Contributions to Discrete Mathematics

Volume 3, Number 1, Pages 81–95
ISSN 1715-0868

A SURVEY ON SEMIOVALS

GYÖRGY KISS

Dedicated to the centenary of the birth of Ferenc Kárteszi (1907–1989).

Abstract. A *semioval* in a finite projective plane is a non-empty pointset $\mathcal{S}$ with the property that for every point in $\mathcal{S}$ there exists a unique line t_P such that $S \cap t_P = \{P\}$. This line is called the *tangent* to $\mathcal{S}$ at P.

Semiovals arise in several parts of finite geometries: as absolute points of a polarity (ovals, unitals), as special minimal blocking sets (vertexless triangle), in connection with cryptography (determining sets). We survey the results on semiovals and give some new proofs.

1. The beginning, semi quadratic sets and semi-ovoids

Semiovals first appeared as special examples of *semi-quadratic sets.* Let Π be a projective space and $\mathcal{Q} = (\mathcal{P}, \mathcal{L})$ be a pair consisting of a set $\mathcal{P}$ of points of Π, and a set $\mathcal{L}$ of lines of Π. A *tangent* to $\mathcal{Q}$ at $P \in \mathcal{P}$ is a line $\ell \in \mathcal{L}$ such that P is on ℓ, and either $\ell \cap \mathcal{P} = \{P\}$, or $\ell \in \mathcal{L}$. $\mathcal{Q}$ is called semi quadratic set (SQS), if every point on a line of $\mathcal{L}$ belongs to $\mathcal{P}$, and for all $P \in \mathcal{P}$ the union $\mathcal{T}_P$ of all tangents to $\mathcal{Q}$ at P is either a hyperplane or the whole space Π. A lot of attempts were made to classify all SQS, but the problem is still open in general. For the known results about SQS we refer to [8] and [20].

An SQS $\mathcal{Q} = (\mathcal{P}, \mathcal{L})$ is called a *semi-ovoid* (or *semioval* if $\dim \Pi = 2$), if $\mathcal{L} = \varnothing$ and $\mathcal{P}$ contains at least 2 points. The complete characterization of semi-ovoids was given by J. Thas [32]. Using elementary double counting arguments, he proved the following results.

Theorem 1.1.

- *The only semi-ovoids of $PG(3, q)$ are the ovoids (set of $q^2 + 1$ points, no three of them are collinear).*
- *In $PG(n, q)$, $n > 3$, there are no semi-ovoids.*

2000 *Mathematics Subject Classification.* Primary 51E20. Secondary 51E21.

Key words and phrases. Semi-quadratic set, polarity, blocking set.

The research was supported by the Hungarian National Foundation for Scientific Research Grant No. NK 67867, Slovenian-Hungarian Intergovernmental Scientific and Technological Cooperation Project Grant No. SLO-9/05, and Hungarian National Office of Research and Technology within the framework of the "Öveges József" programme.

In the planar case the situation is much more complicated. It is easy to see, that the following simpler definition of semiovals is equivalent to the previously given one.

Definition 1.2. *Let Π_q be a projective plane of order q. A semioval in Π_q is a non-empty pointset $\mathcal{S}$ with the property that for every point in $\mathcal{S}$ there exists a unique line t_P such that $S \cap t_P = \{P\}$. This line is called the tangent to $\mathcal{S}$ at P.*

Throughout this paper Π_q will denote an arbitrary projective plane of order q, while $\mathrm{PG}(2,q)$ will denote the Desarguesian projective plane of order q. $\mathcal{S}$ will always denote a semioval, and for a point $P \in \mathcal{S}$, t_P will denote the tangent line to $\mathcal{S}$ at P.

The classical examples of semiovals arise from polarities (ovals and unitals). These objects are the smallest and the largest semiovals, proved independently by Hubaut [18] and J. Thas [32].

Theorem 1.3. *Let $\mathcal{S}$ be a semioval in a projective plane of order q. Then*

$$q + 1 \leq |\mathcal{S}| \leq q\sqrt{q} + 1.$$

The two extremes are also characterized, equality holds in Theorem 1.3 if and only if $\mathcal{S}$ is an oval or a unital. Each line of Π_q intersects an oval in 0, 1 or 2 points, while it intersects a unital in 0, 1 or $\sqrt{q}+1$ points. This extra property leads us to the subject of the next section.

2. Regular semiovals

The notion of regular semioval was introduced by de Finis [10] in the following way.

Definition 2.1. *Let $\mathcal{S}$ be a semioval in Π_q. If all nontangent lines intersect $\mathcal{S}$ in either 0 or a constant number a of points, then $\mathcal{S}$ is called regular semioval with character a.*

In the same paper he calculated some possible parameters for these objects, but he was not able to give any new examples. The investigation of regular semiovals was continued by Blokhuis and Szőnyi [7]. They proved the following results.

Theorem 2.2. *Let $\mathcal{S}$ be a regular semioval with character a in Π_q. Then $\mathcal{S}$ is an oval (thus $a = 2$), or a divides $q-1$ and the points not on $\mathcal{S}$ are on 0 or on a tangents.*

A consequence of this theorem is that the tangents of $\mathcal{S}$ form a regular semioval on the dual plane of Π_q. (This was proved by de Finis, too.)

Theorem 2.3. *Let $\mathcal{S}$ be a regular semioval with character a in $PG(2,q)$. Then there are two possibilities:*

(1) *$\mathcal{S}$ is a unital (thus $a = \sqrt{q}+1$);*

(2) $a-1$ *and* q *are coprimes, and the tangents at collinear points of* $\mathcal{S}$ *are concurrent.*

This theorem implies that with every a-secant there is associated a point, namely the point of intersection of the tangents at the points of the a-secant, and also to every tangent there is associated a point, namely the point of the semioval. The obvious next step would be to extend this correspondence to a polarity of $\mathrm{PG}(2,q)$, which then would imply that the regular semiovals are the ovals and the unitals. Blokhuis and Szőnyi conjectured that this is possible, but they were not able to prove it.

