Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 151-154*

Semiovals in projective planes of small order

György Kiss[1] kissgy@cs.elte.hu
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

S. Marcugini†, F. Pambianco[2] gino, fernanda@dipmat.unipg.it
Department of Mathematics and Informatics, University of Perugia,
I-06123 Perugia, via Vanvitelli 1, ITALY

Abstract. Semiovals in PG$(2, q)$ for $q \leq 13$ are investigated. New examples are constructed, some characterization theorems and non-existence results of semiovals with extra properties are proved.

1 Introduction

Let Π be a projective plane of order q. A *semioval* in Π 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. The classical examples of semiovals arise from polarities (ovals and unitals), and from the theory of blocking sets (the vertexless triangle). The semiovals are interesting objects in their own right, but the study of semiovals is also motivated by their applications to cryptography. Batten [1] constructed an effective message sending scenario which use determining sets. She proved that determining sets in projective planes correspond to blocking semiovals. A *blocking semioval* is a semioval $\mathcal{S}$ such that every line of Π contains at least one point of $\mathcal{S}$ and at least one point which is not in $\mathcal{S}$. A blocking semioval that can be constructed in every projective plane of order $q > 2$ is the vertexless triangle.

It is known that $q + 1 \leq |\mathcal{S}| \leq q\sqrt{q} + 1$ and both bounds are sharp [10], [6], the extremes occur when $\mathcal{S}$ is an oval or a unital. In Section 2 we give the complete spectrum of the sizes of semiovals for $q \leq 9$. Besides, we determine the number of distinct semiovals up to collineations for $q \leq 7$. We also present the classification of small size semiovals for $q = 8, 9$ and new examples for $q = 11$ and 13. These semiovals were found by computer search.

Blocking semiovals in PG$(2, 7)$ were classified by Ranson and Dover [9]. The plane of order 7 contains several interesting semiovals. In Section 3 some characterization theorems for these semiovals are given.

2 On the spectrum of size for $q \leq 13$

For planes of order $q \leq 5$ the complete spectrum of the sizes and the number of projectively non-isomorphic semiovals has been known.

Case $q = 2$. Because of the bounds of the size, each semioval consists of three points, and these points are not collinear, hence semiovals are ovals.

Case $q = 3$. 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 $\mathcal{S}$ because $\lfloor 3\sqrt{3} + 1 \rfloor = 6$. 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 there is only one projectively non-isomorphic class of semiovals of order six in $\mathrm{PG}(2, 3)$.

Case $q = 4$. The possible sizes of $\mathcal{S}$ are $5, 6, 7, 8$ and 9. If $|\mathcal{S}| = 5$, then $\mathcal{S}$ is an oval. If $|\mathcal{S}| > 5$, then $\mathcal{S}$ contains three collinear points. Semiovals with large secants were investigated by Dover [4]. He proved that if $\mathcal{S}$ is a semioval in a projective plane of order $q > 3$, then $\mathcal{S}$ does not contain q collinear points, and if $|\mathcal{S}| = 2q-1$, then $\mathcal{S}$ has no $(q-1)$-secant. In our case $\mathcal{S}$ has $3 = q-1$ collinear points, hence $|\mathcal{S}| \neq 7 = 2q - 1$. The cases $|\mathcal{S}| = 2q - 2 = 6$ and $|\mathcal{S}| = 9 = 3q - 3$ are also characterized by Dover [4], these are a triangle with its vertices and all points on one side removed, and the vertexless triangle, respectively. Let us remark that in $\mathrm{PG}(2, 4)$ each unital is a vertexless triangle and vice versa. If $|\mathcal{S}| = 8$, then an exhaustive computer search shows that the only semiovals of this size are vertexless triangles with one point deleted.

For $q > 4$ the situation becomes more and more complicated. Semiovals of size $2(q-1)+k$ for all $0 \leq k \leq q-1$ 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 $[2q, 3q - 3]$. For $q \leq 9$, by exhaustive computer search, we found the following sizes.

Theorem 2.1 *The spectrum of the sizes of semiovals in $PG(2, q)$ is the following:*

- *If $q = 2$ then $|\mathcal{S}| = 3$.*
- *If $q = 3$ then $|\mathcal{S}| \in \{4, 6\}$.*
- *If $q = 4$ then $|\mathcal{S}| \in \{5, 6, 8, 9\}$.*

- *If* $q = 5$ *then* $|\mathcal{S}| \in \{6, 8, 9, 10, 11, 12\}$.
- *If* $q = 7$ *then* $|\mathcal{S}| \in \{8, 9, 12, 13, 14, 15, 16, 17, 18, 19\}$.
- *If* $q = 8$ *then* $|\mathcal{S}| \in \{9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23\}$
- *If* $q = 9$ *then*
  $|\mathcal{S}| \in \{10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28\}$.

