

A stability theorem for lines in Galois planes of prime order

Tamás Szőnyi and Zsuzsa Weiner *

July 18, 2014

Abstract

In this paper we prove that a point set of size less than $\frac{3}{2}(q+1)$ in $\text{PG}(2, q)$, q prime, that has relatively few 0-secants must contain many collinear points. More precise bounds can be found in Theorem 2.4.

1 Introduction

A *blocking set* B of $\text{PG}(2, q)$ is a set of points intersecting each line in at least one point. Lines intersecting B in exactly one point are called *tangents*. 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. The smallest examples are lines and a blocking set that does not contain a line is called *non-trivial*. For a survey on blocking sets, the reader is referred to [10]. When q is a prime, Blokhuis [1] proved an old conjecture by Di Paola.

Result 1.1 (Blokhuis [1]) *A non-trivial blocking set in $\text{PG}(2, q)$, q prime, has at least $\frac{3}{2}(q+1)$ points.*

If we delete a few say, ε points from a line, we get a point set intersecting almost all but εq lines. After deleting ε points from a blocking set of size $\frac{3}{2}(q+1)$ (for example, from a projective triangle, see Definition 3.11 in [10])

*The authors were partially supported by OTKA NK 67867 and K 81310 grants and by the ERC Grant DISCRETECONT.

we get at least $\varepsilon \frac{(q-1)}{2}$ 0-secant lines. The situation is similar for blocking sets of size at most $2q$; this follows easily from the result of Blokhuis and Brouwer, see Result 2.1. In general, we cannot expect that the number of points that block the 0-secants is the number of 0-secants divided by constant times q . To illustrate this, let us consider a blocking set which is the union of parabolas for $q \equiv 1 \pmod{4}$ (see Section 3.3 in [10]). Let us delete ε parabolas completely from this blocking set. Since through each point of a parabola, there passes one tangent line, we will get εq 0-secants. These lines cannot be blocked by roughly ε points, since through a point there are at most two tangent lines of a parabola, so one point can block at most 2ε 0-secants. This means, that we would need at least $q/2$ points to block the 0-secants. We will be interested in the question, when the number of points needed to block the 0-secants is roughly the number of 0-secants divided by q . If we add these points to our original set, we get a blocking set. Hence we look for a result guaranteeing that a point set having at most $c\varepsilon q$ 0-secants must contain a blocking set minus roughly ε points. Of course, the situation is also interesting when we have less than q skew lines. In this case we wish to prove that the 0-secants pass through a point. For such a result, formulated in the dual setting, see Proposition 1.5 in [3].

The following old result of Erdős and Lovász can be considered as a stability theorem for lines.

Result 1.2 (Erdős and Lovász, [7]) *A point set of size q in a projective plane of order 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.*

Note that the proof of the theorem of Erdős and Lovász can be extended to sets of size less than $q + \sqrt{q} + 1$ with a weaker bound on the number of 0-secants, that is roughly $(q - \sqrt{q})(\sqrt{q} - k)$. The reason that one needs the bound $q + \sqrt{q} + 1$ on the size of the set is Bruen's theorem, see [5, 6], namely that the size of a non-trivial minimal blocking set is at least $q + \sqrt{q} + 1$.

The main result of the present short note is Theorem 2.4, which can be regarded as an analogue of the Erdős and Lovász theorem (or rather its generalization to $q + k$) for Galois planes of prime order.

2 Results

In this section we will improve on the stability theorem of Erdős and Lovász, when the plane is $\text{PG}(2, q)$, q prime. We are going to show that if B is a point set with $|B| < \frac{3}{2}(q+1)$, having at most $\delta = \varepsilon(q+1)$ 0-secants, then it contains a huge part of a line. Even though the bound in our main result is not sharp, ε can even be cq , where c is a small constant depending on $|B|$, if $|B|$ is not very close to $\frac{3}{2}(q+1)$.

The following result, which is a consequence of the affine blocking set theorem by Jamison [8], and Brouwer, Schrijver [4], will also be used in our proof.

