Blocking Semiovals of Type \((1, M + 1, N + 1)\)

LYNN M. BATTEN\(^1\) AND JEREMY M. DOVER\(^2\)

**Abstract.** We consider the existence of blocking semiovals in finite projective planes which have intersection sizes \(1, m + 1\) or \(n + 1\) with the lines of the plane for \(1 \leq m < n\). For those prime powers \(q \leq 1024\), in almost all cases, we are able to show that, apart from a trivial example, no such blocking semioval exists in a projective plane of order \(q\). We are also able to prove, for general \(q\), that if \(q^2 + q + 1\) is a prime or three times a prime, then only the same trivial example can exist in a projective plane of order \(q\).

**Key words.** projective planes, blocking sets, semiovals

**AMS subject classifications.** 51E20, 51E21

**PII.** S0895480100338002

1. Motivation. Blocking sets in projective planes have been much studied; the “classical” results due to Bruen [7], [8] state that in a projective plane of order \(q\), a blocking set has between \(q + \sqrt{q} + 1\) and \(q^2 - \sqrt{q}\) points. Many additional references, as well as descriptions of applications in game theory and cryptography, can be found in Chapter 8 of Batten [2].

A*semioval* in a projective plane is a set of points \(S\) such that for each point \(P\) of \(S\), there exists a unique line which meets \(S\) in exactly the point \(P\). In [15], Hubaut proved that in a projective plane of order \(q\), a semioval \(S\) has between \(q + 1\) and \(q\sqrt{q} + 1\) points. These two extremes occur in the case when \(S\) is an oval (see [2]) or a unital (see [11]), respectively. In the case of regular semiovals, that is, when \(S\) has constant line size \(a\), considered as a design in its own right, Blokhuis and Szőnyi [5] prove that either \(S\) is an oval or \(a|q - 1\).

Blocking sets and semiovals coincide in the case when each is a unital. In fact, for *minimal* blocking sets (where each point is on at least one tangent), it is known that the upper bound on the number of points is \(q\sqrt{q} + 1\), which is precisely the unital case (see [9]).

This leads to the more general question: in what other cases is a blocking set also a semioval? There is a trivial example on \(3(q - 1)\) points in every finite projective plane of order \(q > 2\). Take three nonconcurrent lines (a “triangle”) and delete the three points where these lines intersect (the “vertices”). It is not difficult to check that this set is a blocking semioval.

As well as being interesting objects in their own right, our main motivation for their study comes from Batten [3], where blocking semiovals are studied in relation to a cryptographic protocol designed by the author.

We say that a set \(X\) of points in a plane \(\Pi\) is of type \((m_1, m_2, \ldots, m_k)\) if each line of \(\Pi\) meets \(X\) in \(m_i\) points for some \(i\), \(1 \leq i \leq k\), and if for each \(m_i\), \(1 \leq i \leq k\), some line of \(\Pi\) meets \(X\) in \(m_i\) points. A unital thus has type \((1, \sqrt{q} + 1)\) and the triangle
with deleted vertices has type \((1, 3, q - 1)\). In case \(q - 1 = 3\), it is easy to see that these two coincide.

It is not difficult, using the methods of Proposition 2.1 of the next section, to show that a blocking semioval of type \((1, n)\), \(n \geq 2\), must be a unital. This result also follows from the deeper work of Tallini-Scafati [20] on the classification of sets of type \((1, n)\). The purpose of this paper is to explore the situation of type \((1, m + 1, n + 1)\) blocking semiovals. (We use \(m + 1\) and \(n + 1\) to facilitate simpler computations.)

In section 2, a number of arithmetic conditions on blocking semiovals of type \((1, m + 1, n + 1)\) are given and families of possible parameters exhibited. The principal result in this direction is the following theorem.

**Theorem 2.3.** Let \(q > 4\) be a square prime power, and let \(\Pi\) be a projective plane of order \(q\). Then 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 \(\Pi\) if and only if \(\frac{\lambda}{\lambda + 2}(q + \sqrt{q})\) is an integer with \(0 \leq \lambda \leq \sqrt{q} - 3\).

Using MAGMA [10], we were able to show that for \(q\) a prime power less than or equal to 1024, there is only a small number of possible blocking semiovals of our type whose existence remains undecided; this is the content of section 3. Other than the triangles with deleted vertices, we know of only one type of blocking semioval with just three intersection numbers. For any Singer cycle \(\sigma\) of \(\text{PG}(2, 7)\), the three point orbits under \(\sigma^3\) are each a blocking semioval of type \((1, 3, 4)\), each containing 19 points. (This set was originally considered by Brouwer [6] in another context.)

The main results of nonexistence are presented in section 4 with the following two theorems.

**Theorem 4.1.** Let \(\Pi\) be a projective plane of order \(q \geq 2\) such that \(q^2 + q + 1\) is prime. Then the only blocking semioval of type \((1, m + 1, n + 1), 1 \leq m < n\), in \(\Pi\) is a triangle with vertices deleted.

**Theorem 4.2.** Let \(\Pi\) be a projective plane of order \(q \geq 2\), \(q \neq 7\), such that \(q^2 + q + 1 = 3p\), \(p\) prime. Then the only blocking semioval of type \((1, m + 1, n + 1), 1 \leq m < n\), in \(\Pi\) is a triangle with vertices deleted.

The “unique tangent” condition ascribed to semiovals has been generalized to the concept of a “strong representative system.” Blokhuis and Metsch [4], for instance, use this setting to show that any semioval or minimal blocking set on \(q\sqrt{q}\) points for \(q\) square and \(q \geq 49\) must be part of a unital. Hence no minimal blocking set of this size exists. We discuss this, as well as some of their other results, further in section 4.

In section 5, we summarize our results and pose several conjectures.

