A Collection of
MTA–ELTE GAC manuscripts

Daniele Bartoli, György Kiss, Stefano Marcugini, Fernanda Pambianco

ON THE SPECTRUM OF SIZES OF SEMIOVALS CONTAINED IN THE HERMITIAN CURVE

2014

MTA–ELTE Geometric and Algebraic Combinatorics Research Group

Hungarian Academy of Sciences
Eötvös University, Budapest
MANUSCRIPTS
On the spectrum of sizes of semiovals contained in the Hermitian curve

Daniele Bartoli† György Kiss‡
Stefano Marcugini§ and Fernanda Pambianco†

Abstract

Some constructions and bounds on the sizes of semiovals contained in the Hermitian curve are given. A construction of an infinite family of 2-blocking sets of the Hermitian curve is also presented.

1 Introduction

Let $\Pi_q$ be a finite projective plane of order $q$ and let $\text{PG}(2,q)$ denote the Desarguesian projective plane over the finite field of $q$ elements, $\mathbb{F}_q$. A semioval $S$ in $\Pi_q$ is a non-empty pointset with the property that for every point $P \in S$ there exists a unique line $t_P$ such that $S \cap t_P = \{P\}$. This line is called the tangent line to $S$ at $P$. The classical examples of semiovals arise from polarities (ovals and unitals), and from the theory of blocking sets. The semiovals are interesting objects in their own right, but the study of semiovals is also motivated by their applications to cryptography.

Batten constructed in [3] an effective message sending scenario which uses determining sets. She showed that blocking semiovals (that is semiovals intersecting each line of $\Pi_q$ in at least one point) are a particular type of determining sets in projective planes.

A semioval (which is also a blocking semioval) existing in every projective plane of order $q > 2$ is the vertexless triangle, the set of points formed by the union of three non-concurrent lines with the points of intersections removed.

†The author acknowledges the support of the European Community under a Marie-Curie Intra-European Fellowship (FACE project: number 626511).
‡The research was supported by the Hungarian National Foundation for Scientific Research, Grant NN 114614.
§The research was supported by the Italian MIUR (progetto 40% “Strutture Geometriche, Combinatoria e loro Applicazioni”), and by GNSAGA-INdAM.

1
It is known that if $S$ is a semioval in $\Pi_q$ then $q + 1 \leq |S| \leq q \sqrt{q} + 1$ and both bounds are sharp [17, 24]; the extremes occur when $S$ is an oval or a unital. In particular in $\text{PG}(2, q)$ a conic has $q + 1$ points and if $q$ is a square then a Hermitian curve has $q \sqrt{q} + 1$ points. A survey on results about semiovals can be found in [18].

In the last years the interest and research on the fundamental problem of determining the spectrum of the values for which there exists a given subconfiguration of points in $\text{PG}(n, q)$ have increased considerably (see for example [1, 2, 16, 19, 21]). For $q \leq 9$, $q$ odd, the spectrum of sizes of semiovals was determined by Lisoněk [20] by exhaustive computer search. Kiss, Marcugini, and Pambianco [19] extended Lisoněk’s results to the cases $q = 11$ and 13.

There are many known constructions and theoretical results about semiovals, in particular those that either contain large collinear subsets in which case their size is close to the lower bound, or their size is close to the upper bound. In the latter case Kiss, Marcugini and Pambianco [19] constructed semiovals by careful deletion of points from a unital. If $q$ is an odd square then they gave explicit examples of semiovals of size $k$ for all $k$ satisfying the inequalities $q(\sqrt{q} + 1)/2 \leq k \leq q \sqrt{q} + 1$ and they proved existence if $q[4 \log q] + 1 \leq k \leq q \sqrt{q} + 1$ holds. The unital they started from was originally constructed by Szőnyi [23]. It is a pencil of superosculating conics which is also a minimal blocking set. Later on, Dover and Mellinger gave the complete characterization of semiovals from unions of conics [8].

More recently, constructions of semiovals with size roughly $q \sqrt{q}/2$, that is far from both the upper and lower bound, appeared in the literature; see [9, 10].

Our goal in this paper is to give similar constructions and estimates on the sizes of semiovals coming from the classical unital, the Hermitian curve. The main result is an explicit construction of semiovals of size $k$ for all $k$ satisfying the inequalities $2q \sqrt{q} + 4q - 2\sqrt{q} - 3 \sqrt{q} + 1 \leq k \leq q \sqrt{q} + 1$ if $q = s^4$ and odd (see Corollary 2.10). We also present explicit examples for other values of $q$ and prove the existence of semiovals of size $k$ for $q$ odd if $(q - \sqrt{q} + 1) \left(\frac{4(\sqrt{q} + 1)}{\sqrt{q} - 1} \log q\right) \leq k \leq q \sqrt{q} + 1$. If $q$ is large enough, then this gives a slight improvement on the previously known bound for almost all $q$. Our main tools are the application of proper blocking sets of the Hermitian curve constructed by Blokhuis et al. [4] and the decomposition of the Hermitian curve into a union of $(q - \sqrt{q} + 1)$-arcs, originally given by Seib [22], see in English in [12].

Finally, in the last section, we present a construction of an infinite family of 2-blocking sets of the Hermitian curve.
2 Explicit constructions of semiovals

For the sake of convenience from now on we work in the Desarguesian planes $\text{PG}(2,q^2)$. In this section we construct various examples of semiovals in $\text{PG}(2,q^2)$ arising from the points of the Hermitian curve $\mathcal{H}_q$. This curve has $q^3 + 1$ points, there is a unique tangent line to $\mathcal{H}_q$ at each of its points and each of the other $q^4 - q^3 + q^2$ lines of $\text{PG}(2,q^2)$ is a $(q + 1)$-secant of $\mathcal{H}_q$. A pointset $\mathcal{D} \subset \mathcal{H}_q$ is called a 2-blocking set if each $(q+1)$-secant contains at least 2 points of $\mathcal{D}$. For a detailed description of $\mathcal{H}_q$ we refer to [14].

