LOWER BOUNDS ON BLOCKING SETS

A. A. BRUEN AND B. L. ROTHSCHILD

In memory of Ernst Straus

In a geometry the notion of *blocking set* ordinarily refers to a set of points meeting every line. (For projective planes convention requires in addition that the blocking set not contain all the points of any one line.) In this paper we obtain lower bounds for the size of a blocking set for projective planes and inversive planes, which are equal to or improvements on the best previously known bounds. If the notion of blocking set is generalized to families of disjoint subspaces rather than sets of points, then (partial) spreads are included, and we obtain a lower bound for the size of a maximum partial spread of *m*-spaces in projective (2m + 1)-space. The technique is that of Glynn, counting various sets of intersecting subspaces in two ways to obtain inequalities.

If we are considering any geometry (affine, projective, inverse, etc...) we can use the following definition:

DEFINITION. A set S of mutually disjoint k-subspaces is a (k, l)-blocking set if every l-subspace meets some member of S.

In the case of k = 0, l = 1 we have ordinary blocking sets, except for the case of the projective plane, where conventionally the condition that S contain no line is required for blocking sets. If k = l, then we have a maximum partial spread of k-spaces. These are the two cases for which there are some known bounds.

We consider first the case of k = 0, l = 1 in the inversive plane of order q [4]. The relevant features of this geometry are that there are $q^2 + 1$ points, $(q^2 + 1)q$ lines (called "circles" sometimes), q(q + 1) lines through each point, (q + 1) lines through any two points, and one line through any three points. Suppose we have a set S of x points, and denote by n_i the number of lines containing exactly *i* points of S, $i \ge 0$. (We note that $n_i = 0$ for i > q + 1 as lines have q + 1 points.) If S is a blocking set, then $n_0 = 0$.

Counting all lines gives

(1)
$$\sum_{i\geq 1} n_i = (q^2 + 1)q.$$

Similarly we get equations (2), (3), (4) below by counting in two ways the numbers respectively of pairs (P; L), $(\{P, Q\}; L)$, and $(\{P, Q, R\}; L)$, where P, Q, R are points of the set S on a line L.

(2)
$$\sum_{i\geq 1}n_i = (q^2 + q)x$$

(3)
$$\sum_{i\geq 1} \binom{i}{2} n_i = \binom{x}{2} (q+1)$$

(4)
$$\sum_{i\geq 1} {i \choose 3} n_i = {x \choose 3}.$$

Consider the polynomial (used in [6]) P(i) = (i - 1)(i - 3)(i - 4). It is non-negative for all positive integers *i*. Rewriting the polynomial we obtain

$$P(i) = 6\binom{i}{3} - 10\binom{i}{2} + 12i - 12.$$

Using (1)–(4) above we get

(5)
$$0 \le \sum_{i\ge 1} n_i P(i) = 6 \sum_{i\ge 1} {i \choose 3} n_i - 10 \sum_{i\ge 1} {i \choose 2} n_i + 12 \sum_{i\ge 1} in_i - 12 \sum_{i\ge 1} n_i$$
$$= 6 {x \choose 3} - 10 {x \choose 2} (q+1) + 12 (q^2+q) x - 12 (q^2+1) q.$$

Now let $x = \lambda q$. We get from (5) a non-negative cubic polynomial in q with leading coefficient

$$(\lambda^3-5\lambda^2+12\lambda-12)=(\lambda-2)(\lambda^2-3\lambda+6).$$

Then for $\lambda < 2$ this is negative, and for q large enough (depending on λ) the polynomial in q is negative, contradicting (5). Thus we get:

THEOREM 1. If S is a blocking set in the inverse plane of order q, and $\varepsilon > 0$, then $|S| \ge (2 - \varepsilon)q$ for q sufficiently large.

We can refine the argument a little by taking x = 2q - k. Then the polynomial in (5) becomes quadratic in q:

(6)
$$(2-4k)q^2 + (k^2 + 15k + 2)q - (k^3 + 8k^2 + 7k).$$

If we have k > 1/2, then (6) is negative for q sufficiently large. Thus we must have $k \le 1/2$, or $x \ge 2q - 1/2$. As x is an integer, $x \ge 2q$, for q sufficiently large. In fact, if we examine the polynomial above carefully, we see that the polynomial will be negative for all values of q if $k \ge 3$, for

all but q = 3 if k = 2, and for $q \ge 9$ if k = 1. Hence we get:

THEOREM 1'. If S is a blocking set in the inverse plane of order q, then $|S| \ge 2q$ for $q \ge 9$, and $|S| \ge 2q - 1$ for $q \ne 3$.

