Blocking sets and algebraic curves

P. Sziklai* and T. Szőnyi*

Abstract

A typical method in Galois geometry is to associate an algebraic curve to a pointset of the plane or space. The classical example of this method is Segre's theory of complete arcs, which is one of the most successfull methods in finite geometry. The aim of this paper is to illustrate the method on blocking set. This new approach is due to the second author [39], and in some cases it gives better results than Blokhuis' lacunary polynomial method for blocking sets.

1 Introduction

A *blocking set* in a projective plane is a set B of points, such that every line contains at least one point of B. If B contains a line, it is called *trivial*. If no proper subset of B is a blocking set it is called *minimal*. The terminology is not uniform: most authors use the word blocking set for non trivial ones. This terminology is motivated by the original game theory background of blocking sets. Trivial blocking sets are sometimes called intersection sets. Also, instead of minimal, some authors use the word irreducible. Our terminology essentially comes from the more general setting of 1–covers of hypergraphs.

There are several good survey papers on blocking sets, which are recommended to the interested reader: the paper by Berardi and Eugeni [3] concentrates on history, the game theory motivation and various constructions, Blokhuis' excellent paper [7] focusses on lacunary polynomials and blocking sets. The survey paper [37] collects some applications of the probabilistic method together with some constructions, but mainly in spaces of higher dimensions. The superb survey paper by Füredi [22] discusses the combinatorial background, but it also contains lots of useful information on blocking sets in finite planes and more generally in block designs. The Handbook chapter [1] by Noga Alon discusses Rédei's work on lacunary polynomials and it contains essentially everything that was known before Blokhuis' breakthrough [6]. The present survey is devoted to the application of algebraic curves in the theory of blocking sets. A different application of essentially the same ideas can be found in [38]. More generally, [40] is a survey on various applications of algebraic curves in finite geometry and combinatorics.

Throughout this paper we will work on the Desarguesian projective plane PG(2,q), where $q = p^n$, p prime, $n \geq 1$, but we try to indicate which results are valid without this assumption.

*Research was partially supported by OTKA Grants 19367 and T-014302 and by the COST project with contract number ERBCIPACT930113.

One of the most interesting questions about blocking sets is to determine the size of the smallest non-trivial one. The first result in this direction is due to Bruen ([16, 17]) who proved that $|B| \geq q + \sqrt{q} + 1$ for any non-trivial blocking set in any projective plane of order q. Moreover, he also characterized blocking sets of size $q + \sqrt{q} + 1$; they are precisely the Baer-subplanes (i.e. subplanes of order $\sqrt{q}$). For planes of non-square order, this bound was improved to $q+\sqrt{2q}+1$ by Blokhuis, Brouwer [9] and Bruen, Silverman [18], independently to each other. In contrast with Bruen's original bound, these results are not combinatorial, the proofs make use of the fact that the plane is the Galois plane $\mathrm{PG}(2, q)$. Using purely combinatorial methods, only weaker results are known, see Bierbrauer [5] and Kitto [29]. Then Blokhuis [6] showed that $|B| \geq 3(p + 1)/2$ if the order p is a prime, confirming a 25-year old conjecture by Jane di Paola [32]. For planes of non-prime and non-square order Blokhuis [7] also improved the bound to $|B| \geq q + \sqrt{qp} + 1$. Recently Blokhuis, Storme and the second author [13] showed that $|B| \geq q + q^{2/3} + 1$, if q is a non-square and $p \geq 5$. For $p = 2, 3$ we obtained the weaker bound $|B| \geq q + q^{2/3}/2^{1/3} + 1$. The other natural question after Bruen's result is to consider blocking sets in planes of square order which do not contain a Baer-subplane. The first result in this direction is due to Bruen and Thas [19]; they showed that blocking sets of size $q + \sqrt{q} + 2$ (q square) necessarily contain a Baer-subplane. This means that for the size of a non-trivial minimal blocking set which is not a Baer-subplane, $|B| \geq q + \sqrt{q} + 3$ holds. Again, their proof was combinatorial. This bound was improved to $q + \sqrt{2q} + 1 - 1/(2q)$ by Bruen, Silverman [18], and to $q + 2\sqrt{q} + 1$ by Ball and Blokhuis [2]. The first improvement is almost combinatorial in the sense that the fact that the plane is desarguesian is only used for blocking sets of Rédei type (see the definition later). The second one was proved using lacunary polynomials. In the manuscript [13] the bound is improved to $q + q^{2/3} + 1$, if $p \geq 5$ and in the particular case $q = p^2$ to $q + q^{3/4}/\sqrt{2} + 1$.

On the other hand, there are few constructions known, even in the Galois plane $\mathrm{PG}(2, q)$. For any odd q there is a blocking set of size $3(q + 1)/2$, called the *projective triangle* in [16, Thm. 13.4.1]. For q even there is a similar blocking set, called the *projective triad* in [16, Thm 13.4.2], consisting of $(3q + 2)/2$ points. The known smaller examples have size between $q + q/p^e + 1$ and $q + (q - 1)/(p^e - 1)$ for a divisor e of n, see Brouwer and Wilbrink [15]. Actually, the construction scheme of Brouwer and Wilbrink works also in some translation planes.

