

A New Lower Bound for the Size of an Affine Blocking Set

Maarten De Boeck

Vakgroep Wiskunde
Universiteit Gent
Flanders, Belgium

maarten.deboeck@ugent.be

Geertrui Van de Voorde

School of Mathematics and Statistics
University of Canterbury
Christchurch, New Zealand

geertrui.vandevoorde@canterbury.ac.nz

Submitted: Apr 25, 2018; Accepted: Nov 8, 2018; Published: Nov 30, 2018

© The authors. Released under the CC BY-ND license (International 4.0).

Abstract

A blocking set in an affine plane is a set of points B such that every line contains at least one point of B . The best known lower bound for blocking sets in non-desarguesian affine planes was derived in the 1980's by Bruen and Silverman. In this note, we improve on this result by showing that a blocking set of an affine plane of order q , $q \geq 25$, contains at least $q + \lfloor \sqrt{q} \rfloor + 3$ points.

Mathematics Subject Classifications: 51E21

1 Introduction and preliminaries

Definition 1. A blocking set in an affine plane \mathcal{A} (or an *affine blocking set*) is a point set B such that every line of \mathcal{A} contains at least one point of B .

In general, little is known about the smallest affine blocking sets, especially when compared to the knowledge about small blocking sets in projective planes (see amongst others [1, 4, 9, 11]). For the classical (desarguesian) affine plane $AG(2, q)$ we have the following result, obtained independently by Jamison and by Brouwer and Schrijver.

Theorem 2 ([3] and [10]). *A blocking set of $AG(2, q)$ has size at least $2q - 1$.*

If an affine blocking set B in a non-desarguesian plane of order q contains a line, then it is easy to see that B contains at least $2q - 1$ points. However, without the assumption that the blocking set contains a line, the bound from Theorem 2 cannot be generalised to non-desarguesian affine planes. This was first noticed in [5] (see also [2]) where it was shown that each of the non-desarguesian affine planes of order 9 admits a blocking set of order 16. More generally, it is shown in [8] that for q square, $q \geq 9$, there exist an affine plane of order q admitting a blocking set of size at most $\frac{4}{3}q + \frac{5}{3}\sqrt{q}$.

The following result by Bruen and Thas gives a lower bound on the size of an affine blocking set.

Theorem 3 ([7, Cor. 2]). *If \mathcal{S} is a blocking set of an affine plane of order q , then*

$$|\mathcal{S}| \geq q + 1 + \frac{\sqrt{4q^3 - 4q + 1} - 1}{2q}.$$

If q is a square, this implies $|\mathcal{S}| \geq q + \sqrt{q} + 1$.

This result was improved by Bruen and Silverman.

Theorem 4 ([6, Theorem 3.1]). *If \mathcal{S} is a blocking set of an affine plane of order $q > 3$, then*

$$|\mathcal{S}| > q + \sqrt{q} + 1.$$

If $q \geq 4$ is a square, this implies $|\mathcal{S}| \geq q + \sqrt{q} + 2$.

We can embed an affine plane \mathcal{A} in a projective plane \mathcal{P} by adding the parallel classes as points and a unique line ℓ_∞ containing precisely these points (the line ‘at infinity’). This process is called *completion*. By adding one point on ℓ_∞ to a blocking set of \mathcal{A} we get a blocking set of \mathcal{P} . Using this correspondence, we can see that the non-square case of the Theorem 4 also follows from the main result of [1].

In this paper, we will prove the following:

Main Theorem. *A blocking set of an affine plane of order q , $q \geq 25$, contains at least $q + \lfloor \sqrt{q} \rfloor + 3$ points.*

Note that all known blocking sets of non-desarguesian affine planes of order $q < 25$ also have size at least $q + \lfloor \sqrt{q} \rfloor + 3$. We mentioned the affine planes of order 9 above. In [8] the construction of a blocking set in an affine plane derived from the Hall plane of order 16 is described: it has size at least 24 and at most 28.

2 The proof of the main theorem

The following lemma will be used in the proof of our main theorem.

Lemma 5. *Let $b > 1$ be an integer and let $k, m \in \mathbb{N}$ be such that $k \equiv m \pmod{b-1}$ and $m < b-1$. If $a_1, \dots, a_b \in \mathbb{N}$ satisfy $\sum_{i=1}^b (i-1)a_i = k$, then $\sum_{i=1}^b (b-i)(i-1)a_i \geq m(b-1-m)$.*

Proof. Let ℓ be an integer such that $k = \ell(b-1) + m$. We first argue that $\sum_{i=1}^b (i-1)^2 a_i \leq \ell(b-1)^2 + m^2$ and that equality is reached if and only if $a_b = \ell$, $a_{m+1} = 1$ and all a_i 's with $i \in \{2, \dots, b-1\} \setminus \{m+1\}$ equal zero. If $a_1, \dots, a_b \in \mathbb{N}$ satisfy $\sum_{i=1}^b (i-1)a_i = k$ and we can find an $a_j \geq 2$ for some $2 \leq j \leq b-1$, then set

$$a'_i = \begin{cases} a_i - 2 & \text{if } i = j \\ a_i + 1 & \text{if } \begin{cases} i = 2j - 1 & \text{if } 2j \leq b \\ i \in \{2j - b, b\} & \text{if } 2j > b \end{cases} \\ a_i & \text{else} \end{cases}.$$

