On nuclei and blocking sets in Desarguesian spaces

Simeon Ball *
Technische Universiteit Eindhoven,
5600 MB Eindhoven,
The Netherlands.

Abstract

A generalisation is given to recent results concerning the possible number of nuclei to a set of points in $PG(n, q)$. As an application of this we obtain new lower bounds on the size of a t-fold blocking set of $AG(n, q)$ in the case $(t, q) > 1$.

1. Introduction

Let $\Pi_n = PG(n, q)$ be the n-dimensional Desarguesian projective space of order q and let $\mathcal{A}_n = AG(n, q)$ be the n-dimensional Desarguesian affine space of order q. Let $\mathcal{S}$ be a subset of the points of Π_n. A point P of $\Pi_n \setminus \mathcal{S}$ is a *t-fold nucleus* of $\mathcal{S}$ if every line through P meets at least t points of $\mathcal{S}$. This definition is consistent with [8] where some background results concerning nuclei appear for $n = 2$ and $t = 1$ in Section 13.7, and general t in Section 13.8. For general n the definition follows Sziklai [10]. Let $\mathcal{N}^t(\mathcal{S})$ denote the set of t-fold nuclei of $\mathcal{S}$. A 1-fold nucleus is called a nucleus. Recall that a set $\mathcal{S}$ is a *t-fold blocking set* if every line contains at least t points of $\mathcal{S}$ or, equivalently, the set $\mathcal{S} \cup \mathcal{N}^t(\mathcal{S})$ contains every point. A 1-fold blocking set is a blocking set. For a detailed background on blocking sets, multiple blocking sets and nuclei in $\mathcal{A}_2$ and Π_2, see [8].

The main result of [1] is that a $(q+1)$-set in $\mathcal{A}_2$ has at most $q-1$ nuclei. The only known examples of sets that have this number of nuclei are a set consisting of a line together with a point, and a sporadic example in $AG(2, 5)$, where the 10 points of a Desargues configuration can be partitioned into a set of size 6 and 4 nuclei. It remains an intriguing problem to characterise the sets $\mathcal{S}$ of size $q+1$ having exactly $q-1$ nuclei. Partial results in this direction appear in [2].

In [3] it is shown that a $(q+k)$-set in $\mathcal{A}_2$ has at most $k(q-1)$ nuclei, and as a consequence of this that a blocking set in $\mathcal{A}_2$ has at least $2q-1$ points, a result proved originally by Jamison [9] and independently Brouwer and Schrijver [5]. This bound was generalised to $tq + q - t$ for t-fold blocking sets in $\mathcal{A}_2$ by Bruen [6].

The notion of t-fold nucleus was first introduced by Blokhuis in [4], where it was shown that a $(tq + t + k - 1)$-set has at most $k(q-1)$ t-fold nuclei provided that the binomial coefficient $\binom{t+k-1}{k}$ is non-zero modulo p, where p denotes the characteristic of $GF(q)$. It follows directly from this that a t-fold blocking set in $\mathcal{A}_2$ has at least $tq + q - 1$ points

*The author gratefully acknowledges the support of the Australian Research Council Large Grant Scheme. The initial part of this research was carried out at the University of Adelaide and the University of Western Australia.

for $(t,q)=1$. Blokhuis mentions that it is surprising that his nuclei result implies lower bounds for t-fold blocking sets in $\mathcal{A}_2$ for $(t,q)=1$ yet does not appear to imply Bruen's general bound. He states "It seemed therefore natural to expect that this [Bruen's] bound also would follow as a corollary from a more general result on multiple nuclei". In this paper such a general result is given, however, Bruen's bound and the new lower bounds for blocking sets in $\mathcal{A}_2$ follow directly from Blokhuis' result as well. To conclude this introduction we mention that Sziklai [10] has generalised the result in [4]. He concludes that a set $\mathcal{S}$ of size $t\theta_{n-1}+k-1$, with i points lying in some hyperplane $\mathcal{H}$, has at most $k(q-1)$ t-fold nuclei in $\mathcal{A}_n=\Pi_n\setminus\mathcal{H}$, provided that the binomial coefficient $\binom{t\theta_{n-1}+k-i-1}{k}$ is non-zero modulo p. Throughout $\theta_n=(q^{n+1}-1)/(q-1)$, the number of points of Π_n.

