AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **52** (2012), Pages 269–280

Some new results on small blocking semiovals

Jeremy M. Dover

Dover Networks LLC
445 Poplar Leaf Dr.
Edgewater, MD 20137
U.S.A.
jeremy@dovernetworks.com

In memoriam Barbara Bloom Ranson: student, colleague, friend

Abstract

A blocking semioval S in a projective plane of order q is a set of points such that every line meets S in at least one point (the blocking property), and every point of S lies on a unique tangent line (the semioval property). The set of points on the sides of a triangle, excluding the vertices, is a blocking semioval in any projective plane of order $q > 2$, and has size $3q - 3$. The size of a blocking semioval is constrained to be between $2q + 2$ and $q\sqrt{q} + 1$, and generically we call a blocking semioval "small" if its size is less than $3q - 3$.

In this paper we give several new constructions of small blocking semiovals in even order Desarguesian planes and also prove some non-existence results in planes of order 8 and 9 which allow us to determine exactly the size of the smallest blocking semioval in most planes of these orders. In addition, we give an improvement to the lower bound on the size of a blocking semioval in a plane of order q to a value on the order of $2q + \sqrt{2q}$.

1 Introduction

In a projective plane π, a **semioval** is a set of points S such that there is a unique tangent line (i.e., line with one point contact) at each point. A set of points S in π is called a **blocking set** if every line of π meets S in at least one point, but S contains no line. A set of points in π is called a **blocking semioval** if it is both a blocking set and a semioval.

The study of blocking semiovals is motivated by their connections to a cryptographic protocol invented by Batten [1], but they have geometric interest in their own right, in that a blocking semioval is simultaneously a minimal blocking set and a

Table 1: Sizes of smallest known blocking semiovals

Order (q)	Minimum Size
q prime, $q \equiv 1 \pmod 3$	$3q - 5$
q prime, $q \not\equiv 1 \pmod 3$	$3q - 4$
$q = r^e$, $e \geq 2$, $r \geq 3$ a prime power	$3q - r - 2$
$q = 2^e$, e odd, composite	$3q - e' - 2$, for e' the largest proper divisor of e
$q = 2^e$, e prime	$3q - 4$

maximal semioval. Much of the initial work on blocking semiovals focused on "small" blocking semiovals, both in the sense of identifying asymptotic lower bounds on the size of blocking semiovals as a function of the order q of the ambient projective plane π, as well as identifying minimum examples of blocking semiovals.

In the current literature, the best known asymptotic lower bound on the size of a blocking semioval in a plane of order $q \geq 7$ is $2q + 2$, proven by the author in [3], while the weaker bound of $2q + 1$ is true for planes of order $q \geq 4$. For some small orders, blocking semiovals have been completely classified, thus the minimum size is known. $PG(2, 2)$ contains no blocking semiovals, and the only blocking semioval in either $PG(2, 3)$ or $PG(2, 4)$ is the vertexless triangle, of size 6 and 9 respectively. The author [3] shows $PG(2, 5)$ has blocking semiovals of size 11 and 12, while Ranson and Dover [8] enumerate the blocking semiovals in $PG(2, 7)$, with 16 being the smallest size.

$PG(2, 8)$ provides the first case where there is a difference between the lower bound $2q + 2 = 18$ and 20, the size of the smallest known blocking semioval (given in Suetake [9]), and the disparity between the bound and the smallest known examples grows significantly thereafter. Indeed, the best known constructions grow asymptotically as $3q$, while the lower bound grows asymptotically as $2q$. Kiss [6] provides a good survey of the known constructions of blocking semiovals in Desarguesian planes, from which we can extract the smallest known for certain orders; see Table 1.

Additional examples of small blocking semiovals admitting homology groups are given by Suetake [10], while blocking semiovals that contain conics have been studied by Dover, Mellinger and Wantz [4]. Work has also been done on blocking semiovals in non-Desarguesian projective planes; see for example Jacobs [5] and Nakagawa and Suetake [7].

In this paper, we provide some new results on small blocking semiovals, both by providing constructions and non-existence proofs of smaller examples in some cases and by improving the lower bound on their size.

2 Some new families in even order planes

Of the known constructions for blocking semiovals, only the one given by the author in [3] applies to the Desarguesian plane of order $q = 2^e$ for prime e. We provide two

new constructions of blocking semiovals in these planes, one of which provides a new set of smallest known examples. In these constructions, we model $PG(2,q)$ using homogeneous coordinates, denoting point coordinates in parentheses (x,y,z), and line coordinates in brackets $[a,b,c]$. Both constructions are based on modifications of the vertexless triangle Δ, the set of points on the lines $[1,0,0]$, $[0,1,0]$, and $[0,0,1]$, excepting the points $(1,0,0)$, $(0,1,0)$, and $(0,0,1)$.

