On bisecants of Rédei type blocking sets and applications

Bence Csajbók*

Abstract

If $\mathcal{B}$ is a minimal blocking set of size less than $3(q+1)/2$ in $\mathrm{PG}(2,q)$, q is a power of the prime p, then Szőnyi's result states that each line meets $\mathcal{B}$ in $1 \pmod p$ points. It follows that $\mathcal{B}$ cannot have bisecants, i.e. lines meeting $\mathcal{B}$ in exactly two points. If $q > 13$, then there is only one known minimal blocking set of size $3(q+1)/2$ in $\mathrm{PG}(2,q)$, the so called projective triangle. This blocking set is of Rédei type and it has $3(q-1)/2$ bisecants, which have a very strict structure. We use polynomial techniques to derive structural results on Rédei type blocking sets from information on their bisecants. We apply our results to point sets of $\mathrm{PG}(2,q)$ with few odd-secants.

In particular, we improve the lower bound of Balister, Bollobás, Füredi and Thompson on the number of odd-secants of a $(q+2)$-set in $\mathrm{PG}(2,q)$ and we answer a related open question of Vandendriessche. We prove structural results for semiovals and derive the non existence of semiovals of size $q+3$ when $p \neq 3$ and $q > 5$. This extends a result of Blokhuis who classified semiovals of size $q+2$, and a result of Bartoli who classified semiovals of size $q+3$ when $q \leqslant 17$. In the q even case we can say more applying a result of Szőnyi and Weiner about the stability of sets of even type. We also obtain a new proof to a result of Gács and Weiner about $(q+t,t)$-arcs of type $(0,2,t)$ and to one part of a result of Ball, Blokhuis, Brouwer, Storme and Szőnyi about functions over $\mathrm{GF}(q)$ determining less than $(q+3)/2$ directions.

AMS subject classification: 51E20, 51E21

*Research supported by the Hungarian National Foundation for Scientific Research, Grant No. K 81310 and by the Italian Ministry of Education, University and Research (PRIN 2012 project "Strutture geometriche, combinatoria e loro applicazioni")

1 Introduction

A *blocking set* $\mathcal{B}$ of $\mathrm{PG}(2,q)$, the Desarguesian projective plane of order q, is a point set meeting every line of the plane. $\mathcal{B}$ is called *non-trivial* if it contains no line and *minimal* if $\mathcal{B}$ is minimal subject to set inclusion. A point $P \in \mathcal{B}$ is said to be *essential* if $\mathcal{B}\setminus\{P\}$ is not a blocking set. For a point set $\mathcal{S}$ and a line ℓ we say that ℓ is a k-secant of $\mathcal{S}$ if ℓ meets $\mathcal{S}$ in k points. If $k=1$, $k=2$, or $k=3$, then we call ℓ a tangent to $\mathcal{S}$, a bisecant of $\mathcal{S}$, or a trisecant of $\mathcal{S}$, respectively. We usually consider $\mathrm{PG}(2,q)$ as $\mathrm{AG}(2,q)$, the Desarguesian affine plane of order q, extended by the line at infinity, ℓ_∞. Throughout the paper q will always denote a power of p, p prime. For the points of $\mathrm{AG}(2,q)$ we use cartesian coordinates. The infinite point (or *direction*) of lines with slope m will be denoted by (m), the infinite point of vertical lines will be denoted by (∞). Let $\mathcal{U}=\{(a_i,b_i)\}_{i=1}^{q}$ be a set of q points of $\mathrm{AG}(2,q)$. The set of *directions determined by* $\mathcal{U}$ is $\mathcal{D}_\mathcal{U} := \left\{\left(\frac{b_i-b_j}{a_i-a_j}\right) : i \neq j\right\}$. It is easy to see that $\mathcal{B}:=\mathcal{U}\cup\mathcal{D}_\mathcal{U}$ is a blocking set of $\mathrm{PG}(2,q)$ with the property that there is a line, the line at infinity, which meets $\mathcal{B}$ in exactly $|\mathcal{B}|-q$ points. If $|\mathcal{D}_\mathcal{U}| \leqslant q$, then $\mathcal{B}$ is minimal. Conversely, if $\mathcal{B}$ is a minimal blocking set of size $q+N \leqslant 2q$ and there is a line meeting $\mathcal{B}$ in N points, then $\mathcal{B}$ can be obtained from the above construction. Blocking sets of size $q+N \leqslant 2q$ with an N-secant are called blocking sets of *Rédei type*, the N-secants of the blocking set are called *Rédei lines*. If the q-set $\mathcal{U}$ does not determine every direction, then $\mathcal{U}$ is affinely equivalent to the graph of a function f from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$, i.e. $\mathcal{U}=\{(x,f(x))\colon x\in \mathrm{GF}(q)\}$. Note that $f(x)-cx$ is a permutation polynomial if and only if (c) is a direction not determined by the graph of f, see [14] by Evans, Greene, Niederreiter. A blocking set is said to be *small*, if its size is less than $q+(q+3)/2$. Small minimal Rédei type blocking sets, or equivalently, functions determining less than $(q+3)/2$ directions, have been characterized by Ball, Blokhuis, Brouwer, Storme, Szőnyi and Ball, see [3, 2]. From these results it follows that such blocking sets meet each line of the plane in $1 \pmod p$ points. This property holds for any small minimal blocking set, as it was proved by Szőnyi in [25].

It follows from the above mentioned results that minimal blocking sets with bisecants cannot be small. If q is odd, then the smallest known non-small minimal Rédei type blocking set is the following set of $q+(q+3)/2$ points (up to projective equivalence):

$$\mathcal{B} := \{(0:1:a),\ (1:0:a),\ (-a:1:0)\colon a \text{ a square in } \mathrm{GF}(q)\} \cup \{(0:0:1)\}.$$

In the book of Hirschfeld [17, Lemma 13.6 (i)] this example is called the *projective triangle*. $\mathcal{B}$ has three Rédei lines and has the following properties.

Through each point of $\mathcal{B}$ there passes a bisecant of $\mathcal{B}$. If $\mathcal{H} \subset \mathcal{B}$ is a set of collinear points such that there passes a unique bisecant of $\mathcal{B}$ through each point of $\mathcal{H}$ and there is a Rédei line ℓ disjoint from $\mathcal{H}$, then the bisecants through the points of $\mathcal{H}$ are contained in a pencil. In Theorem 2.4 we show that this property holds for any Rédei type blocking set. In fact, we prove the following stronger result. If R_1 and R_2 are points of $\mathcal{B}\backslash\ell$, such that for $i = 1, 2$ there is a unique bisecant of $\mathcal{B}$ through R_i and there is a point $T \in \ell$, such that TR_1 and TR_2 meet $\mathcal{B}$ in at least four points, then for each $M \in \ell$ the lines R_1M and R_2M meet $\mathcal{B}$ in the same number of points. The essential part of our proof is algebraic, it is based on polynomials over $\mathrm{GF}(q)$. We apply our results to point sets of $\mathrm{PG}(2, q)$ with few odd-secants, which we detail in the next paragraphs.

A semioval $\mathcal{S}$ of a finite projective plane is a point set with the property that at each point of $\mathcal{S}$ there passes exactly one tangent to $\mathcal{S}$. For a survey on semiovals see [19] by Kiss. In $\mathrm{PG}(2, q)$ Blokhuis characterized semiovals of size $q - 1 + a$, $a > 2$, meeting each line in 0,1,2, or a points. He also proved that there is no semioval of size $q + 2$ in $\mathrm{PG}(2, q)$, $q > 7$, see [6] and [9], where the term *seminuclear set* was used for semiovals of size $q + 2$. For another characterization of semiovals with special intersection pattern with respect to lines see [15] by Gács. We refine Blokhuis' characterization to obtain new structural results about semiovals of size $q - 1 + a$ containing a collinear points. As an application, we prove the non-existence of semiovals of size $q + 3$ in $\mathrm{PG}(2, q)$, $5 < q$ odd when $p \neq 3$. For $q \leqslant 17$ this was also proved by Bartoli in [4]. When q is small, then the spectrum of the sizes of semiovals in $\mathrm{PG}(2, q)$ is known, see [23] by Lisonek for $q \leqslant 7$ and [20] by Kiss, Marcugini and Pambianco for $q = 9$. When q is even, then a stronger result follows from [27, Theorem 5.3] by Szőnyi and Weiner on the stability of sets of even type.

In the recent article [1] by Balister, Bollobás, Füredi and Thompson, the minimum number of odd-secants of an n-set in $\mathrm{PG}(2, q)$, q odd, was investigated. They studied in detail the case of $n = q + 2$. In our last section we improve their lower bound and we answer a related open question of Vandendriessche from [28].

Our Theorem 2.3 yields a new proof to [16, Theorem 2.5] by Gács and Weiner about $(q + t, t)$-arcs of type $(0, 2, t)$. In Section 3 we explain some connections between Theorem 2.3 and the direction problem.

2 Bisecants of Rédei type blocking sets

Lemma 2.1. *Let $\mathcal{U}$ be a set of q points in $\mathrm{AG}(2,q)$ and denote by $\mathcal{D}_{\mathcal{U}}$ the set of directions determined by $\mathcal{U}$. Take a point $R = (a_0, b_0) \in \mathcal{U}$ and denote the remaining $q-1$ points of $\mathcal{U}$ by (a_i, b_i) for $i = 1, 2, \ldots, q-1$. Consider the following polynomial:*

$$f(Y) := \prod_{i=1}^{q-1} ((a_i - a_0)Y - (b_i - b_0)) \in \mathrm{GF}(q)[Y]. \tag{1}$$

For $m \in \mathrm{GF}(q)$ the following holds.