We find that $\sum_{i=1}^b (i-1)a'_i = k$ and that $\sum_{i=1}^b (i-1)^2 a_i < \sum_{i=1}^b (i-1)^2 a'_i$. If $a_1, \dots, a_b \in \mathbb{N}$ satisfy $\sum_{i=1}^b (i-1)a_i = k$ and we can find $a_j, a_{j'} \geq 1$ for $2 \leq j \neq j' \leq b-1$, then set

$$a'_i = \begin{cases} a_i - 1 & \text{if } i \in \{j, j'\} \\ a_i + 1 & \text{if } \begin{cases} i = j + j' - 1 & \text{if } j + j' \leq b \\ i \in \{j + j' - b, b\} & \text{if } j + j' > b \end{cases} \\ a_i & \text{else} \end{cases}.$$

We find that $\sum_{i=1}^b (i-1)a'_i = k$ and that $\sum_{i=1}^b (i-1)^2 a_i < \sum_{i=1}^b (i-1)^2 a'_i$. From these arguments the claim follows. Now, we find immediately that

$$\begin{aligned} \sum_{i=1}^b (b-i)(i-1)a_i &= (b-1) \sum_{i=1}^b (i-1)a_i - \sum_{i=1}^b (i-1)^2 a_i \\ &\geq (b-1)k - (\ell(b-1)^2 + m^2) = m(b-1-m). \quad \square \end{aligned}$$

We will prove our main theorem in the dual setting. A line ℓ of a plane Π is said to *cover* a point P if P lies on ℓ . It is now easy to see that the following lemma holds.

Lemma 6. *The dual of an affine blocking set (considered as a subset of the projective plane Π obtained through completion), is a set of lines in the dual of Π , covering all the points but one.*

Definition 7. Let \mathcal{L} be a set of lines of a projective plane \mathcal{P} . A k -*knot* is a point of \mathcal{P} that lies on exactly k lines of \mathcal{L} .

Lemma 8. *Let P be a point of an axiomatic projective plane \mathcal{P} of order q , and let \mathcal{L} be a set of lines in \mathcal{P} such that all points but P are on a line of \mathcal{L} , and P is not. Let k be such that \mathcal{L} has no k' -knot for $k' > k$. Let x_i denote the number of i -knots in \mathcal{P} . Then, for all \bar{k} :*

$$\sum_{i=1}^k (i-1)(\bar{k}-i)x_i = -|\mathcal{L}|(|\mathcal{L}|-1) + \bar{k}|\mathcal{L}|(q+1) - \bar{k}(q^2+q).$$

Proof. We denote the number of i -knots (points on exactly i lines of \mathcal{L}) by x_i , $i = 1, \dots, k$. We do the standard countings: first we count the number of points, then the number of

pairs $\{(P, \ell) \mid P \text{ is a point on the line } \ell \in \mathcal{L}\}$ and finally the number of triples $\{(P, \ell, m) \mid \ell, m \in \mathcal{L}, \ell \neq m, P \text{ a point on } \ell \text{ and } m\}$. We find

$$\sum_{i=1}^k x_i = q^2 + q, \quad \sum_{i=1}^k ix_i = |\mathcal{L}|(q+1), \quad \sum_{i=1}^k i(i-1)x_i = |\mathcal{L}|(|\mathcal{L}|-1).$$

Now we can execute the following calculation:

$$\begin{aligned} \sum_{i=1}^k (i-1)(\bar{k}-i)x_i &= -\sum_{i=1}^k i(i-1)x_i + \bar{k}\sum_{i=1}^k ix_i - \bar{k}\sum_{i=1}^k x_i \\ &= -|\mathcal{L}|(|\mathcal{L}|-1) + \bar{k}|\mathcal{L}|(q+1) - \bar{k}(q^2+q). \quad \square \end{aligned}$$

Lemma 9. *Let P be a point of an axiomatic projective plane \mathcal{P} of order q , $q \geq 9$, and let \mathcal{L} be a set of less than $2q-1$ lines in \mathcal{P} such that all points but P are on a line of \mathcal{L} , and P is not. Let k be such that \mathcal{L} admits a k -knot but no k' -knot for $k' > k$. Then $k < q$, $|\mathcal{L}| \geq q+k$ and $k > \lfloor \sqrt{q} \rfloor$.*

Proof. It is immediate that \mathcal{L} does not admit a $(q+1)$ -knot as the $q+1$ lines through some fixed point cover all points. If \mathcal{L} admits a q -knot R , then \mathcal{L} has to contain at least $q-1$ lines not through R , in order to cover the points of PR different from P and R . So, $|\mathcal{L}| \geq 2q-1$, a contradiction.

Let k be such that \mathcal{L} admits a k -knot, but no k' -knot for $k' > k$, and let K be a k -knot. We may assume that $k \leq q-1$, and so we can find a line ℓ through K not in \mathcal{L} and not through P . Since all points on ℓ different from K are contained in a line of \mathcal{L} and these lines are necessarily different, we have $|\mathcal{L}| \geq q+k$.

