page 1 / 27

go back

full screen

close

quit

Semiarcs with a long secant in $\mathrm{PG}(2, q)$

Bence Csajbók* Tamás Héger† György Kiss‡

Abstract

A t-semiarc is a point set $\mathcal{S}_t$ with the property that the number of tangent lines to $\mathcal{S}_t$ at each of its points is t. We show that if a small t-semiarc $\mathcal{S}_t$ in $\mathrm{PG}(2, q)$ has a large collinear subset $\mathcal{K}$, then the tangents to $\mathcal{S}_t$ at the points of $\mathcal{K}$ can be blocked by t points not in $\mathcal{K}$. In fact, we give a more general result for small point sets with less uniform tangent distribution. We show that in $\mathrm{PG}(2, q)$ small t-semiarcs are related to certain small blocking sets and give some characterization theorems for small semiarcs with large collinear subsets.

Keywords: finite plane, semiarc, semioval, blocking set, Szőnyi–Weiner Lemma

MSC 2010: 51E20, 51E21

1. Introduction

Ovals, k-arcs and semiovals of finite projective planes are interesting geometric structures which also have applications to coding theory and cryptography. For details we refer the reader to [3, 14, 22, 24, 27].

Semiarcs are natural generalizations of arcs. Throughout the paper Π_q denotes an arbitrary projective plane of order q. By $\mathrm{PG}(2, q)$ and $\mathrm{AG}(2, q)$ we denote the desarguesian projective and affine planes. A non-empty point set

*Author was supported by the Hungarian National Foundation for Scientific Research (OTKA), Grant No. K 81310.

†Author was supported by the Hungarian National Foundation for Scientific Research (OTKA), Grant No. K 81310 and by ERC Grant No. 227701 DISCRETECONT.

‡Author was supported by the Hungarian National Foundation for Scientific Research (OTKA), Grant No. K 81310 and by the Slovenian–Hungarian Intergovernmental Scientific and Technological Cooperation Project, Grant No. TÉT 10-1-2011-0606.

$\subset \Pi_q$ is called a *t-semiarc* if for every point $P \in$ there exist exactly $t \geq 1$ lines $\ell_1, \ell_2, \ldots, \ell_t$ such that $\cap \, \ell_i = \{P\}$ for $i = 1, 2, \ldots, t$. These lines are called the *tangents* to at P. If a line ℓ meets in k points, then ℓ is called a *k-secant* of ; a 0-secant is also called a *skew line* to . We say that a k-secant is *long*, if $q - k$ is a small number (which will be given a precise meaning later). The classical examples of t-semiarcs are the k-arcs (with $t = q + 2 - k$), subplanes (with $t = q - m$, where m is the order of the subplane) and semiovals (i.e. semiarcs with $t = 1$, e.g. ovals or unitals). Note that if we allowed $t = 0$, a 0-semiarc would be a set without tangents (a so-called *untouchable set*); see [11, 9, 38].

The complete classification of semiarcs is hopeless. The aim of this paper is to investigate and characterize semiarcs having some additional properties. In Section 2 we consider a very special class, namely t-semiarcs of size $k + q - t$ having a k-secant. These point sets are closely related to the widely studied structures defining few directions [1, 6, 7, 35]. In Section 3 we prove that in $\mathrm{PG}(2, q)$ if a small t-semiarc has a large collinear subset $\mathcal{K}$, then the tangent lines at the points of $\mathcal{K}$ belong to t pencils whose carriers are not in $\mathcal{K}$. This result generalizes the main result in Kiss [26]. Small semiovals with large collinear subsets were studied in arbitrary projective planes as well, see Bartoli [2] and Dover [18]. The essential part of our proof is algebraic, it is based on an application of the Rédei polynomial and the Szőnyi–Weiner Lemma. In fact, the main result of this section is more general as it is valid for small point sets with less uniform tangent distribution as well. In Section 4 we associate to each t-semiarc a blocking set. If is small and has a long secant, then the associated blocking set is small. Applying theorems about the structure of small blocking sets we prove some characterization theorems for semiarcs.

When $t \geq q - 2$, then it is easy to characterize t-semiarcs. If $t = q + 1$, q or $q - 1$, then is a single point, a subset of a line of size at least two, or three non-collinear points, respectively; see [16, Proposition 2.1]. Hence, if no other bound is specified, we usually assume that $t \leq q - 2$. If $t = q - 2$, then it follows from [16, Proposition 3.1] that is one of the following three configurations: four points in general position, the six vertices of a complete quadrilateral, or a Fano subplane. Thus sometimes we may assume that $t \leq q - 3$, which we indicate individually.

Throughout the paper we use the following notation. We denote points at infinity of $\mathrm{PG}(2, q)$, i.e. points on the line $\ell_\infty = [0 : 0 : 1]$, by (m) instead of the homogeneous coordinates $(1 : m : 0)$. We simply write Y_∞ and X_∞ instead of $(0 : 1 : 0)$ and $(1 : 0 : 0)$, respectively. The points of ℓ_∞ are also called directions. For affine points, i.e. points of $\mathrm{PG}(2, q) \setminus \ell_\infty$, we use the Cartesian coordinates (a, b) instead of $(a : b : 1)$. If P and Q are distinct points in Π_q, then PQ denotes the unique line joining them. If $\mathcal{A}$ and $\mathcal{B}$ are two point sets in Π_q, then $\mathcal{A} \triangle \mathcal{B}$

ACADEMIA
PRESS
UNIVERSITEIT
GENT

denotes their symmetric difference, i.e. $(\mathcal{A} \setminus \mathcal{B}) \cup (\mathcal{B} \setminus \mathcal{A})$.

Blocking sets play an important role in our proofs. For the sake of completeness we collect the basic definitions and some results about these objects. A *blocking set* $\mathcal{B}$ in a projective or affine plane is a set of points which intersects every line. If $\mathcal{B}$ contains a line, then it is called *trivial*. A point P in a blocking set $\mathcal{B}$ is *essential* if $\mathcal{B} \setminus \{P\}$ is not a blocking set, i.e. there is a tangent line to $\mathcal{B}$ at the point P. A blocking set is said to be *minimal* when no proper subset of it is a blocking set or, equivalently, each of its points is essential. If ℓ is a line containing at most q points of a blocking set $\mathcal{B}$ in Π_q, then $|\mathcal{B}| \geq q + |\ell \cap \mathcal{B}|$. In case of equality $\mathcal{B}$ is a blocking set of *Rédei type* and ℓ is a *Rédei line* of $\mathcal{B}$. Note that we also consider a line to be a blocking set of Rédei type. A blocking set in $\mathrm{PG}(2,q)$ is said to be *small* if its size is less than $3(q+1)/2$. We close this section by collecting some results on blocking sets by Szőnyi; Polverino, Sziklai and Szőnyi; and Blokhuis, Bruen, Storme and Szőnyi.

Theorem 1.1 ([34, Remark 3.3 and Corollary 4.8]). *Let $\mathcal{B}$ be a blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime. If $|\mathcal{B}| \leq 2q$, then $\mathcal{B}$ contains a unique minimal blocking set. If $\mathcal{B}$ is a small minimal blocking set, then each line intersects $\mathcal{B}$ in $1 \pmod{p}$ points.*

Note that a blocking set contains a unique minimal blocking set if and only if the set of its essential points is a blocking set. The next result generalizes the second part of the above theorem.

Theorem 1.2 ([32, Corollary 5.1], [31, 34]). *Let $\mathcal{B}$ be a small minimal blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime. Then there exists a positive integer e, called the exponent of $\mathcal{B}$, such that e divides h, and*

$$q + 1 + p^e \left\lceil \frac{q/p^e + 1}{p^e + 1} \right\rceil \leq |\mathcal{B}| \leq \frac{1 + (p^e+1)(q+1) - \sqrt{D}}{2},$$

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

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

Theorem 1.3 ([4, 10, 13]). *Let $\mathcal{B}$ be a minimal blocking set in $\mathrm{PG}(2,q)$, $q = p^h$, p prime. Let $|\mathcal{B}| = q + 1 + k$, and let $c_p = 2^{-1/3}$ for $p = 2, 3$ and $c_p = 1$ for $p > 3$. Then the following hold.*

1. *If $h = 1$ and $k \leq (q+1)/2$, then $\mathcal{B}$ is a line, or $k = (q+1)/2$ and each point of $\mathcal{B}$ has exactly $(q-1)/2$ tangent lines.*

2. *If $h = 2d + 1$ and $k < c_p q^{2/3}$, then $\mathcal{B}$ is a line.*

3. *If $k \leq \sqrt{q}$, then $\mathcal{B}$ is a line, or $k = \sqrt{q}$ and $\mathcal{B}$ is a Baer subplane (i.e. a subplane of order $\sqrt{q}$).*

We remark that the third point of the above theorem holds in arbitrary finite projective planes.

2. Semiarcs and the direction problem

In this section we give and characterize several examples of semiarcs with a particular extremal property. We will often need the following basic observation.

Proposition 2.1. *Let be a t-semiarc in Π_q, and let ℓ be an arbitrary line. Then $|| \geq q - t + |\ell \cap|$. If equality holds, then for any line ℓ' intersecting $\setminus \ell$ in at least two points we have $\ell \cap \ell' \notin$.*

Proof. Let $k = |\ell \cap|$. As through any point of there are $q + 1 - t$ non-tangent lines to , we clearly have $|| \geq q+2-t$; thus the assertion trivially holds for $k \leq 1$. Suppose $k \geq 2$. For any point $P \in \cap \ell$ there are $q + 1 - t$ non-tangent lines to through P, one of which is ℓ, and each of the remaining $q - t$ non-tangent lines contains at least one point from $\setminus \ell$. In case of equality we see that lines through the points of $\ell \cap$ different from ℓ contain either one or zero points from $\setminus \ell$. □

If k is the size of the largest collinear subset of a semioval , then, by the above proposition, we may always assume that $|| = k + q - t + \varepsilon$ where $\varepsilon \geq 0$. In this section we investigate the case $\varepsilon = 0$.

Definition 2.2. We call a t-semiarc *tight* if $|| = q - t + |\ell \cap|$ holds for some line ℓ. Such lines are called *maximal secants (of)*. For a semiarc , $\kappa()$ denotes the largest number k such that admits a k-secant.

Notice that for any t-semiarc , $t < q$ implies $\kappa() \leq q + 1 - t$. Csajbók investigated the case of equality.

Theorem 2.3 ([15, Theorem 4])**.** *In* $\mathrm{PG}(2, q)$*, if a t-semiarc with a $(q + 1 - t)$-secant exists, then $t \geq (q - 1)/2$.*

Thus, if t is small, then $\kappa() \leq q - t$ follows, and hence a tight t-semiarc has at most $2(q - t)$ points.

Example 2.4 (V_t-configuration)**.** Let ℓ_1 and ℓ_2 be two distinct lines in Π_q, and let $\mathcal{T}_1 \subset \ell_1 \setminus \ell_2$, $\mathcal{T}_2 \subset \ell_2 \setminus \ell_1$, $|\mathcal{T}_1| = |\mathcal{T}_2| = t$ and $1 \leq t \leq q-2$. Then $= (\ell_1 \triangle \ell_2) \setminus (\mathcal{T}_1 \cup \mathcal{T}_2)$ is a t-semiarc. Such semiarcs are called V_t-configurations; they are tight and have $2(q-t)$ points.

