Nuclei in Projective Planes

F. Mazzocca

Socrates Intensive Course
Finite Geometry and its Applications
Ghent, 3–14 April 2000

1 Definition and examples

Definition 1.1 *Let B be a set of $q+1$ points in $\mathsf{PG}(2,q)$. A point $a \notin B$ is said to be a* nucleus *of B if every line through a meets B. The set of all nuclei of B is denoted by $\mathcal{N}(B)$.*

Clearly, if a is a nucleus of B, then every line through a meets B in exactly one point.

We will start by showing why it is interesting to study nuclei in $\mathsf{PG}(2,q)$. We describe a construction that was used to construct the so called Figueroa planes.

Let π be a projective plane $\mathsf{PG}(2,q)$ and let A be a set of points in π. Suppose we want to construct a new projective plane π' with the same pointset as π. Furthermore we want every line of π intersecting A to be a line of π'. Since we want to obtain a new plane, we have to change some line of π external to A into some new set B of $q+1$ points of π. Since in a plane two lines always intersect, every line meeting A has to meet B. Thus A is a set of nuclei of B, i.e. $A \subseteq \mathcal{N}(B)$. Now take a look at the following theorem.

Theorem 1.2 (Bruen & Thas: q even, [6]; Segre & Korchmáros: every q, [10]) *Let A be an irreducible conic in $\mathsf{PG}(2,q)$. Let B be a set of $(q+1)$ points, $A \cap B = \emptyset$, such that every line meeting A meets B. Then B is an external line to the conic A.*

This theorem shows us that we cannot start with A an irreducible conic and obtain a new plane π'.

Remark 1.3 $\mathcal{N}(B) = \mathsf{PG}(2,q) \setminus B$ iff B is a line. Indeed, if $\mathcal{N}(B) = \mathsf{PG}(2,q) \setminus B$, then B is a blocking set of size $q+1$. It is well known that such a set must be a line. On the other hand, if B is a line, then it is obvious that $\mathcal{N}(B) = \mathsf{PG}(2,q) \setminus B$.

Remark 1.4 If B is not a line, then—by deleting a line missing the set $B \cup \mathcal{N}(B)$—we can work in the plane $\mathsf{AG}(2,q)$.

Problem 1.5 How large can $\mathcal{N}(B)$ be if B is not a line?

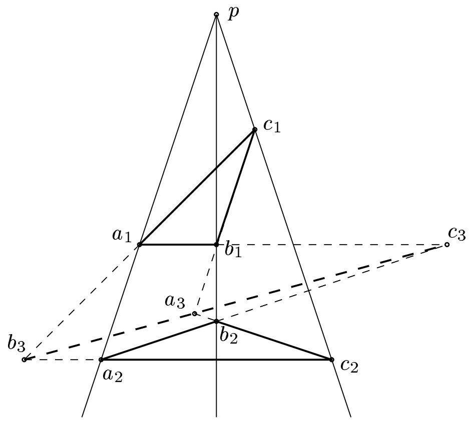

Figure 1: Desargues' configuration.

Since examples are known where $|\mathcal{N}(B)| = q - 1$ (see Examples 1.7 and 1.8), this problem has been solved by the following theorem.

Theorem 1.6 (Blokhuis & Wilbrink, [4]) *If B is not a line, then $\mathcal{N}(B) \leq q - 1$.*

We will prove this theorem later on (see page 3), but first we will look at some more examples.

Example 1.7 Let l be a line in $\mathsf{PG}(2, q)$, c a point on l, and a a point not on l. Then $B = (l \setminus \{c\}) \cup \{a\}$ is a set of $q + 1$ points, and $\mathcal{N}(B) = ac \setminus \{a, c\}$. In this case $|\mathcal{N}(B)| = q - 1$.

Example 1.8 We consider Desargues' configuration in $\mathsf{PG}(2, 5)$ and refer to Figure 1 for the notations. Let $B = \{a_2, b_2, c_2, a_3, b_3, c_3\}$. Then $|B| = q + 1$ and $\mathcal{N}(B) = \{p, a_1, b_1, c_1\}$. As in the previous example, $|\mathcal{N}(B)| = q - 1$.

Examples 1.7 and 1.8 are the only known cases where the bound of Theorem 1.6 is reached. A natural question is the following one.

Problem 1.9 Are there examples different from these two such that $|\mathcal{N}(B)| = q - 1$?

This is a question that is as yet left unanswered.

Remark 1.10 Let q be a square and $\pi = \mathsf{PG}(2, \sqrt{q}) \subset \mathsf{PG}(2, q)$. If $x \in \pi$, then $\sqrt{q} + 1$ lines through x are lines of π, i.e. they intersect π in $\sqrt{q}+1$ points; the other lines through x only contain one point, x, of π. If $x \notin \pi$, then exactly one line through x is a line of π, i.e. intersects π in $\sqrt{q} + 1$ points; the other lines through x only contain one point of π.

Example 1.11 Let q be a square. Let $\pi = \mathsf{PG}(2, \sqrt{q}) \subset \mathsf{PG}(2, q)$ and $x \in \pi$. Let l be a line of π through x. Then $B = (\pi \setminus l) \cup \{x\}$ is a set of $q + 1$ points. Taking into account the properties enumerated in Remark 1.10, it can easily be seen that $\mathcal{N}(B) = l \setminus \pi$. Thus, in this case $|\mathcal{N}(B)| = q - \sqrt{q}$.

