# Blocking sets of the Hermitian unital

A. Blokhuis, A. E. Brouwer, D. Jungnickel, V. Krčadinac,
S. Rottey, L. Storme, T. Szőnyi, and P. Vandendriessche

October 18, 2013

**Abstract**

It is known that the classical unital arising from the Hermitian curve in $\mathrm{PG}(2,9)$ does not have a 2-coloring without monochromatic lines. Here we show that for $q \geq 4$ the Hermitian curve in $\mathrm{PG}(2,q^2)$ does possess 2-colorings without monochromatic lines. We present general constructions and also prove a lower bound on the size of blocking sets in the classical unital.

## 1 Introduction

In any point-line geometry (or, much more generally, any hypergraph) a *blocking set* is a subset $B$ of the point set that has nonempty intersection with each line (or each edge).

Blocking sets in the finite projective planes $\mathrm{PG}(2,q)$ have been investigated in great detail [17, 18]. Since in a projective plane any two lines meet, every set containing a line is a blocking set. A blocking set of a projective plane is called *non-trivial* or *proper* when it does not contain a line. We shall also call blocking sets in other point-line geometries *proper* when they do not contain a line. By definition the complement of a proper blocking set is again one, and every 2-coloring (vertex coloring with two colors such that no line is monochromatic) provides a complementary pair of proper blocking sets.

A blocking set is *minimal* when no proper subset is a blocking set. A blocking set in $\mathrm{PG}(2,q)$ is *small* when its size is smaller than $3(q+1)/2$.

This latter definition was motivated by the important results of Sziklai and Szőnyi, who proved a 1 (mod $p$) result for small minimal blocking sets $B$ in $\mathrm{PG}(2,q)$.

**Theorem 1.1** (Sziklai and Szőnyi [17, 18]). *Let $B$ be a small minimal blocking set in $PG(2,q)$, $q = p^h$, $p$ prime, $h \geq 1$. Then $B$ intersects every line in* $1 \pmod{p}$ *points.*

*If $e$ is the largest integer such that $B$ intersects every line in* $1 \pmod{p^e}$ *points, then $e$ is a divisor of $h$, and every line of $PG(2,q)$ that intersects $B$ in exactly $1+p^e$ points intersects $B$ in a subline $PG(1,p^e)$.*

In this note we investigate blocking sets in the classical unital $\mathcal{U}$ arising from the Hermitian curve $\mathcal{H}(2,q^2)$ of $\mathrm{PG}(2,q^2)$. The lines of the unital are the intersections with $\mathcal{U}$ of projective lines that meet $\mathcal{U}$ in at least 2 (and then precisely $q+1$) points.

This research is in part motivated by [1], where an exhaustive search for the unitals of order 3 containing proper blocking sets was performed. That search showed that there are 68806 distinct 2-$(28,4,1)$ unital designs containing a proper blocking set. The classical unital, arising from the Hermitian curve in $\mathrm{PG}(2,9)$, does not contain a proper blocking set. This poses the question of blocking sets in the Hermitian curves $\mathcal{H}(2,q^2)$ of $\mathrm{PG}(2,q^2)$ for general $q$.

A second motivation is given by the Shift-Blocking Set Problem discussed in §1.1 below.

We show that for $q \geq 4$, the Hermitian curves $\mathcal{H}(2,q^2)$ contain proper blocking sets. We present general constructions of (proper) blocking sets and also prove a lower bound on the size. The lower bound is obtained via the polynomial method, and makes use of a $1 \pmod{p}$ result which arises from the applied techniques.

## 1.1 Green-black colorings

Let a proper green-black coloring of the plane $\mathrm{PG}(2,n)$ be a coloring of the points with the colors green and black such that every point $P$ is on a line $L$ that is completely green, with the possible exception of the point $P$ itself. At least how many green points must there be, or, equivalently, at most how many black points? This question is related to the Flat-Containing and Shift-Blocking Set Problem [5].

By definition, every black point is on a tangent, that is, a line containing no further black point. This immediately gives the upper bound $n^{3/2}+1$ for the number of black points ([12]).

In order to find examples close to this bound, let $n = q^2$, and let $\mathcal{U}$ be the set of points (of size $q^3 + 1$) of a classical unital in $\mathrm{PG}(2, n)$, and let $B$ be a blocking set in $\mathcal{U}$. Then we can take $\mathcal{U} \setminus B$ as the set of black points, while the points of $B$, and all points outside $\mathcal{U}$, are green. Indeed, for a point $P$ of the unital, we can take for $L$ the tangent at $P$. For a point $P$ outside, the line $M = P^{\perp}$ meets $\mathcal{U}$ in a line of $\mathcal{U}$ that is blocked by $B$ in a (green) point $Q$, and we can take for $L$ the (entirely green) tangent line at $Q$.

This motivates the search for small blocking sets in $\mathcal{U}$. In fact what is needed here is something slightly more general. Let us call a subset $S$ of $\mathcal{U}$ *green* when $\mathcal{U} \setminus S$ can be taken as the set of black points in a proper green-black coloring. Then blocking sets of the unital are green. As we shall see, there are also other green sets.

## 1.2 Small $q$

Let $\min_g(q)$, $\min_b(q)$ and $\min_{pb}(q)$ be the sizes of the smallest green set, blocking set and proper blocking set, respectively, in the unital $\mathcal{U}$ of $\mathrm{PG}(2, q^2)$. Clearly $\min_g(q) \le \min_b(q) \le \min_{pb}(q)$. For small $q$ we have the following

| $q$ | $\min_g(q)$ | $\min_b(q)$ | $\min_{pb}(q)$ |
|---|---|---|---|
| 2 | 3 | 5 | - |
| 3 | 10 | 13 | - |
| 4 | 15 | 25 | 26 |

That is, the unital does not have a proper blocking set for $q = 2, 3$, and for $q = 4$ there are proper blocking sets, but the smallest blocking sets contain a line. A green set that does not contain a (unital) line is a blocking set. The smallest green sets contain lines.