All the known examples have a very specific structure. Let B be a non-trivial minimal blocking set, and let L be a line containing $l < q + 1$ points of B. Then, by considering the lines through a point P of L not belonging to the blocking set, it follows immediately that $|B| \geq q + l$. If we have equality, then every line through P different from L contains precisely one point of B. Blocking sets of this kind are called *of Rédei type* and were studied in [7] and [5]. If the line L is chosen as the line at infinity, then $B \setminus L$ can be identified with the graph of a funcion on $\mathrm{GF}(q)$. This was the setting in which Rédei considered the problem. If $l < (q + 1)/2$, then it follows from Rédei's work [13, §36] that each line intersects the blocking set in 1 (mod p) points. Moreover, from his results we get that for a non-trivial blocking set B of Rédei-type either $|B| \geq q + (q + 1)/2$, or $q+1+(q-1)/(p^e+1) \leq |B| \leq q+(q-1)/(p^e-1)$ for some e, $1 \leq e \leq [n/2]$. His result was improved in [5], namely it was shown that in the former case $|B| \geq q+1+(q+1)/2$, and in the latter $e = n/2$ or $e \leq n/3$. The first improvement was also obtained using permutation polynomials in a different context, see Evans, Greene and Niederreiter [21]. Examples of

Rédei type blocking sets are known for $e|n$, see [33], §36; 3, 4. Recently Blokhuis et al. [8] proved that only divisors of n can occur as e's (at least when $p^e \geq 4$) and they also determined the structure of Rédei type blocking sets with $e > 1$. In particular, they improved the lower bound to $q + q/p^e + 1$. In the case $q = p^3$ the blocking sets are equivalent to the examples given in Rédei's book. We shall return to planes of order p^3 later in a more general setting. It is generally believed that all small blocking sets are of Rédei type. The first indication in this direction is a result of the second author, which we discuss in Section 2.2.

In the last section we give some examples showing how the curves defined look like, how the theorems proved work in practice.

2 The Rédei polynomial and its applications for blocking sets

In this section the approach of associating curves or pairs of curves to blocking sets will be discussed. We shall follow the papers [39], [11]. In some cases the proofs given here are less detailed than the original ones, the reader may want to consult the original papers. The bounds for the size of a minimal blocking set will follow from Bézout's Theorem applied for the pair of curves. The first paper in which algebraic curves were used to prove results on blocking sets was by Blokhuis, Pellikaan and Szőnyi [11], where just one curve was defined. We first try to show what can be deduced from one curve associated to a blocking set, then discuss the results of [39] that used a pair of curves. For the sake of completeness, also the proof of the lemmas that are particularly relevant for the method are repeated. In some sense the approach goes parallel to Segre's theory of complete arcs using curves and the generalized Menelaus' theorem. We tried to emphasize the points when the results correspond to each other.

2.1 One curve

Let B be a blocking set of $\mathrm{PG}(2, q)$. A point $P \in B$ is called *essential* if $B \setminus \{P\}$ is not a blocking set. The blocking set B is minimal if and only if every $P \in B$ is essential. Geometrically this means that through each point of the blocking set B there is a line intersecting B in just one point. According to the standard terminology such a line will be called a *tangent* and, more generally, a line intersecting B in r points will be called an *r-secant* (or a *line of length r*). Let L be the line at infinity, and suppose that $(\infty) \in D = L \cap B$.

Throughout the paper we use the usual representation of $\mathrm{AG}(2, q)$ and $\mathrm{PG}(2, q)$. This means that the points have affine coordinates (x, y) where x, y are elements of $\mathrm{GF}(q)$. The lines of this affine plane have equation $mX + b - Y = 0$ or $X = c$. The coefficient m is the *slope* of the line, and the *infinite points* can be identified with slopes. So (m) will denote the infinite point of lines with slope m. Similarly (∞) will be the infinite point of vertical lines, that is lines with equation $X = c$.

Give affine coordinates to the points of $U := B \setminus L$; namely, let $U = \{(a_i, b_i) : i = 1, ..., q + k\}$. Define $N := |D|$. So $|B| = q + k + N$.

Definition 2.1 *([10], [39]) The* Rédei-polynomial *of U is defined as follows:*

$$H(X,Y) := \prod_i (X + a_i Y - b_i) = X^{q+k} + h_1(Y)X^{q+k-1} + ... + h_{q+k}(Y). \qquad (1)$$

Note that for all $j = 1, ..., q+k$: $\deg(h_j) \leq j$. If $H(X,Y)$ is considered for a fixed $Y = y$ as a polynomial of X, then we write $H_y(X)$ (or just $H(X,y)$).

Definition 2.2 *([11], [39]) Let $\mathcal{C}$ be the affine curve of degree k defined by*

$$f(X,Y) = X^k + h_1(Y)X^{k-1} + \ldots + h_k(Y).$$

Multiple components are allowed here.

Note that as $\deg(h_j) \leq j$, the polynomial $f(X,Y)$ has degree k indeed. Note also that the X-degree of f is its total degree. This will be used later. The next proposition summarizes some important properties of the Rédei polynomial and of this cycle.

Theorem 2.3 *([39])*

(1.) For a fixed $(y) \in L \setminus B$ the polynomial $(X^q - X)$ divides $H_y(X)$. Moreover, if $k < q-1$ then $H_y(X)/(X^q - X) = f(X,y)$ for every $(y) \in L \setminus B$; and $f(X,y)$ splits into linear factors over GF(q) for these fixed y's.

(2.) For a fixed (y), the element x is an r-fold root of $H_y(X)$ if and only if the line with equation $Y = yX + x$ intersects U in exactly r points.

(3.) If the line with equation $Y = y$ ($(y) \in L \setminus B$) meets $f(X,Y)$ at (x,y) with multiplicity m, then the line with equation $Y = yX + x$ meets U in exactly $m+1$ points.

The first part of this theorem shows that the curve f has a lot of GF(q)-rational points, the second part helps us translate geometric properties of U into properties of f.
Proof: (2) is straightforward from the definition of the Rédei polynomial. The multiplicity of a root $X = x$ is the number linear factors in the product defining $H(X,Y)$ that vanish at (x,y), which is just the number of points of U lying on the line $Y = yX + x$. The first part of (1) follows from (2) and the well-known fact that $\prod_{x \in GF(q)}(X - x) = X^q - X$. The rest of (1) is obvious. To prove (3) note that if the intersection multiplicity is m, then x is an $(m+1)$-fold root of $H_y(X)$. Now the assertion follows from (2). □

The facts given in Theorem 2.3 will be used frequently without further reference.