Result 2.1 (Blokhuis and Brouwer, [2]) *Let B be a blocking set in $\text{PG}(2, q)$, $|B| = 2q - s$ and let P be an essential point of B . Then there are at least $s + 1$ tangents through P .*

Lemma 2.2 *Let B be a point set in $\text{PG}(2, q)$, $|B| < \frac{3}{2}(q+1)$. Assume that there are δ 0-secants to B . Then the total number τ of tangents of B is at least $(q+1)(2q - |B| - \frac{2\delta}{q+1})$. Hence there is a point P of B so that there are at least $\frac{2}{3}(2q - |B| - \frac{2\delta}{q+1})$ tangents through P .*

PROOF. Take a 0-secant ℓ of B . If there is no such a line then B is a blocking set and (by Result 2.1) through any essential point of B there pass at least $\frac{1}{2}(q+1) - 1$ tangents. Let the points of ℓ be denoted by P_1, \dots, P_{q+1} and let ν_i be the number of 0-secants, τ_i be the number of tangents through P_i . Looking at B from P_i one gets $q - (\nu_i + \tau_i) \leq (|B| - \tau_i)/2$, which implies that $2\nu_i + \tau_i \geq 2q - |B|$. Summing over all i we get that $(q+1)(2q - |B|) \leq 2\delta + \tau$, from which $\tau \geq (q+1)(2q - |B| - \frac{2\delta}{q+1}) + 1$ follows. On the other hand, if we add up the number of tangents at the points of B , we get τ , so there is a point which has at least the average number of tangents. ■

The following lemma is an easy folklore result in algebraic geometry.

Lemma 2.3 *Let S be a set of points in $\text{AG}(2, q)$. Then there exists a non-zero two-variable polynomial of degree at most $\sqrt{2|S|} - 1$, so that it vanishes at every point of S .*

PROOF. Each point $(u, v) \in S$, gives a linear equation for the coefficients of the desired polynomial p . Hence we have a homogeneous system of $|S|$ such

linear equations. When $\deg(p) \geq \sqrt{2|S|} - 1$, then the number of coefficients is larger than $|S|$, so we have a non-trivial solution. ■

The proof of our main theorem is motivated by [1] and [9].

Theorem 2.4 *Let B be a set of points of $\text{PG}(2, q)$, $q = p$ prime, with at most $\frac{3}{2}(q+1) - \beta$ points. Suppose that the number δ of 0-secants 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.*

PROOF. Choose the coordinate system in such a way that (∞) is a point of B with at least $\frac{2}{3}(2q - |B| - \frac{2\delta}{q+1})$ tangents, one of them be the line at infinity. Let $U = \{(a_i, b_i) : i = 1, \dots, |B| - 1\}$ be the affine part of B . The 0-secants of B can be written as $Y = m_j X + c_j$, $j = 1, \dots, \delta$. Consider the polynomial $a(x, y)$ of the smallest degree Δ , which vanishes at the points (c_j, m_j) , $j = 1, \dots, \delta$. By Lemma 2.3, $\Delta \leq \sqrt{2\delta} - 1$. Now write up the polynomial

$$H(X, Y) = \left(\prod (X + a_i Y - b_i) \right) a(X, Y).$$

The first product is the Rédei polynomial of U . This polynomial H vanishes for every (x, y) , hence it can be written as

$$H(X, Y) = (X^q - X)f(X, Y) + (Y^q - Y)g(X, Y),$$

where $\deg(f), \deg(g) \leq |B| - 1 - q + \Delta$. As in Blokhuis [1], consider the terms of highest degree of this equation and substitute $Y = 1$ in it. Then we get a polynomial equation

$$h^*(X) = \left(\prod (X + a_i) \right) a^*(X) = X^q f^*(X) + g^*(X),$$

where $X^q \nmid g^*(X)$. We may suppose that f^* and g^* are coprime, since otherwise we could divide by their greatest common divisor and obtain an equation of the same type with smaller degrees. Denote by s the maximum of the degrees of f^* and g^* after this division. The roots of $h^*(X)$ in $\text{GF}(q)$ are also roots of $Xf^*(X) + g^*(X)$. The multiple roots of $h^*(X)$ in $\text{GF}(q)$ are also roots of $X^q(f^*(X))' + (g^*(X))'$. The roots not in $\text{GF}(q)$ are roots of $a^*(x)$. Hence

$$h^*(X) | (Xf^*(X) + g^*(X))((f^*(X))'g^*(X) - (g^*(X))'f^*(X))a^*(X). \quad (1)$$

If the polynomial on the right hand side of (1) is non-zero, then comparing the degrees gives $q + s \leq s + 1 + 2s - 2 + \Delta$, that is $s \geq (q + 1 - \Delta)/2$. Since $s \leq |B| - 1 - q + \Delta$, then $|B| \geq \frac{3}{2}(q + 1) - \frac{3}{2}\Delta$, which is a contradiction.