Let us remark, that the absoute points of a polarity always form a regular semioval in $\mathrm{PG}(2,q)$, but the situation is different in translation planes. Ganley [15] gave an example of a class of commutative semifield planes of order q with a polarity having $q^{5/4}$ absolute points. The semiovals formed by these points are not regular ones.

The longstanding regular semioval conjecture in the Desarguesian planes was finally proved by Gács [15].

Theorem 2.4. *Let* $\mathcal{S}$ *be a regular semioval in* $PG(2,q)$*. Then* $\mathcal{S}$ *is either an oval or a unital.*

Using the result of Blokhuis and Szőnyi [7], that the a-secants of a possible counterexample form a regular semioval in the dual plane, and a Segre-type trick due to Thas [33], he proved that the points on an a-secant form a set projectively equivalent to the a^{th} roots of unity. After this, one easily proves that there are certain transformations of the projective line leaving the a^{th} roots of unity invariant. Since these transformations can be classified, this gives enough information to have a contradiction.

3. Blocking semiovals

The first examples of semiovals other than ovals or unitals were the vertexless triangles. These objects first appeared as minimal blocking sets. A *blocking set* in a projective plane is a set of points which meets every line but does not contain any line. A blocking set is said to be *minimal* when no proper subset of it is a blocking set. A semioval $\mathcal{S}$ is called *blocking semioval*, if it is a blocking set. A blocking semioval is a minimal blocking set, because at each point there is a tangent line. Minimal blocking sets are one of the most studied objects in finite planes, for a survey on blocking sets we refer to [29]. The investigation of blocking semiovals was originally motivated by Batten [3]. She constructed a message sending scenario which uses determining sets. Blocking semiovals are examples of determining sets in projective planes.

The first examples of blocking semiovals other than the vertexless triangles and unitals, were found by computer search [3]. These examples come from subgroups of a Singer group of $\mathrm{PG}(2,q)$, and they have an extra property: there are only a few intersection numbers with the lines of the plane.

A set $\mathcal{A}$ of points in a plane Π_q is of type $(i_1, i_2, \ldots, i_k)$ if each line of Π_q meets $\mathcal{A}$ in i_j points for some j, and for each i_j some line meets $\mathcal{A}$ in exactly i_j points. The numbers i_j are called the intersection numbers of $\mathcal{A}$. If a semioval has only two intersection numbers, one of these must be 1, hence the semioval is a set of type $(1, k)$. These sets were characterized by Tallini Scafati [30, 31], there are only two classes, unitals and Baer subplanes. A Baer subplane has $q - \sqrt{q}$ tangent lines at each point, so it is not a semioval. Hence we have the following theorem.

Theorem 3.1. *The only semiovals with two intersection numbers are unitals.*

Blocking semiovals with three intersection numbers were studied by Batten and Dover [2]. They gave arithmetic conditions on blocking semiovals of type $(1, m+1, n+1)$, and they also exhibited families of possible parameters. Their main result is the following theorem.

Theorem 3.2. *Let $q > 4$ be a square prime power, and let Π_q be a projective plane of order q. A blocking semioval of type $(1, \sqrt{q} - 1 - \lambda, \sqrt{q} + 1)$ and size $(q + \sqrt{q} + 1)(\sqrt{q} - 1 - \lambda)$ is arithmetically feasible in Π_q if and only if $\lambda(q + \sqrt{q})/(\lambda + 2)$ is an integer with $0 \leq \lambda \leq \sqrt{q} - 3$.*

In $\mathrm{PG}(2, q)$ for $q \leq 1024$ they found only one blocking semioval with three intersection numbers other than the vertexless triangle. This is a cyclic semioval in $\mathrm{PG}(2, 7)$. If σ is a Singer cycle of the plane, then each point orbit of σ^3 is a blocking semioval of type $(1, 3, 4)$.

They also proved nonexistence results. In this direction their main theorem is the following.

Theorem 3.3. *Let Π_q be a projective plane of order $q \neq 7$. If $q^2 + q + 1 = p$ or $q^2 + q + 1 = 3p$, p prime, then each blocking semioval of type $(1, m, n)$ in Π_q is a vertexless triangle.*

It is well-known, that a blocking set of a projective plane of order q contains at least $q + \sqrt{q} + 1$ points. This lower bound can never be met by a blocking semioval, because any blocking set of size $q + \sqrt{q} + 1$ must be a Baer subplane. Much better lower bounds for the size of a blocking semioval were proved by Dover [12].

Theorem 3.4. *Let Π_q be a projective plane of order $q \geq 7$, and let $\mathcal{S}$ be a blocking semioval in Π_q. Then $|\mathcal{S}| \geq 2q + 2$.*

If a blocking semioval contains a large collinear subset, then the following sharper bound is valid.

