On multiple nuclei and a conjecture of Lunelli and Sce

A. Blokhuis

Dedicated to J. A. Thas on his fiftieth birthday

Abstract

We obtain new lower bounds on the size of a t-fold blocking set in $\mathrm{AG}(2,q)$, in the case that $(t,q)=1$. As a consequence, we get that the Lunelli-Sce conjecture on the maximal size of a (k,n)-arc is true in the affine plane.

1 Introduction

Let $\mathcal{A}=\mathrm{AG}(2,q)$ be the desarguesian affine plane of order q. A *nucleus* of a set S of $q+1$ points of $\mathcal{A}$, is a point $P\notin S$, with the property, that every line through P meets the set S (exactly once). The main result [4] is, that a $(q+1)$-set has at most $q-1$ nuclei. The only known examples of sets having this number of nuclei, are a set consisting of a line together with a point outside, and a sporadic example in the plane of order 5, where the 10 points of a Desargues configuration can be partitioned into sets of size 6 and 4, where the second set consists precisely of the nuclei of the first. It appears to be a difficult problem, to characterize the sets S with exactly this number of nuclei. Partial results in this direction were obtained in [3].

In [2], the notion of nucleus was extended to arbitrary sets. Here P is a (generalized) nucleus of S, if $P\notin S$, and every line through P contains a point of S. The main result was, that a set of size $q+k$ has at most $k(q-1)$ nuclei, and again this result is best possible (for $k<q$). As a corollary of this result, one obtains the

Received by the editors in February 1994
AMS Mathematics Subject Classification: Primary 51E21, Secondary 05B25
Keywords: Nuclei, t-fold blocking set, (k,n)-arcs.

lower bound $2q-1$ for the size of a blocking set, a result conjectured by Doyen [8], and proved first by Jamison [10] and independently by Brouwer and Schrijver [5]. A set S is a *blocking set* if every line contains at least one point of S. Hence if S is a blocking set, all other points are nuclei of S.

Using essentially the methods of Jamison and Brouwer-Schrijver, Bruen [6] obtained the lower bound $(t+1)q-t$, for the size of *t-fold blocking set*, that is a set intersecting every line at least t times. For certain pairs (t,q), this bound is again sharp. It seemed therefore natural to expect, that this bound also would follow as a corollary from a more general result on multiple nuclei. It is a bit surprising that this only works if $(t,q)=1$, more surprising is, that the bound we get is essentially better, namely $(t+1)q-1$.

2 Multiple nuclei

Let S be a collection of points in $\mathcal{A}=\mathrm{AG}(2,q)$. A point $P\notin S$ is called a *t-fold nucleus* of S, if every line through P meets the set S in at least t points. In order to possess a t-fold nucleus, the set S obviously has to have at least $t(q+1)$ points. The following theorem gives an upper bound on the number of t-fold nuclei of a set. Here p denotes the characteristic of $\mathrm{GF}(q)$.

Theorem 2.1 *The number of t-fold nuclei of a set S of $t(q+1)+k-1$ points in $AG(2,q)$, is at most $k(q-1)$, provided that $\binom{t+k-1}{k}\neq 0 \bmod p$.*

Proof. We restrict to the case $k<q$, since otherwise everything is obvious. We may identify the points of $\mathcal{A}$ with the elements of $\mathrm{GF}(q^2)$ in a suitable way. Through every point of $\mathcal{A}$ there are $q+1$ lines, one from each parallel class. There is a natural correspondence between the $q+1$ different parallel classes, and the $(q+1)$-st roots of unity in $\mathrm{GF}(q^2)$. For two points a and b, the direction of the line joining them corresponds to the value of $(a-b)^{q-1}$.

With the set S, considered as a subset of $\mathrm{GF}(q^2)$, we associate the following polynomial in two variables

$$F(X,T)=\prod_{s\in S}(T-(X-s)^{q-1}).$$

Consider now a t-fold nucleus x of S. This means, that every line through x contains at least t points of S. If we consider the multiset

$$\{(x-s)^{q-1}\mid s\in S\},$$

then every $(q+1)$-st root of unity occurs at least t times. This implies that the polynomial $F(x,T)\in\mathrm{GF}(q)[T]$ is divisible by

$$(T^{q+1}-1)^t,$$

whenever x is a t-fold nucleus of S. Let $\sigma_j(X)\in\mathrm{GF}(q)[X]$ denote the j-th elementary symmetric function of the set of polynomials:

$$\{(X-s)^{q-1}\mid s\in S\}.$$

Note that σ_j has degree at most $j(q-1)$, and the degree equals $j(q-1)$, precisely if the binomial coefficient $\binom{|S|}{j}$ doesn't vanish. If the polynomial F is expanded in powers of the variable T, we get

$$F(X,T) = \sum_{j=0}^{|S|} (-1)^j \sigma_j(X) T^{|S|-j}.$$

If we now substitute for the variable X a t-fold nucleus x of S, and use the divisibility property above, we get (with $|S| = t(q+1)+k-1$):

$$F(x,T) = (T^{q+1}-1)^t (T^k + \text{ terms of lower degree }).$$

Expanding this again, we note that the coefficient of $T^{t(q+1)-1}$ is zero, since $k < q$. Since this coefficient equals $(-1)^k \sigma_k(x)$, we see that $\sigma_k(x) = 0$, for all t-fold nuclei x of S. If

$$\binom{t(q+1)+k-1}{k} \neq 0,$$

then $\sigma_k(X)$ has degree $k(q-1)$, and hence the number of t-fold nuclei of S is at most this number. □

If the binomial coefficient vanishes, then it might be that $\sigma_k(X)$ vanishes identically, and we have no conclusion (this indeed may happen).