The third term on the right hand side of (1) cannot be the zero polynomial, since the terms of highest degree of $a(X, Y)$ form a homogeneous polynomial and so $(Y - 1)$ cannot be a factor of it.

If the first term on the right hand side of (1) is the zero polynomial then $h^*(X)$ is divisible by $(X^q - X)$. Since $a^*(X)$ has degree at most Δ , the remaining $q - \Delta$ factors of $(X^q - X)$ must arise from the product $\prod (X + a_i)$. Geometrically this would imply that through the point (∞) there pass at most $\Delta + 1$ tangents, which contradicts the choice of (∞) . (Here we use that $\Delta + 1 < \frac{2}{3}(2q - |B| - \frac{2\delta}{q+1})$.)

If the second term is zero, then, since f^* and g^* are coprime, $f^*(X)|(f^*(X))'$ and similarly $g^*(X)|(g^*(X))'$. Hence $(f^*(X))' = (g^*(X))' = 0$. For $q = p$ prime, it implies that either $|B| \geq 2q + 1 - \Delta$ (which is not possible by our upper bound on $|B|$) or $aX^q + b$ divides $h^*(X)$. Since $aX^q + b = (aX + b)^q$ and at most Δ of these factors can come from $a^*(X)$, then there is a line ℓ (through (∞)) that contains at least $q + 1 - \Delta$ points of B . Finally, assume that $|\ell \cap B| = q + 1 - k$, $k \leq \Delta$. Then the 0-secants pass through the k missing points of ℓ . Since $|B| \leq \frac{3}{2}q + 1 - \frac{3}{2}\Delta$ then the number of 0-secants is at least $k(q - (\frac{3}{2}q + 1 - \frac{3}{2}\Delta - q - 1 + k)) \leq \frac{1}{2}k(q + 1)$. Hence $k \leq \frac{2\delta}{q+1}$. ■

Let us see now some constructions for sets with few 0-secants not containing a very large collinear subset. Deleting ε points from a line or a projective triangle yields εq or at least $\varepsilon \frac{q-1}{2}$ 0-secants, respectively. In the former case the number of deleted points is $\frac{\delta}{q}$, in the latter case it is roughly $\frac{2\delta}{q}$. The constructions below can be regarded as generalizations of the Rédei-Megyési construction for blocking sets (see Theorem 3.10 in [10]). In the constructions we use standard notation: affine points are denoted as (u, v) , ideal point as (m) or (∞) .

Construction 2.5 *Assume that $3|q - 1$ and let H be a subgroup of $GF(q)^*$, $|H| = \frac{q-1}{3}$. Furthermore, let B be the set of size $q + 2$, where*

$$B = \{(0, h) | h \in H\} \cup \{(h, 0) | h \in H\} \cup \{(h) | h \in H\} \cup \{(0, 0)\} \cup (0) \cup (\infty)\}.$$

Then the number of 0-secants to B is $\frac{2}{9}(q - 1)^2$. Add $k < \frac{q+17}{6}$ ideal points not in B to obtain B' . Then the total number of 0-secants to B' is $(\frac{2}{3}(q - 1) - k)\frac{1}{3}(q - 1)$.

The sets constructed above have less than $(\frac{3}{2}(q+1) - |B'|)\frac{q-1}{2}$ 0-secants (this is what we would get for a set contained in a projective triangle) and are not contained in a projective triangle.

In general, one could choose a multiplicative subgroup H (of size $\frac{q-1}{t}$) from the line $Y = 0$, s cosets of H from the line $X = 0$, and the same s cosets from the ideal line. For example, when $t = 2s$, $|B'| = q + 2 + \frac{q-1}{2s}$ and the number of 0-secants is roughly $\frac{q-1}{2}(\frac{q-1}{2} - \frac{q-1}{2s})$, which is the same as one could get by deleting $(\frac{q-1}{2} - \frac{q-1}{2s})$ appropriate points from a projective triangle. For $t > 2$ the cosets can be chosen in such a way that the set is not contained in a projective triangle.