Theorem 3.5. *Let Π_q be a projective plane of order $q \geq 3$, and let $\mathcal{S}$ be a blocking semioval in Π_q. If $\mathcal{S}$ has a $(q-k)$-secant, $1 \leq k \leq q-1$, then*

$$|\mathcal{S}| \geq \left\lceil \frac{3k+4}{k+2} q - k \right\rceil.$$

On the other hand, the size of the smallest known blocking semioval in Π_q is approximately $3q$. Only a few examples of small blocking semiovals have been constructed so far. Ranson, Dover [24], [25] and Suetake [27] provide computational results in planes of small order. The known infinite families of small blocking semiovals are as follow:

(1) The vertexless triangle is a blocking semioval of size $3q-3$ in any plane of order q.
(2) If $q=r^e$, $r\geq 3$, r is a prime power, $e\geq 2$ and $2\leq n\leq r$, then there exist blocking semiovals of size $3q-n-2$ in $\mathrm{PG}(2,q)$.
(3) If $q=r^{e_1e_2}$, $r\geq 3$, r is a prime power, $e_1\neq 1$, $e_2\neq 1$ and $3\leq n\leq r$, then there exist blocking semiovals of size $3q-n-2$ in $\mathrm{PG}(2,q)$.
(4) If $q=r^e$, $r\geq 3$, r is a prime power and $e\geq 2$ then there exist blocking semiovals of size $3q-r-2$ in $\mathrm{PG}(2,q)$.
(5) In $\mathrm{PG}(2,q)$, q odd, five types of blocking semiovals can be constructed from the vertexless triangle by deleting some (3, 5 or 6) points, and simultaneously adding some (3,4,5 or 7) extra points. The sizes of these semiovals are $3q-n$, where $n=2,3,4$ or 5.

Families (2)–(4) were constructed by Suetake. For the detailed description of (2) and (3), see [26], for (4) see [27]. A special case of (2) was also constructed by Dover [13]. The five families of (5) were constructed by Ranson and Dover [25].

Each member of these infinite families contains at least one large collinear subset. This fact motivates the study of semiovals with large collinear subsets.

4. Semiovals with large collinear subsets

A line ℓ, or any proper subset of ℓ is not a semioval, because the number of tangent lines at each of its point is greater than 1. A semioval $\mathcal{S}$ could not contain a whole line ℓ, because if $P\in\mathcal{S}\setminus\ell$, then any line through P meets ℓ, hence there is no tangent to $\mathcal{S}$ at P. In $\mathrm{PG}(2,2)$ and $\mathrm{PG}(2,3)$ there are semiovals containing q (that is 2 or 3, respectively) collinear points. But for $q>3$ the size of the largest collinear subset in a semioval is at most $q-1$.

Theorem 4.1. *Let $\mathcal{S}$ be a semioval in Π_q, $q>3$. Then for any line ℓ the intersection $\mathcal{S}\cap\ell$ contains at most $q-1$ points.*

Proof. Suppose that $|\mathcal{S}\cap\ell|=q$. Then there is a unique point $T\in\ell\setminus\mathcal{S}$. If $P\in\mathcal{S}\setminus\ell$, then t_P must meet ℓ in T. Hence $|\mathcal{S}\setminus\ell|\leq q$, because the tangents at distinct points are distinct lines, there are $q+1$ lines through T, but one of them, ℓ, could not be a tangent line. On the other hand, if $R\in\ell\setminus\{T\}$, then there are $q+1$ lines through R, one of them is ℓ, one of them is t_R, but each of the remaining $q-1$ contains at least one point of $\mathcal{S}\setminus\ell$, thus $|\mathcal{S}\setminus\ell|\geq q-1$.

Suppose that $|\mathcal{S}\setminus\ell|=q-1$, and let P_1 and P_2 be two distinct points in $\mathcal{S}\setminus\ell$ (they exist because $q>3$). If $P_1P_2\cap\ell=T$, then there is no tangent

line to $\mathcal{S}$ at P_1 (and at P_2). If $P_1P_2 \cap \ell = R \neq T$, then there are more than one tangent lines at R, both of these are contradictions.

If $|\mathcal{S} \setminus \ell| = q$, then let $\mathcal{S} \setminus \ell = \{P_1, P_2, \ldots, P_q\}$. Now no line of type P_iP_j meets ℓ in T, because we have already seen, that $t_{P_i} = P_iT$. Consider the $q(q-1)/2$ pairs of points $\{P_i, P_j\}$ for all $i \neq j$. Each pair corresponds to a line P_iP_j. Suppose, that $\{P_i, P_j\} \neq \{P_k, P_l\}$ and $P_iP_j \cap P_kP_l = R \in \ell \setminus \{T\}$. Then there would be more than one tangent line at R, hence the lines corresponding to distinct pairs meet $\ell \setminus \{T\}$ in distinct points. This implies

$$\frac{q(q-1)}{2} \leq q.$$

So $q \leq 3$, a contradiction. □

A longer proof of the previous theorem was given by Dover [13], who first investigated semiovals with large collinear subsets. He proved the following properties of these semiovals.

Theorem 4.2. *Let $\mathcal{S}$ be a semioval in a projective plane Π_q of order $q > 3$. Then*

(1) *$|\mathcal{S} \cap \ell| \leq q-1$ for any line ℓ of Π_q.*
(2) *If $\mathcal{S}$ has a $(q-1)$-secant, then $|\mathcal{S}| = 2q-2$, or $2q \leq |\mathcal{S}| \leq 3q-3$. If $|\mathcal{S}| = 2q-2$, then $\mathcal{S}$ consists of $q-1$ points on each of two lines which intersect in a point not in $\mathcal{S}$, while if $|\mathcal{S}| = 3q-3$, then $\mathcal{S}$ is a vertexless triangle.*
(3) *If $q > 5$ and $\mathcal{S}$ has more than one $(q-1)$-secant, then $\mathcal{S}$ can be obtained from a vertexless triangle by removing some subset of points from one side.*

If the largest collinear subset of $\mathcal{S}$ contains only all but three points of a line, then the combinatorial arguments of the proof of Theorem 4.2 do not work any more. Only one result is known in a very special case, see [14].

Theorem 4.3. *If $|\mathcal{S}| = 2q-1$ and $\mathcal{S}$ has a $(q-2)$-secant, then $q = 7$ and $\mathcal{S}$ has exactly two $(q-2)$-secants.*

If a semioval has a large secant and its size is small, then Kiss [21] proved that the tangents at the points of the large secant are concurrent. Hence these semiovals in some sense similar to regular semiovals.