The best previous value for a lower bound for |S| was 2q - 1.

A word of explanation for the choice of P(i) is in order. There are many choices that could be made for the cubic polynomial P(i) so that it will be positive for all values of *i* between 1 and q + 1 (the number of points on a line in the inversive plane). Among those of the form (i - 1)(i - a)(i - (a + 1)) we would like to find the integer *a* which gives the strongest inequality on λ . That is, we use (x - 1)(x - a)(x - (a + 1)), and express it in terms of binomial coefficients. Then using (1)–(4) we get an inequality like (5) (with different coefficients). Letting $x = \lambda q$ in that inequality gives a non-negative cubic polynomial in *q* with leading coefficient

$$f(\lambda, a) = \lambda^3 - (2a-1)\lambda^2 + (a^2+a)\lambda - (a^2+a).$$

There is some λ_0 for which $f(\lambda, a) \le 0$ when $\lambda \le \lambda_0$. (λ_0 will be the smallest real root of $f(\lambda, a)$ of course.) We want to choose a to maximize λ_0 .

Now suppose for some $a \lambda_0 \ge 2$. Then

$$0 \ge f(2, a) = 8 - 4(2a - 1) + (a^2 + a)2 - (a^2 + a)$$
$$= a^2 - 7a + 12 = (a - 3)(a - 4).$$

Thus a = 3 or a = 4. Both $f(\lambda, 3)$ and $f(\lambda, 4)$ have a single real root, which in both cases is 2. So we look at the second (quadratic) term in the polynomial corresponding to (5) to see that a = 3 gives the better inequality

Glynn [6] used this polynomial originally to prove

THEOREM 2. Let S be a maximal partial spread of lines in PG(3, q), then $|S| \ge 2q$.

We recall that a maximal partial spread here is a set of disjoint lines meeting all lines of the space in at least one point. In our earlier notation k = l = 1, n = 3. We generalize the argument to the case n = 2m + 1, k = l = m. That is, we consider maximal partial spreads of *m*-spaces in PG(2m + 1, q) a set of disjoint *m*-spaces which intersects every *m*-space in at least a point. The best bound previously known on the size of a maximal partial spread is $(q + \sqrt{q} + 1)$ [1]. Using an argument like the one above, but necessarily a bit more complicated, we get:

THEOREM 3. If S is a maximal partial spread of m-spaces in PG(2m + 1, q), then $|S| \ge 2q - 1$, for q sufficiently large.

Proof. For
$$m = 1$$
 Theorem 2 applies, so we assume $m \ge 2$. We let
$$\begin{bmatrix} l \\ k \end{bmatrix}_q = \frac{(q^l - 1) \cdots (q^{l-k+1} - 1)}{(q^k - 1) \cdots (q - 1)},$$

which is the number of vector k-supspaces of an *l*-dimensional vector space over GF(q). We will write just $\binom{l}{k}$, suppressing the q, since there is no danger of ambiguity. The number of projective k-subspaces of projective L-space is then $\binom{l+1}{k+1}$. In what follows all spaces and subspaces will be *projective* spaces unless otherwise stated. The principal fact we need about these numbers is that as $q \to \infty$

$$(7) \begin{bmatrix} l \\ k \end{bmatrix} = q^{(l-k)k} \begin{cases} 1 + O(q^{-1}), & l \ge k \ge 0, \\ 1 + q^{-1} + O(q^{-2}), & l-1 \ge k \ge 1, \\ 1 + q^{-1} + 2q^{-2} + O(q^{-1}), & l+2 \ge k \ge 2, \\ 1 + q^{-1} + 2q^{-2} + 3q^{-3} + O(q^{-4}), & l-3 \ge k \ge 3. \end{cases}$$

This follows simply by expanding the numerator and denominator of $\binom{l}{k}$ as polynomials in q and then using 'long division'.

We also need the following fact.

