On the stability of small blocking sets

Tamás Szőnyi and Zsuzsa Weiner *

March 10, 2014

Abstract

A stability theorem says that a nearly extremal object can be obtained from an extremal one by "small changes". In this paper, we study the relation of sets having few 0-secants and blocking sets.

1 Introduction

A *blocking set* is a point set intersecting each line. It is easy to see that the smallest blocking sets of projective planes are lines. A blocking set is *minimal*, when no proper subset of it is a blocking set. For an arbitrary set S of points a line is called an i-secant of S if it meets S in precisely i points. 0-secants and 1-secants will sometimes be called skew lines and tangents, respectively.

Using combinatorial arguments Bruen proved that the second smallest examples of minimal blocking sets of $\mathrm{PG}(2,q)$ have at least $q+\sqrt{q}+1$ points. When q is a square, minimal blocking sets of this size exist; they are the points of a Baer subplane, that is a subplane of order $\sqrt{q}$. In general, minimal blocking sets of size $\frac{3}{2}(q+1)$ always exist in $\mathrm{PG}(2,q)$, see for example [10] and [5].

Before going into details about small blocking sets, let us recall an important result of Jamison [11] and Brouwer and Schrijver [6]: the affine blocking set theorem.

*The authors were partially supported by K 81310 grant. The second author was also supported by the ERC grant No. 227701 DISCRETECONT. The final version was prepared with the help of the MTA-ELTE GAC Research Group.

Result 1.1 (Jamison, Brouwer and Schrijver) *A blocking set in* $\mathrm{AG}(2,q)$ *contains at least* $2q-1$ *points.*

There are lots of interesting results on blocking sets, for a survey see [10], [5]; and [14]. Many of them concentrate on *small* blocking sets of $\mathrm{PG}(2,q)$, these are blocking sets whose cardinality is less than $\frac{3}{2}(q+1)$. In some cases small minimal blocking sets are already characterized.

Result 1.2 (1) (Blokhuis, [1]) *If* $q=p$ *prime, then the small minimal blocking sets in* $\mathrm{PG}(2,p)$ *are lines;*

(2) ([15]) *If* $q=p^2$, p *prime, then the small minimal blocking sets in* $\mathrm{PG}(2,p^2)$ *are lines and Baer subplanes;*

(3) (Polverino, [12]) *If* $q=p^3$, p *prime, then small minimal blocking sets in* $\mathrm{PG}(2,p^3)$ *have size* $q+1$, p^3+p^2+1 *or* p^3+p^2+p+1 *and they are unique.*

In general, it is known that the sizes of small minimal blocking sets can take only certain values.

Result 1.3 ([15]) *The size of a small minimal blocking set in* $\mathrm{PG}(2,q)$, $q=p^h$, p *prime, is* 1 *modulo* p.

There are important improvements on the above result, see Sziklai [13]. Roughly speaking it says that the size of a small minimal blocking set is around $q+\frac{q}{p^e}$ for some e dividing h.

In an earlier paper [17] we studied the stability of lines in $\mathrm{PG}(2,p)$, p prime and obtained the following result.

Result 1.4 *Let* B *be a set of points of* $\mathrm{PG}(2,q)$, $q=p$ *prime, that has at most* $\frac{3}{2}(q+1)-\beta$ *(*$\beta>0$*) points. Suppose that the number of* 0*-secants,* δ *is less than* $(\frac{2}{3}(\beta+1))^2/2$. *Then there is a line that contains at least* $q-\frac{2\delta}{q+1}$ *points.*

Note that for $|B|=cq$, $c\geq 1$ the bound on δ in the above theorem is $c'q^2$.

In Sections 3 and 4, we study the stability of small blocking sets of $\mathrm{PG}(2,q)$, q not a prime. The difference compared to the prime case is that we typically have several inequivalent small minimal blocking sets. The main result of Section 3 is the following theorem.

Theorem 1.5 *Let B be a point set in $\mathrm{PG}(2,q)$, $q \geq 16$, of size less than $\frac{3}{2}(q+1)$. Denote the number of 0-secants of B by δ, and assume that*

$$\delta < \min\left((q-1)\frac{2q+1-|B|}{2(|B|-q)}, \frac{1}{2}(q-\sqrt{q})^{3/2}\right). \tag{1}$$

Then B can be obtained from a blocking set by deleting at most $\frac{\delta}{2q+1-|B|}+\frac{1}{2}$ points of it.

When $|B|$ is relatively far from q and gets closer to $\frac{3}{2}(q+1)$ then the bound on δ gets worse. Therefore, the aim of Section 4 is to find a uniform bound on δ that works in the whole interval $[q, \frac{3}{2}(q+1)-o(q)]$. Such a bound can be found in Theorem 4.1.

2 Algebraic background

The following folklore result in algebraic geometry will be used in our proof.

Lemma 2.1 *Let S be a set of points in $\mathrm{PG}(2,q)$. Then there exists a non-zero three-variable homogeneous polynomial of degree at most $\sqrt{2|S|}-1$, so that it vanishes at every point of S.* ■

The affine version of this result was used in [17].

2.1 The Rédei polynomial

Let ℓ_∞ be the line at infinity in $\mathrm{PG}(2,q)$ and let $U = \{(a_i, b_i) : i = 1, ..., n\}$ be a set of points in $\mathrm{PG}(2,q) \setminus \ell_\infty$. Then the *Rédei polynomial of U* is the following polynomial in two variables:

$$H(X,Y) = \prod_{i=1}^{n}(X + a_iY - b_i) = \sum_{j=0}^{n} h_j(Y)X^{n-j}.$$

Note that $h_j(Y)$ is a polynomial of degree at most j. Instead of the above two-variable Rédei polynomial we shall also use the homogeneous version of it, that is for a subset $B^* = \{(a_i, b_i, c_i) : i = 1, \ldots, n\}$ we define

$$H^*(X,Y,Z) = \prod_{i=1}^{n}(c_iX + a_iY - b_iZ) = \sum_{j=0}^{n} h_j(Y,Z)X^{n-j}.$$

Here the coefficients $h_j(Y,Z)$ are either zero or homogeneous polynomials of degree at most j. It is not difficult to see that the Rédei polynomial encodes the intersection numbers of U and the affine lines.