For $q = 2, 3$ we performed an exhaustive computer search and the situation is the following. In $\text{PG}(2,4)$, semiovals contained in the Hermitian curve exist only of sizes 6, 8, 9: this means that Theorem 2.1 gives the complete spectrum of semiovals contained in the Hermitian curve for $q = 2$. The spectrum of the sizes of semiovals contained in the Hermitian curve of $\text{PG}(2,9)$ and the number of inequivalent examples (up to collineations) are presented in Table 1.

Our first, obvious construction does not depend on the parity of $q$.

**Theorem 2.1.** Let $q \geq 2$. In $\text{PG}(2,q^2)$ there exists a semioval $\mathcal{S} \subset \mathcal{H}_q$ of size $k$ for all $k \in \{q^3 - q^2 + q\} \cup [q^3 - q^2 + q + 2, q^3 + 1]$.

**Proof.** Let $P$ be a point in $\mathcal{H}_q$ and $\ell_1, \ell_2, \ldots, \ell_{q-1}$ be $(q + 1)$-secants through $P$. Let $\mathcal{T} = \bigcup_{i=1}^{q-1} \ell_i$. Then $\mathcal{H}_q \setminus \mathcal{T}$ is a semioval of size $q^3 - q^2 + q$ because if $\ell$ is a $(q+1)$-secant of $\mathcal{H}_q$ then we either deleted all of its points, or at most $q-1$ of its points. Hence no former secant line becomes a tangent line to $\mathcal{H}_q \setminus \mathcal{T}$, and there is exactly one tangent line at each point of $\mathcal{H}_q \setminus \mathcal{T}$, then $\mathcal{H}_q \setminus \mathcal{T}$ is a semioval of size $q^3 - q^2 + q$. Also, we can add $k \in [2, q^2 - q + 1]$ points from $\mathcal{T}$ in a way that no other tangent lines are created. In fact, it is sufficient to control that in each line $\ell_1, \ell_2, \ldots, \ell_{q-1}$ the number of added points is different from 1. This is always possible since $k \neq 1$.

In particular, for $q = 3$, Theorem 2.1 provides the existence of semiovals of sizes 21, 23–28; see also Table 1.

For the constructions we need the following elementary observations.
Proposition 2.2. Let $S$ be a semioval. Suppose that the pointset $T \subset S$ has the property that if $\ell$ is a secant line to $S$ then the inequality $|S \cap \ell| \geq |T \cap \ell| + 2$ holds. Then $S \setminus T$ is a semiowal and $S$ contains semiowals of size $k$ for all $k$ satisfying the inequalities $|S \setminus T| \leq k \leq |S|$.

Proof. Let $R$ be a point of $S \setminus T$. Then the tangent to $S$ at $R$ is obviously a tangent to $S \setminus T$ at $R$. We have to prove that no new tangents appear after the deletion of points of $T$. But if a line $\ell$ meets $S$ in more than one point, then

$$|(S \setminus T) \cap \ell| = |S \cap \ell| - |T \cap \ell| \geq 2.$$ 

Thus no former secant line becomes tangent line to $S \setminus T$, so it is a semiowal.

Let $|S \setminus T| = k_0$. If $U$ is any subset of $k - k_0$ points of $T$ then $(S \setminus T) \cup U \subset S$ is a semiowal of size $k$. \hfill \Box

Corollary 2.3. Let $B$ be a 2-blocking set of $H_q$. Then in PG$(2, q^2)$ there exist semiowals of size $k$ for all $k$ satisfying the inequalities $|B| \leq k \leq q^3 + 1$.

Proof. The set $T = H_q \setminus B$ satisfies the condition of Proposition 2.2. \hfill \Box

The next two algebraic constructions work for all $q$, but the lower bound for the size depends on the parity of $q$. We use the following description of $H_q \subset$ PG$(2, q^2)$. The curve $H_q$ is defined by the equation

$$X_2X_0^q + X_2^qX_0 + X_1^{q+1} = 0.$$  \hfill (1)

Let $c \in \mathbb{F}_{q^2}$ be a fixed root of the equation $c^q + c + 1 = 0$. Consider the set

$$M = \{m \in \mathbb{F}_{q^2} \mid m^q + m = 0\},$$  \hfill (2)

then the points of $H_q$ are

$$\{(1 : u : cu^{q+1} + m) \mid u \in \mathbb{F}_{q^2}, m \in M\} \cup \{(0 : 0 : 1)\}.  \hfill (3)$$

If $q$ is an odd prime power then let $h$ be a fixed non-square in $\mathbb{F}_q$ and consider $\mathbb{F}_{q^2} = \mathbb{F}_q[i]$ where $i^2 = h$. Then $i^q + i = 0$, $i^q = i^q$ and $i^{q+1} = -h$.

If $q$ is even then let $h \in \mathbb{F}_q$ be an element with $\text{Tr}_{\mathbb{F}_{q}/\mathbb{F}_2}(h) = 1$. Let $i$ satisfy $i^2 + i + h = 0$, and consider $\mathbb{F}_{q^2} = \mathbb{F}_q[i]$. Then $i^q + i = 1$, $i^q = i + h$ and $i^{q+1} = h$.

For all $q$ we represent the elements $x$ of $\mathbb{F}_{q^2}$ as $x = x_1 + ix_2$ where $x_1, x_2 \in \mathbb{F}_q$.  

4
Theorem 2.4. Let \( v \in \mathbb{F}_q \), \( q \geq 3 \), be a fixed element and
\[
T_v = \{(1, u + iv, c(u + iv)^{q+1} + m) : u \in \mathbb{F}_q, m \in M, m \neq 0\}
\]
bear a subset of points in \( \mathcal{H}_q \). The lines through \((0 : 0 : 1)\) meet \( T_v \) in either 0 or \( q-1 \) points, and all other lines meet \( T_v \) in at most 2 points.