PROPOSITION. Let N be an n-dimensional projective space over GF(q). Let L be an l-dimensional subspace, G a g-dimensional subspace such that $L \supseteq G$. Then the number of k-dimensional subspaces K with $K \cap L = G$ is given by

(8)
$$\begin{bmatrix} n-l\\k-g \end{bmatrix} q^{(k-g)(l-g)}.$$

We note that when l = g this is the number of k-supspaces containing G, $\binom{n-g}{k-g}$, a formula used repeatedly below. Also, if g = -1 we get $\binom{n-1}{k+1}q^{(k+1)(l+1)}$ for the number of k-spaces not meeting a fixed l-space at all. Let S denote a maximal partial spread of m-spaces in PG(2m + 1, q), and let |S| = x. Let n_i denote the number of m-spaces meeting exactly i members of S in at least one point. Then corresponding to (1)-(4) we get:

(9)
$$\sum_{i\geq 1} n_i = q^{m^2 + 2m + 1} (1 + q^{-1} + O(q^{-2}))$$

(10)
$$\sum_{i\geq 1} in_i = xq^{m^2+2m} (1+2q^{-1}+O(q^{-2}))$$

(11)
$$\sum_{i\geq 1} {i \choose 2} n_i = {x \choose 2} q^{m^2+2m-1} (1+3q^{-1}+O(q^{-2}))$$

(12)
$$\sum_{i\geq 1} \binom{i}{3} n_i = \binom{x}{3} q^{m^2+2m-2} (1+4q^{-1}+O(q^{-2})).$$

The equations (9)–(12) are obtained below by counting (in two ways) the numbers respectively of all M, pairs (N; M), pairs $(\{N, P\}; M)$, and pairs $(\{N, P, Q\}; M)$, where N, P, Q are *m*-spaces in S meeting an *m*-space M (not necessarily in S).

Equation (9) is clear since the summation gives the total number of m-spaces, which is

$$\begin{bmatrix} 2m+2\\m+1 \end{bmatrix} = q^{m^2+2m+1} + q^{m^2+2m} + O(q^{m^2+2m-1})$$

by (7).

For equation (10), the summation on the left enumerates all pairs (N; M) where N is in S and M is an arbitrary *m*-space meeting N in at least a point. Alternatively all such pairs can be found by selecting N (x ways) and then choosing M to meet N. There are $\begin{bmatrix} 2m+2\\m+1 \end{bmatrix}$ *m*-spaces all together of which, by (8), $q^{(m+1)^2}$ don't meet N. Thus the total number of pairs is

$$x\left(\left[\frac{2m+2}{m+1}\right]-q^{(m+1)^2}\right),$$

which is $xq^{m^2+2m}(1+2q^{-1}+O(q^{-2}))$ by (7).

To get (11) we can use a truncated form of the method of inclusion and exclusion. We want to enumerate the pairs $(\{N, P\}; M)$ where N and P are in S and M is any m-space meeting N and P. We can construct all of these by first picking $\{N, P\}$. (There are $\binom{x}{2}$ ways to do this.) Then we let α be the number of ways to choose M given N and P. We can overestimate α as follows: There are $\binom{m+1}{1}$ ways to choose a point in N, and the same for P. Then M can be chosen in $\binom{2m}{m-1}$ ways to contain both points. Thus α is at most

$$\alpha' = \begin{bmatrix} m+1\\1 \end{bmatrix}^2 \begin{bmatrix} 2m\\m-1 \end{bmatrix} = q^{m^2+2m-1} (1+3q^{-1}+O(q^{-2})),$$

from (7). But we overestimate here because some choices for M meet N and P in more than a point, and are thus counted multiply. A space M meeting N in a k-subspace, K, and P in an l-subspace, L, will be counted

$$\binom{k+1}{1}\binom{l+1}{1}$$

times. There are

$$\binom{m+1}{k+1}\binom{m+1}{l+1}$$

choices for the subspace K and L, and then M can be chosen in at most

$$\begin{bmatrix} 2m-k-l\\m-k-l-1 \end{bmatrix}$$

ways to contain K and L. Thus the excess $\alpha' - \alpha$ is at most

$$\begin{aligned} \alpha'' &= \sum_{\substack{k,l \ge 0 \\ k+l \ge 1}} \left[\frac{k+1}{1} \right] \left[\frac{l+1}{1} \right] \left[\frac{m+1}{k+1} \right] \left[\frac{m+1}{l+1} \right] \left[\frac{2m-k-l}{m-k-l-1} \right] \\ &= \sum_{\substack{k,l \ge 0 \\ k+l \ge 1}} O\left(q^{m^2+2m-k-l-k^2-l^2-1} \right) = O\left(q^{m^2+2m-3} \right) \end{aligned}$$

Thus $\alpha' \ge \alpha \ge \alpha' - \alpha''$, and $\alpha = q^{m^2 + 2m - 1}(1 + 3q^{-1} + O(q^{-2}))$. Finally, $\binom{x}{2}\alpha = \binom{x}{2}q^{m^2 + 2m - 1}(1 + 3q^{-1} + O(q^{-2}))$

establishing (11).