We describe the green examples. Note that a subset $S$ of $\mathcal{U}$ is green precisely when for each non-tangent line $L$ disjoint from $S$, the nonisotropic point $L^{\perp}$ lies on a non-tangent line $M$, where $M \cap \mathcal{U} \subseteq S$.

For $q = 2$ the unital is an affine plane $\mathrm{AG}(2, 3)$. Pick for $S$ an affine line. The two parallel lines have perps that lie on this line.

For $q = 3$, let $P$ be a point of the unital, and let $K, L, M$ be three unital lines on $P$ without transversal. Then $S = K \cup L \cup M$ has size 10 and is green.

For $q = 4$, let $P, Q, R$ be an orthogonal basis: three mutually orthogonal nonisotropic points. The three lines $PQ$, $PR$ and $QR$ meet $\mathcal{U}$ in $5{+}5{+}5 = 15$ points, and one checks that this 15-set is green.

Let $\min_{ip}(q)$ be the size of the smallest blocking set of the Miquelian inversive plane of order $q$ (the $S(3, q+1, q^2+1)$ formed by the points and circles on an elliptic quadric in $\mathrm{PG}(3, q)$). Below we shall see that $\min_b(q) \leq q(\min_{ip}(q) - 1) + 1$. For small $q$ we have

| $q$ | 2 | 3 | 4 | 5 | 7 | 8 |
|---|---|---|---|---|---|---|
| $\min_{ip}(q)$ | 3 | 5 | 8 | 10 | 17 | 20 |

.

## 2 A lower bound on the size of a blocking set of the Hermitian curve

Consider $\mathrm{PG}(2, q^2)$. We denote the points by $(x : y : z)$ and the lines by $[t : u : v]$, where the point $(x : y : z)$ and the line $[t : u : v]$ are incident when $tx + uy + vz = 0$.

The map $(x : y : z) \mapsto [z^q : y^q : x^q]$ defines a unitary polarity. Points of the associated unital $\mathcal{U}$ are the points $(x : y : z)$ satisfying $(x : y : z)I[z^q : y^q : x^q]$, so $xz^q + y^{q+1} + zx^q = 0$. The tangents of $\mathcal{U}$ are the lines $[t : u : v]$ satisfying the same equation, so $tv^q + u^{q+1} + vt^q = 0$.

The 'infinite horizontal' point $\infty := (1 : 0 : 0)$ belongs to $\mathcal{U}$. Its pole $\infty^\perp$, the tangent to $\mathcal{U}$ in $\infty$, is the line $[0 : 0 : 1]$, i.e., the line 'at infinity' $Z = 0$.

We wish to block the lines of the unital, i.e., the subsets of size $q + 1$ of $\mathcal{U}$ that are of the form $\ell \cap \mathcal{U}$ for some line $\ell$ of $\mathrm{PG}(2, q^2)$. The main result of this section is a lower bound for the size of a blocking set.

**Theorem 2.1.** *Let $S$ be a blocking set of a Hermitian unital $\mathcal{U}$ in $PG(2, q^2)$, then $|S| \geq (3q^2 - 2q - 1)/2$.*

If a subset of $\mathcal{U}$ blocks all projective lines, then also the tangents, and hence the subset must be all of $\mathcal{U}$ (and have size $q^3+1$). Also, $\mathcal{U} \cap \infty^\perp = \{\infty\}$. Therefore our result follows immediately from the following.

**Theorem 2.2.** *Let $S$ be a minimal set of points of $PG(2, q^2)$ that blocks all projective lines that are not tangent to $\mathcal{U}$, but not all projective lines. If $S \cap \infty^\perp = \{\infty\}$, then $|S| \geq (3q^2 - 2q - 1)/2$.*

For example, let $L$ be a secant line to $\mathcal{U}$ containing $\infty$. Let $P$ be a nonisotropic point of $L$. One may take for $S$ the set of all points of $L$ except $P$, together with some point on each of the $q^2 - q - 1$ other secant lines on $P$. Now $|S| = 2q^2 - q - 1$.

**Proof:** Since a unital point outside $S$ is on $q^2$ unital lines, $|S| \geq q^2$, and it is easy to see that equality cannot hold. Put $B := \{(a,b) \mid (a:b:1) \in S\}$ so that $|S| = |B| + 1$, and let $|B| = q^2 - q + k$.

**Part 1: Polynomial reformulation.**

The set $S$ is a blocking set of $\mathcal{U}$ if and only if the polynomial $H(U,V)$ defined by

$$H(U,V) = C(U,V)R(U,V) = (V^q + V + U^{q+1}) \prod_{(a,b)\in B} (V + a + bU)$$

(with $C(U,V) = V^q + V + U^{q+1}$) vanishes identically in $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$.

Indeed, a line is non-horizontal (does not pass through $\infty$) precisely when it is of the form $[1:u:v]$. Such a line is a tangent to $\mathcal{U}$ when $C(u,v) = 0$ and passes through the point $(a,b)$ when $a+bu+v = 0$. So if $S$ is a blocking set, then $H(u,v) = 0$ for all $u, v$. And conversely, if $H(u,v) = 0$ for all $u, v$ and $[1:u:v]$ is not a tangent, so that $C(u,v) \neq 0$, then $v + a + bu = 0$ for some $(a,b) \in B$, so that this line is blocked by $B$. We shall use later that the number of points of $S$ on the non-horizontal line $[1:u:v]$ (plus 1 if it is a tangent) equals the multiplicity of $v$ as a zero of $H(u,V)$.