Proof. Here we consider \( \mathbb{F}_q^2 = \mathbb{F}_q[i] \). It is clear that a line through \((0 : 0 : 1)\) contains either 0 or \( q-1 \) points of \( \mathcal{T} \). Let \( \ell \) be a line not containing \((0 : 0 : 1)\). First note that the equation of \( \ell \) can be written as \( \alpha X_0 + \beta X_1 + X_2 = 0 \). We claim that \( \ell \) contains at most two points of \( T_v \). First consider the case \( q \) odd. The condition \( u, v \in \mathbb{F}_q \) implies that \((u + iv)^{q+1} = u^2 - hv^2\), thus the points of \( T_v \) can be written as \((1 : u + iv : c(u^2 - hv^2) + m)\), too. If the point \((1 : u + iv : c(u^2 - hv^2) + m)\) is on \( \ell \) then \( \alpha + \beta(u + iv) + c(u^2 - hv^2) + m = 0 \). Rearranging this, we get
\[
m = -cu^2 - \beta u - \alpha - 3ivc + chv^2 \quad \text{and} \quad m^q = -c^3u^2 - \beta^3u - \alpha^3 + 3ivc + c^3hv^2.
\]
But \( m \) satisfies the condition \( m^q + m = 0 \) hence
\[
-(c^3 + c)u^2 - (\beta^3 + \beta)u - \alpha^3 - \alpha + (\beta^3 - \beta)iv + (c^3 + c)hv^2 = 0. \tag{4}
\]
If \( q \) is even then we get a similar equation. The condition \( u, v \in \mathbb{F}_q \) now implies that \((u + iv)^{q+1} = u^2 + uv + hv^2\), thus the points of \( T_v \) can be written as \((1 : u + iv : c(u^2 + uv + hv^2) + m)\). If the point \((1 : u + iv : c(u^2 + hv^2) + m)\) is on \( \ell \) then
\[
m = cu^2 + (\beta + cv)u + \alpha + 3ivc + chv^2 \quad \text{and} \quad m^q = c^3u^2 + (\beta^3 + c^3v)u + \alpha^3 + 3ivc + c^3hv^2 + c^3h^2v.
\]
But \( m \) satisfies the condition \( m^q + m = 0 \) hence
\[
(c^3 + c)u^2 + (\beta^3 + \beta + (c^3 + c)v)u + \alpha^3 + \alpha + (\beta^3 + \beta)iv + \beta^3v + (c^3 + c)hv^2 = 0. \tag{5}
\]
The coefficient of \( u^2 \) in Equations (4) and (5) is 1 since \( c^3 + c + 1 = 0 \). So these are quadratic equations on \( u \), each of them has at most two roots. Hence \( \ell \) contains at most 2 points of \( T_v \). \( \square \)

Theorem 2.5. If \( q \geq 3 \) then in \( \text{PG}(2, q^2) \) there exists a semioline \( S \subset \mathcal{H}_q \) of size \( k \) for all \( k \) satisfying the inequalities
\[
q^3 + 1 \geq k \geq \begin{cases} 
q^3 - 2q^2 + 4q + 1 & \text{if } q \text{ is even}, \\
q^3 - 2q^2 + 5q - 2 & \text{if } q \text{ is odd}.
\end{cases}
\]
Proof. Take the subset
\[ \mathcal{T} = \{ (1 : u : cv^{q+1} + m) \mid u \in \mathbb{F}_q, m \in M, m \neq 0 \} \] (6)
corresponding to the choice \( v = 0 \) in Theorem 2.4. Note that \( |\mathcal{T}| = q(q-1) \). By Proposition 2.2 and Theorem 2.4, \( \mathcal{U} = \mathcal{H}_q \setminus \mathcal{T} \) is a semiomal. When \( q = 3 \), this semiomal has size \( q^3 - q^2 + q + 1 = 22 \), which equals \( q^3 - 2q^2 + 5q - 2 \), proving the result in this case. From now on we assume \( q > 3 \)

In the second step we get smaller semiomals by careful deletion of points of \( \mathcal{U} \).

Let \( M = \{ 0, m_1, \ldots, m_{q-1} \} \) and for \( j = 1, 2, \ldots, q - 1 \) let \( \ell_j \) be the line with equation \( X_2 = (c+m_j)X_0 \). Then \( \ell_j \) passes on the point \( (0 : 1 : 0) \). Consider the lines \( \ell^\alpha \) having equation \( X_1 = \alpha X_0 \).

The point \( \ell^\alpha \cap \ell_j \) has coordinates \( (1 : \alpha : c + m_j) \), thus it belongs to \( \mathcal{T} \) if and only if \( \alpha \in \mathbb{F}_q \) and \( \alpha^{q+1} = 1 \) hold simultaneously. It happens if and only if \( \alpha^2 = 1 \), hence \( \ell_j \) contains \( q - 1 \) or \( q \) points of \( \mathcal{H}_q \setminus \mathcal{T} \) if \( q \) is odd or even, respectively. Consider \( \mathcal{V} = \bigcup_{j=1}^{q-1} \ell_j \) and let \( \mathcal{S}_0 = \mathcal{U} \setminus \mathcal{V} \).

Each \( (q+1) \)-secant of \( \mathcal{H}_q \) not through \( (0 : 0 : 1) \) contains at most two points of \( \mathcal{T} \) and \( q - 3 \) points of \( \mathcal{V} \) hence it is not a tangent to \( \mathcal{S}_0 \). Lines \( \ell^\alpha \) through \( (0 : 0 : 1) \), with \( \alpha \in \mathbb{F}_q \), contains \( 2 \) points of \( \mathcal{S}_0 \), whereas if \( \alpha \not\in \mathbb{F}_q \) then \( \ell^\alpha \) contains at least \( (q+1) - (q-3) = 4 \) points of \( \mathcal{S}_0 \). Then \( \mathcal{S}_0 \) is a semiomal.

The size of \( \mathcal{S}_0 \) is \( q^3 - q^2 + q + 1 - (q-1)(q-3) = q^3 - 2q^2 + 5q - 2 \) if \( q \) is odd and \( q^3 - q^2 + q + 1 - q(q-3) = q^3 - 2q^2 + 4q + 1 \) if \( q \) is even. Note that, contrary to Theorem 2.1, we can add also one point to \( \mathcal{S}_0 \); in fact it is sufficient to add a point of \( \mathcal{T} \setminus \mathcal{V} \) and the new set is still a semiomal. \( \square \)

In particular, Theorem 2.5 provides a semiomal of size 22 for \( q = 3 \) and semiomals of size 49 – 65 for \( q = 4 \).