If $k \leq \lfloor \sqrt{q} \rfloor$, then it follows from Lemma 8 that

$$\begin{aligned} 0 &\leq \sum_{i=1}^k (i-1)(k-i)x_i = -|\mathcal{L}|(|\mathcal{L}|-1) + k(q+1)(|\mathcal{L}|-q) \\ &\leq -|\mathcal{L}|(|\mathcal{L}|-1) + \lfloor \sqrt{q} \rfloor (q+1)(|\mathcal{L}|-q) \end{aligned}$$

where we used that $|\mathcal{L}|-q \geq k > 0$. We set $|\mathcal{L}| = q + \lfloor \sqrt{q} \rfloor + m$ and we find that

$$\begin{aligned} 0 &\leq -(q^2 - q\lfloor \sqrt{q} \rfloor^2) - m^2 - 2q\lfloor \sqrt{q} \rfloor - 2mq - m\lfloor \sqrt{q} \rfloor + q + \lfloor \sqrt{q} \rfloor + m + mq\lfloor \sqrt{q} \rfloor \\ &\leq (m-2)(q\lfloor \sqrt{q} \rfloor - 2q - \lfloor \sqrt{q} \rfloor - m - 1) - 3q - \lfloor \sqrt{q} \rfloor - 2 \\ &= -(m-2)^2 + (m-2)(q\lfloor \sqrt{q} \rfloor - 2q - \lfloor \sqrt{q} \rfloor - 3) - 3q - \lfloor \sqrt{q} \rfloor - 2 \\ &\leq (m-2)(q\lfloor \sqrt{q} \rfloor - 2q - \lfloor \sqrt{q} \rfloor - 3) - 3q - \lfloor \sqrt{q} \rfloor - 2. \end{aligned}$$

We know that $\lfloor \sqrt{q} \rfloor > \sqrt{q}-1$ and hence $q\lfloor \sqrt{q} \rfloor - 2q - \lfloor \sqrt{q} \rfloor - 3 > q\sqrt{q} - 3q - \sqrt{q} - 2$. We can see that $q\sqrt{q} - 3q - \sqrt{q} - 2 > 0$ for $q \geq 12$ and hence that $q\lfloor \sqrt{q} \rfloor - 2q - \lfloor \sqrt{q} \rfloor - 3 > 0$ for $q \geq 9$. Since $q\lfloor \sqrt{q} \rfloor - 2q - \lfloor \sqrt{q} \rfloor - 3 > 0$ for $q \geq 9$ and $-3q - \lfloor \sqrt{q} \rfloor - 2 < 0$, the previous inequality gives a contradiction for $m \leq 2$. \square

Lemma 10. *Let P be a point of an axiomatic projective plane \mathcal{P} of order q , $q \geq 25$, and let \mathcal{L} be a set of at most $q + \lfloor \sqrt{q} \rfloor + 3$ lines in \mathcal{P} such that all points but P are on a line of \mathcal{L} , and P is not. Let k be such that \mathcal{L} admits a k -knot but no k' -knot for $k' > k$. Then $k > \lfloor \sqrt{q} \rfloor + 1$.*

Proof. Note that $2q - 1 > q + \sqrt{q} + 3 \geq q + \lfloor \sqrt{q} \rfloor + 3$ since $q \geq 7$. From Lemma 9, we know that $k > \lfloor \sqrt{q} \rfloor$. If $k = \lfloor \sqrt{q} \rfloor + 1$, then we have $|\mathcal{L}| \geq q + \lfloor \sqrt{q} \rfloor + 1$. Setting $|\mathcal{L}| = q + \lfloor \sqrt{q} \rfloor + 1 + m$ it follows from Lemma 8 that

$$\begin{aligned} & \sum_{i=1}^{\lfloor \sqrt{q} \rfloor + 1} (i-1)(\lfloor \sqrt{q} \rfloor + 1 - i)x_i \\ &= -q \left(q - \lfloor \sqrt{q} \rfloor^2 \right) + \lfloor \sqrt{q} \rfloor + 1 + m \left((q-1) \lfloor \sqrt{q} \rfloor - q - m \right). \end{aligned} \quad (1)$$

We need to show that for $m = 0$ and $m = 1$, we find a contradiction.

Case 1: $m = 0$.

If $m = 0$ the total contribution of the i -knots, $i > 0$, in the left hand side of (1) equals $\lfloor \sqrt{q} \rfloor + 1 - q \left(q - \lfloor \sqrt{q} \rfloor^2 \right)$. We know that 1-knots and $(\lfloor \sqrt{q} \rfloor + 1)$ -knots contribute zero to this sum, 2-knots and $\lfloor \sqrt{q} \rfloor$ -knots contribute $\sqrt{q} - 1$ to this sum, and all other knots contribute at least $2 \lfloor \sqrt{q} \rfloor - 4$ to this sum. Since $\lfloor \sqrt{q} \rfloor \geq 5$ we have $0 < \lfloor \sqrt{q} \rfloor - 1 < 2 \lfloor \sqrt{q} \rfloor - 4 < 2(\lfloor \sqrt{q} \rfloor - 1)$. We look at the different cases.

- If $\lfloor \sqrt{q} \rfloor + 1 - q \left(q - \lfloor \sqrt{q} \rfloor^2 \right) = 0$, then either $\lfloor \sqrt{q} \rfloor + 1 = 0$ or $\lfloor \sqrt{q} \rfloor + 1 \geq q$, which both lead to a contradiction.
- If $\lfloor \sqrt{q} \rfloor + 1 - q \left(q - \lfloor \sqrt{q} \rfloor^2 \right) = \lfloor \sqrt{q} \rfloor - 1$, then $q \left(q - \lfloor \sqrt{q} \rfloor^2 \right) = 2$, which also leads to contradiction since $q \geq 3$.
- If $\lfloor \sqrt{q} \rfloor + 1 - q \left(q - \lfloor \sqrt{q} \rfloor^2 \right) \geq 2 \lfloor \sqrt{q} \rfloor - 4$, then $q \left(q - \lfloor \sqrt{q} \rfloor^2 \right) + (\lfloor \sqrt{q} \rfloor - 5) \leq 0$. Since both terms are non-negative, it follows that $q = 25$ and there is equality in the assumption. So, in this case we find that there is exactly one 3-knot or exactly one 4-knot, and all other points (different from P) are 1-knots or 6-knots. Say there is a 3-knot P' (the argument for a 4-knot is analogous). We count the tuples (Q, ℓ) with $\ell \in \mathcal{L}$ and Q the intersection point of ℓ and PP' . Reducing modulo 5 we find $1 \equiv |\mathcal{L}| \equiv (25 - 1) \cdot 1 + 3 \equiv 2 \pmod{5}$, a contradiction.

