Europ. J. Combinatorics (1989) **10**, 149–160

Intersecting Families of Finite Sets and Fixed-point-Free 2-Elements

P. J. CAMERON, P. FRANKL AND W. M. KANTOR

We study the maximum cardinality of a pairwise-intersecting family of subsets of an n-set, or the size of the smallest set in such a family, under either of the assumptions that it is regular (as a hypergraph) or that it admits a transitive permutation group. Not surprisingly, results under the second assumption are stronger. We also give some results for 4-wise intersecting families under the same assumptions.

1. Introduction and Statement of Results

There is a large collection of results in extremal set theory, concerning families $\mathscr{F}$ of subsets of an n-element set X: typically, these are bounds on the cardinality of $\mathscr{F}$, and characterisations of families attaining the bounds, subject to assumptions about cardinalities of intersections, closure conditions, or exclusion of solutions of various relations such as $F_1 \subseteq F_2$.

In many cases, it is interesting to ask for similar results under a global hypothesis on $\mathscr{F}$. We consider two such hypotheses. We say that $\mathscr{F}$ is *regular* if the number of members of $\mathscr{F}$ containing an element x is a constant (called the *degree* of $\mathscr{F}$); and $\mathscr{F}$ is *transitive* if it is invariant under a transitive group of permutations of X. Obviously, transitivity implies regularity, but not conversely.

Our main concern is with *intersecting families* (containing no two disjoint sets). It is trivial that the cardinality of an intersecting family is at most 2^{n-1}. This bound is realised, for any n, by the (non-regular) family consisting of all sets containing a fixed $x \in X$. However, there are many other families attaining the bound. (We give a general construction in section 2.) If n is odd, the family of sets of cardinality greater than $\frac{1}{2}n$ is intersecting and has cardinality 2^{n-1}, and is transitive (it admits the symmetric group S_n). However, for n even, there may be a regular family but no transitive one of size 2^{n-1} (this holds for $n = 12$), or there may be no regular family of this size (this holds for $n = 4$). We investigate the set

$$A = \{n \in \mathbb{N}: \text{there is a transitive intersecting family } \mathscr{F} \text{ of subsets of an } n\text{-set, with } |\mathscr{F}| = 2^{n-1}\}.$$

It was shown by Isbell [10] that

$$A = \{n \in \mathbb{N}: \text{there is a transitive permutation group of degree } n \text{ containing no fixed-point-free 2-element}\}.$$

The main results on this set are summarised in Theorems 1 and 2.

THEOREM 1. (*i*) $2^a \notin A$ *for all* $a \geqslant 1$.
(*ii*) $3 \cdot 2^a \notin A$ *for all* $a \geqslant 2$.

THEOREM 2. (*i*) *A is multiplicatively closed.*
(*ii*) *A contains all odd numbers.*
(*iii*) *If b is odd and* $b > 1$, *then* $2b \in A$.
(*iv*) *if b is odd and* $b > 3$, *then* $4b \in A$.
(*v*) *A has density* 1.

0195-6698/89/020149+12 $02.00/0

The pioneering work on this question was done by Isbell in the 1960s. He conjectured [10] the existence of a function m such that, if b is odd and $a \geqslant m(b)$, then $2^a \cdot b \notin A$. He claimed to have proved this statement in [11], but the proof is incorrect, and the question is still open. In this direction, Theorem 1(i) is straightforward, and (ii) is established in [4]. However, the obvious conjecture, that $2^a \cdot b \notin A$ if b is odd and $2^a > b$, is false: Peter Neumann (personal communication) showed that $56 \in A$, and his construction easily extends to give two infinite families of examples. We give a variety of constructions in section 4.

We also give lower bounds for the size of a set in such a family.

THEOREM 3. *Let $\mathcal{F}$ be an intersecting family of size 2^{n-1} and $F \in \mathcal{F}$.*
(i) If $\mathcal{F}$ is transitive, then $|F| \geqslant n^{1/2}$.
(ii) If $\mathcal{F}$ is regular, then $|F| \geqslant \frac{1}{2}\log_2(\pi n/2)$.

The first inequality is essentially best possible; but we have no examples remotely near the second.

We also investigate the function $f(n)$ defined by

$$2^{n-1} - f(n) = \max\{|\mathcal{F}|: \mathcal{F} \text{ is a transitive intersecting family of subsets of an } n\text{-set}\}.$$

(Another interpretation of $f(n)$ will be given later.) Clearly $f(n) = 0$ iff $n \in A$; we evaluate $f(n)$ in some other cases:

THEOREM 4. *(i) $f(2^a) = \Sigma_{i=0}^{a-1} 2^{2^i}$ for $a \geqslant 1$.*
(ii) $f(12) = 48$.

We also consider t-wise intersecting families with $t > 2$, that is, families in which any t sets have non-empty intersection. The family of all sets containing x is t-wise intersecting for all t and has cardinality 2^{n-1}. But with our global assumptions, 4-wise intersecting families are smaller:

THEOREM 5. *(i) If $\mathcal{F}$ is 4-wise intersecting and transitive, then $|\mathcal{F}| \leqslant 2^n \cdot \exp(-(n \ln 2/2)^{1/3})$.*
(ii) If $\mathcal{F}$ is 4-wise intersecting and regular and closed under taking supersets, then $|\mathcal{F}| \leqslant 2^n \cdot n^{-0.347}$.

PROBLEM. Is it true that a 3-wise intersecting transitive (or regular) family $\mathcal{F}$ must have $|\mathcal{F}| = o(2^n)$?

The method of proof of Theorem 5 gives a result which is of independent interest.