Lemma 2.2 *For a fixed $y \in \mathrm{GF}(q)$, the element $x \in \mathrm{GF}(q)$ is an r-fold root of $H(X,y)$ if and only if the line with equation $Y = yX + x$ intersects U in exactly r points. Similarly, for a fixed $x \in \mathrm{GF}(q)$, the element $y \in \mathrm{GF}(q)$ is an r-fold root of $H(x,Y)$ if and only if the line with equation $Y = yX + x$ intersects U in exactly r points.* ■

Of course, the same applies for the homogeneous version H^* of the Rédei polynomial:

For a fixed $(z,y,0) \in \ell_\infty$, the element $x \in \mathrm{GF}(q)$ is an r-fold root of $H(X,y,z)$ if and only if the line with equation $zY = yX + xZ$ intersects U in exactly r points.

2.2 A bound on the degree of the greatest common divisor

The proofs in this paper will use certain polynomials related to the Rédei polynomials defined above. It will turn out that the degree of the greatest common divisor of these polynomials after substituting a value to one of the variables, has nice geometric meaning; and so the next result plays a crucial role in this paper. For details, see Corollary 2.4 in [19].

Result 2.3 *Suppose that the polynomials $u(X,Y) = \sum_{i=0}^{n} u_i(Y)X^{n-i}$ and $v(X,Y) = \sum_{i=0}^{n-m} v_i(Y)X^{n-m-i}$, $m > 0$, satisfy $\deg u_i(Y) \le i$ and $\deg v_i(Y) \le i$ and $u_0 \neq 0$, $v \neq 0$.*

Furthermore, assume that there exists a value y, so that the degree of the greatest common divisor of $u(X,y)$ and $v(X,y)$ is $n-d$. Denote by n_h, the number of values y' for which $\deg(\gcd(u(X,y'),v(X,y'))) = n-(d-h)$.

Then

$$\sum_{h=1}^{d-1} h n_h \le d(d-m).$$ ■

3 Stability theorems for small blocking sets

A *blocking set* B of $\mathrm{PG}(2,q)$ is a set of points intersecting each line in at least one point. Lines intersecting B in exactly one point are called *tangent*s. A point is *essential* to B, if through it there passes at least one tangent of B. The blocking set is *minimal* if all of its points are essential. Geometrically this means that there is a tangent line at each point. The minimal blocking set B is *small*, if $|B| < 3(q+1)/2$.

If we delete few, say ε, points from a line, we get a point set intersecting almost all but roughly εq lines. The next result is a stability result for lines.

Result 3.1 (Erdős and Lovász, [8]) *A point set of size q in $\mathrm{PG}(2,q)$, with less than $\sqrt{q+1}(q+1-\sqrt{q+1})$ 0-secants always contains at least $q+1-\sqrt{q+1}$ points from a line.*

This result can easily be extended to sets of size $q+k$, $(k \leq \sqrt{q}+1)$, as follows. The proof can be found in [3].

Result 3.2 *A point set of size $q+k$, $k \leq \sqrt{q}+1$, in $\mathrm{PG}(2,q)$, with less than $([\sqrt{q}]+1-k)(q-[\sqrt{q}])$ 0-secants always contains at least $q+k-[\sqrt{q}]+1$ points from a line.*

Both result are (essentially) sharp for q square: deleting an appropriate number of points from a Baer subplane gives the desired number of 0-secants.

Our aim is to obtain a similar stability theorem for small blocking sets. The next result helps us estimate the number of 0-secants we get by deleting an essential point from a small blocking set. It is a consequence of Result 1.1.

Result 3.3 (Blokhuis and Brouwer, [2]) *Let B be a blocking set in $\mathrm{PG}(2,q)$, $|B| = 2q-s$ and let P be an essential point of B. Then there are at least $s+1$ tangents through P.*

Hence if we delete ε essential points from a small blocking set B then we get at least $\varepsilon(2q+1-|B|)$ skew lines. This also shows that in a stability theorem, where we have a set S ($|S| < 2q$) with δ 0-secants, then to obtain a blocking set containing S one has to add at least $\frac{\delta}{2q+1-|S|}$ points. For more details and motivation about stability theorems for blocking sets, see [17]. The main result of this section is Theorem 1.5, which is immediate when the size of B is relatively large.

Proposition 3.4 (1) ([4]) *Assume that for the size of B, $\frac{3}{2}q - 2 \leq |B| \leq 2q-2$ holds and $\delta < 2(2q-1-|B|)$. Then B can be obtained from a blocking set by deleting at most one point.*

(2) ([3]) *If $\frac{7}{6}q \leq |B| < \frac{3}{2}q - 2$, and $\delta \leq 3(2q - 1 - |B|) - (q + a + 1)/2$, (where $a = 1$ for q even, $a = 0$ for q odd), then B can be obtained from a blocking set by deleting at most two points.* ■

Remark 3.5 For the sake of simplicity later we shall use Proposition 3.4 for $|B| > \frac{5}{4}q$. When $|B|$ is close to $\frac{7}{6}q$, then the bound in Proposition 3.4 is weaker than the one in Theorem 1.5. The point when the two bounds are the same is roughly $|B| = (1+c)q$, where c is the smaller root of $6c^2-6c+1 = 0$, that is when c is approximately $(3 - \sqrt{3})/6 = 0,211...$ Note also that (1) of Proposition 3.4 is sharp, see [4].

As the above proposition shows, Theorem 1.5 is weak when the size of B is in the upper part of the given interval. The aim of the next section is to improve on this result, when $|B|$ is relatively large.

To prove Theorem 1.5 we need the following two lemmas.

Lemma 3.6 *Let B be a point set of size less than $2q$ in $\mathrm{PG}(2, q)$, $q \geq 16$, and assume that the number of 0-secants of B, δ, is less than $(q^2 - q)/2$.*

(1) Denote by s the number of 0-secants of B passing through a point $P(\notin B)$. Then $(2q + 1 - |B| - s)s \leq \delta$.