Since $H(U,V)$ vanishes identically, it belongs to the ideal generated by $U^{q^2} - U$ and $V^{q^2} - V$, so

$$H(U,V) = C(U,V)R(U,V) = (V^{q^2} - V)f(U,V) + (U^{q^2} - U)g(U,V).$$

We may suppose that $|S| < 2q^2 - q$ (the lower bound we are proving is smaller), so that $H$ has degree smaller than $2q^2$. All terms involving $U^{q^2}$ in $f$ can be moved over to $g$. Then no cancellation occurs, and $f$ and $g$ have total degree at most $k+1$. Since $H$ has a term $U^{q+1}V^{q^2-q+k}$ that must be from $(V^{q^2} - V)f$, it follows that $f$ has degree precisely $k+1$. Since $\deg_V H = q^2 + k$, it follows that $\deg_V f = k$.

If $f$ and $g$ have a common factor $r(U,V)$, then the polynomial $H/r$ vanishes identically. If $r$ is linear, this means that we can delete a point from $S$ and find a smaller blocking set. If $r$ is not linear then it must equal $C$ (up to a constant factor) since $C$ is irreducible. This would mean that $S$ is a blocking set of the entire plane $\mathrm{PG}(2,q^2)$, contrary to our hypothesis. So $f$ and $g$ are coprime.

**Part 2:** *Let $u, v \in \mathbb{F}_{q^2}$. If $f(u,v) = 0$, then also $g(u,v) = 0$.*

For fixed $u \in \mathbb{F}_{q^2}$,

$$H(u,V) = C(u,V)R(u,V) = (V^{q^2} - V)f(u,V),$$

since $u^{q^2} - u = 0$. It follows that $v$ is (at least) a double root of $H(u,V)$. Since $C(u,V) = V^q + V + u^{q+1}$ has derivative 1, $v$ is at most single zero of $C(u,V)$. For each factor $r(U,V)$ of $H(U,V)$, if $v$ is a zero of $r(u,V)$, then $u$ is a zero of $r(U,v)$. It follows that $u$ is (at least) a double root of $H(U,v) = C(U,v)R(U,v) = (U^{q^2} - U)g(U,v)$, and hence $g(u,v) = 0$.

**Part 3:**

Observe that the nonzero polynomial $f(u,V)$ is fully reducible (factors into linear factors) over $\mathbb{F}_{q^2}$, for any $u \in \mathbb{F}_{q^2}$. Indeed, $(V^{q^2} - V)f(u,V) = C(u,V)R(u,V)$ and both $C(u,V)$ and $R(u,V)$ are fully reducible.

We apply the following lemma.

**Lemma 2.3.** ([4, p. 145]) *Let $h = h(X,Y)$ be a polynomial of total degree $d$ over $\mathbb{F}_q$ without nontrivial common factor with $\partial_Y h$. Let $M$ be the number of zeros of $h$ in $\mathbb{F}_q^2$, where each zero $(x,y)$ is counted with the multiplicity that $y$ has as zero of $h(x,Y)$. Then the total number of zeros of $h$ (each counted once) is at least $M - d(d-1)$.*

Let $f = f_0 \cdots f_m$ be the factorization of $f$ into irreducible components. Let $d_i = \deg(f_i)$ and $d_i' = \deg_V(f_i)$. Then $d_i' \le d_i$ and $d_0' + \cdots + d_m' = k$ and $d_0 + \cdots + d_m = k+1$. Hence, $d_i' = d_i - 1$ for a single component $f_i$, and $d_j' = d_j$ for $j \ne i$.

Suppose that $f$ has an irreducible factor $f_0$ with $\partial_V f_0 \ne 0$. Put $m := \deg f_0$ so that $1 \le m \le \deg f = k+1$, then $\deg_V(f_0) = m - \epsilon$, with $\epsilon \in \{0,1\}$, and $\epsilon = 0$ if $m = 1$.

Let $N$ be the number of zeros of $f_0$ in $\mathbb{F}_{q^2}^2$. On the one hand, since $f$ and $g$ have no common factor, and all zeros of $f$ are also zeros of $g$, Bézout gives $N \le \deg f_0 \deg g \le m(k+1)$. On the other hand, for any fixed $u \in \mathbb{F}_{q^2}$ the polynomial $f_0(u,V)$ of degree $\deg f_0 = m - \epsilon$ has $m - \epsilon$ zeros, counted with multiplicity, altogether $q^2(m-\epsilon)$. The Lemma now yields the lower bound $N \ge q^2(m-\epsilon) - m(m-1)$, and combining upper and lower bound yields

$$q^2(m-\epsilon) - m(m-1) \le m(k+1).$$

If $\epsilon = 0$ this gives $k \ge \frac{1}{2}(q^2-1)$. If $\epsilon = 1$ and $m > 2$ this gives $k \ge \frac{1}{2}(q^2-3)$. If $\epsilon = 1$ and $m = 2$ then no point was counted with multiplicity $> 1$, and

$q^2(m-\epsilon) \leq m(k+1)$ gives $k \geq \frac{1}{2}(q^2-2)$. Hence $|S| = q^2-q+1+k \geq \frac{1}{2}(3q^2-2q-1)$ in these cases, as desired.

If $\partial_V f_i = 0$ for all $i$, then $\partial_V f = 0$, so that $f(u,V)$ is a $p$-th power, and the multiplicity of $v$ as root of $H(u,V) = (V^{q^2}-V)f(u,V)$ is 1 (mod $p$). By an earlier remark, this means that all non-horizontal lines intersect the set $S$ in 1 (mod $p$) points if they are non-tangent, and in 0 (mod $p$) points if they are tangent.

