Blocking Sets of the Hermitian Unital

Dieter Jungnickel
Institut für Mathematik
Universität Augsburg

December 6, 2013
1. Blocking sets on Hermitian curves
2. A lower bound
3. Background: Unitals via difference sets
4. A geometric construction
5. Explicit examples

The talk is based on joint work with A. Blokhuis, A. Brouwer, V. Krcadinac, S. Rottey, L. Storme, T. Szőnyi and P. Vandendriessche.
Hermitian unitals

- **Hermitian curve** \( \mathcal{H}_{2,q^2} \) in \( PG(2, q^2) \):

\[
\mathcal{H}_{2,q^2} : (x \ y \ z) A \begin{pmatrix} x^q \\ y^q \\ z^q \end{pmatrix} = 0,
\]

with \( \det(A) \neq 0 \), \( A = (a_{ij}) \), and \( a_{ij}^q = a_{ji} \).

- Any line of \( PG(2, q^2) \) intersects \( \mathcal{H}_{2,q^2} \) in 1 point (tangent) or in \( q + 1 \) points (secant).

- A secant intersects \( \mathcal{H}_{2,q^2} \) in a Baer subline \( PG(1, q) \) (**block**).

- Classical \( (q^3 + 1, q + 1, 1) \)-design (**Hermitian unital**).
$\mathcal{H}_{2,4}$ yields $AG(2,3)$ embedded in $PG(2,4)$
Blocking sets

Definition.

1. **Blocking set** $B$ on $\mathcal{H}_{2,q^2}$: a set of points intersecting every block, but not containing any block completely.

2. **Minimal** blocking set $B$: no proper subset of $B$ still is a blocking set.

Computer Results (A. Al-Azemi, A. Betten and D. Betten, *Unital designs with blocking sets*):

- 68806 different $2-(28, 4, 1)$ unital designs have blocking sets.
- $\mathcal{H}_{2,9}$: no blocking sets.
Theorem. Let $B$ be a blocking set of a Hermitian unital $\mathcal{U}$ in $\mathrm{PG}(2, q^2)$, $q = p^h$, $p$ prime. Then

$$|B| \geq \frac{3q^2 - 2q - 1}{2} = q^2 - q + 1 + \frac{q^2 - 3}{2}.$$

The setup:

- Points of $\mathcal{U}$: $(x : y : z)$ with $(x : y : z) I [z^q : y^q : x^q]$, so $xz^q + y^{q+1} + zx^q = 0$.
- Tangents of $\mathcal{U}$: the lines $[t : u : v]$ with $tv^q + u^{q+1} + vt^q = 0$.
- Line at infinity: $z = 0$, the tangent in $(1 : 0 : 0)$. 
\( B = S \cup \{(1 : 0 : 0)\} \)

\( S := \{(a, b) \mid (a : b : 1) \in B\} \)

Line \([1 : u : v] : X + uY + v = 0\)

Tangent line \([1 : u : v] : vq + v + u^{q+1} = 0\)

A unital point outside \(B\) is on \(q^2\) unital lines: \(|S| \geq q^2\)

\(|B| = |S| + 1 =: q^2 - q + 1 + k\)

Claim: \(k \geq \frac{1}{2}(q^2 - 3)\)

W.l.o.g. \(|S| < 2q^2 - q - 1\)

\(B\) minimal \(\implies b \neq 0\) for all \((a, b) \in S\)
The polynomial method

\[ H(U, V) = C(U, V)R(U, V) \]

\[ := (V^q + V + U^{q+1}) \prod_{(a,b) \in S} (V + a + bU) \]

\( H(U, V) \) vanishes identically on \( \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \)!