Case 2: $m = 1$.

If $m = 1$ the total contribution of the i -knots, $i > 0$, in the left hand side of (1) equals $q \left(\lfloor \sqrt{q} \rfloor - 1 \right) - q \left(q - \lfloor \sqrt{q} \rfloor^2 \right)$. We know that \mathcal{L} admits a $(\lfloor \sqrt{q} \rfloor + 1)$ -knot, say K . Let ℓ be a line through K and denote the number of i -knots on ℓ by a_i .

If $\ell \notin \mathcal{L}$, then we have $\sum_{i=1}^{\lfloor \sqrt{q} \rfloor + 1} i a_i = q + \lfloor \sqrt{q} \rfloor + 2$ by counting the tuples (Q, n) with Q on n and $n \in \mathcal{L}$. We also have $\sum_{i=1}^{\lfloor \sqrt{q} \rfloor + 1} a_i = q + 1 - \delta$ where $\delta = 0$ if $P \notin \ell$ and $\delta = 1$

if $P \in \ell$. We find $\sum_{i=1}^{\lfloor \sqrt{q} \rfloor + 1} (i-1)a_i = \lfloor \sqrt{q} \rfloor + 1 + \delta$. Using Lemma 5 with $b = \lfloor \sqrt{q} \rfloor + 1$, $k = \lfloor \sqrt{q} \rfloor + \delta + 1$, $m = \delta + 1$, we find that the points on ℓ contribute at least $\lfloor \sqrt{q} \rfloor - 1$ to the sum in (1) if $P \notin \ell$ (so if $\delta = 0$) and that the points on the line KP (so, for $\delta = 1$) contribute at least $2(\lfloor \sqrt{q} \rfloor - 2)$.

If $\ell \in \mathcal{L}$ we have $\sum_{i=1}^{\lfloor \sqrt{q} \rfloor + 1} (i-1)a_i = q + \lfloor \sqrt{q} \rfloor + 1$ by counting the tuples (Q, n) with Q on n and $n \in \mathcal{L} \setminus \{\ell\}$. We now distinguish between two cases.

- (i) If $q + \lfloor \sqrt{q} \rfloor + 1 \not\equiv 0 \pmod{\lfloor \sqrt{q} \rfloor}$, then we find that not all points on $\ell \in \mathcal{L}$ can be 1-knots and $(\lfloor \sqrt{q} \rfloor + 1)$ -knots, hence the points on ℓ contribute at least $\lfloor \sqrt{q} \rfloor - 1$ to the sum in (1). It follows that

$$\begin{aligned} q(\lfloor \sqrt{q} \rfloor - 1) - q(q - \lfloor \sqrt{q} \rfloor^2) &= \sum_{i=1}^{\sqrt{q}+1} (i-1)(\lfloor \sqrt{q} \rfloor + 1 - i)x_i \\ &\geq q(\lfloor \sqrt{q} \rfloor - 1) + 2(\lfloor \sqrt{q} \rfloor - 2), \end{aligned}$$

hence

$$q(q - \lfloor \sqrt{q} \rfloor^2) + 2(\lfloor \sqrt{q} \rfloor - 2) \leq 0,$$

a contradiction since $q > 4$. Note that the contribution of K is necessarily 0 so it does not matter that we counted this point $q + 1$ times.

- (ii) If $q + \lfloor \sqrt{q} \rfloor + 1 \equiv 0 \pmod{\lfloor \sqrt{q} \rfloor}$, then $q = \lfloor \sqrt{q} \rfloor (\lfloor \sqrt{q} \rfloor + \varepsilon) - 1$ for some $\varepsilon \in \{1, 2\}$ since $\lfloor \sqrt{q} \rfloor (\lfloor \sqrt{q} \rfloor + 0) - 1 \leq \sqrt{q}\sqrt{q} - 1 < q$ and $\lfloor \sqrt{q} \rfloor (\lfloor \sqrt{q} \rfloor + 3) - 1 > (\sqrt{q} - 1)(\sqrt{q} + 2) - 1 \geq q$ for $q \geq 9$. Using the previous argument, only looking at lines through K not in \mathcal{L} , we then find

$$\begin{aligned} q(\lfloor \sqrt{q} \rfloor - 1) - q(q - \lfloor \sqrt{q} \rfloor^2) &= \sum_{i=1}^{\sqrt{q}+1} (i-1)(\lfloor \sqrt{q} \rfloor + 1 - i)x_i \\ &\geq (q - \lfloor \sqrt{q} \rfloor - 1)(\lfloor \sqrt{q} \rfloor - 1) + 2(\lfloor \sqrt{q} \rfloor - 2), \end{aligned}$$