THEOREM 6. *Let G be a transitive permutation group on an n-set X, and T a t-subset of X. let*

$$\mathcal{F} = \{F: F \subseteq X, F \cap g(T) \neq \varnothing \text{ for all } g \in G\}.$$

Then $|\mathcal{F}| \leqslant (2^t - 1)^{n/t}$.

Equality holds, for example, if T is a block of imprimitivity for G.

REMARK. By analogy with the alternative characterisation of the set A given before Theorem 1, we could define, for any prime p, the set

$$A_p = \{n \in \mathbb{N}: \text{there is a transitive permutation group of degree } n \text{ containing no fixed-point-free } p\text{-element}\}$$

and conjecture the existence of a function m_p suc that, if $n = p^a . b$ with $p \nmid b$ and $a \geqslant m_p(b)$, then $n \notin A_p$. It is trivial that if $n = p^a . b$ with $a \geqslant 1$ and $b < p$, then $n \notin A_p$; but we have no further results on this problem. The question is partly motivated by a theorem of [6] according to which any transitive permutation group of degree $n > 1$ contains a fixed-point-free p-element for *some* prime p.

We always use log to denote logarithms to base 2, and in for natural logarithms.

We are grateful to Roy Meshulam and Peter Neumann for helpful discussions.

2. Transitive Intersecting Families

For the remainder of the paper, X denotes a set of cardinality n, and $\mathscr{F}$ a family of subsets of X.

Lemma 2.1. Let $\mathscr{F}$ be an intersecting family. Then $|\mathscr{F}| \leqslant 2^{n-1}$; equality holds if and only if $\mathscr{F}$ contains one of each complementary pair of subsets of X. If $|\mathscr{F}| = 2^{n-1}$, then $\mathscr{F}$ is closed under taking supersets.

Proof. All but the last sentence follows from the observation that $\mathscr{F}$ contains at most one of each complementary pair of subsets. If $|\mathscr{F}| = 2^{n-1}$, $F \in \mathscr{F}$, and $G \supseteq F$, then $F \cap (X \backslash G) = \varnothing$, so $X \backslash G \notin \mathscr{F}$, and $G \in \mathscr{F}$.

A set B is called a *blocking set* for the family $\mathscr{F}$ if it meets every member of $\mathscr{F}$ and contains none; that is, $F \cap B \neq \varnothing$ and $F \cap (X \backslash B) \neq \varnothing$ for all $F \in \mathscr{F}$. Obviously, the complement of a blocking set is a blocking set.

Lemma 2.2. *Let $\mathscr{F}$ be an intersecting family. Let*

$$\mathscr{F}_1 = \{G \subseteq X : F \subseteq G \text{ for some } F \in \mathscr{F}\},$$

and let $\mathscr{F}_2$ consist of one of each complementary pair of blocking sets of $\mathscr{F}$, chosen according to the rule that if $|B| \neq |X \backslash B|$ then the larger set is chosen. Then $\mathscr{F}_1 \cup \mathscr{F}_2$ is an interesting family of cardinality 2^{n-1} containing $\mathscr{F}$.

Proof. It is clear that $\mathscr{F}_1 \cup \mathscr{F}_2$ is intersecting. Let Y be any subset of X. If Y contains a member of $\mathscr{F}$, then $Y \in \mathscr{F}_1$; if Y is disjoint from a member of $\mathscr{F}$, then $X \backslash Y \in \mathscr{F}_1$; and if neither holds, then Y is an $\mathscr{F}$-blocking set, so either Y or $X \backslash Y$ is in $\mathscr{F}_2$.

Proposition 2.3. *Let $\mathscr{F}$ be an intersecting family, and G a subgroup of* Aut($\mathscr{F}$) *which contains no fixed-point-free 2-element. Then there is an intersecting family $\mathscr{F}' \supseteq \mathscr{F}$ with $|\mathscr{F}'| = 2^{n-1}$ and $G \leqslant$ Aut($\mathscr{F}'$).*

Proof. A permutation of X interchanges some complementary pair of subsets iff all its cycles have even length, that is, iff some odd power of it is a fixed-point-free 2-element (interchanging the same pair of sets). So, if G contains no fixed-point-free 2-element, then the orbits of G on $\frac{1}{2}n$-sets fall into 'dual' pairs, the dual of an orbit consisting of all complements of sets in that orbit. Thus the choices in Lemma 2.2 can be made in a G-invariant way.

Remark. If n is odd, there are no fixed-point-free 2-elements; so any intersecting family can be enlarged to one of size 2^{n-1} without destroying any automorphisms.

From this result, we obtain Isbell's characterisation of the set A:

Corollary 2.4 *$n \in A$ iff there is a transitive permutation group of degree n containing no fixed-point-free 2-element.*

PROOF. The reverse implication is immediate from Proposition 2.3, taking $\mathscr{F} = \varnothing$. For the forward implication, the first sentence of the proof of the proposition shows that, if $\mathscr{F}$ is intersecting and $|\mathscr{F}| = 2^{n-1}$, then $\mathrm{Aut}(\mathscr{F})$ contains no fixed-point-free 2-elements.

Let $m_r(n)$ and $m_t(n)$ be the maximum sizes of regular (resp. transitive) intersecting families of sets; and, for n even, let $m'_r(n)$ and $m'_t(n)$ be the maximum sizes of regular (resp. transitive) intersecting families of $\frac{1}{2}n$-sets. For $0 \leqslant k \leqslant n$, and any family $\mathscr{F}$, let $\mathscr{F}_k$ denote the family

$$\{F \subseteq X : F \in \mathscr{F}, |F| = k\}.$$

LEMMA 2.5 *(i) if $\mathscr{F}$ is transitive, then $\mathscr{F}_k$ is transitive for all k.*
(ii) If $\mathscr{F}_k$ is regular for all k, then $\mathscr{F}$ is regular.