### 2. Arithmetic conditions

In this section, we begin with a lemma which describes the various arithmetic conditions which constrain the parameters of our semiovals for which we need some notation. Let \(\Pi\) be a projective plane of order \(q\), and let \(S\) be a blocking semioval with three intersection numbers in \(\Pi\). Let \(v\) denote the number of points in \(S\), and let \(m + 1\) and \(n + 1\) denote the nontangent line intersection sizes of \(S\), where we may assume without loss of generality that \(m < n\). As every point of \(S\) lies on exactly one tangent, it is a simple computation to show that there exist constants \(a\) and \(b\) such that every point of \(S\) lies on exactly \(b\) \((m + 1)\)-secants and \(a\) \((n + 1)\)-secants. The numbers \((v, m + 1, n + 1, a, b)\) are called the parameters of the blocking semioval \(S\).

We can now prove the following proposition.

**Proposition 2.1.** Let \(\Pi\) be a projective plane of order \(q > 2\), and let \(S\) be a blocking semioval in \(\Pi\) with parameters \((v, m + 1, n + 1, a, b)\). Then the following
conditions hold:

\begin{align*}
\text{(1)} & \quad v = 1 + an + bm, \\
\text{(2)} & \quad q^2 + q + 1 = v \left( 1 + \frac{b}{m+1} + \frac{a}{n+1} \right), \\
\text{(3)} & \quad a + b = q, \\
\text{(4)} & \quad m < \sqrt{q}, \\
\text{(5)} & \quad v \geq (m+1)(n+1), \\
\text{(6)} & \quad m + n \leq q.
\end{align*}

Further, equality holds in inequalities (5) and (6) if and only if \( S \) is a triangle with vertices removed.

\textit{Proof}. Equation (1) can be obtained by counting the number of points in \( S \) in two different ways, and (3) arises from counting the number of lines through a point of \( S \).

To obtain (2), notice that every line must be either a tangent, \((m+1)\)-secant, or \((n+1)\)-secant to \( S \). One can easily count that there are \( v \) tangents, \( \frac{vb}{m+1} (m+1) \)-secants, and \( \frac{va}{n+1} (n+1) \)-secants to \( S \). The sum of these three numbers must equal the number of lines in the plane \( q^2 + q + 1 \), which establishes the equality.

Inequality (4) can be proven by contradiction. Suppose \( m \geq \sqrt{q} \). As \( n > m \), we know \( n > \sqrt{q} \) as well. Using our second condition, we have \( v = 1 + an + bm > 1 + a\sqrt{q} + b\sqrt{q} \). This latter expression equals \( q\sqrt{q} + 1 \) using our first condition. However, no semioval may contain more than \( q\sqrt{q} + 1 \) points (see Hubaut [15]), which is our contradiction.

To establish inequality (5), we proceed by assuming \( v \leq (m+1)(n+1) \). We compute

\begin{align*}
\text{as} & \geq 1 \text{ and } n > m, \text{ we know the term } (a-1)(n-m) \text{ is nonnegative, which implies } (a-1)(n-m) \leq mn, \text{ with equality if and only if } a = 1. \text{ This forces } n \geq q - 2, \text{ again with equality if and only if } a = 1.
\end{align*}

If \( a > 1 \), then \( n > q - 2 \), which forces some line to meet \( S \) in at least \( q \) points. From Dover [12], this only can happen in \( PG(2,3) \), and in that one case, \( v = (m+1)(n+1) \). However, if \( a = 1 \), this quickly forces \( b = q - 1 \) and \( n = q - 2 \). Using (1) and (2), one can solve for \( m \) to find \( m = 3 \), which forces \( v = 3q - 3 \). Again from Dover [12], any semi oval with \( 3q - 3 \) points such that some line meets it in \( q - 1 \) points must be a triangle with deleted vertices.

To prove inequality (6), begin with (2), clear denominators, and subtract \( v(m+1)(n+1) \) from both sides to get

\begin{align*}
\text{(7)} & \quad (q^2 + q + 1 - v)(m+1)(n+1) = v(bn + am + a + b).
\end{align*}

Using (3) directly and in conjunction with (1) in

\begin{align*}
bn + am & = (a+b)n + (a+b)m - (an+bm) \\
& = q(n+m) - (v-1),
\end{align*}
we can substitute into (7) to obtain
\[(q^2 + q + 1 - v)(m + 1)(n + 1) = (q(n + m + 1) + 1 - v)v,\]
By inequality (5), we have \(v \geq (m + 1)(n + 1)\) with equality if and only if \(S\) is a triangle. Using this fact on the right-hand side of (8) and cancelling we find
\[q^2 + q + 1 - v \leq q(n + m + 1) + 1 - v,\]
which implies \(m + n \geq q\), with equality if and only if \(S\) is a triangle, as claimed.

We call any set of parameters \((v, m + 1, n + 1, a, b)\) which satisfy the conditions of Proposition 2.1 arithmetically feasible. We now wish to give some examples of arithmetically feasible parameter sets.

**Proposition 2.2.** For any prime power \(q \geq 5\), the parameter set of the triangle with deleted vertices, \((3q^2 - 3, 3q - 1, q - 1)\), is always arithmetically feasible. Further, for all planes of order \(q \geq 5\) such a blocking semioval exists, and any blocking semioval with these parameters must be a triangle with deleted vertices.

**Proof.** The proof follows directly from the existence of vertexless triangles and Proposition 2.1.

We note here that the triangle forms a blocking semioval in all planes of order \(q > 2\), yet we did not include the cases \(q = 3, 4\) in Proposition 2.2. The reason is that if \(q = 3\), this would force \(m\) to be greater than \(n\), contrary to our assumption that \(m < n\). In the case \(q = 4\), \(m = n\) and our blocking semioval has only one nontangent intersection number, not two. As mentioned in the introduction, this forces the vertexless triangle to be a unital when \(q = 4\).