3 Multiple blocking sets and (k,n)-arcs

Recall that a t-fold blocking set is a set S, meeting every line at least t times. For such a set, every other point of the plane is a t-fold nucleus. Using the result in the previous section, we now can prove the following.

Theorem 3.1 *Let S be a t-fold blocking set in $AG(2,q)$, where $(t,q) = 1$. Then*

$$|S| \geq (t+1)q - 1.$$

Proof. We show that a set of size $(t+1)q - 2 = t(q+1) + q - t - 2$ cannot be a t-fold blocking set. First of all consider the binomial coefficient

$$\binom{q-t-2+t}{q-t-1} = \binom{q-2}{t-1}.$$

It is easily verified, for instance using Lucas' Theorem, that this only vanishes if $p \mid t$, where p is the characteristic of GF(q) (we obviously may assume $t \leq q$). Since $(t,q) = 1$, this is not the case. It follows, that we may apply the bound on the number of t-fold nuclei, and we get that S has at most $k(q-1) = (q-t-1)(q-1)$ nuclei. We now get a contradiction, since

$$(q-t-1)(q-1) + (t+1)q - 2 = q^2 - q + t - 1 < q^2.$$

A (k,n)-*arc* (in $\mathrm{PG}(2,q)$ or $\mathrm{AG}(2,q)$), is a set S of k points with the property, that every line contains at most n points of S. Most authors add the condition, that there should be some line meeting S in exactly n points. There is an obvious relation between (k,n)-arcs and multiple blocking sets: the complement of a (k,n)-arc is a $(q-n)$-fold blocking set of size q^2-k.

It was shown by Barlotti [1], that $k \leq (n-1)q+n$. Equality in the bound is only possible if $n \mid q$. In fact the only known non-trivial examples (that is with $1 < n < q$) meeting the bound with equality are hyperovals and more generally, Denniston arcs [7], with $q = 2^h$, and n an arbitrary divisor of q. It is conjectured [12], that no (non-trivial) examples exist for odd q, but this has only been proved for q a power of 3 and $n = 3$ or $q/3$ [12]. In the case that n does not divide q, that is $(n,q) = 1$ it was shown by Lunelli and Sce [11], that $k \leq (n-1)q+(n-3)$ provided that $n \geq 4$, and $k \leq (n-1)q+(n-4)$ if $n \geq 9$. Moreover they conjectured, that if $(n,q) = 1$ then $k \leq (n-1)q+1$. An infinite sequence of examples realizing this bound (with $n = (q+1)/2$) is provided by the set consisting of the interior points of an irreducible conic, together with one arbitrary point on the conic. Note that this set is in fact contained in the affine plane if we take for the line at infinity a tangent of the conic (not the one at the chosen point of course). Other examples meeting the bound are conics in planes of odd order, and unitals (in planes of square order). This last example is not contained in an affine plane.

In general their conjecture is false, as was shown by Hill and Mason [9]. A typical counterexample, for q a square and $n = q-\sqrt{q}-1$, is the complement of the set of points of two disjoint Baer subplanes. From our bound on t-fold blocking sets in the affine plane however we see that this exactly corresponds to the bound conjectured by Lunelli and Sce. Hence their conjecture is true for affine planes.

References

[1] **A. Barlotti**. Sui $(k,n)_q$-archi di un piano lineare finito. *Boll. Un. Mat. Ital.*, 11, pp. 553–556, 1956.

[2] **A. Blokhuis**. On nuclei and affine blocking sets. Preprint, 1993.

[3] **A. Blokhuis and F. Mazzocca**. On maximal sets of nuclei in $\mathrm{PG}(2,q)$ and quasi-odd sets in $\mathrm{AG}(2,q)$. In J. W. P. Hirschfeld, D. R. Hughes, and J. A. Thas, editors, *Advances in Finite Geometries and Designs*, pages 35–46. Oxford University Press, 1991.

[4] **A. Blokhuis and H. A. Wilbrink**. A characterization of exterior lines of certain sets of points in $\mathrm{PG}(2,q)$. *Geom. Dedicata*, 23, pp. 253–254, 1987.

[5] **A. E. Brouwer and A. Schrijver**. The blocking number of an affine space. *J. Combin. Theory Ser. A*, 24, pp. 251–253, 1978.

[6] **A. A. Bruen**. Polynomial multiplicities over finite fields and intersection sets. *J. Combin. Theory (A)*, 60, pp. 19–33, 1992.

[7] **R. H. F. Denniston**. Some maximal arcs in finite projective planes. *J. Combin. Theory*, 6, pp. 317–319, 1969.

[8] **J. Doyen**. Lecture in Oberwolfach, 1976.

[9] **R. Hill and J. M. Mason**. On (k, n)-arcs and the falsity of the Lunelli-Sce conjecture. In *Finite Geometries and Designs*, volume 49 of *L. M. S. Lecture Note Series*, pages 153–168, 1980.

[10] **R. Jamison**. Covering finite fields with cosets of subspaces. *J. Combin. Theory Ser. A*, 22, pp. 253–266, 1977.

[11] **L. Lunelli and M. Sce**. Considerazioni arithmetiche e risultati sperimentali sui $\{K; n\}_q$-archi. *Ist. Lombardo Accad. Sci. Rend. A*, 98, pp. 3–52, 1964.

[12] **J. A. Thas**. Some results concerning $\{(q+1)(n-1); n\}$–arcs and $\{qn-q+n; n\}$–arcs in finite projective planes of order q. *J. Combin. Theory Ser. A*, 19, pp. 228–232, 1975.

Aart Blokhuis
Techn. University Eindhoven
P.O. Box 513
5600 MB Eindhoven
The Netherlands.