1. *The line through R with direction m meets $\mathcal{U}$ in k_m points if and only if m is a $(k_m - 1)$-fold root of $f(Y)$.*
2. *If $(m) \notin \mathcal{D}_{\mathcal{U}}$, then $f(m) = -1$.*
3. *If $(\infty) \notin \mathcal{D}_{\mathcal{U}}$, then the coefficient of Y^{q-1} in f is -1.*

Proof. We have $(a_j - a_0)m - (b_j - b_0) = 0$ for some $j \in \{1, 2, \ldots, q-1\}$ if and only if (m), R and (a_j, b_j) are collinear. This proves part 1. To prove part 2, note that $(a_j - a_0)m - (b_j - b_0) = (a_k - a_0)m - (b_k - b_0)$ for some $j, k \in \{1, 2, \ldots, q-1\}$, $j \neq k$, if and only if $(a_j - a_k)m - (b_j - b_k) = 0$, i.e. if and only if (a_j, b_j), (a_k, b_k) and (m) are collinear. If $(m) \notin \mathcal{D}_{\mathcal{U}}$, then this cannot be and hence $\{(a_i - a_0)m - (b_i - b_0) \colon i = 1, 2, \ldots, q-1\}$ is the set of non-zero elements of $\mathrm{GF}(q)$. It follows that in this case $f(m) = -1$. If $(\infty) \notin \mathcal{D}_{\mathcal{U}}$, then $\{a_i - a_0 \colon i = 1, 2, \ldots, q-1\}$ is the set of non-zero elements of $\mathrm{GF}(q)$, and hence $\prod_{i=1}^{q-1}(a_i - a_0) = -1$. ■

Remark 2.2. *For a set of affine points $\mathcal{U} = \{(a_i, b_i)\}_{i=0}^{k}$ the Rédei polynomial of $\mathcal{U}$ is $\prod_{i=0}^{k}(X + a_iY - b_i) = \sum_{j=0}^{k+1} h_j(Y)X^{k+1-j} \in \mathrm{GF}(q)[X, Y]$, where $h_j(Y) \in \mathrm{GF}(q)[Y]$ is a polynomial of degree at most j. Now suppose that $\mathcal{U}$ is a q-set and $(a_0, b_0) = (0, 0)$. Then $h_{q-1}(Y) = \sum_{j=0}^{q-1}\prod_{i \neq j}(a_iY - b_i) = \prod_{i=1}^{q-1}(a_iY - b_i)$ is the polynomial associated to the affine q-set $\mathcal{U}$ as in Lemma 2.1. This polynomial also appears in Section 4 of Ball's paper [2].*

Theorem 2.3. *Let $\mathcal{B}$ be a blocking set of Rédei type in $\mathrm{PG}(2,q)$, with Rédei line ℓ.*

1. *If there is a point in $\mathcal{B} \setminus \ell$ which is not incident with any bisecant of $\mathcal{B}$, then $\mathcal{B}$ is minimal and $|\ell \cap \mathcal{B}| \equiv 1 \pmod{p}$.*
2. *If $R, R' \in \mathcal{B} \setminus \ell$ such that R and R' are not incident with any bisecant of $\mathcal{B}$, then $|RM \cap \mathcal{B}| = |R'M \cap \mathcal{B}|$ for each $M \in \ell$.*

Proof. It is easy to see that if there is a point $R \in \mathcal{B}\backslash\ell$, such that there is no bisecant of $\mathcal{B}$ through R, then $|\mathcal{B} \cap \ell| \leqslant q-1$. First we show that $\mathcal{B}$ is minimal. As $\mathcal{B}$ is of Rédei type, the points of $\mathcal{B}\backslash\ell$ are essential in $\mathcal{B}$. Take a point $D \in \mathcal{B} \cap \ell$. As there is no bisecant through R, it follows that DR meets $\mathcal{B}$ in at least three points and hence there is a tangent to $\mathcal{B}$ at D, i.e. D is essential in $\mathcal{B}$.

We may assume that $\ell = \ell_\infty$ and $(\infty) \notin \mathcal{B}$. Let $R = (a_0, b_0)$ be a point of $\mathcal{B}\backslash\ell$ which is not incident with any bisecant of $\mathcal{B}$ and let $\mathcal{U} = \mathcal{B}\backslash\ell_\infty = \{(a_i, b_i)\}_{i=0}^{q-1}$. Consider the polynomial $f(Y) = \prod_{i=1}^{q-1}((a_i - a_0)Y - (b_i - b_0))$ introduced in (1). Let $m \in \mathrm{GF}(q)$. According to Lemma 2.1 we have the following.

- If $(m) \in \mathcal{B}$, then $f(m) = 0$,
- if $(m) \notin \mathcal{B}$, then $f(m) = -1$,
- the coefficient of Y^{q-1} in f is -1.

Now let $\ell_\infty\backslash(\mathcal{B} \cup \{(\infty)\}) = \{(m_1), (m_2), \ldots, (m_k)\}$ and consider the polynomial

$$g(Y) := \sum_{i=1}^{k} (Y - m_i)^{q-1} - k.$$

For $m \in \mathrm{GF}(q)$ we have $g(m) = f(m)$. As both polynomials have degree at most $q-1$, it follows that $g(Y) = f(Y)$. The coefficient of Y^{q-1} is k in g and hence $p \mid k+1$. As $k+1 = q+1-|\mathcal{B} \cap \ell_\infty|$, part 1 follows.

For $(m) \notin \mathcal{B}$ the line through any point of $\mathcal{U}$ with slope m meets $\mathcal{B}$ in 1 point. For $(m) \in \mathcal{B}$ the line through R with slope m meets $\mathcal{B}$ in $k_m + 2$ points if and only if m is a k_m-fold root of $f(Y)$. As $f(Y) = g(Y)$, and the coefficients of $g(Y)$ depend only on the points of $\mathcal{B} \cap \ell_\infty$, it follows that k_m does not depend on the initial choice of the point R, as long as the chosen point is not incident with any bisecant of $\mathcal{B}$. This proves part 2. ∎

Theorem 2.4. *Let $\mathcal{B}$ be a blocking set of Rédei type in $\mathrm{PG}(2,q)$, with Rédei line ℓ.*

1. *If there is a point in $\mathcal{B}\backslash\ell$ contained in a unique bisecant of $\mathcal{B}$, then $|\mathcal{B} \cap \ell| \not\equiv 1 \pmod p$.*
2. *If $R_1, R_2 \in \mathcal{B}\backslash\ell$, each of them is contained in a unique bisecant of $\mathcal{B}$ and there is a point $T \in \ell$ such that R_1T and R_2T both meet $\mathcal{B}$ in at least four points, then for each $M \in \ell$ we have $|MR_1 \cap \mathcal{B}| = |MR_2 \cap \mathcal{B}|$.*

3. If $R_1, R_2 \in \mathcal{B}\setminus\ell$, each of them is contained in a unique bisecant of $\mathcal{B}$ and the common point of these bisecants is on the line ℓ, then for each $M \in \ell$ we have $|MR_1 \cap \mathcal{B}| = |MR_2 \cap \mathcal{B}|$.

Proof. Let R be a point of $\mathcal{B}\setminus\ell$ contained in a unique bisecant r of $\mathcal{B}$. First suppose $|\mathcal{B} \cap \ell| = q$. Then part 1 is trivial and there is no line through R meeting $\mathcal{B}$ in at least 4 points, since otherwise we would get more than one bisecants through R. Suppose that R' is another point of $\mathcal{B}\setminus\ell$ contained in a unique bisecant r' of $\mathcal{B}$ and $r \cap r' \in \ell$. Let $\{Q\} = \ell\setminus\mathcal{B}$. Then RQ and $R'Q$ are tangents to $\mathcal{B}$ and $|MR \cap \mathcal{B}| = |MR' \cap \mathcal{B}| = 3$ for each $M \in (\ell \cap \mathcal{B})\setminus\{r \cap r'\}$. From now on, we assume $k := q - |\mathcal{B} \cap \ell| \geqslant 1$.

First we prove the theorem when $\mathcal{B}$ is minimal. We may assume $\ell = \ell_\infty$ and $\ell_\infty\setminus\mathcal{B} = \{(\infty), (m_1), \ldots, (m_k)\}$.

As in the proof of Theorem 2.3, let $\mathcal{U} = \mathcal{B}\setminus\ell_\infty = \{(a_i, b_i)\}_{i=0}^{q-1}$ and define $f(Y)$ as in (1). Take $m \in \mathrm{GF}(q)$ and let t be the slope of the unique bisecant through R. From Lemma 2.1 we obtain the following.

$$f(m) = \begin{cases} -1 & \text{if } (m) \notin \mathcal{B}, \\ 0 & \text{if } (m) \in \mathcal{B}\setminus\{(t)\}, \\ f(t) \neq 0 & \text{if } m = t. \end{cases}$$

Consider the polynomial

$$g(Y) := f(t) + |\mathcal{B} \cap \ell_\infty| + \sum_{i=1}^{k}(Y - m_i)^{q-1} - f(t)(Y - t)^{q-1}. \tag{2}$$

For $m \in \mathrm{GF}(q)$ we have $g(m) = f(m)$. As both polynomials have degree at most $q - 1$, it follows that $g(Y) = f(Y)$. The coefficient of Y^{q-1} is $-|\mathcal{B} \cap \ell_\infty| - f(t)$ in g and -1 in f. It follows that $p \mid |\mathcal{B} \cap \ell_\infty| + f(t) - 1$ and hence $f(t) \equiv 1 - |\mathcal{B} \cap \ell_\infty| \equiv k + 1 \pmod{p}$. If $|\mathcal{B} \cap \ell_\infty| \equiv 1 \pmod{p}$, then $f(t) = 0$, a contradiction. This proves part 1.

Now consider

$$\partial_Y g(Y) = -\sum_{i=1}^{k}(Y - m_i)^{q-2} + (k + 1)(Y - t)^{q-2},$$

and

$$w(Y) := (Y - t)\prod_{i=1}^{k}(Y - m_i)\partial_Y g(Y) =$$

$$-\sum_{i=1}^{k}(Y - m_i)^{q-1}(Y - t)\prod_{j\neq i}(Y - m_j) + (k + 1)(Y - t)^{q-1}\prod_{j=1}^{k}(Y - m_j).$$

If $(m) \in \mathcal{B}\setminus\{(t)\}$, then

$$w(m) = -\sum_{i=1}^{k}(m-t)\prod_{j\neq i}(m-m_j) + (k+1)\prod_{j=1}^{k}(m-m_j).$$

Suppose that the line through R with direction m meets $\mathcal{B}$ in at least four points. Then m is a multiple root of $f(Y)$ and hence it is also a root of $w(Y)$. It follows that m is a root of

$$\tilde{w}(Y) := -(Y-t)\sum_{i=1}^{k}\prod_{j\neq i}(Y-m_j) + (k+1)\prod_{j=1}^{k}(Y-m_j). \tag{3}$$

Note that $\sum_{i=1}^{k}\prod_{j\neq i}(m-m_j) = 0$ and $\tilde{w}(m) = 0$ together would imply $(k+1)\prod_{j=1}^{k}(m-m_j) = 0$, which cannot be since $(m) \notin \{(m_1), \ldots, (m_k)\}$ and $p \nmid k+1$. It follows that t can be expressed from m and $m_1, \ldots, m_k$ in the following way:

$$t = m - \frac{(k+1)\prod_{j=1}^{k}(m-m_j)}{\sum_{i=1}^{k}\prod_{j\neq i}(m-m_j)}. \tag{4}$$

Now let R_1 and R_2 be two points as in part 2 and let $T = (m)$. It follows from (4) that the bisecants through these points have the same slope. Then, according to (2), $f(Y) = g(Y)$ does not depend on the choice of R_i, for $i = 1, 2$. The assertion follows from Lemma 2.1 part 1.

If R_1 and R_2 are two points as in part 3, then the bisecants through these points have the same slope. It follows that $f(Y) = g(Y)$ does not depend on the choice of R_i, for $i = 1, 2$. As above, the assertion follows from Lemma 2.1 part 1.