The next lemma shows that the linear components of f correspond to points of B which are not essential.

Lemma 2.4 *([39]) (1) If a point $P(a,b) \in B$ is not essential, then $X + aY - b$ divides $f(X,Y)$ (as polynomials in two variables).*

(2) Conversely, if $2(q+1-N) > q+k$ and $X + aY - b$ divides $f(X,Y)$, then $(a,b) \in B$ and (a,b) is not essential.

Proof: (1): Take an $(y_0) \in L \setminus B$. For this y_0 there are at least two points of B on the line with slope y_0 through P, hence $(X + ay_0 - b)$ divides $f(X, y_0)$. In other words, the line $L : X + aY - b$ and $\mathcal{C}$ have a common point for $Y = y_0$. This happens for $q + 1 - N$ values of y_0, so Bézout's theorem implies $L \subset \mathcal{C}$.

(2): Conversely, if $X + aY - b$ divides $f(X, Y)$, then for every $(y_0) \in L \setminus B$ the line with slope y_0 through (a, b) intersects B in at least two points. If $(a, b) \notin B$, then $|B| \geq 2(q+1-N)+N$. Putting $|B| = q+k+N$ gives a contradiction. Hence $(a, b) \in B$. Since every line with slope y_0, $(y_0) \in L \setminus B$, contains at least two points of B, the point (a, b) cannot be essential. □

If the line at infinity is a tangent, then the previous lemma simply says that there are no linear components of f if $|B| < 2q$. Note that also in Segre's theory there is a lemma corresponding to this one (see [26], Lemmas 10.3.2 and 10.4.), and it plays an important role in proving the incompleteness of arcs.

Recall also a lower bound on the number of GF(q)-rational points of certain components of f, see Blokhuis, Pellikaan, Szőnyi [11]. From now on suppose that the line at infinity is a tangent, that is $D = \{(\infty)\}$ (i.e. $N = 1$).

Lemma 2.5 *([11]) Suppose that $D = \{(\infty)\}$.*

(1) The sum of the intersection multiplicities $I(P, f \cap h_P)$ over all GF(q)-rational points of f is exactly qk, where h_P denotes the horizontal line through P. If h is a component of f, then the corresponding sum for h is precisely $q \deg(h)$.

(2) Let $h(X, Y)$ be a component of $f(X, Y)$ and suppose that it has neither multiple components nor components with zero partial derivative w.r.t. X. Then the number of GF(q)-rational points of h is at least

$$q \deg(h) - \deg(h)(\deg(h) - 1).$$

Proof: Let $s = \deg(h)$. For any fixed $Y = y$ the polynomial $f(X, y)$ is the product of linear factors over GF(q), hence the same is true for every divisor of f. So the number of points, counted with the intersection multiplicity of f and the horizontal line at that point, is exactly qs. Here one has to use that the X-degree of h is the same as its total degree. To count the number of points without this multiplicity we have to subtract the number of affine intersections of h and h'_X (see [11]); Bézout's theorem then gives the result. Note also that in this counting of common points of h and h'_X are counted once if $I(P; h \cap h_P)$ is not divisible by p, and the points with intersection multiplicity divisible by p are not counted at all. □

These elementary observations already yield interesting results on blocking sets. First of all let us see a proof of the affine blocking set theorem, due to Jamison [28] and Brouwer–Schrijver [14]. Before the proof recall the following result from [39].

Lemma 2.6 *If the smallest blocking set of $AG(2, q)$ has size at most r then in $PG(2, q)$ there is a blocking set of size at most $r + 2$ which contains two different minimal blocking sets, and vice versa.* □

Since the proof is not difficult, it is left to the reader. This is Proposition 3.1 in [39].

Theorem 2.7 *(Affine blocking set theorem; Jamison [28], Brouwer–Schrijver [14]) For blocking sets in $AG(2,q)$ we have $|S| \geq 2q-1$.*

Proof: Suppose to the contrary that $|S| \leq 2q-2$. By the previous lemma take a blocking set B of $\mathrm{PG}(2,q)$ of size $2q$ with two points P_1, P_2 that cannot be deleted simultaneously. Pick a point $P \in B$, $P \neq P_1, P_2$, and consider the non-tangent lines through P. We can always choose the line at infinity as a line disjoint from $\{P_1, P_2\}$ and intersecting B in at least 2 and at most $q-1$ points. Let $P_i : (a_i, b_i)$ be the two non-essential points that cannot be deleted simultaneously (so $|P_1P_2 \cap B| = 2$). By Lemma 2.4 (1), $X + a_iY - b_i$ $(i = 1, 2)$ divide $f(X, Y)$. If y_0 is the slope of the line P_1P_2, then this implies $x^* = -a_1y_0 + b_1 = -a_2y_0 + b_2$ is a root of $H(X, y_0)$ with multiplicity 3. This means that P_1P_2 meets B in at least 3 points, a contradiction. □

The vice versa part of Proposition 2.6 is interesting in itself. Using Theorem 2.7 it gives that blocking sets of size at most $2q$ contain a *unique* minimal blocking set. There is a similar phenomenon for arcs, an arc of size $k \geq (q+4)/2$ (if q is even), of size $k \geq (2q+5)/3$ (q odd) is contained in a unique complete (maximal subject to inclusion) arc, see [41], [36].

Now we can repeat a lemma of Blokhuis and Brouwer.