We now give a result which describes a family of feasible parameters for every \(q > 2\) of square prime power order. Unlike Proposition 2.2, we know of no semioval with these parameters which exists.

**Theorem 2.3.** Let \(q > 4\) be a square prime power, and let \(\Pi\) be a projective plane of order \(q\). The parameter set
\[
v = (q + \sqrt{q} + 1)(\sqrt{q} - (1 + \lambda)),
m + 1 = (\sqrt{q} - (1 + \lambda)),
n + 1 = \sqrt{q} + 1,
a = q - (1 + \mu),
b = 1 + \mu
\]
is arithmetically feasible if and only if \(\mu = \frac{\lambda}{\lambda + 2}(q + \sqrt{q})\) is an integer with \(0 \leq \lambda \leq \sqrt{q} - 3\).

**Proof.** Checking the arithmetic conditions of Proposition 2.1 for these parameters is tedious but straightforward, and thus it is left to the reader.

**Corollary 2.4.** The parameter sets \((q\sqrt{q} - 1, \sqrt{q} - 1, \sqrt{q} + 1, q - 1)\) and \(((q + \sqrt{q} + 1)(\sqrt{q} - 3), \sqrt{q} - 3, \sqrt{q} + 1, q - (1 + \frac{1}{2}(q + \sqrt{q}))\) are arithmetically feasible for all square prime powers \(q \geq 25\) with the first parameter set being arithmetically feasible for all \(q \geq 9\).

**Proof.** The first set corresponds to the trivial case \(\lambda = 0\), while the second set corresponds to \(\lambda = 2\), which requires \(\sqrt{q} \geq 5\), as \(\lambda \leq \sqrt{q} - 3\).

As mentioned previously, it is unknown if blocking semiows with the second parameter set exist. Blokhuis and Metsch [4] have shown that no blocking semiow with the parameter set in Theorem 2.3 with \(\lambda = 0\) can exist in \(PG(2, q)\) when \(q\) is odd, and Ball [1] has proven a similar result for even \(q\).
Table 1
Sporadic arithmetically feasible parameter sets.

<table>
<thead>
<tr>
<th>Order of plane</th>
<th>v</th>
<th>m + 1</th>
<th>n + 1</th>
<th>a</th>
<th>b</th>
<th>Exists?</th>
</tr>
</thead>
<tbody>
<tr>
<td>q = 7</td>
<td>19</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>Yes by [6]</td>
</tr>
<tr>
<td>q = 16</td>
<td>49</td>
<td>3</td>
<td>7</td>
<td>4</td>
<td>12</td>
<td>?</td>
</tr>
<tr>
<td>q = 25</td>
<td>56</td>
<td>2</td>
<td>8</td>
<td>5</td>
<td>20</td>
<td>?</td>
</tr>
<tr>
<td>q = 64</td>
<td>209</td>
<td>3</td>
<td>11</td>
<td>10</td>
<td>54</td>
<td>No by Prop. 3.2</td>
</tr>
<tr>
<td>q = 121</td>
<td>1134</td>
<td>10</td>
<td>54</td>
<td>1</td>
<td>120</td>
<td>No by Prop. 3.1</td>
</tr>
<tr>
<td></td>
<td>518</td>
<td>2</td>
<td>6</td>
<td>99</td>
<td>22</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>342</td>
<td>2</td>
<td>6</td>
<td>55</td>
<td>66</td>
<td>?</td>
</tr>
<tr>
<td>q = 191</td>
<td>1612</td>
<td>7</td>
<td>12</td>
<td>93</td>
<td>98</td>
<td>?</td>
</tr>
<tr>
<td>q = 263</td>
<td>4251</td>
<td>17</td>
<td>18</td>
<td>42</td>
<td>221</td>
<td>?</td>
</tr>
<tr>
<td>q = 343</td>
<td>3774</td>
<td>10</td>
<td>17</td>
<td>98</td>
<td>245</td>
<td>No by Prop. 3.2</td>
</tr>
<tr>
<td>q = 373</td>
<td>7154</td>
<td>20</td>
<td>22</td>
<td>33</td>
<td>340</td>
<td>?</td>
</tr>
<tr>
<td>q = 947</td>
<td>19390</td>
<td>18</td>
<td>25</td>
<td>470</td>
<td>477</td>
<td>?</td>
</tr>
<tr>
<td>q = 1024</td>
<td>38889</td>
<td>5</td>
<td>13</td>
<td>224</td>
<td>800</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>11585</td>
<td>5</td>
<td>13</td>
<td>936</td>
<td>88</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>11585</td>
<td>11</td>
<td>35</td>
<td>56</td>
<td>968</td>
<td>No by Prop. 3.2</td>
</tr>
</tbody>
</table>

Table 1 details all arithmetically feasible parameters of all prime powers up to and including 1024, excepting those parameters shown to be feasible in Proposition 2.2 and Theorem 2.3. For omitted orders, the parameters given by the applicable results above are the only possibilities.

An exhaustive computer search using the package MAGMA [10] was used to obtain these possibilities for those values of $q$ which could not be eliminated using the results of the next section. We note that inequality (4) was used strongly in this search to limit the possibilities for $m$.

3. Eliminating possible parameter sets. In this section we prove several results which will allow us to rule out a number of the possibilities in Table 1. The first deals with the case where $a = 1$.

**Proposition 3.1.** Let $\Pi$ be a projective plane of order $q$, and let $S$ be a blocking semi-oval in $\Pi$ with parameters $(v, m + 1, n + 1, a, q - 1)$. Then $m$ must divide $q - n$ and $v - (q + 1)$.