Theorem 4.4. *Let $\mathcal{S}$ be a semioval in the Desarguesian plane $PG(2,q)$. If there exist integers $1 \leq t$ and $-1 \leq k$ such that $\mathcal{S}$ has a $(q-t)$-secant, $|\mathcal{S}| = 2q-t+k$, $2(t+k) < q$ and $t+4(k+1) < q$, then the tangent lines at the points of the $(q-t)$-secant are concurrent.*

The proof of the theorem is algebraic, it is based on an application of the Rédei polynomial associated to those points of $\mathcal{S}$ which do not lie on the $(q-t)$-secant. If $t = 1$, then Theorem 4.4 implies the following embedding property of small semiovals.

Corollary 4.5. *Let $\mathcal{S}$ be a semioval in the Desarguesian plane* $\mathrm{PG}(2,q)$. *If $|\mathcal{S}| < 2q + (q-9)/4$ and $\mathcal{S}$ has a $(q-1)$-secant, then $\mathcal{S}$ is a subset of a vertexless triangle.*

The following example shows that Theorem 4.4 could not be extended to semiovals of size greater than approximately $3q$.

Example 4.6. *Suppose that* $q \equiv -1 \pmod 4$. *Let us coordinatize $PG(2,q)$ in the usual way. Then the point set*

$$\begin{aligned} S = &\{(a,a,1) : 0 \neq a \in \mathrm{GF}(q)\} \\ &\cup \{(0,b,1) : b \text{ is a square in } \mathrm{GF}^*(q)\} \\ &\cup \{(c,0,1) : c \text{ is a non-square in } \mathrm{GF}^*(q)\} \\ &\cup \{(d,1,0) : d \neq 0,1,\ d \in \mathrm{GF}(q)\} \end{aligned}$$

is a semioval of size $3q-4$.

The line $X_1 = X_2$ is a $(q-1)$-secant of $\mathcal{S}$, but the tangent to $\mathcal{S}$ at the point $P_a = (a,a,1)$ has equation $X_1 = aX_3$ or $X_2 = aX_3$ according to whether a is a square or a non-square element in $\mathrm{GF}^*(q)$. Hence the tangent lines at the points of the $(q-1)$-secant are not concurrent. But the semioval $\mathcal{S}$ has got not only a $(q-1)$-secant, but a $(q-2)$-secant, too. The line $X_3 = 0$ meets $\mathcal{S}$ in $(q-2)$ points and the tangents to $\mathcal{S}$ at these points are concurrent.

There is only one more known infinite class of semiovals with $(q-2)$-secants: the vertexless triangle without three points which are collinear but do not lie on the same side of the triangle. This semioval is formed by three $(q-2)$-secants and the tangent lines at collinear points are concurrent. So it seems to be possible to characterize those semiovals which have more than one large collinear subsets. The known examples support the following conjecture.

Conjecture. *If $\mathcal{S}$ is a semioval in Π_q and there are at least two lines ℓ_1, ℓ_2 such that $|\mathcal{S} \cap \ell_i| \geq q-2$ for $i = 1,2$, then $\mathcal{S}$ is contained in the union of at most four lines.*

In the next section we collect the results about semiovals contained in the union of few lines.

5. Semiovals contained in the union of three lines

It is easy to describe those semiovals which are contained in the union of two lines. The proof of the following theorem is self-evident.

Theorem 5.1. *Let $\mathcal{S}$ be a semioval in Π_q. If $\mathcal{S}$ is contained in the union of two lines ℓ_1 and ℓ_2, then $|\mathcal{S}| = 2(q-1)$ and $\mathcal{S} = \ell_1 \cup \ell_2 \setminus \{\ell_1 \cap \ell_2, Q_1, Q_2\}$ where $Q_i \in \ell_i$ for $i = 1,2$.*

If $\mathcal{S}$ is contained in the union of three lines, then the classification is not so simple. The problem was studied by Kiss and Ruff [22] when the three lines form a triangle, and by Blokhuis, Kiss, Kovács, Malnič, Marušič and

Ruff [6] when the three lines are concurrent. All of the results of the rest of this section can be found in these two papers.

First consider the triangle case. There are much better bounds on the size of $\mathcal{S}$ than the general ones.

Theorem 5.2. *Let $\mathcal{S}$ be a semioval in a projective plane Π_q. If $\mathcal{S}$ is contained in the union of three lines then*

$$\frac{3(q-1)}{2} \leq |S| \leq 3(q-1).$$

The upper bound is a trivial consequence of Theorem 4.2, while the lower bound comes from a simple double counting. It is also easy to prove that $\mathcal{S}$ contains at most one vertex of the triangle in which $\mathcal{S}$ is contained. If $\mathcal{S}$ contains exactly one vertex, then we have the following classification for Desarguesian planes.

Theorem 5.3. *A semioval in $PG(2,q)$ which is contained in the sides of a triangle and which contains one vertex of this triangle has a $(q-2)$-secant and two $(t+1)$-secants where t is a suitable integer. This type of semiovals exists if and only if $q=4$ and $t=1$, $q=8$ and $t=4$ or $q=32$ and $t=26$.*

The proof of this theorem is quite long. It starts with the following elementary observation: since $\mathcal{S}$ contains one vertex of the triangle, it must contain a $(q-2)$-secant. After choosing a suitable system of reference, one can prove that the existence of $\mathcal{S}$ is equivalent to the existence of certain cyclic difference sets in $\mathrm{GF}^*(q)$. Calculating the parameters of this difference set we conclude that the diophantine equation $2^r = x^2 + 7$ has to have a solution. It is known that this equation has only five pairs of solution, three of them correspond to semiovals, while the other two do not.

All of the known semiovals in nondesarguesian planes which are contained in the sides of a triangle, do not contain any vertex of this triangle. So Theorem 5.3 might be true in general, but to give a simple, combinatorial proof seems to be difficult.