Example 1.12 Let q be a square. Let $\pi = \mathsf{PG}(2, \sqrt{q}) \subset \mathsf{PG}(2, q)$ and let l and m be two lines of π. Then $B = (l \setminus \pi) \cup (m \cap \pi)$ is a set of $q+1$ points and $\mathcal{N}(B) = \pi \setminus (l \cup m))$. This implies that $|\mathcal{N}(B)| = \sqrt{q}(\sqrt{q} - 1)$. Note that this construction also holds for an arbitrary subplane π of a given plane $\mathsf{PG}(2, q)$, i.e. π must not be a Baer subplane of a plane $\mathsf{PG}(2, q)$ with q square.

Example 1.13 Let $\pi = \mathsf{PG}(2, q')$ be a subplane of $\mathsf{PG}(2, q)$, and let B' be a set of $q'+1$ points in π. Now consider a line l in $\mathsf{PG}(2, q)$ containing a line of π. Then $B = B' \cup (l \setminus \pi)$ is a set of $q+1$ points and $\mathcal{N}(B) \supseteq \mathcal{N}(B') \setminus l$.

Remark 1.14 A *Rédei blocking set* in $\mathsf{PG}(2, q)$ is a blocking set X of size $q+K$ such that there exists a line that intersects X in exactly K points. For example, consider a set B of $q+1$ points in $\mathsf{PG}(2, q)$, and let l be a line that intersects B in exactly one point. Then $X = B \cup (l \setminus \mathcal{N}(B))$ is a Rédei blocking set.

Example 1.15 Let X be a Rédei blocking set in $\mathsf{PG}(2, q)$. Let $|X| = q + K$ and let l be a line intersecting X in K points, one of which is y. Then $B = (X \setminus l) \cup \{y\}$ is a set of $q+1$ points and $\mathcal{N}(B) \supseteq l \setminus X$. Thus $|\mathcal{N}(B)| \geq q + 1 - K$.

2 Some results

Properties 2.1 In order to prove Theorem 1.6 we need some preliminary results.

1. In $\mathsf{GF}(q^2)$ the equation $X^{q+1} = 1$ has exactly $q+1$ roots $\epsilon_0, \epsilon_1, \ldots, \epsilon_q$.

   $$\Rightarrow \prod_j (X - \epsilon_j) = X^{q+1} - 1 \Rightarrow \epsilon_0 + \epsilon_1 + \ldots + \epsilon_q = 0$$

   If $a \in \mathsf{GF}(q^2)$, $a \neq 0$, then $a^{q-1} = \epsilon_j$ for some j.

2. Since $\mathsf{AG}(2, q) \cong \mathsf{GF}(q^2)$, we can identify the points of $\mathsf{AG}(2, q)$ with elements of the field $\mathsf{GF}(q^2)$. Three points a, b, c are collinear iff $(b - a) = \lambda(c - a)$ for some $\lambda \in \mathsf{GF}(q) \setminus \{0\}$ iff $(b - a)^{q-1} = (c - a)^{q-1}$. Two lines ab and $a'b'$ are parallel, i.e. intersect on the line at infinity l_∞, iff $(b - a)^{q-1} = (b' - a')^{q-1}$.

3. A polynomial $f \in \mathsf{GF}(q)[x_1, \ldots, x_n]$ is called *reduced* iff $\deg_{x_j} f \leq q - 1$, $j = 1, \ldots, n$. For any polynomial g there exists a unique reduced polynomial $\tilde{g}$ and a polynomial h that is everywhere 0 in $\mathsf{GF}(q)$, such that $g = \tilde{g} + h$.

Proof of Theorem 1.6 Suppose $q = p^r$ and $B = \{b_0, b_1, \ldots, b_q\}$ is a set of $q+1$ points in $\mathsf{PG}(2, q)$, B not a line. Let l be a line missing B and $\mathcal{N}(B)$, and let $\mathsf{AG}(2, q)$ be the affine plane obtained by deleting $l = l_\infty$ from π. Consider the polynomial

$$f(x) = \sum_{b \in B} (x - b)^{q-1}$$

over $\mathsf{GF}(q^2)$. Then $\deg f = q-1$, since the coefficient of x^{q-1} is $q+1 \equiv 1 \pmod q$. Now let $a \in \mathcal{N}(B)$. Then

$$f(a) = (a-b_0)^{q-1} + (a-b_1)^{q-1} + \ldots + (a-b_q)^{q-1}.$$

By Property 2.1.1 $(a-b_i)^{q-1} = \epsilon_j$ for some j, but by Property 2.1.2 $(a-b_i)^{q-1} \neq (a-b_k)^{q-1}$ for $i \neq k$. Thus $f(a) = \sum_j \epsilon_j = 0$, such that every nucleus of B is a root of $f(x)$. $\square$

This theorem can be generalized as follows.

Theorem 2.2 $\boxed{\text{ref?}}$ *Let $r(B)$ denote the number of points b in B such that every line through b meets B in $1 \pmod p$ points. Then $|\mathcal{N}(B)| \leq q-1-r(B)$.*

Consider Example 1.11 in the case $q=4$. Let $b=x$. Then every line through b meets B in $1 \pmod 2$ elements, $r(B)=1$, and $|\mathcal{N}(B)| = 4-1-1 = 2$.

Problem 2.3 Find other examples where $r(B) > 0$ and where equality is reached.