For (12), the left side enumerates the number of pairs ({ N, P, Q }; M) where N, P, Q are in S and all three meet the *m*-space M. The right side of (12) is a little delicate. Let α denote the number of ways of choosing M given N, P, Q. Then the right side of (12) is $\binom{x}{3}\alpha$. There are $\binom{m+1}{1}^3$ ways to choose a point from each N, P, Q. Of the choices, only $\binom{m+1}{1}$ are colinear triples. The number *m*-spaces M containing three colinear points is $\binom{2m}{m-2}$, whereas the number containing three points in general position is $\binom{2m-1}{m-2}$. Thus α is at most

$$\alpha' = \left(\begin{bmatrix} m+1\\1 \end{bmatrix}^3 - \begin{bmatrix} m+1\\1 \end{bmatrix} \right) \begin{bmatrix} 2m-1\\m-2 \end{bmatrix} + \begin{bmatrix} m+1\\1 \end{bmatrix} \begin{bmatrix} 2m\\m-1 \end{bmatrix}$$
$$= q^{m^2 + 2m - 2} (1 + 4q^{-1} + O(q^{-2}))$$

by (7) for $m \ge 3$. For m = 2 we get $\binom{2m-1}{m-2} = 1$ and

 $\alpha \leq (q^6 + 3q^5 + O(q^4)) + (q^5 + O(q^4)) = q^6 + 4q^5F + O(q^4).$

Thus

$$\alpha \leq q^{m^2+2m-2} (1+4q^{-1}+O(q^{-2}))$$
 for $m \geq 2$.

Again the upper bound is an overestimate because some choices for M meet N, P, Q respectively in h-, k- and l-spaces, where h, k, $l \ge 0$, $h + k + l \ge 1$. Each M is multiply counted, the number of times depending on the relative positions of the h-, k- and l-spaces, call them H, K, L.

308

Suppose $(H + K) \cap L = Z$, a z-dimensional projective subspace of L. Given h, k, l and z we can choose H, K and L in the following manner.

First we assume by a proper choice of basis that when N, P, Q are considered as (m + 1)-dimensional vector subspaces of (2m + 2)dimensional space we have bases e_1, \ldots, e_{m+1} for N, f_1, \ldots, f_{m+1} for P, and $e_1 + f_1, \ldots, e_{m+1} + f_{m+1}$ for Q, where the e_i and f_j are all independent. Let Π_N be the projection from Q to N, and Π_P from Q to P, $\Pi_N(e_i + f_i) = e_i$, $\Pi_P(e_i + f_i) = f_i$. The condition that $(H + K) \cap L = Z$ is equivalent to $\Pi_N^{-1}(H) \cap \Pi_P^{-1}(K) \cap L = Z$. Thus we can choose $Z([m+1]_{z+1}]$ choices), then $H \supseteq \Pi_N(Z)$ and $K \supseteq \Pi_P(Z)$ (at most $[m-2]_{k-z} [m-2]$ choices). Finally we choose L (at most $[m-2]_{r-z} [m-2]_{k-z}$ ways, which is the number of all M containing H, K, L. The number of times each M is counted by α' is $[n+1]_1[n+1][n+1]_1[n+1]$. So the amount $\alpha' - \alpha$ of the overestimate is at most

$$\alpha'' = \sum_{h,k,l,z} {m+1 \brack z+1} {m-z \brack h-z} {m-z \brack k-z} {m-z \brack l-z}$$
$$\cdot {2m-h-k-l+z \atop m-h-k-l+z-1} {h+1 \brack l+1} {k+1 \atop 1} {l+1 \atop 1}$$
$$= O(q^{m^2+m-mz-z^2-1-h(h-z)-k(k-z)-l(l-z)}) = O(q^{m^2+2m-4})$$

since h, k, $l \ge 0$ and $h + k + l \ge 1$. These estimates give $\alpha' \ge \alpha \ge \alpha' - \alpha''$, so $\alpha = q^{m^2 + 2m^{-2}}(1 + 4q^{-1} + O(q^{-2}))$, which establishes (12).