Now suppose that $\mathcal{B}$ is not minimal and $R_1 \in \mathcal{B}\setminus\ell$ is contained in a unique bisecant of $\mathcal{B}$. As $\mathcal{B}$ is a blocking set of Rédei type, the points of $\mathcal{B}\setminus\ell$ are essential in $\mathcal{B}$. Let $C \in \mathcal{B} \cap \ell$ such that $\mathcal{B}' := \mathcal{B}\setminus\{C\}$ is a blocking set. In this case for each $P \in \mathcal{B}\setminus\ell$ the line PC is a bisecant of $\mathcal{B}$ and R_1C is the unique bisecant of $\mathcal{B}$ through R_1. It follows that there is no bisecant of $\mathcal{B}'$ through R_1. Then Theorem 2.3 yields that $|\ell \cap \mathcal{B}'| \equiv 1 \pmod{p}$. As $|\ell \cap \mathcal{B}| = |\ell \cap \mathcal{B}'| + 1$, we proved part 1.

If R_2 is another point of $\mathcal{B}\setminus\ell$ such that R_2 is contained in a unique bisecant of $\mathcal{B}$, then there is no bisecant of $\mathcal{B}'$ through R_2 and hence parts 2 and 3 follow from Theorem 2.3 part 2. ■

3 Connections with the direction problem

Let $\mathcal{B}$ be a blocking set in $\mathrm{PG}(2,q)$. We recall $q = p^h$, p prime. The *exponent* of $\mathcal{B}$ is the maximal integer $0 \leqslant e \leqslant h$ such that each line meets $\mathcal{B}$ in 1 (mod p^e) points. We recall the following two results about the exponent.

Theorem 3.1 (Szőnyi [25])**.** *Let $\mathcal{B}$ be a small minimal blocking set in $\mathrm{PG}(2,q)$. Then $\mathcal{B}$ has positive exponent.*

Theorem 3.2 (Sziklai [24])**.** *Let $\mathcal{B}$ be a small minimal blocking set in $\mathrm{PG}(2,q)$. Then the exponent of $\mathcal{B}$ divides h.*

Proposition 3.3. *Let $\mathcal{B}$ be a blocking set of Rédei type in $\mathrm{PG}(2,q)$, with Rédei line ℓ . Suppose that $\mathcal{B}$ does not have bisecants. Then $\mathcal{B}$ has positive exponent and for each point $M \in \ell \cap \mathcal{B}$ the lines through M different from ℓ meet $\mathcal{B}$ in 1 or in $p^t + 1$ points, where t is a positive integer depending only on the choice of M.*

Proof. Theorem 2.3 part 1 yields that ℓ meets $\mathcal{B}$ in $1 \pmod p$ points. Lines meeting ℓ not in $\mathcal{B}$ are tangents to $\mathcal{B}$. For any $M \in \ell \cap \mathcal{B}$ Theorem 2.3 part 2 yields that MR meets $\mathcal{B}\backslash\ell$ in the same number of points for each $R \in \mathcal{B}\backslash\ell$. Denote this number by k. Then k divides $|\mathcal{B}\backslash\ell| = q$. As $\mathcal{B}$ does not have bisecants, it follows that $k > 1$ and hence $k = p^t$ for some positive integer t.
■

The following result is a consequence of the lower bound on the size of an affine blocking set due to Brouwer and Schrijver [11] and Jamison [18].

Theorem 3.4 (Blokhuis and Brouwer [7, pg. 133])**.** *If $\mathcal{B}$ is a minimal blocking set of size $q + N$, then there are at least $q + 1 - N$ tangents to $\mathcal{B}$ at each point of $\mathcal{B}$.*

Theorem 3.5. *Let f be a function from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ and let N be the number of directions determined by f. If any line with a direction determined by f that is incident with a point of the graph of f is incident with at least two points of the graph of f, then each line meets the graph of f in p^t points for some integer t and*

$$q/s + 1 \leqslant N \leqslant (q-1)/(s-1),$$

where $s = \min\{p^t\colon$ there is line meeting the graph of f in $p^t > 1$ points$\}$.

Proof. If $\mathcal{U}$ denotes the graph of f, then $\mathcal{B} := \mathcal{U} \cup \mathcal{D}_{\mathcal{U}}$ is a blocking set of Rédei type without bisecants. Proposition 3.3 yields that each line meets

$\mathcal{U}$ in p^t points for some integer t, with $t = 0$ only for lines with direction not in $\mathcal{D}_\mathcal{U}$. Take a point $R \in \mathcal{U}$ and let $\mathcal{D}_\mathcal{U} = \{D_1, D_2, \ldots, D_N\}$. Then $|D_i R \cap \mathcal{B}| \geqslant s+1$ yields $|\mathcal{B}| = q+N \geqslant Ns+1$ and hence $(q-1)/(s-1) \geqslant N$. Take a line m meeting $\mathcal{U}$ in s points and let $M = m \cap \ell_\infty$. According to Proposition 3.3 the lines through M meet $\mathcal{U}$ in 0 or in s points. Theorem 3.4 yields that the number of lines through M that meet $\mathcal{U}$ is at most $N-1$. It follows that $(N-1)s \geqslant q$ and hence $N \geqslant q/s + 1$. ■

Applying Theorems 3.5 and 3.1 we can give a new proof to the following result.

Theorem 3.6 (part of Ball et al. [3] and Ball [2])**.** *Let f be a function from* $\mathrm{GF}(q)$ *to* $\mathrm{GF}(q)$ *and let N be the number of directions determined by f. Let $s = p^e$ be maximal such that any line with a direction determined by f that is incident with a point of the graph of f is incident with a multiple of s points of the graph of f. Then one of the following holds.*

1. *$s = 1$ and $(q+3)/2 \leqslant N \leqslant q+1$,*
2. *$q/s + 1 \leqslant N \leqslant (q-1)/(s-1)$,*
3. *$s = q$ and $N = 1$.*

Proof. The point set $\mathcal{B} := \mathcal{U} \cup \mathcal{D}_\mathcal{U}$ is a minimal blocking set of Rédei type. If $s = 1$, then $\mathcal{B}$ cannot be small because of Szőnyi's Theorem 3.1 and hence $N \geqslant (q+3)/2$. If $s > 1$, then the bounds on N follow from Theorem 3.5. ■

In [3] and [2] it was also proved that for $s > 2$ the graph of f is $\mathrm{GF}(s)$-linear and that $\mathrm{GF}(s)$ is a subfield of $\mathrm{GF}(q)$. Note that Theorem 3.2 by Sziklai generalizes the latter result.

4 Small semiovals

An *oval* of a projective plane of order q is a set of $q+1$ points such that no three of them are collinear. It is easy to see that ovals are semiovals. The smallest known *non-oval semioval*, i.e. semioval which is not an oval, is due to Blokhuis.

Example 4.1 (Blokhuis [6])**.** *Let $\mathcal{S}$ be the following point set in* $\mathrm{PG}(2,q)$*, $3 < q$ odd, $\mathcal{S} = \{(0:1:s), (s:0:1), (1:s:0) \colon -s$ is not a square$\}$. Then $\mathcal{S}$ is a semioval of size* $3(q-1)/2$.

Conjecture 4.2 (Kiss et al. [20, Conjecture 11]). *If a semioval in* $\mathrm{PG}(2,q)$*,* $q > 7$*, has less than* $3(q-1)/2$ *points, then it has exactly* $q+1$ *points and it is an oval.*

Let $\mathcal{S}$ be a semioval and ℓ a line meeting $\mathcal{S}$ in at least two points. Take a point $P \in \mathcal{S} \cap \ell$. As there is a unique tangent to $\mathcal{S}$ at P, it follows that $|\mathcal{S} \backslash \ell| \geqslant q-1$, and hence $|\mathcal{S}| \geqslant |\mathcal{S} \cap \ell| + q - 1 \geqslant q+1$. It is convenient to denote the size of $\mathcal{S}$ by $q-1+a$, where $a \geqslant 2$ holds automatically. Then each line meets $\mathcal{S}$ in at most a points.

Theorem 4.3 (Blokhuis [6]). *Let* $\mathcal{S}$ *be a semioval of size* $q-1+a$*,* $a > 2$*, in* $\mathrm{PG}(2,q)$ *and suppose that each line meets* $\mathcal{S}$ *in* 0*,* 1*,* 2*, or in* a *points. Then* $\mathcal{S}$ *is the symmetric difference of two lines with one further point removed from both lines, or* $\mathcal{S}$ *is projectively equivalent to Example 4.1.*

If $\mathcal{S}$ is a semioval of size $q+2$, then each line meets $\mathcal{S}$ in at most three points, thus Theorem 4.3 yields the following.

Theorem 4.4 (Blokhuis [6]). *Let* $\mathcal{S}$ *be a semioval of size* $q+2$ *in* $\mathrm{PG}(2,q)$*. Then* $\mathcal{S}$ *is the symmetric difference of two lines with one further point removed from both lines in* $\mathrm{PG}(2,4)$*, or* $\mathcal{S}$ *is projectively equivalent to Example 4.1 in* $\mathrm{PG}(2,7)$*.*

We also recall the following well-known result by Blokhuis which will be applied several times. For another proof and possible generalizations see [26, Remark 7] by Szőnyi, or [12, Corollary 3.6] by Csajbók, Héger and Kiss.

Proposition 4.5 (Blokhuis [6, Proposition 2]). *Let* $\mathcal{S}$ *be a point set of* $\mathrm{PG}(2,q)$*,* $q > 2$*, of size* $q-1+a$*,* $a \geqslant 2$*, with an* a*-secant* ℓ*. If there is a unique tangent to* $\mathcal{S}$ *at each point of* $\ell \cap \mathcal{S}$*, then these tangents are contained in a pencil. The carrier of this pencil is called the* nucleus *of* ℓ *and it is denoted by* N_ℓ*. For the sake of simplicity, the nucleus of a line* ℓ_i *will be denoted by* N_i*.*

If $\mathcal{A}$ and $\mathcal{B}$ are two point sets, then $\mathcal{A}\Delta\mathcal{B}$ denotes their symmetric difference, that is $(\mathcal{A}\backslash\mathcal{B}) \cup (\mathcal{B}\backslash\mathcal{A})$.