hence

$$\begin{aligned} q(q - \lfloor \sqrt{q} \rfloor^2) - (\lfloor \sqrt{q} \rfloor^2 - 2\lfloor \sqrt{q} \rfloor + 3) &\leq 0, \\ \Leftrightarrow \varepsilon \lfloor \sqrt{q} \rfloor^3 + (\varepsilon^2 - 2)\lfloor \sqrt{q} \rfloor^2 - 2(\varepsilon - 1)\lfloor \sqrt{q} \rfloor - 2 &\leq 0 \end{aligned}$$

a contradiction for $\varepsilon \in \{1, 2\}$ since $q \geq 4$. □

Lemma 11. *Let P be a point of an axiomatic projective plane \mathcal{P} of order q , $q \geq 25$, and let \mathcal{L} be a set of lines in \mathcal{P} such that all points but P are on a line of \mathcal{L} , and P is not. Let k be such that \mathcal{L} admits a k -knot but no k' -knot for $k' > k$. Suppose that $k = \lfloor \sqrt{q} \rfloor + 2$ and that \mathcal{L} has size $q + \lfloor \sqrt{q} \rfloor + 2$, then the number of $(\lfloor \sqrt{q} \rfloor + 2)$ -knots is at most 5.*

Proof. We will first prove that there can be at most three $(\lfloor\sqrt{q}\rfloor + 2)$ -knots on a line. Assume that K_1, K_2, K_3, K_4 are four $(\lfloor\sqrt{q}\rfloor + 2)$ -knots on a line; necessarily this line is in \mathcal{L} . The point P is not on ℓ . On the line PK_1 there is precisely one 2-knot T ; the remaining $q - 1$ points are 1-knots. Consider the lines $TK_i, i = 2, 3, 4$. They do not contain the point P , and hence, if TK_i is not a line of \mathcal{L} , all $q - 1$ points, different from T and K_i have to be covered by one of the remaining $q + \lfloor\sqrt{q}\rfloor + 2 - (\lfloor\sqrt{q}\rfloor + 2) - 2 = q - 2$ lines of \mathcal{L} not through T and K_i which is impossible. We conclude that the lines $TK_i, i = 2, 3, 4$ are lines of \mathcal{L} . But this is a contradiction as T is on exactly two lines of \mathcal{L} .

We now prove that $d \leq 5$. Let K_1, \dots, K_6 be six $(\lfloor\sqrt{q}\rfloor + 2)$ -knots. For any $K_i, i = 1, \dots, 6$, we know that there is exactly one 2-knot T_i on the line PK_i . If $i \neq j$, then T_iK_j is a line not containing P , hence, using the same argument as above, T_iK_j is a line of \mathcal{L} . As there are only two lines of \mathcal{L} through $T_i, i = 1, \dots, 6$, one of them contains at least three $(\lfloor\sqrt{q}\rfloor + 2)$ -knots. So, we know that three of the points K_1, \dots, K_6 are collinear, say K_1, K_2 and K_3 , and we denote the line they are on by ℓ . As there are only two lines of \mathcal{L} through a 2-knot we have immediately that $T_i \in \ell$ for $i = 4, 5, 6$. Moreover, the other line of \mathcal{L} through T_i contains K_j and $K_{j'}$ for $\{i, j, j'\} = \{4, 5, 6\}$. Now, the two lines of \mathcal{L} through T_1 must be T_1K_2 and T_1K_3 . Each of the $(\lfloor\sqrt{q}\rfloor + 2)$ -knots K_4, K_5 and K_6 must be on one of these two lines, so one of these two lines contains at least two of them. Say, without loss of generality that K_4 and K_5 are on T_1K_2 . However, then T_6 is also on this line, which implies $T_6 = K_2$ since both points are also on ℓ , a contradiction. \square

Theorem 12. *Let P be a point of an axiomatic projective plane \mathcal{P} of order q , and let \mathcal{L} be a set of lines in \mathcal{P} such that all points but P are on a line of \mathcal{L} , and P is not. If $q \geq 25$, then $|\mathcal{L}| \geq q + \lfloor\sqrt{q}\rfloor + 3$.*

Proof. By Lemma 9, we have that $|\mathcal{L}| \geq q + \lfloor\sqrt{q}\rfloor + 3$ if $k \geq \lfloor\sqrt{q}\rfloor + 3$. By Lemma 10, $k > \lfloor\sqrt{q}\rfloor + 1$. So it follows that we only need to rule out the case $k = \lfloor\sqrt{q}\rfloor + 2$ in order to obtain that $|\mathcal{L}| \geq q + \lfloor\sqrt{q}\rfloor + 3$.

If $k = \lfloor\sqrt{q}\rfloor + 2$, then we know $|\mathcal{L}| \geq q + \lfloor\sqrt{q}\rfloor + 2$ and we may assume that $|\mathcal{L}| = q + \lfloor\sqrt{q}\rfloor + 2$. We set $d = x_{\lfloor\sqrt{q}\rfloor+2}$ for ease of notation. It then follows from Lemma 8 that

$$\sum_{j=1}^{\lfloor\sqrt{q}\rfloor+1} (j-1)(\lfloor\sqrt{q}\rfloor+1-j)x_j = q(\lfloor\sqrt{q}\rfloor-1) - q(q - \lfloor\sqrt{q}\rfloor^2) + d(\lfloor\sqrt{q}\rfloor+1). \quad (2)$$