\[ H(U, V) = (V^{q^2} - V)f(U, V) + (U^{q^2} - U)g(U, V) \]

with

- \( \deg(f), \deg(g) \leq k + 1 \)
- \( \deg(f) = k + 1, \quad \text{deg}_V f = k \)
- Common linear factor $V + a_i + Ub_i$ of $f(U, V)$ and $g(U, V)$
  - non-necessary point for $B$.
- $C(U, V)$ divides $f(U, V)$ and $g(U, V)$
  - $B$ blocking set of $\text{PG}(2, q^2)$, so $B = \mathcal{H}_{2,q^2}$
- $f$ and $g$ are coprime.
- If $f(u, v) = 0$, then also $g(u, v) = 0$.
- $f(u, V)$ is fully reducible over $\mathbb{F}_{q^2}$ for all $u \in \mathbb{F}_{q^2}$.
- Let $f = f_0 \cdots f_m$ be the factorization of $f$ into irreducible components.
Case 1

There is an irreducible factor $f_0$ of $f$ with $\partial_V f_0 \not\equiv 0$.

- Put $m := \deg f_0$, so that $1 \leq m \leq \deg f = k + 1$.

Then $\deg_V (f_0) = m - \epsilon$, with $\epsilon \in \{0, 1\}$, and $\epsilon = 0$ for $m = 1$.

- Let $N$ be the number of zeros of $f_0$ in $\mathbb{F}_{q^2}$.

- By Bézout’s theorem, $N \leq \deg f_0 \deg g \leq m(k + 1)$.

- As $f(u, V)$ is fully reducible for all $u$, the number $M$ of zeros counted with multiplicity is $q^2(m - \epsilon)$.

- Now $N \geq M - m(m - 1)$.

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

- By case analysis, $k \geq \frac{1}{2}(q^2 - 3)$. 
Case 2

\[ \partial_V f_i \equiv 0 \text{ for all irreducible factors } f_i \text{ of } f. \]

- \( f(u, V) \) is a \( p \)-th power.
- The multiplicity of \( v \) as a root of \( H(u, V) = (V^{q^2} - V)f(u, V) \) is 1 \((\text{mod } p)\).
- All (non-horizontal) secants intersect \( B \) in 1 \((\text{mod } p)\) points.
- Summing over a parallel class of \( \mathcal{U} \):
  \[ |B| \equiv (q^2 - q + 1) \cdot 1 \equiv 1 \pmod{p}. \]
- Summing over the \( q^2 \) lines through a point \( p \not\in B \):
  \[ |B| \equiv q^2 \cdot 1 \equiv 0 \pmod{p}. \]
Represent $\text{PG}(2, q^2)$ via a planar difference set $D$ in the cyclic group $G$ of order $q^4 + q^2 + 1$.

Let $D$ be fixed by every multiplier.

$G = A \times B$, where $|A| = q^2 - q + 1$ and $|B| = q^2 + q + 1$.

The cosets of $A$ are arcs, the cosets of $B$ Baer subplanes.

Elements of $G$: pairs $(i, j)$ with $0 \leq i \leq q^2 - q$ and $0 \leq j \leq q^2 + q$.

The multiplier $q^3$ maps $(i, j)$ to $(-i, j)$.

$g \mapsto D - q^3g$ defines a Hermitian polarity.

The absolute points give the Hermitian unital $\mathcal{U} = \{a + \beta \mid a \in A, 2\beta \in B \cap D\}$.

$\mathcal{U}$ is the union of $q + 1$ cosets of $A$. 
Theorem. \( \mathcal{H}_{2,q^2} \), with \( q \geq 7 \), has blocking sets of size

\[
\frac{q^3 + 1}{2} \quad \text{if } q \text{ is odd,}
\]

\[
\frac{q^3 - q^2 + q}{2} \quad \text{if } q \text{ is even.}
\]

Idea of proof:

- Let \( q \) be odd. Partition the \( q + 1 \) cosets of \( A \) into two sets of size \( (q + 1)/2 \) such that the union of each is a blocking set of \( U \).
- If \( q \) is even, partition \( U \) into collections of \( q/2 \) and \( q/2 + 1 \) cosets of \( A \) forming blocking sets.
Hermitian curve partitioned into arcs

\[ \mathcal{H}_{2,q^2} \]
Proof for \( q \) odd

The point set of \( U \) is \( A + \frac{1}{2}(B \cap D) \), and \( \frac{1}{2}(B \cap D) \) is an oval \( O \) in the Baer subplane \( B \).