Example 4.6 (Csajbók, Héger and Kiss [12, Example 2.12]). *Let* $\mathcal{B}'$ *be a blocking set of Rédei type in* $\mathrm{PG}(2,q)$*, with Rédei line* ℓ*. Suppose that there is a point* $P \in \mathcal{B}'\backslash\ell$ *such that the bisecants of* $\mathcal{B}'$ *pass through* P *and there is no trisecant of* $\mathcal{B}'$ *through* P*. For example, if* $\mathcal{B}'$ *has exponent* e *and* $p^e \geqslant 3$ *(cf. Section 3), then* $\mathcal{B}'$ *has no bisecants or trisecants and hence one can choose any point* $P \in \mathcal{B}'\backslash\ell$*. Take a point* $W \in \ell\backslash\mathcal{B}'$ *and let* $\mathcal{S} = (\ell\Delta\mathcal{B}')\backslash\{W,P\}$*. Then* $\mathcal{S}$ *is a semioval of size* $q-1+a$*, where* $a = |\ell \cap \mathcal{S}|$*.*

Remark 4.7. *The blocking set $\mathcal{B}'$ in Example 4.6 is necessarily minimal. To see this consider any point $R \in \mathcal{B}' \backslash (\ell \cup \{P\})$. As the bisecants of $\mathcal{B}'$ pass through P, it follows that there is no bisecant of $\mathcal{B}'$ through R and hence Theorem 2.3 part 1 yields that $\mathcal{B}'$ is minimal.* ■

Lemma 4.8. *Let $\mathcal{S}$ be a semioval of size $q-1+a$ in $\mathrm{PG}(2,q)$ and suppose that there is a line ℓ which is an a-secant of $\mathcal{S}$. Denote the set of tangents through the points of $\mathcal{S}\backslash\ell$ by $\mathcal{L}$ and let $\mathcal{B} = \{N_\ell\} \cup (\mathcal{S}\Delta\ell)$. Then one of the following holds.*

1. *$\mathcal{S}$ is an oval.*
2. *$\mathcal{L}$ is contained in a pencil with carrier C. Then $C \in \ell$ and $\mathcal{B}' := \mathcal{B}\backslash\{C\}$ is a blocking set of Rédei type with Rédei line ℓ. In this case $\mathcal{S}$ can be obtained from $\mathcal{B}'$ as in Example 4.6 with $P = N_\ell$ and $W = C$.*
3. *$\mathcal{L}$ is not contained in a pencil. Then $\mathcal{B}$ is a minimal blocking set of Rédei type with Rédei line ℓ and*
   - *(a) $p \nmid a$,*
   - *(b) for any $R \in \mathcal{S}\backslash\ell$ the line RN_ℓ is not a tangent to $\mathcal{S}$,*
   - *(c) if $R_1, R_2 \in \mathcal{S}\backslash\ell$ and there is a point $T \in \ell$ such that R_iT meets $\mathcal{S} \cup \{N_\ell\}$ in at least three points for $i = 1, 2$, then for each $M \in \ell$ we have $|R_1M \cap (\mathcal{S} \cup \{N_\ell\})| = |R_2M \cap (\mathcal{S} \cup \{N_\ell\})|$,*
   - *(d) if $R_1, R_2 \in \mathcal{S}\backslash\ell$ and the tangents to $\mathcal{S}$ at these two points meet each other on the line ℓ, then for each $M \in \ell$ we have $|R_1M \cap (\mathcal{S} \cup \{N_\ell\})| = |R_2M \cap (\mathcal{S} \cup \{N_\ell\})|$.*

Proof. First we show that $\mathcal{B}$ is a blocking set of Rédei type. Take a point $R \in \mathcal{S}\backslash\ell$. As there is a tangent to $\mathcal{S}$ at R it follows that ℓ meets $\mathcal{S}$ in at most q points and hence ℓ is blocked by $\mathcal{B}$. Lines meeting ℓ not in $\mathcal{S}$ are blocked by $\mathcal{B}$ since $\ell\backslash\mathcal{S} \subset \mathcal{B}$. If a line m meets ℓ in $\mathcal{S}$, then either m is a tangent to $\mathcal{S}$ and hence $N_\ell \in m$, or m is not a tangent to $\mathcal{S}$ and hence there is a point of $\mathcal{S}\backslash\ell$ contained in m. As $\{N_\ell\} \cup (\mathcal{S}\backslash\ell) \subset \mathcal{B}$, it follows that m is blocked by $\mathcal{B}$ and hence $\mathcal{B}$ is a blocking set. The line ℓ meets $\mathcal{B}$ in $|\mathcal{B}| - q$ points, thus $\mathcal{B}$ is of Rédei type and ℓ is a Rédei line of $\mathcal{B}$.

If $a = 2$, then $\mathcal{S}$ is an oval. From now on we assume $a \geqslant 3$. First suppose that $\mathcal{L}$ is contained in a pencil with carrier C. If $C \notin \ell$, then $|\mathcal{L}| \leqslant q+1-a$, but $|\mathcal{L}| = |\mathcal{S}\backslash\ell| = q-1$. It follows that $C \in \ell$.

Let $\mathcal{B}' = \mathcal{B}\backslash\{C\}$. In this paragraph we prove that $\mathcal{B}'$ is a blocking set. It is enough to show that the lines through C are blocked by $\mathcal{B}'$. This trivially holds for the $q-1$ lines in $\mathcal{L}$. First we show that $\mathcal{B}'$ blocks ℓ too. Suppose to the contrary that $\ell\backslash(\mathcal{S}\cup\{C\})=\varnothing$ and hence $a=q$. As $a\geqslant 3$, we have $q\geqslant 3$ and hence there are at least two points in $\mathcal{S}\backslash\ell$. Take $R,Q\in\mathcal{S}\backslash\ell$ and let $M=RQ\cap\ell$. Since $M\neq C$, we have $M\in\mathcal{S}$. Then there are at least two tangents to $\mathcal{S}$ incident with M and this contradiction shows that ℓ is blocked by $\mathcal{B}'$. Now we show $CN_\ell\notin\mathcal{L}$. Suppose to the contrary that CN_ℓ is a tangent to $\mathcal{S}$ at some $V\in\mathcal{S}\backslash\ell$. Then VC is a trisecant of $\mathcal{B}$. If there were a bisecant v of $\mathcal{B}$ through V, then, by the construction of $\mathcal{B}$, v would be a tangent to $\mathcal{S}$ at V. This cannot be since the unique tangent to $\mathcal{S}$ at V is VC, which is a trisecant of $\mathcal{B}$ and hence $v\neq VC$. For any $V'\in\mathcal{S}\backslash(\ell\cup\{V\})$, there is a unique bisecant of $\mathcal{B}$ through V', namely $V'C$. We have shown that there is a point in $\mathcal{B}\backslash\ell$ not incident with any bisecant of $\mathcal{B}$ and there are points in $\mathcal{B}\backslash\ell$ incident with a unique bisecant of $\mathcal{B}$. This cannot be because of Theorem 2.3 part 1 and Theorem 2.4 part 1. It follows that CN_ℓ is not a tangent to $\mathcal{S}$. As CN_ℓ is blocked by $\mathcal{B}'$ and the other q lines through C, ℓ and the lines of $\mathcal{L}$, are also blocked, it follows that $\mathcal{B}'$ is a blocking set. It is easy to see that ℓ is a Rédei line of $\mathcal{B}'$.

We show that there is no bisecant of $\mathcal{B}'$ through the points of $\mathcal{S}\backslash\ell$. Take a point $R\in\mathcal{S}\backslash\ell$ and suppose to the contrary that there is a bisecant b of $\mathcal{B}'$ through R. Then, by the construction of $\mathcal{B}'$, the line b is a tangent to $\mathcal{S}$ at R. This is a contradiction since $b\neq RC$. It follows that if $\mathcal{B}'$ has bisecants, then they pass through N_ℓ. If there were a trisecant t of $\mathcal{B}'$ through N_ℓ, then let $V=t\cap\mathcal{S}$. It follows that t is a tangent to $\mathcal{S}$ at V. But we have already seen that there is no line of $\mathcal{L}$ incident with N_ℓ. This finishes the proof of part 2.

Now suppose that $\mathcal{S}$ is as in part 3. If $\mathcal{B}$ were not minimal, then the line set $\mathcal{L}$ would be contained in a pencil with carrier on ℓ, a contradiction. Take a point $R\in\mathcal{S}\backslash\ell$. If RN_ℓ is the tangent to $\mathcal{S}$ at R, then there is no bisecant of $\mathcal{B}$ through R, thus $p\mid a$ (cf. Theorem 2.3 part 1). If RN_ℓ is not the tangent to $\mathcal{S}$ at R, then there is a unique bisecant of $\mathcal{B}$ through R (the tangent to $\mathcal{S}$ at R), thus $p\nmid a$ (cf. Theorem 2.4 part 1). It follows that if any of the lines of $\mathcal{L}$ is incident with N_ℓ, or if $p\mid a$, then the whole line set $\mathcal{L}$ is contained in the pencil with carrier N_ℓ, a contradiction. This proves parts (a) and (b). Parts (c) and (d) follow from Theorem 2.4 parts 2 and 3, respectively. ∎

Remark 4.9. *The properties (a)-(d) in part 3 of Lemma 4.8 also hold when $\mathcal{S}$ is as in Example 4.6. From the properties of the point P in Example 4.6 it follows that for $R\in\mathcal{S}\backslash\ell$ the line RP is not a tangent to $\mathcal{S}$ and this proves (b). As for any two points $R_1,R_2\in\mathcal{S}\backslash\ell$ there is no bisecant of $\mathcal{B}'$ incident* *with R_1 or R_2, properties (a), (c) and (d) follow from Theorem 2.3.* ∎

Theorem 4.10. *Let $\mathcal{S}$ be a semioval of size $q-1+a$, $a>2$, which admits an a-secant ℓ, and let $m \neq \ell$ be a k-secant of $\mathcal{S}$.*

1. *For each $R \in \mathcal{S}\backslash\ell$, the line RN_ℓ is not a tangent to $\mathcal{S}$.*
2. *If $k \geqslant 3$, then the tangents to $\mathcal{S}$ at the points of m are contained in a pencil with carrier on ℓ.*
3. *If $k > (a-1)/2$, then $k = a$ and $N_\ell \in m$, or $k = \lceil a/2 \rceil$ and $N_\ell \notin m$.*

Proof. Part 1 follows from Lemma 4.8 part 3 (b), and part 2 follows from Lemma 4.8 part (c) with $T = m \cap \ell$.