Theorem 2.1. *In $PG(2,q)$ with $q \geq 8$ even, let Δ be a vertexless triangle as defined above. For a fixed $\sigma \in GF(q) \setminus \{0,1\}$, let $\tau = \frac{\sigma}{1+\sigma}$ and define $D = \{(1,1,0),(0,1,1),(1,0,\sigma),(1,0,\tau)\}$ and $A = \{(1,1,1),(1,\sigma,\sigma),(1,\tau,\tau)\}$. Then $S = (\Delta \setminus D) \cup A$ is a blocking semioval of size $3q-4$.*

Proof. Note that the removal of each point of D from Δ causes its Δ-tangent to become unblocked in $\Delta' = \Delta \setminus D$. Moreover a pair of removed points in D can either cause no problem (as long as q is big enough, which needs to be checked) if both lie together on a side of Δ, create an extra tangent if we remove two points from a 3-secant, or create an unblocked line if we remove all three points from a 3-secant. We then check that each of these problems is remedied by adding the points of A, additionally making sure that each point of A is the only point added to exactly one unblocked line, resulting in a tangent line to S at that point. The proof technique utilized in Ranson and Dover [8] gives a concise method for representing this information and allowing the reader to check that all conditions are satisfied.

We see that we are removing no more than two points from any side of Δ, so all sides of Δ remain at least 2-secants to S since $q \geq 8$. The remainder of the proof is summarized in Table 2. □

Our next construction is similar, but allows us to reduce the size of the blocking semioval to $3q-5$.

Theorem 2.2. *In $PG(2,q)$ with $q \geq 8$ even, let Δ be a vertexless triangle as defined above. For a fixed $\sigma \in GF(q) \setminus \{0\}$ such that $\sigma^3 \neq 1$, let $\tau = \frac{\sigma}{1+\sigma}$ and define $D = \{(1,1,0),(1,\sigma,0),(0,1,1),(1,0,1),(1,0,\sigma),(1,0,\tau),(1,0,1+\sigma)\}$ and $A = \{(1,1,1),(1,\sigma,1+\sigma),(1,1+\sigma,\sigma),(1,1,1+\sigma),(1,\tau,\tau)\}$. Then $S = (\Delta \setminus D) \cup A$ is a blocking semioval of size $3q-5$.*

Proof. We are removing no more than four points from any side of Δ, so all sides of Δ remain at least 2-secants to S since $q \geq 8$. The remainder of the proof is summarized in Table 3. Note that the condition $\sigma^3 \neq 1$ is necessary both to prevent the degenerate condition where $\sigma = 1$, but also to prevent unwanted incidences, e.g., we do not want $(1,1,1+\sigma)$ to lie on the line $[0,1,\sigma]$. □

Since Theorem 2.2 provides a construction of blocking semiovals for all Desarguesian planes of even order greater than 8, we obtain a new family of smallest known blocking semiovals in the planes of order $q = 2^e$ for odd prime e.

Table 2: Effects of Additions and Deletions of Points for Theorem 2.1

Lines unblocked by Δ'	Why?	Added Points	Tangent to S
$[1,1,0]$	Δ-tangent at $(1,1,0)$	$(1,1,1)$	Yes
$[0,1,1]$	Δ-tangent at $(0,1,1)$	$(1,1,1)$,$(1,\sigma,\sigma)$,$(1,\tau,\tau)$	No
$[\sigma,0,1]$	Δ-tangent at $(1,0,\sigma)$	$(1,\sigma,\sigma)$	Yes
$[\tau,0,1]$	Δ-tangent at $(1,0,\tau)$	$(1,\tau,\tau)$	Yes

