly independent over the rationals. Then*

$$|\mathcal{F}^g|/\binom{k+h}{g} \geqq |\mathcal{F}|/\binom{k+h}{h}. \tag{5}$$

2. The proof of Theorem 1.7 in case $k=2t+1$

Let us write $k-t=p$. Then $t=p-1$ and $k=2p-1$ holds. We prove a somewhat stronger statement:

Theorem 2.1. *Suppose* $\mathcal{F}\subseteqq\binom{X}{2p-1}$, *and* $\mathcal{F}$ *is* $(p-1)$*-avoiding. Then the columns of* $M^{p-1}(\mathcal{F})$ *are linearly independent over* GF(p) *(and consequently over the rationals), in particular*

$$|\mathcal{F}| \leqq |\mathcal{F}^{p-1}| \leqq \binom{n}{p-1}. \tag{6}$$

Moreover $|\mathcal{F}|=|\mathcal{F}^{p-1}|$ *holds if and only if for some* PS$(n, 3p-2, p-1)$, $\mathcal{S}$ *we have* $\mathcal{F}=\mathcal{S}^{2p-1}$.

Proof. Let us set $M=M^{p-1}(\mathcal{F})$ and let us consider $N=M^*M$ (M^* is the transposed of M). Then N is an m by m matrix with general entry n_{ij} equal to the scalar product of the i'th and j'th column of M. Since the columns are (0, 1)-vectors, this scalar product is just the number of $(p-1)$-subsets in the intersection $F_i\cap F_j$, i.e. $\binom{|F_i\cap F_j|}{p-1}$. Thus the diagonal entries of N are equal to $\binom{2p-1}{p-1}\equiv 1 \pmod p$. Since $\mathcal{F}$ is $(p-1)$-avoiding the off-diagonal entries are all from 0, $\binom{p}{p-1}, ..., \binom{2p-2}{p-1}$. These numbers are all congruent to 0 modulo p. Thus over GF(p) N is the m by m identity matrix. I_m Hence, rank $M=$ rank $N=m$ holds, proving the first statement of the theorem.

From now on assume $m=b$. Then M is a square-matrix. Since $M^*M\equiv I_m \pmod p$, $MM^*\equiv I_m \pmod p$ holds as well. Let us translate this identity to the language of sets. The general entry a_{ij} of MM^* is just the number of sets in $\mathcal{F}$ which contain $G_i\cup G_j$. Thus for $i\neq j$ this number is always divisible by p. In particular, if it is non-zero then it is at least p. This yields the following proposition.

Proposition 2.2. *Suppose* $A\in\mathcal{F}^{2p-2}$. *Then there are at least p members of* $\mathcal{F}$ *which contain* A. ∎

Next we prove that we must have equality. In fact Theorem 1.10. implies:

$$|\mathscr{F}^{2p-2}| \geqq |\mathscr{F}|\binom{3p-2}{2p-2}\Big/\binom{3p-2}{2p-1} = |\mathscr{F}|(2p-1)/p. \tag{7}$$

Denoting by e the number of pairs (A, F) with $A\subset F\in\mathscr{F}$, $|A|=2p-2$, we obviously have $e=(2p-1)|\mathscr{F}|$. Using (7) we obtain

$$e \leqq p|\mathscr{F}^{2p-2}|. \tag{8}$$

Now (8) tells that on the average every $A\in\mathscr{F}^{2p-2}$ is contained in at most p members of $\mathscr{F}$. Comparing this with Proposition 2.2. we infer that we must have always equality. This gives the case $s=2p-2$ of the following lemma.

Lemma 2.3. *Suppose s is an integer, $p-1\leqq s\leqq 2p-2$, and $A\in\mathscr{F}^s$. Then there is a set* $P=P(A)\in\binom{X}{3p-2-s}$ such that

$$\left\{G\in\binom{X-A}{2p-1-s}: (A\cup G)\in\mathscr{F}\right\} = \binom{P}{2p-1-s}.$$

Proof of the lemma. We apply induction on $2p-2-s$. We have already settled the case $s=2p-2$. Suppose $s<2p-2$ and the statement of the lemma is verified for $s+1$. Since $A\in\mathscr{F}^s$ we may choose A', F such that $A\subset A'\subset F\in\mathscr{F}$, and $|A'|=s+1$ holds. Let us write $(A'-A)\cup P(A')=\{y_1, \dots, y_{3p-2-s}\}$.

