



***Minimal blocking sets of size $q^2 + 2$ of $\mathbb{Q}(4, q)$,
 q an odd prime, do not exist***

Jan De Beule

joint work with: Klaus Metsch

Ghent University

Dept. Pure Mathematics and Computeralgebra

Definitions

A finite generalized quadrangle (GQ) of order (s, t) is a point-line incidence geometry satisfying the following axioms.

- ⑥ Each point is incident with $1 + t$ lines ($t \geq 1$) and two different points determine at most one line.
- ⑥ Each line is incident with $1 + s$ lines ($s \geq 1$) and two different lines determine at most one points.
- ⑥ If x is a point and L is a lines not incident with x , then there is a unique pair $(y, M) \in \mathcal{P} \times \mathcal{B}$ for which $x \text{ I } M \text{ I } y \text{ I } L$.

Two classical GQs of order q

- ⑥ We consider the non-singular parabolic quadric in $\text{PG}(4, q)$, denoted with $Q(4, q)$; it contains points and lines constituting a GQ of order q
- ⑥ We consider the points of $\text{PG}(3, q)$ together with the totally isotropic lines of $\text{PG}(3, q)$ with respect to a fixed symplectic polarity of $\text{PG}(3, q)$; these sets of points and lines constitute a GQ of order q .
- ⑥ If \mathcal{S} is a GQ, then \mathcal{S}^D is the dual of \mathcal{S} , i.e. the GQ obtained by interchanging the role of the points and lines of \mathcal{S} . It is known that $Q(4, q) \cong W(3, q)^D$.

Definitions again

Consider a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$.

- ⑥ An *ovoid* is a set \mathcal{O} of points of \mathcal{S} such that every line of \mathcal{S} meets the set \mathcal{O} in exactly one point
- ⑥ A *blocking set* is a set \mathcal{B} of points of \mathcal{S} such that every line of \mathcal{S} meets the set \mathcal{B} in at least one point.
- ⑥ A blocking set \mathcal{B} is called *minimal* if $\mathcal{B} \setminus \{p\}$ is not a blocking set for any point $p \in \mathcal{B}$.

a non-singular elliptic quadric $Q^-(3, q)$, contained in $Q(4, q)$, constitutes always an ovoid of $Q(4, q)$. When q is an odd prime, elliptic quadrics are the only examples. (Ball et al.)

The problem

Suppose that \mathcal{B} is a minimal blocking set of $Q(4, q)$ different from an ovoid.

- ⑥ When q is even, then $|\mathcal{B}| > q^2 + 1 + \sqrt{q}$ (Eisfeld et al.)
- ⑥ Can we find a lower bound when q is odd?
- ⑥ $|\mathcal{B}| = q^2 + 2$ is impossible when $q = 3, 5, 7$
- ⑥ Is it possible that $|\mathcal{B}| = q^2 + 2$ when q is odd?

Dualising $Q(4, q)$

Consider again any GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$.

- ⑥ A *spread* is a set \mathcal{R} of lines of \mathcal{S} such that every point of \mathcal{S} lies on exactly one line of \mathcal{R} .
- ⑥ A *cover* is a set \mathcal{C} of lines of \mathcal{S} such that every point of \mathcal{S} lies on at least one line of \mathcal{C} . A cover is *minimal* if $\mathcal{C} \setminus \{L\}$ is not a cover for any line $L \in \mathcal{C}$.

An ovoid of $Q(4, q)$ becomes a *spread* of $W(3, q)$.

A (minimal) blocking set of $Q(4, q)$ becomes a (minimal) cover of $W(3, q)$.

Known results I

Consider a cover \mathcal{C} of $W(3, q)$. A *multiple point* is a point of $W(3, q)$ covered by at least two lines of \mathcal{C} .

- ⑥ The multiple points form a sum of lines of $PG(3, q)$.
- ⑥ If \mathcal{C} is a minimal cover of $W(3, q)$ of size $q^2 + 2$, the multiple points lie on a line of $W(3, q) \setminus \mathcal{C}$.
- ⑥ Dually: if \mathcal{B} is a minimal blocking set of $Q(4, q)$ of size $q^2 + 2$, there are $q + 1$ secants sharing a common point $m \in Q(4, q) \setminus \mathcal{B}$.

Known results II

- ⑥ An ovoid \mathcal{O} of $Q(4, q)$, $q = p^h$, p prime, intersects any $Q^-(3, q)$ in $1 \pmod p$ points
- ⑥ This is proved using an algebraic description of $W(3, q)$ in the field $GF(q^4)$.

Using the structure of the multiple lines and the algebraic description, can we find intersection numbers with elliptic quadrics for a blocking set of size $q^2 + 2$?