Proposition 2.5 ([16, Proposition 2.2])**.** *Let Π_q be a projective plane of order q, and let $t \leq q-2$. If a t-semiarc in Π_q is contained in the union of two lines, then is a V_t-configuration.*

It is easy to give a combinatorial characterization of t-semiarcs of size $2(q-t)$ with a $(q-t)$-secant. For semiovals, this was also done by Bartoli [2, Corollary 9].

Proposition 2.6. *Let Π_q be a projective plane of order q, and let $t \leq q-2$. If is a t-semiarc of size $2(q-t)$ with a $(q-t)$-secant ℓ (i.e. a tight t-semiarc of size $2(q-t)$), then is a V_t-configuration.*

Proof. Let $\mathcal{U} = \setminus \ell$. Recall that if ℓ' is a line joining two points of $\mathcal{U}$, then $\ell \cap \ell' \notin$. Now suppose to the contrary that there exist three non-collinear points in $\mathcal{U}$. They determine three lines, each of which intersects ℓ in $\ell \setminus$; hence at these three points of $\mathcal{U}$ there are at most $t-1$ tangents to , a contradiction. Thus the points of $\mathcal{U}$ are contained in a line ℓ' and $\ell \cap \ell' \notin$. $\square$

The following example shows the existence of tight t-semiarcs with three maximal secants for odd values of t.

Example 2.7. Let C denote the set of non-squares in the field $\mathrm{GF}(q)$, q odd. The point set $\{(0:1:s), (s:0:1), (1:s:0) \ : \ -s \in C\}$ is a semioval in $\mathrm{PG}(2,q)$ of size $3(q-1)/2$ with three $(q-1)/2$-secants, see Blokhuis [5]. We refer to this construction as *Blokhuis' semioval*. If we delete $r < (q-1)/2 - 2$ points from each of the $(q-1)/2$-secants, then the remaining point set is a tight t-semiarc with three maximal secants, where $\kappa() = (q-1)/2 - r$ and $t = 2r+1$.

There also exist examples if t is even. To give their construction, we need some notation. A (k,n)*-arc* is a set of k points such that each line contains at most n of these points. A set $\mathcal{T}$ of $q+t$ points in Π_q for which each line meets $\mathcal{T}$ in 0, 2 or t points ($t \neq 0, 2$) is either an oval (for $t=1$), or a $(q+t,\, t)$-arc of type $(0,\, 2,\, t)$. Korchmáros and Mazzocca [29, Proposition 2.1] proved that $(q+t,\, t)$-arcs of type $(0,\, 2,\, t)$ exist in Π_q only if q is even and $t \mid q$. They also provided infinite families of examples in $\mathrm{PG}(2,q)$ whenever the field $\mathrm{GF}(q/t)$ is a subfield of $\mathrm{GF}(q)$. It is easy to see that through each point of $\mathcal{T}$ there passes exactly one t-secant. In [21] new constructions were given by Gács and Weiner, and they proved that in $\mathrm{PG}(2,q)$ the $q/t+1$ t-secants of $\mathcal{T}$ pass through one point, called the t-nucleus of $\mathcal{T}$ (for $t=1$ and arbitrary projective plane of even order, see e.g. [24, Lemma 8.6]). Recently Vandendriessche [39] found a new infinite family with $t=q/4$. Using linear sets, De Boeck and Van de Voorde have reinterpreted this family, and also described a new family with $t=q/4$ [17].

Example 2.8. Let $\mathcal{T}$ be a $(q+\tau,\,\tau)$-arc of type $(0,\,2,\,\tau)$ in Π_q. Delete $1\leq r<\tau-2$ points from each of the τ-secants of $\mathcal{T}$. The remaining points form a tight t-semiarc with $q/\tau+1$ maximal secants, $t=rq/\tau$ and $\kappa()=\tau-r$.

Since $(q+q/2,\,q/2)$-arcs of type $(0,\,2,\,q/2)$ exist in $\mathrm{PG}(2,q)$, q even, this construction gives t-semiarcs for each $t\leq q-6$, t even.

The so-called direction problem is closely related to tight semiarcs. We briefly collect the basic definitions and some results about this problem. Consider $\mathrm{PG}(2,q)=\mathrm{AG}(2,q)\cup\ell_\infty$. Let $\mathcal{U}$ be a set of points of $\mathrm{AG}(2,q)$. A point P of ℓ_∞ is called a *direction determined by* $\mathcal{U}$ if there is a line through P that contains at least two points of $\mathcal{U}$. The set of directions determined by $\mathcal{U}$ is denoted by $D_{\mathcal{U}}$. If $|\mathcal{U}|=q$, then $\mathcal{U}\cup D_{\mathcal{U}}$ is a blocking set of Rédei type. If $Y_\infty\notin D_{\mathcal{U}}$, then $\mathcal{U}$ can be considered as a graph of a function. Note that all these definitions make sense in non-desarguesian planes as well. Using these notions, we first give a general example of tight semiarcs.

Example 2.9. Let ℓ be a line of Π_q, and let $\mathcal{U}$ be a set of $m<q$ points in the affine plane $\Pi_q\setminus\ell$. Consider directions with respect to $\ell=\ell_\infty$. Assume $|D_{\mathcal{U}}|<m$, and denote $q-m$ by t. Let $\overline{D}=\ell_\infty\setminus D_{\mathcal{U}}$ and let $\mathcal{T}\subset\overline{D}$ be a set of t points. Suppose that $\mathcal{U}\cup D_{\mathcal{U}}$ does not have 2-secants. Then the set $\mathcal{S}_t=\mathcal{U}\cup(\overline{D}\setminus\mathcal{T})$ is a tight t-semiarc with $\kappa(\mathcal{S}_t)=m-|D_{\mathcal{U}}|+1$.

Proof. As $|\ell_\infty\cap\mathcal{S}_t|=q+1-|D_{\mathcal{U}}|-t=m-|D_{\mathcal{U}}|+1>1$, ℓ_∞ is not tangent to $\mathcal{S}_t$. If $P\in\overline{D}\setminus\mathcal{T}$, then all lines through P, except ℓ_∞, intersect $\mathcal{U}$ in either zero or one point, hence the number of tangents through P to $\mathcal{S}_t$ is $q-|\mathcal{U}|=t$. Now let $P\in\mathcal{U}$, and consider a line ℓ through P. According to whether ℓ intersects ℓ_∞ in $D_{\mathcal{U}}$, $\overline{D}\setminus\mathcal{T}$ or $\mathcal{T}$, $|\ell\cap\mathcal{S}_t|$ is at least two, exactly two or exactly one, respectively. Thus there pass precisely $|\mathcal{T}|=t$ tangents to $\mathcal{S}_t$ through P. $\square$

We will consider two particular examples.

Example 2.10 (Altered Baer subplane)**.** Let $\Pi_{\sqrt{q}}$ be a Baer subplane in the projective plane Π_q, $q\geq 9$, and let ℓ be an extended line of $\Pi_{\sqrt{q}}$. Let $\mathcal{P}$ be a set of $1\leq t\leq q-\sqrt{q}-2$ points in $\Pi_{\sqrt{q}}\setminus\ell$ such that no line intersects $\mathcal{P}$ in exactly $\sqrt{q}-1$ points. For example, a $(t,\,\sqrt{q}-2)$-arc is a good choice for $\mathcal{P}$. Example 2.9 with $\mathcal{U}=\Pi_{\sqrt{q}}\setminus(\ell\cup\mathcal{P})$ gives a tight t-semiarc with $\kappa()=q-\sqrt{q}-t$.

The other particular semiarc obtained from Example 2.9 is based on the following result of Blokhuis et al. [6] and Ball [1].

Theorem 2.11 ([6, 1]). *Let $\mathcal{U} \subset \mathrm{AG}(2, q)$, $q = p^h$, p prime, be a point set of size q. Let $z = p^e$ be maximal having the property that if $P \in D_{\mathcal{U}}$ and ℓ is a line through P, then ℓ intersects $\mathcal{U}$ in $0 \pmod z$ points. Then one of the following holds:*

1. *$z = 1$ and $(q + 3)/2 \le |D_{\mathcal{U}}| \le q + 1$,*
2. *$\mathrm{GF}(z)$ is a subfield of $\mathrm{GF}(q)$ and $q/z + 1 \le |D_{\mathcal{U}}| \le (q - 1)/(z - 1)$,*
3. *$z = q$ and $|D_{\mathcal{U}}| = 1$.*

Let $\mathcal{B}$ be a small blocking set of Rédei type in $\mathrm{PG}(2, q)$, $q = p^h$, p prime, and let ℓ be one of its Rédei lines. Since $|\mathcal{B}| < 3(q+1)/2$, we have $|\ell \cap \mathcal{B}| < (q+3)/2$. Hence the previous theorem implies that there exists an integer e such that e divides h, $1 < p^e \le q$ holds, and each affine line intersects $\mathcal{B}$ in $1 \pmod{p^e}$ points.

Example 2.12 (Altered Rédei type blocking set). Let $\mathcal{B}$ be a small minimal blocking set of Rédei type in $\mathrm{PG}(2, q)$, $q = p^h$, p prime, and let ℓ be a Rédei line of $\mathcal{B}$. Let $\mathcal{P}$ be a set of $1 \le t \le q - |\mathcal{B} \cap \ell| - 1$ points in $\mathcal{B} \setminus \ell$ such that for each line ℓ' intersecting $\mathcal{B}$ in more than one point we have $|\ell' \cap \mathcal{P}| \ne |\ell' \cap \mathcal{B}| - 2$. For example, if $z = p^e$ denotes the maximal number such that each line intersects $\mathcal{B}$ in $1 \pmod z$ points (cf. Theorem 2.11) and $z \ge 3$, then a $(t, z - 2)$-arc is a good choice for $\mathcal{P}$. Example 2.9 with $\mathcal{U} = \mathcal{B} \setminus (\ell \cup \mathcal{P})$ gives a tight t-semiarc with $\kappa() = 2q + 1 - |\mathcal{B}| - t$. (Note that if $\mathcal{B}$ is a line, then is a V_t-configuration.)

Next we show that a tight semiarc in $\mathrm{PG}(2, q)$, if t is small and $\kappa()$ is large, is an altered Rédei type blocking set. To this end, besides the results about the number of directions determined by a set of q affine points, we also need results on the extendability of a set of almost q affine points to a set of q points such that the two point sets determine the same directions. The first such extendability theorem was proved by Blokhuis [5]; see also Szőnyi [35].

Theorem 2.13 ([5, Proposition 2], [35, Remark 7]). *Let $\mathcal{U} \subset \mathrm{AG}(2, q)$, $q \ge 3$, be a point set of size $q - 1$. Then there exists a unique point P such that the point set $\mathcal{U} \cup \{P\}$ determines the same directions as $\mathcal{U}$.*

Extending a result of Szőnyi [35, Theorem 4], Sziklai proved the following theorem.

Theorem 2.14 ([33, Theorem 3.1]). *Let $\mathcal{U} \subset \mathrm{AG}(2, q)$ be a point set of size $q - n$ where $n \le \alpha\sqrt{q}$ for some $1/2 \le \alpha < 1$. If $|D_{\mathcal{U}}| < (q + 1)(1 - \alpha)$, then $\mathcal{U}$ can be extended to a set $\mathcal{U}'$ of size q such that $\mathcal{U}'$ determines the same directions as $\mathcal{U}$.*

ACADEMIA PRESS

We also need the following lemma.