Δ'-multiple points	Δ'-tangent	Why tangent?	Added points
$(1,0,1)$	$[1,0,1]$	Δ-tangent	$(1,1,1)$
	$[1,1,1]$	$(1,1,0)$,$(0,1,1)$ del'd	none
$(0,1,\sigma)$	$[0,\sigma,1]$	Δ-tangent	none
	$[\sigma,\sigma,1]$	$(1,1,0)$,$(1,0,\sigma)$ del'd	$(1,\tau,\tau)$
$(0,1,\tau)$	$[0,\tau,1]$	Δ-tangent	none
	$[\tau,\tau,1]$	$(1,1,0)$,$(1,0,\tau)$ del'd	$(1,\sigma,\sigma)$
$(1,\sigma,0)$	$[\sigma,1,0]$	Δ-tangent	$(1,\sigma,\sigma)$
	$[\sigma,1,1]$	$(0,1,1)$,$(1,0,\sigma)$ del'd	none
$(1,\tau,0)$	$[\tau,1,0]$	Δ-tangent	$(1,\tau,\tau)$
	$[\tau,1,1]$	$(0,1,1)$,$(1,0,\tau)$ del'd	none

3 An improved lower bound

As previously mentioned, the best general purpose lower bound on the size of blocking semioval in a plane of order $q \geq 7$ is $2q+2$. To improve this bound, we need the following Theorem, which was proven as Theorem 3.1 in Dover [3].

Theorem 3.1. *Let Π be a projective plane of order $q \geq 3$, and let S be a blocking semioval in Π. If S has a $(q-k)$-secant, $1 \leq k < q-1$, then S contains at least $\frac{3k+4}{k+2}q - k$ points.*

Even in that paper it was informally noted that the existence of blocking semiovals of size $2q+2$ was unlikely, given that they would be forced to have mostly "small" secants. The following Lemma formalizes that concept.

Lemma 3.2. *Let π be a projective plane of order q and let α be a fixed positive integer. If $q > 3\alpha+3$ then for every blocking semioval S in π that has size $2q+\alpha$, no line meets S in more than $\alpha+2$ points.*

Proof. Letting S be as in the Lemma statement, suppose S has a $(q-k)$-secant for some $k > 0$. By Theorem 3.1 we have the inequality

$$2q + \alpha = |S| \geq \frac{3k+4}{k+2}q - k.$$

Multiplying through by $k+2$ and collecting like terms yields

$$(k+2)(k+\alpha) \geq kq.$$

Table 3: Effects of Additions and Deletions of Points for Theorem 2.2

Lines unblocked by Δ'	Why?	Added Points	Tangent to S
$[1,1,0]$	Δ-tangent at $(1,1,0)$	$(1,1,1)$, $(1,1,1+\sigma)$	No
$[\sigma,1,0]$	Δ-tangent at $(1,\sigma,0)$	$(1,\sigma,1+\sigma)$	Yes
$[0,1,1]$	Δ-tangent at $(0,1,1)$	$(1,1,1)$,$(1,\tau,\tau)$	No
$[1,0,1]$	Δ-tangent at $(1,0,1)$	$(1,1,1)$	Yes
$[\sigma,0,1]$	Δ-tangent at $(1,0,\sigma)$	$(1,1+\sigma,\sigma)$	Yes
$[\tau,0,1]$	Δ-tangent at $(1,0,\tau)$	$(1,\tau,\tau)$	Yes
$[1+\sigma,0,1]$	Δ-tangent at $(1,0,1+\sigma)$	$(1,1,1+\sigma)$, $(1,\sigma,1+\sigma)$	No
$[1,1,1]$	del $(1,1,0)$,$(1,0,1)$,$(0,1,1)$	$(1,\sigma,1+\sigma)$,$(1,1+\sigma,\sigma)$	No
$[\sigma,1,1]$	del $(1,\sigma,0)$,$(0,1,1)$,$(1,0,\sigma)$	$(1,1,1+\sigma)$	Yes