The proof is obvious. The converse of (i) is clearly false, since we may take transitive families $\mathscr{F}_k$ and $\mathscr{F}_l$ for which $\mathrm{Aut}(\mathscr{F}_k \cup \mathscr{F}_l) = \mathrm{Aut}(\mathscr{F}_k) \cap \mathrm{Aut}(\mathscr{F}_l)$ is intransitive. It is true, however, that if $\mathrm{Aut}(\mathscr{F}_k)$ is transitive and $\mathrm{Aut}(\mathscr{F}_l) = S_n$ for all $l \neq k$, then $\mathrm{Aut}(\mathscr{F})$ is transitive.

The converse of (ii) is false, even if $\mathscr{F}$ is intersecting and $|\mathscr{F}| = 2^{n-1}$, as the following example shows.

EXAMPLE 2.6. Let X be a large finite set whose cardinality is coprime to 10. Choose a random partition of X into 10 parts, labelled with the 2-subsets of $\{1, \ldots, 5\}$, say $X_{12}, \ldots, X_{45}$. let A_i be the union of the four parts whose labels contain i; then $A_i \cap A_j = X_{ij}$ for $i \neq j$. Let P be a cyclic group of permutations of X (any transitive group of polynomially bounded size would do), and set

$$\mathscr{A} = \{\pi(A_i) : \pi \in P, 1 \leqslant i \leqslant 5\}.$$

It can be shown that, with probability exponentially close to 1, $\mathscr{A}$ is an intersecting antichain and $|A_i| < \frac{1}{2}n$ for all i.

Now let $\mathscr{A}'$ be obtained as in Proposition 2.3; that is, $\mathscr{A}'$ consists of all sets containing a member of $\mathscr{A}$ together with all blocking sets of size greater than n. Finally, set

$$\mathscr{F} = \mathscr{A}' \backslash \{A_1, \ldots, A_5\} \cup \{X \backslash A_1, \ldots, X \backslash A_5\}.$$

Then $\mathscr{F}$ is intersecting and $|\mathscr{F}| = |\mathscr{A}'| = 2^{n-1}$. Also, $\mathscr{A}'$ is transitive, hence regular; and, since each point lies in two of the five sets A_i, the passage from $\mathscr{A}'$ to $\mathscr{F}$ increases the degree by one. Moreover, since $5 \nmid n$, not all A_i have the same size, so $\mathscr{F}_k$ is not regular for some k.

PROPOSITION 2.7 *(i)* $2^{n-1} - m_t(n) = \frac{1}{2}\binom{n}{\frac{1}{2}n} - m'_t(n)$.
(ii) $2^{n-1} - m_r(n) \leqslant \frac{1}{2}\binom{n}{\frac{1}{2}n} - m'_r(n)$.

PROOF. The inequality $\leqslant$ is obtained in each case by taking a transitive or regular intersecting family of n-sets of maximum size and adjoining all sets of size greater than $\frac{1}{2}n$ (using Lemma 2.4(11) and the remark following it). The reverse inequality is obtained by taking a transitive intersecting family $\mathscr{F}$ of maximum size and considering $\mathscr{F}_{\frac{1}{2}n}$.

We do not know whether equality necessarily holds in (ii). However, it is known for which n the right-hand side is zero, in view of the following result of Brace and Daykin [2]:

THEOREM 2.8 $m'_r(n) = \frac{1}{2}\binom{n}{\frac{1}{2}n}$ *iff n is not a power of* 2.

It follows that $m_r(n) = 2^{n-1}$ if n is not a power of 2.

PROBLEM 2.9. For $n = 2^a$, $a \geqslant 1$, is there a regular intersecting family of cardinality 2^{n-1}?

If $\mathscr{F}$ were such a family, then $\mathscr{F}_{\frac{1}{2}n}$ would not be regular; this easily implies that $\mathscr{F}$ would contain sets of cardinality less than $\frac{1}{2}n$. It can be shown that no such family exists for $n = 2, 4, 8$.

3. ON NUMBERS NOT IN A

Let G be a permutation group on X, where $|X| = n$. We say that a subset Y of X is *flipped* by G if some element of G interchanges Y with its complement. (Such a permutation must have all its cycles of even length; and, if Y is flipped by G, then some fixed-point-free 2-element flips it.)

Let $f(n)$ be the minimum, over all transitive permutation groups G of degree n, of the number of sets flipped by G. Clearly we can take the minimum over all *minimal transitive* groups G, those such that every proper subgroup of G is intransitive.

LEMMA 3.1. (*i*) $m_i'(n) = \frac{1}{2}\binom{n}{\frac{1}{2}n} - \frac{1}{2}f(n)$.
(*ii*) $m_i(n) = 2^{n-1} - \frac{1}{2}f(n)$.

PROOF. (i) The $\frac{1}{2}n$-sets not flipped by a group G fall into dual pairs of orbits, as in Proposition 2.3. A maximal G-invariant intersecting family of $\frac{1}{2}n$-sets consists of the union of one of each dual pair of orbits.

(ii) Clear from (i) and Proposition 2.7(i).

Hence $f(n) = 0$ iff $n \in A$.

The first family of numbers not in A are the powers of 2, about which the next result gives complete information.

THEOREM 3.2 (*i*) *For $n > 1$, n is a power of 2 iff every transitive permutation group of degree n contains a fixed-point-free involution.*
(*ii*) *If $n = 2^a (a \geqslant 1)$, then $n \notin A$ and $f(n) = \Sigma_{i=0}^{a-1} 2^{2^i}$; moreover, the configuration of $f(n)$ sets of size $\frac{1}{2}n$ is unique.*

PROOF. Let G be a transitive group of degree 2^a ($a \geqslant 1$). A Sylow 2-subgroup of G is transitive; without loss of generality, we may assume that G is a 2-group.