For each affine point $P$, let the horizontal line on $P$ contain $e_P+1$ points of $S$ (including $\infty$). Summing the contributions of all lines on $P$ to $|S|$, we find from the tangents 0, and from the ($q^2-q-1$ or $q^2-1$) non-horizontal secants $-1$, and from the horizontal secant $e_P+1$ (all mod $p$), so that $|S| \equiv e_P$ (mod $p$) for all $P$. Summing the contributions of the horizontal lines we see $|S| \equiv 1$ (mod $p$). It follows that $e_P \equiv 1$ (mod $p$) and the point $\infty$ was not needed to block the horizontal lines. □

# 3 Small blocking sets

In this section we find small blocking sets of Hermitian curves, not necessarily proper. In the next section proper examples will be constructed.

## 3.1 Fractional covers

For blocking sets in general we can apply a bound of Lovász relating the minimum size of a blocking set (cover) $\tau$ and that of a fractional cover $\tau^*$ of a hypergraph with maximum degree $D$:

$$\tau \leq (1+\log D)\tau^*$$

(see [10], Corollary 6.29). For the unital $\mathcal{U}$, taking every point with weight $1/(q+1)$ gives us $\tau^* = q^2-q+1$, $D = q^2$, so $\tau \leq (q^2-q+1)(1+2\log q)$.

## 3.2 Geometric construction

Let $\mathcal{U}$ be the classical unital in $\mathrm{PG}(2,q^2)$, and consider a blocking set $B$ of $\mathcal{U}$ that is the union of a number of lines on a fixed point $p$ of $\mathcal{U}$. The line pencil $\mathcal{L}_p$ of the lines on $p$ in $\mathrm{PG}(2,q^2)$ has the structure of a projective line with distinguished element $L_\infty$, the tangent to $\mathcal{U}$ at $p$. For each unital line

$M$ not on $p$ the set $M_p = \{L \in \mathcal{L}_p \mid L \cap M \neq 0\}$ is a Baer subline of $\mathcal{L}_p$, and each Baer subline of $\mathcal{L}_p$ not containing $L_\infty$ arises in this way for $q$ pairwise disjoint lines $M$. We find $|B| = 1 + qm$, where $m$ is the size of a blocking set of the Baer sublines not on $L_\infty$ of the line $\mathcal{L}_p$.

The set $\mathcal{L}_p \setminus \{L_\infty\}$ carries the structure of an affine plane $\mathrm{AG}(2, q)$ of which the lines are the Baer sublines of $\mathcal{L}_p$ on $L_\infty$. The remaining Baer sublines form a system of circles. Any three noncollinear points determine a unique circle. Here we have $q^2(q-1)$ circles, each of size $q+1$, in a set of size $q^2$, and $D = q^2 - 1$, so Lovász' bound gives $m < q(1 + 2\log q)$. We did not lose anything (in the estimate) by taking $B$ of special shape.

Consider a blocking set $C$ of this collection of circles that is the union of a number of parallel lines. Then $|C| = qn$, where $n$ is the size of a blocking set for the collection of projections of the circles on a fixed line. We have $q(q-1)$ projections, each of size more than $q/2$, in a set of size $q$.

In order to block $N$ subsets of a $q$-set, each of size $> q/2$, one needs not more than $1 + \log_2 N$ points: if one picks the points of the blocking set greedily, each new point blocks at least half of the sets that were not blocked yet. So, we find a blocking set of size less than $1 + 2\log_2 q \sim 2.89 \log q$ and lost a factor 1.44 in the estimate.

# 4 Proper blocking sets of Hermitian curves

We now construct proper blocking sets of Hermitian curves.

## 4.1 Probabilistic constructions

Radhakrishnan and Srinivasan [14, Theorem 2.1] show using probabilistic methods that any $n$-uniform hypergraph with at most $0.1\sqrt{n/\log n}\, 2^n$ edges is 2-colorable, so contains a proper blocking set. (Their constant 0.1 can be improved to 0.7 for sufficiently large $n$.) In our case $n = q + 1$ and the number of edges is $q^4 - q^3 + q^2$, so a unital has a proper blocking set when $q > 17$.

An older bound by Erdős [7] gets the same conclusion when the number of edges is not more than $2^{n-1}$, and this applies when $q \geq 16$.

A result by Erdős and Lovász [8, Theorem 2] says that any $n$-uniform hypergraph in which each point is in at most $2^{n-1}/4n$ edges, is 2-colorable. In our case $n = q+1$ and each point is in $q^2$ edges, so this suffices for $q > 13$.

If we choose points for our blocking set at random with probability $p = 5(\log q)/q$, then the expected number of monochromatic edges is roughly $1/q < 1/2$, and now we can assume (just using Chebyshev's inequality) that in addition the size will be close to the expectation, so $5q^2 \log q$.

We now present two different geometric constructions.

## 4.2 A geometric construction

In this section we construct a proper blocking set in the classical unital $\mathcal{H}(2, q^2)$ in $\mathrm{PG}(2, q^2)$ for $q \geq 7$ and for $q = 4$.

We use the model of the unital from [3], [9], and [15]. A detailed description of this approach is also given in the survey paper [11].

Identify the points of the plane $\mathrm{PG}(2, q^2)$ with the elements of the cyclic group $G$ of order $q^4 + q^2 + 1$, where the lines are given by $D + a$, with $D$ a planar difference set, chosen in such a way that $D$ is fixed by every multiplier. Then $G = A \times B$, where $A$ is the unique subgroup of $G$ of order $q^2 - q + 1$ and $B$ is the unique subgroup of order $q^2 + q + 1$. We may now write elements of $G$ as pairs $g \equiv (i, j)$, $0 \leq g \leq q^4 + q^2$, $0 \leq i \leq q^2 - q$, $0 \leq j \leq q^2 + q$, $i \equiv g \pmod{q^2 - q + 1}$, and $j \equiv g \pmod{q^2 + q + 1}$. The subgroup $A$ and its cosets are arcs, while the subgroup $B$ and its cosets are Baer subplanes. The map $g \mapsto \mu g$, where $\mu = q^3$, maps the point $(i, j)$ onto the point $(-i, j)$. The map $g \mapsto D - \mu g$ defines a Hermitian polarity, with absolute points given by the Hermitian curve $\mathcal{U} = \{a + \beta \mid a \in A, 2\beta \in B \cap D\}$. So $\mathcal{U}$ is the union of $q + 1$ cosets of the subgroup $A$.