Δ'-multiple points	Δ'-tangent	Why tangent?	Added points
$(1,1+\sigma,0)$	$[1+\sigma,1,0]$	Δ-tangent	$(1,1+\sigma,\sigma)$
	$[1+\sigma,1,1]$	$(1,0,1+\sigma)$,$(0,1,1)$ del'd	none
$(1,\tau,0)$	$[\tau,1,0]$	Δ-tangent	$(1,\tau,\tau)$
	$[\tau,1,1]$	$(0,1,1)$,$(1,0,\tau)$ del'd	none
$(0,1,\sigma)$	$[0,\sigma,1]$	Δ-tangent	none
	$[\sigma,\sigma,1]$	$(1,1,0)$,$(1,0,\sigma)$ del'd	$(1,\tau,\tau)$
$(0,1,1+\sigma)$	$[0,1+\sigma,1]$	Δ-tangent	$(1,1,1+\sigma)$
	$[1+\sigma,1+\sigma,1]$	$(1,1,0)$,$(1,0,1+\sigma)$ del'd	none
$(0,1,\tau)$	$[0,\tau,1]$	Δ-tangent	$(1,1+\sigma,\sigma)$
	$[\tau,\tau,1]$	$(1,1,0)$,$(1,0,\tau)$ del'd	none
$(0,\sigma,1)$	$[0,1,\sigma]$	Δ-tangent	none
	$[\sigma,1,\sigma]$	$(1,\sigma,0)$,$(1,0,1)$ del'd	$(1,\tau,\tau)$
$(0,\tau,1)$	$[0,1,\tau]$	Δ-tangent	$(1,\sigma,1+\sigma)$
	$[\sigma,1,\tau]$	$(1,\sigma,0)$,$(1,0,1+\sigma)$ del'd	none
$(0,\sigma,\tau)$	$[0,\tau,\sigma]$	Δ-tangent	none
	$[\sigma\tau,\tau,\sigma]$	$(1,\sigma,0)$,$(1,0,\tau)$ del'd	$(1,1,1)$

Finally dividing both sides by k and expanding yields

$$k+\alpha+2+\frac{2\alpha}{k}\geq q.$$

Suppose first that $1\leq k\leq 2\alpha$. Over this interval and considering the left-hand side of this inequality as a function of k, simple calculus shows that the maximum value occurs at one of the endpoints of the interval, meaning the maximum value is $3\alpha+3$. But since q is restricted to be greater than this quantity, S must have no $(q-k)$-secants for $1\leq k\leq 2\alpha$.

Now if $k>2\alpha$, we can write $k\geq q-(\alpha+2)-\frac{2\alpha}{k}$. The term $\frac{2\alpha}{k}$ is strictly between 0 and 1, and since k, q and α are integers we can write $k\geq q-(\alpha+2)$. So every line of π is a $(q-k)$-secant to S for some $k\geq q-(\alpha+2)$, or equivalently every line of π is an m-secant to S for some $m\leq\alpha+2$. □

For a blocking semioval S in a plane π of order q, we let $|S| = q + \lambda$ for some $\lambda > 0$, and let x_i denote the number of lines of π meeting S in exactly i points. S being a blocking semioval shows that $x_0 = 0$ and $x_1 = q + \lambda$, and simple counting yields the following equations:

$$\sum_{i=2}^{q-1} x_i = q^2 + 1 - \lambda \tag{1}$$

$$\sum_{i=2}^{q-1} i x_i = q^2 + q\lambda \tag{2}$$

$$\sum_{i=2}^{q-1} i(i-1) x_i = \lambda^2 + (2q-1)\lambda + (q^2 - q) \tag{3}$$

From the weaker lower bound of $2q$ on the size of a blocking semioval in a plane of order q given in Dover [3] which holds for all $q \geq 3$, we may write $\lambda = q + \alpha$ for some $\alpha \geq 0$. We then "diagonalize" these equations, yielding the equivalent system of equations:

$$x_2 + \sum_{i=5}^{q-1} \left[\frac{1}{2}i^2 - \frac{7}{2}i + 6\right] x_i = 2q^2 - (\alpha+7)q + \frac{1}{2}(\alpha^2 - 13\alpha + 12) \tag{4}$$

$$x_3 + \sum_{i=5}^{q-1} \left[-i^2 + 6i - 8\right] x_i = -2q^2 + (\alpha+10)q - (\alpha^2 - 9\alpha + 8) \tag{5}$$

$$x_4 + \sum_{i=5}^{q-1} \left[\frac{1}{2}i^2 - \frac{5}{2}i + 3\right] x_i = q^2 - 4q + \frac{1}{2}(\alpha^2 - 7\alpha + 6) \tag{6}$$

Proposition 3.3. *For any nonnegative integer α, all blocking semiovals S in a projective plane of order $q > \frac{1}{2}\alpha^2 + \frac{1}{2}\alpha + 6$ satisfy $|S| > 2q + \alpha$.*

Proof. Let π be a projective plane of order q and S a blocking semioval in π. From Dover [3], every blocking semioval in a plane of order $q \geq 4$ has at least $2q+1$ points, and every blocking semioval in a plane of order $q \geq 7$ has at least $2q + 2$ points, proving the result for $\alpha = 0, 1$.