To prove part 3 first suppose $k > (a+1)/2$ and $N_\ell \notin m$. Let $m \cap \mathcal{S} = \{R_1, R_2, \ldots, R_k\}$. The lines R_iN_ℓ for $i = 1, 2, \ldots, k$ cannot be bisecants of $\mathcal{S} \cup \{N_\ell\}$ since they are not tangents to $\mathcal{S}$. Thus each of these lines meets $\mathcal{S} \cup \{N_\ell\}$ in at least three points. Let $B_i = \ell \cap R_iN_\ell$, then we have $|R_iB_i \cap (\mathcal{S} \cup \{N_\ell\})| \geqslant 3$ for $i \in \{1, 2, \ldots, k\}$. We apply Lemma 4.8 part 3 (c) with $T = \ell \cap m$ (note that $k > (a+1)/2 \geqslant 2$). For $j \in \{2, \ldots, k\}$ we obtain $|R_1B_j \cap (\mathcal{S} \cup \{N_\ell\})| = |R_jB_j \cap (\mathcal{S} \cup \{N_\ell\})|$, thus also $|R_1B_j \cap (\mathcal{S} \cup \{N_\ell\})| \geqslant 3$ for $j \in \{2, 3, \ldots, k\}$. We have $N_\ell \in R_1B_1$ and hence $N_\ell \notin R_1B_j$ for $j \in \{2, 3, \ldots, k\}$. It follows that $R_1B_2 \cup R_1B_3 \cup \ldots R_1B_k \cup m$ contains at least $2(k-1) + k = 3k - 2$ points of $\mathcal{S}$. As there is a unique tangent to $\mathcal{S}$ at R_1, we must have $a + (q-1) - (3k-2) \geqslant q - k$. This is a contradiction when $k > (a+1)/2$. It follows that lines meeting $\mathcal{S}$ in more than $(a+1)/2$ points have to pass through N_ℓ.

Now suppose that m is a k-secant of $\mathcal{S}$ with $(a-1)/2 < k < a$ and $N_\ell \in m$. Take a point $R \in m \cap \mathcal{S}$. As $k < a$, there is at least one other line m' through R meeting $\mathcal{S}$ in at least three points. Let $R' \in (m' \cap \mathcal{S})\backslash\{R\}$. Lemma 4.8 part 3 (c) with $T = m' \cap \ell$ and $M = m \cap \ell$ yields that the line joining R' and $m \cap \ell$ meets $\mathcal{S}$ in $|(\mathcal{S} \cup \{N_\ell\}) \cap m| = k + 1 > (a+1)/2$ points. Then, according to the previous paragraph, this line also passes through N_ℓ, a contradiction. It follows that either $k = a$ and hence $N_l \in m$, or $N_l \notin m$ and hence $(a-1)/2 < k \leqslant (a+1)/2$. ∎

Lemma 4.11. *Let $\mathcal{S}$ be a semioval of size $q-1+a$ in $\mathrm{PG}(2,q)$. For each point $R \in \mathcal{S}$ the number of lines through R meeting $\mathcal{S}$ in at least three points is at most $a-2$.* ∎

Theorem 4.12. *Let $\mathcal{S}$ be a semioval of size $q-1+a$, $a>2$, in $\mathrm{PG}(2,q)$. If $\mathcal{S}$ has two a-secants, then one of the following holds.*

1. *$\mathcal{S}$ is the symmetric difference of two lines with one further point removed from both lines.*

2. *$\mathcal{S}$ is projectively equivalent to Example 4.1.*

Proof. Let ℓ_1 and ℓ_2 be two a-secants of $\mathcal{S}$ and let $\mathcal{S}' = \mathcal{S}\backslash(\ell_1 \cup \ell_2)$. Theorem 4.10 yields $N_1 \in \ell_2$ and $N_2 \in \ell_1$. If $\mathcal{S}' = \emptyset$, then $\mathcal{S} \subseteq \ell_1 \cup \ell_2$ and it is easy to see that $\mathcal{S}$ is as in part 1. If $\mathcal{S}' \neq \emptyset$, then take any point $R \in \mathcal{S}'$. We show that the tangent to $\mathcal{S}$ at R passes through $P := \ell_1 \cap \ell_2$. As $a > 2$, there is a line r through R meeting $\mathcal{S}$ in at least 3 points. According to Theorem 4.10 part 2, the tangents to $\mathcal{S}$ at the points of $r \cap \mathcal{S}$ pass through a unique point of ℓ_1, and also through a unique point of ℓ_2. It follows that these tangents pass through the point P.

We show that $\mathcal{S}'$ is contained in the line $\ell_3 := N_1N_2$. Suppose, contrary to our claim, that there is a point $R \in \mathcal{S}'\backslash\ell_3$. There is a line r through R meeting $\mathcal{S}$ in at least three points. Since $R \notin \ell_3$, r cannot be incident with both N_1 and N_2. We may assume $N_2 \notin r$. Let $M = r \cap \ell_1$. Note that $M \notin \mathcal{S} \cup \{N_2, P\}$. Take a point $Q \in \ell_2 \cap \mathcal{S}$. Since the unique tangent to $\mathcal{S}$ at Q is QN_2, it follows that QM is a bisecant of $\mathcal{S}$ and it contains a unique point of $\mathcal{S}'$. Denote this point by R'. The tangents to $\mathcal{S}$ at R and R' pass through the same point of ℓ_1, namely P, and hence we can apply Lemma 4.8 part 3 (d). It follows that $2 = |MR' \cap (\mathcal{S} \cup \{N_1\})| = |MR \cap (\mathcal{S} \cup \{N_1\})| \geqslant 3$. This contradiction shows $\mathcal{S}' \subset \ell_3$. Lines meeting each of ℓ_1, ℓ_2 and ℓ_3 meet $\mathcal{S}$ in at most two points. Take any point $H \in \mathcal{S} \cap \ell_3$. Since the tangent to $\mathcal{S}$ at H is PH, and the other lines through H are not tangents, we obtain $2a = |\ell_1 \cap \mathcal{S}| + |\ell_2 \cap \mathcal{S}| = q - 1$ and hence $a = (q-1)/2$. The size of $\mathcal{S}$ is $q - 1 + a = 2a + |\mathcal{S}'|$, so $|\mathcal{S}'| = a = (q-1)/2$. It is easy to show that $\mathcal{S}$ is projectively equivalent to Example 4.1. For the complete description of semiovals contained in the sides of a vertexless triangle see the paper of Kiss and Ruff [21]. ■

A *(k, n)-arc* of $\mathrm{PG}(2, q)$ is a set of k points such that each line meets the k-set in at most n points.

Theorem 4.13. *Let $\mathcal{S}$ be a semioval of size $q + 3$ in $\mathrm{PG}(2, q)$, q is a power of the prime p. Then $q = 5$ and $\mathcal{S}$ is the symmetric difference of two lines with one further point removed from both lines, or $q = 9$ and $\mathcal{S}$ is as in Example 4.1, or $p = 3$ and $\mathcal{S}$ is a $(q + 3, 3)$-arc.*

Proof. It is easy to see that the points of $\mathcal{S}$ fall into the following two types:

- points contained in a unique 4-secant and in $q - 1$ bisecants,

- points contained in two trisecants and in $q-2$ bisecants.

If $\mathcal{S}$ does not have 4-secants, then the number of trisecants of $\mathcal{S}$ is $(q+3)2/3$, thus $3 \mid q$. Now suppose that $\mathcal{S}$ has a 4-secant, ℓ. Theorem 4.10 with $a=4$ yields that $\mathcal{S}$ does not have trisecants. The assertion follows from Theorem 4.12. ■

5 Small semiovals when q is even

We will use the following theorem by Szőnyi and Weiner. This result was proved by the so called resultant method. We say that a line ℓ is an *odd-secant* (resp. *even-secant*) of $\mathcal{S}$ if $|\ell \cap \mathcal{S}|$ is odd (resp. even). A *set of even type* is a point set $\mathcal{H}$ such that each line is an even-secant of $\mathcal{H}$.

Theorem 5.1 (Szőnyi and Weiner, [27]). *Assume that the point set $\mathcal{H}$ in $\mathrm{PG}(2,q)$, $16<q$ even, has δ odd-secants, where $\delta < (\lfloor\sqrt{q}\rfloor+1)(q+1-\lfloor\sqrt{q}\rfloor)$. Then there exists a unique set $\mathcal{H}'$ of even type, such that $|\mathcal{H}\Delta\mathcal{H}'| = \left\lceil \frac{\delta}{q+1} \right\rceil$.*

As a corollary of the above result, Szőnyi and Weiner gave a lower bound on the size of those point sets of $\mathrm{PG}(2,q)$, $16<q$ even, which do not have tangents but have at least one odd-secant, see [27]. In this section we prove a similar lower bound on the size of non-oval semiovals.

Lemma 5.2. *Let $\mathcal{S}$ be a semioval in Π_q, that is, a projective plane of order q. If $|\mathcal{S}| = q+1+\epsilon$, then $\mathcal{S}$ has at most $|\mathcal{S}|(1+\epsilon/3)$ odd-secants.*

Proof. Take $P \in \mathcal{S}$, then there passes exactly one tangent and there pass at most ϵ other odd-secants of $\mathcal{S}$ through P. In this way the non-tangent odd-secants have been counted at least three times. ■

Corollary 5.3. *If $\mathcal{S}$ is a semioval in $\mathrm{PG}(2,q)$, $16<q$ even, and $|\mathcal{S}| \leqslant q+3\lfloor\sqrt{q}\rfloor-11$, then $\mathcal{S}$ is an oval.*

Proof. If δ denotes the number of odd-secants of $\mathcal{S}$, then Lemma 5.2 yields:

$$\delta \leqslant (q+3\lfloor\sqrt{q}\rfloor-11)(\lfloor\sqrt{q}\rfloor-3) < (\lfloor\sqrt{q}\rfloor+1)(q-\lfloor\sqrt{q}\rfloor+1).$$

By Theorem 5.1 we can construct a set of even type $\mathcal{H}$ from $\mathcal{S}$ by modifying (add to $\mathcal{S}$ or delete from $\mathcal{S}$) $\left\lceil \frac{\delta}{q+1} \right\rceil \leqslant \lfloor\sqrt{q}\rfloor+1$ points of $\mathrm{PG}(2,q)$.

If $P \in \mathcal{S}$ is a modified (and hence deleted) point, then the number of lines through P which are not tangents to $\mathcal{S}$ and do not contain modified points is at least $q-\left(\left\lceil \frac{\delta}{q+1} \right\rceil - 1\right)$. These lines are even-secants of $\mathcal{H}$ and hence they are non-tangent odd-secants of $\mathcal{S}$. It follows that the size of $\mathcal{S}$ is at least $1 + 2(q - \lfloor\sqrt{q}\rfloor)$, a contradiction.