Lemma 2.15. *Let z and t be two positive integers such that $z \geq 3$ and $t \leq \sqrt{q(z-1)/z}$. Let $\mathcal{U} \subset \mathrm{AG}(2,q)$ be a set of $q-t$ affine points, and let $E \subseteq F$ be two sets of directions satisfying the following properties:*

1. *there are at least t tangents to $\mathcal{U}$ with direction in F through each point of $\mathcal{U}$;*
2. *there exists a suitable set of t affine points, $\mathcal{P}$, such that $\mathcal{U} \cap \mathcal{P} = \emptyset$ and each tangent to $\mathcal{U}$ with direction not in E intersects $\mathcal{U} \cup \mathcal{P}$ in $0 \pmod{z}$ points.*

Then $|E| \geq t$.

Proof. If ℓ is a tangent to $\mathcal{U}$ intersecting $F \setminus E$, then $|\mathcal{P} \cap \ell| \equiv -1 \pmod{z}$. The maximum number of such tangent lines is $\frac{t(t-1)}{(z-1)(z-2)}$. Hence at least $(q-t)t - \frac{t(t-1)}{(z-1)(z-2)}$ tangents to $\mathcal{U}$ have direction in E. This implies

$$|E|q \geq (q-t)t - \frac{t(t-1)}{(z-1)(z-2)}, \quad \text{thus} \quad (|E|-t)q \geq -t^2 - \frac{t(t-1)}{(z-1)(z-2)}.$$

If $|E|-t$ is a negative integer, then this inequality gives $q < t^2 \frac{(z-1)(z-2)+1}{(z-1)(z-2)} \leq t^2 z/(z-1)$, contradicting the assumption $t \leq \sqrt{q(z-1)/z}$. □

Theorem 2.16. *Let be a tight t-semiarc in $\mathrm{PG}(2,q)$, $q = p^h$, p prime. Suppose that one of the following conditions hold:*

- *$t = 1$, $q > 4$ and $\kappa(\mathcal{S}_1) > (q-1)/2$, or*
- *$2 \leq t \leq \alpha\sqrt{q}$ and $\kappa() > \alpha(q+1)$ for some $1/2 \leq \alpha \leq \sqrt{(p-1)/p}$ if p is an odd prime, and $1/2 \leq \alpha \leq \sqrt{3}/2$ if $p = 2$.*

Then is an altered Rédei type blocking set.

Proof. Let $k = \kappa()$ and let ℓ be a k-secant of . Take ℓ as the line at infinity and let $\mathcal{U} = \setminus \ell \subseteq \mathrm{AG}(2,q)$. The directions in $\cap \ell$ are not determined by $\mathcal{U}$, hence $|D_{\mathcal{U}}| \leq q+1-k$. We can apply Theorem 2.13 when $t = 1$; if $t \geq 2$, then the conditions of Theorem 2.14 hold since $|\mathcal{U}| = q-t$, $t \leq \alpha\sqrt{q}$ and $|D_{\mathcal{U}}| < (q+1)(1-\alpha)$. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_t\}$ be a set of t points such that $\mathcal{U} \cup \mathcal{P}$ determines the same directions as $\mathcal{U}$.

First consider the case $t \geq 2$. We have $|D_{\mathcal{U}}| < (q+1)/2$, thus applying Theorem 2.11 we get that there exists an integer $z = p^e \geq 3$ such that each affine line with direction in $D_{\mathcal{U}}$ intersects $\mathcal{U} \cup \mathcal{P}$ in $0 \pmod{z}$ points. We can apply Lemma 2.15 with $F = \ell \setminus$ and $E = \ell \setminus (\cup D_{\mathcal{U}})$ to obtain $|E| \geq t$. Note that in the case $p = 2$ we have $z \geq 4$, hence $\alpha \leq \sqrt{3}/2$ is enough to apply Lemma 2.15. On the other hand the lines joining any point of E with any point of $\mathcal{U}$ are tangents to , thus $|E| \leq t$. The same observation implies that each of the tangents to at the points of $\mathcal{U}$ meets E. Let $\mathcal{B} = \mathcal{U} \cup \mathcal{P} \cup D_{\mathcal{U}}$, which is a small blocking set of Rédei type. Let $\ell' \neq \ell$ be a line intersecting $\mathcal{B}$ in more than one point and let $M = \ell' \cap \ell$. Then $M \in D_{\mathcal{U}} \subseteq \mathcal{B}$ and $M \notin E$. If $|\ell' \cap \mathcal{P}| = |\ell' \cap \mathcal{B}| - 2$, then ℓ' would be a tangent to at the unique point of $\ell' \cap \mathcal{U}$, but this is a contradiction since $M \notin E$. We obtained Example 2.12.

If $t = 1$, then in the same way (using Theorem 2.13 instead of 2.14) we get that there exists an integer $z = p^e \geq 2$ such that each affine line with direction in $D_{\mathcal{U}}$ intersects $\mathcal{U} \cup \{P_1\}$ in $0 \pmod z$ points. If $z \geq 3$, then we can finish the proof as above; otherwise Theorem 2.11 implies $|D_{\mathcal{U}}| \geq q/2 + 1$. Compared to $|D_{\mathcal{U}}| < (q+3)/2$, we get $|D_{\mathcal{U}}| = q/2 + 1$ and hence $k = q/2$. This means that each of the $q - 1$ tangent lines to $\mathcal{S}_1$ at the points of $\mathcal{U}$ intersects ℓ in $D_{\mathcal{U}}$. Thus these lines have $0 \pmod{z = 2}$ points in $\mathcal{U} \cup \{P_1\}$, so they pass through P_1. If $q > 4$, then $q - 1 > q/2 + 1$, thus at least one of these tangents would intersect ℓ in $\mathcal{S}_1$, a contradiction. $\square$

In desarguesian planes of prime or prime square order, there are stronger results regarding the direction problem. As a corollary, we get the characterization of Blokhuis' semioval and the altered Baer subplane semioval. The three cases of the next theorem were proved by Lovász and Schrijver [30], by Gács [19], and by Gács, Lovász and Szőnyi [20], respectively.

Theorem 2.17 ([30, 19, 20]). *Let $\mathcal{U}$ be a set of q points in $\mathrm{AG}(2,q)$, $q = p^h$, $h \leq 2$, p prime.*

1. *If $h = 1$ and $|D_{\mathcal{U}}| = (p+3)/2$, then $\mathcal{U}$ is affinely equivalent to the graph of the function $x \mapsto x^{\frac{p+1}{2}}$.*
2. *If $h = 1$ and $|D_{\mathcal{U}}| > (p+3)/2$, then $|D_{\mathcal{U}}| \geq \lfloor 2(p-1)/3 \rfloor + 1$.*
3. *If $h = 2$ and $|D_{\mathcal{U}}| \geq (p^2+3)/2$, then either $|D_{\mathcal{U}}| = (p^2+3)/2$ and $\mathcal{U}$ is affinely equivalent to the graph of the function $x \mapsto x^{\frac{p^2+1}{2}}$, or $|D_{\mathcal{U}}| \geq (p^2+p)/2 + 1$.*

Corollary 2.18. *Let $\mathcal{S}_1$ be a tight semioval in $\mathrm{PG}(2,q)$, $3 \leq q = p^h$, $h \leq 2$, p prime. Then we have the following.*

1. *If $h = 1$ and $\kappa(\mathcal{S}_1) > \min\{(p-3)/2, (p+4)/3\}$, then there are two possibilities:*
   - *$\mathcal{S}_1$ is a V_1-configuration,*

ACADEMIA PRESS
UNIVERSITEIT GENT

- *$\mathcal{S}_1$ is Blokhuis' semioval (cf. Example 2.7).*

2. *If $h = 2$ and $\kappa(\mathcal{S}_1) > (p^2 - p)/2$, then there are four possibilities:*

   - *$\mathcal{S}_1$ is of a V_1-configuration,*
   - *$\mathcal{S}_1$ is Blokhuis' semioval,*
   - *$\mathcal{S}_1$ is an altered Baer subplane,*
   - *$p = 2$ and $\mathcal{S}_1$ is an oval in $\mathrm{PG}(2,4)$.*

Proof. Let $k = \kappa(\mathcal{S}_1)$, and let ℓ be a k-secant of $\mathcal{S}_1$. Consider ℓ as the line at infinity and let $\mathcal{U} = \mathcal{S}_1 \setminus \ell$. The points of $\ell \cap \mathcal{S}_1$ are not determined directions, hence we have $k + |D_{\mathcal{U}}| \leq q + 1$. As the point set $\mathcal{U}$ has size $q - 1$, it follows from Theorem 2.13 that there exists a point P such that $\mathcal{U} \cup \{P\}$ determines the same directions as $\mathcal{U}$.

First consider the case $h = 1$. If $k > \min\{(p-3)/2,\ (p+4)/3\}$, then $|D_{\mathcal{U}}| < \max\{\lfloor 2(p-1)/3 \rfloor + 1,\ (p+5)/2\}$ and thus Theorems 2.11 and 2.17 imply that either $|D_{\mathcal{U}}| = 1$ and $\mathcal{U}$ is contained in a line, or $|D_{\mathcal{U}}| = (p+3)/2$ and $\mathcal{U} \cup \{P\}$ is affinely equivalent to the graph of the function $x \mapsto x^{\frac{p+1}{2}}$. In the first case it is easy to see that $\mathcal{S}_1$ is a V_1-configuration. In the latter case the graph of $x \mapsto x^{\frac{p+1}{2}}$ is contained in two lines, namely $[1:1:0]$ and $[1:-1:0]$, and these lines are $(p+1)/2$-secants of $\mathcal{U} \cup \{P\}$. It is easy to see that P has to be the point $(0:0:1)$, thus $\mathcal{S}_1$ has (at least) two $(p-1)/2$-secants, and it is contained in a vertexless triangle. Such semiovals were characterized by Kiss and Ruff [28, Theorem 3.3]; it follows from their characterization that $\mathcal{S}_1$ must be Blokhuis' semioval.

Now suppose that $h = 2$. If $k > (p^2 - p)/2$, then $|D_{\mathcal{U}}| < (p^2 + p)/2 + 1$, thus $|D_{\mathcal{U}}| \in \{1, (p^2+3)/2\}$ or $1 < |D_{\mathcal{U}}| < (p^2+3)/2$. If $|D_{\mathcal{U}}| = 1$ or $|D_{\mathcal{U}}| = (p^2+3)/2$, then we can argue as before. In the remaining case it follows from Theorems 2.11 and 1.3 (or already from [34, Theorem 5.7]), that $|D_{\mathcal{U}}| = p + 1$ and $\mathcal{U} \cup \{P\} \cup D_{\mathcal{U}}$ is a Baer subplane. If $p > 2$, then $\mathcal{S}_1$ has exactly $p^2 - p - k$ tangents at each point of $\mathcal{U}$, hence $k = p^2 - p - 1$ and $\mathcal{S}_1$ is an altered Baer subplane. Finally, if $p = 2$, then $k \geq 2$ and $|D_{\mathcal{U}}| = p + 1 = 3$, thus $k = 2$ and $\mathcal{S}_1$ is an oval in $\mathrm{PG}(2,4)$. $\square$

3. Proof of the main lemma

First we collect the most important properties of the Rédei polynomial. Consider a point set $\mathcal{U} = \{(a_i, b_i) : i = 1, 2, \ldots, |\mathcal{U}|\}$ of the affine plane $\mathrm{AG}(2,q)$. The

ACADEMIA PRESS
UNIVERSITEIT GENT

Rédei polynomial of $\mathcal{U}$ is

$$H(X,Y) = \prod_{i=1}^{|\mathcal{U}|}(X + a_iY - b_i) \in \mathrm{GF}(q)[X,Y].$$

For any fixed value $y \in \mathrm{GF}(q)$, the univariate polynomial $H(X,y) \in \mathrm{GF}(q)[X]$ is fully reducible and it reflects some geometric properties of $\mathcal{U}$.