Let $|S| = 2q + \alpha$ where we assume $\alpha \geq 2$. Noting that $\frac{1}{2}\alpha^2 + \frac{1}{2}\alpha + 6 \geq 3\alpha + 3$ for all integral α (with equality for $\alpha = 2, 3$), we have $q > 3\alpha + 3$. By Lemma 3.2, this implies that no line of π meets S in more than $\alpha + 2$ points. Letting x_i denote the number of lines meeting S in exactly i points as above, the following specializations of Equations 5 and 6 hold:

$$x_3 + \sum_{i=5}^{\alpha+2} \left[-i^2 + 6i - 8\right] x_i = -2q^2 + (\alpha+10)q - (\alpha^2 - 9\alpha + 8)$$

$$x_4 + \sum_{i=5}^{\alpha+2} \left[\frac{1}{2}i^2 - \frac{5}{2}i + 3\right] x_i = q^2 - 4q + \frac{1}{2}(\alpha^2 - 7\alpha + 6)$$

We combine these two equations by adding $(\alpha-1)$ times the first to $2(\alpha-2)$ to the second to obtain

$$(\alpha-1)x_3 + 2(\alpha-2)x_4 + \sum_{i=5}^{\alpha+2}\left[-i^2+(\alpha+4)i-(2\alpha+4)\right]x_i = \\ -2q^2+(\alpha^2+\alpha+6)q+(\alpha-1)(\alpha+4) \tag{7}$$

The polynomial $-i^2+(\alpha+4)i-(2\alpha+4)$ is only nonnegative between its roots, but those roots are 2 and $\alpha+2$. Hence on the left side of Equation 7, all of the x_i's and all of their coefficients are nonnegative, forcing the right side $-2q^2+(\alpha^2+\alpha+6)q+(\alpha-1)(\alpha+4)$ to be nonnegative. Taking the derivative of this polynomial, we see that it decreases for all $q > \frac{1}{4}(\alpha^2+\alpha+6)$, thus also for $q > \frac{1}{2}\alpha^2+\frac{1}{2}\alpha+6$. Since this polynomial evaluates to $-2\alpha^2-40$ for $q=\frac{1}{2}\alpha^2+\frac{1}{2}\alpha+6$, we have that the right side of Equation 7 is negative for all $q > \frac{1}{2}\alpha^2+\frac{1}{2}\alpha+6$, giving a contradiction that shows no blocking semioval of size $2q+\alpha$ can exist in a projective plane of order greater than $\frac{1}{2}\alpha^2+\frac{1}{2}\alpha+6$, as claimed. □

Restating this result in a different form, we have

Theorem 3.4. *Let S be a blocking semioval in a projective plane π of order $q \geq 7$. Then $|S| \geq 2q+\sqrt{2q-\frac{47}{4}}-\frac{1}{2}$.*

Proof. Let S be a blocking semioval in π and suppose $|S| = 2q+\alpha$. By the contrapositive of Proposition 3.3, this forces $q \leq \frac{1}{2}\alpha^2+\frac{1}{2}\alpha+6$, or equivalently $2q \leq \alpha^2+\alpha+12$. Completing the square on the right-hand side yields $2q-\frac{47}{4} \leq \left(\alpha+\frac{1}{2}\right)^2$, and solving for α completes the result. □

While this is asymptotically a significantly better bound than the previously known $2q+2$, it is actually worse in the case $q=7$. This discrepancy occurs because the proof given here does not make use of the fact that every blocking semioval in a plane of order $q > 5$ is known to have at least one line meeting it in 4 or more points. However $q=7$ is the only case affected by this quirk.

4 Planes of order 8 and 9

As previously mentioned, the minimum size of a blocking semioval in a (necessarily Desarguesian) projective plane of order q is known for $q = 3, 4, 5, 7$; in these cases the best known lower bound equals the size of the smallest known blocking semioval. In the Desarguesian plane of order 8 and the four projective planes of order 9 this is not the case. In $PG(2,8)$ Theorem 3.4 shows that any blocking semioval must have at least 18 points. Theorem 2.2 gives an example of a blocking semioval of size 19 in that plane, currently the smallest known. In a projective plane of order $q=9$, Theorem 3.4 shows that a blocking semioval must have at least 20 points, but the smallest known blocking semiovals have size 21. Nakagawa and Suetake [7]

give examples of blocking semiovals of size 21 in each of the three non-Desarguesian projective planes of order 9, but interestingly no example of a blocking semioval of size 21 is known in $PG(2,9)$. In this section we determine the size of the smallest blocking semioval in $PG(2,8)$ as well as the three non-Desarguesian planes of order 9, which will demonstrate that the lower bound given by Theorem 3.4 is not sharp.