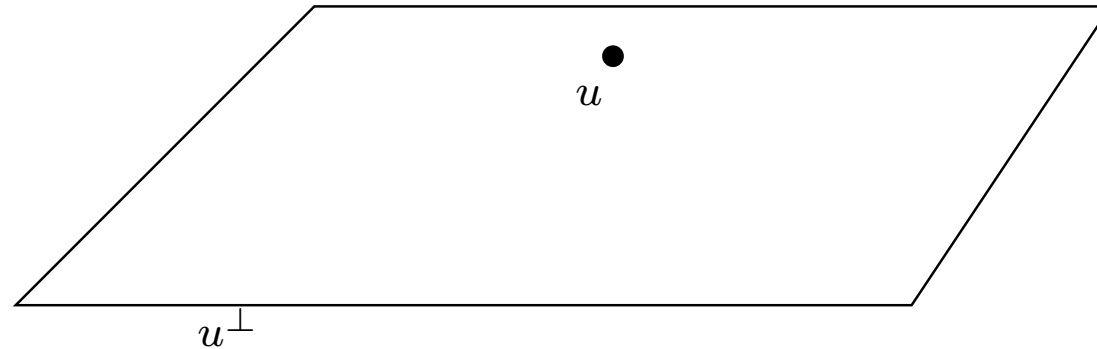
Analyzing the 1 mod p proof

- ⑥ There are $q^3 + q^2 + q + 1$ lines of $\text{PG}(3, q)$ which are also lines of $W(3, q)$. We distinguish two types of lines of $W(3, q)$, depending on the algebraic description. There are exactly $q^2 + 1$ lines of type 1, which constitute a regular spread of $W(3, q)$. Call this set of lines \mathcal{R} . There are $q^3 + q$ lines of type 2.
- ⑥ Consider an arbitrary spread S of $W(3, q)$, it can contain lines of both types.
- ⑥ Compute $|\mathcal{R} \cap S| \pmod p$

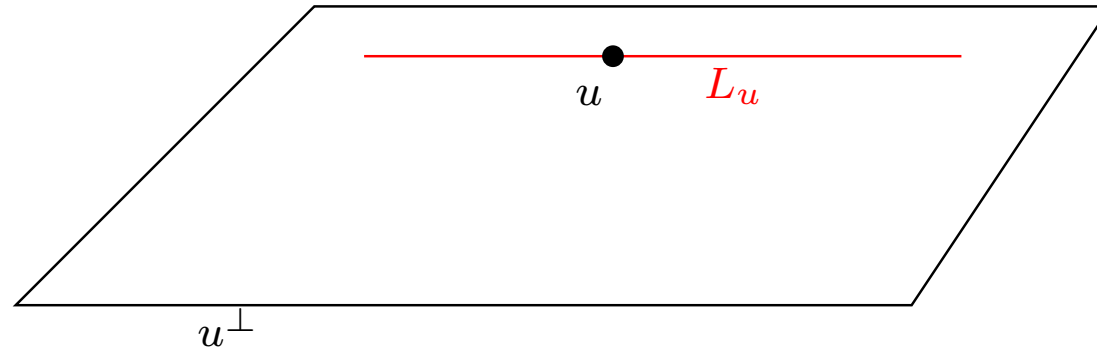
Analyzing the 1 mod p proof II

- ⑥ Lines of type 1 are represented by elements $e \in \text{GF}(q^4)$, for which $e^{q^2+1} = 1$.
- ⑥ Lines of type 2 are represented by elements $d \in \text{GF}(q^4)$, for which $\gamma d^{q^3+q} - \gamma^{-1} d^{q^2+1} + 1 = 0$, $\gamma = \Gamma^{1-q}$, $\Gamma^{q^2-1} = -1$.