Now consider the case when $\mathcal{S}$ does not contain any vertex of the triangle. Then there are two classes of these semiovals.

Theorem 5.4. *If a semioval S in $PG(2,q)$ is contained in the sides of a triangle $\mathcal{T}$ and does not contain any vertex of $\mathcal{T}$, then there are two possibilities:*

(1) *$\mathcal{S}$ has two $(q-1)$-secants and a k-secant. Semiovals in this class exist for all $1 < k < q$.*
(2) *$\mathcal{S}$ has three $(q-1-d)$-secants where d is a suitable divisor of $q-1$.*

Semiovals of type (1) exist in any plane. They can be constructed by the simple expedient of deleting some points from one side of a vertexless triangle. The existence of semiovals of type (2) is nontrivial. The proof uses coordinates, and shows that such a semioval corresponds to a subgroup of $\mathrm{GF}^*(q)$.

Now consider the case of three concurrent lines. There are only two known examples which are not contained in the union of any two of these lines. One of them is trivial: an irreducible conic $\mathcal{C}$ in $\mathrm{PG}(2,5)$ has 6 points, and if B is any interior point of it, then $\mathcal{C}$ is contained in the union of the three secants passing through B. The other example is the following infinite family arising from Baer subplanes of $\mathrm{PG}(2,s^2)$.

Example 5.5. *Let $q = s^2$ and let ℓ_1, ℓ_2, ℓ_3 be three concurrent lines in $PG(2,q)$. Choose Baer sublines $\overline{\ell}_1 \subset \ell_1$, $\overline{\ell}_2 \subset \ell_2$, and $\overline{\ell}_3 \subset \ell_3$ in such a way that, for any triple of distinct $i,j,k \in \{1,2,3\}$, the Baer subplane $\mathcal{B}_{j,k} = \langle \overline{\ell}_j, \overline{\ell}_k \rangle$ meets the line ℓ_i only in the common point C. Then $\mathcal{S} = (\ell_1 \setminus \overline{\ell}_1) \cup (\ell_2 \setminus \overline{\ell}_2) \cup (\ell_3 \setminus \overline{\ell}_3)$ is a semioval which has $3(q - \sqrt{q})$ points.*

These semiovals have two extra properties:

(1) Each of the three lines whose union contains $\mathcal{S}$, meets $\mathcal{S}$ in the same number of points.
(2) Let ℓ_1, ℓ_2 and ℓ_3 be the three concurrent lines whose union contains $\mathcal{S}$, and let C be the common point of these lines. If P is any point of the set $\ell_1 \cup \ell_2 \cup \ell_3 \setminus (\mathcal{S} \cup \{C\})$, then the number of 2-secants of $\mathcal{S}$ passing through P is a constant.

Property 1 holds in general. One can prove the following theorem by simple double counting of the 2-secants of $\mathcal{S}$.

Theorem 5.6. *If a semioval $\mathcal{S}$ in Π_q, $q > 3$, is contained in the union of three concurrent lines, ℓ_1, ℓ_2 and ℓ_3, then there exists a number a for which $|\mathcal{S} \cap \ell_i| = a$ for $i = 1,2,3$.*

Applying the result of Theorem 5.6, one can show that the semiovals of Example 5.5 have the largest possible size.

Theorem 5.7. *If a semioval $\mathcal{S}$ in Π_q, $q > 3$, is contained in the union of three concurrent lines, then $|\mathcal{S}| \leq 3\lceil q - \sqrt{q} \rceil$.*

The lower bound of Theorem 5.2 can also be slightly improved in Desarguesian planes in the case of concurrent lines.

Theorem 5.8. *If a semioval $\mathcal{S}$ in $PG(2,q)$ is contained in the union of three concurrent lines then $|S| > 3(q-1)/2$ for $q > 9$.*

Perhaps Property 2 of semiovals in Example 5.5 also holds in general. Neither the proof, nor any counterexample is known. This property leads to the notion of *strong semioval.*

Definition 5.9. *Let ℓ_1, ℓ_2 and ℓ_3 be the three concurrent lines whose union contains $\mathcal{S}$. We denote by C the common point of these three lines and by $\mathcal{L}$ the union of ℓ_1, ℓ_2 and ℓ_3. And finally, we let $\mathcal{L}_i = \mathcal{S} \cap \ell_i$ $(i = 1,2,3)$. The semioval $\mathcal{S}$ is strong, if for any point $K \in \mathcal{L} \setminus (\mathcal{S} \cup \{C\})$, the number of two-secants of $\mathcal{S}$ passing through K is independent of K.*

An algebraic description of strong semiovals in $\mathrm{PG}(2,q)$ is given in [6]. A strong semioval corresponds to an ordered triple (S,T,R), where R,S and T are certain subsets of $\mathrm{GF}(q)$, satisfying the following conditions:

$$
\begin{aligned}
|S+u\cap -T| &= \begin{cases} 2a-q+1, & \text{if } u\in R,\\ k, & \text{if } u\notin R,\end{cases}\\
|T+u\cap -R| &= \begin{cases} 2a-q+1, & \text{if } u\in S,\\ k, & \text{if } u\notin S,\end{cases}\\
|R+u\cap -S| &= \begin{cases} 2a-q+1, & \text{if } u\in T,\\ k, & \text{if } u\notin T,\end{cases}
\end{aligned}
\tag{5.1}
$$

where a is the same as in Theorem 5.6, and k is the *parameter* of $\mathcal{S}$. This parameter depends on q and a, as seen below.

Proposition 5.10. *Let $\mathcal{S}$ be a strong semioval in $PG(2,q)$ with parameter k. If $\mathcal{S}$ consists of $3a$ points, then*

$$k=a-\frac{a}{q-a}.$$

The divisibility condition $q-a \mid a$ implies the following non-existence result.

