stichting
mathematisch
centrum

MC

DEPARTMENT OF PURE MATHEMATICS ZN 64/76 JUNE

A.E. BROUWER & A. SCHRIJVER

THE BLOCKING NUMBER OF AN AFFINE SPACE

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

AMS(MOS) subject classification scheme (1970): 05B25, 05B40

The blocking number of an affine space

by

A.E. Brouwer & A. Schrijver

ABSTRACT

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

KEY WORDS & PHRASES: *affine space, blocking*

J. DOYEN [1] proved that the minimum cardinality of a subset of PG(2,n) intersecting all lines equals n + 1, where this minimum is attained only if such a subset is a line. He also showed that in each affine plane AG(2,n) there is a subset of cardinality 2n - 1, intersecting all lines (by taking e.g. the union of two intersecting lines) and that for some small values of n there are no such subsets with fewer points. He conjectured that for all values of n there is no subset of AG(2,n), intersecting all lines and with fewer than 2n - 1 points. This is shown by the following theorem.

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

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

<u>PROOF</u>. Let n be a prime-power and let AG(k,n) be the k-dimensional affine space over GF(n). We first observe that there is always a subset of cardinality k(n-1) + 1 intersecting all hyperplanes. For the union of k independent lines through one given point intersects all hyperplanes and has cardinality k(n-1) + 1. Secondly suppose $A \subset AG(k,n)$ intersects all hyperplanes. We may suppose that $\underline{0} = (0, \ldots, 0) \in A$; let $B = A \backslash \{\underline{0}\}$. Then B intersects all hyperplanes not through $\underline{0}$. A hyperplane not through $\underline{0}$ is determined by an equation

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

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

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

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

Now a well-known theorem says that if $P(x_1, \ldots, x_k)$ is a polynomial which only assumes the value zero then $P(x_1, \ldots, x_k) \in (x_1^n-x_1, \ldots, x_k^n-x_k)$, that is, there are polynomials $P_i(x_1, \ldots, x_k)$ (for i = 1, ..., k) such that

$$P(x_1,\ldots,x_k) = P_1(x_1,\ldots,x_k)(x_1^n-x_1) + \ldots\ldots + P_k(x_1,\ldots,x_k)(x_k^n-x_k).$$

Now let

$$F(x_1,\ldots,x_k) = F_1(x_1,\ldots,x_k)(x_1^n-x_1) + \ldots\ldots + F_k(x_1,\ldots,x_k)(x_k^n-x_k) + J(x_1,\ldots,x_k),$$

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

$$(x_i^{n-1}-1) \mid J(x_1,\ldots,x_k),$$

or

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

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

REFERENCE

[1] DOYEN, J., *lecture at Oberwolfach*, May 1976.