(2) If $|B| \leq \frac{5}{4}q$ and $\delta < \min\left((q-1)\frac{2q+1-|B|}{2(|B|-q)}, \frac{1}{2}(q - \sqrt{q})^{3/2}\right)$, then through any point (not in B) there are at most $\frac{\delta}{2q+1-|B|} + \frac{1}{2}$ or at least $2q+1-|B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ 0-secants of B.

Proof. Let ℓ_∞ be a line intersecting B in $k > 0$ points and let $(\infty) \in B$. Furthermore, assume that $|B| - k \neq q$.

This can be done, otherwise every line that intersects B would intersect it in k points. Since $|B| < 2q$, counting the points of B through a point in B, we get that $k = 2$. Hence B is a hyperoval, but this contradicts our assumption on δ.

Assume that there is an ideal point different from (∞) through which there pass t affine lines intersecting $B \setminus \ell_\infty$ in at least one point. The number

of affine lines intersecting B can be interpreted as the degree of the greatest common divisor of the Rédei polynomial $u(X,Y) = H(X,Y)$ of $U = B \setminus \ell_\infty$, and the polynomial $v(X,Y) = X^q - X$. We note that both polynomials have leading coefficient 1, and by the choice of ℓ_∞ their degree is not the same, so Result 2.3 can be applied. Denote by n_{t+h} the number of ideal points different from (∞) through which there pass $(t+h)$, $h \geq 0$, affine lines intersecting $B \setminus \ell_\infty$. Hence, by Result 2.3, $\sum_{h=1}^{q-t} hn_{t+h} \leq (|B| - k - t)(q-t)$. Suppose that P is a point of $\ell_\infty \setminus B$ and assume that through P there pass $q-t$ affine lines not intersecting $B \setminus \ell_\infty$. Denote by $r_{(q-t)-h}$ the number of ideal points different from (∞) through which there pass $(q-t)-h$ affine 0-secants. Through these points there pass $t+h$ affine lines intersecting $B \setminus \ell_\infty$, hence $\sum_{h=1}^{q-t} hr_{(q-t)-h} = \sum_{h=1}^{q-t} hn_{t+h}$. Hence, by counting the number of skew lines through the points of $\ell_\infty \setminus B$, we get a lower bound on δ:

$$(q+1-k)(q-t) - \sum_{h=1}^{q-t} hr_{(q-t)-h} \leq \delta. \tag{2}$$

Using $\sum_{h=1}^{q-t} hr_{(q-t)-h} = \sum_{h=1}^{q-t} hn_{t+h} \leq (|B| - k - t)(q-t)$ and substituting $s = (q-t)$, we get *(1)* of the present lemma:

$$(2q + 1 - |B| - s)s \leq \delta. \tag{3}$$

To prove the second part of the lemma, we use the estimate $1 - \frac{x}{2} - \frac{x^2}{4} \leq \sqrt{1-x}$, which is true for $x \leq \frac{3}{4}$. The roots of the quadratic equation coming from (3) are:

$$s_{1,2} = (2q + 1 - |B|)\frac{1 \pm \sqrt{1-x}}{2}, \tag{4}$$

where $x = \frac{4\delta}{(2q+1-|B|)^2}$. The condition $x \leq \frac{3}{4}$ can easily be checked for $q \geq 16$. To get *(2)* of the present lemma, we need that $(2q + 1 - |B|)\frac{x^2}{4} \leq 1$, that is $\frac{4\delta^2}{(2q+1-|B|)^3} \leq 1$. To see this, the first term of the minimum in the estimate for δ is used for $|B| > q + \sqrt{q} + 1$ and it reduces to $\frac{(q-1)^2}{(|B|-q)^2(2q+1-|B|)} \leq 1$. Note that the denominator is monotone in the interval $[q + \sqrt{q} + 1, 1.5q]$ and it takes its minimum when $|B| = q + \sqrt{q} + 1$, hence the result follows. For $|B| \leq q + \sqrt{q} + 1$, the second term of the minimum in the estimate for δ gives immediately that $\frac{4\delta^2}{(2q+1-|B|)^3} \leq 1$. ■

Remark 3.7 Lemma 3.6 1) implies the Jamison, Brouwer-Schrijver result on affine blocking sets immediately. If there was an affine blocking set B of size $|B| = 2q-2$ then we would get $(2q+1-|B|-s)s \leq \delta = 1$ for any point not in B. From $(3-s)s \leq 1$, $s = 0$ follows which is a contradiction for points on the 0-secant ℓ_∞. Similarly, Result 3.3 is also an immediate consequence of Lemma 3.6 1). Take a blocking set B and a point $P \in B$. The 0-secants of the set $S = B \setminus \{P\}$ are just the tangents to B at P, so $\delta = t_P$ for S. For the point P, Lemma 3.6 1) gives $(2q+1-(|B|-1)-t_P)t_P \leq t_P$, which gives $t_P \geq 2q+1-|B|$ indeed.

Lemma 3.8 *Assume that* $|B| \leq \frac{5}{4}q$ *and*

$$\delta < \min\left((q-1)\frac{2q+1-|B|}{2(|B|-q)}, \frac{1}{2}(q-\sqrt{q})^{3/2}\right).$$

Let N *be the set of points through which there are at least* $2q+1-|B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ *skew lines to* B*. Then* $B' = B \cup N$ *is a blocking set.*

Proof. Assume to the contrary that there exists a line ℓ, skew to B, so that through each point of ℓ there pass less than $2q+1-|B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ skew lines of B. Then, by Lemma 3.6 (2), through each of these points there pass at most $\frac{\delta}{2q+1-|B|} + \frac{1}{2}$ skew lines (including ℓ). Counting the skew lines of B through the points of ℓ, we get an upper bound on δ. Namely,we get

$$\delta \leq 1 + (q+1)(\frac{\delta}{2q+1-|B|} - \frac{1}{2}) = \delta + \frac{\delta(|B|-q)}{2q+1-|B|} - \frac{q+1}{2} + 1 \qquad (5)$$

This is in contradiction with the first term of the min in the bound on δ. Hence on each of the skew lines, there is at least one point through which there pass at least $2q+1-|B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ skew lines. ■