**Theorem 2.6.** If \( q > 2 \) then in \( \text{PG}(2,q^2) \) there exists a semiomal \( \mathcal{S} \subset \mathcal{H}_q \) of size \( k \) for all \( k \) satisfying the inequalities

\[
q^3 + 1 \geq k \geq \begin{cases} 
\frac{q^3 + q^2 - q + 2}{3} & \text{if } q \text{ is odd}, \\
\frac{q^3 + 3q^2 - 2q + 2}{2} & \text{if } q \text{ is even}.
\end{cases}
\]

Proof. Let \( v_1, v_2, \ldots, v_{(q-1)/2} \) be distinct elements of \( \mathbb{F}_q \) and let \( \mathcal{T} = \bigcup_{j=1}^{(q-1)/2} \mathcal{T}_{v_j} \), where \( \mathcal{T}_{v_j} \) is defined as in Theorem 2.4. We show that \( \mathcal{S}_0 = \mathcal{H}_q \setminus \mathcal{T} \) is a semiomal.

Because of Proposition 2.2 it is enough to prove that any \( (q+1) \)-secant of \( \mathcal{H}_q \) contains at most \( q - 1 \) points of \( \mathcal{T} \). This is obvious if a line does not contain the point \( P \) because in this case it contains at most two points from each set \( \mathcal{T}_{v_j} \). Consider the lines through the point \( P = (0 : 0 : 1) \). The line \( X_0 = 0 \) is the tangent to \( \mathcal{H}_q \) at \( P \), while a line \( \ell^\alpha \) having equation \( X_1 = \alpha X_0 \) meets \( \mathcal{T}_{v_j} \) in
points whose second coordinate is \( \alpha \). Thus \( \ell^a \) contains \( q - 1 \) points of \( \mathcal{T}_v \) if \( (\alpha - iv) \in \mathbb{F}_q \) and no points of \( \mathcal{T}_v \) if \( (\alpha - iv) \notin \mathbb{F}_q \).

The size of \( \mathcal{S}_0 \) is \( q^3 + 1 - q(q - 1)^2/2 \) if \( q \) is odd and \( q^3 + 1 - q(q - 1)(q - 2)/2 \) if \( q \) is even. Thus the theorem follows from Proposition 2.2.

Theorem 2.6 provides for \( q > 4 \) a better bound with the respect to Theorems 2.1 and 2.5, whereas for \( q = 3 \) and \( q = 4 \) Theorems 2.1 and 2.5 are better.

If \( q - 1 \) has suitable divisors then we can construct smaller semioids than in Theorem 2.5. We distinguish the cases \( q \) even and \( q \) odd.

First let \( q \) be an odd prime power. The following lemma due to Blokhuis et al. [4] gives information on the irreducibility of a particular plane curve.

**Lemma 2.7** ([4], Lemma 4.5). Let \( q \) be odd. If \( n_1^2 \neq 2d_1 + hn_2 \) then the algebraic curve in \( \text{PG}(2, q) \) defined as

\[
X_{\text{odd}} : 2n_1 X_0^r X_2^r + 2hn_2 X_1 X_2^{2r-1} + 2d_1 X_2^{2r} + X_0^2 + hX_1^2 X_2^{2r-2} = 0
\]

is absolutely irreducible and it has genus \( g = r - 1 \).

If \( q \) is even then a similar lemma holds.

**Lemma 2.8** ([4], page 14). Let \( q \) be even. If \( n_1^2 \neq n_1n_2 + hn_2 + d_2 \) then the algebraic curve in \( \text{PG}(2, q) \) defined as

\[
X_{\text{even}} : (n_1 + n_2)X_1X_2^{2r-1} + n_2X_0^r X_2^r + d_2X_2^{2r} + X_0^2 + X_0^r X_1 X_2^{r-1} + hX_1^2 X_2^{2r-2} = 0
\]

is absolutely irreducible and it has genus \( g \leq r - 1 \).

Using these lemmas, Blokhuis et al. [4] constructed a blocking set of \( \mathcal{H}_q \). With a slight modification of their proof we can prove the existence of a family of semioids contained in the Hermitian curve.

**Theorem 2.9.** Let \( q \) be a prime power and \( r \) be a divisor of \( q - 1 \) for which \( r < \frac{q^2}{2} \) holds. Then in \( \text{PG}(2, q^2) \) there exists a semioid \( \mathcal{S} \subset \mathcal{H}_q \) of size \( k \) for all \( k \) satisfying the inequalities

\[
\left( q + \frac{(q - 1)q}{r} \right)(q - 1) + q^2 + 1 \leq k \leq q^3 + 1.
\]

**Proof.** The equation of \( \mathcal{H}_q \) is the same

\[
X_2X_0^q + X_2^qX_0 + X_1^{q+1} = 0
\]
as in the previous proof, but we use another description of its points.

The point \( X_\infty = (1 : 0 : 0) \) is on \( \mathcal{H}_q \) and the line \( \ell_\infty : X_2 = 0 \) is the tangent to \( \mathcal{H}_q \) at \( X_\infty \). Choose \( \ell_\infty \) as line at infinity and consider \( \text{PG}(2, q^2) \) as the union of \( \text{AG}(2, q^2) \) and \( \ell_\infty \). Let \( \mathcal{U} \) be the affine part of \( \mathcal{H}_q \). Then the equation of \( \mathcal{U} \) is

\[
X^q + X + Y^{q+1} = 0.
\]  

(10)

The tangent to \( \mathcal{H}_q \) at the affine point \((a, b)\) has equation \( X = -b^qY - a^q \). Thus a non-horizontal affine line \( X = nY + d \) is a tangent to \( \mathcal{H}_q \) if and only if \( n^{q+1} = d^q + d \).

Take the following pointset

\[
\mathcal{B} = \{(x, y, 1) : (x, y) \in \mathcal{U} \mid y = u^r + iv, u, v \in \mathbb{F}_q \} \cup \{(1 : 0 : 0)\} \subset \mathcal{H}_q.
\]

(11)

For all \( u, v \in \mathbb{F}_q \) the horizontal affine line with equation \( Y = y_0 \), with \( y_0 = u^r + iv \) for some \( u, v \in \mathbb{F}_q \), contains \( q \) affine points of \( \mathcal{B} \). If \( y_0 \neq u^r + iv \) for any \( u, v \in \mathbb{F}_q \) then the other horizontal lines \( Y = y_0 \) do not contain any affine point of \( \mathcal{B} \). There is exactly one point of the line \( \ell_\infty \) in \( \mathcal{B} \). Thus \( \mathcal{B} \) consists of \( \left( q + \frac{(q-1)q}{r} \right) q + 1 \) points.