Construction 2.6 *Let A and B be less than p and let B^* be a the following set.*

$$B^* = \{(1, a) | 0 \leq a \leq A\} \cup \{(0, -b) | 0 \leq b \leq B\} \cup \{(\infty)\} \cup \{(c) | 0 \leq c \leq A+B\}.$$

Then B^ has $2(A+B) + 4$ points and the total number of 0-secants to B^* is $(q-1-A-B)(q-A-B-2)$.*

One can modify this construction and delete some points (c) ($0 \leq c \leq A+B$) which are on many tangents of B^ . To be more concrete choose α and β , so that $\alpha \leq A+B-\beta$. Let*

$$B^{**} = \{(B^* \cap AG(2, p)) \cup (\infty) \cup \{(c) | \alpha \leq c \leq A+B-\beta\}.$$

*Then $|B^{**}| = 2(A+B) + 4 - \alpha - \beta$ and there are $(q-1-A-B)(q-A-B-2) + \frac{\alpha}{2}(2q+\alpha-3-2(A+B)) + \frac{\beta}{2}(2q+\beta-3-2(A+B))$ 0-secants.*

For $A = B = \frac{p}{4}$, B^* has size $p+4$ and the number of 0-secants is roughly $\frac{p^2}{4}$, which is the number of 0-secants of the a point set obtained by keeping these many points of a projective triangle, but this set obviously cannot be embedded in a projective triangle. One can also combine Constructions 2.6 and 2.5 by replacing arithmetic by geometric progressions. For example, if $t = 5$, H is a multiplicative subgroup and ω generates G/H then

$$B^{***} = \{(0, h) | h \in H \cup \omega H\} \cup \{(h, 0) | h \in H \cup \omega^{-1} H\} \cup \{(h) | h \in H \cup \omega H \cup \omega^2 H\} \cup \{(0, 0)\} \cup (0) \cup (\infty)\}$$

has $3 + \frac{7}{5}(q-1)$ points and $\delta = \frac{2}{25}(q-1)^2$ 0-secants. By deleting the points (h) , $h \in \omega^2 H$ we get a set of size $3 + \frac{6}{5}(q-1)$ points which has $\delta = \frac{4}{25}(q-1)^2$.

All the examples given above can be obtained from a blocking set contained in the union of three lines by deleting quite a few points. In some cases they have less 0-secants than a set of the same size contained in the projective triangle. The examples also show that we cannot expect $\frac{\delta}{q+1}$ missing points from a line in Theorem 2.4.

Remark 2.7 1) In the case corresponding to the Erdős and Lovász theorem, that is when $|B| = q$, we can allow roughly $\frac{q^2}{18}$ 0-secants to guarantee a collinear subset of size at least $\frac{8q}{9}$ in B . The bound $\frac{q^2}{18}$ can most likely be improved but we do need an upper bound of the form cq^2 , ($c \leq \frac{1}{2}$) on the number of 0-secants as shown by the constructions above.

2) If a set B has size $|B| = cq$ for some $c < 1$ then the number of 0-secants is at least $(1 - c)q(q + 1)$. This can be seen by counting 0-secants through points of a fixed 0-secant. Hence our theorem gives a non-trivial bound only if $(1 - c)q(q + 1) < (\frac{2}{3}(\beta + 1))^2/2$, where $\beta = (\frac{3}{2} - c)q$. Roughly speaking, this gives that for a fixed $c < 1$, the value of δ has to be smaller than $(1 - \frac{2}{3}c)^2q^2/2$, which gives the equation $4c^2 + 6c - 9 = 0$ for the critical value of c . The positive root of the equation is $\frac{-3 + \sqrt{45}}{4} \approx 0.927$. So our result gives a non-trivial stability theorem also for sets of size cq , $1 > c > \frac{-3 + \sqrt{45}}{4} \approx 0.927$.

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, Covering all points except one, *J. Alg. Combin.* **32** (2010), 59–66.
- [4] A. E. BROUWER, A. SCHRIJVER, The blocking number of an affine space, *J. Comb. Theory Ser. A* **24** (1978), 251–253.
- [5] A. A. BRUEN, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.
- [6] A. A. BRUEN, Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.

- [7] 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.
- [8] R. E. JAMISON, Covering finite fields with cosets of subspaces, *J. Comb. Theory Ser. A* **22** (1977), 253–266.
- [9] T. SZŐNYI, Around Rédei’s theorem, *Discrete Math.* **208/9** (1999), 557–575.
- [10] T. SZŐNYI, A. GÁCS, ZS. WEINER, On the spectrum of minimal blocking sets, *J. Geometry* **76** (2003), 256–281.

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, weiner@cs.elte.hu

Tamás Szőnyi,
Computer and Automation Research Institute of the Hungarian Academy of
Sciences
H-1111 Budapest, Lágymányosi út 11, HUNGARY

Zsuzsa Weiner
Prezi.com
H-1088 Budapest, Krúdy Gyula utca 12, HUNGARY
e-mail: zsuzsa.weiner@prezi.com