Lemma 3.1 (folklore)**.** *Let $H(X,Y)$ be the Rédei polynomial of the point set $\mathcal{U}$, and let $y \in \mathrm{GF}(q)$. Then $X = x$ is a root of $H(X,y)$ with multiplicity r if and only if the line with equation $Y = yX + x$ meets $\mathcal{U}$ in exactly r points.*

We need another result on polynomials which will be crucial in the proof. For $r \in \mathbb{R}$, let $r^+ = \max\{0, r\}$.

Theorem 3.2 (Szőnyi–Weiner Lemma, [37, Corollary 2.4], [23, Appendix, Result 6])**.** *Let f and g be two-variable polynomials in $\mathrm{GF}(q)[X,Y]$. Let $d = \deg f$ and suppose that the coefficient of X^d in f is non-zero. For $y \in \mathrm{GF}(q)$, let $h_y = \deg \gcd(f(X,y), g(X,y))$, where $\gcd$ denotes the greatest common divisor of the two polynomials in $\mathrm{GF}(q)[X]$. Then for any $y_0 \in \mathrm{GF}(q)$,*

$$\sum_{y \in \mathrm{GF}(q)} (h_y - h_{y_0})^+ \leq (\deg f(X,Y) - h_{y_0})(\deg g(X,Y) - h_{y_0}).$$

A *partial cover* of $\mathrm{PG}(2,q)$ with $h > 0$ holes is a set of lines in $\mathrm{PG}(2,q)$ such that the union of these lines covers all but h points. We will also use the dual of the following result due to Blokhuis, Brouwer and Szőnyi [8].

Theorem 3.3 ([8, Proposition 1.5])**.** *A partial cover of $\mathrm{PG}(2,q)$ with $h > 0$ holes, not all on one line if $h > 2$, has size at least $2q - 1 - h/2$.*

Note that the following, main lemma is not restricted to t-semiarcs. The *carrier* of a pencil is the common point of the lines belonging to the pencil.

Lemma 3.4. *Let $\mathcal{S}$ be a set of s points in $\mathrm{PG}(2,q)$, let ℓ be a k-secant of $\mathcal{S}$ with $2 \leq k \leq q$, and let $1 \leq t \leq q-3$ be an integer. Suppose that through each point of $\mathcal{S} \cap \ell$ there pass exactly t tangent lines to $\mathcal{S}$, and let $s = k + q - t + \varepsilon$ for some $\varepsilon \geq 0$. Let $A(n)$ be the set of those points in $\ell \setminus \mathcal{S}$ through which there pass at most n skew lines to $\mathcal{S}$. Then the following hold.*

- *If $t = 1$, then*

    1. *$\varepsilon < \frac{k}{2} - 1$ implies that the k tangent lines at the points of $\mathcal{S} \cap \ell$ and the skew lines through the points of $A(2)$ belong to a pencil (hence $A(2) \setminus A(1)$ is empty),*

ACADEMIA PRESS
UNIVERSITEIT GENT

2. $\varepsilon < \frac{2k}{3} - 2$ *implies that the k tangent lines at the points of $\mathcal{S} \cap \ell$ either belong to two pencils or they form a dual arc $\mathcal{K}$. If $k < q$, then the skew lines through the points of $A(2)$ belong to the same pencils or extend $\mathcal{K}$ to a larger dual arc.*

- *If $t \geq 2$ and $k > q - \frac{q}{t} + 1$, then*

3. $\varepsilon < \frac{k}{t+1} - \frac{t}{2}$ *implies that the kt tangent lines at the points of $\mathcal{S} \cap \ell$ and the skew lines through the points of $A(t+1)$ belong to t pencils whose carriers are not on ℓ (hence $A(t+1) \setminus A(t)$ is empty),*

4. $\varepsilon < \frac{k}{t+1} - 1$ *and $t \leq \sqrt{q}$ imply that the kt tangent lines at the points of $\mathcal{S} \cap \ell$ belong to $t+1$ pencils whose carriers are not on ℓ. If $k < q$, then the skew lines through the points of $A(t+1)$ belong to the same pencils.*

Proof. Consider the line set

$$\mathcal{L} = \{r \in \mathrm{PG}(2,q) \colon r \cap \ell \in ((\mathcal{S} \cap \ell) \cup A(t+1)), r \cap (\mathcal{S} \setminus \ell) = \emptyset\},$$

i.e. the set of tangent lines to $\mathcal{S}$ at the points of $\mathcal{S} \cap \ell$ together with the set of skew lines to $\mathcal{S}$ through the points of $A(t+1)$. For each point $P \in \mathrm{PG}(2,q) \setminus \ell$ we define the *index of* P, in notation $\mathrm{ind}(P)$, as the number of lines of $\mathcal{L}$ that pass through P. Finally, let $\delta = |\{r \in \mathcal{L} \colon r \cap \ell \in A(t+1)\}|$ and let $a = |A(t+1)|$. For technical reasons, we also need a variant of these definitions. For any $Q \in \ell$, let $\mathcal{L}_Q = \{r \in \mathcal{L} \colon Q \notin r\}$, $k_Q = |(\ell \cap \mathcal{S}) \setminus \{Q\}|$, $\delta_Q = |\{r \in \mathcal{L} \colon r \cap \ell \in A(t+1) \setminus \{Q\}\}|$ and $a_Q = |A(t+1) \setminus \{Q\}|$. The Q-*index of* P, $\mathrm{ind}_Q(P)$, is the number of lines of $\mathcal{L}_Q$ that pass through P. If $P = (m)$, we write e.g. $\mathrm{ind}(m)$ instead of $\mathrm{ind}((m))$. Note that if $Q \in \ell \setminus (\mathcal{S} \cup A(t+1))$, then $\mathrm{ind}_Q(P) = \mathrm{ind}(P)$ for all $P \in \mathrm{PG}(2,q) \setminus \ell$.

First we are about to estimate the possible values of the Q-index of a point $P \in \mathrm{PG}(2,q) \setminus (\mathcal{S} \cup \ell)$ for an arbitrarily chosen $Q \in \ell$. Choose the system of reference so that $P \in \ell_\infty \setminus \{Y_\infty\}$, $Q = Y_\infty$ and ℓ is the line $[1:0:0]$. Then $P = (y_0)$ for some $y_0 \in \mathrm{GF}(q)$. Let $\{(0, c_1), \ldots, (0, c_{k_Q + a_Q})\}$ be the set of points of $((\mathcal{S} \cap \ell) \cup A(t+1)) \setminus \{Q\}$, let $D = (\ell_\infty \setminus \{Y_\infty\}) \cap \mathcal{S}$, $|D| = d$ and let $\mathcal{U} = \mathcal{S} \setminus (\ell \cup \ell_\infty) = \{(a_1, b_1), \ldots, (a_{s-d-k}, b_{s-d-k})\}$. Consider the Rédei polynomials of $((\mathcal{S} \cap \ell) \cup A(t+1)) \setminus \{Q\}$ and $\mathcal{U}$. Let us denote them by $f(X,Y) = \prod_{j=1}^{k_Q + a_Q}(X - c_j)$ and $g(X,Y) = \prod_{j=1}^{s-d-k}(X + a_j Y - b_j)$, respectively. Let $\overline{D} = \ell_\infty \setminus (D \cup \{Y_\infty\})$. Then for any point $(y) \in \overline{D}$,

$$h_y := \deg \gcd\left(f(X,y), g(X,y)\right) = k_Q + a_Q - \mathrm{ind}_Q\,(y).$$

Applying the Szőnyi–Weiner Lemma for the polynomials $f(X,Y)$ and $g(X,Y)$

ACADEMIA PRESS

UNIVERSITEIT GENT

we get

$$\sum_{(y)\in\overline{D}} (\mathrm{ind}_Q(y_0) - \mathrm{ind}_Q(y)) \le \sum_{(y)\in \mathrm{GF}(q)} (\mathrm{ind}_Q(y_0) - \mathrm{ind}_Q(y))^+$$
$$\le \mathrm{ind}_Q(y_0)(s - d - k - k_Q - a_Q + \mathrm{ind}_Q(y_0)).$$

After rearranging it we obtain

$$0 \le \mathrm{ind}_Q(y_0)^2 - \mathrm{ind}_Q(y_0)(q + k + k_Q + a_Q - s) + \sum_{(y)\in\overline{D}} \mathrm{ind}_Q(y). \tag{1}$$

As $\sum_{(y)\in\overline{D}} \mathrm{ind}_Q(y) = k_Q t + \delta_Q$ and $s = k + q - t + \varepsilon$, we have

$$0 \le \mathrm{ind}_Q(y_0)^2 - \mathrm{ind}_Q(y_0)(k_Q + a_Q + t - \varepsilon) + k_Q t + \delta_Q. \tag{2}$$

First we simultaneously prove parts 1, 3 and 4. Here we always choose Q so that $Q \in \ell \setminus \mathcal{S}$, whence $k_Q = k$ follows. Thus the condition $\varepsilon < \frac{k}{t+1} - 1$ and the obvious fact $\delta_Q \le (t+1)a_Q$ imply that (2) gives a contradiction for $t + 1 \le \mathrm{ind}_Q(y_0) \le k + a_Q - \varepsilon - 1$. We say that a point P has *large Q-index* if $\mathrm{ind}_Q(P) \ge k + a_Q - \varepsilon$ holds. Let $\mathcal{P}_Q$ denote the set of points with large Q-index.

Now we are going to prove that each line ℓ' of $\mathcal{L}_Q$ contains a point of $\mathcal{P}_Q$. First suppose that $\ell' \in \mathcal{L}_Q$ is a tangent to $\mathcal{S}$ at a point $T \in \ell \cap \mathcal{S}$. Suppose to the contrary that each point of ℓ' has Q-index at most t. Then

$$\sum_{P\in\ell'\setminus T} \mathrm{ind}_Q(P) \le tq. \tag{3}$$

On the other hand, as every tangent to $\mathcal{S}$ through the points of $(\mathcal{S} \cap \ell) \setminus T$ intersects ℓ', the sum on the left-hand side is at least $(k-1)t + q$, contradicting our assumption on k. Similarly, if ℓ' is a skew line to $\mathcal{S}$ passing through a point $T \in A(t+1) \setminus \{Q\}$, then the right-hand side of (3) remains the same and the left-hand side is at least $kt + q$, which is a contradiction, too. Hence $\mathcal{L}_Q$ is contained in the union of pencils with carriers in $\mathcal{P}_Q$.

Clearly, $|\mathcal{P}_Q| \ge t$. On the other hand, suppose that there are more than t points with large Q-index and let $R_1, R_2, \ldots, R_{t+1}$ be $t+1$ of them. Then

$$(t+1)(k + a_Q - \varepsilon) \le \sum_{j=1}^{t+1} \mathrm{ind}_Q(R_j) \le tk + (t+1)a_Q + \binom{t+1}{2}.$$

This is a contradiction if $\varepsilon < \frac{k}{t+1} - \frac{t}{2}$, which holds in parts 1 and 3. Regarding part 4, if there were more than $t+1$ points with large Q-index, then an analogous argument and $\varepsilon < \frac{2k}{t+2} - \frac{t+1}{2}$ would yield a contradiction. As $\varepsilon < \frac{k}{t+1} - 1$, the bound on ε follows from the condition on k and $t \le \sqrt{q}$.