First consider the case \( q \) odd. Let \( \ell \) be a non-horizontal affine line with equation \( X = nY + d \). Let \( n = n_1 + in_2 \) and \( d = d_1 + id_2 \) where \( n_1, n_2, d_1, d_2 \in \mathbb{F}_q \). Then

\[
\ell \cap \mathcal{B} = \{(x, y) \in \mathcal{U} \mid y = u^r + iv, 2n_1u^r + 2hn_2v + 2d_1 + u^{2r} - hv^2 = 0, u, v \in \mathbb{F}_q \}.
\]

Thus affine points \((x, u^r + iv)\) of \( \mathcal{B} \) on the line \( \ell \) correspond to points of the curve having affine equation

\[
A_{\text{odd}} : \quad 2n_1U^r + 2hn_2V + 2d_1 + U^{2r} - hV^2 = 0.
\]

This curve is the affine part of the curve \( \mathcal{X}_{\text{odd}} \) in \( \text{PG}(2, q) \). Suppose that \( \ell \) is not a tangent line to \( \mathcal{U} \). Then \( n^{q+1} \neq d^q + d \). It holds if and only if \( n_1^2 \neq 2d_1 + hn_2^2 \). So in this case by Lemma 2.7, \( \mathcal{X}_{\text{odd}} \) is absolutely irreducible and its genus is equal to \( r - 1 \).

If \( q \) is even and \( \ell \) is a non-horizontal affine line with equation \( X = nY + d \), \( n = n_1 + in_2 \) and \( d = d_1 + id_2 \) where \( n_1, n_2, d_1, d_2 \in \mathbb{F}_q \) then

\[
\ell \cap \mathcal{B} = \{(x, y) \in \mathcal{U} \mid y = u^r + iv, n_2u^r + (n_1 + n_2)v + d_2 + u^{2r} + u^rv + hv^2 = 0, u, v \in \mathbb{F}_q \}.
\]

Thus affine points \((x, u^r + iv)\) of \( \mathcal{B} \) on the line \( \ell \) correspond to points of the curve having affine equation

\[
A_{\text{even}} : \quad n_2U^r + (n_1 + n_2)V + d_2 + U^{2r} + U^rV + hV^2 = 0.
\]
This curve is the affine part of the curve \( X_{\text{even}} \) in PG(2, q). Suppose that \( \ell \) is not a tangent line to \( U \). Then \( n^{d+1} \neq d^3 + d \). It holds if and only if \( n_1^2 \neq n_1 n_2 + h n_2^2 + d_2 \). So in this case by Lemma 2.8, \( X_{\text{even}} \) is absolutely irreducible and its genus is at most \( r - 1 \).

For all \( q \), the Hasse-Weil bound implies that each of the curves \( X_{\text{odd}} \) and \( X_{\text{even}} \) has at least \( q + 1 - 2(r - 1)/\sqrt{q} \) points in PG(2, q). Both curves have a unique point at infinity, \((0 : 1 : 0)\), so each curve contains at least \( q + 1 - 2(r - 1)/\sqrt{q} - 1 \) affine points. Now consider the points of the curves \( A_{\text{odd}} \) and \( A_{\text{even}} \).

We claim that if \( B = (x, u^r + iv) \) is an affine point of \( \ell \cap B \) then there are at most \( r \) affine points on \( A_{\text{odd}} \) (or \( A_{\text{even}} \)) corresponding to \( B \). If two points \( A_1 = (u_1, v_1) \) and \( A_2 = (u_2, v_2) \) on the curve correspond to \( B \) then \( u^r = u_1^r = u_2^r \) and \( v = v_1 = v_2 \) hold. If \( u = 0 \) then these equations imply \( A_1 = A_2 \), while in the case \( u \neq 0 \) we get \( u_1 = \epsilon_1 u \) and \( u_2 = \epsilon_2 u \) where \( \epsilon_1 \) and \( \epsilon_2 \) are \( r \)-th roots of unity in \( \mathbb{F}_q \). The points \( A_1 \) and \( A_2 \) are distinct if and only if \( \epsilon_1 \neq \epsilon_2 \). Thus there at most \( r \) affine points of the curves corresponding to a given point of \( \ell \cap B \). Hence \( \ell \cap B \) contains at least

\[
\frac{(q + 1 - (2r - 2)/\sqrt{q}) - 1}{r}
\]

points, and by the assumption on \( r \) this number is greater than 2. Thus the set \( \ell \cap B \) contains at least two points.

All horizontal lines pass through \((1 : 0 : 0) \in B \). Since no horizontal line is a tangent line to \( U \), it is sufficient to add one point for each of the lines with equation \( Y = y_0 \), \( y_0 \neq u^r + iv \) for any \( u, v \in \mathbb{F}_q \), to extend \( B \) to a 2-blocking set of \( H_q \). Let \( S_0 \) be the set obtained from \( B \) by adding these extra points. Then the size of \( S_0 \) is

\[
\left( \frac{q + (q - 1)q}{r} \right) q + 1 + \left( q^2 - \frac{q + (q - 1)q}{r} \right) = \left( q + \frac{(q - 1)q}{r} \right) (q - 1) + q^2 + 1.
\]

Now the theorem follows from Corollary 2.3. \( \square \)

The lower bound on the size of the semiroll in Theorem 2.9 depends on the divisor \( r \) of \( q - 1 \). The greater \( r \) the smaller the size of \( S_0 \), but the method works only if \( r < \sqrt{q}/2 \) holds. Note that if we take \( r = 1 \) in Theorem 2.9 then the semiroll obtained is just the Hermitian curve itself. If \( 1 < r \) then the condition \( r < \sqrt{q}/2 \) implies \( q > 16 \).

Also, if \( q \) is even or odd, then sometimes \( q - 1 = p \) or \( q - 1 = 2p \), respectively, where \( p \) is a prime number. Hence there is no \( r \neq 1 \) (e.g. in the cases \( q = 32, 128 \)) or the best possible value is
$r = 2$ (e.g. in the cases $q = 23, 27$). In the case $r = 2$ Theorem 2.9 gives semiovals of sizes

$$\frac{q^3 + 2q^2 - q + 2}{2} \leq k \leq q^3 + 1.$$  

This is the same as the result of Theorem 2.6.