Proposition 2.8 *([9]) There are at most k^2 lines not through (∞) that meet B in at least two points.*

Proof: Take any point $P \in B$ and choose the coordinate system so that $P = (\infty)$ and the line at infinity is a tangent to B. Denote by t the number of tangents through P. Put one point on these tangent except the line at infinity. Then an affine blocking set of size $|B| - 1 + t - 1$ is obtained. The affine blocking set theorem gives $t \leq 2q + 1 - |B|$. Since P was arbitrary, this estimate holds for any point of B. Now if our blocking set contains (∞) and the line at infinity is a tangent, then with $|B| = q + k + 1$ it follows that the total number of tangents not through (∞) is at least $(q+k)(q-k)$, which means that there are at most k^2 non-vertical lines intersecting B in at least two points. □

Now we are ready to prove Blokhuis' theorem in the prime case.

Theorem 2.9 *(Blokhuis [6]) In $PG(2,p)$, p prime, the size of a non-trivial blocking set is at least $3(p+1)/2$.*

Proof: Take a component h (of degree s) of f. Since p is prime, it cannot have zero partial derivative with respect to X. Therefore it has at least $ps - s(s-1)$ points by Lemma 2.5. On the other hand, again since p is prime, it cannot be non-classical with respect to lines. Therefore, by Proposition 0.1 in Stöhr-Voloch [35], it has at most $s(p+s-1)/2$ $\mathrm{GF}(p)$-rational points. This implies

$$ps - s(s-1) \leq s(p+s-1)/2,$$

which means $s \geq (p+3)/3$. In particular, if $|B| < p + 1 + 2(p+3)/3$, then the curve f must be (absolutely) irreducible. Now Lemma 2.5 can be applied to f itself and it says that f has at least $pk - k(k-1)$ points. On the other hand, the previous lemma shows

that it can have at most k^2 points over GF(p). Solving the inequality $pk - k(k-1) \leq k^2$ implies $k \geq (p+1)/2$ indeed. □

Let us repeat the interesting observation that for $|B| < p + 1 + 2(p+3)/3$ the curve f itself must be irreducible. A second proof of a slightly weaker bound will be given in Proposition **??**. In case of a prime-power q the same argument shows that for $|B| \leq p + (p+3)/3$ each component of f whose partial derivative with respect to X is not identically zero must be non-classical with respect to lines. However, the existence of such non-classical components can be excluded by using a pair of curves, as we shall soon see.

2.2 Two curves

In this section we will present the method using two curves. As an application we show that blocking sets of size less than $3(q+1)/2$ intersect every line in 1 modulo p points. This immediately implies Blokhuis' theorem for blocking sets in PG$(2, p)$.

Let now B be a minimal blocking set of PG$(2, q)$ and as usual write it as $B = U \cup D$, where U is the affine part. Only blocking sets with size at most $2q - 1$ will be considered.

It will be convenient to suppose that $D = \{(\infty)\}$ and that the line with equation $x = 0$ does not intersect U. This can be guaranteed by Lemma 2.8. Let $U = \{(a_i, b_i) : i = 1, \ldots q + k\}$ and write up the Rédei polynomial $H(X, Y) = \prod(X + a_i Y - b_i)$ (see Definition 2.1). Since $H(X, Y)$ vanishes for all $(x, y) \in GF(q) \times GF(q)$ (see Proposition 2.3 (1)), we can write it as

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

where $\deg(f), \deg(g) \leq k$ as polynomials in two variables (see [7], [2]). Note that f here is the same as the one defined in Definition 2.2. If one fixes $Y = y$ then $H(X, y)$ is divisible by $(X^q - X)$ and for an $(x, y) \in GF(q) \times GF(q)$: $f(x, y) = 0$ if and only if the line with equation $Y = yX + x$ intersects U in at least two points (cf. Proposition 2.3 (3)). One can repeat the same reasoning for g and this immediately gives the following lemma.

Lemma 2.10 *([39]) If $D = \{(\infty)\}$ and the line $x = 0$ intersects B in just (∞), then the curves f and g have the same set of GF(q)-rational affine points.*

Proof: Since this observation is crucial, a direct proof is also included. Consider the Rédei polynomial $H(X, Y)$. For an element $(x, y) \in GF(q) \times GF(q) : -f(x, y) = H'_X(x, y)$ and similarly $-g(x, y) = H'_Y(x, y)$. Since H is a product of linear factors and $H(x, y) = 0$, $H'_X(x, y) = 0$ if and only if there are two linear factors vanishing at (x, y). The same is true for H'_Y, hence the two derivatives are zero for the same values (x, y). □

Lemma 2.11 *([39]) The polynomials f and g cannot have a common factor.*

Proof: Such a factor must divide $H(X, Y)$, hence it must be divisible by $X + a_i Y - b_i$ for some i. Lemma 2.4 (2) gives ($N = 1$, $k \leq q - 2$) that the point (a_i, b_i) can be deleted, a contradiction. □

Therefore, (f, g) is a pair of polynomials (curves) having no common factor (component), but they pass through the same set of GF(q)-rational points. Using Bézout's theorem it immediately gives Lemma 2.8 back. However, if one does not suppose that the line with equation $x = 0$ does not intersect U, then everything remains the same except that in Lemma 4.1 only the implication $f(x, y) = 0 \Rightarrow g(x, y) = 0$ holds. In this case the curve $g(X, Y)$ has some components of type $X - b_j = 0$, where $(0, b_j)$ is a point of U.

Lemmas 2.10 and 2.11 can also be used to show that all the components of f have identically zero partial derivative with respect to X. Note that for any component h of f the total degree of h is the same as its degree in X.