If $k + |A(t+1)| < q+1$, then let Q be any point of $\ell \setminus (\mathcal{S} \cup A(t+1))$. Thus the lines of $\mathcal{L}_Q = \mathcal{L}$ are contained in t pencils (or $t+1$ in part 4) whose carriers have large Q-index. In this case parts 1, 3 and 4 are proved.

Assume now $k + |A(t+1)| = q+1$. If $k = q$, then let Q be the unique point contained in $A(t+1)$. In case of part 4, the pencils with carriers with large Q-index contain the lines of $\mathcal{L}_Q$, which was to be shown. In case of parts 1 and 3 we obtain a contradiction in the following way. The kt tangents at the points of $\ell \cap \mathcal{S}$ are contained in t pencils having carriers with large Q-index. If $t = 1$, then through the point $R \in \mathcal{P}_Q$ there pass q tangent lines, hence the points of $\mathcal{S} \setminus \ell$ are contained in the line RQ. Thus through Q there pass only two non-skew lines, ℓ and RQ. The condition $q - 3 \geq t = 1$ implies $(q+1) - 2 > 2$, hence $Q \notin A(2)$, a contradiction. If $t > 1$, then it is easy to see that $\mathcal{P}_Q \cup (\mathcal{S} \setminus \ell)$ is contained in a line through Q. Again $q - 3 \geq t$ implies that through Q there pass more than $t+1$ skew lines, hence $Q \notin A(t+1)$, a contradiction.

If $k < q$, then let Q_1 and Q_2 be two distinct points of $A(t+1)$. As seen before, the lines of $\mathcal{L}_{Q_i}$ are blocked by the points of $\mathcal{P}_{Q_i}$ for $i = 1, 2$, hence, by $\mathcal{L}_{Q_1} \cup \mathcal{L}_{Q_2} = \mathcal{L}$, it is enough to show that $\mathcal{P}_{Q_1} = \mathcal{P}_{Q_2}$. If a point is in $\mathcal{P}_{Q_i}$, then its Q_i-index is at least $k + a_{Q_i} - \varepsilon = q - \varepsilon$, while the other points have Q_i-index at most t for $i = 1, 2$. The inequality $|\mathrm{ind}_{Q_1}(P) - \mathrm{ind}_{Q_2}(P)| \leq 1$ obviously holds, thus it is enough to show that $q - \varepsilon - t > 1$, which follows from the assumptions $\varepsilon < \frac{k}{t+1} - 1$ and $t \leq q - 3$.

Finally, we prove part 2. We distinguish three cases.

(a) If $k + |A(2)| < q+1$, then let Q be any point of $\ell \setminus (\mathcal{S} \cup A(2))$. Here $\mathcal{L}_Q = \mathcal{L}$.

(b) If $k + |A(2)| = q+1$ and $k \leq q-1$, then the choice of Q will depend on the point $P \in \mathrm{PG}(2, q) \setminus (\ell \cup \mathcal{S})$ whose index is to be estimated. In this case let Q be any point of ℓ such that PQ intersects $\mathcal{S} \setminus \ell$ (as $\mathcal{S} \setminus \ell$ is not empty, Q can be chosen in this way). Note that $PQ \notin \mathcal{L}$, thus in this case $\mathrm{ind}_Q(P) = \mathrm{ind}(P)$.

(c) If $k + |A(2)| = q+1$ and $k = q$, then let Q be the unique point contained in $A(2)$.

In cases (a) and (b) we are to prove that $\mathcal{L}$ is either a dual arc or is contained in the union of two pencils; in case (c) we have to prove the same regarding the line set $\mathcal{L}_Q$. In all cases

$$\frac{2k}{3} - 2 \leq \frac{2k_Q}{3} - 2 + \frac{a_Q}{3} \tag{4}$$

follows from $k_Q = k$, except in case (b), where (4) follows from $k_Q \geq k - 1$ and

$a_Q \geq 2$. Thus our assumption $\varepsilon < 2k/3 - 2$ yields

$$\varepsilon < \frac{2k_Q}{3} - 2 + \frac{a_Q}{3}, \tag{5}$$

and so (2) gives a contradiction for $3 \leq \mathrm{ind}_Q(P) \leq k_Q + a_Q - 2 - \varepsilon$.

In cases (a) and (c) it follows that the lines of $\mathcal{L}_Q$ either form a dual arc and we are finished, or there is a point R with Q-index at least $k_Q + a_Q - 1 - \varepsilon$. In case (b) either $\mathcal{L}$ is a dual arc and we are finished, or there is a point R with index at least $q - 1 - \varepsilon$ (since in this case $k_Q + a_Q = q$). So it remains to handle the case when such a point R exists. Let $\mathcal{B} = (\ell \setminus (\mathcal{S} \cup A(2))) \cup (\mathcal{S} \setminus \ell) \cup R$ and denote by h the number of lines of $\mathrm{PG}(2,q)$ not blocked by $\mathcal{B}$. It is easy to see that, apart from ℓ, $\mathcal{B}$ blocks all but at most $(k + 2|A(2)|) - (k_Q + a_Q - 1 - \varepsilon)$ lines of $\mathrm{PG}(2,q)$. In case (a) $\mathcal{B}$ blocks ℓ and $k + |A(2)| = k_Q + a_Q$, hence

$$h \leq |A(2)| + 1 + \varepsilon. \tag{6}$$

In cases (b) and (c) $\mathcal{B}$ does not block ℓ and $k + |A(2)| = (k_Q + a_Q) + 1$, thus

$$h \leq |A(2)| + 3 + \varepsilon. \tag{7}$$

Suppose to the contrary that these h lines do not pass through one point. Then by the dual of Theorem 3.3 we have

$$|\mathcal{B}| = q + 1 - (k + |A(2)|) + (q - 1 + \varepsilon) + 1 \geq 2q - 1 - h/2.$$

Rearranging it we obtain $\varepsilon \geq k + |A(2)| - 2 - h/2$. In case (a), together with (6), this would imply $\varepsilon \geq 2k/3 - 5/3 + |A(2)|/3$. In cases (b) and (c), together with (7), $\varepsilon \geq (q+k)/3 - 2$ would follow. Both cases yield a contradiction because of our assumption on ε. Hence the corresponding lines can be blocked by R and one more point, thus they belong to two pencils. □

Although the forthcoming applications in this paper all use Lemma 3.4, we shall give another, more general but less detailed result whose proof is based on the very same ideas.

Theorem 3.5. *Suppose that $\mathcal{S} \subset \mathrm{PG}(2,q)$ is a point set, ℓ is a line, and let $s = |\mathcal{S} \setminus \ell|$. Let $\mathcal{K} \subset \ell \setminus \mathcal{S}$ be a set of $k \leq q$ points. Denote by $\mathcal{L}$ the set of skew lines to $\mathcal{S}$ through the points of $\mathcal{K}$, not including ℓ, and let $\delta = |\mathcal{L}|$. Let m be an integer such that any point of $\mathcal{K}$ is incident with at most m lines of $\mathcal{L}$. Suppose that there exists an integer t such that $(t-1)q + m < \delta < (t+1)(k + q - s - t - 1)$. If $\delta < (n+1)(k + q - s - t - n/2)$ for some integer n, then the lines of $\mathcal{L}$ belong to n pencils whose carriers are not on ℓ.*

Proof. Let the index of a point P, $\mathrm{ind}(P)$, be the number of lines of $\mathcal{L}$ incident with P. Similarly as in the proof of Lemma 3.4, let $P \in \mathrm{PG}(2,q) \setminus (\mathcal{S} \cup \ell)$; we may assume that ℓ is the line $[1:0:0]$, $P = (y_0) \in \ell_\infty \setminus \{Y_\infty\}$ and $Y_\infty \notin \mathcal{K}$. Let $D = (\ell_\infty \setminus \{Y_\infty\}) \cap \mathcal{S}$, $|D| = d$ and let $\mathcal{U} = \mathcal{S} \setminus (\ell \cup \ell_\infty)$. Again, let $g(X,Y)$ and $f(X,Y)$ be the Rédei polynomials of $\mathcal{K}$ and $\mathcal{U}$; their degrees are k and $s-d$, respectively. Let $\overline{D} = \ell_\infty \setminus (D \cup \{Y_\infty\})$. Then for any point $(y) \in \overline{D}$,

$$h_y := \deg \gcd\left(f(X,y), g(X,y)\right) = k - \mathrm{ind}(y).$$

Applying the Szőnyi–Weiner Lemma we get

$$(q-d)\mathrm{ind}(y_0) - \delta = \sum_{(y)\in\overline{D}} (\mathrm{ind}(y_0) - \mathrm{ind}(y)) \le \mathrm{ind}(y_0)(s-d-k+\mathrm{ind}(y_0)).$$

After rearranging it we obtain

$$0 \le \mathrm{ind}(P)^2 - \mathrm{ind}(P)(q+k-s) + \delta. \tag{8}$$

Assuming $\mathrm{ind}(P) = t+1$, (8) contradicts $\delta < (t+1)(k+q-s-t-1)$, hence either $\mathrm{ind}(P) \le t$ or $\mathrm{ind}(P) \ge q+k-s-t$. Suppose that there is a line of $\mathcal{L}$ containing no point with large index. Then $\delta \le m + q(t-1)$ follows, a contradiction. Hence the lines of $\mathcal{L}$ are blocked by the points with large index. If there were at least $n+1$ such points, then $\delta \ge (n+1)(q+k-s-t) - \binom{n+1}{2}$ would follow, contradicting $\delta < (n+1)(k+q-s-t-n/2)$. □

In [36, Section 3], among other techniques, Szőnyi and Weiner also use their lemma (Lemma 3.2) in basically the same way to derive a result roughly saying that if a small point set has only a few skew lines to it, then it can be extended to a blocking set by adding a few points to it. Now, with the notation of Theorem 3.5, extending the set $(\mathcal{S} \cup \ell) \setminus \mathcal{K}$ to a blocking set by adding n points to it is equivalent to finding n pencils that contain the lines of $\mathcal{L}$. However, the points found using the result of [36] might also be on ℓ. Now let us give some immediate consequences of Lemma 3.4.

Corollary 3.6. *Let $\mathcal{S}_1$ be a semioval in $\mathrm{PG}(2,q)$ and let ℓ be a k-secant of $\mathcal{S}_1$. If $|\mathcal{S}_1| < q + \frac{3k}{2} - 2$, then the k tangent lines at the points of $\mathcal{S}_1 \cap \ell$ belong to a pencil. If $|\mathcal{S}_1| < q + \frac{5k}{3} - 3$, then the k tangent lines at the points of $\mathcal{S}_1 \cap \ell$ either belong to two pencils or they form a dual k-arc.*

If $k = q-1$, then we get a stronger result than the previous characterization of Kiss [26, Corollary 3.1].