Thus each of the modified points has been added. Suppose $|\mathcal{S}| > q + 1$. As there is a tangent to $\mathcal{S}$ at each point of $\mathcal{S}$, we have $2 \leqslant \left\lceil \frac{\delta}{q+1} \right\rceil$. Let A and B be two modified (and hence added) points. If the line AB contains another added point C, then through one of the points A, B, C there pass at most $(|\mathcal{S}| - 1)/3 + 1$ tangents to $\mathcal{S}$. If AB does not contain further added points, then AB cannot be a tangent to $\mathcal{S}$ and hence through one of the points A, B there pass at most $|\mathcal{S}|/2$ tangents to $\mathcal{S}$. Let A be an added point through which there pass at most $|\mathcal{S}|/2$ tangents to $\mathcal{S}$ and denote the number of these tangents by τ. Through A there pass at least $q + 1 - \tau - \left(\left\lceil \frac{\delta}{q+1} \right\rceil - 1\right)$ lines meeting $\mathcal{S}$ in at least two points. Thus from $\tau \leqslant |\mathcal{S}|/2$ and from the assumption on the size of $\mathcal{S}$ we get

$$q+3\lfloor\sqrt{q}\rfloor-11 \geqslant \tau+2(q+1-\tau-\lfloor\sqrt{q}\rfloor) \geqslant 2(q-\lfloor\sqrt{q}\rfloor+1)-(q+3\lfloor\sqrt{q}\rfloor-12)/2.$$

After rearranging we obtain $0 \geqslant q - 13\lfloor\sqrt{q}\rfloor + 38$, which is a contradiction. It follows that $|\mathcal{S}| \leqslant q + 1$, but also $|\mathcal{S}| \geqslant q + 1$ and $\mathcal{S}$ is an oval in the case of equality. ■

6 Point sets with few odd-secants in $\mathrm{PG}(2, q)$, q odd

Some combinatorial results of this section hold in every finite projective plane. As before, by Π_q we denote an arbitrary projective plane of order q.

Definition 6.1. *Fix a point set $\mathcal{S} \subseteq \Pi_q$. For a positive integer i and a point $P \in \mathcal{S}$ we denote by $t_i(P)$ the number of i-secants of $\mathcal{S}$ through P. The weight of P, in notation $w(P)$, is defined as follows.*

$$w(P) := \sum_{i \text{ odd}} t_i(P)/i.$$

For a subset $\mathcal{P} \subseteq \mathcal{S}$, let $w(\mathcal{P}) = \sum_{P\in\mathcal{P}} w(P)$. Suppose that $w(P)$ is known for $P \in \{P_1, P_2, \ldots, P_m\} \subseteq \mathcal{S} \cap \ell$, where ℓ is a line meeting $\mathcal{S}$ in at least m points. Then the type of ℓ is

$$[w(P_1), w(P_2), \ldots, w(P_m)].$$

Suppose that the value of $t_i(P)$ is known for a point $P \in \mathcal{S}$ and for $1 \leqslant i \leqslant q + 1$. Let $\{a_1, a_2, \ldots, a_k\} = \{i \colon t_i(P) \neq 0\}$, then the type of P is

$$[a_{1\, t_{a_1}(P)}, a_{2\, t_{a_2}(P)}, \ldots, a_{k\, t_{a_k}(P)}].$$

Example 6.2 (Balister et al. [1])**.** *Let $\mathcal{S} = \mathcal{C} \cup \{P\}$, where $\mathcal{C}$ is a conic of* $\mathrm{PG}(2,q)$*, q odd, and $P \notin \mathcal{C}$ is an external point of $\mathcal{C}$, that is, a point contained in two tangents to $\mathcal{C}$. Then the type of P is $[1_{(q-1)/2}, 2_2, 3_{(q-1)/2}]$ and $w(P) = (q-1)/2 + (q-1)/6$. If T_1 and T_2 are the points of $\mathcal{C}$ contained in the tangents to $\mathcal{C}$ at P, then the type of T_i is $[2_{q+1}]$ and $w(T_i) = 0$ for $i = 1, 2$. Each point of $\mathcal{C}\backslash\{T_1, T_2\}$ has type $[1_1, 2_{q-1}, 3_1]$ and weight $4/3$. The number of odd-secants of $\mathcal{S}$ is $2q - 2$.*

Theorem 6.3 (Balister et al. [1, Theorem 6])**.** *The minimal number of odd-secants of a $(q+2)$-set in* $\mathrm{PG}(2,q)$*, q odd, is $2q-2$ when $q \leqslant 13$. For $q \geqslant 7$, it is at least $3(q+1)/2$.*

Conjecture 6.4 (Balister et al. [1, Conjecture 11])**.** *The minimal number of odd-secants of a $(q+2)$-set in* $\mathrm{PG}(2,q)$*, q odd, is $2q-2$.*

The following propositions are straightforward.

Proposition 6.5. *The number of odd-secants of $\mathcal{S}$ is $w(\mathcal{S}) = \sum_{P\in\mathcal{S}} w(P)$.* ■

Proposition 6.6. *Let $\mathcal{S}$ be a $(q+2)$-set in Π_q and let P be a point of $\mathcal{S}$. The smallest possible weights of P are as follows:*

- *$w(P) = 0$ if and only if the type of P is $[2_{q+1}]$,*
- *$w(P) = 4/3$ if and only if the type of P is $[1_1, 2_{q-1}, 3_1]$,*
- *$w(P) = 2$ if and only if the type of P is $[1_2, 2_{q-2}, 4_1]$,*
- *$w(P) = 8/3$ if and only if the type of P is $[1_2, 2_{q-3}, 3_2]$,*
- *$w(P) = 16/5$ if and only if the type of P is $[1_3, 2_{q-2}, 5_1]$,*
- *$w(P) = 10/3$ if and only if the type of P is $[1_3, 2_{q-3}, 3_1, 4_1]$.* ■

Proposition 6.7. *Let $\mathcal{S}$ be a point set of size $q+2$ in Π_q and let P be a point of $\mathcal{S}$.*

1. *If P is contained in a k-secant, then $w(P) \geqslant k-2$,*
2. *if P is contained in at least k trisecants, then $w(P) \geqslant \frac{4}{3}k$.*

Proof. In part 1, the number of tangents to $\mathcal{S}$ at P is at least $q-(q+2-k) = k-2$. In part 2, P is incident with at least $q+1-k-(q+2-(2k+1)) = k$ tangents to $\mathcal{S}$, thus $w(P) \geqslant k/3 + k$. ■

Theorem 6.8 (Bichara and Korchmáros [5, Theorem 1])**.** *Let $\mathcal{S}$ be a point set of size $q+2$ in $\mathrm{PG}(2,q)$. If q is odd, then $\mathcal{S}$ contains at most two points with weight 0, that is, points of type $[2_{q+1}]$.*

Lemma 6.9. *Let $\mathcal{S}$ be a point set of size $q+k$ in $\mathrm{PG}(2,q)$ for some $k \geqslant 3$. Suppose that ℓ_1 is a k-secant of $\mathcal{S}$ meeting $\mathcal{S}$ only in points of type $[2_q, k_1]$. Then the k-secants of $\mathcal{S}$ containing a point of type $[2_q, k_1]$ are concurrent.*

Proof. Let ℓ_2, ℓ_3 be two k-secants of $\mathcal{S}$ with the given property and let $R_i \in \ell_i \cap \mathcal{S}$ be a point of type $[2_q, k_1]$ for $i = 2, 3$. It is easy to see that $\mathcal{B} := \ell \Delta \mathcal{S}$ is a blocking set of Rédei type and R_2, R_3 are not incident with any bisecant of $\mathcal{B}$. It follows from Theorem 2.3 part 2 that $\ell_2 \cap \ell_3 \in \ell_1$. ■

Definition 6.10. *A* $(q+t,t)$-arc of type $(0,2,t)$ *is a point set $\mathcal{T}$ of size $(q+t)$ in $\mathrm{PG}(2,q)$ such that each line meets $\mathcal{T}$ in 0,2 or t points. In honor of Korchmáros and Mazzocca such point sets are also called* KM-arcs *in the literature.*

Let $\mathcal{T}$ be a $(q+t,t)$-arc of type $(0,2,t)$. It is easy to see that for $t > 2$ there is a unique t-secant through each point of $\mathcal{T}$. It can be proved that $2 \leqslant t < q$ implies q even, see [22] by Korchmáros and Mazzocca. As the points of $\mathcal{T}$ are of type $[2_q, t_1]$, the following theorem by Gács and Weiner also follows from Lemma 6.9. For recent results on KM-arcs we refer the reader to [13].

Theorem 6.11 (Gács and Weiner [16, Theorem 2.5])**.** *Let $\mathcal{T}$ be a $(q+t,t)$-arc of type $(0,2,t)$ in $\mathrm{PG}(2,q)$. If $t > 2$, then the t-secants of $\mathcal{T}$ pass through a unique point.* ■

The proof of our next result is based on the counting technique of Segre. A *dual arc* is a set of lines such that no three of them are concurrent.

Theorem 6.12. *Let $\mathcal{S}$ be a point set of size $q+k$ in $\mathrm{PG}(2,q)$, q odd.*

1. *If $k = 1$, then the tangents to $\mathcal{S}$ at points of type $[1_1, 2_q]$ form a dual arc.*

2. *If $k = 2$, then there are at most two points of type $[2_{q+1}]$.*

3. *If $k \geqslant 3$, then the k-secants of $\mathcal{S}$ containing a point of type $[2_q, k_1]$ form a dual arc.*

Proof. Suppose the contrary. If $k = 1$, then let A, B and C be points of type $[1_1, 2_q]$ such that the tangents through these points pass through a common point D. If $k = 2$, then let A, B and C be three points of type $[2_{q+1}]$ and take a point $D \notin (\mathcal{S} \cup AB \cup BC \cup CA)$. If $k \geqslant 3$, then let A, B and C be points of type $[2_q, k_1]$ such that the k-secants through these points pass through a common point $D \notin (AB \cup BC \cup CA)$. In all cases, A, B, C and D are in general position, thus we may assume $A = (\infty)$, $B = (0, 0)$, $C = (0)$ and $D = (1, 1)$. Let $\mathcal{S}' = \mathcal{S} \backslash \{A, B, C\}$. Note that AB, BC and CA are bisecants of $\mathcal{S}$ and CA is the line at infinity, thus $\mathcal{S}'$ is a set of $q + k - 3$ affine points, say $\mathcal{S}' = \{(a_i, b_i)\}_{i=1}^{q+k-3}$. For $i \in \{1, 2, \ldots, q + k - 3\}$ we have the following.

- The line joining (a_i, b_i) and A meets BC in $(a_i, 0)$,
- the line joining (a_i, b_i) and B meets AC in (b_i/a_i),
- the line joining (a_i, b_i) and C meets AB in $(0, b_i)$.

The lines AD, BD and CD meet $\mathcal{S}'$ in $k - 1$ points. The lines AP for $P \in \mathcal{S}' \backslash AD$ meet $\mathcal{S}'$ in a unique point. Since the first coordinate of the points of $AD \cap \mathcal{S}'$ is 1, it follows that $\{a_i\}_{i=1}^{q+k-3}$ is a multiset containing each element of $\mathrm{GF}(q) \backslash \{0, 1\}$ once, and containing 1 $k - 1$ times. Thus $\prod_{i=1}^{q+k-3} a_i = -1$. Similarly, the lines through B yield $\prod_{i=1}^{q+k-3} b_i/a_i = -1$, and the lines through C yield $\prod_{i=1}^{q+k-3} b_i = -1$. It follows that

$$1 = (-1)(-1) = \left(\prod_{i=1}^{q+k-3} a_i\right)\left(\prod_{i=1}^{q+k-3} \frac{b_i}{a_i}\right) = \prod_{i=1}^{q+k-3} b_i = -1,$$

a contradiction for odd q. ■

The following immediate consequence of Theorem 6.12 and Lemma 6.9 will be used frequently.