**Proof.** First suppose that every point $P$ off $S$ lies on an $(n + 1)$-secant. Since there are precisely $\frac{v}{n+1}$ $(n + 1)$-secants to $S$, there are at most $\frac{v}{n+1}(q - n)$ points outside of $S$. Therefore $q^2 + q + 1 - v \leq \frac{v}{n+1}(q - n)$, which we can rearrange to obtain $q^2 + q + 1 \leq \frac{v(q+1)}{n+1}$.

Solving this inequality for $v$, we find that $v \geq \frac{(n+1)(q^2+q+1)}{q+1}$, which we can divide through to get $v > q(n + 1)$. However, again from (1) we have $v = n + 1 + (q - 1)m$, which implies $(q - 1)m > (q - 1)(n + 1)$, contradicting the fact that $m < n$.

Hence there must exist a point $P$ which lies on no $(n + 1)$-secants. Suppose $P$ lies on $x$ tangents and $y (m + 1)$-secants. Then simple counting yields that $x + y = q + 1$ and $x + (m + 1)y = v$. Subtracting these yields $my = v - (q + 1)$. Using (1) to substitute in for $v$ yields $my = 1 + n + (q - 1)m - q - 1$. Rearranging gives us $m(y - q + 1) = n - q$, which implies that $m$ divides $q - n$. That $m$ divides $v - (q + 1)$ now quickly follows from (1).

In particular, this proposition rules out the possibility that a blocking semi-oval in a plane of order 121 with parameters $(1134, 10, 54, 1, 120)$ could exist (see Table 1), as 9 does not divide 121 - 53 = 68.

Up to this point, we have focused on the “internal” structure of a blocking semi-
oval. We would now like to prove a result concerning points outside the semioval; this
will give us a strong divisibility condition amongst our parameters.

PROPOSITION 3.2. Let II be a projective plane of order q, and let S be a blocking
semiaval in II with parameters \((v, m + 1, n + 1, a, b)\). For every point \(P\) outside of S,
let \(d(P)\) denote the number of tangents to S passing through \(P\), \(e(P)\) the number of
\((m + 1)\)-secants, and \(f(P)\) the number of \((n + 1)\)-secants. Then we have

\[
\begin{align*}
nd(P) &\equiv q + n \pmod{n - m}, \\
me(P) &\equiv v - (q + 1) \pmod{n}, \\
f(P) &\equiv v - (q + 1) \pmod{m}.
\end{align*}
\]

Proof. Counting lines through \(P\), we have the relation \(d(P) + e(P) + f(P) = q + 1\).
By counting pairs of points \((P, Q)\), where \(Q \in S\), we obtain \(d(P) + (m + 1)e(P) +
(n + 1)f(P) = v\).

Multiply the first relation through by \(n\) to obtain \(nd(P) + ne(P) + nf(P) =
n(q + 1)\), which we can rewrite as \(nd(P) + (n - m)e(P) + me(P) + nf(P) = n(q + 1)\).
Notice from our second relation that \(me(P) + nf(P) = v - (d(P) + e(P) + f(P)) =
v - (q + 1)\). Hence we have \(nd(P) + (n - m)e(P) = (n + 1)(q + 1) - v\). From (1) we
know \(v = 1 + an + bm\), from which we can get \(v = 1 + (a + b)n + b(m - n)\). Putting
this all together we obtain \(nd(P) + (n - m)e(P) = (n + 1)(q + 1) - (1 + qn - b(n - m))\).
Finally reducing modulo \(n - m\) we obtain \(nd(P) \equiv q + n \pmod{n - m}\), as claimed.

To obtain the latter two relations in the proposition, we need recall only that
\(me(P) + nf(P) = v - (q + 1)\), which we can successively reduce modulo \(m\) and
\(n\).

To use this result effectively, we need the following two counts. Let \(S\) be a blocking
semiaval with parameters \((v, m + 1, n + 1, a, b)\) in a plane of order \(q\). We first count
all of the pairs \((P, \ell)\), where \(P\) is a point off of \(S\) and \(\ell\) is a line through \(P\) which is
tangent to \(S\). On the one hand, there are \(v\) tangents to \(S\), each of which contains
\(q\) points off \(S\), yielding \(qv\) pairs. On the other hand, for each point \(P\) off \(S\), there
are \(d(P)\) (using the notation of Proposition 3.2) lines which can pair with it. Hence
we have the equation \(\sum_P d(P) = qv\), where the sum is taken over all points \(P\) off
\(S\). A similar count of triples \((P, \ell_1, \ell_2)\), where \(\ell_1\) and \(\ell_2\) are distinct tangents to \(S\
meeting in \(P\), yields the equation \(\sum_P d(P)(d(P) - 1) = v(v - 1)\). From this we obtain
\(\sum_P d(P)^2 = v(q + v - 1)\).

Let us look at the possible parameter set \((209, 3, 11, 10, 54)\) in a plane of order
64. By Proposition 3.2, we know that for any point \(P\) off \(S\), we have \(10d(P) \equiv 74\n(mod 8)\), or \(d(P) \equiv 1\ (mod 4)\). In particular \(d(P)\) cannot take on the values 2, 3, or 4.

Consider \(\sum_P (d(P)^2 - 5)\). By the above paragraph, no term of this
sum can be negative. Further, this sum must be divisible by \(4^2\). For this particular
case, we have \(\sum_P d(P) = 13376\) and \(\sum_P d(P)^2 = 56848\). Thus we can evaluate
\(\sum_P (d(P)^2 - 5) = 56848 - 6(13376) + 5(64^2 + 64 + 1 - 209) = -19456\).
This contradicts the fact that all of our summands are nonnegative, implying that no
blocking semiaval with these parameters can exist. A similar argument rules out the
possible parameter set in a plane of order 343 and the third possibility for a plane of
order 1024.

We performed a similar analysis for \(e(P)\) and \(f(P)\) but were unable to rule out
any additional parameter sets. We are left with the unresolved sporadic cases in Table
2.
Table 2
Unresolved sporadic parameter sets.

