# A New Blocking Semioval

Christina Jacobs
Department of Mathematics
Washington State University
Pullman, WA 99164-3113

June 11, 2004

## 1 Introduction

Let $\Pi = (P, L)$ be a projective plane of order $n$. A *blocking set* in $\Pi$ is a set $B$ of points such that for every line 1 of $\Pi$ there is at least one point of 1 in $B$, but 1 is not entirely contained in $B$. Blocking sets have been extensively studied, see for example, Berardi and Eugeni [2].

A *semioval* in $\Pi$ is a set $S$ of points such that for every point $P \in S$ there is a unique tangent to $S$ containing $P$. Here, as usual, a tangent to $S$ is a line of $\Pi$ meeting $S$ in exactly one point. The concept of semioval is a generalization of the concept of oval. An *oval* in $\Pi$ is a set of $n+1$ points such that no three are collinear. Since two points in $\Pi$ lie on a unique line, and since there are $n+1$ lines through a point of $\Pi$, it is clear that an oval is a semioval. Ovals have also been extensively studied, but semiovals have so far received little attention. (See Hughes and Piper [5], Chapter XII.)

One type of semioval that has recently received some attention is the blocking semioval. A *blocking semioval* in $\Pi$ is a blocking set that is also a semioval. That is, a blocking semioval is a set $S$ of points in $\Pi$ satisfying: (1) every line 1 of $\Pi$ contains a point of $S$ and a point not in $S$; (2) for every point $P$ of $S$ there is a unique tangent to $S$ containing $P$. One interesting aspect of a blocking semioval is that it is both a minimal blocking set and a maximal semioval [4].

Batten [1] initiated the study of blocking semiovals when she showed they had an important role to play in cryptography. Dover [4] discovered bounds on the size of a blocking semioval $S$ and on the size of $S \cap l$, where 1 is a line of $\Pi$. Furthermore, Dover [4], Dover and Ranson [6] verified the existence of some infinite families of blocking semiovals.

A *vertexless triangle* in the projective plane $\Pi$ is constructed as follows. Let $1_1$, $1_2$, $1_3$ be three nonconcurrent lines in $\Pi$, that is, they do not meet in a common point. If $P_1$, $P_2$, $P_3$ are the three points of intersection determined by $l_1$, $l_2$, $l_3$, then the set $(l_1 \cup l_2 \cup l_3) - \{P_1, P_2, P_3\}$ consisting of the points in the three lines different from $P1$, $P2$, and $P3$ forms a vertexless triangle. See Figure 1.

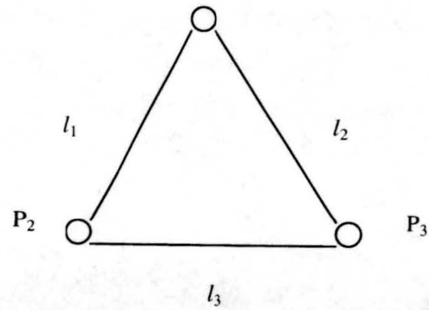


**Figure 1.** Vertexless Triangle

For $n > 2$, a vertexless triangle $T$ is a blocking semioval. (If $Q \in T$ is in the line $l_i$ then the line determined by $Q$ and $l_j \cap l_k$ is the tangent to $T$ through $Q$.) All other known blocking semiovals have been found only in desarguesian projective planes.

In this article we give an example of a blocking semioval occuring in a nondesarguesian plane. Our example occurs in the translation plane coordinatized by the nearfield of order $n$. It probably can be extended to all nearfield planes of order $p^2$, $p$ a prime. The example is not a vertexless triangle, the only other known blocking semioval occuring in a nondesarguesian plane; so it is new. Suetake [7] studied some blocking semiovals in $PG(2, n)$ with nontrivial homologies and constructed three families of blocking semiovals.

In Section 2 we recall the definition of the nearfield of order 9. In Section 3 we give some background information on blocking semiovals. In Section 4 we describe the new blocking semioval and show that it is not a vertexless triangle.

# 2 Coordinatizing a projective plane using a nearfield

Let $F$ be the field of nine elements obtained by adjoining to $GF(3)$ the element $\alpha$ satisfying $\alpha^2 + 1 = 0$ or $\alpha^2 = 2$. The nearfield $K$ of order nine can then be defined as follows. The elements of $K$ are the elements of $F$ and the addition of $K$ is that of $F$. The multiplication, denoted by $\cdot$, in the nearfield $K$ is given by

$$a \cdot b = \begin{cases} ab & \text{if } b^2 \in GF(3) \\ a^3 b & \text{if } b^2 \notin GF(3) \end{cases} .$$

Here the multiplication on the right is that of $F$ [3].

A projective plane **N** coordinatized by $K$ can be defined as follows. First, the affine plane **A** coordinatized by $K$ consists of the points $(a, b)$, where $a, b \in K$. The lines of **A** are given by equations of the form

$$y = x \cdot m + k, \qquad m, k \in K \tag{1}$$

and

$$x = a, \qquad a \in K \tag{2}$$

For example, an equation of type (1) represents the set of points $(a, b)$ with $b = a \cdot m + k$. An equation of type (2) represents the set of points $(a, b)$, where $a$ is fixed and $b$ ranges over all of $K$. A line of type (1) is said to have slope $m$. A line of type (2) is said to be vertical.