We start with projective planes of order $q = 9$, which perhaps surprisingly is easier to deal with. In [7], Nakagawa and Suetake show via computer search that there is no blocking semioval with 20 points that admits an 8-secant in any projective plane of order 9. Combining their work with an extension of Lemma 3.2 allows us to prove a stronger nonexistence result.

Theorem 4.1. *No projective plane of order* 9 *contains a blocking semioval with* 20 *points.*

Proof. Suppose there exists a plane π of order $q = 9$ containing a blocking semioval S of size $20 = 2q + 2$ points. Using the same analysis as in the proof of Lemma 3.2, if S has a $(q-k)$-secant, then k must satisfy the inequality $k + 4 + \frac{4}{k} \geq 9$. Simple enumeration thus shows that a line of π can meet S in either 8 points, or at most 5 points. Nakagawa and Suetake [7] have found that no blocking semioval of size 20 in a plane of order 9 can have an 8-secant, therefore no line of π can meet S in more than 5 points.

Denoting the number of lines meeting S in i points as x_i, we utilize Equations 4, 5 and 6 to obtain the following relationships:

$$\begin{aligned} x_2 + x_5 &= 76 \\ x_3 - 3x_5 &= -48 \\ x_4 + 3x_5 &= 43 \end{aligned}$$

Adding the latter two of these equations yields $x_3 + x_4 = -5$, clearly a contradiction since x_3 and x_4 are nonnegative. Thus no projective plane of order 9 can have a blocking semioval of size 20. □

Disproving the existence of a blocking semioval of size 18 in $PG(2,8)$ requires more substantial case checking. Throughout we let $\mathbf{S}$ denote a blocking semioval in $PG(2,8)$ with 18 points, and as above let x_i denote the number of i-secants to $\mathbf{S}$. From Dover [3] $x_i = 0$ for all $i \geq 8$, and $x_7 = 0$ by Suetake [9], where it is shown via computer search that any blocking semioval in $PG(2,8)$ with a 7-secant must have at least 20 points. Specializing Equations 4, 5 and 6 for $\mathbf{S}$ we have the following relationships:

$$x_2 + x_5 + 3x_6 = 51 \tag{8}$$

$$x_3 - 3x_5 - 8x_6 = -26 \tag{9}$$

$$x_4 + 3x_5 + 6x_6 = 30 \tag{10}$$

We begin with a lemma that gives us more information about potential 5- and 6-secants to $\mathbf{S}$.

Lemma 4.2. *If a blocking semioval* $\mathbf{S}$ *of size* 18 *in* $PG(2,8)$ *exists, then*

1. *If* $\mathbf{S}$ *has a* 5*-secant* m*, then three of the four points on* m *not in* $\mathbf{S}$ *lie on three tangents, five* 2*-secants and one* 5*-secant to* $\mathbf{S}$*, while the fourth point lies on four tangents, three* 2*-secants, one* 3*-secant and one* 5*-secant to* $\mathbf{S}$*.*
2. *If* $\mathbf{S}$ *has a* 6*-secant* ℓ*, then the three points of* ℓ *not in* $\mathbf{S}$ *lie on four tangents, four* 2*-secants and one* 6*-secant to* $\mathbf{S}$*.*

Proof. Let m be a 5-secant to $\mathbf{S}$, and let Υ be the set of four points of m not in $\mathbf{S}$. For any point $P \in \Upsilon$, there are 9 lines through P, each of which contains at least 1 point of $\mathbf{S}$ since $\mathbf{S}$ is blocking. One of these lines is m, so the remaining 8 lines through P must be covered by the 13 points of $\mathbf{S}$ not on m. We claim at least three of these lines are tangents to $\mathbf{S}$; if not, then at least six lines through P would meet $\mathbf{S} \setminus m$ in at least two points, forcing there to be at least 14 points of $\mathbf{S}$ off m. Hence every point $P \in \Upsilon$ lies on at least 3 tangents to $\mathbf{S}$.

Since $\mathbf{S}$ is a semioval, exactly 13 tangent lines to $\mathbf{S}$ meet m in a point of Υ, forcing three points of Υ, which we denote with the subset Υ_3, to lie on exactly three tangents to $\mathbf{S}$, and the fourth point of Υ, denoted P_4, to lie on exactly four tangents to $\mathbf{S}$. For a point P of Υ_3, in addition to the 5-secant m and the three tangent lines, there are five lines that must each meet $\mathbf{S}$ in at least 2 points. These five lines must cover 10 points of $\mathbf{S}$ hence each point of Υ_3 lies on three tangents, five 2-secants, and one 5-secant. Similarly, P_4 lies on four tangents, three 2-secants, one 3-secant and one 5-secant.