Proof of Theorem 1.5: By Proposition 3.4, we may assume that $|B| \leq \frac{5}{4}q$. We construct the point set B' by adding the points through which there pass at least $2q+1-|B| - \frac{\delta}{2q+1-|B|} - \frac{1}{2}$ skew lines to B. As before we distinguish the cases when $|B| > q+\sqrt{q}+1$ and $|B| \leq q+\sqrt{q}+1$. In the former case the number of 0-secants through the points in N is at least $\frac{3}{4}q - \frac{3}{2}$. Counting the skew lines through these points, we see at least $\frac{3}{4}q - \frac{3}{2} + \frac{3}{4}q - \frac{5}{2} + \ldots$ 0-secants, which shows that there were less than $\lceil \frac{1}{4}q \rceil$ such points for $\sqrt{q} \geq 4$. Hence

$|B'| = |B| + |N| < 3q/2$ and by Lemma 3.8, B' is a blocking set. In the latter case when $|B| \leq q + \sqrt{q} + 1$ the large indices are at least $q - \frac{3}{2}\sqrt{q} - \frac{1}{2}$ and similarly to the other case we get that $|B'| < 3q/2$.

Let x be the minimum number of points we need to add to B in order to obtain a blocking set B^*. (Note that $|B^*| \leq |B'| < 3q/2$.) By Result 3.3, through each essential point of this blocking set (these are exactly the points of $B^* \setminus B$) there pass at least $2q+1-|B|-x \geq q/2$ skew lines. Hence in total, B has at least $xq/2$ skew lines, which shows that $x \leq 2\delta/q$. Knowing this we see that the minimum x guarantees $x(2q+1-|B^*|)$ skew lines. This gives the equation $x(2q+1-|B|-x) \leq \delta$, which is the same quadratic equation that we considered in Lemma 3.6 *(2)*. Hence $x \leq \frac{\delta}{2q+1-|B|} + \frac{1}{2}$. ■

Remark 3.9 1) For $q < 16$ or more generally for small q, one can apply Proposition 3.4 or Result 3.2. For example, for $q = 13$, $|B| = 16$, Proposition 3.4 gives $\delta \leq 20$, which is larger than $(q - \sqrt{q})^{3/2}$. For $|B| = 15, 14$, Result 3.2 gives $\delta < 20$ and 30, respectively. For $|B| = 13$, Result 3.1 gives $\delta \leq 14\sqrt{14} - 14$ and Result 3.2 gives $\delta < 40$. Similar improvements can also be obtained for $q = 11$. Note also that for $q = 16$ (and for somewhat larger values of q), Results 3.1 and 3.2 and Proposition 3.4 yield better bounds than $(q - \sqrt{q})^{3/2}$.

2) The proof of Lemma 3.6 (2) shows that for $q > q_0(\varepsilon)$ it is enough to assume $\delta \leq (\frac{1}{\sqrt{2}} - \varepsilon)q\sqrt{q}$ to get the same conclusion as in Theorem 1.5. Indeed, instead of the constant 4 in $1 - \frac{x}{2} - \frac{x^2}{4} \leq \sqrt{1-x}$ one can put any constant smaller than 8, so in $(2q+1-|B|)\frac{x^2}{4} \leq 1$ we could put any constant smaller than 8 in place of 4, which shows that $\delta \leq (\frac{1}{\sqrt{2}} - \varepsilon)q\sqrt{q}$ would guarantee this condition if q is large enough.

4 Stability theorems for small blocking sets II

As mentioned before, in this section we are going to improve on Theorem 1.5, when the size of our point set is relatively large. As remarked earlier, Theorem 1.5 is quite weak in this case. The aim is to find a uniform bound on δ that works in the whole interval $[q, \frac{3}{2}(q+1) - o(q)]$. The proof is guided by the ideas of the paper [15], where it is shown that each line intersects

a small minimal blocking set in 1 mod p points. In case of a *small almost blocking set* B, a very similar argument to those in [15] will show that B contains a point set intersecting *almost every line* in 1 mod p points and so its size cannot be too large. Finally, using Lemma 3.6, we show that we can add few points to B so that we obtain a blocking set.

Theorem 4.1 *Let B be a point set in* $\mathrm{PG}(2,q)$, $q=p^h$, $h>1$, *and suppose that the number of* 0*-secants, δ, of B is at most $\frac{1}{100}pq$. Assume that $|B|<\frac{3}{2}(q+1-\sqrt{2\delta})$. Then B can be obtained from a blocking set by deleting at most $\frac{\delta}{2q+1-|B|}+\frac{1}{100}$ points of it.*

Remark 4.2 Note that, for $|B|<q+50\frac{q}{p}$, Theorem 1.5 and Propsition 3.4 give better result. Hence we may assume that $|B|\geq q+50\frac{q}{p}$ and so $p>100$ (otherwise $|B|>\frac{3}{2}q$); which will be our assumption throughout the rest of this paper.

To prove the theorem our main aim is first to show that B can be embedded in a blocking set of size less than $\frac{3}{2}(q+1)$, and then the result will follow immediately.

For the points (a_r,b_r,c_r) of B, consider the three-variable homogeneous Rédei polynomial $H_B^*(X,Y,Z)=\prod_{r=1}^{|B|}(c_rX+a_rY-b_rZ)=\sum_{j=0}^{|B|}h_j(Y,Z)X^{|B|-j}$ introduced in Subsection 2.1. As the homogeneous Rédei polynomial encodes the intersection multiplicities of B and the lines, we see that the line $wY=vX+uZ$ is a 0-secant of B if and only if $H^*(u,v,w)\neq 0$.

Using Lemma 2.1, we see that there exists a non-zero, three-variable homogeneous polynomial $\tilde{a}(X,Y,Z)$ over $\mathrm{GF}(q)$, of degree at most $\sqrt{2\delta}-1$, such that for each skew line $wY=uX+vZ$ to B, where $w,u,v\in\mathrm{GF}(q)$, $\tilde{a}(u,v,w)=0$.