We now take another look at Theorem 1.2. One could ask oneself the question whether this is a general property for maximal arcs, "If A is a maximal arc that is a subset of $\mathcal{N}(B)$ for some $(q+1)$-set B, does it follow that B is a line"? The answer is "no". This can be shown by the following counterexample. Let $\epsilon_0, \epsilon_1, \ldots, \epsilon_q$ be defined as in Property 2.1.1, but ordered in such a way that $\epsilon_0 = \omega^0, \epsilon_1 = \omega^1, \ldots, \epsilon_q = \omega^q$, for some generator ω. Call the roots ϵ_{2h+1} odd roots, and the roots ϵ_{2h} even roots. For two odd roots, ϵ_{2i+1} and ϵ_{2j+1}, consider the point of intersection $< \epsilon_{2i+1}, \epsilon_{2j+1} > \cap l_\infty$. Now let

$$B = \{\text{odd roots}\} \cup \{\text{points on } l_\infty \text{ as defined above}\},$$

then the following holds.

Theorem 2.4 (Fisher, [8]) *If $q \geq 9$, $q \equiv 1 \pmod 4$, then—for B as defined above— $|B| = q+1$, $\mathcal{N}(B) = \{$even roots$\} \cup \{$the origin$\}$ and $\mathcal{N}(B)$ is a complete $(q+3)/2$-arc.*

3 The Segre-Korchmáros lemma and its applications

In the proof of Theorem 1.2, Segre and Korchmáros use a lemma that doesn't use the fact that we are dealing with conics.

Lemma 3.1 (Segre-Korchmáros lemma, [10]) *Let a, b, c be the vertices of a triangle contained in $\mathcal{N}(B)$. Then $ab \cap B$, $bc \cap B$ and $ca \cap B$ are collinear.*

Proof Since $|ab \cap B| = 1$, let $ab \cap B = \{c_1\}$. Similarly, let $bc \cap B = \{a_1\}$ and $ca \cap B = \{b_1\}$. Introduce coordinates in the following way: $a = (1,0,0)$, $b = (0,1,0)$ and $c = (0,0,1)$. Then $a_1 = (0,\alpha,1)$, $b_1 = (1,0,\beta)$ and $c_1 = (\gamma,1,0)$ for some $\alpha, \beta, \gamma \neq 0$. Now consider the lines $X_2 = \lambda X_3, \lambda \neq 0$. These are the lines through a different from ac and ab. Similarly we have the lines $X_1 = \nu X_2, \nu \neq 0$ through c different from ac and bc and we have the lines $X_3 = \mu X_1, \mu \neq 0$ through b different from ab and bc. We will simply denote these lines by λ, ν and μ. Three such lines λ, ν and μ are concurrent iff

$$\begin{vmatrix} 0 & 1 & -\lambda \\ -\mu & 0 & 1 \\ 1 & -\nu & 0 \end{vmatrix} = 0 \text{ iff } \lambda\mu\nu = 1.$$

Now let $e \in B \setminus \{a_1, b_1, c_1\}$. Connect e to a, b and c by three lines $\lambda(e)$, $\mu(e)$ and $\nu(e)$. Then

$$-1 = \left(\prod_{\lambda\neq 0} \lambda\right)\left(\prod_{\mu\neq 0} \mu\right)\left(\prod_{\nu\neq 0} \nu\right) = \alpha\beta\gamma \prod_{e\in B, e\neq a_1,b_1,c_1} \lambda(e)\mu(e)\nu(e) = \alpha\beta\gamma.$$

The second equation can be seen as follows. Letting e vary in $B \setminus \{a_1, b_1, c_1\}$, $\lambda(e)$ reaches all values of $\mathsf{GF}(q) \setminus \{\alpha\}$. Similar arguments hold for $\mu(e)$ and $\nu(e)$. Thus

$$0 = \alpha\beta\gamma + 1 = \begin{vmatrix} 0 & \alpha & 1 \\ 1 & 0 & \beta \\ \gamma & 1 & 0 \end{vmatrix},$$

which implies that a_1, b_1 and c_1 are collinear. □

Remark 3.2 It is possible to prove the Blokhuis-Wilbrink theorem, using the Segre-Korchmáros lemma, see page 7.

The following theorem is due to Bruen and gives an upper bound on the number of collinear points in $\mathcal{N}(B)$, using the Segre-Korchmáros lemma.

Theorem 3.3 *Suppose B is not a line and $\mathcal{N}(B)$ contains n points on some line l and at least one point not on l. Then $n \leq \frac{q}{2}$.*

Proof Denote the points of $\mathcal{N}(B)$ on l by $a_1, \ldots, a_n$. As l is a line containing nuclei of B, it meets B in exactly one point, say y. By assumption, there exists a point $x \in \mathcal{N}(B) \setminus l$; for $i = 1, \ldots n$ we denote the unique point $a_i x \cap B$ by b_i. For all $i \neq j$, $i, j \in \{1, \ldots, n\}$, a_i, a_j and x form a triangle of points of $\mathcal{N}(B)$, so the Segre-Korchmáros lemma implies that the points y, b_i and b_j are collinear. Hence we obtain a line $m = yb_1$ with $n+1$ points of B. Now choose a point $b \in B \setminus m$, which exists because B is assumed not to be a line. Then, for $i = 1, \ldots, n$, the line bb_i intersects l in some point a'_i which is not a nucleus of B. Now counting the points on the line l, we obtain n points of $\mathcal{N}(B)$, a unique point $y \in B$ and at least n points $a'_1, \ldots, a'_n$ not belonging to $\mathcal{N}(B)$. Hence n must satisfy $2n + 1 \leq q + 1$, or $n \leq \frac{q}{2}$. □

As an immediate corollary, we find the following.