<table>
<thead>
<tr>
<th>Order of plane</th>
<th>(v)</th>
<th>(m+1)</th>
<th>(n+1)</th>
<th>(a)</th>
<th>(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(q = 16)</td>
<td>49</td>
<td>4</td>
<td>7</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>(q = 25)</td>
<td>56</td>
<td>2</td>
<td>8</td>
<td>5</td>
<td>20</td>
</tr>
<tr>
<td>(q = 121)</td>
<td>518</td>
<td>2</td>
<td>6</td>
<td>99</td>
<td>22</td>
</tr>
<tr>
<td>(q = 256)</td>
<td>550</td>
<td>4</td>
<td>8</td>
<td>55</td>
<td>66</td>
</tr>
<tr>
<td>(q = 191)</td>
<td>1612</td>
<td>7</td>
<td>12</td>
<td>93</td>
<td>98</td>
</tr>
<tr>
<td>(q = 263)</td>
<td>4251</td>
<td>17</td>
<td>18</td>
<td>42</td>
<td>221</td>
</tr>
<tr>
<td>(q = 373)</td>
<td>7154</td>
<td>20</td>
<td>22</td>
<td>33</td>
<td>340</td>
</tr>
<tr>
<td>(q = 947)</td>
<td>1612</td>
<td>5</td>
<td>13</td>
<td>224</td>
<td>800</td>
</tr>
<tr>
<td>(q = 1024)</td>
<td>5889</td>
<td>5</td>
<td>13</td>
<td>936</td>
<td>88</td>
</tr>
</tbody>
</table>

4. The \(p\) and \(3p\) cases. The prime factorization of \(q^2 + q + 1\) can be used in conjunction with (2) of Proposition 2.1 to yield some information about blocking semiolas in the plane. Thus, in this section, we consider several special cases of this factorization. Note that representations of \(q^2 + q + 1\) have been much studied in number theory (see, for example, Mordell [18]). In particular, the cases where \(q^2 + q + 1\) is a prime power or divisible by 3 have been given much attention [14], [17], [19].

The simplest case to tackle is \(q^2 + q + 1\) prime, which occurs quite frequently for \(q \leq 1024\).

**Theorem 4.1.** Let \(\Pi\) be a projective plane of order \(q \geq 2\) such that \(q^2 + q + 1\) is prime. Then the only blocking semiola of type \((1, m+1, n+1), 1 \leq m < n\), in \(\Pi\) is a triangle with vertices deleted.

**Proof.** Let \(p = q^2 + q + 1\) and \(S\) be a blocking semiola of type \((1, m+1, n+1), 1 \leq m < n\), on \(v\) points in \(\Pi\). By (2) of Proposition 2.1, \(p(m+1)(n+1) = v[(m+1)(n+1) + a(m+1) + b(n+1)]\). Since \(v\) must be less than \(p\), \(v \mid (m+1)(n+1)\). By inequality (5) of Proposition 2.1, \(S\) is a triangle with vertices deleted.

Since approximately half of all values of \(q^2 + q + 1\), \(q\) a prime power, are congruent to 0 modulo 3, it is worthwhile to examine the case when 3 divides the number of points in the plane. In case \(q = 7\), \(q^2 + q + 1 = 57 = 3 \cdot 19\), and as we saw in the previous section, there is a semiola decomposition of the plane of the type wanted. We next show that for \(q^2 + q + 1\) equal to 3 times a prime, the case \(q = 7\) is the only one in which a nontrivial semiola of our type can occur.

**Theorem 4.2.** Let \(\Pi\) be a projective plane of order \(q \geq 2, q \neq 7\), such that \(q^2 + q + 1 = 3p, p\) prime. Then the only blocking semiola of type \((1, m+1, n+1), 1 \leq m < n\), in \(\Pi\) is a triangle with vertices deleted.

**Proof.** For \(q < 7\), the only value of \(q^2 + q + 1\) of the desired form is 21 with \(q = 4\). By inequality (6) of Proposition 2.1, \(v \leq 9\) in this case. Applying (2) and (3) of Proposition 2.1 and noting that the only possible values for \(m\) and \(n\) are 1 and 2, respectively, we find that there are no semiolas of type \((1, 2, 3)\) in this plane.

From now on, we assume \(q \geq 8\). Proposition 2.1 yields

\[
3p(m+1)(n+1) = v[(m+1)(n+1) + a(m+1) + b(n+1)].
\]

Now \(3p > v \geq (m+1)(n+1)\) by inequality (5) of Proposition 2.1 implies \((3p, (m+1)(n+1)) = 1, 3\) or \(p\). We consider several cases.

1. Suppose this is \(p\). Then \(p \mid (m+1)(n+1)\) and \(p \leq (m+1)(n+1) < 3p\) implies \((m+1)(n+1) = p\) or \(2p\).
(a) If \((m + 1)(n + 1) = p\), (9) implies \(v \mid 3p^2\), and the only factors of \(v\) are 3 and \(p\). Together with \(v < 3p^2\), either \(v = 3\), which is too small, or \(v = p = (m + 1)(n + 1)\), which yields the triangle by Proposition 2.1.

(b) If \((m + 1)(n + 1) = 2p\), (9) implies \(v \mid 6p^2\). Together with \((m + 1)(n + 1) = 2p \leq v < 3p\), we obtain \(v = 2p = (m + 1)(n + 1)\) and thus we have the triangle.

2. Now suppose \((3p, (m + 1)(n + 1)) = 1\) or 3. Then from (9) we have \(v \mid 3m + 3n + 1\) or \(v \mid p\).

(a) Suppose \(p \mid v\). Then \(v = p\) or \(2p\). In either situation, we get \(p \leq q\sqrt{q} + 1\), the maximum size of any semioval, while \(3p = q^2 + q + 1 > 3q\sqrt{q} + 3\) yields a contradiction if \(q \geq 8\).