Delete each linear component $(c_iX+a_iY-b_iZ)$ of $\tilde{a}$ and add the corresponding projective point (a_i,b_i,c_i) to B, if it was not in B. If a linear component has multiplicity more than one, the corresponding point should be added to B only once. *We will denote the new polynomial by $\tilde{a}_1$ and the new set by B_1.* Hence

$$|B_1|<3(q+1)/2-\sqrt{2\delta}/2-\deg(\tilde{a}_1)-1. \tag{6}$$

Assume that B_1 is not yet a blocking set. *Our aim is to choose the coordinate system in such a way that the total degree of $H_{B_1}^*\tilde{a}_1$ is equal to its*

X-degree. Let us choose the coordinate system so that the line $Z = 0$ is skew to B_1, which makes the total degree of $H^*_{B_1}$ equal to its X-degree. As $\tilde{a}_1$ has no linear component, it intersects the line pencil through (∞) in less than $\sqrt{2\delta}$ lines; hence we can choose the line $X = 0$ to be one of the lines through (∞) that is not in $\tilde{a}_1$. This means that $\tilde{a}_1(1, 0, 0) \neq 0$, so the total degree of $\tilde{a}_1$ is also equal to its X-degree; hence we are done.

Note that, in this new coordinate system, B_1 is an affine point set. Let $a^*(X, Y, Z)$ be the polynomial $\tilde{a}_1(X, Y, Z)$ in this new coordinate system. We will substitute $Z = 1$, hence we will consider the two variable (affine) Rédei polynomial $H_{B_1}(X, Y)$ and the two variable polynomial $a(X, Y) = a^*(X, Y, 1)$, where $\deg(\tilde{a}_1) = \deg(a^*)$. By the construction of $a(X, Y)$, the polynomial $H_{B_1}a$ vanishes for all $(x, y) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$. If there is a factor $d(X, Y)$ of $a(X, Y)$, so that $(H_{B_1}\frac{a}{d})(x, y) = 0$ for every pair (x, y), then we delete this factor from a. We repeat this process until there is no such factor.

It causes no ambiguity if we also denote the resulting polynomial by $a(X, Y)$ and $\deg a = t$. Note that $t \leq \deg(\tilde{a}_1)$. The situation is summarised in the next proposition, where the upper bound on the degree of $H_{B_1}a$ follows from (6).

Proposition 4.3 *We obtained a polynomial $a(X, Y)$, such that*

$$\deg(H_{B_1}a) < 3(q + 1)/2 - \sqrt{2\delta}/2 - 1,$$

and $a(X, Y)$ has no linear component. Furthermore, $H_{B_1}(x, y)a(x, y) = 0$ for every pair $(x, y) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$, and a is minimal in the sense that this property will not hold if we delete any factor of a.

Hence, we can write $H_{B_1}a$ as

$$H_{B_1}(X, Y)a(X, Y) = (X^q - X)f(X, Y) + (Y^q - Y)g(X, Y), \qquad (7)$$

where $\deg(f)$, $\deg(g) \leq |B_1| - q + \deg(a) = |B_1| - q + t < (q + 1 - \sqrt{2\delta})/2$.

Denote by $C(X, Y)$ the product of the common factors (with multiplicity) of $f(X, Y)$ and $g(X, Y)$.

$$H_{B_1}(X, Y)a(X, Y) = C(X, Y)((X^q - X)\tilde{f}(X, Y) + (Y^q - Y)\tilde{g}(X, Y)), \quad (8)$$

where $\tilde{f}$ and $\tilde{g}$ have no common factors. Furthermore, $\deg(\tilde{f})$, $\deg(\tilde{g})$ are at most $|B_1| - q + \deg(a) - \deg_X(C) = |B_1| - q + t - \deg_X(C) < (q + 1 - \sqrt{2\delta})/2$. By

the minimality of a, the polynomials C and a cannot have a common factor, hence $C(X,Y)|H_{B_1}(X,Y)$.

All the factors of $C(X,Y)$ have multiplicity one and are of the form $(X + a_kY - b_k)$. Furthermore, the points $(a_k, b_k, 1)$ corresponding to the linear factors of $C(X,Y)$ are in B_1.

Let $\mathcal{C}$ denote the set of these points, hence $|\mathcal{C}| = \deg_X(C)$. From above, $\mathcal{C} \subset B_1$.

Proposition 4.4 *Let $B_2 = B_1 \setminus \mathcal{C}$, which is an affine point set. Construct its Rédei polynomial $H_{B_2}(X,Y)$. Then, by (8),*

$$H_{B_2}(X,Y)a(X,Y) = (X^q - X)\tilde{f}(X,Y) + (Y^q - Y)\tilde{g}(X,Y), \qquad (9)$$

where $deg(\tilde{f})$, $deg(\tilde{g})$ are at most $|B_1| - q + \deg(a) - \deg_X(C) = |B_2| - q + t < (q + 1 - \sqrt{2\delta})/2$.

As the next lemma shows, through each point of $\mathcal{C}$, there pass few 0-secants of B_2 only.

Lemma 4.5 *If $(X + a_kY - b_k)$ is a factor of $C(X,Y)$ then the number of 0-secants of B_2 through $(a_k, b_k, 1)$ $(\in B_1 \setminus B_2)$ is at most $t + 1$. In particular, $|B_2| \geq q - t$.*

Proof. We have seen that $(X + a_kY - b_k)$ cannot divide $a(X,Y)$. Hence by Bézout's theorem, a and $(X + a_kY - b_k)$ have at most t common points.

For any value y, $x = b_k - a_ky$ is a root of the right-hand side of equation (9), and so this also holds for the left-hand side. Hence there are at least $q - t$ values y, such that $x = b_k - a_ky$ is a root of $H_{B_2}(X,y)$. For these values, the line $Y = yX + x$ (through $(a_k, b_k, 1)$) intersects B_2. Now the lemma follows, since the lines through $(a_k, b_k, 1)$ are either of type $Y = yX + x$ or vertical, so there are at most $t + 1$ 0-secants. If $|B_2| < q - t$, then through any point not in B_2 there would pass at least $t + 2$ 0-secants to B_2, a contradiction. ■

Let $\overline{\mathrm{GF}(q)}$ denote the algebraic closure of $\mathrm{GF}(q)$.