Now let ℓ be a 6-secant to $\mathbf{S}$, and let Ψ be the set of three points on ℓ not contained in $\mathbf{S}$. If $P \in \Psi$, the eight lines through P other than ℓ are all blocked by the 12 points of $\mathbf{S}$ not on ℓ. Letting t denote the number of tangent lines through P, we must have $12 \geq t + 2 \times (8 - t)$, thus $t \geq 4$, with equality only if every line through P not tangent to $\mathbf{S}$, and not ℓ, is a 2-secant. Each of the three points in Ψ must lie on at least four tangents to $\mathbf{S}$, but only 12 tangents to $\mathbf{S}$ meet ℓ in a point of Ψ. Thus each point of Ψ lies on four tangents, four 2-secants and one 6-secant to $\mathbf{S}$, as claimed. □

The following corollary collects some useful consequences of this Lemma.

Corollary 4.3. *If a blocking semioval* $\mathbf{S}$ *of size* 18 *in* $PG(2,8)$ *exists, then*

1. *If* ℓ *is a* 6*-secant to* $\mathbf{S}$*, every* k*-secant to* $\mathbf{S}$ *with* $k \geq 3$ *meets* ℓ *in a point of* $\mathbf{S}$*.*
2. *If* m *is a* 5*-secant to* $\mathbf{S}$*, every* k*-secant to* $\mathbf{S}$ *with* $k \geq 3$ *meets* m *in a point of* $\mathbf{S}$*, except for a unique* 3*-secant.*

Corollary 4.3 allows us to eliminate several possible configurations from consideration.

Proposition 4.4. *If a blocking semioval* $\mathbf{S}$ *of size* 18 *in* $PG(2,8)$ *exists, then* $\mathbf{S}$ *has a* 6*-secant.*

Proof. Let $\mathbf{S}$ be as in the Proposition statement, and recall that x_i denotes the number of lines intersecting $\mathbf{S}$ in exactly i points. By way of contradiction assume that $\mathbf{S}$ has no 6-secant, i.e., $x_6 = 0$. Then Equations 8, 9 and 10 reduce to

$$\begin{aligned} x_2 + x_5 &= 51 \\ x_3 - 3x_5 &= -26 \\ x_4 + 3x_5 &= 30 \end{aligned}$$

Adding the latter two equations shows that $x_3 + x_4 = 4$, and the last equation shows that x_4 is divisible by 3, so the only possible intersection patterns for $\mathbf{S}$ are $(x_2, x_3, x_4, x_5) = (42, 1, 3, 9)$ or $(x_2, x_3, x_4, x_5) = (41, 4, 0, 10)$. In particular, $\mathbf{S}$ must have a 5-secant.

Suppose first that $(x_2, x_3, x_4, x_5) = (42, 1, 3, 9)$. In this case, $\mathbf{S}$ has exactly one 3-secant and nine 5-secants. By Corollary 4.3, we know that each of the 5-secants must meet the 3-secant in a point not on $\mathbf{S}$, of which there are 6 possible choice. Thus the 3-secant must have a point Q not in $\mathbf{S}$ which lies on at least two 5-secants. But this forces two 5-secants to meet in a point not in $\mathbf{S}$, which cannot occur by Corollary 4.3. Thus $\mathbf{S}$ cannot have this intersection pattern.

Now assume that $(x_2, x_3, x_4, x_5) = (41, 4, 0, 10)$. We first show by way of contradiction that no point of $\mathbf{S}$ can lie on more than three 5-secants. Clearly no point of $\mathbf{S}$ can lie on five or more 5-secants, since this would force $\mathbf{S}$ to have at least 21 points. Assume there exists a point P that lies on four 5-secants to $\mathbf{S}$. Each of these four 5-secants contains P and four other points of $\mathbf{S}$ accounting for 17 points of $\mathbf{S}$, hence there is a unique point $Q \in \mathbf{S}$ not on any of these four 5-secants. Let m be any other 5-secant to $\mathbf{S}$. m meets each of the four 5-secants through P in at most one point, implying that the fifth point of $\mathbf{S}$ on m must be Q. But there are six other 5-secants to $\mathbf{S}$, forcing Q to lie on six 5-secants, which cannot happen.