Corollary 3.4 *If B is not a line and $\mathcal{N}(B)$ contains at least $\frac{q+1}{2}$ collinear points, then all nuclei of B are collinear.*

Now we characterize pairs $(B, \mathcal{N}(B))$ with the property that $\mathcal{N}(B)$ contains a lot of collinear points.

Result 3.5 *If $\mathcal{N}(B)$ contains at least $q-\sqrt{q}$ collinear points, then one of the following possibilities occurs:*

(i) B is a line;

(ii) B consists of q points on a line and one point off this line (see Example 1.7); or

(iii) q is a square and $B=(\pi \setminus l) \cup \{x\}$, where π is a Baer subplane of $\mathsf{PG}(2,q)$, l is a line of π and x is a point of π on l (see Example 1.11).

Proof Suppose l is a line with $l \cap \mathcal{N}(B) = q-n$, $n \leq \sqrt{q}$. The set $S := B \cup (l \setminus \mathcal{N}(B))$ is a set of points meeting every line of $\mathsf{PG}(2,q)$, because a line of $\mathsf{PG}(2,q)$ either meets l in a point of $l \setminus \mathcal{N}(B) \subseteq S$, or in a point of $\mathcal{N}(B)$, in which case the line also meets $B \subseteq S$. If B is not a line nor as described in (ii), S is a non-trivial blocking set of $\mathsf{PG}(2,q)$ and hence $q+1+n = |S| \geq q+\sqrt{q}+1$, so $n \geq \sqrt{q}$. Thus $n=\sqrt{q}$ and $|S| = q+\sqrt{q}+1$, which means that S is a Baer subplane of $\mathsf{PG}(2,q)$. Consequently B is as described in (iii). □

We can also say something about $\mathcal{N}(B)$ if B contains many collinear points.

Result 3.6 *Suppose that B contains $q+1-e$ collinear points, $2 \leq e \leq q-1$. Then $|\mathcal{N}(B)| \leq e(e-1)$ with equality holding if and only if $B = (\pi \cap l) \cup (m \setminus \pi)$ and $\mathcal{N}(B) = \pi \setminus (l \cup m)$ for some subplane π of $\mathsf{PG}(2,q)$ and l, m two different lines of π.*

Proof Let l be the line of $\mathsf{PG}(2,q)$, containing $q+1-e$ points of B, $2 \leq e \leq q-1$. Denote the points of $l \setminus B$ by $x_1, \ldots, x_e$ and the points of $B \setminus l$ by $b_1, \ldots, b_e$. Remark that $\mathcal{N}(B) \cap l = \emptyset$, because l contains at least two points of B. For an arbitrary point $a \in \mathcal{N}(B)$, we consider the lines ab_1 and ab_2; they intersect l in two different points not belonging to B, so in some x_i and x_j $(i \neq j)$. Hence every point of $\mathcal{N}(B)$ is the intersection of b_1x_i and b_2x_j for some pair (x_i, x_j), $i \neq j$. As there are $e(e-1)$ such pairs (x_i, x_j), we have found that $|\mathcal{N}(B)| \leq e(e-1)$.

Now suppose that equality holds, so $|\mathcal{N}(B)| = e(e-1)$. This means that every two lines b_1x_i and b_2x_j, $i \neq j$, intersect in a point of $\mathcal{N}(B)$. By fixing some $i \in \{1, \ldots, e\}$, we see that the line b_1x_i contains exactly $e-1$ points of $\mathcal{N}(B)$. Similarly, every line b_ix_j, $i, j \in \{1, \ldots, e\}$, shares exactly $e-1$ points with $\mathcal{N}(B)$. By means of a counting argument, one shows that the set of points $\mathcal{N}(B) \cup \{x_i \mid i=1,\ldots,e\} \cup \{b_i \mid i=1,\ldots,e\} \cup \{b_1b_2 \cap l\}$ forms a subplane of order e, where Pappus' theorem must be used to show that the points $b_1, \ldots, b_e$ are collinear. This completes the proof. □

Remark 3.7 The extremal configuration of this theorem in case $e=\sqrt{q}$ corresponds to Example 1.12, where a Baer subplane was considered.

We shall now give an alternative proof of the Blokhuis-Wilbrink theorem. So let B be a set of $q+1$ points, B not a line, in $\mathsf{PG}(2,q)=\alpha$. Let l be a line skew to $B \cup \mathcal{N}(B)$. Embed α in $\mathsf{PG}(3,q)$, and consider a point $v \in \mathsf{PG}(3,q) \setminus \alpha$. Call Γ_v the cone $< v, \mathcal{N}(B) >$,

projecting the set $\mathcal{N}(B)$ from v. Define C_v as $\Gamma_v \setminus (\mathcal{N}(B) \cup \{v\})$.
We define a relation $\sim$ on C_v in the following way: $x \sim y$ if either $x = y$ or if the line xy meets α in a point of B.