Corollary 3.7. *Let $\mathcal{S}_1$ be a semioval in $\mathrm{PG}(2,q)$. If $\mathcal{S}_1$ has a $(q-1)$-secant ℓ and $|\mathcal{S}_1| < \frac{5q}{2} - \frac{7}{2}$ holds, then $\mathcal{S}_1$ is contained in a vertexless triangle and it has two $(q-1)$-secants.*

Proof. Let $\ell \setminus \mathcal{S}_1 = \{A, B\}$. It follows from Corollary 3.6 that the tangents at the points of $\mathcal{S}_1 \cap AB$ are contained in a pencil with carrier C. Thus $\mathcal{S}_1$ is contained in the sides of the triangle ABC. Suppose to the contrary that AC and BC both intersect $\mathcal{S}_1$ in less than $q-1$ points. Then there exist P, Q such that $P \in AC \setminus (\mathcal{S}_1 \cup \{A, C\})$ and $Q \in BC \setminus (\mathcal{S}_1 \cup \{B, C\})$. The point $E := PQ \cap AB$ is in $\mathcal{S}_1$ and PQ is a tangent to $\mathcal{S}_1$ at E. This is a contradiction since $C \notin PQ$. □

Note that for a t-semiarc , as $t < q$ implies $\kappa() \leq q+1-t$, the assumption $q - \frac{q}{t} + 1 < k$ in Lemma 3.4 can hold only if $t < \sqrt{q}$.

Corollary 3.8. *Let be a t-semiarc in* $\mathrm{PG}(2,q)$*,* $q \geq 7$*, with* $1 < t < \sqrt{q}$*. Suppose that has a k-secant ℓ and $k > q - \frac{q}{t} + 1$. If $|| < (q-t+k) + \frac{k}{t+1} - 1$, then the kt tangent lines at the points of $\cap \ell$ belong to $t+1$ pencils. If $|| < (q-t+k) + \frac{k}{t+1} - \frac{t}{2}$, then the kt tangent lines at the points of $\cap \ell$ belong to t pencils.*

Remark 3.9. Theorem 2.13 follows from Lemma 3.4 with $t = 1$ and $\varepsilon = 0$. To see this, let $\mathcal{S} = \mathcal{U} \cup (\ell_\infty \setminus D_{\mathcal{U}})$. Then through each point of $\ell_\infty \cap \mathcal{S}$, there passes a unique tangent to $\mathcal{S}$. According to Lemma 3.4, these tangent lines are contained in a pencil, whose carrier can be added to $\mathcal{U}$.

Example 3.10. It follows from Theorem 3.3 that a cover of the complement of a conic in $\mathrm{PG}(2,q)$, q odd, by external lines, contains at least $3(q-1)/2$ lines, see [8, Proposition 1.6]. Blokhuis et al. also remark that this bound can be reached for $q = 3, 5, 7, 11$ and there is no other example of this size for $q < 25$, q odd. Now, let ℓ be a tangent to a conic $\mathcal{C}$ at the point $P \in \mathcal{C}$ and let $\mathcal{U}$ be a set of $3(q-1)/2$ interior points of the conic such that these points block each non-tangent line. From the dual of Blokhuis et al.'s result we know that such set of interior points exists in case of $q = 3, 5, 7, 11$. Let $\mathcal{S} = (\mathcal{U} \cup \ell) \setminus \{P\}$. Then the tangents to $\mathcal{S}$ at the points of $\ell \cap \mathcal{S}$ obviously do not pass through one point and this shows that part 1 of Lemma 3.4 is sharp if $k = q$ and $q = 5, 7, 11$.

Example 3.11 ([28, Theorem 3.2])**.** In $\mathrm{PG}(2,8)$, there exists a semioval $\mathcal{S}_1$ of size 15 contained in a triangle without two of its vertices. The side opposite to the one vertex contained in $\mathcal{S}_1$ is a 6-secant and the other two sides are 5-secants. The tangents at the points of the 6-secant do not pass through one point. Hence Corollary 3.6 is sharp at least for $q = 8$.

In the following we give some examples for small t-semiarcs with long secants in the cases $t = 1, 2, 3$ such that the tangents at the points of a long secant do not belong to t pencils. These assertions can be easily proved using Menelaus' Theorem. Denote by $\mathrm{GF}(q)^+$ and $\mathrm{GF}(q)^\times$ the additive and multiplicative groups of the field $\mathrm{GF}(q)$, $q = p^h$, p prime, respectively, and by $A \oplus B$ the direct sum of the groups A and B.

Example 3.12 ([28, p. 104]). Consider $\mathrm{GF}(q)$, q square, as the quadratic extension of $\mathrm{GF}(\sqrt{q})$ by i. Then the point set

$$\begin{aligned}\mathcal{S}_1 = ([1:0:0] \cup [1:0:1] \cup [0:0:1]) \\ \setminus \{Y_\infty, (0:s:1), (1:si:1), (1:s+si:0)\colon s \in \mathrm{GF}(\sqrt{q})\}\end{aligned} \tag{9}$$

is a semioval in $\mathrm{PG}(2,q)$ with three $(q-\sqrt{q})$-secants if $q>4$.

Example 3.13 ([16, p. 689]). Let $\mathrm{GF}(q)^+ = A \oplus B$, where A and B are proper subgroups of $\mathrm{GF}(q)^+$ and let $X = A \cup B$. The point set

$$\mathcal{S}_2 = \{(0:s:1), (1:s:1), (1:s:0)\colon s \in \mathrm{GF}(q) \setminus X\}$$

is a 2-semiarc in $\mathrm{PG}(2,q)$ with three $(q+1-|A|-|B|)$-secants if $q>4$. Note that $2\sqrt{q} \le |A|+|B| \le q/p+p$.

Example 3.14. Similarly, let $\mathrm{GF}(q)^\times = A \oplus B$ and $X = A \cup B$, where A and B are proper subgroups of $\mathrm{GF}(q)^\times$. The point set

$$\mathcal{S}_3 = \{(0:s:1), (s:0:1), (1:-s:0)\colon s \in \mathrm{GF}(q) \setminus (X \cup \{0\})\}$$

is a 3-semiarc in $\mathrm{PG}(2,q)$ with three $(q-|A|-|B|)$-secants if $q>7$. Note that $2\sqrt{q} \le |A|+|B| \le (q+3)/2$.

4. Semiarcs and blocking sets

In this section we associate blocking sets to semiarcs. Using strong characterization results on blocking sets, we characterize small semiarcs with long secants. Note that the next lemma is not restricted to t-semiarcs.

Lemma 4.1. *Let $\mathcal{S}$ be a set of points in Π_q, let ℓ be a k-secant of $\mathcal{S}$ with $2 \le k \le q$, and let $1 \le t \le q-3$ and $n \ge t$ be integers. Suppose that through each point of $\mathcal{S} \cap \ell$ there pass exactly t tangent lines to $\mathcal{S}$, and let $|\mathcal{S}| = k+q-t+\varepsilon$ for some $\varepsilon \ge 0$. Let $A(n)$ be the set of those points in $\ell \setminus \mathcal{S}$ through which there pass at most n skew lines to $\mathcal{S}$. Assume that the kt tangent lines to $\mathcal{S}$ at the points of $\mathcal{S} \cap \ell$ and the skew lines through the points of $A(n)$ belong to n pencils. Let $\mathcal{P}$ be the set of carriers of these pencils and assume that $\mathcal{P} \cap \ell = \emptyset$. Define the point set $\mathcal{B}_n(\mathcal{S},\ell)$ in the following way:*

$$\mathcal{B}_n(\mathcal{S},\ell) := (\ell \setminus (A(n) \cup \mathcal{S})) \cup (\mathcal{S} \setminus \ell) \cup \mathcal{P}.$$

Then $\mathcal{B}_n(\mathcal{S},\ell)$ has size $2q+1+\varepsilon+n-t-k-|A(n)|$. If $\ell \cap \mathcal{B}_n(\mathcal{S},\ell) = \emptyset$ (i.e. $\ell \subseteq A(n) \cup \mathcal{S}$), then $\mathcal{B}_n(\mathcal{S},\ell)$ is an affine blocking set in the affine plane $\Pi_q \setminus \ell$; otherwise $\mathcal{B}_n(\mathcal{S},\ell)$ is a blocking set in Π_q. In the latter case the points of $\ell \cap \mathcal{B}_n(\mathcal{S},\ell)$ are essential points.

ACADEMIA PRESS
UNIVERSITEIT GENT

Proof. Let $\ell' \neq \ell$ be any line in Π_q and let E be the point $\ell \cap \ell'$. If ℓ' meets $(\ell \setminus (A(n) \cup \mathcal{S})) \cup (\mathcal{S} \setminus \ell)$, then ℓ' is blocked by $\mathcal{B}_n(\mathcal{S}, \ell)$. Otherwise ℓ' is a tangent to $\mathcal{S}$ at a point of $\ell \cap \mathcal{S}$ or ℓ' is a skew line to $\mathcal{S}$ that intersects $A(n)$. In both cases ℓ' is blocked by $\mathcal{P}$, hence it is also blocked by $\mathcal{B}_n(\mathcal{S}, \ell)$.

If $\ell \subseteq A(n) \cup \mathcal{S}$, then $\mathcal{B}_n(\mathcal{S}, \ell)$ is an affine blocking set in the affine plane $\Pi_q \setminus \ell$. Otherwise ℓ is blocked by $\ell \setminus (A(n) \cup \mathcal{S})$ and hence $\mathcal{B}_n(\mathcal{S}, \ell)$ is a blocking set in Π_q. In the latter case through each point of $\ell \cap \mathcal{B}_n(\mathcal{S}, \ell)$ there pass at least $n+1$ skew lines to $\mathcal{S}$ and hence through each of them there is at least one tangent to $\mathcal{B}_n(\mathcal{S}, \ell)$. □

In $\mathrm{PG}(2, q)$ we will combine Lemma 4.1 with Lemma 3.4 in the cases $n = t$ or $n = t+1$ to obtain small blocking sets from small semiarcs having a long secant. The point set $\mathcal{B}_n(\mathcal{S}, \ell)$ is an affine blocking set if and only if $k + |A(n)| = q + 1$, and in this case $|\mathcal{B}_n(\mathcal{S}, \ell)| = q + \varepsilon + n - t$. An affine blocking set in $\mathrm{AG}(2, q)$ has at least $2q - 1$ points (see [12] or [25]; also follows from Theorem 3.3). Hence if we consider $\mathrm{PG}(2, q)$, then $\varepsilon < q - n + t - 1$ implies that $\mathcal{B}_n(\mathcal{S}, \ell)$ is not an affine blocking set. This condition will always hold for $n = t$ or $n = t + 1$.

Example 4.2. If $\mathcal{S}_1$ is Blokhuis' semioval and ℓ is one of the $(q-1)/2$-secants of $\mathcal{S}_1$, then $\mathcal{S}_1$ and ℓ satisfy the conditions of Lemma 4.1 with $n = 1$ and the obtained blocking set $\mathcal{B}_1(\mathcal{S}_1, \ell)$ is a minimal blocking set called the projective triangle (see e.g. [24, Lemma 13.6]).

Lemma 4.3. *Let be a t-semiarc in $\mathrm{PG}(2, q)$, $q = p^h$, p prime, with $t \leq \sqrt{2q/3}$. Let ℓ be a k-secant of and suppose that and ℓ satisfy the conditions of Lemma 4.1 with $n = t$. With the notation of Lemma 4.1, if $p = 2$ and $\varepsilon < k - \frac{4}{5}(q-1)$, or p is odd and $\varepsilon < k - \frac{1}{2}(q-1)$, then $|A(t)| \geq t$.*

Proof. In both cases we have $|\mathcal{B}_t(, \ell)| = 2q+1+\varepsilon-k-|A(t)| < 3(q+1)/2$, hence $\mathcal{B}_t(, \ell)$ is a small blocking set. Let $\mathcal{B}$ be the unique (cf. Theorem 1.1) minimal blocking set contained in it and let e be the exponent of $\mathcal{B}$ (cf. Theorem 1.2). Note that if $\varepsilon < k - \frac{4}{5}(q-1)$, then $p^e \geq 8$ follows from Theorem 1.2. Also $p^e \geq 3$ holds when p is odd.