Corollary 5.11. *There is no strong semioval in $PG(2,p)$ if p is an odd prime.*

Combining the algebraic description (5.1) and a classical result on group factorizations due to Rédei, a complete characterization of strong semiovals in $\mathrm{PG}(2,p^2)$, p an odd prime can be given.

Theorem 5.12. *If $\mathcal{S}$ is a strong semioval in $PG(2,p^2)$, p an odd prime, and $\mathcal{S}$ is contained in the union of lines ℓ_1,ℓ_2 and ℓ_3, then $\mathcal{L}\setminus\mathcal{S}$ can be described as the point set*

$$\big\{\,(-1,a,1),(0,b,1),(1,i,ci+f(c)) : a,b,c\in GF(p)\,\big\}\cup\big\{\,C\big\}, \tag{5.2}$$

where $C=(0,1,0)$, $i^2=\varepsilon$ for a non-square element ε of $GF(p)$, $GF(p^2)$ is the extension of $GF(p)$ by i, and finally, f is a permutation of $GF(p)$.

If a strong semioval $\mathcal{S}$ in $\mathrm{PG}(2,q)$ has less than $3(q-\sqrt{q})$ points, then some divisibility conditions can be proved using group algebras and character theory. These conditions imply some nonexistence results, see [6].

Theorem 5.13. *If $\mathcal{S}$ is a strong semioval of cardinality $|\mathcal{S}|=3(p^m-p^l)$, $m/2<l<m$, in $PG(2,q)$, $q=p^m$ odd, then*

$$(p-1)(p^{2l-m}-1)^2 \mid (p^{m-l}-1). \tag{5.3}$$

Corollary 5.14. *If $\mathcal{S}$ is a strong semioval in $PG(2,p^m)$, where p is an odd prime, and*

$$m\le\begin{cases}(p-1)^2 & \text{if } p\equiv -1 \pmod 4,\\ 2(p-1)^2 & \text{if } p\equiv 1 \pmod 4,\end{cases}$$

then $|\mathcal{S}|=3(q-\sqrt{q})$.

6. The spectrum of the sizes of semiovals

For planes of small order the complete spectrum of the sizes and the number of projectively non-isomorphic semiovals are known.

6.1. $q = 2$**.** Because of Theorem 1.1, each semioval consists of three points, and these points are not collinear, hence semiovals are ovals.

6.2. $q = 3$**.** If a semioval $\mathcal{S}$ is not an oval, then there is a line ℓ which contains three points of $\mathcal{S}$, say A, B and C. There are four lines through each of these points, one of them is the tangent, but the others must meet $\mathcal{S}$. Hence $\mathcal{S}$ contains at least two points not on ℓ. Let $D, E \in \mathcal{S} \setminus \ell$. If F is the fourth point of the line ℓ, then $t_D \cap \ell = t_E \cap \ell = F$, thus $DE \cap \ell \neq F$. Without loss of generality we may assume, that $DE \cap \ell = A$. This implies that $\mathcal{S}$ must contain a sixth point G, otherwise there would be two tangents through A. But 6 is an upper bound of the cardinality of $\mathcal{S}$ by Theorem 1.1. If $G = BD \cap CE$, then it is easy to check that the set $\{A, B, C, D, E, G\}$ is a semioval. These points form the vertices of a complete quadrilateral. Hence we proved that there are two projectively non-isomorphic classes of semiovals in $\mathrm{PG}(2, 3)$.

6.3. $q = 4$**.** The possible sizes of $\mathcal{S}$ are $5, 6, 7, 8$ and 9. It follows from Theoem 4.2, that if $|\mathcal{S}| > 5$, then $\mathcal{S}$ has at least one $(q-1)$-secant, hence $|\mathcal{S}| \neq 2q - 1 = 7$. The cases $|\mathcal{S}| = 2q - 2 = 6$ and $|\mathcal{S}| = 9 = 3q - 3$ are also characterized by the same theorem, these are a triangle with its vertices and all points on one side removed, and the vertexless triangle, respectively. If $|\mathcal{S}| = 8$, then an exhaustive computer search [13] shows that the only semiovals of this class are vertexless triangles with one point deleted.

6.4. $q > 4$**.** For $q > 4$ the situation becomes more and more complicated. Semiovals of size $2(q-1)+k$ for all $k \leq q-1$ and $k \neq 1$ can be constructed easily. If we delete any set of $q - 1 - k$ points from one side of a vertexless triangle, then the remaining points form a semioval $\mathcal{S}$ and $|\mathcal{S}| = 2(q-1)+k$. Hence the spectrum of sizes always contains $2q - 2$ and all integers in the interval $[2q, 3q-3]$. Table 1 gives the sizes of the known semiovals in $\mathrm{PG}(2, q)$ for small order planes. For $q \leq 9$, q odd, the complete spectrum of sizes was determined by exhaustive computer search, while for $q = 11$ and 13 the examples were found by a backtracking algorithm [14].
These results support the following conjecture.

Conjecture. *If a semioval $\mathcal{S}$ has less than $3(q-1)/2$ points in Π_q, then $\mathcal{S}$ is an oval.*

There is only one nonexistence result known for small semiovals. A *seminuclear set* was defined by Blokhuis and Bruen [5] as a set of $q + 2$ points in Π_q blocking $(q+2)(q+1)/2 + (q+2)/3$ lines. (This is the minimum number of lines blocked by $q+2$ points.) They proved that seminuclear sets are semiovals (although they did not call them semiovals) of size $q + 2$. A few years later Blokhuis [4] proved, that seminuclear sets exist in $\mathrm{PG}(2, q)$

q	spectrum of sizes	upper bound, $\lfloor q\sqrt{q}+1 \rfloor$
2	3	3
3	4,6	6
4	5,6,8,9	9
5	6,8,9,10,11,12	12
7	8,9,12 - 19	19
8	9,14,16 - 21	23
9	10,12 - 28	28
11	12,15,20,22 - 34	37
13	14,18,24,26 - 40	47

TABLE 1. Sizes of known semiovals

if and only if $q = 4$ or $q = 7$. He also characterized these sets, and proved the following theorem.