Let m be any 5-secant. The other nine 5-secants must meet m in points of $\mathbf{S}$ by Corollary 4.3, but each such point can lie on at most two 5-secants other than m. Thus four of the points in $m \cap \mathbf{S}$ lie on exactly three 5-secants, while the remaining point of $m \cap \mathbf{S}$ lies on exactly two 5-secants. Let X denote the number of points of $\mathbf{S}$ lying on three 5-secants, and count the set $\{(P, m)\}$ of flags in two ways, where P is a point of $\mathbf{S}$ lying on exactly three 5-secants, and m is a 5-secant incident with P. Choosing the line first, there are 10 ways to pick a 5-secant, and then 4 ways to pick a point of $\mathbf{S}$ on that line in lying on three 5-secants, making the size of this set 40. On the other hand there are X choices for the point, and then 3 choices for a 5-secant passing through it, implying $3X = 40$. This forces X to be non-integral, a contradiction.

Therefore $\mathbf{S}$ cannot have either of the possible intersection patterns with $x_6 = 0$, implying $\mathbf{S}$ must have a 6-secant. □

At this point, we appeal to a computer search. Letting $\mathbf{S}$ be our putative blocking semioval of size 18 in $\pi = PG(2, 8)$, we note that $\mathbf{S}$ must have a 6-secant, which we can without loss of generality assume is $\ell = [0, 0, 1]$. The automorphism group of π

is 3-transitive on points of ℓ, so we may assume without loss of generality that all points of ℓ other than $\Phi = \{(1,0,0),(0,1,0),(1,1,0)\}$ are in $\mathbf{S}$. By Lemma 4.2 we know that for each point $P \in \Phi$ exactly four lines through P other than $[0,0,1]$ must be tangents to $\mathbf{S}$.

Using the computer algebra package Magma [2], we can quickly determine that up to projective equivalence, there are only 76 configurations of twelve lines with four lines meeting ℓ in each point of Φ. For each set $\{T_1,\ldots,T_{12}\}$ of putative tangent lines we can complete our search by looking at all sets $\{S_1,\ldots,S_{12}\}$ of twelve points such that S_i incident with T_j if and only if $i=j$, since any point on more than one T_i would lie on multiple tangents. Our check consists of testing the blocking semioval property on the set $\{S_1,\ldots,S_{12}\} \cup (\ell \setminus \Phi)$. Using Magma to perform this search, our program generated no blocking semiovals of size 18 in $PG(2,8)$ with a 6-secant, with the search lasting about 2 hours.

Putting all of these pieces together allows us to state the following

Theorem 4.5. *$PG(2,8)$ contains no blocking semioval of size 18.*

5 Conclusion

Despite the improvement in the lower bound on the size of a blocking semioval in a plane of order q from Theorem 3.4, this bound is still not sharp in either the small order cases or compared asymptotically to the best known constructions. However we seem to have wrung all of the possible improvement from the existing techniques, suggesting that a new approach is needed, either in formulating a new lower bound or in construction.

We also determined that the size of the smallest blocking semioval in $PG(2,8)$ is 19, and that the size of the smallest blocking semioval in a non-Desarguesian plane of order 9 is 21. However there remains a discrepancy in $PG(2,9)$, where the smallest possible size for a blocking semioval is 21 points, while the smallest known has 22 points.

References

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

[2] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system I, The user language, *J. Symbolic Comput.* 24 (3–4) (1997), 235–265.

[3] Jeremy M. Dover, A lower bound on blocking semiovals, *European J. Combin.* 21 (5) (2000), 571–577.

[4] Jeremy M. Dover, Keith E. Mellinger, and Kenneth L. Wantz, Blocking semiovals containing conics, *Adv. Geom.* (to appear).

[5] Christina Jacobs, A new blocking semioval, *Bull. Inst. Combin. Appl.* 42 (2004), 19–24.

[6] Győrgy Kiss, A survey on semiovals, *Contrib. Discrete Math.* 3 (1) (2008), 81–95.

[7] Nobuo Nakagawa and Chihiro Suetake, On blocking semiovals with an 8-secant in projective planes of order 9, *Hokkaido Math. J.* 35 (2) (2006), 437–456.

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

[9] Chihiro Suetake, Two families of blocking semiovals, *European J. Combin.* 21 (7) (2000), 973–980.

[10] Chihiro Suetake, Some blocking semiovals which admit a homology group, *European J. Combin.* 21 (7) (2000), 967–972.

(Received 27 July 2011)