(b) Suppose \(v \mid 3(m + 1)(n + 1)\). Then \(v = x(m + 1)(n + 1)\) where \(x = 1, \frac{3}{2}\), or 3. The first case yields the triangle, so we consider separately the cases \(v = \frac{3}{2}(m + 1)(n + 1)\) and \(v = 3(m + 1)(n + 1)\).

First assume \(v = \frac{3}{2}(m + 1)(n + 1)\). Applying Proposition 2.1 to (9), we obtain

\[
2p = \frac{3}{2}(q^2 + q + 1) = q(m + n + 1) + 1 - \frac{3}{2}(m + 1)(n + 1).
\]

This yields

\[
(2q - 1)^2 - (2q - 1)(3m + 3n - 1) + 3mn + 1 = 0,
\]

which has roots

\[
2q - 1 = \frac{3m + 3n - 1 \pm \sqrt{(3m + 3n - 1)^2 - 4(3mn + 1)}}{2}.
\]

Now \((3m + 3n - 1)^2 - 4(3mn + 1) > (3n - m + 3)^2\) if \(m \geq 2\), which gives either \(4q - 2 > 3m + 3n - 1 + (3n - m + 3)\) or \(4q - 2 < 3m + 3n - 1 - (3n - m + 3)\). The second of these yields, using inequality (4) of Proposition 2.1, \(4q < 4m - 2 < 4\sqrt{q} - 2\), which is false for \(q \geq 2\). From the first of these, we obtain \(4q > 6n + 2m + 4\). On the other hand, using (1) and (3) of Proposition 2.1, and assuming \(b \leq q - 2\), we obtain \(q \leq 3(n + 1)/2 - (n - 3)/2m + 2\). Putting inequalities together, we get \(6n + 2m + 6 \leq 4q \leq 6n + 6 - 2(n - 3)/m + 8\); hence \(2(n - 3)/m + 2m \leq 8\), which is false for \(n \geq 3\) and \(m > 4\). It remains, for this value of \(v\), to consider the separate cases \(b = q - 1\), \(n = 2\), \(m = 1\), and \(n \geq 3\) while \(m = 2, 3,\) or 4.

If \(m = 1\), substituting in (10) yields \(4q - 2 = 2\) or \(6n + 2\). Only \(q = (3n + 2)/2\) is possible; so \(n = 2(q - 1)/3\), and \(v = 2q + 1\). No blocking semioval of this size can exist for \(q \geq 7\) by Dover [13], \(n\) being an integer forces \(q \equiv 1\) (mod 3), so the only remaining \(q\) for which \(n\) is an integer is 4, and this yields the vertexless triangle.

If \(n = 2\), (10) yields \(4q - 2 = 3m + 5 \pm \sqrt{(3m + 1)^2 + 20}\). The discriminant is a square only if \(m = 1\) (implying \(q = 4\)), and in this case, we obtain the triangle with deleted vertices. The cases \(m = 2, 3,\) and 4 can be eliminated in the same way. For instance, \(m = 4\) yields \((3n + 3)^2 + 108\) a square, implying that 108 factors as \((x + y)(x - y)\), where \(y = 3n + 3\). This is not possible for \(n\) an integer larger than 1. Finally, suppose \(a = 1, b = q - 1\). By Proposition 3.1, \(m \mid v - (q + 1)\), which implies \(2m \mid 3n - 2q + 1\). So \(2m \mid 2q(3n - 2q + 1)\). However, from (9), using \(3p = q^2 + q + 1\), we get \(2(q^2 + q + 1) = 3(m + 1)(n + 2) + 3(q - 1)(n + 1)\), from which \(m \mid 2q^2 - 3q\). It follows that \(2m \mid 4q^2 - 2q - 6nq - 2 + 2q(3n - 2q + 1) = -2\). The situation \(m = 1\) was dealt with above.

In order to eliminate the possibility that \(v = 3(m + 1)(n + 1)\), we first show that it implies \(b = q - 2\), or \(n = (q - 1)/3\) or \((q - 1)/4\), or \(m \leq 2\).

First suppose that \(a = 1\). By Proposition 3.1, we must have \(m \mid v - (q + 1)\). As \(v = 3(m + 1)(n + 1)\), this implies \(m \mid 3n + q + 2\). However, from (9), we obtain
and using inequality (4) of Proposition 2.1, it follows that \( q \equiv q - 1 \), \( n + 1 \) and therefore \( m | (q - 1)^2 - (q - 1)(3n + 1) \). Thus \( m | 3n - q + 4 \), finally yielding \( m | 2 \), which forces \( m \leq 2 \).

Now assuming that \( a \geq 2 \), we have \( b \leq q - 3 \). If \( b = q - 2 \), we are done. So suppose \( b \leq q - 3 \). Using (1) of Proposition 2.1 yields \( q n = b(n - m) + 3(m + 1)(n + 1) - 1 \leq (q - 3)(n - m) + 3(mn + n + m) + 2 \), implying \( m q \leq 3mn + 6m + 2 \), and so \( q \leq 3n + 6 + \frac{2}{m} \).

As we may assume \( m > 2 \), then \( q \leq 3n + 6 \), or \( n \geq (q - 6)/3 \). We proceed to determine precisely the possible values for \( n \).