To obtain the projective plane **N** we add to the affine plane **A** points $(m)$, one for each $m \in K$. Furthermore, we require that for each $m$ all lines of slope $m$ in **A** go through $(m)$. [That is, we add $(m)$ to each of the sets $y = x \cdot m + k$.] Also, we add one more point $(\infty)$ to **A**, and we add the point to each vertical line. Finally, the points $(m)$, $m \in K$, and $(\infty)$ form a new line called the line at infinity.

It is in the projective plane **N**, sometimes referred to as the Hall plane, that we find a new blocking semioval, which is described in the next section.

# 3 A new blocking semioval in the nearfield plane of order 9

In the projective plane **N** of Section 2 consider the set $S'$ consisting of all points in **N** satisfying the equation

$$y^2 - x^2 = 1. \tag{3}$$

Out of the $9^2 + 9 + 1 = 91$ points of **N**, there are 20 points satisfying the equation (3):

$$\begin{array}{ccc} (1, \alpha) & (2, \alpha) & (\alpha, 0) \\ (1, \alpha+1) & (2, \alpha+1) & (\alpha+1, 0) \\ (1, \alpha+2) & (2, \alpha+2) & (\alpha+2, 0) \\ (1, 2\alpha) & (2, 2\alpha) & (2\alpha, 0) \\ (1, 2\alpha+1) & (2, 2\alpha+1) & (2\alpha+1, 0) \\ (1, 2\alpha+2) & (2, 2\alpha+2) & (2\alpha+2, 0) \\ \multicolumn{3}{c}{(0,1) \qquad\qquad (0,2)} \end{array} \tag{4}$$

These points are the elements of $S'$.

Of the 20 points of $S'$ there are 18 with a unique tangent as given in Table 1:

| Point | Tangent Line |
|---|---|
| $(1, \alpha)$ | $y = x \cdot 2\alpha + 2\alpha$ |
| $(1, \alpha + 1)$ | $y = x \cdot (2\alpha + 2) + (2\alpha + 2)$ |
| $(1, \alpha + 2)$ | $y = x \cdot (2\alpha + 1) + (2\alpha + 1)$ |
| $(1, 2\alpha)$ | $y = x \cdot \alpha + \alpha$ |
| $(1, 2\alpha + 1)$ | $y = x \cdot (\alpha + 2) + (\alpha + 2)$ |
| $(1, 2\alpha + 2)$ | $y = x \cdot (\alpha + 1) + (\alpha + 1)$ |
| $(2, \alpha)$ | $y = x \cdot \alpha + 2\alpha$ |
| $(2, \alpha + 1)$ | $y = x \cdot (\alpha + 1) + (2\alpha + 2)$ |
| $(2, \alpha + 2)$ | $y = x \cdot (\alpha + 2) + (2\alpha + 1)$ |
| $(2, 2\alpha)$ | $y = x \cdot 2\alpha + \alpha$ |
| $(2, 2\alpha + 1)$ | $y = x \cdot (2\alpha + 1) + (\alpha + 2)$ |
| $(2, 2\alpha + 2)$ | $y = x \cdot (2\alpha + 2) + (\alpha + 1)$ |
| $(\alpha, 0)$ | $x = \alpha$ |
| $(\alpha + 1, 0)$ | $x = \alpha + 1$ |
| $(\alpha + 2, 0)$ | $x = \alpha + 2$ |
| $(2\alpha, 0)$ | $x = 2\alpha$ |
| $(2\alpha + 1, 0)$ | $x = 2\alpha + 1$ |
| $(2\alpha + 2, 0)$ | $x = 2\alpha + 2$ |

**Table 1:** Tangents to the Set $S'$

The last two points of $S'$ listed in (4) each have three tangents as given in Table 2:

| Point | Tangents |
|---|---|
| $(0, 1)$ | $y = 1,\ y = x + 1,\ y = x \cdot 2 + 1$ |
| $(0, 2)$ | $y = 2,\ y = x + 2,\ y = x \cdot 2 + 2$ |

**Table 2:** Points of $S'$ with Three Tangents

Furthermore, there are exactly three lines which do not intersect $S'$; they are

$$y = x, \qquad y = x \cdot 2, \qquad \ell_\infty, \text{ the line at infinity} \tag{5}$$

All other lines of $\mathbf{N}$ intersect $S'$. For example, Table 3 lists the lines through the point $(1, \alpha)$ and their points of intersection with $S'$.