Corollary 6.13. *Let $\mathcal{S}$ be a point set of size $q + k$, $k \geqslant 3$, in $\mathrm{PG}(2, q)$. If there exist three k-secants of $\mathcal{S}$, ℓ_1, ℓ_2 and ℓ_3, such that the points of $\ell_1 \cap \mathcal{S}$ are of type $[2_q, k_1]$ and both $\ell_2 \cap \mathcal{S}$ and $\ell_3 \cap \mathcal{S}$ contain at least one point of type $[2_q, k_1]$, then q is even.*

Proof. Lemma 6.9 yields $\ell_2 \cap \ell_3 \in \ell_1$, but then Theorem 6.12 implies q even. ■

For the definition of a nucleus N_i of a line ℓ_i see Proposition 4.5.

Lemma 6.14. *Let $\mathcal{S}$ be a set of $q-1+a$ points, $a \geqslant 3$, in $\mathrm{PG}(2,q)$, where q is a power of the prime p. Suppose that ℓ_1 and ℓ_2 are a-secants of $\mathcal{S}$ such that there is a unique tangent to $\mathcal{S}$ at each point of $\mathcal{S} \cap \ell_i$, for $i = 1, 2$.*

1. *Either $N_1 \in \ell_2$ and $N_2 \in \ell_1$, or*
2. *$N_1 = N_2$, $p \mid a$ and for each $R \in \mathcal{S}$ if there is a unique tangent r to $\mathcal{S}$ at R, then r passes through the common nucleus.*
3. *Let ℓ_3 be another a-secant of $\mathcal{S}$ such that there is a unique tangent to $\mathcal{S}$ at each point of $\mathcal{S} \cap \ell_3$. If q or a is odd, then $\ell_3 = N_1N_2$, thus in this case ℓ_3 is uniquely determined.*

Proof. If $\ell_1 \cap \ell_2 \in \mathcal{S}$, then $|\mathcal{S}| \geqslant 2a + q - 3$, which cannot be since $a \geqslant 3$. First assume $N_1 \neq N_2$ and suppose to the contrary $N_2 \notin \ell_1$. Then $\mathcal{B} := \{N_1\} \cup (\ell_1 \Delta \mathcal{S})$ is a blocking set of Rédei type. There is a unique bisecant of $\mathcal{B}$ at each point of $\mathcal{S} \cap \ell_2$ (the tangent to $\mathcal{S}$). This is a contradiction since these bisecants should pass through the same point of ℓ_1 (apply Theorem 2.4 part 2 with $T = \ell_1 \cap \ell_2$).

If $N_1 = N_2 =: N$, then we define $\mathcal{B}$ in the same way. Then there is no bisecant of $\mathcal{B}$ through the points of $\mathcal{B} \cap \ell_2$. Theorem 2.3 yields $p \mid a$. Take a point $R \in \mathcal{S} \backslash (\ell_1 \cup \ell_2)$ incident with a unique tangent r to $\mathcal{S}$. If $N \notin r$, then r is the unique bisecant of $\mathcal{B}$ through R, a contradiction because of Theorem 2.4 part 1.

Suppose that ℓ_3 is an a-secant with properties as in part 3. Then either $\ell_3 = N_1N_2$ and $N_3 = \ell_1 \cap \ell_2$, or $N_3 = N_1 = N_2 =: N$ and $p \mid a$. In the latter case Corollary 6.13 applied to $\mathcal{S} \cup \{N\}$ and to the lines ℓ_1, ℓ_2 and ℓ_3 yields $p = 2$. ■

Lemma 6.15. *Let $\mathcal{S}$ be a set of $q+2$ points in $\mathrm{PG}(2,q)$, q is a power of the odd prime p, and suppose that ℓ is a trisecant of $\mathcal{S}$ of type $[4/3, 4/3, 4/3]$.*

1. *If $p = 3$, then the tangents at the points of $\mathcal{S}$ with weight $4/3$ pass through N_ℓ. There is at most one other trisecant of $\mathcal{S}$ of type $[4/3]$.*
2. *If $p \neq 3$, then the trisecants of type $[4/3, 4/3]$ pass through N_ℓ. Suppose that there is another trisecant ℓ_1 of type $[4/3, 4/3, 4/3]$. Then there is at most one other trisecant of type $[4/3, 4/3]$, which is $N_\ell N_1$. If $N_\ell N_1$ is a trisecant of type $[4/3, 4/3]$, then the tangents at the points of $N_\ell N_1$ with weight $4/3$ pass through $\ell \cap \ell_1$.*

Proof. Let $\mathcal{B}$ denote the Rédei type blocking set $(\ell \Delta \mathcal{S}) \cup \{N_\ell\}$.

First we prove part 1. Take $A \in \mathcal{S}\backslash\ell$ such that $w(A) = 4/3$ and denote the tangent to $\mathcal{S}$ at A by a. If $N_\ell \notin a$, then there is a unique bisecant of $\mathcal{B}$ through A, thus Theorem 2.4 yields $p \neq 3$, a contradiction. Denote the trisecant through A by ℓ_1. If there were a trisecant ℓ_2 of type $[4/3]$ different from ℓ and ℓ_1, then Corollary 6.13 applied to $\mathcal{S} \cup \{N_\ell\}$ and to the lines ℓ, ℓ_1 and ℓ_2 would yield q even, a contradiction.

Now we prove part 2. First suppose to the contrary that there is a trisecant ℓ_2 of type $[4/3, 4/3]$ with $N_\ell \notin \ell_2$. Let $A, B \in \ell_2 \cap \mathcal{S}$ such that $w(A) = w(B) = 4/3$. Denote the tangents to $\mathcal{S}$ at these two points by a and b, respectively. We have $N_\ell \notin a$ and $N_\ell \notin b$, since otherwise we would get points not incident with any bisecant of $\mathcal{B}$, a contradiction as $p \neq 3$ (cf. Theorem 2.3). It follows that $N_\ell A$ and $N_\ell B$ are 4-secants of $\mathcal{B}$. Let $M = N_\ell A \cap \ell$. Then Theorem 2.4 part 2 (with $T = \ell \cap \ell_2$) yields that MB is also a 4-secant of $\mathcal{B}$ and hence a trisecant of $\mathcal{S}$ (we have $N_\ell \notin MB$). A contradiction, since $MB \neq \ell_2$. It follows that $N_\ell \in \ell_2$.

Let ℓ_1 be trisecant of $\mathcal{S}$ of type $[4/3, 4/3, 4/3]$ and let ℓ_2, A, B, a and b be defined as in the previous paragraph. It follows from Lemma 6.14 that $N_\ell \in \ell_1$ and $N_1 \in \ell$. It also follows from the previous paragraph that $N_1 \in \ell_2$ and $N_\ell \in \ell_2$, thus $\ell_2 = N_1 N_\ell$. Theorem 2.4 applied to $\mathcal{B}$ and to $(\ell_1 \Delta \mathcal{S}) \cup \{N_1\}$ yields that a and b pass through a unique point of ℓ and through a unique point of ℓ_1, thus they pass through $\ell \cap \ell_1$. ■

Let $\mathcal{S}$ be a set of $q + 2$ points of $\mathrm{PG}(2, q)$, q odd. Since $q + 2$ is odd, each point $P \notin \mathcal{S}$ is incident with an odd-secant of $\mathcal{S}$. It follows that the odd-secants of $\mathcal{S}$ cover the points of $\mathrm{PG}(2, q)$ except for the points of $\mathcal{S}$ with weight zero. For partial covers of $\mathrm{PG}(2, q)$ we refer the reader to [8, Proposition 1.5]. The lower bound on the size of an affine blocking set [11, 18] yields the following result. Its proof can be found in [10] at the top of page 211, as part of a more complex argument. For a proof in the dual setting see [1, Lemma 10].

Lemma 6.16 (Blokhuis and Mazzocca [10])**.** *Let $\mathcal{S}$ be a set of $q+2$ points of $\mathrm{PG}(2, q)$, q odd. If $\mathcal{S}$ has $d \in \{1, 2\}$ points with weight zero, then the number of odd-secants of $\mathcal{S}$ is at least $2q - d$.*

Theorem 6.17. *Let $\mathcal{S}$ be a point set of size $q + 2$ in $\mathrm{PG}(2, q)$, $13 < q$ odd. Then the number of odd-secants of $\mathcal{S}$ is at least $\lceil \frac{8}{5}q + \frac{12}{5} \rceil$.*

Proof. Let d denote the number of points of $\mathcal{S}$ with weight zero. Theorem 6.8 of Bichara and Korchmáros yields $d \leqslant 2$. If $d \in \{1, 2\}$, then Lemma 6.16 yields $w(\mathcal{S}) \geqslant 2q - 2$, which is at least $\lceil \frac{8}{5}q + \frac{12}{5} \rceil$ when $q \geqslant 11$. From now on we assume $d = 0$. Consider the following subsets of $\mathcal{S}$:

$$\mathcal{B} := \{P \in \mathcal{S} \colon P \text{ is contained in a trisecant of type } [4/3,4/3,4/3]\},$$

$$\mathcal{C} := \{P \in \mathcal{S} \colon w(P) \neq 4/3,\ P \text{ is contained in a trisecant of type } [4/3]\}.$$

Denote the size of $\mathcal{C}$ by m and let $\mathcal{C} = \{P_1, P_2, \ldots, P_m\}$. For $i = 1, 2, \ldots, m$, let

$$V_i = \{Q \in \mathcal{S} \colon w(Q) = 4/3 \text{ and } QP_i \text{ is a trisecant}\} \cup \{P_i\}.$$

Also, let $D_1 := V_1$ and $D_i := V_i \backslash (\cup_{j=1}^{i-1} V_j)$ for $i \in \{2, 3, \ldots, m\}$. Of course the sets $D_1, D_2, \ldots, D_m$ are disjoint and $P_i \in D_i \subseteq V_i$. The point set $\mathcal{D} := \cup_{i=1}^{m} D_i$ contains each point of $\mathcal{S} \backslash \mathcal{B}$ with weight 4/3. Note that each point of D_i has weight 4/3, except P_i. We introduce the following notion. For a point set $\mathcal{U} \subseteq \mathcal{S}$ let $\alpha(\mathcal{U})$ denote the average weight of the points in $\mathcal{U}$, that is, $\alpha(\mathcal{U}) = w(\mathcal{U})/|\mathcal{U}|$. First we prove $\alpha(D_i) \geqslant 8/5$ for $i = 1, 2, \ldots, m$. If $t_3(P_i) = k$ (cf. Definition 6.1), then

$$|D_i| \leqslant |V_i| \leqslant 2k + 1. \tag{5}$$

If $k = 1$, then Proposition 6.6 yields $w(P_i) \geqslant 10/3$ (since $w(P_i) \neq 4/3$), hence in this case we have

$$\alpha(D_i) \geqslant \frac{10/3 + (|D_i| - 1)4/3}{|D_i|} = 4/3 + \frac{2}{|D_i|} \geqslant 2. \tag{6}$$

If $k \geqslant 2$, then Proposition 6.7 yields $w(P_i) \geqslant 4k/3$, thus

$$\alpha(D_i) \geqslant \frac{4k/3 + (|D_i| - 1)4/3}{|D_i|} = 4/3 + \frac{(k-1)4/3}{|D_i|} \geqslant 2 - \frac{2}{2k+1} \geqslant 8/5. \tag{7}$$

We define a further subset of $\mathcal{S}$, $\mathcal{E} := \mathcal{S} \backslash (\mathcal{B} \cup \mathcal{D})$. Note that $w(\mathcal{D}) \geqslant |\mathcal{D}|\frac{8}{5}$ and $w(\mathcal{E}) \geqslant |\mathcal{E}|2$, since each point of $\mathcal{E}$ has weight at least 2 (see Porposition 6.6). The point sets $\mathcal{B}$, $\mathcal{D}$ and $\mathcal{E}$ form a partition of $\mathcal{S}$, thus $w(\mathcal{S}) = w(\mathcal{B}) + w(\mathcal{D}) + w(\mathcal{E})$. We distinguish three main cases.