To complete the proof of Theorem 3, we use the same polynomial as in Theorem 1, namely,

$$(i-1)(i-3)(i-4) = 6\binom{i}{3} - 10\binom{i}{2} + 12i - 12.$$

Thus

$$0 \leq \sum_{i \leq 1} \left(6 \binom{i}{3} - 10 \binom{i}{2} + 12i - 12 \right) n_1$$

=
$$6 \sum_{i \geq 1} \binom{i}{3} n_i - 10 \sum_{i \geq 1} \binom{i}{2} n_i + 12 \sum_{i \geq 1} i n_i - 12 \sum n_i$$

and using (9)–(12)

$$= 6\binom{x}{3}q^{m^2+2m-2}(1+4q^{-1}+O(q^{-2}))$$

-10 $\binom{x}{2}q^{m^2+2m-1}(1+3q^{-1}+O(q^{-2}))$
+12 $xq^{m^2+2m}(1+2q^{-1}+O(q^{-2}))$
-12 $q^{m^2+2m+1}(1+q^{-1}+O(q^{-2})).$

Letting x = 2q - k, expanding, and collecting terms gives a polynomial in q with leading term $(6 - 4k)q^{m^2 + 2m}$. This is negative for k > 3/2. Thus for q large enough, the polynomial is negative, a contradiction. Since k must be integral, we must have $x \ge 2q - 1$. This completes the proof.

Next we consider the case of the projective plane. Recall that a blocking set here is a set of points meeting all lines but containing none. We note that the result below agrees with that of Bruen [2], [3].

THEOREM 4. Let S be a blocking set in a projective plane of order q. Then $|S| \ge q + \sqrt{q+1}$.

Proof. The proof uses the same technique as before, but now with a different polynomial.

Let |S| = q + k. Let n_i denote the number of lines containing exactly *i* points of *S*. Then $n_0 = 0$. Further, let *t* denote the largest number of points of *S* on any line, say the line *L*. Then there must be a point *P* on *L* not in *S*. There are *q* lines other than *L* meeting *P*, and each has at least one point of *S* on it. Thus $|S| \ge t + q$. Hence $k \ge t$, and we have $n_i = 0$ for i > k. Thus, in the summations below we need only sum up to i = k. We need three relations now:

(13)
$$\sum_{i=1}^{k} n_{i} = (q^{2} + q + 1)$$

(14)
$$\sum_{i=1}^{k} in_{i} = (k+q)(q+1)$$

(15)
$$\sum_{i=1}^{k} {i \choose 2} n_i = {k+q \choose 2}.$$

(13) just enumerates all the lines. (14) counts in two ways the pairs (P; L) where P is a point of S and L a line containing it. (15) counts all $(\{P, Q\}; L)$ where P and Q are points of S on L.

Now for $1 \le i \le k$ the polynomial

$$(i-1)(k-i) = -2\binom{i}{2} + ki - k$$

is non-negative. Of all quadratic polynomials with leading term $-i^2$ and non-negative for $1 \le i \le k$, this one has the smallest value for $1 \le i \le k$. Thus we might expect the sharpest inequality to result. Using (13)–(15) we

get

$$0 \le \sum_{i=1}^{k} (i+1)(k-i)n_i = \sum_{i=1}^{k} \left(-2\binom{i}{2} + ki - k\right)n_i$$
$$= -2\binom{k+q}{2} + k(k+q)(q+1) - (1^2 + q + 1)k$$
$$= q((1-k)^2 - q).$$

This implies $q \le (1 - k)^2$, or $k \ge \sqrt{q} + 1$, completing the proof.

The authors wish to thank A. Dress, N. M. Singhi and S. Sane for helpful comments.

References

- [1] A. Beutelspacher, *Blocking sets and partial spreads in finite projective spaces*, Geom. Dedicata, **9** (1980), 425–449.
- [2] A. A. Bruen, Baer subplanes and blocking sets, Bull. Amer. Math. Soc., 76 (1970), 342-334.
- [3] _____, Blocking sets in finite projective planes, SIAM J. Appl. Math., 21 (1971), 380–392.
- [4] P. Dembowski, Finite Geometries, Springer, Berlin, 1968.
- [5] G. L. Ebert, A New Lower Bound for msp Spreads, Pros. of the 10th Conference on Combinories, Graph Theory and Computing, April 7–6, 1979, Florida Atlantic University.
- [6] D. G. Glynn, A lower bound for maximal partial spreads in PG(3, q), Ars Comb., 13 (1982), 39–40.

Received September 12, 1984.

UNIVERSITY OF CALIFORNIA LOS ANGELES, CA 90024