Lemma 3.8 *The relation $\sim$ defined above is an equivalence relation.*

Proof The relation is clearly reflexive and symmetric, we prove the transitivity. Assume $x \sim y$ and $y \sim z$. We may assume that x, y, z are three different points. If x, y, z are collinear, then this line meets B, hence $x \sim z$. If x, y, z form a triangle, then call x' (resp. y', z') the projection of x (resp. y, z) from v onto α. Since $x \sim y$, we have $x'y' \cap xy \in B$. Because a line though a point of the nucleus meets B in exactly one point, it follows that $(x'y' \cap xy) = (x'y' \cap B)$. Analogously, we have that $(y'z' \cap yz) = (y'z' \cap B)$. The points x', y', z' form a triangle in $\mathcal{N}(B)$, hence we can apply the Segre-Korchmáros lemma, to see that $x'y' \cap B$, $x'z' \cap B$ and $y'z' \cap B$ are collinear. By the theorem of Desargues, also the points $x'y' \cap xy$, $x'z' \cap xz$ and $y'z' \cap yz$ are collinear. Finally, $(xz \cap \alpha) = (xz \cap x'z')$ is a point on the line through $x'y' \cap xy$ and $y'z' \cap yz$. Hence $xz \cap \alpha = x'z' \cap B \in B$, so $x \sim z$. □

Alternative proof of Theorem 1.6 We use the notations of Lemma 3.8. Since the line through two elements in the same equivalence class of the relation $\sim$ has to meet α, a plane through l, the line in α skew to $B \cup \mathcal{N}(B)$, can contain at most one element of such a class. Since the size of an equivalence class equals $|\mathcal{N}(B)|$, it follows immediately that $|\mathcal{N}(B)| \leq q - 1$. □

Using similar techniques, Mazzocca, et al. $\boxed{\text{ref?}}$ proved the following improvement of the Bruen theorem (Theorem 3.3).

Theorem 3.9 *Assume $|\mathcal{N}(B)| = q - 1$, q is even, and $\mathcal{N}(B)$ contains more than $\frac{q}{4} - 3$ collinear points, then B is as in Example 1.7.*

Let π_q denote a finite projective plane of order q (q not necessarily a prime power). Let n be such that $q = n(n+1)$ (n not necessarily an integer). The following theorem was proved by Wettl [11].

Theorem 3.10 $|\mathcal{N}(B)| \leq n^3 + n^2 + n + 1$.

Problem 3.11 If n is an integer, is the bound $|\mathcal{N}(B)| \leq n^3 + n^2 + n + 1$ sharp?

Finally, we mention an important result which is an immediate corollary of the Segre-Korchmáros lemma.

Result 3.12 *Whenever four nuclei are the vertices of a complete quadrangle whose six sides meet B in distinct points, then either those six points are collinear, or they form, together with the four vertices, the points of a Desargues configuration.*

Proof Immediate. □

4 Sets with the maximal number of nuclei

We shortly recall the result of Blokhuis and Wilbrink (Theorem 1.6), which says that if B is not a line, then $|\mathcal{N}(B)| \leq q-1$. In this section, we investigate sets B for which this upper bound is reached.

Theorem 4.1 (Blokhuis & Mazzocca, [2]) *Suppose that B is set of $q+1$ points in $\mathsf{PG}(2,q)$, $q = p^r$ for some prime p. If B is not a line and $|\mathcal{N}(B)| = q-1$, then no line intersects $B \cup \mathcal{N}(B)$ in $1 \pmod p$ points.*

Proof Let l be a line of $\mathsf{PG}(2,q)$. We consider two cases: (i) l intersects B in $k > 1$ points; (ii) l intersects B in one point.
(i) $|l \cap B| = k > 1$
We want to show that $k \not\equiv 1 \pmod p$, so assume that in fact $k \equiv 1 \pmod p$. As $l \cap \mathcal{N}(B) = \emptyset$, we can consider the affine plane $\mathsf{AG}(2,q) = \mathsf{PG}(2,q) \setminus l$, which we identify as usual with $\mathsf{GF}(q^2)$. Consider the set $B' := B \setminus (l \cap B) := \{b_1, \ldots, b_{q+1-k}\}$. Define

$$\sigma_m := (-1)^m \sum b_{i_1} b_{i_2} \ldots b_{i_m},$$

where the sum runs over all subsets of m elements of B', and

$$g(x) := \prod_{b \in B'} (x-b) = \sum_{m=0}^{q+1-k} \sigma_m x^{q+1-k-m}.$$

We may assume without loss of generality that we have chosen the origin of $\mathsf{AG}(2,q)$ such that $0 \in B$, so it follows that

$$\sigma_{q+1-k} = (-1)^{q+1-k} \prod_{b \in B'} b = 0,$$

and it also holds that

$$\sigma_{q-k} = (-1)^{q-k} \prod_{b \in B' \setminus \{0\}} b \neq 0. \tag{1}$$

Now we consider another polynomial, namely

$$f(x) := \sum_{b \in B'} (x-b)^{q-1}.$$

We notice two things. First of all, the coefficient of x^{q-1} in $f(x)$ equals $|B'| = q+1-k \equiv 0 \pmod p$, as $k \equiv 1 \pmod p$ by assumption. So, the degree of f is less than $q-1$. Second, for every $a \in \mathcal{N}(B)$, the lines $ab_1, \ldots, ab_{q+1-k}$ meet $l = l_\infty$ in the same points, namely the $q+1-k$ points of $l \setminus B$. Since the value of $(x-b)^{q-1}$ only depends on the direction of the line joining x and b (see Property 2.1.2), there exists a constant c such that $f(a) = \sum_{b \in B'} (a-b)^{q-1} = c$ for all $a \in \mathcal{N}(B)$. Consequently, the polynomial $f(x) - c$ has at least $|\mathcal{N}(B)| = q-1$ roots, which implies that it must be the zero polynomial, since its degree is less than $q-1$. We conclude that $f(x) \equiv c$.
Next, we define