Theorem 2.12 *([39]) If $k < (q + 1)/2$ and $h(X, Y)$ is an irreducible polynomial that divides $f(X, Y)$, then $h'_X = 0$.*

Proof: Suppose to the contrary that h is a component with nonzero partial derivative. Denote its degree by s. By Lemma 2.5 the number of GF(q)-rational points on h is at least $qs - s(s - 1)$. Since these points are also on g, Bézout's theorem gives

$$qs - s(s - 1) \leq sk,$$

since by Lemma 2.11, g and h cannot have a common component. This immediately implies $q + 1 \leq k + s$ and from $s \leq k$ it follows that $k \geq (q + 1)/2$, a contradiction. □

Of course, this theorem also implies Blokhuis' theorem in the prime case.

Corollary 2.13 *(Blokhuis [6]) If $q = p$ is a prime, then $|B| \geq 3(q + 1)/2$ for the size of a non-trivial blocking set.* □

Proposition 2.14 *If $q = p$ is a prime and $|B| < q + 1 + 2(q + 1)/3$, then the curves f (and g) are irreducible.*

Proof: Suppose to the contrary that f is not irreducible, and let h be a component of f of degree at most $k/2$. The proof of Theorem 2.12 gives $q + 1 \leq k + \deg(h) \leq 3k/2$, that is $k \geq 2(q + 1)/3$. □

The following corollary generalizes the similar result of Rédei on blocking sets of *Rédei type*.

Corollary 2.15 *([39]) If B is a blocking set of size less than $3(q + 1)/2$, then each line intersects it in 1 modulo p points.*

Proof: Since all the components of f contain only terms of exponent (in X) divisible by p, for any fixed $Y = y$ the polynomial $f(X, y)$ itself is the p-th power of a polynomial. This means that at each point (x, y) the line $Y = y$ intersects $f(X, Y)$ with multiplicity divisible by p, so the line $Y = yX + x$ intersects U in 1 modulo p points. □

In the case $q = p^n$ one can prove the following theorem by refining the counting of rational points in the proof of Theorem 2.12.

Theorem 2.16 *(Szőnyi [39]) Let B be a minimal blocking set in $PG(2,q)$, $q=p^n$. Suppose that $|B|<3(q+1)/2$. Then*

$$q+1+\frac{q}{p^e+2}\le |B|\le \frac{qp^e+1-\sqrt{(qp^e+1)^2-4q^2p^e}}{2}, \tag{2}$$

for some integer e, $1\le e\le n/2$. This means that asymptotically

$$|B|\le q+\frac{q}{p^e}+2\frac{q}{p^{2e}}+5\frac{q}{p^{3e}}+\dots . \tag{3}$$

To be more concrete, we have $|B|\le q+9q/(4p^e)$ for every p and e.

If $|B|$ lies in the interval belonging to e and $p^e\neq 4,8$, then each line intersects B in 1 modulo p^e points.

The fact that the lines intersect the blocking set in 1 modulo p^e points was conjectured by Blokhuis [7]. Actually, the lower bounds obtained in Theorem 2.16 are slightly weaker than Blokhuis' lower bounds proved using lacunary polynomials [7]. The consequence of Theorem 2.16 in the particular case $q=p^2$ is the following.

Theorem 2.17 *([39]) Let $q=p^2$ and B be a minimal blocking set which is not a Baer-subplane. Then $|B|\ge 3(q+1)/2$.*

Actually, the same is true for blocking sets with any square q and $e=n/2$. At this point it is worthwhile to note the following interpretation of this theorem: if B is a non-trivial blocking set of size $|B|<3(q+1)/2$, then there is a Baer-subplane contained in it. The bound is essentially better than the previously known ones, we refer to the Introduction for a brief history of results regarding this question.

One can also relate Blokhuis' lacunary polynomial approach to the present one based on algebraic curves, and can prove that the two exponents e are the same. This also permits us to use some recent results from the manuscript [13], which imply that for $p\ge 5$: $n/2>e>n/3$ is not possible. On the other hand, using the fact that each line intersects our blocking sets in 1 modulo p^e points, also the upper bound can slightly be improved. These observations are essentially due to Blokhuis and Polverino [12], who obtained the following theorem.

Theorem 2.18 *(Blokhuis, Polverino) With the notation of Theorem 2.16*

$$q+1+p^e\lceil\frac{q/p^e+1}{p^e+1}\rceil\le |B|\le \frac{1+(p^e+1)(q+1)-\sqrt{\Delta}}{2},$$

where $\Delta=(1+(p^e+1)(q+1))^2-4(p^e+1)(q^2+q+1)$.

Note that this new upper bound is asymptotically $q+q/p^e+q/p^{2e}+2q/p^{3e}+\dots$. This improvement can be used to determine the possible sizes of minimal blocking sets in $\mathrm{PG}(2,p^3)$ as the following corollary shows.

Corollary 2.19 *(Blokhuis, Polverino) Let B be a non-trivial minimal blocking set in $PG(2,p^3)$. Then $|B|=p^3+p^2+1$ or p^3+p^2+p+1.*

The same result for Rédei type blocking sets was already proved by Rédei. Again, the result extends immediately to blocking sets with $e = n/3$. Note that there are examples of minimal blocking sets (of Rédei type) for both cardinalities.

Using the previous results on blocking sets one can improve on the Lunelli, Sce bound for the cardinality of a complete arc, since the secants of a complete arc form a blocking set in the dual plane.

Theorem 2.20 *(Blokhuis, Ball, Blokhuis–Polverino) For a complete k-arc in $PG(2,q)$ we have $k \geq \sqrt{3q}$, if $q = p, p^2$ or p^3, where p is a prime.*

The following application illustrates the method, and shows the parallelity of the ideas concerning lacunary polynomials and algebraic curves. The famous Gács-conjecture [23] stated that in PG(2,p) a minimum blocking set (i.e. of size $3(p+1)/2$) always has many 2-secants. The curves can be used to show this. In the case of the Rédei type example (which is the projective triangle) the 2-secants pass through the vertices of the triangle, so there are exactly $3(p-1)/2$ such lines. In case of the sporadic example for $q = 7$, one can verify directly that there are 12 2-secants, see Ex. 4 in the last section. In that representation there are two 2-secants through the points of D and one through the other points of the infinite line L_∞.