Lemma 4.6 *For any $(x,y) \in \overline{\mathrm{GF}(q)} \times \mathrm{GF}(q)$, $\tilde{f}(x,y) = 0$ implies $\tilde{g}(x,y)a(x,y) = 0$.*

PROOF. Suppose that for a fixed $Y = y$, $y \in \mathrm{GF}(q)$, x is a root of $\tilde{f}(X, y)$. Then, by equation (9), the intersection multiplicity of $H_{B_2}(X, Y)a(X, Y)$ and the line $Y = y$ at (x, y) is at least two if $x \in \mathrm{GF}(q)$. Now assume that $a(x, y) \neq 0$, then Lemma 2.2 implies that the line $Y = yX + x$ intersects B_2 in at least two points. Hence the intersection multiplicity of the line $X = x$ and $H_{B_2}(X, Y)$ at (x, y) is also at least two, and so by equation (9), $\tilde{g}(x, y) = 0$. If $x \notin \mathrm{GF}(q)$, then x is a root of $H_{B_2}(X, y)a(X, y)$, and since the roots of $H_{B_2}(X, y)$ are in $\mathrm{GF}(q)$, we have that $a(x, y)$=0. ■

Lemma 4.7 *Let $h(X, Y)$ be an irreducible polynomial over the algebraic closure of* $\mathrm{GF}(q)$ *dividing $\tilde{f}$. Then $\frac{\partial h}{\partial X} = 0$.*

PROOF. Assume that $\deg h = s$, and by the choice of our coordinate system $\deg_X h = s$. Then the sum of the intersection multiplicities $I(P, h \cap l_P)$ over $\overline{\mathrm{GF}(q)} \times \mathrm{GF}(q)$ is exactly sq, where l_P denotes the horizontal line through P. If $\frac{\partial h}{\partial X} \neq 0$, then the number of points counted without multiplicity is at least $sq - s(s-1)$, where the subtracted correction term counts the common points of h and $\frac{\partial h}{\partial X}$. These points are also on $\tilde{g}a$. Since $\tilde{f}$ and $\tilde{g}$ have no common factors, if $h|\tilde{g}a$, h must divide a. Hence h divides the right-hand side of (9), h is of the form $Y - m$, which is impossible, since a has no linear component.

Hence we can apply Bézout's theorem for the polynomials h and $\tilde{g}a$:

$$sq - s(s-1) \leq s\frac{(q - 1 + \sqrt{2\delta})}{2}.$$

The left-hand side counts the number of points of h, the right-hand side uses the bound on the degree of $\tilde{g}$ in Proposition 4.4. After simplifying the inequality, we get that $(q + 3 - \sqrt{2\delta})/2 \leq s$; which is a contradiction. ■

By Lemma 4.7, for a fixed $Y = y$, $\tilde{f}(X, y)$ is a p-th power, that is

$$\tilde{f}(X, y) = (w_y(X))^p. \tag{10}$$

Using equations (9) and (10), we get that for any $y \in \mathrm{GF}(q)$,

$$H_{B_2}(X, y)a(X, y) = (X^q - X)\tilde{f}(X, y) = (X^q - X)(w_y(X))^p. \tag{11}$$

As the next lemma shows, this equation helps us bound the size of B_2.

Lemma 4.8 *The size of B_2 is less than $q + 5\frac{q}{p}$ ($p > 100$).*

PROOF. As noted in Remark 4.2, we may assume that $p > 100$. Let S be the sum of the intersection multiplicities $I(P, \tilde{f} \cap h_P)$, where h_P are the horizontal lines through those points $P \in \overline{\mathrm{GF}(q)} \times \mathrm{GF}(q)$, where these intersection multiplicities are at least p.

For a fixed value $y \in \mathrm{GF}(q)$, $\tilde{f}(X, y) = (w_y(X))^p$ splits into linear factors over $\overline{\mathrm{GF(q)}}$, hence $S = q \cdot \deg_X(\tilde{f})$.

Now we will give an upper bound on S. First of all note that

$$I(P, \tilde{f} \cap h_P) = I(P, H_{B_2} \cap h_P) + I(P, a \cap h_P) - \mu,$$

for all points P; where μ is 1 when $x \in \mathrm{GF}(q)$ and 0 otherwise. The first term of the right hand-side of equation (11) is $(X^q - X)$, that splits into different linear factors over $\mathrm{GF}(q)$; which explains the term μ in the above expression.

By Bézout's theorem, the sum of the intersection multiplicities $I(P, a \cap h_P)$ over all points $P \in \overline{\mathrm{GF}(q)} \times \mathrm{GF}(q)$ is at most $q\deg(a) = qt$. To give an upper bound for the sum of the intersection multiplicities $I(P, H_{B_2} \cap h_P)$ (when for each P, $I(P, \tilde{f} \cap h_P) \geq p$), we will distinguish between the points P according to $I(P, H_{B_2} \cap h_P) \geq (p+3)/2$ or $I(P, H_{B_2} \cap h_P) < (p+3)/2$.

By Lemma 2.2, the first case considers those points $P(x, y)$ that correspond to lines $Y = yX + x$ intersecting B_2 in at least $(p+3)/2$ points. In this case we automatically have $x \in \mathrm{GF}(q)$. Hence for these points P, the sum of the intersection multiplicities $I(P, H_{B_2} \cap h_P)$ is exactly the number of incident point-line pairs, where the point lies in B_2 and the line is an i-secant with $i \geq (p+3)/2$. The number of i-secants with $i \geq (p+3)/2$ through a point of B_2 is at most $2(|B_2|-1)/(p+1)$, hence the number of these incident point-line pairs is at most $2|B_2|(|B_2|-1)/(p+1)$.