Let z be an involution in the centre of G. Then z is fixed-point-free and flips $2^{2^{a-1}}$ sets, namely, all those containing one point from ech cycle of z. Now let B be the set of cycles of z, and H the group induced on B by G. Then H is a transitive 2-group of degree 2^{a-1}. By induction, H flips at least $\Sigma_{i=0}^{a-2} 2^{2^i}$ sets. Each of these yields a set (the union of the corresponding cycles of z) flipped by G; and none of these coincides with a set already described, since none of the earlier sets is a union of cycles of z. Thus

$$f(n) \geqslant \sum_{i=0}^{a-1} 2^{2^i}.$$

The cyclic group of order n realises the value $\Sigma_{i=0}^{a-1} 2^{2^i}$, since for $j = 0, \ldots, a-1$, the elements of order 2^{j+1} are fixed-point-free and all flip the same $2^{2^{a-j-1}}$ sets, all of which are fixed by elements of smaller order.

The uniqueness of the minimal configuration also follows from the above inductive proof: the configuration on $2n$ points is found from that on n points by replacing each point

x by two points x_1, x_2, and then adjoining each set which contains exactly one point from each pair.

Finally, we prove the converse of (i). Suppose that $n = 2^a \cdot b$, with b odd and $b > 1$. Let $X = \{x_{ij} : 1 \leqslant i \leqslant 2^a,\ 1 \leqslant j \leqslant b\}$. For $1 \leqslant j \leqslant b$, let s_j be the permutation $(x_{1j}\, x_{2j} \cdots x_{2^a j})$, and let t be the permutation

$$\prod_{i=1}^{2^a} (x_{i1}\, x_{i2} \cdots x_{ib}).$$

Let

$$N = \{s_1^{k_1} \cdots s_b^{k_b} : k_1 + \cdots + k_b \equiv 0 \pmod{2^a}\},$$

and let C be the group generated by t. The product $G = NC$ is transitive of degree n. Any involution z in this group lies in N and has the form $s_1^{e_1} \cdots s_b^{e_b}$, where $e_j = 0$ or 2^{a-1} for $j = 1, \ldots, b$; since b is odd, $e_j = 0$ for some j, and z fixes the point x_{1j}.

REMARK 3.3. (i) Note that $m_t'(2) = m_t'(4) = 0$; these are the only even numbers n for which $m_t'(n) = 0$.
(ii) The extremal configuration of $m_t'(2^a)$ intersecting sets is not unique, because of the choices of orbits involved.
(ii) One remaining problem is that of determining the minimal transitive 2-groups, other than cyclic groups, which flip exactly $f(n)$ sets. (Both the Klein group of order 4 and the quaternion group of order 8 have this property.)

By Theorem 1, we have $3.2^a \notin A$ for $a \geqslant 2$. For the first of these values, we can compute the value of f (Theorem 4(ii)).

PROOF OF THEOREM 4(ii). It is straightforward to show that the group defined in the last part of the proof of Theorem 3.2 flips exactly 48 sets. We must establish that any minimal transitive group of degree 12 flips at least 48 sets.

Lemma 3.4. (i) The only minimal transitive groups of degree 6 are the cyclic and dihedral groups (acting regularly) and the alternating group A_4 (acting on the cosets of a subgroup of order 2).
(ii) Any minimal transitive group of degree 12 is a $\{2, 3\}$-group.

PROOF. We give the argument for (ii); (i) is similar but easier. First, using Sims' list of primitive groups [14] and the subgroup structure of these groups, we see that a minimal transitive group of degree 12 is necessarily imprimitive. If it has a block of imprimitivity of size 3 or 4, it is contained in S_3 wr S_4 or S_4 w S_3, and so is necessarily a $\{2, 3\}$ group. If it has a block of size 2, then either the group $\bar{G}$ induced on the set of blocks is minimal transitive of degree 6 (in which case the result follows from (i)), or else a proper transitive subgroup of $\bar{G}$ acts with two orbits of length 6 (each of which is also a block for G).

So we may assume that G has two blocks of size 6, and that the group induced by a block on its setwise stabiliser is one of PSL(2, 5), PGL(2, 5), A_6 or S_6. Let H be the subgroup fixing the two blocks. Then H has a unique minimal characteristic subgroup, which is normal in G; by minimality, we may assume that H is PSL(2, 5), PSL(2, 5) $\times$ PSL(2, 5), A_6, or $A_6 \times A_6$ if $H = S \times S$, then $G = S$ wr C_2, and G contains a proper transitive subgroup $S_0 \times C_2$, where S_0 is a diagonal subgroup of $S \times S$. If H is simple, $g \in G \backslash H$, and K is a transitive subgroup of H normalised by g, then $K\langle g\rangle$ is a transitive subgroup of G. The proof is finished by showing that any coset of Inn(H) in Aut(H) contains an automorphism which normalises a transitive subgroup K of H. (K can be chosen to be a Sylow 2- or 3-normaliser of H.)

We return now to the proof that $f(12) = 48$. Let G be a transitive group of degree 12. We may assume that G contains no fixed-point-free involution, since such an involution flips 64 sets. Also, we may assume that G is minimal transitive. From this it follows, both that G is a $\{2, 3\}$-group (Lemma 3.4(ii)), and that any odd permutation in G must be fixed-point-free (for otherwise the even permutations in G would form a proper transitive subgroup). By Burnside's theorem, G is solvable, and so a minimal normal subgroup N of G is elementary abelian, and has orbits of length 2, 3 or 4. We treat these cases in turn.