Now, let K be an i -knot with $4 \leq i \leq \lfloor\sqrt{q}\rfloor$, let $\ell \notin \mathcal{L}$ be a line through K and denote the number of j -knots on ℓ different from K and P by a_j . Then we have $\sum_{j=1}^{\lfloor\sqrt{q}\rfloor+2} ja_j = q + \lfloor\sqrt{q}\rfloor + 2 - i$ by counting the tuples (Q, n) with $\{Q\} = \ell \cap n, Q \neq K$ and $n \in \mathcal{L}$. We also have $\sum_{j=1}^{\lfloor\sqrt{q}\rfloor+2} a_j = q - \delta$ where $\delta = 0$ if $P \notin \ell$ and $\delta = 1$ if $P \in \ell$. We find $\sum_{j=1}^{\lfloor\sqrt{q}\rfloor+2} (j-1)a_j = \lfloor\sqrt{q}\rfloor + 2 - i + \delta$. Moreover, as $\lfloor\sqrt{q}\rfloor + 2 - i + \delta \leq \lfloor\sqrt{q}\rfloor - 1$, we have $\sum_{j=1}^{\lfloor\sqrt{q}\rfloor+1} (j-1)a_j = \lfloor\sqrt{q}\rfloor + 2 - i + \delta$. So we find that the points on $\ell \neq KP$ different from

K contribute at least $(\lfloor \sqrt{q} \rfloor + 2 - i)(i - 2)$ to the sum in (2) by Lemma 5; the points on KP different from K contribute at least $(\lfloor \sqrt{q} \rfloor + 3 - i)(i - 3)$ to the sum in (2). None of these contributions includes the point K , but K itself contributes $(\lfloor \sqrt{q} \rfloor + 1 - i)(i - 1)$ to the sum in (2). We find that

$$\begin{aligned} q(\lfloor \sqrt{q} \rfloor - 1) - q(q - \lfloor \sqrt{q} \rfloor^2) + d(\lfloor \sqrt{q} \rfloor + 1) &= \sum_{j=1}^{\lfloor \sqrt{q} \rfloor + 1} (j - 1)(\lfloor \sqrt{q} \rfloor + 1 - j)x_j \\ &\geq (q - i)(\lfloor \sqrt{q} \rfloor + 2 - i)(i - 2) \\ &\quad + (\lfloor \sqrt{q} \rfloor + 3 - i)(i - 3) \\ &\quad + (\lfloor \sqrt{q} \rfloor + 1 - i)(i - 1). \end{aligned} \quad (3)$$

Hence,

$$\begin{aligned} 0 \geq i^3 - (q + \lfloor \sqrt{q} \rfloor + 6)i^2 + (q \lfloor \sqrt{q} \rfloor + 4q + 4 \lfloor \sqrt{q} \rfloor + 12)i - d(\lfloor \sqrt{q} \rfloor + 1) \\ + q^2 - q \lfloor \sqrt{q} \rfloor^2 - 3q \lfloor \sqrt{q} \rfloor - 3q - 4 \lfloor \sqrt{q} \rfloor - 10. \end{aligned} \quad (4)$$

For $i = 4$ we find, using that $d \leq 5$ from Lemma 11,

$$0 \geq q^2 - q \lfloor \sqrt{q} \rfloor^2 + q \lfloor \sqrt{q} \rfloor - 3q - 4 \lfloor \sqrt{q} \rfloor + 6 - d(\lfloor \sqrt{q} \rfloor + 1) \geq q \lfloor \sqrt{q} \rfloor - 3q - 9 \lfloor \sqrt{q} \rfloor + 1,$$

which is a contradiction for $q \geq 25$. For $i = \lfloor \sqrt{q} \rfloor$ we find, again using that $d \leq 5$ from Lemma 11,

$$\begin{aligned} 0 \geq q^2 - q \lfloor \sqrt{q} \rfloor^2 + q \lfloor \sqrt{q} \rfloor - 3q - 2 \lfloor \sqrt{q} \rfloor^2 + 8 \lfloor \sqrt{q} \rfloor - 10 - d(\lfloor \sqrt{q} \rfloor + 1) \\ \geq q \lfloor \sqrt{q} \rfloor - 3q - 2 \lfloor \sqrt{q} \rfloor^2 + 3 \lfloor \sqrt{q} \rfloor - 15, \end{aligned}$$

which is a contradiction for $q > 25$. Since the right hand side of (4) is function of degree 3 in i it can easily be checked that it is first increasing and then decreasing on the interval $[4, \lfloor \sqrt{q} \rfloor]$ for $q \geq 25$: looking at its derivative we see that the function is decreasing on

$$\left] \frac{q + [q] - \sqrt{q^2 - q[q] + [q]^2}}{3} + 2, \frac{q + [q] + \sqrt{q^2 - q[q] + [q]^2}}{3} + 2 \right[\text{ and}$$

$$4 \leq \frac{q + [q] - \sqrt{q^2 - q[q] + [q]^2}}{3} + 2 \leq [q] \leq \frac{q + [q] + \sqrt{q^2 - q[q] + [q]^2}}{3} + 2.$$

So, the minimum of this function on this interval is to be found at one of its endpoints. So, as we have a contradiction for $i = 4$ and $i = \lfloor \sqrt{q} \rfloor$, we have a contradiction for all i with $4 \leq i \leq \lfloor \sqrt{q} \rfloor$.