$$\pi_m := \sum_{b \in B'} b^m,$$

then $f(x)$ can be written as

$$f(x) = \sum_{b\in B'} \sum_{m=0}^{q-1} (-1)^m \binom{q-1}{m} b^m x^{q-1-m} = \sum_{m=0}^{q-1} \pi_m x^{q-1-m},$$

because it can be shown (Exercise) that $\binom{q-1}{m} \equiv (-1)^m \pmod p$. From this expression and the fact that $f(x) \equiv c$, we deduce that $\pi_0 = \pi_1 = \ldots \pi_{q-2} = 0$ and $\pi_{q-1} = c$. Finally, we use the Newton formulas which relate π_m and σ_m:

$$\sum_{m=0}^{n-1} \pi_{n-m}\sigma_m + n\sigma_n = 0.$$

For $n = q - k < q - 1$ we obtain:

$$\sum_{m=0}^{q-k-1} \pi_{q-k-m}\sigma_m + (q-k)\sigma_{q-k} = 0.$$

But we also know that $\pi_{q-k-m} = 0$ for $m = 0, 1, \ldots, q-k-1$, so $(q-k)\sigma_{q-k} = 0$. By assumption, $k \equiv 1 \pmod p$, hence $q - k \neq 0$ and $\sigma_{q-k} = 0$ must hold. This contradicts (1).
(ii) $|l \cap B| = 1$
We will not include the proof here; the idea is the same as in the previous case, but one has to apply tricks which make it more complicated. □

Corollaries 4.2 *The previous theorem has two obvious corollaries.*

1. *If $|\mathcal{N}(B)| = q - 1$, the set $B \cup \mathcal{N}(B)$ has no tangents (1-secants).*
2. *If $p = 2$ and $|\mathcal{N}(B)| = q - 1$, $B \cup \mathcal{N}(B)$ is an even set, which means that every line meets $B \cup \mathcal{N}(B)$ in an even number of points. The set $\mathcal{N}(B)$ then has the property that every line of the plane either is external to $\mathcal{N}(B)$, or meets $\mathcal{N}(B)$ in an odd number of points. Sets of points in a projective or affine plane with this property are called* quasi-odd *sets. Concerning quasi-odd sets, we have the following theorem.*

We will discuss quasi-odd sets briefly in the following section.

5 Quasi-odd sets

Theorem 5.1 (Blokhuis & Mazzocca, [2]) *Let A be a quasi-odd set in the Desarguesian $\mathsf{AG}(2, q)$, q even. Then $|A| \leq q - 1$.*

Proof Identify $\mathsf{AG}(2, q)$ with $\mathsf{GF}(q^2)$ and consider the polynomial

$$f(x) = \sum_{a\in A} (x - a)^{q-1}.$$

Suppose that A is not empty, then counting the points of A on all lines through a fixed $a \in A$ yields that $|A|$ is odd. It follows that $f(x)$ is not identically zero, for the coefficient of x^{q-1} equals $|A| \equiv 1 \pmod p$. For $x \in \mathsf{GF}(q^2)$, the value of $(x-a)^{q-1}$ only depends on the direction of the line xa (see Property 2.1.1). If $a \in A$, every direction will occur an even number of times, so $f(a) = 0$ for all $a \in A$. Consequently $|A| \leq \deg(f) = q-1$. □

There are only a few examples known of quasi-odd sets of maximal size; they can all be considered in $\mathsf{PG}(2,q)$ as well as in $\mathsf{AG}(2,q)$:

1. $q-1$ points on a line;
2. $\mathsf{PG}(2,2) \subseteq \mathsf{PG}(2,8)$ or $\mathsf{AG}(2,8)$;
3. $\mathsf{PG}(2,\sqrt{q}) \setminus \mathcal{H} \subseteq \mathsf{PG}(2,q)$ or $\mathsf{AG}(2,q)$, with $\mathcal{H}$ a hyperoval;
4. $\mathsf{PG}(n,2)$ embedded as a linear space in $\mathsf{AG}(2,2^{n+1})$ or in $\mathsf{PG}(2,2^{n+1})$; this example includes (2) as a special case.

Finally, we observe that Theorem 4.1 suggests the following question: given a quasi-odd set A of maximal size in $\mathsf{PG}(2,q)$, is it possible to find some $(q+1)$-set B such that $A = \mathcal{N}(B)$? This problem is still open.

6 Generalizations

The following definition is due to Blokhuis, and is a more general definition of a nucleus than Definition 1.1.

Definition 6.1 *Let B be a set of points in $\mathsf{AG}(2,q)$ (not necessarily of size $q+1$). A point p not in B is called a nucleus of B, if every line through p meets B.*

Remark 6.2 B is a blocking set iff $\mathcal{N}(B) = \mathsf{AG}(2,q) \setminus B$.