1. There is no trisecant of $\mathcal{S}$ of type $[4/3, 4/3, 4/3]$. Then we obtain $w(\mathcal{S}) \geqslant (q+2)\frac{8}{5}$.

2. There is at least one trisecant of $\mathcal{S}$ of type $[4/3, 4/3, 4/3]$ and $p \neq 3$. Denote the number of trisecants of $\mathcal{S}$ of type $[4/3, 4/3, 4/3]$ by s. Lemma 6.15 yields $s \leqslant 3$. If $s = 1$, then $w(s) \geqslant 3\frac{4}{3} + (q-1)\frac{8}{5} = q\frac{8}{5} + \frac{12}{5}$. If $s = 2$, then according to Lemma 6.15 there is at most one other trisecant of type $[4/3, 4/3]$. Thus in (5) we have $|D_i| \leqslant |V_i| \leqslant k + 2$,

where $k = t_3(P_i)$. If $k = 1$, then similarly to (6) we obtain $\alpha(D_i) \geqslant 2$. If $k \geqslant 2$, then similarly to (7) we obtain $\alpha(D_i) \geqslant \frac{5}{3}$. It follows that $w(\mathcal{S}) \geqslant 6\frac{4}{3} + (q-4)\frac{5}{3} = q\frac{5}{3} + \frac{4}{3}$. If $s = 3$, then according to Lemma 6.15 there is no other trisecant of type $[4/3, 4/3]$. Thus in (5) we have $|D_i| \leqslant |V_i| \leqslant k+1$. If $k = 1$, then similarly to (6) we obtain $\alpha(D_i) \geqslant \frac{7}{3}$, if $k \geqslant 2$, then similarly to (7) we obtain $\alpha(D_i) \geqslant \frac{16}{9}$. It follows that $w(\mathcal{S}) \geqslant 9\frac{4}{3} + (q-7)\frac{16}{9} = q\frac{16}{9} - \frac{4}{9}$.

3. There is at least one trisecant ℓ of $\mathcal{S}$ of type $[4/3, 4/3, 4/3]$ and $p = 3$. It follows from Lemma 6.15 that the number g of further trisecants of type $[4/3]$ is at most one. First suppose $g = 0$. As $\mathcal{D}$ is empty, we obtain $w(\mathcal{S}) \geqslant 3\frac{4}{3} + (q-1)2 \geqslant 2q + 2$. If $g = 1$, then let $r \neq \ell$ be the other trisecant of $\mathcal{S}$ of type $[4/3]$. Let $t \in \{1, 2, 3\}$ be the number of points with weight $4/3$ in $r \cap \mathcal{S}$. It follows that $w(\mathcal{S}) \geqslant (3+t)\frac{4}{3} + (3-t)\frac{8}{3} + (q-4)2 \geqslant 6\frac{4}{3} + (q-4)2 = 2q$. ∎

For a line set $\mathcal{L}$ of $\mathrm{AG}(2, q)$, q odd, denote by $\tilde{w}(\mathcal{L})$ the set of affine points contained in an odd number of lines of $\mathcal{L}$. [28, Theorem 3.2] by Vandendriessche classifies those line sets $\mathcal{L}$ of $\mathrm{AG}(2, q)$ for which $|\mathcal{L}| + \tilde{w}(\mathcal{L}) \leqslant 2q$, except for one open case ([28, Open Problem 3.3]), which we recall here. For applications in coding theory we refer the reader to the Introduction of the paper of Vandendriessche and the references there.

Example 6.18 (Vandendriessche [28, Example 3.1 (i)])**.** *$\mathcal{L}$ is a set of $q+k$ lines in $\mathrm{AG}(2, q)$, q odd, with the following properties. There is an m-set $\mathcal{S} \subset \ell_\infty$ with $4 \leqslant m \leqslant q-1$ and an odd positive integer k such that exactly k lines of $\mathcal{L}$ pass through each point of $\mathcal{S}$ and $\tilde{w}(\mathcal{L}) = q - k$.*

Proposition 6.19. *Example 6.18 cannot exist.*

Proof. The dual of the line set $\mathcal{L}$ in Example 6.18 is a point set $\mathcal{B}$ of size $q+k$ in $\mathrm{PG}(2, q)$, such that there is a point $O \notin \mathcal{B}$ (corresponding to ℓ_∞), with the properties that through O there pass m k-secants of $\mathcal{B}$, $\ell_1, \ell_2, \ldots, \ell_m$, and the number of odd-secants of $\mathcal{B}$ not containing O is $q - k$ (q, m and k are as in Example 6.18).

As $q + k$ is even and k is odd, it follows for $i \in \{1, 2, \ldots, m\}$ and for any $R \in \ell_i \backslash (\mathcal{B} \cup \{O\})$ that through R there passes at least one odd-secant of $\mathcal{B}$, which is different from ℓ_i. As the number of odd-secants of $\mathcal{B}$ not containing O is $q - k$, and $|\ell_i \backslash (\mathcal{B} \cup \{O\})| = q - k$, it follows that there is a unique odd-secant of $\mathcal{B}$ through each point of $\mathcal{B} \cap \ell_i$, namely ℓ_i. But $|\mathcal{B} \backslash \ell_i| = q$, thus lines not containing O and meeting ℓ_i in $\mathcal{B}$ are bisecants of $\mathcal{B}$ (otherwise we would get tangents to $\mathcal{B}$ not containing O at some point of $\ell_i \cap \mathcal{B}$). Then for $i \in \{1, 2, \ldots, m\}$ the points of $\mathcal{B} \cap \ell_i$ are of type $[2_q, k_1]$. As $m \geqslant 3$ and the lines $\ell_1, \ldots, \ell_m$ are concurrent, Theorem 6.12 yields a contradiction for odd q. ■

Remark 6.20. *Together with other ideas, our method yields lower bounds on number of odd-secants of* $(q+3)$*-sets and* $(q+4)$*-sets as well. We will present these results elsewhere.*

Acknowledgement. The author is grateful to the referees for their useful comments, in particular for the insight that a previous version of Theorem 4.12 can be improved.

References

[1] P. Balister, B. Bollobás, Z. Füredi and J. Thompson, *Minimal Symmetric Differences of Lines in Projective Planes*, J. Combin. Des. 22(10) (2014), 435–451.

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

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

[4] D. Bartoli, *On the Structure of Semiovals of Small Size*, J. Combin. Des. 22(12) (2014), 525-536.

[5] A. Bichara and G. Korchmáros, *Note on* $(q+2)$*-sets in a Galois plane of order* q, Ann. Discrete Math. 14 (1980), 117–121.

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

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

[8] A. Blokhuis, A.E. Brouwer and T. Szőnyi, *Covering all points except one*, J. Algebraic Combin. 32 (2010), 59–66.

[9] A. Blokhuis and A.A. Bruen, *The minimal number of lines intersected by a set of* $q+2$ *points, blocking sets and intersecting circles*, J. Combin. Theory Ser. A 50 (1989), 308-315.

[10] A. Blokhuis and F. Mazzocca, *The finite field Kakeya problem*, Building Bridges 205–218, Bolyai Soc. Math. Stud. 19, Springer, Berlin, 2008.

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

[12] B. Csajbók, T. Héger and Gy. Kiss, *Semiarcs with a long secant in* $\mathrm{PG}(2,q)$, Innov. Incidence Geom. 14 (2015), 1–26.

[13] M. De Boeck and G. Van de Voorde, *A linear set view on KM-arcs*, to appear in J. Algebraic Combin., DOI 10.1007/s10801-015-0661-7

[14] R.J. Evans, J. Greene, H. Niederreiter, *Linearized polynomials and permutation polynomials of finite fields*, Michigan Math. J. 39 (1992), 405–413.

[15] A. Gács, *On regular semiovals in* $\mathrm{PG}(2,q)$, J. Algebraic Combin. 23 (2006), 71–77.

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

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

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

[19] Gy. Kiss, *A survey on semiovals*, Contrib. Discrete Math. 3 (2008), 81–95.

[20] Gy. Kiss, S. Marcugini and F. Pambianco, *On the spectrum of the sizes of semiovals in* $\mathrm{PG}(2,q)$*, q odd*, Discrete Math. 310 (2010), 3188–3193.

[21] Gy. Kiss and J. Ruff, *Notes on Small Semiovals*, Annales Univ. Sci. Budapest 47 (2004), 143–151.

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

[23] P. Lisonek, Computer-assisted Studies in Algebraic Combinatorics, Ph.D. Thesis, RISC, J. Kepler University Linz, 1994.

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

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

[26] T. Szőnyi, *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.

[27] T. Szőnyi and Zs. Weiner, *On the stability of the sets of even type*, Adv. Math. 267 (2014), 381-394.

[28] P. Vandendriessche, *On small line sets with few odd-points*, Des. Codes Cryptogr. 75 (2015), 453–463.

Bence Csajbók
Dipartimento di Tecnica e Gestione dei Sistemi Industriali,
Università di Padova,
Stradella S. Nicola, 3, I-36100 Vicenza, Italy
and
MTA–ELTE Geometric and Algebraic Combinatorics Research Group,
Eötvös Loránd University,
1117 Budapest, Pázmány Péter Sétány 1/C, Hungary,
e-mail: csajbok.bence@gmail.com