For $q \leq 7$ we have determined the number of non-equivalent semiovals up to collineations. For $q \leq 4$ there is only one class for each size, as follows from the previous description. For $q = 5, 7$ the results are summarized in Table 1.
For $q = 8, 9$ we have classified the examples of minimum order which are not ovals. In both cases the minimum order is twelve and there are, respectively, four and one classes. Besides, for $q = 8$, we have proven that there are only two classes of semiovals of size 13.

PG(2,5)	size of $\mathcal{S}$	6	8	9	10	11	12			
	# of distinct classes	1	1	2	3	2	1			
PG(2,7)	size of $\mathcal{S}$	8	9	12	13	14	15	16	17	18	19
	# of distinct classes	1	1	10	21	69	118	82	21	7	1

Table 1

We have also found examples of the following sizes:

Theorem 2.2

- *In* $PG(2, 11)$ *there are semiovals of size* $12, 15, 20, 22 - 34$.
- *In* $PG(2, 13)$ *there are semiovals of size* $14, 18, 24, 26 - 40$.

3 The exceptional semiovals in PG$(2, 7)$

There are some interesting semiovals in PG$(2, 7)$. The first one has only $q + 2$ points. If $q = 7$, then $q+2 = 3(q-1)/2$, and the semioval belongs to an infinite class of semiovals which was described by Kiss and Ruff [8]. The following classification theorem is a consequence of a result of Blokhuis [3].

Theorem 3.1 *If* $|\mathcal{S}| = q + 2$, q *odd, then* $q = 7$. $\mathcal{S}$ *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 it is contained in a vertexless triangle.* □

PG$(2, 7)$ contains a semioval of size $13 = 2 \cdot 7 - 1$. There is no known infinite class of semiovals of size $2q - 1$. There are only three known semiovals of this size, they exist on the planes of order 5, 7 and 9. The following theorem of Faina, Kiss, Marcugini and Pambianco [5] characterizes the case $q = 7$.

Theorem 3.2 *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.* □

Batten and Dover [2] found a cyclic semioval in PG$(2, 7)$. It follows from our computer search, that this semioval is projectively unique. Hence we have the following theorem.

Theorem 3.3 *If $\mathcal{S}$ is a semioval in PG$(2, 7)$ then $|\mathcal{S}| \leq 19$. If $|\mathcal{S}| = 19$, then $\mathcal{S}$ is cyclic.* □

Cyclic semiovals are rare objects. There are only two known examples. The other one can be found in PG$(2, 81)$, it has 511 points, see [5]. The following nonexistence result was proved by Faina, Kiss, Marcugini and Pambianco [5].

Theorem 3.4 *There is no cyclic semioval in PG$(2, q)$ if $q \equiv 2 \pmod 3$.* □

They also prowed by exhaustive computer search, that PG$(2, 3^r)$ does not contain a cyclic semioval if $r \leq 11$ and $r \neq 4$.

References

[1] L. M. Batten, Determining sets, *Australas. J. Combin.* 22, 2000, 167-176.

[2] L. M. Batten, J. M. Dover, Blocking semiovals of type $(1, m + 1, n + 1)$, *SIAM J. Discr. Math.* 14, 2001, 446-457.

[3] A. Blokhuis, Characterization of seminuclear sets in a finite projective plane, *J. Geom.* 40, 1991, 15-19.

[4] J. M. Dover, Semiovals with large collinear subsets, *J. Geom.* 69, 2000, 58-67.

[5] G. Faina, Gy. Kiss, S. Marcugini, F. Pambianco, On the spectrum of the sizes of semiovals in PG(2,q), q odd, submitted.

[6] 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.

[7] Gy. Kiss, A survey on semiovals, *Contrib. Discr. Math.* 3, 2008, 81-95 (electronic).

[8] Gy. Kiss, J. Ruff, Notes on small semiovals, *Ann. Univ. Sci. Budapest*, Eötvös Sect. Math. 47, 2004, 97-105.

[9] B. B. Ranson, J. M. Dover, Blocking semiovals in PG$(2, 7)$ and beyond, *Europ. J. Combin.* 24, 2003, 183-193.

[10] J. A. Thas, On semiovals and semiovoids, *Geom. Dedic.* 3, 1974, 229-231.