Theorem 6.1. *Let $\mathcal{S}$ be a semioval in $PG(2, q)$, q odd. If $|\mathcal{S}| = q + 2$, then $q = 7$ and $\mathcal{S}$ is projectively equivalent to the set of points*

$$\{(0, 1, s), (s, 0, 1), (1, s, 0) : s \text{ is a square in } \mathrm{GF}(7)\},$$

hence $\mathcal{S}$ is contained in a vertexless triangle.

His proof is based on a beautiful application of Ceva's Theorem, but quite long. Using results of Szőnyi [28] about the size of minimal blocking sets in $\mathrm{PG}(2, q)$, a short proof of the essential part of this Theorem can be given.

Proof. Suppose that $|\mathcal{S}| = q+2$ and q odd. Then each line meets $\mathcal{S}$ in $0, 1, 2$ or 3 points, and each point of $\mathcal{S}$ is on a unique 3-secant. Hence there are $(q + 2)/3$ 3-secants and so $q + 2$ is divisible by 3. If $P \notin \mathcal{S}$ is any point, then the lines through P give a partition of the points of $\mathcal{S}$. The cardinality of $\mathcal{S}$ is odd, hence the number of lines through P which meet $\mathcal{S}$ in either 1 or 3 points is odd. Thus if we consider now the dual plane, then the $q + 2$ tangents and the $(q+2)/3$ 3-secants form a blocking set $\mathcal{B}$ of size $4(q+2)/3$. If $q > 9$, then this blocking set is minimal, because otherwise it would contain a point L such that each line through L would meet in $\mathcal{B}$ some other points, too. By duality it would imply the existence of a line ℓ such that each point in $\mathcal{S} \setminus \ell$ is incident with at least 2 more lines of the set of the tangents and 3-secants of $\mathcal{S}$. Hence the cardinality of this set is at least $1 + 2(q - 2)$. But $1 + 2(q - 2) > 4(q + 2)/3$ if $q > 9$, so $\mathcal{B}$ is minimal.

For minimal blocking set of size less than $3(q + 1)/2$, Szőnyi [28] proved that if $q = p^e$, p prime, then each line of $\mathrm{PG}(2, q)$ meets the minimal blocking set in 1 modulo p points. But in our case the lines corresponding to the points of $\mathcal{S}$ meet $\mathcal{B}$ in 2 points, because each point of $\mathcal{S}$ lies on exactly one tangent to $\mathcal{S}$ and on exactly one 3-secant. 2 is not congruent to 1 modulo p, this contradiction shows that $q \leq 9$. We also have $q \equiv 1 \pmod 6$, hence the only possibility is $q = 7$. □

A possible way of constructing (not necessarily small) semiovals is to find them in the cyclic model of $\mathrm{PG}(2,q)$. But cyclic semiovals are rare objects. There are only two known examples. We have already mentioned in Section 3 the cyclic semioval of size 19 in $\mathrm{PG}(2,7)$, the other one is in $\mathrm{PG}(2,3^5)$, see [14], its size is 511, so it is not small. The following nonexistence result was also proved in [14].

Theorem 6.2. *There is no cyclic semioval in $PG(2,q)$ if $q \equiv 2 \pmod 3$.*

Large semiovals in $\mathrm{PG}(2,q)$, q odd, were constructed by Faina, Kiss, Marcugini and Pambianco [14]. Their construction is based on a method developed by Hirschfeld and Szőnyi [17] and by Baker and Ebert [1] for constructing unitals as union of conics. Let $\mathcal{P}_a$ be the conic with equation

$$\mathcal{P}_a : X_2X_3 = X_1^2 + aX_3^2.$$

Then the construction is the following.

Example 6.3. *Let $q \equiv 1 \pmod 4$. If $\{a_1, a_2, \ldots, a_k\} \subset GF(q)$ is a subset of $k \geq 2$ elements such that $a_i - a_j$ is a nonsquare for all $i \neq j$, then the sets*

$$\mathcal{S} = \bigcup_{i=1}^{k} \mathcal{P}_{a_i} \quad \text{and} \quad \mathcal{S}_1 = \bigcup_{j=1}^{k} \mathcal{P}_{a_i} \setminus \{(0,1,0)\}$$

are semiovals of size $kq+1$ and kq, respectively.

If $q = s^2$ and α is a nonsquare element in $\mathrm{GF}(q)$, then the s-element set $\{\alpha a_i : a_i \in \mathrm{GF}(s)\}$ gives semiovals of sizes $q\sqrt{q}+1$ and $q\sqrt{q}$, respectively. Using the elementary observation, that if the point $P \in \mathcal{S}$ has the property, that each line passing through P other than t_P meets $\mathcal{S}$ in at least two points, then $\mathcal{S} \setminus \{P\}$ is also a semioval, we get the following theorem.

Theorem 6.4. *Let q be an odd square and m be an integer satisfying*

$$q\frac{\sqrt{q}+1}{2} \leq m \leq q\sqrt{q}+1.$$

Then $PG(2,q)$ contains semiovals of size m.

It also follows from the construction, that any subset of $1 \leq k \leq \sqrt{q}$ conics of the set $\mathcal{S} = \bigcup_{j=1}^{\sqrt{q}} \mathcal{P}_{a_{i_j}}$ forms a semioval of size $kq+1$.

If q is an odd power of an odd prime, then the sizes of the largest known semiovals are far away from the upper bound of Theorem 1.1. The best known example also comes from Example 6.3 (see [14]).