As a next step we prove:

Proposition 2.4. *Either the lemma holds for A with $P(A)=\{y_1, \dots, y_{3p-2-s}\}$ or A is contained in more than $\binom{3p-2-s}{2p-1-s}$ sets in $\mathscr{F}$.*

Proof. We apply the inductional hypothesis to $A_i=A\cup\{y_i\}$, $1\leqq i\leqq 3p-2-s$, and obtain sets $P_i\in\binom{X-A_i}{(3p-2-(s+1))}$ such that for every $G\in\binom{P_i}{2p-2-s}$ we have $A\subset(A_i\cup G)\in\mathscr{F}$. Counted with multiplicity this would give us $(3p-2-s)\binom{3p-3-s}{2p-2-s}$ sets $F\in\mathscr{F}$, containing A. Each particular F is counted exactly $|(F-A)\cap\{y_1, \dots, y_{3p-2-s}\}|$ times. Thus at most $(2p-1-s)$-times. Thus there are at least $\frac{3p-2-s}{2p-1-s}\binom{3p-3-s}{2p-2-s}=\binom{3p-2-s}{2p-1-s}$ such sets. Moreover, in order to have equality it is necessary that $(F-A)\subset\{y_1, \dots, y_{3p-2-s}\}$ holds for every F satisfying $A\subset F\in\mathscr{F}$. We conclude $P_i=\{y_1, \dots, y_{3p-2-s}\}-\{y_i\}$, and that the lemma holds with $P(A)=\{y_1, \dots, y_{3p-2-s}\}$. ∎

We go on with the proof of the lemma. By Theorem 1.10. we have:

$$|\mathscr{F}^s| \geqq |\mathscr{F}|\binom{3p-2}{s}\Big/\binom{3p-2}{2p-1} = |\mathscr{F}|\binom{2p-1}{s}\Big/\binom{3p-2-s}{2p-1-s}, \tag{9}$$ or, equivalently,

$$|\mathscr{F}^s|\binom{3p-2-s}{2p-1-s} \geqq |\mathscr{F}|\binom{2p-1}{s}.$$

Counting again the number of pairs (A, F) satisfying $A\subset F\in\mathcal{F}$, $|A|=s$, in two different ways, using Proposition 2.4, we obtain:

$$|\mathcal{F}^s|\binom{3p-2-s}{2p-1-s} \leqq |\mathcal{F}|\binom{2p-1}{s}. \tag{10}$$

Comparing (9) and (10) we infer that equality must hold in both cases and consequently in Proposition 2.4 always the first case appears, finishing the proof of the lemma. ▮▮

Now we continue the proof of Theorem 2.1. Let us define $\mathcal{S}=\{A\cup P(A)\colon A\in\mathcal{F}^{p-1}\}$. We consider $\mathcal{S}$ as a subset of $\binom{X}{3p-2}$, i.e. taking each $(3p-2)$-set only once. By definition $\mathcal{F}\subseteq\mathcal{S}^{2p-1}$ holds. We want to prove that $\mathcal{S}$ is a $\mathrm{PS}(n, 3p-2, p-1)$ i.e. for $S\neq S'\in\mathcal{S}$ we have $|S\cap S'|<p-1$. Suppose the contrary that is $p-1\leqq|S\cap S'|$, but $|S\cup S'|>3p-2$. Let $A, A'\in\mathcal{F}^{p-1}$ be such that $S=A\cup P(A)$ and $S'=A'\cup P(A')$ hold. It is easy to see that one can find a p-element set $B\subset(S-A)$ satisfying $p-1\leqq|(A\cup B)\cap S'|<|(A\cup B)|=2p-1$. Once B chosen take a p-subset, B' of $S'-A'$ such that $|(A\cup B)|\cap|(A'\cup B')|=p-1$. This is possible because $p-1\leqq|(A\cup B)\cap S'|\leqq 2p-2$. But $A\cup B$ and $A'\cup B'$ are both in $\mathcal{F}$, contradicting to the fact that $\mathcal{F}$ is $(p-1)$-avoiding. Thus $\mathcal{F}$ is a $\mathrm{PS}(n, 3p-2, p-1)$.