Now we bound the sum of the intersection multiplicities $I(P, H_{B_2} \cap h_P)$ over the points P, for which $I(P, H_{B_2} \cap h_P) < (p+3)/2$ (and $I(P, \tilde{f} \cap h_P) \geq p$). For these points, when $x \in \mathrm{GF}(q)$, $I(P, a \cap h_P) \geq (p-1)/2$ (see the equation at the beginning of the proof) and so $I(P, a \cap \tilde{f}) \geq (p-1)/2$. When $x \notin \mathrm{GF}(q)$, the intersection multiplicity $I(P, H_{B_2} \cap h_P)$ is obviously 0 and so we get that $I(P, a \cap h_P) \geq p$ and hence $I(P, a \cap \tilde{f}) \geq p$. Hence by Bézout's theorem the number of such points P is at most $(\deg(\tilde{f})\deg(a))/((p-1)/2)$. For each of these points P, $I(P, H_{B_2} \cap h_P) \leq (p+3)/2$, hence the sum of these intersection multiplicities is at most $\frac{p+3}{p+1}\deg(\tilde{f})\deg(a) = \frac{p+3}{p+1}(|B_2| - q + t)t$. Hence

$$q(|B_2|+t-q) \le S \le \frac{2|B_2|(|B_2|-1)}{p+1} + \frac{p+3}{p+1}(|B_2|-q+t)t + qt.$$

Subtracting $q(|B_2|+t-q)$ and dividing by $2/(p+1)$ both sides of the above inequality gives

$$0 \le |B_2|(|B_2|-1) + \frac{p+3}{2}(|B_2|-q+t)t - \frac{q(p+1)}{2}(|B_2|-q).$$

For $|B_2| = q$, the right-hand side of the inequality is obviously positive. It is not difficult to check that for $|B_2| = q+5\frac{q}{p}$, the right-hand side is negative. So the right-hand side has a root between q and $q+5\frac{q}{p} < \frac{3}{2}q$. The constant term in the above inequality is $\frac{p+3}{2}(t-q)t + \frac{q^2(p+1)}{2}$, that is larger than $\frac{9}{4}q^2$, hence the other root must be larger than $\frac{3}{2}q$. So we indeed get $|B_2| < q+5\frac{q}{p}$. ■

In the sequel, we will use bounds on the set $\mathcal{C} = B_1 \setminus B_2$. Note that Lemma 4.8 gives an upper bound, Lemma 4.5 gives a lower bound on the size of B_2.

Lemma 4.9 *The number of* 0*-secants of* B_2*,* δ'*, is at most* $0.083q\sqrt{pq}$*.*

PROOF. Originally B had at most $\frac{1}{100}pq$ 0-secants. To obtain B_2 we added some points and deleted the points of $\mathcal{C}$. By Lemma 4.5, after deleting the points of $\mathcal{C}$, we may get at most $|\mathcal{C}|(t+1) \le (\frac{q}{2})\sqrt{\frac{2}{100}pq}$ new 0-secants. Hence $\delta' \le (\frac{q}{2}+t)\sqrt{\frac{2}{100}pq} + \frac{1}{100}pq \le 0.083q\sqrt{pq}$. ■

Lemma 4.10 *The number of* 0*-secants of* B_2 *through a point is either at most* $\frac{\delta'}{2q+1-|B_2|} + \frac{1}{30}p$ *or at least* $2q+1-|B_2| - (\frac{\delta'}{2q+1-|B_2|} + \frac{1}{30}p)$*.*

PROOF. Let s denote the number of skew lines of B_2 through P. By Lemma 3.6, $(2q+1-|B_2|-s)s \le \delta'$. As in Lemma 3.6 *(2)*, we use the estimate $1 - \frac{x}{2} - \frac{x^2}{4} \le \sqrt{1-x}$, which is certainly true for $x \le \frac{3}{4}$. It is used for $x = \frac{4\delta'}{(2q+1-|B_2|)^2}$, and using Lemma 4.9, $|B_2| \le q+5\frac{q}{p}$, and $p \ge 100$ it is

easy to check that $x \leq \frac{3}{4}$ indeed. The extra cp term comes from the above estimate, and it gives $\frac{4\delta'^2}{(2q+1-|B_2|)^3}$, which is at most $(4 \cdot 0.083^2/0.95^3)p \leq \frac{p}{30}$. So we get that $s \leq \frac{\delta'}{2q+1-|B_2|} + \frac{1}{30}p$ or $s \geq 2q+1-|B_2| - (\frac{\delta'}{2q+1-|B_2|} + \frac{1}{30}p)$. ■

Proof of Theorem 4.1. We show that B can be embedded in a blocking set of size less than $\frac{3}{2}(q+1)$. Construct the point set B_1 (see the beginning of this section). If B_1 is a blocking set, then we are done. Otherwise, construct the point set B_2.

By Lemma 4.8, B_2 has less than $q + 5\frac{q}{p}$ points. We will show that the number of 0-secants δ' of B_2 (which is at least the number of 0-secants of B_1) is at most $\frac{1}{10}pq - \frac{q}{2}$; then Theorem 1.5 finishes our proof.

Assume to the contrary that $\delta' > \frac{1}{10}pq - \frac{q}{2}$. By the construction of B_2, all the 0-secants of B_2 that are not skew to B pass through one of the points of $\mathcal{C}$. There are at least $\delta' - \frac{1}{100}pq$ such 0-secants, hence there exists a point $P \in \mathcal{C}$ through which there pass at least $\frac{\delta'}{|\mathcal{C}|} - \frac{pq}{100|\mathcal{C}|}$ 0-secants of B_2. We will show that the number of 0-secants through P lies in the interval that is forbidden by Lemma 4.10, hence we get a contradiction. By Lemma 4.5, we know $|B_2| \geq q - t$.

It is easy to show that $\frac{\delta'}{|\mathcal{C}|} - \frac{pq}{100|\mathcal{C}|} > \frac{\delta'}{2q+1-|B_2|} + \frac{1}{30}p$. This is equivalent to proving that $\frac{\delta'}{|\mathcal{C}|} - \frac{pq}{100|\mathcal{C}|} - \frac{\delta'}{2q+1-|B_2|} > \frac{1}{30}p$. For a lower bound of the left hand side we can use $|\mathcal{C}| < \frac{q}{2}$, $|B_2| < q + 5\frac{q}{p}$ and $\frac{pq}{10} - \frac{q}{2} < \delta'$ (and $\delta' - \frac{pq}{100} \geq \frac{8}{9}\delta'$ as $p > 100$); and so we get $\frac{7}{90}p - \frac{8}{9} > \frac{1}{30}p$.

To get a contradiction with Lemma 4.10, now we only have to show that the number of 0-secants of B_2 through any point of $\mathcal{C}$ is less than $2q+1-|B_2| - (\frac{\delta'}{2q+1-|B_2|} + \frac{1}{30}p)$. Using Lemma 4.9 and $|B_2| < q + 5\frac{q}{p}$, we get that $t + 1 < 2q + 1 - |B_2| - (\frac{\delta'}{2q+1-|B_2|} + \frac{1}{30}p)$.