N-orbits of length 2. We can identify N with a binary linear code of length 6, in which all words have even weight and no word has weight 6, and which has a transitive automorphism group. Up to isomorphism, the only such code is spanned by (1 1 1 1 0 0) and (1 1 0 0 1 1). So $N \simeq V_4$. Moreover, G/N is a minimal transitive group of degree 6, necessarily regular or isomorphic to A_4, by Lemma 3.4(i). If G/N is regular, then a Sylow 2-subgroup P of G has order 8, and all its involutions lie in N (since elements outside N are fixed-point-free); so P is abelian, and $P \leqslant C_G(N)$. If $G/N \simeq S_3$, then G is generated by its Sylow 2-subgroups, and $N \leqslant Z(G)$; if $G/N \simeq C_6$, then G has a normal Sylow 2-subgroup $P \simeq C_4 \times C_2$ admitting no automorphism of order 3, so we have $P \leqslant Z(G)$. This is impossible, since $Z(G)$ is semiregular.

So we have $G/N \simeq A_4$. Then G has a normal Sylow 2-subgroup P of order 16 with an automorphism of order 3 acting non-trivially on both N and P/N. This implies that P is abelian, whence regular on each of its orbits of length 4. Thus there are only three distinct stabilisers in P, containing between them 10 elements. The remaining 6 elements of P fall into 3 inverse pairs of elements of order 4, each a product of two 2-cycles and two 4-cycles and so flipping 16 sets; and there is no overlap, since a set flipped by such an element contains two N-orbits lying in distinct P-orbits and the inverse pair is determined by these P-orbits. So G flips 48 sets.

N-orbits of length 3. Now N is an elementary abelian 3-group; and, if K is the kernel of the action of G on the set of N-orbits, then $|G/K| = 4$.

If $|N| = 3$, then any 2-element normalises N, so N and a Sylow 2-subgroup generate a regular subgroup, containing a fixed-point-free involution. So we may assume that $|N| \geqslant 9$. From the fact that each coset of K in G except K itself contains a fixed-point-free 2-element, we see that, for each pair of N-orbits, there is a set flipped by G containing two points from each of these orbits and one point from each of the other two. No such set can be fixed by an element of N, so there are at least $6 \cdot 9 = 54$ sets flipped by G.

N-orbits of length 4. Since N acts regularly on each orbit, the number of fixed points of any element of N is a multiple of 4. Since the average number of fixed points is the number of orbits, namely 3, some element of N is a fixed-point-free involution.

REMARK 3.5. The proof of Theorem 1(ii) given by [4] is a straightforward induction starting with the case $n = 12$. Can similar methods yield lower bounds for $f(2^a \cdot 3)$ for $a \geqslant 3$?

4. NUMBERS IN A

In this section, we prove Theorem 2, and give a variety of constructions exhibiting further members of A.

PROOF OF THEOREM 2. (i) If G_i is a transitive permutation group on X_i containing no fixed-point-free 2-element for $i = 1, 2$, then $G_1 \times G_2$ acting on $X_1 \times X_2$ has the same property.

(ii) A set of odd size admits no fixed-point-free 2-element.

(iii) The group constructed in Theorem 3.2, with degree $n = 2^a . b$, with $b > 1$ odd, contains no fixed-point-free involution; but, if $a = 1$, it contains no 2-element of order greater than 2.

(v) It follows from (i)–(iii) that, if B is the set of natural numbers having at least as many odd as even prime factors (counted with multiplicities), then $B \subseteq A$; it suffices to show that B has density 1. Take $\varepsilon > 0$ arbitrary. Choose k so large that $2^k > 1/\varepsilon$. let $\mathbb{N}\backslash B = C_1 \cup C_2$, where

$$C_1 = \{n \in \mathbb{N}\backslash B : 2^{k+1} | b\}, \qquad C_2 = \mathbb{N}\backslash B\backslash C_1.$$

Then C_1 has density at most $1/2^{k+1} < \varepsilon/2$. Also, every number in C_2 has at most $2k$ prime factors; it suffices to show that the set D_m of numbers with exactly m prime factors has density 0. This is true because

$$\sum_{\substack{n \leqslant X \\ n \in D_m}} 1/n \leqslant \Big(\sum_{\substack{p \leqslant X \\ p \in D_1}} 1/p \Big)^m \sim (\ln \ln x)^m,$$

while $\Sigma_{n \leqslant x} 1/n \sim \ln x$.

(iv) First, we re-cast slightly the group used in (iii). Let H be the additive group of all binary b-tuples of even weight, and C the cyclic group of order b of co-ordinate permutations. Then C acts on H, and we take G to be the semi-direct product. Since b is odd, any element of H has an entry 0, and so some conjugate of it lies in the subgroup H_1 of H defined by the equation $x_1 = 0$. Thus, representing G on the $2b$ cosets of H_1, every 2-element (that is, every element of H) has a fixed point.

To establish (iv), we use the same group, but replace H_1 by the subgroup H_2 defined by the equations $x_2 = 0$, $x_1 = x_3$. Every element h of H has an odd number of zeros, hence a run of consecutive zeros of odd length (regarding it as cyclically ordered). Thus h has either three consecutive zeros, or a run . . . 101 . . . ; in either case, some cyclic shift is in H_2. Now, if $b > 3$, the equations $x_1 + \cdots + x_b = 0$, $x_2 = 0$, $x_1 = x_3$ are independent; so $|H : H_2| = 4$, $|G : H_2| = 4b$, establishing the result.