Lemma 6.3 *Let $\underline{x} = (x_1, x_2, \ldots, x_{q+n})$ be a sequence of elements in $\mathsf{GF}(q^2)$, where $n \leq q$. Assume the sequence contains all the $(q+1)$-roots of 1. Let $\sigma_n(\underline{x}) := (-1)^n \sum x_{j_1} x_{j_2} \ldots x_{j_n}$, where the sum goes over all n-tuples in $x_1, x_2, \ldots, x_{q+n}$. Then $\sigma_n(\underline{x}) = 0$.*

Proof Assume $x_1, \ldots x_{q+1}$ are the $(q+1)$-roots of 1. Then $(t^{q+1}-1) = \prod_{j=1}^{q+1}(t-x_j)$. Define $F(t)$ as

$$F(t) = \prod_{j=1}^{q+n}(t-x_j) = \sum_{j=0}^{q+n} \sigma_j(\underline{x}) t^{q+n-j}. \tag{2}$$

Hence $\sigma_n(\underline{x})$ is the coefficient of t^q in $F(t)$. Since $(t^{q+1}-1) = \prod_{j=1}^{q+1}(t-x_j)$, we can write $F(t)$ as $(t^{q+1}-1)(t^{n-1}+G(t))$, where $G(t)$ is a polynomial of degree less than $n-1$. Hence the coefficient of t^q in $F(t)$ equals 0. □

We will use the following notation. Let a and b be nonnegative integers, then

$$\binom{a}{b} = \begin{cases} 0 & \text{if } a < b, \\ 1 & \text{if } a = b = 0, \\ \frac{a!}{b!(a-b)!} & \text{if } 1 \leq b \leq a. \end{cases}$$

Lemma 6.4 *For a and b nonnegative integers with p-adic expansions $a = a_0 + a_1p + a_2p^2 + \ldots$ and $b = b_0 + b_1p + b_2p^2 + \ldots + b_np^n$, we have*

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_n}{b_n} \pmod{p}.$$

Proof See [1]. □

Lemma 6.5 *If $q = p^h$, then $\binom{q+n}{n}$ $(n \leq q)$ is not divisible by p.*

Proof This follows immediately from the preceding lemma. □

Theorem 6.6 $\boxed{\text{ref?}}$ *If $|B| = q + n$, $q \geq n > 0$, then $|\mathcal{N}(B)| \leq n(q-1)$.*

Proof Let $B = \{x_1, \ldots, x_{q+n}\}$. Let $F(t) = \sigma_n((t-x_1)^{q-1}, (t-x_2)^{q-1}, \ldots, (t-x_{q+n})^{q-1})$. The coefficient of $t^{n(q-1)}$ in $F(t)$ is equal to $\binom{q+n}{n} \not\equiv 0 \pmod{p}$. Hence F has degree $n(q-1)$. Take a point $p \in \mathcal{N}(B)$ (this represents an element of $\mathsf{GF}(q^2)$), and calculate $F(a)$. Since $(\alpha^{q-1})^{q+1} = 1$ for $\alpha \in \mathsf{GF}(q^2)$, we have by Lemma 6.3 and by Property 2.1.2, that $F(p) = 0$. Hence all nuclei are roots of the polynomial F of degree $n(q-1)$, and the lemma follows. □

Example 6.7 Let B be a set consisting of a line l in $\mathsf{AG}(2,q)$ and n points of $m \setminus l$, where m is a line not parallel to l. Then $\mathcal{N}(B)$ consists of the points (not on B) on the n lines parallel to l, meeting the line m in a point of B. This example reaches equality in Theorem 6.6.

The previous theorem yields a very important result on blocking sets in $\mathsf{AG}(2,q)$. This result was already proved by Jamison [9] and by Brouwer and Schrijver [5].

Corollary 6.8 *Suppose B is a blocking set in $\mathsf{AG}(2,q)$, then $|B| \geq 2q-1$.*

Proof Suppose $|B| = q + n$, then $|\mathcal{N}(B)| = q^2 - q - n \leq n(q-1)$. Hence $n \geq q-1$. □

Example 6.9 The set $\{(x,y)|x = 0 \vee y = 0\} \cup \{(1,1), p\} \setminus \{(0,1),(1,0)\}$ in $\mathsf{AG}(2,q)$, where p is an arbitrary point on the line $< (0,1),(1,0) >$ is a blocking set of size $2q-1$.

7 Further generalizations

Definition 7.1 *An* n-fold nucleus *for a set B is a point such that every line through this point meets B in at least n points.*

Remark 7.2 Work on n-fold nuclei is important for n-fold blocking sets, these are sets such that every line meets the set in at least n points. Interesting work in this area has been done by Szönyi and by Sziklai.

Definition 7.3 *Let B be a set of q^2+q+1 points in* $\mathsf{PG}(3,q)$*. A point $p \notin B$ is a* nucleus *for the set B if every line through p meets the set B.*

Clearly, if a is a nucleus of B, then every line through a meets B in exactly one point.

Remark 7.4

1. $\mathcal{N}(B) = \mathsf{PG}(3,q) \setminus B$ iff B is a plane; from now on we exclude that B is a plane.

2. We have two cases, (1) B is affine, i.e. there is a plane skew to B; then one can prove that $|\mathcal{N}(B)| \leq q-1$ (similar proof as in dimension 2); (2) B is a blocking set w.r.t. planes.