Theorem 2.21 *Let B be a blocking set of cardinality $3(p+1)/2$ in $PG(2,p)$.*
(1) There are at least $(p+1)/2$ lines intersecting it in exactly 2 points.
(2) Through each points of B there are exactly $(p-1)/2$ tangents.

Proof: Consider $f(X,Y)$. It has degree $k = (p+1)/2$ and it has at most k^2 points by Lemma 2.8. On the other hand, it has at least $qk - k(k-1)$ points, see Lemma 2.5. So we must have equality here. Now (2) follows from Lemma 2.8 which says that there are at least $p - k$ tangents at each points. Since there are exactly k^2 non-tangents in this case, it follows that the number of tangents must be exactly $p - k = (p-1)/2$ at each point.

To see (1), observe that the curve has at least $pk - 2k(k-1)$ simple points, where the tangent is not horizontal. Since $pk - 2k(k-1) = k(p+2-2k) = k$, we indeed have at least $(p+1)/2$ 2-secants. □

Remark. (2) follows immediately also from the original lacunary polynomial argument of Blokhuis.

3 Minimum blocking sets in planes of prime order

In PG$(2,p)$, p prime Blokhuis [6] showed that a non-trivial blocking set must contain at least $3(p+1)/2$ points. As mentioned in the Introduction, there are blocking sets having precisely this number of points and the known examples are of Rédei type with just one exception for $p = 7$. Rédei type blocking sets of size $3(p+1)/2$ were characterized by Lovász and Schrijver [30], the sporadic example for $p = 7$ by Gács, Sziklai, Szőnyi [25]. In case of the sporadic example the is a line intersecting the blocking set in $(p+1)/2$ points, which is one less than for blocking sets of Rédei type. For a detailed description of this sporadic example we refer to Example 4 in the next section. Gács went one step

further, he showed in [24] that all the blocking sets of size $3(p+1)/2$ for which there is a line intersecting it in $(p-1)/2$ points (p prime), are of Rédei type with respect to another line. Using curves one can prove that a minimum blocking set cannot be too close to being of Rédei type, see [11]. Actually, this was the result motivating Gács' work, he did the missing case. This section follows closely the paper [11] by Blokhuis, Pellikaan and Szőnyi.

When $q = p$ the Hasse–Weil estimate is not strong enough if the degree of the curve is not very small. Instead we can use the following bound, due to Stöhr–Voloch (see [35], Lemma 2.):

$$N \leq 2n(n-3) + 2n(p+5)/5,$$

where N is the number of GF(p)-rational points and $n \leq p/2$ is the degree of the curve. The next theorem more or less shows that a minimum size blocking set in PG$(2,p)$ cannot be of almost Rédei type.

Theorem 3.1 *Let $q = p$ a prime, and B be a blocking set of cardinality $3(p+1)/2$ in $PG(2,p)$. Suppose that a line L intersects B in at most $(p+3)/2-3$ points. Then*

$$|B \cap L| \leq \frac{(p+3)}{2} - \frac{(p+45)}{20}.$$

Proof: Let $\mathcal{C}_j$ be an irreducible component of degree $s \geq 3$. The number of GF(p)-rational points of $\mathcal{C}_j$ is at least (by Lemma 2.5)

$$(q+1-N)s - s(s-1) \leq (\frac{p-1}{2} + s)s - s(s-1) \leq 2s(s-3) + 2s(p+5)/5,$$

and this yields the bound $s \geq (p+45)/20$. Therefore each component of $\mathcal{C}$ has degree at most two. If there is a linear component, then $|B| \geq 2(p+1-N) > 3(p+1)/2$, if $s \geq 2$, and it is impossible. Similarly, if there is an irreducible component of degree 2, then it has at least $((p-1)/2+s)2 - 2 > 3(p+1)/2$ points, which is again impossible if $s \geq 3$. □

4 Examples

In this section we compute the curves f, g for some well-known blocking sets. The computations are also used to illustrate several results and ideas of the Sections 1, 2.

Ex.1 The *projective triangle.* Let q be odd, $U = \{(0,0)\} \cup \{(0,a) : a \in GF(q)^{*2}\} \cup \{(a,0) : a \in GF(q)^{*2}\}$. We remark that $D = \{(-a) : a \in GF(q)^{*2}\} \cup \{(0)\} \cup \{\infty\}$. Then

$$H(X,Y) = X(X^{\frac{q-1}{2}} - 1)(X^{\frac{q-1}{2}} - (-Y)^{\frac{q-1}{2}}).$$

Substituting (–1) times a non-square (square) element of the field into Y we get $X^q - X$ (or $X(X^{\frac{q-1}{2}} - 1)^2$, resp.).