We will show that if $q$ is odd and $q \geq 7$, then it is possible to partition this collection of $q + 1$ cosets of $A$ into two sets of size $(q + 1)/2$ such that the union of each is a (proper) blocking set of the Hermitian unital $\mathcal{U}$.

Let $\ell \subset G$ be a line of the plane $\mathrm{PG}(2, q^2)$. Then $\ell$ intersects each coset of $A$ in 0, 1, or 2 points, since cosets of $A$ are $(q^2 - q + 1)$-arcs. The $q^2 - q + 1$ translates of $\ell$ by an element of $A$ all determine the same intersection pattern. The cosets of $B$ form a partition of the plane $\mathrm{PG}(2, q^2)$ into Baer subplanes $\mathrm{PG}(2, q)$, and $\ell$ intersects exactly one of these Baer subplanes in a Baer subline. By taking a suitable translate of $\ell$, we may assume that this Baer subplane is $B$ itself.

Since multiplication by $\mu$ sends the point $(i, j)$ to the point $(-i, j)$, this map fixes cosets of $A$ (setwise), and fixes $B$ pointwise. It follows that also the line $\ell$ is fixed (setwise) by multiplication by $\mu$. Consequently, $\ell$ intersects the cosets of $A$ containing a point of the subline $B \cap \ell$ in exactly one point, and the other cosets in 0 or 2 points.

The unital $\mathcal{U}$ is of the form $\mathcal{U} = A + \frac{1}{2}(B \cap D)$, and if $q$ is odd, then $\frac{1}{2}(B \cap D)$ is an oval in the Baer subplane $B$ [3, p. 65]. This means that the intersection pattern of $\ell$ with the $q+1$ cosets of $A$ that partition the unital $\mathcal{U}$ (let us call them $\mathcal{U}$-cosets of $A$) can be of three types.

If $\ell \cap B$ is a tangent of the oval $\frac{1}{2}(B \cap D)$, then $\ell$ is a tangent of the unital $\mathcal{U}$ as well, and so of no interest from the blocking set point of view. If $\ell \cap B$ is a secant line of the oval $\frac{1}{2}(B \cap D)$, then this means that $\ell$ intersects two $\mathcal{U}$-cosets of $A$ in a single point, and the remaining ones in 0 or 2 points, where both possibilities happen precisely $(q-1)/2$ times. Finally if $\ell \cap B$ is an external line of the oval $\frac{1}{2}(B \cap D)$, then $\ell$ intersects all $\mathcal{U}$-cosets of $A$ in 0 or 2 points, and both possibilities happen precisely $(q+1)/2$ times. There are $(q^2-q)/2$ external lines, and hence $(q^2-q)/2$ partitions of the set of $\mathcal{U}$-cosets of $A$ into two sets of size $(q+1)/2$ that do not lead to proper blocking sets of $\mathcal{U}$. If $\frac{1}{2}\binom{q+1}{(q+1)/2} > \frac{1}{2}(q^2-q)$, then there is a partition of $\mathcal{U}$ into two unions of $(q+1)/2$ cosets of the subgroup $A$, that are both blocking sets. This happens for $q \geq 7$.

If $q = 5$, then the 10 external lines determine 10 distinct triples of $\mathcal{U}$-cosets of $A$, no two disjoint, so we find blocking sets (of size 63) but no proper blocking sets in this way.

If $q$ is even, the situation is slightly different: in this case 2 is a multiplier that fixes both $B$ and $D$, and $\frac{1}{2}(B \cap D) = B \cap D$ is a line in $B$. Now for a line $\ell$ in the plane $\mathrm{PG}(2, q^2)$, such that $\ell \cap B$ is a line in the Baer subplane $B$, we have three possibilities: either $\ell = D$, with intersection pattern $1^{q+1}$, or $\ell$ is a tangent of $\mathcal{U}$, or $\ell$ has intersection pattern $1^1$, $0^{q/2}$, $2^{q/2}$. We now want to partition the unital $\mathcal{U}$ into collections of $q/2$ and $q/2+1$ cosets of $A$ to construct proper blocking sets of $\mathcal{U}$, and the only thing to avoid is to take a $q/2$-set corresponding to the 0's in the intersection pattern of a line $\ell$, so there are at most $q^2-1$ such $q/2$-sets, but $q^2 - 1 < \binom{q+1}{q/2}$ for $q \geq 8$.

If $q = 4$, then multiplication by 2 has two orbits on the $\mathcal{U}$-cosets of $A$, of sizes 2 and 3, and their unions form a complementary pair of proper blocking sets (of sizes 26 and 39).

So far we constructed proper blocking sets for $q > 3$, $q \neq 5$. For $q = 5$ the above method fails, but a random greedy computer search shows that $\mathcal{H}(2, 25)$ does contain disjoint blocking sets of sizes 45 and 51, so that there exist proper blocking sets of all sizes from 45 to 81.

We summarize the above discussion in the main theorem of this article.