The situation is much better if $q$ is an odd square. In the case $q = s^2$, $s$ odd, one can always choose $r = (s - 1)/2$: this is the greatest possible divisor of $q - 1$ satisfying the condition $r < \sqrt{q}/2$. In this case Theorem 2.9 has the following

**Corollary 2.10.** Let $q$ be an odd square. Then in $\text{PG}(2, q^2)$ there exists a semioval $S \subset \mathcal{H}_q$ of size $k$ for all $k$ satisfying the inequalities

$$2q^2 \sqrt{q} + 4q^2 - 2q \sqrt{q} - 3q + 1 \leq k \leq q^3 + 1.$$

If $q \geq 49$, then this extends the spectrum of sizes of constructed semiovals in $\text{PG}(2, q^2)$ significantly, because previously the corresponding lower bound was $(q^3 + q^2)/2$ (see [19]).

If $q = s^2$, $s$ odd and $t > 2$ then $r = s - 1$ is always a possible choice. In this case the size of the smallest semioval we get is roughly $q^2 \sqrt{q^{t-1}}$.

3 The proof of existence of smaller semiovals

If $q$ is odd then we can prove the existence of much smaller semiovals using a theorem about dominating sets of bipartite graphs. Let $A$ and $B$ be the two vertex subsets of a bipartite graph.

We say that a vertex $v \in B$ dominates the subset $S \subset A$, if for any $s \in S$ there is an edge between $v$ and $s$. A subset $B' \subset B$ is a dominating set, if for any $a \in A$ there exists $b' \in B'$ which dominates $a$. The following lemma is due to S. K. Stein, the proof can be found e.g. in [13].

**Lemma 3.1.** Let $A$ and $B$ be the two vertex subsets of a bipartite graph. Denote by $d$ the minimum degree in $A$. If $A$ has at least two elements, then there is a set $B' \subset B$ dominating the vertices of $A$ with

$$|B'| \leq \left\lceil \frac{|B| \log(|A|)}{d} \right\rceil,$$

where $\log$ denotes natural base logarithm.

**Theorem 3.2.** Let $q \geq 27$ be odd and $k$ be an integer satisfying

$$(q^2 - q + 1) \left\lceil \frac{8(q + 1)}{q - 1} \log q \right\rceil \leq k \leq q^3 + 1,$$

10
where \( \log \) denotes the natural base logarithm. Then \( \text{PG}(2, q^2) \) contains semirows of size \( k \).

Proof. First note that \( (q^2 - q + 1) \frac{8(q+1)}{q-1} \log q \leq q^3 + 1 \) if and only if \( q \geq 27 \). The Hermitian curve \( \mathcal{H}_q \) is the disjoint union of \( q + 1 \ (q^2 - q + 1) \)-arcs. Let \( \mathcal{C} = \{ \mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{q+1} \} \) denote the set of these arcs. If \( P \) is a point of \( \mathcal{H}_q \) that belongs to \( \mathcal{C}_i \), then the set of the \( q + 1 \) tangents to \( \mathcal{C}_i \) at \( P \) contains the unique tangent to \( \mathcal{H}_q \) at \( P \), while each of the remaining \( q \) lines is a tangent to exactly one different element of \( \mathcal{C} \); see [4, page 10]. Thus any bisecant of \( \mathcal{C}_i \) is a tangent to either 0 or 2 other arcs from \( \mathcal{C} \), hence is a bisecant of \( (q - 1)/2 \) or \( (q + 1)/2 \) elements of \( \mathcal{C} \).

We define a bipartite graph with two vertex subsets \( A \) and \( B \). Let the vertices in \( B \) be the \( (q^2 - q + 1) \)-arcs giving the decomposition of \( \mathcal{H} \), and the vertices in \( A \) be those lines that are not tangents to \( \mathcal{H}_q \). Let \( a \in A \) and \( b \in B \) be joined if and only if the corresponding line is a bisecant of the corresponding arc. Then \( |B| = q + 1 \), \( |A| = q^2 - q^3 + q^2 \) and \( d = (q - 1)/2 \). Hence from Lemma 3.1 we get that there exists \( B' \subset B \) dominating \( A \), and

\[
|B'| \leq \left| A \right| \frac{\log(|A|)}{d} = \left( q + 1 \right) \frac{\log(q^2 - q^2 + q^2)}{(q - 1)/2} \leq \left( \frac{8(q+1)}{q-1} \log q \right).
\]

Thus there exists a subset of \( \left[ \frac{8(q+1)}{q-1} \log q \right] \) arcs of \( \mathcal{C} \) such that each secant of \( \mathcal{H}_q \) meets the union of these arcs \( \mathcal{V} \) in at least two points. Hence \( \mathcal{V} \) is a semirow of size

\[
k_0 \leq (q^2 - q + 1) \left[ \frac{8(q+1)}{q-1} \log q \right]. \tag{12}
\]

If \( k_0 \leq k \leq q^3 + 1 \) then Corollary 2.3 guarantees the existence of a semirow of size \( k \).

In [19] it was proved that there exist semirows of sizes greater than

\[
q^2 \left[ \frac{8q}{q + 1} \log q \right] + 1. \tag{13}
\]

The bound (12) is smaller than the bound (13) for infinitely many \( q \). In fact, this happens when

\[
\left[ \frac{8q}{q + 1} \log q \right] = \left[ \frac{8(q+1)}{q-1} \log q \right].
\]

Let \( e = \lfloor \log q \rfloor \) and \( f = \log q - \lfloor \log q \rfloor \). The previous equality is satisfied whenever

\[
\frac{e}{q} \leq f < \frac{q-1}{8(q+1)} - \frac{2e}{q+1}.
\]
If $q$ is large enough, then $\frac{\varepsilon}{q} = \epsilon$, with $\epsilon$ close to zero, and $\frac{q^{-1}}{8(q+1)} - \frac{2\epsilon}{q+1}$ is greater than $1/9$. Therefore, for all $q$ such that

$$\epsilon \leq \log q - |\log q| < \frac{1}{9},$$

our bound is better than the previously known (the smallest prime power satisfying this condition is $q = 137$).