This construction suggests an obvious generalisation. By (i), it is reasonable to concentrate on the case when $b = p$ is an odd prime. Define a function $w(p)$ as follows. Let C be the cyclic group of order p, and V the unique (up to similarity) non-trivial irreducible C-module over GF(2). The dimension of V is the order of 2 mod p, say d, and V can be realised as the additive group of GF(2^d), with C the unique subgroup of order p in the multiplicative group. Now let $w(p)$ be the maximum codimension of a subspace W of V with the property that the images of W under C cover V.

PROPOSITION 4.1. *$2^a . p \in A$ for all $a \leqslant w(p)$.*

PROOF. Let W be as in the definition, with codimension $w(p)$. Let U be a subspace containing W and having codimension a. Now let G be the semi-direct product of V by C, acting on the cosets of U.

PROPOSITION 4.2. Let p be a prime greater than 3, and let d be the order of 2 mod p. Then

$$\max(2, \lfloor 2 \log p \rfloor - d) \leqslant w(p) \leqslant \lfloor \log p \rfloor$$

The upper bound is attained if $p = (2^d - 1)/(2^e - 1)$ for some e dividing d, and so, in particular, if p is a Fermat or Mersenne prime.

PROOF. The lower bound 2 is established by the same argument as Theorem 2(iv); for the other lower bound see (3). The upper bound is trivial: $|V| = 2^d$, $|W| = 2^{d - w(p)}$, and p images of W cover V.

Suppose that e divides d. Then we can regard V as a GF(2^e)-space of dimension d/e. If $p = (2^d - 1)/(2^e - 1)$, then C permutes transitively the one-dimensional GF(2^e)-spaces, so the images of one of these (say W) cover V; and the GF(2)-codimension of W is $d - e$.

This result yields a number of primes p for which $w(p) > 2$ (although as yet, with present knowledge, only finitely many): in addition to Fermat and Mersenne primes greater than 7, there are others given by the last assertion (for example, $w(73) = 6$), or by the lower bound involving d (for example, $w(178\,481) \geqslant 11$). We have established by computation the values $w(11) = w(13) = 2$, $w(23) = w(43) = 3$, $w(89) = 6$. It is an open problem to establish that $w(p) > 2$ for infinitely many p; but perhaps it is even the case that $w(p) \to \infty$ as $p \to \infty$.

The upper bound in Proposition 4.2 means that we can never construct a member of A whose 2-part exceeds its odd part by this method. Moreover, the multiplicative closure of A does not lift this limitation either. To do better with these methods, we need to ensure that the number of conjugates of the subgroup U of V exceeds the index of V in G. For this, we need to use a non-abelian group V. This argument is due to Peter Neumann. The next result extends his observation that $56 \in A$.

PROPOSITION 4.3. *(i) If n is even, then $2^a(2^n - 1) \in A$ for all $a \leqslant 3n/2 - 2$.*
(ii) If n is odd, then $2^a(2^n - 1) \in A$ for all $a \leqslant 2n - 2$.

PROOF. (i) Let $q = 2^{\frac{1}{2}n}$. Let G be the stabiliser of a point in the group $PGU(3, q)$ (in its usual 2-transitive permutation representation). Then G has a normal subgroup V of order q^3, and G/V is cyclic of order $q^2 - 1$. Moreover, the following are proved by straightforward calculation: (a) The centre of V is elementary abelian of order q, and $V/Z(V)$ is elementary abelian of order q^2; (b) $|C_G(V)| = q^2$ for all $v \in V \backslash Z(V)$; (c) G/V acts transitively on $Z(V)$ and on $V/Z(V)$ by conjugation.

It follows that V is the union of three G-conjugacy classes, namely $\{1\}$, $Z(V)\backslash\{1\}$, and $V\backslash Z(V)$. So, if H is a subgroup of G containing an element of $V\backslash Z(V)$ (all such elements have order 4, and their squares lie in $Z(V)$), then G, acting on the cosets of H, has no fixed-point-free 2-element. Moreover, $|G:H| = (2^n - 1)2^{3n/2-f}$, where $|H| = 2^f$; here f can be any number in the range $2 \leqslant f \leqslant 3n/2$.

(ii) If n is odd, let $q = 2^n$, and let G be the stabiliser of a point in $Sz(q)$. Then $|G| = q^2(q - 1)$. If H contains an element of order 4 then, again, H meets every conjugacy class in $V = 0_2(G)$, and the conclusion follows as in (i).

REMARK 4.4. Many more constructions can be devised. For example, if G is a group with elementary abelian Sylow 2-subgroups and only one conjugacy class of involutions (such as $PSL(2, 2^n)$, or the Ree group ${}^2G_2(3^{2n+1})$), and H any subgroup of G of even order, then $|G:H| \in A$. But for every number which we have been able to show to lie in A, we can in fact demonstrate this using Theorem 2 and Propositions 4.1–4.3.

5. On 4-Wise Intersecting Transitive Families

In this section, we prove Theorem 5(i) and Theorem 6. The proofs depend on a result from [5] which we now state.

Let $\bar{x} = (x_1, \ldots, x_n)$ be a random vector-variable. For $A \subseteq X = \{1, \ldots, n\}$, let $\bar{x}_A$ denote the restriction of $\bar{x}$ to the co-ordinates in A, that is, $\bar{x}_A = (x_a : a \in A)$. For example, $\bar{x}_{\{i\}}$ is simply the random variable x_i. Let $H_A = H(\bar{x}_A)$ be the binary entropy of $\bar{x}_A$.