Using (2) of Proposition 2.1, substituting for \( v \), and applying (3) of the proposition, we obtain \( 3(m + 1)(n + 1) + 3(bn + am) = (q - 1)^2 \). Using (1) and (3) then yields

\[
(q - 1)^2 - 3(q - 1)(n + 1) + 3(2mn + n + m + 1) = 0,
\]
a quadratic in \( q - 1 \). Therefore

\[
q - 1 = \frac{3(n + m) \pm \sqrt{9n^2 + 9m^2 - 6mn - 12n - 12m - 12}}{2}.
\]

(Note that (11) is independent of assumptions on \( m \) or \( n \).) Since \( n > m > 2 \), and using inequality (4) of Proposition 2.1, it follows that \( q - 1 > |3(n + m) + \sqrt{9n^2 + 9m^2 - 18mn - 12n + 12m + 4}|/2 = (3(n + m) + (3n - 3m - 2))/2 = 3n - 1 \), or \( q - 1 < 3n + 1 < 3\sqrt{q} + 1 \). In this latter case, \( q \leq 12 \). However, \( 3 | q^2 + q + 1 \) implies \( q \neq 8, 9, 11, 12 \), and no projective plane of order 10 exists (see Lam, Thiel, and Swiercz [16]). Thus this case is eliminated. Consequently, \( n < q/3 \). Again, \( q \equiv 1(\text{mod} 3) \), since \( 3 | q^2 + q + 1 \), and thus \((q - 6)/3 \leq n < q/3 \) implies \( 3n = q - 1 \) or \( q - 4 \).

We proceed to eliminate each of the above cases.

Suppose \( m = 1 \). Substituting in (11) gives \((q - 1)^2 - 3(q - 1)(n + 1) + 3(3n + 2) = 0 \), so \((q - 1)^2 - 3(q - 1)(n + 1) + 9(n + 1) = 3 \). The fact that \( 3 | q^2 + q + 1 \) again gives \( 3 | q - 1 \), and so 9 divides the left-hand side but not the right, a contradiction.

Suppose \( m = 2 \). Using (11) again yields \( 3n = [(q - 6)(q - 2) + 4]/(q - 6) = q - 2 + \frac{4}{q - 6} \). Since this must be an integer, \( q \geq 8 \) and the fact that no projective plane of order 10 exists give a contradiction.

Suppose \( 3n = q - 1 \). Substituting in (11) gives \( 9n^2 - 9n(n + m) + 6mn + 3n + 3m + 3 = 0 \). This forces \( n = 1 + 2/(m - 1) \), which is not possible.

Suppose \( 3n = q - 4 \). So \( q - 1 = 3(n + 1) \), and (11) yields the impossibility \( n(m - 4) = 2(2 - m) \).

We finally consider the case \( b = q - 2 \). Using (1) and (3) of Proposition 2.1, we get \( a = 2 \) and \( v = 3(m + 1)(n + 1) = 1 + 2n + (q - 2)m \), and it follows that \( q = 3n + 5 + \frac{n + 2}{m} \), whence \( m \mid n + 2 \).

Fix a line of size \( n + 1 \) in \( S \). Each of its points is on a second line of this size since \( a = 2 \). Thus the number of lines of this size in \( S \) is at least \( n + 2 \). However, counting the precise number in two ways produces \( \frac{n + 2}{m - 1} \) lines of size \( n + 1 \) or \( 6(m + 1) \). Thus \( n + 2 \leq (6(m + 1)) \). If \( m \geq 6 \), then \( n + 2 \leq 7n \), and we may set \( n + 2 = x m + 2 \leq x \leq 7 \).

From above, \( q = 3x m + x - 1 \). Substituting for \( q \) in (2) in Proposition 2.1 implies

\[
(3x m + x - 1)^2 + 3x m + x = 3(m + 1)(x m - 1) + 3(3x m + x - 3)(x m - 1) + 6(m + 1).
\]

This reduces to \( 3m(2mx - x^2 - 4x + 1) + 12 = (x + 1)^2 \leq 64 \), which implies \( m(2mx - x^2 - 4x + 1) \leq 17 \). If \( m \geq 6 \), then \( 2mx - x^2 - 4x + 1 \leq 2 \), or \( 2(m - x - 4) \leq 1 \). It follows that \( 2m - x - 4 \leq 0 \), which contradicts \( m \geq 6 \).
It remains only to dispose of the cases $m = 3, 4, 5$. We return to the equation $3m(2nx - x^2 - 4x + 1) + 12 = (x + 1)^2$. For $m = 3$, this becomes $5x^2 - 8x - 10 = 0$, which implies $2 \mid x$ and then $4 \mid 10$, a contradiction. For $m = 4$, it becomes $13x^2 - 46x - 23 = 0$, implying $23 \mid x$ and then $(23)^2 \mid 23$, a contradiction. Finally, for $m = 5, 8x^2 + 44x - 13 = 0$ implies the contradiction $2 \mid 3$. \[ \square \]

In attempting to generalize Theorem 4.2 to $q^2 + q + 1$, a product of distinct primes, we have had only partial success. We summarize this in the next result.

**Proposition 4.3.** Let $\Pi$ be a projective plane of order $q \geq 2$ such that $q^2 + q + 1 = p'p$, $p'$, and $p$ both prime, with $p' < p$. Let $S$ be a blocking semioval in $\Pi$ of type $(1, m + 1, n + 1)$. Then $p \not| (m + 1)(n + 1)$; and if $p'|(m + 1)(n + 1)$, then $p'$ divides both $m + 1$ and $n + 1$, or $p'|a$ or $p'|b$.

**Proof.** If $p|(m + 1)(n + 1)$, then $p|m + 1$ or $p|n + 1$ while both of $m + 1$ and $n + 1$ are less than $q$, and $p$ must be bigger than $q$.