Ex.2 Let $q = 4k - 1$. If we transform the previous example using $(x_1', x_2', x_3') = (x_1, x_2, x_1 + x_3)$ then $D = \{(\infty)\}$. The affine points are $(0,0); (1,0); (0,s); (\frac{s}{1+s}, 0); (1, -s)$, where $s \in GF(q)^{*2}$. The corresponding factors of $H(X,Y)$ are $X; (X+Y); (X^{\frac{q-1}{2}} - 1); \frac{1}{2}(X^{\frac{q-1}{2}} + [X+Y]^{\frac{q-1}{2}}); ([X+Y]^{\frac{q-1}{2}} + 1)$. The last two may need some explanation:

$$\prod_{s \in GF(q)^{*2}} (X + \frac{s}{1+s}Y) = Y^{\frac{q-1}{2}} \prod_{s \in GF(q)^{*2}} (\frac{X}{Y} + \frac{s}{1+s}) = \rightarrow;$$

here (in general)

$$\prod_{s \in GF(q)^{*2}} (Z + \frac{s}{1+s}) = \frac{1}{2}((Z+1)^{\frac{q-1}{2}} + Z^{\frac{q-1}{2}});$$

so we have

$$\rightarrow = \frac{1}{2}((X+Y)^{\frac{q-1}{2}} + X^{\frac{q-1}{2}}).$$

The last one is

$$\prod(X + Y + s) = \prod_{t \text{ a non-square}} ((X+Y) - t) = [X+Y]^{\frac{q-1}{2}} + 1.$$

So

$$H(X,Y) = X(X+Y)(X^{\frac{q-1}{2}} - 1)(X^{\frac{q-1}{2}} + [X+Y]^{\frac{q-1}{2}})([X+Y]^{\frac{q-1}{2}} + 1) =$$

$$([X^{\frac{q-1}{2}} - 1]X + [X+Y]^{\frac{q+1}{2}} + [X+Y]) \cdot (X^q - X) \; + \; ([X^{\frac{q-1}{2}} - 1]X) \cdot (Y^q - Y).$$

This illustrates the remark that from the points on the y-axis one gets factors depending only on X in $g(X,Y)$. Indeed, our blocking set is of Rédei type with respect to the y-axis. It therefore gives that $g(X,Y)$ depends only on X. What we need is that $f(X,Y)$ cannot be zero if X is a non-square. Now X is a non-square and $X+Y$ is a square implies that $f(X,Y) = 2Y$, which is impossible. Similarly, if $X+Y$ is a non-square or zero, then $f(X,Y) = -2X$, which is not zero, since X is a non-square.

Ex.3 Let $q = 4k+1$. If we transform example 1 using $(x_1', x_2', x_3') = (x_1 - x_3, x_2, x_1 + x_3)$ then $D = \{(\infty)\}$ and the y-axis is a tangent, too.

$$H(X,Y) = (X-Y)(X+Y)([X-Y]^{\frac{q-1}{2}} + 1)([X+Y]^{\frac{q-1}{2}} + [X-Y]^{\frac{q-1}{2}})([X+Y]^{\frac{q-1}{2}} - 1) =$$

$$([X-Y]^{\frac{q+1}{2}} + [X+Y]^{\frac{q+1}{2}} - 2Y) \cdot (X^q - X) \; + \; ([X-Y]^{\frac{q+1}{2}} - [X+Y]^{\frac{q+1}{2}} + 2X) \cdot (Y^q - Y).$$

Then $f - g = 2([X+Y]^{\frac{q+1}{2}} - [X+Y])$ and $f + g = 2([X-Y]^{\frac{q+1}{2}} - [X-Y])$, which shows that if $X+Y =$ square or $X-Y =$ non-square then $f = 0$ iff $g = 0$. If $X+Y =$ non-square and $X-Y =$ square then $f = 0$ (or $g = 0$) imply $Y = 0$ (or $X = 0$, resp.) from

which X (or Y) should be both a square and a non-square. So this example illustrates Lemma 2.10, 2.11.

Ex.4 The *sporadic almost-Rédei blocking set.* The affine plane of order 3 can be embedded into PG(2,7) as the points of inflexion of a non-singular cubic. The 12 lines of this plane cover each point of PG(2,7), so in the dual plane they form a blocking set of size $12 = 3(7+1)/2$, but its maximal line-intersection is only $4 = (12-7)-1$. A characterization of it can be found in [25].

A representation of this blocking set is the following: its affine part is $U = \{(x, -x^6 + 3x^3 + 1) : x \in GF(7)\} \cup \{(0,-1)\}$, the infinite part is $D = \{(0),(1),(2),(4)\}$. Now

$$H(X,Y) = (X^2-1)(X^2-[Y-3]^2)(X^2-[2Y-3]^2)(X^2-[4Y-3]^2),$$

from which for $\mathcal{C}$ we get $f(X,Y) = X + 0Y + 0 = X$. So the lines joining the origin and any point of D are tangents, all the other lines through the origin are 2-secants.

Ex.5 The *Baer-subplane.*

In $PG(2,q^2)$ the standard embedding of a Baer subplane is $\{(s,t) : s,t \in GF(q)\} \cup \{(m) : m \in GF(q)\} \cup \{(\infty)\}$. If we transform it using $(x_1', x_2', x_3') = (x_1, x_2 + wx_3, x_1 + wx_3)$, where $w \in GF(q^2) \setminus GF(q)$, then the only point on the y-axis and the line at infinity remains (∞).

Now its Rédei polynomial is

$$H(X,Y) = \prod_{s,t \in GF(q)} X + \frac{s}{s+w}Y - \frac{t+w}{s+w} \prod_{m \in GF(q)} X + Y - m =$$

$$[X^q - 1 + Y^q - Y + \frac{w^q}{w-w^q}(Y^q - Y)](X^{q^2} - X) + [X - 1 - \frac{w^q}{w-w^q}(X^q - X)](Y^{q^2} - Y).$$

It can be easily seen again how Lemma 2.10, Lemma 2.11, Theorem 2.12 work.

Acknowledgement. The first author thanks the hospitality of Technische Universiteit, Eindhoven and Universita degli Studi della Basilicata, Potenza, where parts of this paper were written.

References

[1] N. Alon, Tools from higher algebra, Chapter 32 in: *Handbook of Combinatorics* (eds.: R. L. Graham, M. Grötschel, L. Lovász), North-Holland, 1995.