2. Multiple nuclei

Let $\mathcal{S}$ be a subset of $t\theta_{n-1}+k-1$ points of Π_n. The points of $\mathcal{A}_n$ can be identified with the elements of $GF(q^n)$ in a suitable way, so that in fact all point sets can be considered as subsets of this field. Note that three points a, b, c are collinear, precisely when $(a-b)^{q-1}=(a-c)^{q-1}$. If the direction of the line joining a and b is identified with the number $(a-b)^{q-1}$, then a one-to-one correspondence between the θ_{n-1} directions (or parallel classes) and the different θ_{n-1}-st roots of unity in $GF(q^n)$ is obtained.

Theorem 2.1 *Suppose there exists a hyperplane $\mathcal{H}$ containing exactly i points of $\mathcal{S}$. The number of t-fold nuclei in $\mathcal{A}_n=\Pi_n\setminus\mathcal{H}$ is at most $(k+r)(q-1)$ provided that the binomial coefficient*

$$\binom{t\theta_{n-1}+k-i-1}{k+r}\neq 0 \pmod p,$$

for some $r\geq 0$.

Proof : We restrict ourselves to the case $(k+r)(q-1)<q^n-(|\mathcal{S}|-i)$, which implies $k+r<\theta_{n-1}$, since otherwise the bound is obvious. Let $\mathcal{S}_{\mathcal{H}}(=\mathcal{S}\setminus\mathcal{H})$ be the points of $\mathcal{S}$ contained in the affine space $\mathcal{A}_n=\Pi_n\setminus\mathcal{H}$ and consider $\mathcal{S}_{\mathcal{H}}$ as a subset of $GF(q^n)$. We assume without loss of generality that 0 is not in $\mathcal{S}$ and is not a t-fold nucleus of $\mathcal{S}$. Let $\delta_1,....,\delta_i\in GF(q^n)$ correspond to the directions of the lines meeting at the i points of $\mathcal{S}$ in $\mathcal{H}$. Note that since the δ_m correspond to directions $\delta_m^{\theta_{n-1}}=1$ or, alternatively, δ_m is a non-zero $(q-1)$-st power.

Define polynomials F in two variables and σ_j in one variable by

$$F(u,x)=\prod_{m=1}^{i}(1-\delta_m x^{q-1}u)\prod_{b\in\mathcal{S}_{\mathcal{H}}}(1-(1-bx)^{q-1}u)=\sum_{j=0}^{t\theta_{n-1}+k-1}(-1)^j\sigma_j(x)u^j,$$

where σ_j is the j-th symmetric function of the set

$$\mathcal{U}=\{\delta_m x^{q-1}|m=1,...,i\}\cup\{(1-bx)^{q-1}|b\in\mathcal{S}_{\mathcal{H}}\}.$$

Note that the degree of the polynomial $\sigma_j(x)$ is at most $j(q-1)$. Let $N^t_{\mathcal{H}}(\mathcal{S})$ denote the set of t-fold nuclei of the set $\mathcal{S}$ contained in the affine space $\Pi_n\setminus\mathcal{H}$ and define $N^t_{\mathcal{H}}(\mathcal{S})^{[-1]}=\{1/x_0|x_0\in N^t_{\mathcal{H}}(\mathcal{S})\}$.

Consider each linear factor of $F(u,x_0)$ where $x_0\in GF(q^n)$. Each one corresponds to the direction of the line joining $1/x_0$ to a point of $\mathcal{S}$. Note that $(1-bx)^{q-1}=x^{q-1}(1/x-b)^{q-1}$ and in each linear term the direction is permuted by x_0^{q-1}.

For every $x_0 \in N_{\mathcal{H}}^t(\mathcal{S})^{[-1]}$ the multi-set $\mathcal{U}$ contains every θ_{n-1} direction (alternatively θ_{n-1}-st roots of unity) repeated at least t times since there are at least t points of $\mathcal{S}$ on every line through the point corresponding to $1/x_0$. Hence

$$F(u,x_0) = (1-u^{\theta_{n-1}})^t.G(u,x_0) = \sum_{j=0}^{t\theta_{n-1}+k-1} (-1)^j \sigma_j(x_0) u^j$$

where $G(u,x_0)$ is a polynomial of degree $k-1$ in u. The shape of $F(u,x_0)$ implies that the polynomial σ_{k+r} is zero for all $x_0 \in \mathcal{N}_{\mathcal{H}}^t(\mathcal{S})^{[-1]}$ under the assumption that $k+r < \theta_{n-1}$. Hence if $|\mathcal{N}_{\mathcal{H}}^t(\mathcal{S})| > (k+r)(q-1)$ then $\sigma_{k+r} \equiv 0$, since it has degree at most $(k+r)(q-1)$ by definition.