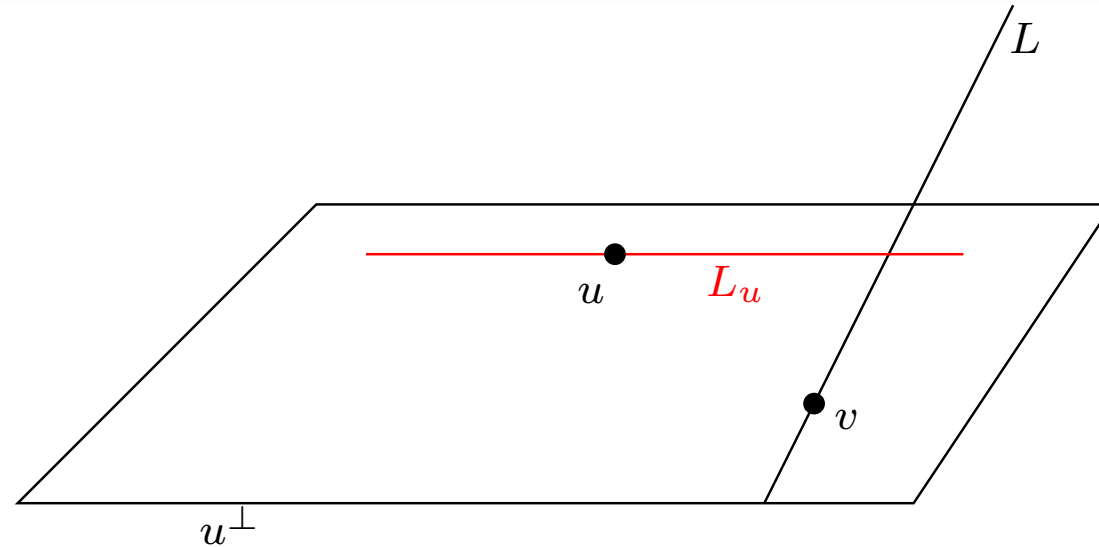
Visualizing the proof



Visualizing the proof



Visualizing the proof



The computation

Let \mathcal{S} be the spread of $W(3, q)$, and let \mathcal{E} be the set of elements of $\text{GF}(q^4)$ representing lines of type 1 of \mathcal{S} and \mathcal{D} the set of elements of $\text{GF}(q^4)$ representing lines of type 2 of \mathcal{S} .

$$\begin{aligned} 0 &= \sum_{v \in u^\perp \setminus L_u} v = \sum_{v \in u^\perp \setminus L_u} v^q \\ &= \sum_{e \in \mathcal{E}} \gamma^{-1} u e (u^{q+1} + e)^{q-1} - \sum_{d \in \mathcal{D}} u (d u^{q+1} + u - \gamma d^q)^{q-1} \end{aligned}$$

The computation II

The polynomial

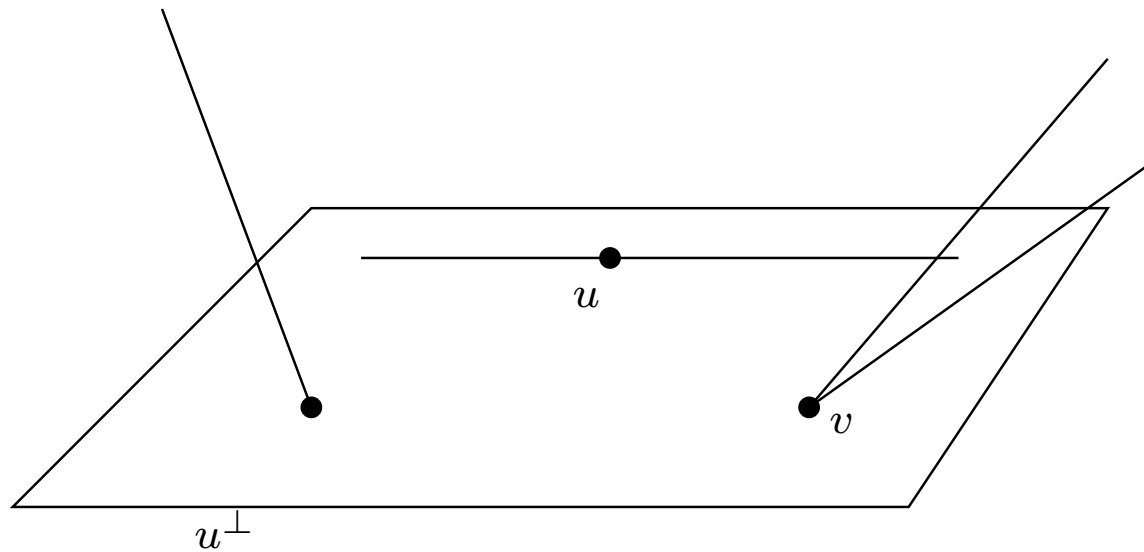
$$f(U) = \sum_{e \in \mathcal{E}} \gamma^{-1} U e (U^{q+1} + e)^{q-1} - \sum_{d \in \mathcal{D}} U (dU^{q+1} + U - \gamma d^q)^{q-1}$$

has $q^3 + q^2 + q + 1$ roots (all points u) and has degree only q^2 .

Hence, $|\mathcal{D}| = 0 \pmod p$ and $|\mathcal{E}| = 1 \pmod p$, since $|\mathcal{D}| + |\mathcal{E}| = q^2 + 1$.