**Theorem 4.1.** *The Hermitian curve $\mathcal{H}(2,q^2)$ contains a proper blocking set if and only if $q > 3$.*

**Remark 4.2.** The above arguments can also be used to show the existence of smaller proper blocking sets. We try to find a blocking set consisting of $r$ cosets of $A$, with $2r \leq q$ as small as possible (the complement will then automatically be a blocking set). We have $q^2$ intersection patterns, each with at most $(q+1)/2$ zero's, implying that at most $q^2\binom{(q+1)/2}{r}$ $r$-tuples are bad, so if $\binom{q+1}{r} > q^2\binom{(q+1)/2}{r}$ then we are fine, and this is certainly the case if $2^r \geq q^2$. This yields proper blocking sets of size $\frac{2\log q}{\log 2}(q^2-q+1)$, a little larger than the blocking sets we got from Lovász' bound.

## 4.3 Explicit examples

We now present a construction that yields explicit examples of proper blocking sets on the Hermitian curve.

**Theorem 4.3.** *Let $r|(q-1)$ where $r > 1$ and $4r^2+1 < q$. Then, for some value $k$ satisfying $1 \leq k \leq q^2-q+1$, the Hermitian curve $\mathcal{U}$ in $PG(2,q^2)$ contains a proper blocking set $B$ of size $k + q(q-1)^2/r$.*

**Remark 4.4.** For $r \sim \sqrt{q}/2$, this construction leads to proper blocking sets on the Hermitian curve $\mathcal{U}$ of $\mathrm{PG}(2,q^2)$ of size approximately $2q^2\sqrt{q}$. One may compare this explicit construction to the result obtained using the probabilistic method (§4.1). As we saw, the probabilistic method leads to blocking sets of cardinality $Cq^2\log q$, for some small constant $C(\leq 5)$.

**The setting.** The Hermitian curve is $\mathcal{U} : X^q + X + Y^{q+1} = 0$ in the affine plane $\mathrm{AG}(2,q^2)$. This Hermitian curve intersects the line at infinity $Z=0$ in the unique point $(x:y:z) = (1:0:0)$.

We first consider the case that $q$ is odd. The case $q$ even is similar, but slightly more complicated. Fix $r$, where $r|(q-1)$. Let $k$ be a fixed non-square in $\mathbb{F}_q$. Let $i^2 = k$, with $i \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then $i^q = -i$, and $i^{q+1} = -k$. We describe the elements $x$ of $\mathbb{F}_{q^2}$ by $x = x_1 + ix_2$, with $x_1, x_2 \in \mathbb{F}_q$.

**Step 1.** First of all we construct a blocking set $B$ of $\mathcal{U}$, defined by

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

So $B$ contains the point $(1:0:0)$ and the points of $\mathcal{U}$ on the horizontal lines $Y = u^r + iv$, $u, v \in \mathbb{F}_q$. Afterwards in Step 2, a modification will be made to the blocking set $B$ to make it proper.

In order to show that $B$ is a blocking set, we have to show that it meets all non-horizontal lines, since the horizontal lines are blocked by $(1:0:0)$. Consider the intersection of a non-horizontal line $X = nY + c$, where $n = n_1 + in_2$ and $c = c_1 + ic_2$ where $n_1, n_2, c_1, c_2 \in \mathbb{F}_q$, with $B$. Substituting $X = nY + c = n(u^r + iv) + c$ in the equation $X^q + X + Y^{q+1} = 0$ of $\mathcal{U}$, and using $i^q = -i$ and $i^{q+1} = -k$, leads to the equation

$$2n_1u^r + 2kn_2v + 2c_1 + u^{2r} - kv^2 = 0.$$

We make the equation homogeneous and denote the algebraic curve in $\mathrm{PG}(2, q)$ defined by this equation by $\Gamma : 2n_1U^rW^r + 2kn_2VW^{2r-1} + 2c_1W^{2r} + U^{2r} - kV^2W^{2r-2} = 0$.

**Lemma 4.5.** *The point* $(0 : 1 : 0)$ *is a point of multiplicity* $2r - 2$*. The algebraic curve* $\Gamma$ *is absolutely irreducible of genus* $r - 1$*.*

**Proof:** If we put $V = 1$ the minimal degree becomes $2r - 2$ so $(0 : 1 : 0)$ is a point of multiplicity $2r - 2$. Next, put $W = 1$. The equation of $\Gamma$ becomes $2n_1U^r + 2kn_2V + 2c_1 + U^{2r} - kV^2 = 0$. This is the hyperelliptic curve $k(V - n_2)^2 = U^{2r} + 2n_1U^r + 2c_1 + kn_2^2$. The only way for this curve to be reducible is that the right hand side is the square $(U^r + n_1)^2$, which implies $n_1^2 = 2c_1 + kn_2^2$, but this means that the line $X = nY + c$ with coordinates $[1 : -n : -c]$ satisfies $-c^q + n^{q+1} - c = 0$, and therefore is a tangent to the unital. So the right hand side factors as $(U^r - \alpha)(U^r - \beta)$ (in $\mathbb{F}_q^2$) where $\alpha$ and $\beta$ are different. Since $r|(q - 1)$ it has no multiple roots, so we have a hyperelliptic curve of genus $g = r - 1$ (see for instance [16], p. 113). $\square$

Using the Hasse-Weil bound we see that $\Gamma$ contains between $q + 1 - (2r - 2)\sqrt{q}$ and $q + 1 + (2r - 2)\sqrt{q}$ points. For small $r$, the lower bound on the cardinality of $\Gamma$ is larger than zero.

We need to convert these bounds on the cardinality of $\Gamma$ into bounds on the number of points of the set $B$ on the non-horizontal line $X = nY + c$. We first determine the number of points of $\Gamma$ on the line $U = 0$. Since $\Gamma$ is absolutely irreducible, we have apart from $(0 : 1 : 0)$ at most two other affine points since $(0 : 1 : 0)$ is a point of multiplicity $2r - 2$ of $\Gamma$. We decrease the lower bound on the cardinality of $\Gamma$ by three, which gives the interval $q-2-(2r-2)\sqrt{q} \le |\Gamma \setminus (U=0)| \le q+1+(2r-2)\sqrt{q}$. Now if $(u,v) \in \Gamma$, with $u \neq 0$, then also every point $(u\xi^i, v)$, $\xi$ a primitive $r$-th root of unity, $i=0,\dots,r-1$, belongs to $\Gamma$. But the points $(u,v)$ and $(u\xi^i,v)$, $i=0,\dots,r-1$, define the same affine points $(x,y)=(x,u^r+iv)$ of the set $B$. Hence, a non-horizontal line $X=nY+c$ contains $z$ points of $B$, where $(q-2-(2r-2)\sqrt{q})/r \le z \le (q+1+(2r-2)\sqrt{q})/r$.