Hence, by Theorem 1.5, we can add at most $\frac{1}{10}p < p$ points to B_2, so that we obtain a blocking set. Note that we constructed B_2 from B by adding at most $\deg(\tilde{a}) < \sqrt{2\delta}$ points to B and deleting some points. Hence in total we can add at most $\sqrt{2\delta} + p < \frac{3}{2}\sqrt{2\delta}$ points to B in order to get a blocking set. This blocking set B^* will have size less than $\frac{3}{2}(q+1)$. We immediately get $\varepsilon \leq \frac{2\delta}{q}$, since any essential point in $B^* \setminus B$ is on at least $q/2$ tangents. This bound can be improved exactly the same way as in Theorem 1.5. Let k denote the minimum number of points that have to be added to B to get a blocking set. Then $k(2q+1-|B|-k) \leq \delta$ with the original δ and not δ'. The usual estimate $1 - \frac{x}{2} - \frac{x^2}{4} \leq \sqrt{1-x}$ with $x = \frac{4\delta}{(2q+1-|B|)^2}$ gives that

$k \leq \frac{\delta}{2q+1-|B|} + \frac{1}{100}$. ■

Remark 4.11 The constant $\frac{1}{100}$ in Theorem 4.1 is of course not sharp. Let $\delta = cpq$. When p is large enough, our proof of Lemma 4.8 could give $|B_2| \leq q + c'\frac{q}{p}$, for any constant $c' > 2$. For large p, the constant in Lemma 4.10 is roughly $\delta' = q\sqrt{c/2}\sqrt{pq}$. The constant in front of the extra term constant times p in Lemma 4.10 is $2cp$. So in the proof of Theorem 4.1 we have $\delta' > (\frac{1}{\sqrt{2}} - \varepsilon)\frac{1}{c'}pq$, by Remark 3.7. To make that proof work we need $\frac{\delta'}{q/2} - \frac{cpq}{q/2} > \frac{\delta'}{q} + 2cp$, which means that $4c < \frac{1}{2\sqrt{2}} - \varepsilon$, that is $c < \frac{1}{8\sqrt{2}} - \varepsilon$, if p is large enough.

Finally, also note that if we consider Lemma 4.8 on its own, it can be improved. For example, it can be showed that $|B_2| < q + 3\frac{q}{p}$, when $p \geq 17$. (This might be useful to compute a bound on p when calculating a better constant in Theorem 4.1.) But by Remark 4.2, the present form of the lemma is sufficient to prove Theorem 4.1.

Acknowledgement. We thank the referees for their useful comments, in particular they pointed out some inaccuracies in the proof of Lemma 4.7 and 4.8.

References

[1] A. Blokhuis, On the size of a blocking set in PG$(2, p)$, *Combinatorica* **14** (1994), 273–276.

[2] A. Blokhuis, A. E. Brouwer, Blocking sets in Desarguesian projective planes, *Bull. London Math. Soc.* **18** (1986), 132–134.

[3] A. Blokhuis, A. E. Brouwer, T. Szőnyi, Zs. Weiner, q-analogues and stability, *J. of Geometry*, **100** (2011), 31–50.

[4] A. Blokhuis, A. E. Brouwer, T. Szőnyi, Covering all points except one, *J. Alg. Combinatorics* **32** (2010), 59–66.

[5] A. Blokhuis, P. Sziklai, T. Szőnyi, Blocking sets in projective spaces, in: *Current research topics in Galois geometry* (Eds: J. De Beule, L. Storme), Nova Science Publishers (2011), 57-80.

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

[7] A. A. Bruen, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.

[8] P. Erdős, L. Lovász, Problems and results on 3-chromatic hypergraphs and some related questions, in: *Infinite and finite sets* (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II, pp. 609–627, Colloq. Math. Soc. János Bolyai, **Vol. 10**, North-Holland, Amsterdam, 1975.

[9] T. Szőnyi, A. Gács, Zs. Weiner, On the spectrum of minimal blocking sets in PG$(2, q)$, *J. of Geometry* **76** (2003), 256–281.

[10] J. W. P. Hirschfeld Projective geometries over finite fields. Second edition. *Oxford Mathematical Monographs.* The Clarendon Press, Oxford University Press, New York, 1998. xiv+555 pp. ISBN: 0-19-850295-8 (Reviewer: T. G. Ostrom) 51E15 (05B25 51A30)

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

[12] O. Polverino, Small blocking sets in PG$(2, p^3)$, *Designs, Codes and Cryptography* **20** (2000), 319–324.

[13] P. Sziklai, On small blocking sets and their linearity, *J. Combin. Th. Ser A.* **115** (2008), 1167-1182.

[14] P. Sziklai, T. Szőnyi, Blocking sets and algebraic curves, *Rend. Circ. Mat. Palermo* **51** (1998), 71–86.

[15] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes, *Finite Fields and Appl.* **3** (1997), 187–202.

[16] T. Szőnyi, On the embedding of (k, p)-arcs, *Designs, Codes, and Cryptography* **18** (1999), 235–246.

[17] T. Szőnyi, Zs. Weiner, A stability theorem for lines in Galois planes of prime order, *Designs, Codes, and Cruptography*, **62** (2012), 103–108.

[18] Zs. Weiner, On (k, p^e)-arcs in Galois planes of order p^h, *Finite Fields and Appl.*, **10** (2004), no.3, 390–404.

[19] Zs. Weiner, T. Szőnyi, Proof of a conjecture of Metsch, *J. of Combin. Theory Ser. A* **118** (2011), 2066–2070.

Authors address:

Tamás Szőnyi, Zsuzsa Weiner
Department of Computer Science, Eötvös Loránd University,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY
e-mail: szonyi@cs.elte.hu

Tamás Szőnyi
Computer and Automation Research Institute of the Hungarian Academy of Sciences
H-1111 Budapest, Lágymányosi út 11, HUNGARY and
MTA ELTE, Geometric and Algebraic Combinatics Research Group
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY

Zsuzsa Weiner
Prezi.com H-1065 Budapest, Nagymező u. 54, HUNGARY
e-mail: zsuzsa.weiner@gmail.com