JOURNAL OF COMBINATORIAL THEORY, Series A 24, 251–253 (1978)

Note

The Blocking Number of an Affine Space

A. E. BROUWER AND A. SCHRIJVER

Stichting Mathematisch Centrum, 2e Boerhaavestraat 49, Amsterdam 1005, Holland

Communicated by the Managing Editors

Received October 18, 1976

It is proved that the minimum cardinality of a subset of $AG(k, q)$ which intersects all hyperplanes is $k(q-1)+1$. In case $k = 2$ this settles a conjecture of J. Doyen.

Doyen [1] proved that the minimum cardinality of a subset of PG$(2, q)$ intersecting all lines equals $q + 1$, where this minimum is attained only if such a subset is a line. He also showed that in each affine plane AG$(2, q)$ there is a subset of cardinality $2q - 1$, intersecting all lines (by taking, e.g., the union of two intersecting lines). He conjectured that for all values of q there is no subset of AG$(2, q)$, intersecting all lines and with fewer than $2q - 1$ points, and verified this conjecture for $q \leqslant 5$. Hansen and Lorea [2] proved it for $q = 7$ by exhaustive computer search, and below we prove the conjecture for all q. This same result has been obtained by R. E. Jamison [3], but with a rather long and involved proof. He proves more than we do, viz.:

> Let V be a vector space of dimension n over a finite field F with q elements. If $0 < k < n$, then any covering of $V^\times$ with nonzero k-flats contains at least $q^{n-k} - 1 + k(q-1)$ k-flats. Furthermore, a covering with this number of k-flats is always possible.

The theorem below is the special case $k = n - 1$.

THEOREM. *Let* AG(k, q) *be the k-dimensional affine space over* GF(q). *Then the minimum cardinality of a subset of* AG(k, q) *which intersects all hyperplanes is* $k(q-1)+1$.

(Note that we do not have any results on non-Desarguesian affine planes.)

Proof. Let q be a prime-power and let AG(k, q) be the k-dimensional affine space over GF(q). We first observe that there is always a subset of

0097-3165/78/0242–0251$02.00/0
Copyright © 1978 by Academic Press, Inc.
All rights of reproduction in any form reserved.

cardinality $k(q-1)+1$ intersecting all hyperplanes. For the union of k independent lines through one given point intersects all hyperplanes and has cardinality $k(q-1)+1$. Secondly suppose $A \subset \mathrm{AG}(k, q)$ intersects all hyperplanes. We may suppose that $0 = (0,..., 0) \in A$; let $B = A\backslash\{0\}$. Then B intersects all hyperplanes not through 0. A hyperplane not through 0 is determined by an equation

$$w_1x_1 + \cdots + w_kx_k = 1,$$

for some $w_1,..., w_k$ in GF(q), not all zero. Hence for all $(w_1,..., w_k) \neq 0$ there exists a $b = (b_1,..., b_k)$ in B such that $w_1b_1 + \cdots + w_kb_k = 1$. Therefore, if we let

$$F(x_1,..., x_k) = \prod_{b\in B} (b_1x_1 + \cdots + b_kx_k - 1),$$

then $F(w_1,..., w_k) = 0$ for all k-tuples $(w_1,..., w_k) \neq 0$.

Now (as one easily proves by induction on k) if $P(x_1,..., x_k)$ is a polynomial which only assumes the value zero then $P(x_1,..., x_k) \in (x_1^q - x_1,..., x_k^q - x_k)$, that is, there are polynomials $P_i(x_1,..., x_k)$ (for $i = 1,..., k$) such that

$$P(x_1,..., x_k) = P_1(x_1,..., x_k)(x_1^q - x_1) + \cdots + P_k(x_1,..., x_k)(x_k^q - x_k).$$

Now let

$$F(x_1,..., x_k) = F_1(x_1,..., x_k)(x_1^q - x_1) + \cdots + F_k(x_1,..., x_k)(x_k^q - x_k) + J(x_1,..., x_k),$$

such that the highest degree of x_i in $J(x_1,..., x_k)$ is at most $q-1$ $(1 \leqslant i \leqslant k)$. Since for each $i = 1,..., k$ the polynomial $x_iF(x_1,..., x_k)$ only assumes the value zero, also for each $i = 1,..., k$ the polynomial $x_iJ(x_1,..., x_k)$ only assumes the value zero. Applying the above mentioned theorem and using the fact that the highest degree of each x_i in $J(x_1,..., x_k)$ is at most $q-1$, it follows that for each $i = 1,..., k$:

$$(x_i^{q-1} - 1) \mid J(x_1,..., x_k),$$

or

$$\prod_{i=1}^{k} (x_i^{q-1} - 1) \mid J(x_1,..., x_k).$$

Since $F(0,..., 0) \neq 0$ and hence $J(0,..., 0) \neq 0$, it follows that the degree of $J(x_1,..., x_k)$ is $k(q-1)$. This implies that the degree of $F(x_1,..., x_k)$ is at least $k(q-1)$. Now, by definition, the degree of $F(x_1,..., x_k)$ equals $|B|$. Hence $|B| \geqslant k(q-1)$ and $|A| \geqslant k(q-1)+1$, proving the theorem. ∎

REFERENCES

1. J. DOYEN, Lecture at Oberwolfach, May 1976.
2. P. HANSEN AND M. LOREA, Le nombre de transversalité du plan affin à 49 sommets, *in* "Analyse appliquée et informatique," (J.-C. Bermond and R. Cori, eds.), pp. 201–209, Bordeaux 1975.
3. R. E. JAMISON, Covering finite fields with cosets of subspaces, *J. Combinatorial Theory Ser. A* **22** (1977), 253–266.

Printed in Belgium