Example 7.5 Consider two planes α and β in $\mathsf{PG}(3,q)$ meeting in a line l, and take a line m in β and a point c in $(\beta \setminus m)$. Let $B = (\alpha \setminus l) \cup (m \setminus l) \cup \{c\}$. Then $\mathcal{N}(B)$ consists of the points on the line $< c, l \cap m >$, different from c and $l \cap m$. In this case B is affine and $|\mathcal{N}(B)| = q-1$.

Theorem 7.6 *Let B be a set of q^2+q+1 points in* $\mathsf{PG}(3,q)$*, B not a plane. If B is a blocking set w.r.t. planes, then $|\mathcal{N}(B)| \leq q(q-1)$.*

Proof There exists a plane π meeting B in less than $q+1$ points (since B is not a plane). Hence there is a line l skew to B. Consider all planes through l. Since B is a blocking set w.r.t. planes, a plane through l contains at least one point of B. Let N be the number of planes through l containing a point of $\mathcal{N}(B)$; such a plane necessarily contains exactly $q+1$ points of B. Hence, we have $|B| = q^2+q+1 \geq q+1+Nq$. This yields $N \leq q$. On the other hand we have $|\mathcal{N}(B)| \leq N(q-1)$, from which the result follows. □

Example 7.7 Consider in the affine plane $\mathsf{AG}(2,q)$ a set B' of size $q+1$, for which $|\mathcal{N}(B')| = q-1$. Embed this affine plane in $\mathsf{PG}(3,q)$ and take a point v outside the projective plane containing $\mathsf{AG}(2,q)$. Let B consist of the points on the cone $< v, B' >$. Then B is a blocking set w.r.t. planes, $\mathcal{N}(B)$ consists of the points on the cone $< v, \mathcal{N}(B') >$ different from v, and $|\mathcal{N}(B)| = q(q-1)$.

Take a set B of points in $\mathsf{PG}(n,q)$. Let L_{n-1} be the set of hyperplanes H, such that $|B \setminus H| \equiv 0 \pmod{p}$. For every integer h, $0 \leq h \leq n-2$, let $L_h(B)$ be the set of all h-dimensional subspaces S such that every hyperplane containing S belongs to L_{n-1}.

Let $L(B) = \cup_{h=0}^{n-1} L_h(B)$.

We say that a subspace is *B-regular*, if it belongs to $L(B)$. We say that B is a *regular set* in $\mathsf{PG}(n,q)$, if all subspaces of $\mathsf{PG}(n,q)$ are B-regular.

Examples 7.8 The following sets are regular sets.

1. An even set in $\mathsf{PG}(2,2^h)$.

2. A subspace (different from a point) in $\mathsf{PG}(n,q)$.

3. A unital in $\mathsf{PG}(2,q^2)$.

4. An ovaloid in $\mathsf{PG}(3,q)$.

Let $F_X = \sum_{\underline{b}\in X}(b_0X_0 + b_1X_1 + b_2X_2 + b_3X_3)^{q-1}$.
Let $G_X = \prod_{\underline{b}\in X}(b_0X_0 + b_1X_1 + b_2X_2 + b_3X_3)$.

Theorem 7.9 (Blokhuis & Mazzocca, [3]) *F_X is the zero-polynomial iff X is regular. G_X has a null polynomial function iff X is a blocking set w.r.t hyperplanes.*

Theorem 7.10 (Blokhuis & Mazzocca, [3]) *If B is not regular, then $|\mathcal{N}(B)| \le q-1$.*

References

[1] Simeon Ball. Multiple blocking sets and arcs in finite planes. *J. London Math. Soc. (2)*, 54(3):581–593, 1996.

[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, New York, Tokyo, 1991. Oxford University Press.

[3] A. Blokhuis and F. Mazzocca. Special point sets in PG(n,q) and the structure of sets with the maximal number of nuclei. *J. Geom.*, 41:33–41, 1991.

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

[5] A. E. Brouwer and A. Schrijver. The blocking number of an affine space. *J. Combinatorial Theory Ser. A*, 24(2):251–253, 1978.

[6] Aiden A. Bruen and Joseph A. Thas. Flocks, chains and configurations in finite geometries. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 59(6):744–748 (1976), 1975.

[7] J. C. Fisher. The nuclei of sets of $q+1$ points in PG$(2,q)$. 1986.

[8] J. Chris Fisher. Conics, order, and k-arcs in AG$(2,q)$ with q odd. *J. Geom.*, 32(1-2):21–39, 1988.

[9] Robert E. Jamison. Covering finite fields with cosets of subspaces. *J. Combinatorial Theory Ser. A*, 22(3):253–266, 1977.

[10] Beniamino Segre and Gabriele Korchmáros. Una proprietà degli insiemi di punti di un piano di Galois caratterizzante quelli formati dai punti delle singole rette esterne ad una conica. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 62(5):613–619, 1977.

[11] F. Wettl. Nuclei in finite non-Desarguesian projective planes. In *Finite geometry and combinatorics (Deinze, 1992)*, pages 405–412. Cambridge Univ. Press, Cambridge, 1993.

F. Mazzocca
Address

Lecture notes by S. Ferret (saferret@cage.rug.ac.be), P. Govaerts (pg@cage.rug.ac.be) and D. Luyckx (dluyck@cage.rug.ac.be). All three work at Ghent University, Department of Pure Mathematics and Computer Algebra, Galglaan 2, 9000 Gent, Belgium.