The points of $\ell \cap \mathcal{B}_t(, \ell)$ are essential points of $\mathcal{B}_t(, \ell)$ hence $\ell \cap \mathcal{B}_t(, \ell) = \ell \cap \mathcal{B}$. The size of $\mathcal{B} \cap (\setminus \ell)$ is at least $q - t$; let $\mathcal{U}$ be $q - t$ points from this point set. Consider ℓ as the line at infinity. We wish to apply Lemma 2.15 with $E = A(t)$, $F = \ell \setminus$, $z = p^e$ and with $\mathcal{P}$ defined as in Lemma 4.1. Note that the points of $\mathcal{P}$ are essential (thus $\mathcal{P} \subset \mathcal{B}$) and $t \leq \sqrt{2q/3} \leq \sqrt{q(z-1)/z}$. Through each point of $\mathcal{U}$ there pass t tangents to . These lines are also tangents to $\mathcal{U}$ and they have direction in F. Let ℓ' be one of these tangents; then $\ell' \cap (\mathcal{B} \setminus \ell) = \ell' \cap (\mathcal{P} \cup \mathcal{U})$. Thus, by $|\ell' \cap \mathcal{B}| \equiv 1 \pmod{z}$, we have that if ℓ' has direction in $F \setminus E$, then

$|\ell' \cap (\mathcal{P} \cup \mathcal{U})| \equiv 0 \pmod{z}$. Hence the two required properties of Lemma 2.15 hold, thus $|A(t)| \geq t$. □

To proceed, we need some results on semiarcs with two long secants proved by Csajbók.

Lemma 4.4 ([15, Theorem 13]). *Let be a t-semiarc in the projective plane Π_q, $1 < t < q$. Suppose that there exist two lines ℓ_1 and ℓ_2 such that $|\ell_1 \setminus (\cup \ell_2)| = n$ and $|\ell_2 \setminus (\cup \ell_1)| = m$. If $\ell_1 \cap \ell_2 \notin$, then $n = m = t$ or $q \leq \min\{n, m\} + 2nm/(t-1)$.*

We cite only three particular cases of the complete characterization of t-semiarcs in $\mathrm{PG}(2, q)$ with two $(q-t)$-secants whose common point is not in the semiarc. Such semiarcs are called *semiarcs of V_t° type*. Note that the tight semiarcs of V_t° type are precisely the V_t-configurations.

Theorem 4.5 ([15, Theorem 22]). *Let be a t-semiarc of V_t° type in $\mathrm{PG}(2, q)$, $q = p^h$, p prime, and let $t \leq q - 2$. Then the following hold.*

1. *If $\gcd(q, t) = 1$, then is contained in a vertexless triangle.*
2. *If $\gcd(q, t) = 1$ and $\gcd(q-1, t-1) = 1$, then is a V_t-configuration.*
3. *If $\gcd(q-1, t) = 1$, then is contained either in a vertexless triangle, or in the union of three concurrent lines with their common point removed.*

Now we are ready to prove our main characterization theorems for small semiarcs with a long secant. We distinguish two cases as the results on blocking sets in $\mathrm{PG}(2, q)$ are stronger if q is a prime.

Theorem 4.6. *Let be a t-semiarc in $\mathrm{PG}(2, p)$, p prime.*

1. *If $t = 1$, $p \geq 5$ and $\kappa(\mathcal{S}_1) \geq \frac{p-1}{2}$, then*
   - *$\mathcal{S}_1$ is contained in a vertexless triangle and has two $(p-1)$-secants, or*
   - *$\mathcal{S}_1$ is projectively equivalent to Blokhuis' semioval, or*
   - $|\mathcal{S}_1| \geq \min\left\{\frac{3\kappa(\mathcal{S}_1)}{2} + p - 2,\ 2\kappa(\mathcal{S}_1) + \frac{p+1}{2}\right\}$.
2. *If $t = 2$, $p \geq 7$ and $\kappa(\mathcal{S}_2) \geq \frac{p+3}{2}$, then*
   - *$\mathcal{S}_2$ is a V_2-configuration, or*
   - $|\mathcal{S}_2| \geq \min\left\{\frac{4\kappa(\mathcal{S}_2)}{3} + p - 3,\ 2\kappa(\mathcal{S}_2) + \frac{p-1}{2}\right\}$.

3. *If $3 \le t < \sqrt{p}$, $p \ge 23$ and $\kappa() > p - \frac{p}{t} + 1$, then*

   - *is contained in a vertexless triangle and has two $(p-t)$-secants, or*
   - $|| \ge \kappa()\frac{t+2}{t+1} + p - t - 1$.

Proof. Let $k = \kappa()$ and let ℓ be a k-secant of . Note that as t is small enough, Theorem 2.3 implies that $k \le q - t$. We define $A(n) \subset \ell$ as usual.

PART 1. Assume that $|\mathcal{S}_1| < \min\left\{\frac{3k}{2} + p - 2,\ 2k + \frac{p+1}{2}\right\}$. If $|\mathcal{S}_1| = k+p-1+\varepsilon$, then we have $\varepsilon < \min\left\{\frac{k}{2} - 1,\ k - \frac{p-3}{2}\right\}$, hence Lemma 3.4 implies that the tangents at the points of $\ell \cap \mathcal{S}_1$ and the skew lines through the points of $A(1)$ are contained in a pencil with carrier P. Construct the small blocking set $\mathcal{B}_1(\mathcal{S}_1, \ell)$ as in Lemma 4.1 with $n = 1$. The size of $\mathcal{B}_1(\mathcal{S}_1, \ell)$ is $2p + 1 + \varepsilon - k - |A(1)| < 3(p+1)/2 + 1$, thus Theorem 1.3 implies that $\mathcal{B}_1(\mathcal{S}_1, \ell)$ either contains a line or it is a minimal blocking set of size $3(p+1)/2$ and each of its points has exactly $(p-1)/2$ tangents.

In the first case, let ℓ_1 be the line contained in $\mathcal{B}_1(\mathcal{S}_1, \ell)$. Since no p points of $\mathcal{S}_1$ can be collinear, it follows from the construction of $\mathcal{B}_1(\mathcal{S}_1, \ell)$ that ℓ_1 is a $(p-1)$-secant of $\mathcal{S}_1$. The assertion now follows from Corollary 3.7. In the latter case, as the number of tangents to $\mathcal{B}_1(\mathcal{S}_1, \ell)$ through P is $k + |A(1)|$, we have that $k + |A(1)| = (p-1)/2$. Then $\varepsilon = 0$ follows from $3(p+1)/2 = |\mathcal{B}_1(\mathcal{S}_1, \ell)| = 2p + 1 + \varepsilon - k - |A(1)|$, hence $\mathcal{S}_1$ is a tight semioval and, by Corollary 2.18, it is projectively equivalent to Blokhuis' semioval.

PART 2. Assume that $|\mathcal{S}_2| < \min\left\{\frac{4k}{3} + p - 3,\ 2k + \frac{p-1}{2}\right\}$. If $|\mathcal{S}_2| = k+p-2+\varepsilon$, then we have $\varepsilon < \min\left\{\frac{k}{3} - 1,\ k - \frac{p-3}{2}\right\}$, hence Lemma 3.4 implies that the tangents at the points of $\ell \cap \mathcal{S}_2$ and the skew lines through the points of $A(2)$ are contained in two pencils whose carriers we denote by P_1 and P_2. Construct the blocking set $\mathcal{B}_2(\mathcal{S}_2, \ell)$ as in Lemma 4.1. Theorem 1.3 implies that $\mathcal{B}_2(\mathcal{S}_2, \ell)$ either contains a line ℓ_1 or it is a minimal blocking set of size $3(p+1)/2$ and each of its points has exactly $(p-1)/2$ tangents.

In the first case, since $\mathcal{S}_2$ cannot have more than $p-2$ collinear points, it follows from the construction of $\mathcal{B}_2(\mathcal{S}_2, \ell)$ that ℓ_1 is a $(p-2)$-secant of $\mathcal{S}_2$, and hence so is ℓ. Then Theorem 4.5 implies that $\mathcal{S}_2$ is a V_2-configuration. In the latter case, both P_1 and P_2 have exactly $(p-1)/2$ tangent lines to $\mathcal{B}_2(\mathcal{S}_2, \ell)$. But this is a contradiction since these two points together have at least $2k$ tangents to $\mathcal{B}_2(\mathcal{S}_2, \ell)$, which is greater than $p-1$.

PART 3. Assume that $|| < k\frac{t+2}{t+1} + p - t - 1$. Then $|| = k + p - t + \varepsilon$, where $\varepsilon < \frac{k}{t+1} - 1$, hence Lemma 3.4 implies that the tangents at the points of $\ell \cap$ are contained in $t+1$ pencils. Construct the blocking set $\mathcal{B}_{t+1}(, \ell)$ as in Lemma 4.1. Since $\varepsilon < \frac{k}{t+1} - 1 < k - \frac{p+1}{2}$ holds by $t \ge 3$ and $k > p - p/t + 1$, $\mathcal{B}_{t+1}(, \ell)$ is small.

Then Theorem 1.3 implies that it contains a line ℓ_1. Note that $\ell_1 \cap \ell \notin$. Since cannot have more than $p-t$ collinear points, by the construction of $\mathcal{B}_{t+1}(,\ell)$ we have that ℓ_1 is a $(p-t)$-secant or a $(p-t-1)$-secant of , and hence so is ℓ. Then (using $p \geq 23$ and $t < \sqrt{p}$) Lemma 4.4 implies that both ℓ and ℓ_1 are $(p-t)$-secants. Since $\gcd(t,p) = 1$, Theorem 4.5 implies that is contained in a vertexless triangle. □

For non-prime values of q, our next theorem roughly says that if t is small, then small t-semiarcs with a long secant are of V_t° type. If q is a square, then we can characterize altered Baer subplanes (Example 2.10) as well. Recall that altered Baer subplanes are t-semiarcs of size $(q-\sqrt{q}-t)+(q-t)$ with a $(q-\sqrt{q}-t)$-secant.

Theorem 4.7. *Let be a t-semiarc in $\mathrm{PG}(2,q)$, $q = p^h$, $h \geq 2$ if p is an odd prime and $h \geq 6$ if $p = 2$. Suppose that*

$$\kappa() \geq \begin{cases} q-\sqrt{q}-t & \text{if } h \text{ is even,} \\ q-c_pq^{2/3}-t & \text{if } h \text{ is odd,} \end{cases}$$

where $c_p = 2^{-1/3}$ for $p = 2,3$ and $c_p = 1$ for $p > 3$ (cf. Theorem 1.3). Then the following hold.