| Lines Through $(1,\alpha)$ | Points of Intersection with $S'$ |
|---|---|
| $x=1$ | $(1,\alpha),(1,\alpha+1),(1,\alpha+2),(1,2\alpha),$ $(1,2\alpha+1),(1,2\alpha+2)$ |
| $y=\alpha$ | $(1,\alpha),(2,\alpha)$ |
| $y=x+(\alpha+2)$ | $(1,\alpha),(2,\alpha+1),(2\alpha+1,0)$ |
| $y=x\cdot 2+(\alpha+1)$ | $(1,\alpha),(2,\alpha+2),(\alpha+1,0)$ |
| $y=x\cdot\alpha$ | $(1,\alpha),(2,2\alpha)$ |
| $y=x\cdot(\alpha+1)+2$ | $(1,\alpha),(0,2),(2\alpha,\alpha+1),(2\alpha+2,0)$ |
| $y=x\cdot(\alpha+2)+1$ | $(1,\alpha),(0,1),(2,2\alpha+2),(\alpha+2,0)$ |
| $y=x\cdot 2\alpha+2\alpha$ | $(1,\alpha)$[ Tangent at $(1,\alpha)$] |
| $y=x\cdot(2\alpha+1)+(2\alpha+2)$ | $(1,\alpha),(2\alpha,0)$ |
| $y=x\cdot(2\alpha+2)+(2\alpha+1)$ | $(1,\alpha),(\alpha,0)$ |

**Table 3:** Lines Through $(1,\alpha)$ and Their Intersections with $S'$

The above shows that the set $S'$ does not form a blocking set - not every line of $\mathbf{N}$ intersects it - nor does it form a semioval - there are points with more than one tangent. However, considering Table 2 and (5), we see that adding the points (1) and (2) to $S'$ to form a new set $S$ of 22 points does give a blocking semioval.

By adding points (1) and (2) the points $(0,1)$ and $(0,2)$ now have unique tangents $y=1$ and $y=2$, respectively. Furthermore, the line $y=x$ is now tangent to the point (1), the line $y=x\cdot 2$ is now tangent to the points (2), and $\ell_\infty$, the line at infinity, meets the expanded set $S$ in the two points (1) and (2). A computation by hand shows that every line of $\mathbf{N}$ meets the set $S$ in 1, 2, 4, or 6 points only. For example, looking at Table 3 we have one tangent $y=x\cdot 2\alpha+2\alpha$, one line ($x=1$) meeting $S$ in six points, four lines ($y=x+(\alpha+2)$, $y=x\cdot 2+(\alpha+1)$, $y=x\cdot(\alpha+1)+2$, $y=x\cdot(\alpha+2)+1$) meeting $S$ in four points, and four lines ($y=\alpha$, $y=x\cdot\alpha$, $y=x\cdot(2\alpha+1)+(2\alpha+2)$, $y=x\cdot(2\alpha+2)+(2\alpha+1)$) meeting $S$ in two points.

The set $S$ cannot be a vertexless triangle. For by Ranson [6; Lemma 2.1] for a vertexless triangle in a projective plane every line meets it in either 1, 3, or $n-1$ points, where $n$ is the order of the plane. Since $S$ has lines meeting in 2, 4, or 6 points it cannot be a vertexess triangle. Thus we have:

**Theorem:** *The set $S$ consisting of the 20 points given in (4) and the points (1) and (2) is a blocking semioval in the nearfield plane $N$ of order 9.*

We also note that for a blocking semioval $B$ in a projective plane $\mathbf{N}$ of order $n$ the size $|B|$ is bounded [4] by

$$2n+1\leq|B|\leq n\sqrt{n}+1$$

our blocking semioval $S$ satisfies these bounds.

# 4 Future directions

By hand computation we have found a blocking semioval in the nearfield plane of order 9. Except for vertexless triangles, it is the first example of a blocking semioval in a nondesarguesian projective plane.

An interesting question is: Can the construction be extended to larger nearfield planes of order $p^2$, $p$ a prime? That is, can the solutions to the equation

$$y^2 - x^2 = 1 \tag{6}$$

in a nearfiled plane of order $p^2$ lead to a blocking semioval? It seems very plausible. However, to answer the question a more theoretical attack is needed. For example, in the nearfield plane of order $7^2 = 49$ there are 176 points satisfying (6).

It would also be interesting to consider equation (6) in the context of certain semifield planes.

# References


[1] L.M. Batten, Protocol for a private key cryptosystem with signature capability based on blocking sets in $t$-designs, preprint.

[2] L. Berardi and F. Eugeni, Blocking sets e teoria dei geochi; origini e problematiche, *Atti Sem. Mat. Fis. Univ. Modena* **36** (1988), no. 1, 165–196.

[3] P. Dembowski *Finite geometries*, Berlin, Springer-Verlag, 1968.

[4] J.M. Dover, A lower bound on blocking semiovals, *European J. Combin.* **21** (2000), no. 5, 571–577.

[5] D.R. Hughes and F.C. Piper, *Projective planes*, New York, Springer-Verlag, 1973.

[6] B. Ranson, A new blocking semioval family, MS Thesis, North Dakota State University, 2001.

[7] C. Suetake, Some blocking semiovals which admit a homology group, *European J. Combin.* **21** (2000), no. 7, 967–972.