PROPOSITION 5.1 [5]. *Suppose that $A_1, \ldots, A_s$ are subsets of X such that each element of X lies in at least d of them. Then we have*

$$dH(\bar{x}) \leqslant \sum_{i=1}^{s} H(\bar{x}_{A_i}).$$

We identify a subset F of X with its characteristic function $\bar{x}(F)$, a zero–one vector of length n. Given a family $\mathcal{F}$ of subsets of X, we use the uniform distribution on $\mathcal{F}$; that is,

$$p(\bar{x} = \bar{x}(F)) = 1/|\mathcal{F}| \text{ for } F.$$

Thus we have $H(\bar{x}) = \Sigma_{i=1}^{m} - (1/m)\log(1/m) = \log m$, where $m = |\mathcal{F}|$.

PROOF OF THEOREM 6. Let G be a transitive permutation group on X, T a t-subset of X, and

$$\mathcal{F} = \{F \subseteq X : F \cap g(T) \neq \varnothing \quad \text{for all } g \in G\},$$

and consider the random variable $\bar{x}$ defined above. For every $g \in G$, $\bar{x}_{g(T)}$ takes at most $2^t - 1$ values, since $(0, \ldots, 0)$ is excluded. Thus we have

$$H(\bar{x}_{g(T)}) \leqslant \log(2^t - 1).$$

On the other hand, the transitivity of G implies that every element of X lies in exactly $|G|t/n$ sets $g(T)$. Thus, by Proposition 5.1,

$$|G|t/n \log |\mathcal{F}| \leqslant |G| \log(2^t - 1)$$

or, equivalently,

$$|\mathcal{F}| \leqslant (2^t - 1)^{n/t}.$$

In [7] it was shown that a transitive 4-wise intersecting family $\mathcal{F}$ satisfies $|\mathcal{F}| \leqslant 2^n/n^{1/2}$. Theorem 5(i), which we now prove, improves this bound considerably.

We need the following easy consequence of a theorem of Katona [13].

PROPOSITION 5.2. *Let r be a positive integer, and $\mathcal{F}$ a family of sets satisfying $|F \cap F'| \geqslant r$ for all $F, F' \in \mathcal{F}$. Then*

$$|\mathcal{F}| \leqslant 2^n \, \mathrm{e}^{-r^2/2n}.$$

PROOF OF THEOREM 5(i). Let $\mathcal{F}$ be transitive and 4-wise intersecting, and $G = \mathrm{Aut}(\mathcal{F})$. Choose $F_1, F_2 \in \mathcal{F}$ so that $|F_1 \cap F_2|$ is minimal. Set $T = F_1 \cap F_2$ and $t = |T|$. Since $\mathcal{F}$ is 4-wise intersecting, the family

$$\mathcal{F}(g(T)) = \{F \cap g(T) : F \in \mathcal{F}\}$$

is intersecting, and so has cardinality at most 2^{t-1} (by Lemma 2.1). Thus

$$H(\bar{x}_{g(T)}) \leqslant \log 2^{t-1} = t - 1.$$

By Proposition 5.1,

$$|G|t/n \log |\mathcal{F}| \leqslant |G|(t - 1),$$

so $|\mathcal{F}| \leqslant 2^n/2^{n/t}$.

Thus the result is true if $t \leqslant (2n^2 \ln 2)^{1/3}$. However, if $t > (2n^2 \ln 2)^{1/3}$, the conclusion is immediate from Katona's result (Proposition 5.2).

6. Regular Filters

A family $\mathcal{F}$ is called a *filter* if $F \in \mathcal{F}$ and $G \supseteq F$ imply $G \in \mathcal{F}$. (This is not standard; we do not reuire $\mathcal{F}$ to be closed under intersection.)

For $x \in X$, the *degree* $d(x)$ of x in $\mathcal{F}$ is the number of members of $\mathcal{F}$ containing x. We require a simple lemma.

LEMMA 6.1. *Suppose that $\mathcal{F}$ is a filter on X and $A \subseteq X$ is such that $F \cap A \neq \emptyset$ for all $F \in \mathcal{F}$. Then the average degree of points of A in $\mathcal{F}$ is at least $\frac{1}{2}|\mathcal{F}|(1 + 1/(2^a - 1))$, where $a = |A|$.*

PROOF. By [12] or more easily by Hall's theorem, the incidence matrix of b-sets and $(a - b)$-sets of an a-set A (with incidence = inclusion) is non-singular. The existence of a non-zero term in the expansion of the determinant shows that, if $b < \frac{1}{2}a$, there is a *matching* $B \mapsto B^*$ from b-sets to $(a - b)$-sets so that $B \subseteq B^*$. Defining

$$f(B) = |\{F \in \mathcal{F} : F \cap A = B\}|,$$

the fact that $\mathcal{F}$ is a filter shows that $f(B) \leqslant f(B^*)$ for all sets B with $|B| < \frac{1}{2}a$.

The average degree of points in A is α, say, where

$$a\alpha = \sum_{X \in A} d_{\mathcal{F}}(x) = \sum_{\emptyset \neq B \subseteq A} |B| f(B),$$

$$\sum_{\substack{\emptyset \neq B \subseteq A \\ |B| < \frac{1}{2}a}} (|B| f(B) + (a - |B|) f(B^*)) + \tfrac{1}{2}a \sum_{B \subseteq A} f(B) + af(A) \geqslant \tfrac{1}{2}a \sum_{\emptyset \neq B \subseteq A} f(B) + \tfrac{1}{2}af(A)$$

$$= \tfrac{1}{2}a|\mathcal{F}| + \tfrac{1}{2}af(A).$$

Again, since $\mathcal{F}$ is a filter and $F \cap A \neq \emptyset$, $f(A) \geqslant |\mathcal{F}|/(2^a - 1)$, from which the result follows.

REMARK. The result can be adjusted if the condition

$$F \in \mathcal{F} \Rightarrow |F \cap A| \geqslant t$$

holds, for fixed t.