This then implies for small values of $r$ that every non-horizontal line $X=nY+c$ contains at least one point of $B$, so that $B$ is indeed a blocking set. Of course $B$ contains some horizontal blocks. To turn $B$ into a proper blocking set we proceed as follows.

**Step 2.** Consider a cyclic $(q^2-q+1)$-arc $A$, contained in $\mathcal{U}$ and passing through $(1:0:0)$. Then exactly $q+1$ lines of $\mathrm{PG}(2,q^2)$ through $(1:0:0)$ are tangent lines to the arc $A$. These $q+1$ lines through $(1:0:0)$ tangent to $A$ form a dual Baer subline at $(1:0:0)$ [9, Theorem 3.4]. One of these $q+1$ lines through $(1:0:0)$ tangent to the arc $A$ is the tangent line $Z=0$ to $\mathcal{U}$ in $(1:0:0)$, and the remaining $q$ are secant lines to $\mathcal{U}$.

We now delete from the blocking set $B$ all points of the arc $A \cap B$, different from $(1:0:0)$, and all points of $B$ lying on these $q$ lines through $(1:0:0)$ secant to $\mathcal{U}$ and tangent to $A$, but different from $(1:0:0)$. We show that for small values of $r$, the set $\tilde{B}$ that remains is a proper blocking set of $\mathcal{U}$. Every horizontal line still is blocked by $(1:0:0)$, but since we delete a point of $B$ on every horizontal line $Y=u^r+iv$, no horizontal block of $\mathcal{U}$ is contained in $\tilde{B}$. Every non-horizontal line $X=nY+c$ contains at most two points of the arc $A$. Similarly, every non-horizontal line $X=nY+c$ contains at most two points of $\mathcal{U}$ on lines of the dual Baer subline of tangents through $(1:0:0)$ to $A$. For, suppose that such a line contains at least three points of $\mathcal{U}$ on lines of this dual Baer subline. Since a Baer subline is uniquely defined by three of its points, this would imply that the line $X=nY+c$ shares $q+1$ points with $\mathcal{U}$ on the lines of this dual Baer subline. But this is impossible, since the line $Z=0$ is one of the lines of this dual Baer subline and this line $Z=0$ is a tangent line to $\mathcal{U}$ only intersecting $\mathcal{U}$ in $(1:0:0)$. So we subtract four from the lower bound on the intersection size of the non-horizontal line $X=nY+c$ with $B$. This leads to the new lower bound $(q-2-(2r-2)\sqrt{q})/r-4$.

Our assumption $4r^2+1<q$ guarantees that this lower bound is still positive, so that the newly obtained set $\tilde{B}$ still blocks all the non-horizontal secant lines to $\mathcal{U}$.

To be sure that the non-horizontal lines do not contain a block, we look at the upper bound on the intersection sizes of these lines with the set $\tilde{B}$. This is $(q+1+(2r-2)\sqrt{q})/r$, which is less than $q+1$, so also the non-horizontal lines do not contain a block of $\mathcal{U}$.

**Cardinality.** Now that we are sure that the constructed set $\tilde{B}$ is a proper blocking set, we investigate its cardinality.

In the first step of the construction, $B$ consists of the point $(1:0:0)$ and of the points of $\mathcal{U}$ on the horizontal lines $Y = u^r + iv$, with $u, v \in \mathbb{F}_q$. There are $q + (q-1)\cdot q/r$ lines, leading to $|B| = 1 + q\cdot(q + \frac{q^2-q}{r})$.

Now in the second step, the points of $B$, different from $(1:0:0)$, lying on a cyclic $(q^2-q+1)$-arc $A$ of $\mathcal{U}$ through $(1:0:0)$ and on the $q$ secants through $(1:0:0)$ to $\mathcal{U}$, tangent to $A$, are deleted from $B$.

We first determine the maximal number of points that can be deleted from the blocking set $B$ in this way. The maximum can only occur when all $q$ secants of $\mathcal{U}$ on $(1:0:0)$ tangent to $A$ contain $q$ points of $B$, different from $(1:0:0)$. This leads to the loss of $q\cdot q = q^2$ points of $B$. Then still $q + (q-1)q/r - q = (q-1)q/r$ horizontal lines remain which still lose one point on the cyclic $(q^2-q+1)$-arc $A$. So the smallest size for the blocking set $\tilde{B}$, is

$$1 + q^2 + \frac{q^3-q^2}{r} - q^2 - \frac{(q-1)q}{r} = 1 + \frac{q^3-2q^2+q}{r}.$$

We now determine the minimal number of points that can be deleted from the blocking set $B$ in this way. The minimum can only occur when all $q$ secants of $\mathcal{U}$ on $(1:0:0)$ tangent to $A$ contain zero points of $B$, different from $(1:0:0)$. Then the $q + (q-1)q/r$ horizontal lines $Y = u^r + iv$ still lose one point on the cyclic $(q^2-q+1)$-arc $A$. So the largest possible size for the blocking set $\tilde{B}$, is

$$1 + q^2 + \frac{q^3-q^2}{r} - q - \frac{(q-1)q}{r} = 1 + q^2 - q + \frac{q^3-2q^2+q}{r}.$$