For $q = 25$ we did not yet exclude $i = 5$. We find a contradiction in (4) if $0 \leq d \leq 4$, and we have equality in (4) if $d = 5$. In the latter case we also have equality in (3) and hence the points on the lines of \mathcal{L} through the 5-knot K should all contribute zero to the sum in (2). If $\ell \in \mathcal{L}$ through K we have

$$\sum_{j=1}^7 (j - 1)a_j = q + \lfloor \sqrt{q} \rfloor + 2 - i = 27$$

by counting the tuples (Q, n) with $\{Q\} = \ell \cap n$, $Q \neq K$ and $n \in \mathcal{L} \setminus \{\ell\}$. Hence, not all points on ℓ different from K can be 1-knots or 6-knots; more precisely, there should be at least two 7-knots on ℓ . It follows that the total number of 7-knots is at least 10, a contradiction.

So far we have concluded that $x_i = 0$ for all i with $4 \leq i \leq \lfloor \sqrt{q} \rfloor$. Now, let K' be a 3-knot, let $\ell \notin \mathcal{L}$ be a line through K' different from $K'P$ and denote the number of j -knots on ℓ different from K' by a_j . Counting the tuples (Q, n) with $\{Q\} = \ell \cap n$, $Q \neq K'$ and $n \in \mathcal{L}$ and using $\sum_{j=1}^{\lfloor \sqrt{q} \rfloor + 2} a_j = q$ we find $\sum_{j=1}^{\lfloor \sqrt{q} \rfloor + 2} (j-1)a_j = \lfloor \sqrt{q} \rfloor - 1$, but as $a_j = 0$ for all $j = 4, \dots, \lfloor \sqrt{q} \rfloor$, we find that

$$a_2 + 2a_3 + \lfloor \sqrt{q} \rfloor a_{\lfloor \sqrt{q} \rfloor + 1} + (\lfloor \sqrt{q} \rfloor + 1) a_{\lfloor \sqrt{q} \rfloor + 2} = \lfloor \sqrt{q} \rfloor - 1$$

and hence that $a_{\lfloor \sqrt{q} \rfloor + 1} = a_{\lfloor \sqrt{q} \rfloor + 2} = 0$. So, the points on ℓ different from K contribute

$$\begin{aligned} a_2 (\lfloor \sqrt{q} \rfloor - 1) + a_3 (2 (\lfloor \sqrt{q} \rfloor - 2)) &= a_2 (\lfloor \sqrt{q} \rfloor - 1) + \frac{\lfloor \sqrt{q} \rfloor - 1 - a_2}{2} (2 (\lfloor \sqrt{q} \rfloor - 2)) \\ &= a_2 + (\lfloor \sqrt{q} \rfloor - 1) (\lfloor \sqrt{q} \rfloor - 2) \end{aligned}$$

hence at least $(\lfloor \sqrt{q} \rfloor - 1) (\lfloor \sqrt{q} \rfloor - 2)$ to the sum in (2). The point K itself also contributes $2 (\lfloor \sqrt{q} \rfloor - 2)$ to this sum. We find

$$\begin{aligned} q (\lfloor \sqrt{q} \rfloor - 1) - q (q - \lfloor \sqrt{q} \rfloor^2) + d (\lfloor \sqrt{q} \rfloor + 1) &= \sum_{j=1}^{\lfloor \sqrt{q} \rfloor + 1} (j-1) (\lfloor \sqrt{q} \rfloor + 1 - j) x_j \\ &\geq (q-3) (\lfloor \sqrt{q} \rfloor - 1) (\lfloor \sqrt{q} \rfloor - 2) \\ &\quad + 2 (\lfloor \sqrt{q} \rfloor - 2) \\ &= q \lfloor \sqrt{q} \rfloor^2 - 3q \lfloor \sqrt{q} \rfloor + 2q - 3 \lfloor \sqrt{q} \rfloor^2 \\ &\quad + 11 \lfloor \sqrt{q} \rfloor - 10. \end{aligned}$$

So, we have, using Lemma 11, that

$$0 \geq q^2 - 4q \lfloor \sqrt{q} \rfloor + 3q - 3 \lfloor \sqrt{q} \rfloor^2 + 11 \lfloor \sqrt{q} \rfloor - 10 - d (\lfloor \sqrt{q} \rfloor + 1) \geq q^2 - 4q \lfloor \sqrt{q} \rfloor + 6 \lfloor \sqrt{q} \rfloor - 15,$$

which is a contradiction for $q \geq 16$.

So far, we know that $x_i = 0$ for all $i \notin \{1, 2, \lfloor \sqrt{q} \rfloor + 1, \lfloor \sqrt{q} \rfloor + 2\}$. We call the $(\lfloor \sqrt{q} \rfloor + 1)$ -knots and the $(\lfloor \sqrt{q} \rfloor + 2)$ -knots *big knots*. It follows from the standard countings that

$$\begin{cases} x_1 + x_2 + x_{\lfloor \sqrt{q} \rfloor + 1} = q^2 + q - d \\ x_1 + 2x_2 + (\lfloor \sqrt{q} \rfloor + 1) x_{\lfloor \sqrt{q} \rfloor + 1} = (q+1)(q + \lfloor \sqrt{q} \rfloor + 2) - (\lfloor \sqrt{q} \rfloor + 2) d \\ 2x_2 + (\lfloor \sqrt{q} \rfloor + 1) \lfloor \sqrt{q} \rfloor x_{\lfloor \sqrt{q} \rfloor + 1} = (q + \lfloor \sqrt{q} \rfloor + 2)(q + \lfloor \sqrt{q} \rfloor + 1) \\ \quad - (\lfloor \sqrt{q} \rfloor + 2)(\lfloor \sqrt{q} \rfloor + 1) d \end{cases}$$

$$\Leftrightarrow \begin{cases} x_1 = q^2 - q \lfloor \sqrt{q} \rfloor - q - d - 1 + \frac{q^2 - q - 2}{\lfloor \sqrt{q} \rfloor} \\ x_2 = q \lfloor \sqrt{q} \rfloor + 2q + d - \frac{q^2 - q - 2d}{\lfloor \sqrt{q} \rfloor - 1} \\ x_{\lfloor \sqrt{q} \rfloor + 1} = 1 - d + \frac{q^2 - q - 2(d-1) \lfloor \sqrt{q} \rfloor - 2}{\lfloor \sqrt{q} \rfloor (\lfloor \sqrt{q} \rfloor - 1)} \end{cases}$$