[2] S. M. Ball and A. Blokhuis, On the size of a double blocking set in PG$(2,q)$, to appear in *Finite Fields and their Applications.*

[3] L. Berardi and F. Eugeni, Blocking sets e teria dei giochi: origini e problematiche, *Atti Aem. Mat. Fis. Univ. Modena* **34** (1988), 165–196.

[4] A. Bichara, G. Korchmáros, n^2-sets in a projective plane which determine exactly n^2+n lines, *Journal of Geometry* **15** (1980), 175–181.

[5] J. Bierbrauer, On minimal blocking sets, *Arch. Math.* **35** (1980), 394-400.

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

[7] A. Blokhuis, Blocking sets in Desarguesian planes, in: *Paul Erdős is Eighty*, Volume 2, (eds: D. Miklós, V.T. Sós and T. Szőnyi), Bolyai Soc. Math. Studies **2** (1996), 133–155.

[8] A. Blokhuis, S. M. Ball, A. E. Brouwer, L. Storme and T. Szőnyi, On the number of slopes determined by a function on a finite field, manuscript, 1996.

[9] A. Blokhuis and A. E. Brouwer, Blocking Sets in Desarguesian Projective Planes, *Bull. London Math. Soc.* **18** (1986), 132–134.

[10] A. Blokhuis, A. E. Brouwer and T. Szőnyi, The number of directions determined by a function f on a finite field, *J. Comb. Theory, Ser. A.* **70** (1995), 349–353.

[11] A. Blokhuis, R. Pellikaan and T. Szőnyi, Blocking sets of almost Rédei type, *J. Comb. Theory Ser. A*, to appear.

[12] A. Blokhuis, O. Polverino, private communication.

[13] A. Blokhuis, L. Storme and T. Szőnyi, Multiple blocking sets and Baer-subplanes, manuscript 1995.

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

[15] A. E. Brouwer and H. A. Wilbrink, Blocking sets in translation planes, *J. of Geometry* **19** (1982), 200.

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

[17] A. A. Bruen, Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.

[18] A. A. Bruen and R. Silverman, Arcs and Blocking Sets II, *Europ. J. Comb.* **8** (1987), 351–356.

[19] A. A. Bruen and J. A. Thas, Blocking Sets, *Geom. Dedicata* **6** (1977), 193–203.

[20] D. A. Drake, A Bound for Blocking Sets in finite projective planes, in: *Contemporary Math.* **111** *"Finite Geometries and Combinatorial Designs"* (eds.: E. S. Kramer and S. S. Magliveras), Amer Math. Soc. 1991, 93–97.

[21] R. Evans, R. Greene and H. Niederreiter, Linearized Polynomials and Permutation Polynomials of Finite Fields, *Michigan Math. J.* **39** (1992), 405–413.

[22] Z. Füredi, Matchings and Covers in hypergraphs, *Graphs and Combin.* **4** (1988), 115–206.

[23] A. Gács, oral communication.

[24] A. Gács, manuscript.

[25] A. Gács, P. Sziklai, T. Szőnyi, Two remarks on blocking sets and nuclei in planes of prime order, *Designs, Codes and Cryptography*, to appear.

[26] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford (1979).

[27] J. W. P. Hirschfeld, Algebraic curves and arcs over finite fields, *Quad. del Dip. di Mat. Lecce*, **Q.-6** (1987).

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

[29] C. Kitto, A bound for blocking sets of maximal type in finite projective planes, *Arch. Math.* **52** (1989), 203–208.

[30] L. Lovász and A. Schrijver, Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981), 449-454.

[31] L. Lunelli, M. Sce, Considerazioni aritmetiche e risultati sperimentali sui $\{K, n\}_q$-archi, *Ist. Lombardo Accad. Sci. Rend. A* **98** (1964), 3–52.

[32] J. di Paola, On minimum blocking coalitions in small projective plane games, *SIAM J. Appl. Math.* **17** (1969), 378–392.

[33] L. Rédei, *Lückenhafte Polynome über endlichen Körpern.* Birkhäuser Verlag, Basel, 1970.

[34] B. Segre, Introduction to Galois geometries (ed. J.W.P. Hirschfeld), *Mem. Accad. Naz. Lincei* **8** (1967), 133-236.

[35] K. O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52** (1986), 1–19.

[36] T. Szőnyi, k-sets in PG$(2, q)$ with a large set of internal nuclei, in: *Proc. Combinatorics'88* (eds.: A. Barlotti et al.), Mediterranean Press, 1991, 499–511.

[37] T. Szőnyi, Blocking sets in finite planes and spaces, *Ratio Math.* **5** (1992), 93–106.

[38] T. Szőnyi, On the number of directions determined by a pointset of an affine Galois plane, *J. Comb. Theory Ser. A*, **74** (1996), **–**.

[39] T. Szőnyi, Blocking sets in desarguesian affine and projective planes, submitted to *Finite Fields and Appl.*

[40] T. Szőnyi, Some applications of algebraic curves in finite geometry and combinatorics, in: *Surveys in Combinatorics* (ed.: R. A. Bailey), Cambridge Univ. Press, to appear.

[41] J. A. Thas, Projective geometry over a finite field, Chapter *in* "Handbook of Incidence Geometry (ed.: F. Buekenhout)," North-Holland, 1995.

[42] J. F. Voloch, Arcs in projective planes over prime fields, *J. of Geometry* **38** (1990), 198–200.

P. Sziklai, MTA MKI, Reáltanoda u. 13-15, H-1053 Budapest, Hungary (sziklai@math-inst.hu)

T. Szőnyi, Dept. of Computer Science, Eötvös Loránd University, Múzeum krt. 6-8, H-1088 Budapest, Hungary (szonyi@cs.elte.hu)

and Dept. of Geometry, Attila József University, Aradi vértanúk tere 1, H-6720 Szeged, Hungary