Theorem 6.5. *Let $q \equiv 1 \pmod 4$, and let c_q be the cardinality of the largest clique in the Paley graph P_q. Then $PG(2,q)$ contains semiovals of size kq and of size $kq+1$ for all $k = 1, 2, \ldots, c_q+1$.*

The size of the largest clique in the Paley-graph is not known if q is a nonsquare. The best known lower bound is approximately $\log q/(2\log 2)$ [9].

Let us finish this survey with an open problem: Prove or disprove that the size of a semioval in a plane of non-square order is less than $cq \log q$ where c is a constant.

References

1. R. D. Baker and G. L. Ebert, *Intersection of unitals in the Desarguesian plane*, Congr. Numer. **70** (1990), 87–94.
2. L. M. Batten and J. M. Dover, *Blocking semiovals of type* $(1, m+1, n+1)$, SIAM J. Discrete Math. **14** (2001), 446–457.
3. L.M. Batten, *Determining sets*, Australas. J. Combin. **22** (2000), 167–176.
4. A. Blokhuis, *Characterization of seminuclear sets in a finite projective plane*, J. Geom. **40** (1991), 15–19.
5. A. Blokhuis and A. A. Bruen, *The minimal number of lines intersected by a set of points and intersecting circles*, J. Combin. Theory Ser. A **50** (1989), 308–315.
6. A. Blokhuis, Gy. Kiss, I. Kovács, A. Malnič, D. Marušič, and J. Ruff, *Semiovals contained in the union of three concurrent lines*, J. Comb. Designs **15** (2007), 491–501.
7. A. Blokhuis and T. Szőnyi, *Note on the structure of semiovals in finite projective planes*, Discrete Math. **106/107** (1992), 61–65.
8. F. Buekenhout, *Characterizations of semi quadrics. A survey*, Colloquio Internazionale sulle Teorie Combinatorie (Roma, 1973), Tomo I, Atti dei Convegni Lincei, no. 17, Accad. Naz. Lincei, Rome, 1976, pp. 393–421.
9. S. D. Cohen, *Clique numbers of Paley graphs*, Quaestiones Math. **11** (1988), 225–231.
10. M. de Finis, *On semiovals in projective planes*, Ars Combin. **24** (1987), no. A, 65–70.
11. A. Delandtsheer, *Finite flag-transitive semiovals*, J. Combin. Theory Ser. A **57** (1991), 60–67.
12. J. M. Dover, *A lower bound on blocking semiovals*, European J. Combin. **21** (2000), 571–577.
13. ———, *Semiovals with large collinear subsets*, J. Geom. **69** (2000), 58–67.
14. G. Faina, Gy. Kiss, S. Marcugini, and F. Pambianco, *On the spectrum of the size of semiovals in* $PG(2, q)$, *q odd*, submitted.
15. A. Gács, *On regular semiovals*, J. Algebraic Combin. **23** (2006), 71–77.
16. M. J. Ganley, *Polarities in translation planes*, Geometriae Dedicata **1** (1972), 103–116.
17. J. W. P. Hirschfeld and T. Szőnyi, *Sets in a finite plane with few intersection numbers and a distinguished point*, Discrete Math. **97** (1991), 229–242.
18. X. Hubaut, *Limitation du nombre de points d'un* (k, n)*-arc regulier d'un plan projectif fini*, Atti. Accad. Naz. Lincei Rend. **8** (1970), 490–493.
19. Ch. Jacobs, *A new blocking semioval*, Bull. Inst. Combin. Appl. **42** (2004), 19–24.
20. P. M. Johnson, *Semiquadratic sets and embedded polar spaces*, J. Geom. **64** (1999), 102–127.
21. Gy. Kiss, *Small semiovals in* $PG(2, q)$, J. Geom., to appear.
22. Gy. Kiss and J. Ruff, *Notes on small semiovals*, Annales Univ. Sci. Budapest. **47** (2004), 143–151.
23. N. Nakagawa and C. Suetake, *On blocking semiovals with an 8-secant in projective planes of order 9*, Hokkaido Math. J. **35** (2006), 437–456.
24. B. B. Ranson, *Blocking semiovals*, Master's thesis, North Dakota State University, 1999.
25. B. B. Ranson and J. M. Dover, *Blocking semiovals in* $PG(2, 7)$ *and beyond*, European J. Combin. **24** (2003), 183–193.
26. C. Suetake, *Some blocking semiovals which admit a homology group*, European J. Combin. **21** (2000), 967–972.
27. ———, *Two families of blocking semiovals*, European J. Combin. **21** (2000), 973–980.

28. T. Szőnyi, *Blocking sets in Desarguesian affine and projective planes*, **3** (1997), 187–202.
29. T. Szőnyi, A. Gács, and Zs. Weiner, *On the spectrum of minimal blocking sets in* $PG(2, q)$, J. Geom. **76** (2003), 256–281.
30. M. Tallini Scafati, $\{k, n\}$*-archi in un piano grafico finito, con particolare riguardo a quelli con due caratteri (note i)*, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **8** (1966), no. 40, 812–818.
31. ———, $\{k, n\}$*-archi in un piano grafico finito, con particolare riguardo a quelli con due caratteri (note ii)*, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **8** (1966), no. 40, 1020–1025.
32. J. A. Thas, *On semi ovals and semi ovoids*, Geom. Dedicata **3** (1974), 229–231.
33. ———, *A combinatorial characterization of Hermitian curves*, J. Algebraic Combin. **1** (1992), 97–102.

Department of Geometry, Eötvös Loránd University
H-1117 Budapest, Pázmány s. 1/c, Hungary
and
Bolyai Institute, University of Szeged
H-6720 Szeged, Aradi vértanúk tere 1, Hungary
E-mail address: kissgy@cs.elte.hu