1. *If $h = 2d$ and $t < (\sqrt{5}-1)(\sqrt{q}-1)/2$, then*
   - *$|| < 2\kappa() + \sqrt{q}$ implies that is of V_t° type;*
   - *$|| = 2\kappa() + \sqrt{q}$ and $q > 9$ implies that is either of V_t° type or an altered Baer subplane.*
2. *If $h = 2d+1$, $|| < 2\kappa() + c_pq^{2/3}$ and $t < q^{1/3} - 3/2$ (or $t < (2q)^{1/3} - 2$ when $p = 2,3$), then is of V_t° type.*

Proof. Let $k = \kappa()$ and let ℓ be a k-secant of . Note that as t is small enough, Theorem 2.3 implies that $k \leq q-t$. We define $A(n) \subset \ell$ as usual. To apply Lemma 3.4, we need $k > q - \frac{q}{t} + 1$; furthermore, $\varepsilon < k/2 - 1$ for $t = 1$ and $\varepsilon < k/(t+1) - t/2$ for $t \geq 2$. Let us first consider the condition on k. If q is a square, then $k \geq q - \sqrt{q} - t > q - \frac{q}{t} + 1$ holds if $t < \Phi(\sqrt{q}-1)$, where $\Phi = \frac{\sqrt{5}-1}{2} \approx 0.618034$. If q is not a square, then $t < q^{1/3} - 3/2$ (or $t < (2q)^{1/3} - 2$ when $p = 2,3$) and $k \geq q - c_pq^{2/3} - t$ imply $k > q - \frac{q}{t} + 1$.

Next we treat the condition on ε. Let us define $b(q)$ as follows:

$$b(q) := \begin{cases} \sqrt{q} & \text{if } h \text{ is even,} \\ c_pq^{2/3} & \text{if } h \text{ is odd.} \end{cases}$$

As $|| = k+q-t+\varepsilon$, $|| \leq 2k+b(q)$ implies $\varepsilon \leq k-q+b(q)+t$.

Suppose first that $t \geq 2$. As $\varepsilon \leq k-q+b(q)+t$, it is enough to prove $k-q+b(q)+t < \frac{k}{t+1} - \frac{t}{2}$. After rearranging we get that this is equivalent to

$$k < (q-t) + \left(\frac{q-b(q)}{t} - \frac{t}{2} - b(q) - \frac{3}{2}\right),$$

thus it is enough to see (as $k \leq q-t$ holds automatically) that

$$\frac{q-b(q)}{t} - \frac{t}{2} - b(q) - \frac{3}{2} > 0.$$

As a function of t the left hand side decreases monotonically. It is positive when t is maximal (under the respective assumptions), hence the condition of Lemma 3.4 on ε is satisfied for $t \geq 2$.

If $t = 1$, then the upper bounds on t imply $q \geq 9$ for $h = 2d$ and $q \geq 27$ for $h = 2d+1$. From these lower bounds on q and from $k \leq q-1$ it follows that $k/2 \leq (q-1)/2 \leq q-b(q)-2$, whence we obtain $k-q+b(q)+1 \leq \frac{k}{2}-1$. If $|\mathcal{S}_1| < 2k+b(q)$, then $\varepsilon < k-q+b(q)+1 \leq \frac{k}{2}-1$. If $|\mathcal{S}_1| = 2k+b(q)$, then $\varepsilon = k-q+b(q)+1$ and we are in the case $h = 2d$; here the assumption $q > 9$ implies $\varepsilon = k-q+b(q)+1 < \frac{k}{2}-1$. Thus the condition of Lemma 3.4 on ε also holds for $t = 1$.

For $|| < 2k+b(q)$, we prove the h even and h odd cases of the theorem simultaneously. Construct the blocking set $\mathcal{B}_t(,\ell)$ as in Lemma 4.1. The conditions in Lemma 4.3 hold, hence the size of $A(t)$ is at least t. The size of $\mathcal{B}_t(,\ell)$ is $2q+1+\varepsilon-k-|A(t)| < q+b(q)+1$, thus Theorem 1.3 implies that $\mathcal{B}_t(,\ell)$ contains a line ℓ_1. Since cannot have more than $q-t$ collinear points, by the construction of $\mathcal{B}_t(,\ell)$ we get that ℓ_1 is a $(q-t)$-secant of , and hence so is ℓ. Thus is of V_t° type.

Now consider the case $|| = 2k+\sqrt{q}$ (hence $\varepsilon = k-q+\sqrt{q}+t$), and suppose that does not have two $(q-t)$-secants. We can repeat the above arguing and get that $\mathcal{B}_t(,\ell)$ is a Baer subplane because of Theorem 1.3. Then $|\mathcal{B}_t(,\ell)| = q+\sqrt{q}+1 = 2q+1+\varepsilon-k-|A(t)|$ yields $|A(t)| = t$. The size of $\ell \cap \mathcal{B}_t(,\ell)$ is either 1 or $\sqrt{q}+1$. In the latter case $k = q-\sqrt{q}-t$ and is an altered Baer subplane. In the first case $k = q-t$; we show that this cannot occur. Denote by R the common point of ℓ and $\mathcal{B}_t(,\ell)$ and let P be any point of $\mathcal{B}_t(,\ell) \setminus (\ell \cup)$. Among the lines of the Baer subplane $\mathcal{B}_t(,\ell)$ there are $\sqrt{q}+1$ lines incident with P. One of them is PR, which meets in at least $\sqrt{q}-t > 1$ points; each of the other $\sqrt{q}$ lines of the subplane intersects in at least $\sqrt{q}+1-t > 1$ points. Thus these $\sqrt{q}+1$ lines cannot be tangents to . But the pencil of lines through P contains $k = q - t$ tangents to , one at each point of $\ell \cap$, too. Thus the total number of lines through P is at least $\sqrt{q}+1+q-t > q+1$, a contradiction. $\square$

References

[1] **S. Ball**, The number of directions determined by a function over a finite field, *J. Combin. Theory Ser. A* **104** (2003), 341–350.

[2] **D. Bartoli**, On the structure of semiovals of small size, *J. Combin. Des.* **22** (2014), 525–536.

[3] **L. M. Batten**, Determining sets, *Australas. J. Combin.* **22** (2000), 167–176.

[4] **A. Blokhuis**, On the size of a blocking set in $\mathrm{PG}(2,p)$, *Combinatorica* **14** (1994), 111–114.

[5] ______, Characterization of seminuclear sets in a finite projective plane, *J. Geom.* **40** (1991), 15–19.

[6] **A. Blokhuis**, **S. Ball**, **A. E. Brouwer**, **L. Storme** and **T. Szőnyi**, On the number of slopes of the graph of a function defined on a finite field, *J. Combin. Theory Ser. A* **86** (1999), 187–196.

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

[8] ______, Covering all points except one, *J. Algebraic Combin.* **32** (2010), 59–66.

[9] **A. Blokhuis**, **Á. Seress** and **H. A. Wilbrink**, On sets of points in $\mathrm{PG}(2,q)$ without tangents. Proceedings of the First International Conference on Blocking Sets (Giessen, 1989). *Mitt. Math. Sem. Giessen* **201** (1991), 39–44.

[10] **A. Blokhuis**, **L. Storme** and **T. Szőnyi**, Lacunary polynomials, multiple blocking sets and Baer subplanes, *J. London Math. Soc.* **60** (1999), 321–332.

[11] **A. Blokhuis**, **T. Szőnyi** and **Zs. Weiner**, On sets without tangents in Galois planes of even order. Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001). *Des. Codes Cryptogr.* **29** (2003), no. 1–3, 91–98.

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

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

[14] **R. Calderbank** and **W. M. Kantor**, The geometry of two-weight codes, *Bull. London Math. Soc.* **18** (1986), no. 2, 97–122.

[15] **B. Csajbók**, Semiarcs with long secants, *Electron. J. Combin.* **21** (2014), # P1.60, 14 pages.

[16] **B. Csajbók** and **Gy. Kiss**, Notes on semiarcs, *Mediterr. J. Math.* **9** (2012), 677–692.

[17] **M. De Boeck** and **G. Van de Voorde**, A linear set view on KM-arcs, submitted (2014).

[18] **J. M. Dover**, Semiovals with large collinear subsets, *J. Geom.* **69** (2000), 58–67.

[19] **A. Gács**, On a generalization of Rédei's theorem, *Combinatorica* **23** (2003), 585–598.

[20] **A. Gács**, **L. Lovász** and **T. Szőnyi**, Directions in $\mathrm{AG}(2,p^2)$, *Innov. Incidence Geom.* **6/7** (2009), 189–201.

[21] **A. Gács** and **Zs. Weiner**, On $(q+t,t)$-arcs of type $(0,2,t)$, *Des. Codes Cryptogr.* **29** (2003), 131–139.

[22] **M. Giulietti** and **E. Montanucci**, On hyperfocused arcs in PG(2,q), *Discrete Math.* **306** (2006), no. 24, 3307–3314.

[23] **T. Héger**, *Some graph theoretic aspects of finite geometries*, PhD Thesis, Eötvös Loránd University (2013).

[24] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, 2^{nd} ed., Clarendon Press, Oxford, 1998.

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

[26] **Gy. Kiss**, Small semiovals in $\mathrm{PG}(2,q)$, *J. Geom.* **88** (2008), 110–115.

[27] ______, A survey on semiovals, *Contrib. Discrete Math.* **3** (2008), 81–95.

[28] **Gy. Kiss** and **J. Ruff**, Notes on small semiovals, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **47** (2004), 97–105.

[29] **G. Korchmáros** and **F. Mazzocca**, On $(q+t,t)$-arcs of type $(0,2,t)$ in a Desarguesian plane of order q, *Math. Proc. Cambridge Philos. Soc.* **108** (1990), 445–459.

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

[31] **O. Polverino**, Small minimal blocking sets and complete k-arcs in $\mathrm{PG}(2,p^3)$, *Discrete Math.* **208/209** (1999), 469–476.

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

[33] ———, Subsets of $\mathrm{GF}(q^2)$ with d-th power differences, *Discrete Math.* **208/209** (1999), 547–555.

[34] **T. Szőnyi**, Blocking Sets in Desarguesian Affine and Projective Planes, *Finite Fields Appl.* **3** (1997), 187–202.

[35] ———, On the number of directions determined by a set of points in an affine Galois plane, *J. Combin. Theory Ser. A* **74** (1996), 141–146.

[36] **T. Szőnyi** and **Zs. Weiner**, On the stability of small blocking sets, *J. Algebraic Combin.* **40** (2014), 279–292.

[37] ———, Proof of a conjecture of Metsch, *J. Combin. Theory Ser. A* **118** (2011), 2066–2070.

[38] ———, On the stability of sets of even type, *Adv. Math.* **267** (2014), 381–394.

[39] **P. Vandendriessche**, Codes of Desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$, *Finite Fields Appl.* **17** (2011), 521–531.

Bence Csajbók

Department of Mathematics, Informatics and Economics, University of Basilicata, Campus Macchia Romana, via dell'Ateneo Lucano, I-85100 Potenza, Italy

and

MTA–ELTE Geometric and Algebraic Combinatorics Research Group, Eötvös Loránd University, 1117 Budapest, Pázmány Péter sétány 1/C, Hungary

e-mail: `csajbokb@cs.elte.hu`

website: `http://www.cs.elte.hu/~csajbokb`

Tamás Héger

Department of Computer Science, and

MTA–ELTE Geometric and Algebraic Combinatorics Research Group, Eötvös Loránd University, 1117 Budapest, Pázmány Péter sétány 1/C, Hungary

e-mail: heger@cs.elte.hu

website: http://www.cs.elte.hu/~hetamas

György Kiss

Department of Geometry, and

MTA–ELTE Geometric and Algebraic Combinatorics Research Group, Eötvös Loránd University, 1117 Budapest, Pázmány Péter sétány 1/C, Hungary

e-mail: kissgy@cs.elte.hu