## 4 2-blocking sets of the Hermitian curve

In this section we present a construction of an infinite family of 2-blocking sets of the Hermitian curve which is a modification of the construction of 1-blocking sets of the Hermitian curve presented in [10]. (I meant the equation (10), but perhaps is some clear in this way) The Hermitian curve we use has affine equation

$$X^q + X + Y^{q+1} = 0.$$

### Proposition 4.1

Let $q$ be an odd prime power and $r$ be a divisor of $q - 1$ such that $1 < r < \frac{\sqrt{q} - 2\log_2 q + 1}{4}$. Then there exists a 2-blocking set of the Hermitian curve for some value of $k$ satisfying the inequalities

$$\frac{q^3 - 3q^2 - 2q}{r} + 2q^2 - q + 2 - 2[\log_2 q + 1] \leq k \leq \frac{q^3 - 3q^2 - 2q}{r} + 2q^2 + q + 2 + 2[\log_2 q + 1].$$

**Proof.** Recall that $\mathcal{U}$ is defined by $X^q + X + Y^{q+1} = 0$. Let $\mathcal{B}$ be defined by

$$\mathcal{B} = \{(x, y, 1) : (x, y) \in \mathcal{U} \mid y = u^r + iv, u, v \in \mathbb{F}_q \} \cup \{(1 : 0 : 0)\} \subset \mathcal{H}_q.$$

As in Theorem 2.9 it is possible to prove that each non-horizontal line, which is not a tangent line of the Hermitian curve, intersects $\mathcal{B}$ in at least $2^{q - 1 - (2r - 2)\sqrt{q}}$ and in at most $2^{q - 1 + (2r - 2)\sqrt{q}}$ points. The horizontal lines are either blocked only by $(1 : 0 : 0)$ or their intersection with $\mathcal{H}_q$ is fully contained in $\mathcal{B}$. Consider a $(q^2 - q + 1)$-arc $\mathcal{C}$ through $(1 : 0 : 0)$ contained in $\mathcal{U}$. Among the $q^2$ horizontal lines through $(1 : 0 : 0)$, $q$ of them intersect $\mathcal{C}$ only in $(1 : 0 : 0)$, while the other $q^2 - q$ contain an extra point of $\mathcal{C}$ other than $(1 : 0 : 0)$. Consider

$$\mathcal{B} := (\mathcal{B} \Delta \mathcal{C}) \cup \{(1 : 0 : 0)\},$$

where $\Delta$ indicates the symmetric difference of the two sets. The set $\mathcal{B}$ still blocks all the non-horizontal lines and they are not completely contained in $\mathcal{B}$, since on each of these lines at most
two points are deleted from $B$ or added to $B$. Also, at most $q$ horizontal lines, namely the $q$
unisection lines to $C$ through $(1 : 0 : 0)$, either intersect $\overline{B}$ only in $(1 : 0 : 0)$ or their intersection
with $H_q$ is fully contained in $\overline{B}$.

Consider $C_1, \ldots, C_{q+1}$ the $(q^2 - q + 1)$-arcs partitioning $\mathcal{U}$ and let $\ell_1, \ldots, \ell_k$ be $k \leq q$
horizontal lines. There exists at least a $(q^2 - q + 1)$-arc $C_i$ contained in $\mathcal{U}$ intersecting at least $\frac{k}{2}$
of such lines. On the contrary, suppose that all the $(q^2 - q + 1)$-arcs contained in $\mathcal{U}$ intersect at most
$\frac{k}{2} - 1$ of such lines. Then, each arc contains at most $k - 2$ points of $\mathcal{U} \cap (\ell_1 \cup \cdots \cup \ell_k)$. Since
$\mathcal{U} \cap (\ell_1 \cup \cdots \cup \ell_k) = kq + 1$, then there should exist at least $\frac{kq + 1}{k/2} > q + 1$ of such arcs contained in
$\mathcal{U}$ and pairwise disjoint. This is a contradiction.

Arguing as before, we can prove that, given $k$ horizontal lines, there exist at most $\lfloor \log_2 k + 1 \rceil$
arcs among $C_1, \ldots, C_{q+1}$ such that their union intersects all the $k$ lines. Note that in this case each
of these lines contains at most $2\lfloor \log_2 k + 1 \rceil$ points from the union of the $(q^2 - q + 1)$-arcs.

Let $\ell_1, \ldots, \ell_{k_1}$ and $r_1, \ldots, r_{k_2}$ be the horizontal lines intersecting $\overline{B}$ only in $(1 : 0 : 0)$ and in $q + 1$
points, respectively. From above we know that $k_1 + k_2 \leq q$. Let $C_{i_1}, \ldots, C_{i_{j_1}}$, $j_1 = \lfloor \log_2 k_1 + 1 \rceil$, be
the $(q^2 - q + 1)$-arcs intersecting $\ell_1, \ldots, \ell_{k_1}$ and let $C_{h_{i_2}}, \ldots, C_{h_{j_2}}$, $j_2 = \lfloor \log_2 k_2 + 1 \rceil$, be the
$(q^2 - q + 1)$-arcs intersecting $r_1, \ldots, r_{k_2}$. In particular, let
\[
\mathcal{B}_1 := (\ell_1 \cup \cdots \cup \ell_{k_1}) \cap (C_{i_1}, \ldots, C_{i_{j_1}})
\]
and
\[
\mathcal{B}_2 := (r_1 \cup \cdots \cup r_{k_2}) \cap (C_{h_{i_2}}, \ldots, C_{h_{j_2}}).
\]
We have that $|\mathcal{B}_1| \leq 2\lfloor \log_2 k_1 + 1 \rceil$ and $|\mathcal{B}_2| \leq 2\lfloor \log_2 k_2 + 1 \rceil$. The set
\[
\overline{B} = (\overline{B} \setminus \mathcal{B}_2) \cup \mathcal{B}_1 \cup \{(1 : 0 : 0)\}
\]
intersects each horizontal line in at least two and in at most $q$ points. Also, since a non-horizontal line $\ell$
intersects $\overline{B}$ in $t$ points, where
\[
2\lfloor \log_2 q + 1 \rceil + 2 < \frac{q - 1 - (2r - 2)\sqrt{q}}{r} \leq t \leq \frac{q - 1 + (2r - 2)\sqrt{q}}{r} < q - 2\lfloor \log_2 q + 1 \rceil,
\]
then $\ell$ intersects $\overline{B}$ in $\overline{t}$ points, where
\[
2 < \frac{q - 1 - (2r - 2)\sqrt{q}}{r} \leq \overline{t} \leq \frac{q - 1 + (2r - 2)\sqrt{q}}{r} < q.
\]
This proves that $\overline{B}$ is a 2-blocking set of the Hermitian curve not containing any block of it.
Finally, note that the size of $\mathcal{B}$ is $\left( q + \frac{(q-1)q}{r} \right) q + 1$ and that the points of $\mathcal{B}$ lie on $s = q + \frac{q(q+1)}{r}$ horizontal lines. Therefore the size of $\bar{\mathcal{B}}$ satisfies