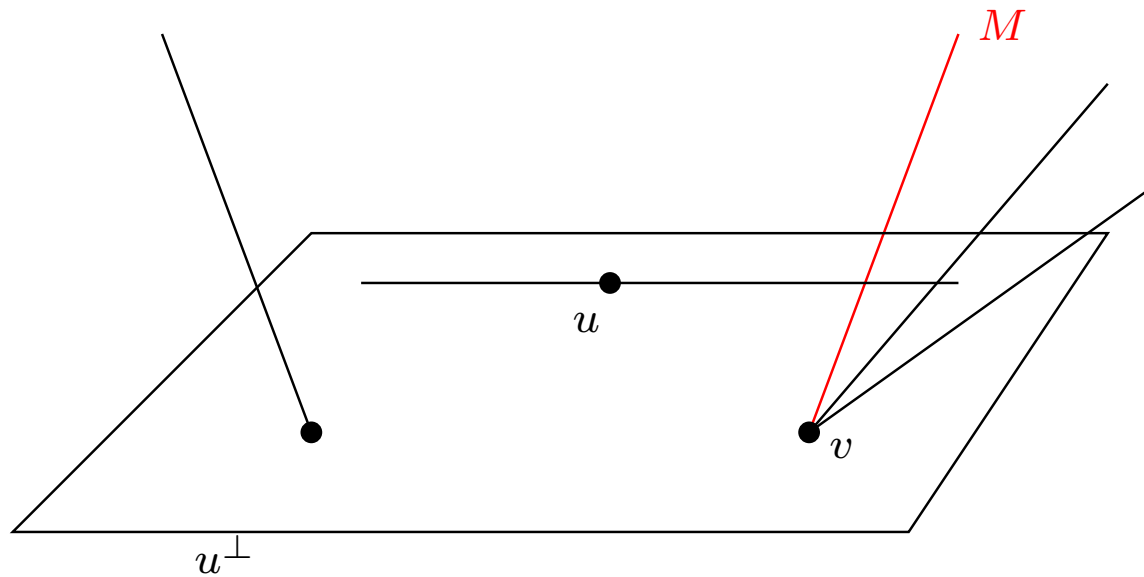
Repeating for the new situation?

Consider a cover of $W(3, q)$ of size $q^2 + 2$.



Repeating for the new situation?

Consider a cover of $W(3, q)$ of size $q^2 + 2$.



Adding negative lines

- ⑥ The multiple line is a line of $W(3, q)$, give it weight -1 .
- ⑥ We consider the polynomial

$$f(U) = \sum_{e \in \mathcal{E}} w_e \gamma^{-1} U e (U^{q+1} + e)^{q-1} - \sum_{d \in \mathcal{D}} w_d U (dU^{q+1} + U - \gamma d^q)^{q-1}$$

This polynomial has $q^3 + q^2$ roots (non-multiple points u), hence, $\sum_{d \in \mathcal{D}} w_d = 0 \pmod p$ and $\sum_{e \in \mathcal{E}} w_e = 1 \pmod p$, since $\sum_{d \in \mathcal{D}} w_d + \sum_{e \in \mathcal{E}} w_e = q^2 + 1$.

The intersection numbers

Consider a (minimal) blocking set \mathcal{B} of $Q(4, q)$, $q = p^h$, p odd prime, m is the common point of the 2-secants, α is a hyperplane of $PG(4, q)$.

- ⑥ $|\alpha \cap \mathcal{B}| = 1 \pmod p$ if $m \notin \alpha$
- ⑥ $|\alpha \cap \mathcal{B}| = 2 \pmod p$ if $m \in \alpha$

More geometry

We suppose that \mathcal{B} is a minimal blocking set of $Q(4, q)$ of size $q^2 + 2$ satisfying the following intersection numbers. The point m is the common point of all two secants to \mathcal{B} .

$$\textcircled{6} \quad |\alpha \cap \mathcal{B}| = 1 \pmod{q} \text{ if } m \notin \alpha$$

$$\textcircled{6} \quad |\alpha \cap \mathcal{B}| = 2 \pmod{q} \text{ if } m \in \alpha$$

Aim: to prove that \mathcal{B} contains an elliptic quadric.

A calculation

Suppose that α is a 3-space of $\text{PG}(4, q)$. Define $i_\alpha := |\alpha \cap \mathcal{B}|$, define t_i as the number of 3-spaces meeting \mathcal{B} in i points. Put $c := \frac{1}{2}(q^2 + 1)$. Then

$$t_{q+2}(q+1)(c-q-2) \geq t_2(q-1)(c-2)$$

$$\sum_{\alpha \in \text{PG}(4, q)} (i_\alpha - 1)(i_\alpha - q - 1)(i_\alpha - c) > 0$$

Another calculation

These two equations imply

$$\sum_{\alpha \in \text{PG}(4, q)} (i_\alpha - 1)(i_\alpha - q - 1)(i_\alpha - c) > 0$$

where the sum now runs over all 3-spaces α for which $i_\alpha \geq q+2$, hence, there is a 3-space containing at least $c = \frac{1}{2}(q^2 + 1)$ points of \mathcal{B} .

The end

A last geometrical lemma implies that \mathcal{B} contains an elliptic quadric. This implies that \mathcal{B} cannot be minimal.