However

$$F(u,0) = (1-u)^{t\theta_{n-1}+k-i-1}$$

and so $\sigma_{k+r}(0)$ is non-zero, and hence σ_{k+r} is not identically zero, whenever

$$\binom{t\theta_{n-1}+k-i-1}{k+r} \neq 0 \pmod{p}.$$

□

3. Affine blocking sets

Recall that a t-fold blocking set in $\mathcal{A}_n$ is a subset $\mathcal{S}$ of points meeting every line of $\mathcal{A}_n$ at least t times. An application of the previous theorem with $i=r=0$ allows us to prove the following theorem. For $(t,q)=1$ this bound can be found in Sziklai [10].

Theorem 3.1 *Let $\mathcal{S}$ be a t-fold blocking set of $\mathcal{A}_n$ and let $e(t)$ be maximal such that $p^{e(t)}|t$. Then the set $\mathcal{S}$ has at least $(t+1)q^{n-1} - p^{e(t)}$ points.*

Proof : Put $k = q^{n-1} - t\theta_{n-2} - p^{e(t)}$ and write $t = \gamma p^{e(t)}$ such that $p \not| \gamma$. Consider the binomial coefficient

$$\binom{t\theta_{n-1}+k-1}{k} = \binom{t\theta_{n-1}+k-1}{t\theta_{n-1}-1} = \binom{tq^{n-1}+q(q^{n-2}-1)+q-p^{e(t)}-1}{tq^{n-1}+tq^{n-2}+....+tq+t-1}.$$

A simple application of Lucas' Theorem implies that this binomial coefficient is non-zero precisely when

$$\binom{q-p^{e(t)}-1}{\gamma p^{e(t)}-1} = \binom{q-2p^{e(t)}+p^{e(t)}-1}{(\gamma-1)p^{e(t)}+p^{e(t)}-1} = \binom{q/p^{e(t)}-2}{\gamma-1} \pmod{p}$$

is non-zero, and it is non-zero since $\gamma \neq 0$ mod p. Hence $\mathcal{S}$ cannot be a t-fold blocking set when $k = q^{n-1} - t\theta_{n-2} - p^{e(t)}$ since $\mathcal{S}$ has at most $k(q-1)$ t-fold nuclei and

$$t\theta_{n-1}+k-1+k(q-1) = t\theta_{n-1}+kq-1 =$$

$$(q^{n-1}-t\theta_{n-2}-p^{e(t)})q + t\theta_{n-1} - 1 = q^n + t - p^{e(t)}q - 1 < q^n.$$

□

Hence for $n=2$ we have proved both the previous lower bounds due to Bruen and Blokhuis. It is worth noting however that we have used Theorem 2.1 only in the case $i=r=0$ which for $n = 2$ is precisely Blokhuis' result on multiple nuclei. The new lower bounds occur for all t such that $(t, q) > 1$ and $t \neq p^e$ for some e. Finally we note that in $AG(2, 2^h)$ the bound is sharp when $t = q - 2^e$. Consider a $(q^2 - 2^e q + q - 2^e)$-set $\mathcal{S}$, the complement of which is a $(2^e q - q + 2^e, 2^e)$-(maximal) arc. A construction due to Denniston [7] implies the existence of such sets for all e. It follows immediately that $\mathcal{S}$ is a $(q - 2^e)$-fold blocking set of $\mathcal{A}_2$ attaining the bound.

References

[1] A. Blokhuis and H. Wilbrink, A characterisation of exterior lines of certain sets of points in $PG(2, q)$, *Geometriae Dedicata*, **23**, (1987), 253–254.

[2] A. Blokhuis and F. Mazzocca, On maximal sets of nuclei in $PG(2, q)$ and quasi-odd sets in $AG(2, q)$. 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.

[3] A. Blokhuis, On nuclei and affine blocking sets, *J. Combin. Theory Ser. A*, **67**, (1994), 273–275.

[4] A. Blokhuis, On multiple nuclei and a conjecture of Lunelli and Sce, *Bull. Belg. Math. Soc.*, **3**, (1994), 349–353.

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

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

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

[8] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second Edition, Clarendon Press, Oxford, 1997.

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

[10] P. Sziklai, Nuclei of point sets in $PG(n, q)$, *Discrete Math.*, **174**, (1997), 323-327.