$$\left( q + \frac{(q-1)q}{r} \right) q + 1 + (q^2 - q - 2s + 1) \leq |\bar{\mathcal{B}}| \leq \left( q + \frac{(q-1)q}{r} \right) q + 1 + (q^2 + q - 2s + 1).$$

To obtain $\bar{\mathcal{B}}$ we add or delete at most $2\lceil \log_2 q + 1 \rceil$ points. So,

$$\left( q + \frac{(q-1)q}{r} \right) q + 1 + (q^2 - q - 2s + 1) - 2\lceil \log_2 q + 1 \rceil \leq |\bar{\mathcal{B}}| \leq \left( q + \frac{(q-1)q}{r} \right) q + 1 + (q^2 + q - 2s + 1) + 2\lceil \log_2 q + 1 \rceil.$$

\hfill \Box

5 Conclusions

In this paper we collected many constructions of semi-ovals arising from the points of a Hermitian curve in $\text{PG}(2, q^2)$. We summarize the results in Table 2, whereas Table 3 shows the situation for $4 \leq q \leq 9$. Finally, by exhaustive computer searches we found the spectrum of semi-ovals contained in the Hermitian curve for $q = 2$ (6, 8, 9) and $q = 3$ (12, 15, 16, 18 – 28).

6 Acknowledgements

The authors would like to thank the anonymous referees for carefully reading the manuscript and suggesting important improvements in Section 2.

References


Table 2: Existence results for semiovals contained in the Hermitian curve

<table>
<thead>
<tr>
<th>Condition</th>
<th>Bound</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$q \geq 2$</td>
<td>$k \in {q^3 - q^2 + q} \cup [q^3 - q^2 + q + 2, q^3 + 1]$</td>
<td>Theorem 2.1</td>
</tr>
<tr>
<td>$q \geq 3$</td>
<td>$q^3 + 1 \geq k \geq \begin{cases} \frac{q^3}{2} - 2q^2 + 4q + 1 &amp; \text{if } q \text{ is even,} \ \frac{q^3}{2} - 2q^2 + 5q - 2 &amp; \text{if } q \text{ is odd.} \end{cases}$</td>
<td>Theorem 2.5</td>
</tr>
<tr>
<td>$q \geq 3$</td>
<td>$q^3 + 1 \geq k \geq \begin{cases} \frac{q^3 + 2q^2 - q + 2}{2} &amp; \text{if } q \text{ is odd,} \ \frac{q^3 + 3q^2 - 2q + 2}{2} &amp; \text{if } q \text{ is even.} \end{cases}$</td>
<td>Theorem 2.6</td>
</tr>
<tr>
<td>$q \geq 17$ odd</td>
<td>$2q^2 \sqrt{q} + 4q^2 - 2q \sqrt{q} - 3q + 1 \leq k \leq q^3 + 1$</td>
<td>Corollary 2.10</td>
</tr>
<tr>
<td>$q \geq 27$</td>
<td>$(q^2 - q + 1) \left\lceil \frac{8(q+1)}{q-1} \log q \right\rceil \leq k \leq q^3 + 1$</td>
<td>Theorem 3.2</td>
</tr>
</tbody>
</table>

Table 3: Spectrum for $4 \leq q \leq 9$

<table>
<thead>
<tr>
<th>$q$</th>
<th>Existing semiovals</th>
<th>References</th>
<th>Spectrum</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>50, 52 – 65</td>
<td>Theorem 2.1</td>
<td>49 – 65</td>
</tr>
<tr>
<td></td>
<td>49 – 65</td>
<td>Theorem 2.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>53 – 65</td>
<td>Theorem 2.6</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>102, 104 – 126</td>
<td>Theorem 2.1</td>
<td>86 – 126</td>
</tr>
<tr>
<td></td>
<td>98 – 126</td>
<td>Theorem 2.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>86 – 126</td>
<td>Theorem 2.6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>301, 303 – 344</td>
<td>Theorem 2.1</td>
<td>218 – 344</td>
</tr>
<tr>
<td></td>
<td>278 – 344</td>
<td>Theorem 2.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>218 – 344</td>
<td>Theorem 2.6</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>456, 458 – 513</td>
<td>Theorem 2.1</td>
<td>345 – 513</td>
</tr>
<tr>
<td></td>
<td>417 – 513</td>
<td>Theorem 2.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>345 – 513</td>
<td>Theorem 2.6</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>648, 650 – 730</td>
<td>Theorem 2.1</td>
<td>442 – 730</td>
</tr>
<tr>
<td></td>
<td>610 – 730</td>
<td>Theorem 2.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>442 – 730</td>
<td>Theorem 2.6</td>
<td></td>
</tr>
</tbody>
</table>


Daniele Bartoli
Department of Mathematics,
Ghent University,
Krijgslaan 281, 9000 Ghent, Belgium
e-mails: dbartoli@cage.ugent.be

György Kiss
Department of Geometry and MTA-ELTE Geometric and Algebraic Combinatorics Research Group
Eötvös Loránd University
1117 Budapest, Pázmány s. 1/c, Hungary
e-mail: kissgy@cs.elte.hu

Stefano Marcugini and Fernanda Pambianco
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia
Via Vanvitelli 1, 06123 Perugia, Italy
e-mails: stefano.marcugini@unipg.it, fernanda.pambianco@unipg.it