Suppose $p'|(m + 1)(n + 1)$. Again, $p'|m + 1$ or $p'|n + 1$. If $p'|m + 1$, set $m + 1 = (p')^a x, p' \not| x, a \geq 1$. So by (2) of Proposition 2.1, $(p')^{a+1} px(n + 1) = v((p')^a x(n + 1) + a(p')^a x + b(n + 1))$, which implies $p'|b(n + 1)$. We may assume $p'|b$ and $p'|n + 1$. Then $p'|v$. Set $v = (p')^d y, p' \not| y, \beta \geq 1$, and $y < p$. So $\alpha + 1 \geq \beta$ and $(p')^{\alpha-\beta+1} px(n + 1) = y(p')^a x(n + 1) + a(p')^a x + b(n + 1))$. If $\alpha - \beta + 1 > 0$, then $p'|y(b(n + 1))$, a contradiction. So $\alpha - \beta + 1 = 0$. Then $px(n + 1) = y((m + 1)(n + 1) + a(m + 1) + b(n + 1))$ and $y < p$ gives $x(n + 1) > (n + 1)(m + 1 + b) + a(m + 1)$, so that $x > m + 1 + b$, which contradicts $x < m + 1$.

If we now suppose that $p'|n + 1$, the argument is completely analogous and introduces only the last possibility that $p'|a$. \[ \square \]

Before leaving this section, we make two observations: first, we look at the case where $m = 1$. Second, noting that no blocking semioval of our type can have size $q\sqrt{q} + 1$, we address the next possibility in a square order plane, i.e., $v = q\sqrt{q}$.

**Proposition 4.4.** Let $\Pi$ be a projective plane of order $q \geq 7$ containing a blocking semioval $S$ of type $(1, 2, n + 1)$ with $n > 1$. Then the $(n + 1)$-secants to $S$ form a dual blocking set, and consequently there are between $q + \sqrt{q} + 1$ and $q^2 - \sqrt{q}$ of them.

**Proof.** No point of $\Pi$ exterior to $S$ is only on tangents to $S$, as this would force $S$ to have exactly $q + 1$ points, which is too small to be a blocking set by Bruen [8]. Nor is any such point only on 2-secants, as this would imply $v = 2q + 2$, giving by (2) of Proposition 2.1, $2(n + 1)(q^2 + q + 1) = 2(q + 1)[2(n + 1) + 2a + b(n + 1)]$. Since $(q^2 + q + 1) = 1$, we obtain $q + 1|n + 1$ while $n + 1 \leq q - 1$. Similarly, if an exterior point is only on $(n + 1)$-secants, then $v = (n + 1)(q + 1)$, and this same equation results in $2(q^2 + q + 1) = (q + 1)[2(n + 1) + 2a + b(n + 1)]$, a contradiction.

Let an exterior point be on $x$ 2-secants and $y$ tangents and assume it is on no $(n + 1)$-secants. Then $2x + y = v$ and $x + y = q + 1$. So $x = v - (q + 1)$ and $y = 2(q + 1) - v \geq 0$. Dover [13] shows that any blocking semioval satisfies $v \geq 2(q + 1)$ for $q \geq 7$. This forces us to have $v = 2q + 2$, which was eliminated in the previous paragraph.

Hence every point lies on at least one $(n + 1)$-secant, and the first paragraph shows no point is only on $(n + 1)$-secants. Therefore the $(n + 1)$-secants form a dual blocking set and the result follows from Bruen [8]. \[ \square \]

Blokhuis and Metsch [4, Theorem 1.2] show that for $q \geq 49$ and square, a semioval on $q\sqrt{q}$ points must be part of a unital and hence cannot be a blocking set. Specializing to the case of semiovals of type $(1, m + 1, n + 1)$, we can generalize this result to the following proposition.

**Proposition 4.5.** Let $\Pi$ be a projective plane of square order $q \geq 2$. Then $\Pi$
contains no blocking semioval of type \((1, m + 1, n + 1), 1 \leq m < n,\) on \(q\sqrt{q}\) points.

Proof. Applying (2) of Proposition 2.1, \((m + 1)(n + 1)(q^2 + q + 1) = q\sqrt{q}[(m + 1)(n + 1) + b(n + 1) + a(m + 1)]\) and \((q\sqrt{q}, q^2 + q + 1) = 1\) implies \(q\sqrt{q}[(m + 1)(n + 1)\) by inequality (5) of Proposition 2.1, and equality results in the triangle \(m = 2, n = q - 2,\) and so \(3(q - 1) = q\sqrt{q}\) that yields \(q|3,\) which is impossible.

Blokhuis and Metsch [4, Theorems 1.3 and 1.4] also consider \(v = q\sqrt{q} - 1,\) proving that if the point/tangent incidences of \(S\) are the point/tangent incidences of a unital, and if \(q \geq 25,\) then \(S\) is indeed part of a unital or a minimal blocking set. If the plane is Desarguesian, only the former of these can hold.

5. Conclusion. We have given a number of conditions which constrain the possible parameters of a blocking semioval with three intersection numbers; while these conditions have eliminated many possibilities, the remaining cases seem very difficult to work with. Indeed, we conjecture that there are no blocking semiovals with three intersection numbers other than the triangle and the sporadic example when \(q = 7.\)

On a more optimistic note, we suspect that some of the remaining sporadic cases may be attackable. For instance, the parameters \((56, 2, 8, 5, 20)\) for a blocking semioval of our type in a plane of order 25 could be analyzed. Indeed, a cursory analysis shows that if such a semioval were to exist, it would imply the existence of a blocking set of size 35 and type \((1, 2, 5)\) in that plane. It is not known if such a set can exist.

One pattern which our data indicates is that in a projective plane of order \(q,\) where \(q^2 + q + 1\) is the product of two distinct primes, the parameter set of the triangle is the only arithmetically feasible parameter set for that order. Proposition 4.3, summarizing our results in this direction, inclines us to believe this conjecture is true.

As a final comment, we note that if \(q = 2^{2k+1}\) for \(1 \leq k \leq 5,\) the only arithmetically feasible parameter sets for a semioval of our type are those of the triangle. We conjecture that this is true for all \(k \geq 1.\)

Acknowledgment. The authors would like to thank the referee for many useful suggestions and particularly for suggesting the method of proof used in Proposition 3.2.

REFERENCES