If C is a $(p-1)$-subset of $(A\cup P(A))\in\mathcal{S}$, $A\in\mathcal{F}^{p-1}$, then we can choose a p-subset B of $P(A)$ such that $C\subset(A\cup B)$, and consequently $C\in\mathcal{F}^{p-1}$ holds. Thus we have $|\mathcal{F}^{p-1}=\mathcal{S}^{p-1}|=\binom{3p-2}{p-1}|\mathcal{S}|$. $\mathcal{F}\subseteq\mathcal{S}^{2p-1}$ implies $|\mathcal{F}|\leqq\binom{3p-2}{2p-1}|\mathcal{S}|$. Using $|\mathcal{F}|=|\mathcal{F}^{p-1}|$ we infer $\mathcal{F}=\mathcal{S}^{2p-1}$. ▮▮▮

Now we deduce the case $k=2t+1$ of Theorem 1.7. from Theorem 2.1. In view of (6) we have $m(n, 2t+1, t)\leqq\binom{n}{t}$. Suppose that for the t-avoiding family $\mathcal{F}\subseteq\binom{X}{2t+1}$ equality holds. Then (6) implies $\mathcal{F}^t=\binom{X}{t}$, and by the second part of Theorem 2.1, for some $\mathrm{PS}(n, 3t+1, t)$, $\mathcal{S}$ we have $\mathcal{F}=\mathcal{S}^{2t+1}$. Since $\mathcal{F}^t=\binom{X}{t}$, every t-subset of X is contained in some $S\in\mathcal{S}$, i.e. $\mathcal{S}$ is an $S(n, 2t+1, t)$, as desired.

3. Proof of Theorem 1.7 in the general case

Let us set $2t+1-k=d$ and suppose d is positive. Let further $\mathcal{F}$ be a t-avoiding family of k-subsets of X. For $D\in\binom{X}{d}$ let us define

$$\mathcal{F}_D = \{F-D\colon D\subset F\in\mathcal{F}\}.$$

Then $\mathcal{F}_D$ is a $(t-d)$-avoiding family of $(2(t-d)+1)$-subsets of $X-D$. Thus we may apply the already settled case of Theorem 1.7 to $\mathcal{F}_D$, and obtain

$$|\mathcal{F}_D| \leqq \binom{n-d}{t-d}. \tag{11}$$

Counting in two different ways the number of pairs (D, F) satisfying $D\subset F\in\mathscr{F}$, $D\in\binom{X}{d}$ we infer:

(12)
$$\sum_{D\in\binom{X}{d}}|\mathscr{F}_D|=\binom{k}{d}|\mathscr{F}|.$$

Combining (11) and (12) we get $(d=2t+1-k)$:

(13)
$$|\mathscr{F}|\leqq\frac{\binom{n+k-2t-1}{k-t-1}\binom{n}{2t+1-k}}{\binom{k}{2t+1-k}}=\frac{n!\,(2k-2t-1)\,!}{(n-t)!\,(k-t-1)!\,k!}=\frac{\binom{n}{t}\binom{2k-t-1}{k}}{\binom{2k-t-1}{t}},$$

proving inequality (4).

Assume that equality holds in (13). Then equality must hold in (11) for every $D\in\binom{X}{d}$. By the already proved case of Theorem 1.7 for every $D\in\binom{X}{d}$ there exists $\mathscr{S}_D$, an $S(n-d, 2k-t-1-d, t-d)$ such that $\mathscr{F}_D=\mathscr{S}_D^{k-d}$ holds. Note that $t-d=k-t-1$ is non-negative and it is positive unless $k=t+1$. However, for $k=t+1$ every t-avoiding family is a $\mathrm{PS}(n, k, t)$ thus the second statement of Theorem 1.7 just coincides with the definition of an $S(n, k, k-1)$. Thus we may assume $d\leqq t-1$ and proceed with the proof of the theorem. Let us define $\mathscr{S}=\{D\cup S_D\colon D\in\binom{X}{d}$, $S_D\in\mathscr{S}_D$. Obviously, $\mathscr{F}\subseteqq\mathscr{S}^k$ holds.