Since x_1 is an integer, there must be an integer a such that $q^2 - q - 2 = a \lfloor \sqrt{q} \rfloor$. Since x_2 is an integer too, $q^2 - q - 2d = a \lfloor \sqrt{q} \rfloor - 2(d-1) \equiv 0 \pmod{\lfloor \sqrt{q} \rfloor - 1}$. So, there must be an integer b such that $a = 2(d-1) + b(\lfloor \sqrt{q} \rfloor - 1)$. We find that

$$\begin{cases} x_1 = q^2 - q \lfloor \sqrt{q} \rfloor - q + b \lfloor \sqrt{q} \rfloor + d - 3 - b \\ x_2 = q \lfloor \sqrt{q} \rfloor + 2q - d - b \lfloor \sqrt{q} \rfloor + 2 \\ x_{\lfloor \sqrt{q} \rfloor + 1} = 1 - d + b \end{cases}$$

By counting the tuples (Q, n) with $\{Q\} = \ell \cap n$, $Q \neq P$ and $n \in \mathcal{L}$ and using $\sum_{j=1}^{\lfloor \sqrt{q} \rfloor + 2} a_j = q$ we find that for a line $\ell \ni P$ (necessarily not in \mathcal{L}) we have that $\sum_{j=1}^{\lfloor \sqrt{q} \rfloor + 2} (j-1)a_j = \lfloor \sqrt{q} \rfloor + 2$ with a_j the number of j -knots on ℓ . We see that there can be at most 1 big knot on a line through P . Hence, $d + x_{\lfloor \sqrt{q} \rfloor + 1}$, the number of big knots, is at most $q + 1$. It follows that $b \leq q$. Consequently,

$$q^2 - q - 2 = \lfloor \sqrt{q} \rfloor (2(d-1) + b(\lfloor \sqrt{q} \rfloor - 1)) \leq q \lfloor \sqrt{q} \rfloor^2 - q \lfloor \sqrt{q} \rfloor + 2(d-1) \lfloor \sqrt{q} \rfloor .$$

However, then, using that $d \leq 5$ from Lemma 11,

$$\begin{aligned} 0 &\geq q^2 - q \lfloor \sqrt{q} \rfloor^2 + q \lfloor \sqrt{q} \rfloor - q - 2(d-1) \lfloor \sqrt{q} \rfloor - 2 \\ &\geq (q^2 - q \lfloor \sqrt{q} \rfloor^2) + q(\lfloor \sqrt{q} \rfloor - 1) - 8 \lfloor \sqrt{q} \rfloor - 2 \\ &\geq q(\lfloor \sqrt{q} \rfloor - 1) - 8 \lfloor \sqrt{q} \rfloor - 2 , \end{aligned}$$

which is a contradiction for $q \geq 10$. □

Corollary 13. *A blocking set of an affine plane of order q contains at least $q + \lfloor \sqrt{q} \rfloor + 3$ points if $q \geq 25$.*

Acknowledgements

This research was performed when the first author was visiting the School of Mathematics and Statistics at the University of Canterbury. He wants to thank the School, and in particular the second author, for their hospitality.

References

- [1] J. Bierbrauer. On minimal blocking sets. *Arch. Math. (Basel)* 35(4):394–400, 1980.
- [2] J. Bierbrauer. Mathematical Reviews MR0695804.
- [3] A.E. Brouwer and A. Schrijver. The blocking number of an affine space. *J. Combin. Theory Ser. A* 24:251–253, 1978.
- [4] A. Bruen. Baer subplanes and blocking sets. *Bull. Amer. Math. Soc.* 76:342–344, 1970.
- [5] A.A. Bruen and M.J. de Resmini. Blocking sets in affine planes. *Ann. Discrete Math.*, 18:169–175, 1983. Combinatorics ‘81 (Rome, 1981).
- [6] A.A. Bruen and R. Silverman. Arcs and blocking sets II. *Europ. J. Combin.*, 8:351–356, 1987.
- [7] A.A. Bruen and J.A. Thas. Blocking sets. *Geom. Dedicata*, 6:193–203, 1977.
- [8] J. De Beule, T. Héger, T. Szőnyi, and G. Van de Voorde. Blocking and double blocking sets in finite planes. *Electronic J. Combin.*, 23(2): #P2.5, 2016.
- [9] D.A. Drake. A bound for blocking sets in finite projective planes. Finite geometries and combinatorial designs, 93–97, , vol. 111, Amer. Math. Soc., 1990. Finite geometries and combinatorial designs (Lincoln, NE, 1987).
- [10] R.E. Jamison. Covering finite fields with cosets of subspaces. *J. Combin. Theory Ser. A* 22:253–266, 1977.
- [11] C. Kitto. A bound for blocking sets of Rédei type in finite projective planes. *Arch. Math. (Basel)* 52(2):203–208, 1989.