**Even $q$.** The preceding results are also valid for $q$ even, but the description of the algebraic curve $\Gamma$ is different. Namely, for $q$ even, let $k \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(k) = 1$. Let $i^2 + i + k = 0$, then $i^q + i = 1, i^2 = i + k$, and $i^{q+1} = k$. Let $\mathcal{U} : X^q + X + Y^{q+1} = 0$. Let $r$ again be a divisor of $q-1$ and denote every non-horizontal line by $X = nY + c$, with $n = n_1 + in_2$ and $c = c_1 + ic_2$, $n_1, n_2, c_1, c_2 \in \mathbb{F}_q$. Then the corresponding algebraic curve $\Gamma$ is

$$\Gamma : (n_1+n_2)VW^{2r-1} + n_2U^rW^r + c_2W^{2r} + U^{2r} + U^rVW^{r-1} + kV^2W^{2r-2} = 0.$$

By putting $V = 1$, it is again observed that the point $(0 : 1 : 0)$ is a singular point of $\Gamma$ with multiplicity $2r - 2$. Next we put $W = 1$ and obtain the (hyperelliptic) curve $kV^2 + (U^r + n_1 + n_2)V + U^{2r} + n_2U^r + c_2 = 0$. As before we can show that this curve is irreducible unless the line $X = nY + c$ is a tangent. The genus of this curve is again $g = r - 1$ [2, p. 317]. This implies that the arguments for $q$ odd also are valid for $q$ even.

This completes the proof of Theorem 4.3.

# References


[1] A. Al-Azemi, A. Betten, and D. Betten, Unital Designs with Blocking Set. (Preprint).

[2] E. Artin, Algebraic numbers and algebraic functions, London: Gordon and Breach, 1967

[3] A. Blokhuis, A.E. Brouwer, and H.A. Wilbrink, Hermitian unitals are codewords. *Discrete Math.* **97** (1991), 63–68.

[4] A. Blokhuis, R. Pellikaan, and T. Szőnyi, Blocking sets of almost Rédei type. *J. Combin. Theory, Ser. A* **78** (1997), 141–150.

[5] A. Blokhuis, V. Lev, Flat-Containing and Shift-Blocking sets in $\mathbb{F}_q^r$. *Moscow J. on Comb. and Number Th.* to appear.

[6] E. Boros and T. Szőnyi, On the sharpness of a theorem of B. Segre. *Combinatorica* **6** (1986), 261–268.

[7] P. Erdős, On a combinatorial problem. *Nordisk Mat. Tidskr.* **11** (1963), 5–10.

[8] P. Erdős and L. Lovász, Problems and results on 3-chromatic hypergraphs and some related questions, pp. 609–627 in: *Infinite and Finite Sets*, Proc. Keszthely 1973, Colloq. Math. Soc. János Bolyai 10, Budapest, 1975.

[9] J.C. Fisher, J.W.P. Hirschfeld, and J.A. Thas, Complete arcs in planes of square order. *Ann. Discrete Math.* **30** (1986), 243–250.

[10] Z. Füredi, Matchings and covers in hypergraphs. *Graphs and Combinatorics* **4** (1988), 115–206.

[11] D. Ghinelli and D. Jungnickel, Some geometric aspects of finite abelian groups. *Rend. Mat., Ser. VII* **26** (2006), 29–68.

[12] T. Illés, T. Szőnyi and F. Wettl, Blocking sets and maximal strong representative systems in finite projective planes, *Mitt. Math. Sem. Giessen* **201** (1991), 97–107.

[13] B.C. Kestenband, A family of complete arcs in finite projective planes. *Colloq. Math.* **57** (1989), 59–67.

[14] J. Radhakrishnan and A. Srinivasan, Improved bounds and algorithms for hypergraph 2-coloring. *Random Structures Algorithms* **16** (2000), no. 1,4–32.

[15] M. Seib, Unitäre Polaritäten endlicher projectiver Ebenen. *Arch. Math.* **21** (1970), 103–112.

[16] H. Stichtenoth, Algebraic Function Fields and Codes. Springer Verlag 1993.

[17] P. Sziklai, On small blocking sets and their linearity. *J. Combin. Theory, Ser. A* **115** (2008), 1167–1182.

[18] T. Szőnyi, Blocking sets in Desarguesian affine and projective planes. *Finite Fields Appl.* **3** (1997), 187–202.

Address of the authors:

A. Blokhuis and A. E. Brouwer, Eindhoven University of Technology, Department of Mathematics and Computing Science, Den Dolech 2, 5600 MB Eindhoven, The Netherlands (aartb@win.tue.nl; aeb@cwi.nl)

D. Jungnickel, Lehrstuhl für Diskrete Mathematik, Optimierung und Operations Research, Universität Augsburg, D–86135 Augsburg, Germany (jungnickel@math.uni-augsburg.de, http://www.math.uni-augsburg.de/opt/)

V. Krčadinac, Department of Mathematics, Faculty of Science, University of Zagreb, Zagreb, Croatia
(krcko@math.hr, http://web.math.pmf.unizg.hr/∼krcko/homepage.html)

S. Rottey, Vrije Universiteit Brussel, Faculty of Engineering, Pleinlaan 2, 1050 Brussel, Belgium (Sara.Rottey@vub.ac.be)

L. Storme and P. Vandendriessche, Ghent University, Department of Mathematics, Krijgslaan 281–S22, 9000 Gent, Belgium (ls@cage.ugent.be, http://cage.ugent.be/∼ls; pv@cage.ugent.be, http://cage.ugent.be/∼pv)

T. Szőnyi, Eötvös Loránd University, Department of Computer Science, and MTA-ELTE Geometric and Algebraic Combinatorics research group Pázmány P. sétány 1/c, 1117 Budapest, Hungary (szonyi@cs.elte.hu)