Lines have three types of intersection pattern with the \( U \)-cosets of \( A \):

- A tangent of \( O \) is also a tangent of the unital \( U \).
- A secant of \( O \) intersects two \( U \)-cosets in a single point, and the remaining ones in 0 or 2 points. Both cases occur \( (q - 1)/2 \) times.
- An external line of \( O \) intersects all \( U \)-cosets of \( A \) in 0 or 2 points. Both cases occur \( (q + 1)/2 \) times.

The \( (q^2 - q)/2 \) external lines give partitions of the set of \( U \)-cosets not leading to blocking sets of \( U \).

As \( \frac{1}{2} \left( \frac{q+1}{(q+1)/2} \right) > \frac{1}{2}(q^2 - q) \) for \( q \geq 7 \), the desired partition of the \( U \)-cosets exists.
The main result

- $q = 2$: Non-existence (well-known)
- $q = 3$: Non-existence by computer search
- $q = 4$: Method works!
- $q = 5$: Method fails, but a random greedy computer search gives blocking sets of all sizes from 45 to 81.

Main Theorem.
The Hermitian unital in $\text{PG}(2, q^2)$ contains a blocking set if and only if $q > 3$. 

Theorem.

Let \( r \mid (q - 1) \), where \( r > 1 \) and \( 4r^2 + 1 < q \).

Then the Hermitian unital in \( \text{PG}(2, q^2) \) contains a blocking set \( B \) of size
\[ k + q(q - 1)^2/r \]
for some \( k \) with \( 1 \leq k \leq q^2 - q + 1 \).

For \( r \sim \sqrt{q}/2 \), this result leads to proper blocking sets of size approximately
\[ 2q^2 \sqrt{q} \].
Sketch of proof for $q$ odd

- We again use the Hermitian curve $\mathcal{H}$ with affine equation $X^q + X + Y^{q+1} = 0$.

- Choose a non-square $k \in \mathbb{F}_q$ and $i \in \mathbb{F}_{q^2}$ with $i^2 = k$.
  Now the elements of $\mathbb{F}_{q^2}$ are $x = x_1 + ix_2$, with $x_1, x_2 \in \mathbb{F}_q$.

- Put $B := \{(x, y) \in \mathcal{H} \mid y = u^r + iv, \text{ with } u, v \in \mathbb{F}_q\} \cup \{(1 : 0 : 0)\}$.
  So $B$ contains $(1 : 0 : 0)$ and the points of $\mathcal{U}$ on the horizontal lines $Y = u^r + iv$, $u, v \in \mathbb{F}_q$.

- Trivially, $B$ meets every horizontal line.

- $B$ meets every non-horizontal line of $\mathcal{H}$ in $z$ points, where $(q - 2 - (2r - 2)\sqrt{q})/r \leq z \leq (q + 1 + (2r - 2)\sqrt{q})/r$. 
Consider a cyclic \((q^2 - q + 1)\)-arc \(A\) in \(\mathcal{H}\) and passing through \((1 : 0 : 0)\).

The \(q + 1\) lines through \((1 : 0 : 0)\) tangent to \(A\) form a dual Baer subline at \((1 : 0 : 0)\).

One of these lines is the tangent line \(Z = 0\) to \(\mathcal{H}\) in \((1 : 0 : 0)\), and the remaining \(q\) are secant lines to \(\mathcal{H}\).

Delete all points \(\neq (1 : 0 : 0)\) of the arc \(A \cap B\) from \(B\).

Delete all points \(\neq (1 : 0 : 0)\) lying on the above \(q\) secants of \(\mathcal{H}\) through \((1 : 0 : 0)\) from \(B\).

This gives the desired blocking set.
Thanks for your attention.