PROOF OF THEOREM 5(ii). Let $\mathcal{F}$ be a 4-wise intersecting regular filter. Choose F_1, F_2, $F_3 \in \mathcal{F}$ so that $A = F_1 \cap F_2 \cap F_3$ has minimal cardinality, say a. By [8], we have $|\mathcal{F}| \leqslant 2^n(\frac{1}{2}(\sqrt{5} - 1))^a$. Hence we are finished if $a > \frac{1}{2}\log n - \log\log n$; so suppose that

$$a \leqslant \tfrac{1}{2}\log n - \log\log n.$$

If d is the degree of $\mathcal{F}$, the lemma yields

$$d/|\mathcal{F}| \geqslant \tfrac{1}{2}(1 + 1/(2^a - 1)).$$

Then for the uniform random variable $\bar{x}$ of the last section, we have

$$H(x_i) \leqslant H(\tfrac{1}{2}(1 + 1/(2^a - 1)),$$

and Proposition 5.1 (with $s = n$, $A_i = \{i\}$) yields

$$\log|\mathcal{F}| \leqslant nH(\tfrac{1}{2}(1 + 1/(2^a - 1))),$$

or

$$|\mathcal{F}| \leqslant 2^n \cdot 2^{nH(\frac{1}{2}(1 + 1/(2^a - 1)))} < 2^n \cdot e^{-n/2^{2a+1}} < 2^n/n.$$

PROOF OF THEOREM 3. The first part is straightforward. By [1], if G is transitive on X, and $Y \subseteq X$ with $|Y| < |X|^{1/2}$, then $Y \cap g(Y) = \emptyset$ for some $g \in G$, and Y cannot be contained in any G-invariant intersecting family.

To see that the result is close to best possible, take a projective plane with a transitive automorphism group G (for example, a Desarguesian plane), and enlarge it to an intersecting family of size 2^{n-1} admitting G, using the remark following Proposition 2.3.

For the second part, suppose that $\mathcal{F}$ is a regular intersecting family of cardinality 2^{n-1}. Then $\mathcal{F}$ is a filter, by Lemma 2.1. Let F be a member of $\mathcal{F}$ of cardinality a. By Lemma 6.1, the degree of any point is at least $\frac{1}{2} \cdot 2^{n-1}(1 + 1/(2^a - 1))$.

On the other hand, the sum of the degrees of all points is equal to the sum of the sizes of all sets in $\mathscr{F}$. This does not exceed the sum of the sizes of the 2^{n-1} largest subsets of X, which is easily seen to be

$$\tfrac{1}{2}n(2^{n-1} + \binom{n}{\lfloor \frac{1}{2}(n-1) \rfloor}).$$

Thus

$$2^{n-1}(1 + 1/(2^a - 1)) \leqslant 2^{n-1} + \binom{n}{\lfloor \frac{1}{2}(n-1) \rfloor},$$

$$2^a - 1 \geqslant 2^{n-1} \Big/ \binom{n}{\lfloor \frac{1}{2}(n-1) \rfloor},$$

from which the result follows.

References

1. B. J. Birch, R. G. Burns, S. O. Macdonald and P. M. Neumann. On the orbit-sizes of permutation groups containing elements separating finite subsets, *Bull. Austral. Math. Soc.*, **14** (1976), 7–10.
2. A. Brace and D. E. Daykin, Sperner-type theorems for finite sets, in: *Combinatorics*, D. R. Woodall and D. J. A. Welsh, eds, 18–37, Inst. Maths Applics, Southend-on-Sea, 1972.
3. P. J. Cameron, Four lectures on projective geometry, in: *Finite geometries*, C. A. Baker and L. M. Batten, eds, 27–63, Marcel Dekker, New York, 1985.
4. P. J. Cameron, L. G. Kovacs, M. F. Newman and C. E. Praeger, Fixed-point-free permutations in transitive permutation groups of prime power order, *Q. J. Math., Oxford* (2), **36** (1985), 273–278.
5. F. R. K. Chung, P. Frankl, R. L. Graham and J. B. Shearer, Some intersection theorems for ordered sets and graphs, *J. Combin. Theory, Ser. A*, **43** (1986), 23–37.
6. B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups II, *J. Reine Angew. Math.*, **328** (1981), 39–57.
7. P. Frankl, Regularity conditions and intersecting hypergraphs, *Proc. Am. Math. Soc.*, **82** (1981), 309–311.
8. P. Frankl, An intersection theorem for finite sets, *Bull. Austral. Math. Soc.*, **15** (1976), 73–79.
9. J. R. Isbell, Homogeneous games, I, *Math. Student*, **25** (1957), 123–128.
10. J. R. Isbell, Homogeneous games, II, *Proc. Am. Math. Soc.*, **11** (1960), 159–161.
11. J. R. Isbell, Homogeneous games, III, in: Advances in game theory, M. Dresher, L. S. Shapley and A. W. Tucker, eds 255–265, Princeton Univ. Press, Princeton, N.J., 1984.
12. W. M. Kantor, On incidence matrices of finite projective and affine space, *Math. Z.*, **124** (1972), 315–318.
13. Gy. Katona, An intersection theorem for systems of finite sets, *Acta Math. Hungar.*, **15** (1964), 329–337.
14. C. C. Sims, Computational methods in the study of permutation groups, in: *Computational problems in abstract algebra*, J. Leech ed., 169–183, Pergamon, Oxford, 1970.

Received 5 March 1987 and in revised form 25 July 1988

P. J. Cameron
School of Mathematical Sciences, Queen Mary College, London E1 4NS, U.K.

P. Frankl
C.N.R.S., Université Paris VII, 75005 Paris, France
and
W. M. Kantor
Department of Mathematics, University of Oregon, Eugene, Oregon 97403, U.S.A.