If $T\in\binom{X}{t}$ then we can choose a $D\in\binom{T}{d}$ and an $S_D\in\mathscr{S}_D$ such that $(T-D)\subset\subset S_D$. Consequently $T\subset(D\cup S_D)\in\mathscr{S}$ holds, showing that every t-subset of X is contained in at least one member of $\mathscr{S}$.

Suppose $S\in\mathscr{S}$, i.e. for some $D\in\binom{X}{d}$ and $S_D\in\mathscr{S}_D$ we have $S=D\cup S_D$. Let D' be an arbitrary d-subset of S satisfying $|D\cap D'|=d-1$. Let F be an arbitrary k-subset of S satisfying $(D\cup D')\subseteqq F$. Let further $S_{D'}$ be the unique member of $\mathscr{S}_{D'}$ which contains $F-D'$. We want to show

Proposition 3.1. $D\cup S_D=D'\cup S_{D'}$.

Proof. Let us argue indirectly and take some element $x\in((D\cup S_D)-(D'\cup S_{D'}))$. Let further y be an arbitrary element of $F-(D\cup D')$. Then $(F-\{y\}\cup\{x\})\in\mathscr{F}$. Thus there is a unique set $R_{D'}\in\mathscr{S}_{D'}$ satisfying $(F'-D')\in\mathscr{S}_{D'}$. However, $((F-D')\cap\cap(F'-D'))\subseteqq(S_{D'}\cap R_{D'})$, i.e. this latter intersection has size at least $k-d-1\geqq\geqq t-d$. Since $\mathscr{S}_{D'}$ is an $S(n-d, 2k-t-1-d, t-d)$ $S_{D'}$ and $R_{D'}$ must coincide, contradicting $x\in(R_{D'}-S_{D'})$. ∎

Since equality is transitive and for every $D''\in\binom{D\cup S_D}{d}$ we can find a chain $D=D_0, \ldots, D_r=D''$ such that $|D_i\cap D_{i+1}|=d-1$ for $i=0, \ldots, r-1$, and all the D_i are d-subsets of $D\cup S_D$; we infer that Proposition 3.1 holds for all d-subsets of

$D \cup S_D$. Consequently, we obtain every $S \in \mathcal{S}$ exactly $\binom{|S|}{d} = \binom{2k-t-1}{d}$ times, yielding:

$$|\mathcal{S}| = \binom{n}{d} |\mathcal{S}_D| \Big/ \binom{2k-t-1}{d} = \binom{n}{t} \Big/ \binom{2k-t-1}{t}.$$

This equality and the fact that every t-subset of X is contained in at least one member of $\mathcal{S}$ imply that $\mathcal{S}$ is an $S(n, 2k-t-1, t)$. Since $|\mathcal{F}| = \binom{2k-t-1}{k} |\mathcal{S}|$, it follows that $\mathcal{F} = \mathcal{S}^k$, concluding the proof of Theorem 1.7.

Added in proof. Recently Z. Füredi and the author proved Conjecture 1.1.

References

[1] P. ERDŐS, Problems and results in graph theory and combinatorial analysis, *Proc. Fifth British Comb. Conf. 1975 Aberdeen, Congressus Numerantium, 15 — Utilitas Math.*, Winnipeg, 1976.
[2] P. ERDŐS, C. KO and R. RADO, Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford (2)*, **12** (1961), 313—320.
[3] P. FRANKL, On families of finite sets no two of which intersect in a singleton, *Bull. Austral. Math. Soc.* **17** (1977), 125—134.
[4] P. FRANKL, Extremal problems and coverings of the space, *European J. Comb.* **1** (1980), 101—106.
[5] P. FRANKL and Z. FÜREDI, On families of finite sets no two of which intersect in a given number of elements, *J. Comb. Th. (A)*, to appear.
[6] P. FRANKL and R. M. WILSON, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357—368.
[7] V. RÖDL, Almost Steiner systems always exist, to appear.

Peter Frankl

Centre National de la Recherche Scientifique
15 Quai Anatole France, 75007 Paris, France