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

Jan De Beule

joint work with: Klaus Metsch

Ghent University

Dept. Pure Mathematics and Computeralgebra

UNIVERSITEIT GENT

Definitions

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

- Each point is incident with $1 + t$ lines ($t \geqslant 1$) and two different points determine at most one line.
- Each line is incident with $1 + s$ lines ($s \geqslant 1$) and two different lines determine at most one points.
- 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 $x \mathrm{~I~} M \mathrm{~I~} y \mathrm{~I~} L$.

Two classical GQs of order q

- We consider the non-singular parabolic quadric in $\mathrm{PG}(4, q)$, denoted with $\mathrm{Q}(4, q)$; it contains points and lines constituting a GQ of order q
- We consider the points of $\mathrm{PG}(3, q)$ together with the totally isotropic lines of $\mathrm{PG}(3, q)$ with respect to a fixed symplectic polarity of $\mathrm{PG}(3, q)$; these sets of points and lines contsitute a GQ of order q.
- 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 $\mathrm{Q}(4, q) \cong \mathrm{W}(3, q)^D$.

UNIVERSITEIT GENT

Definitions again

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

- 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
- 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.
- 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 $\mathrm{Q}^-(3, q)$, contained in $\mathrm{Q}(4, q)$, constitutes always an ovoid of $\mathrm{Q}(4, q)$. When q is an odd prime, elliptic quadrics are the only examples. (Ball et al.)

UNIVERSITEIT GENT

The problem

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

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

UNIVERSITEIT GENT

Dualising $\mathrm{Q}(4,q)$

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

- A *spread* is a set $\mathcal{R}$ of lines of $\mathcal{R}$ such that every point of $\mathcal{S}$ lies on exactly one line of $\mathcal{R}$.
- 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 $\mathrm{Q}(4,q)$ becomes a *spread* of $\mathrm{W}(3,q)$.

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

UNIVERSITEIT GENT

Known results I

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

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

UNIVERSITEIT GENT

Known results II

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

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?

UNIVERSITEIT GENT

Analyzing the 1 mod p proof

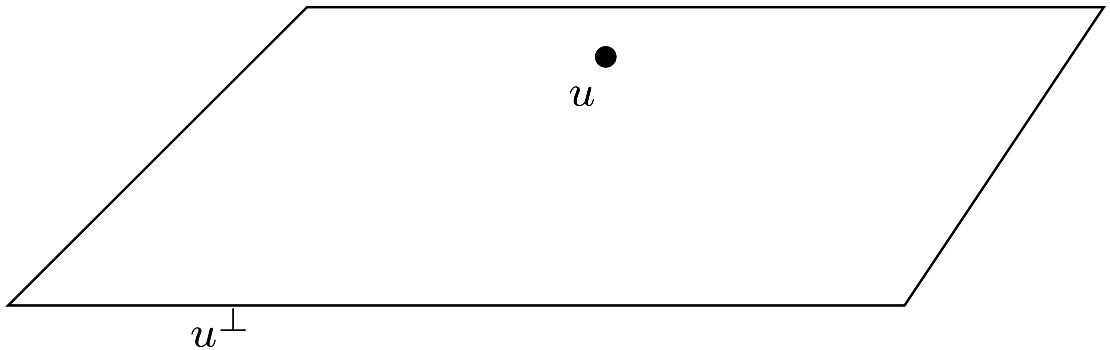
- There are q^3+q^2+q+1 lines of $\mathrm{PG}(3,q)$ which are also lines of $\mathrm{W}(3,q)$. We destinguish two types of lines of $\mathrm{W}(3,q)$, depending on the algebraic description. There are exactly q^2+1 lines of type 1, which constitute a regular spread of $\mathrm{W}(3,q)$, Call this set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

Analyzing the 1 *mod* p *proof II*

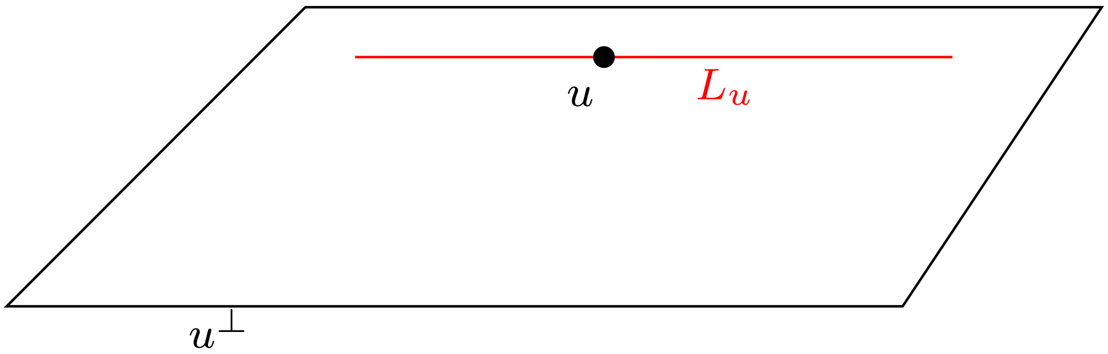
- Lines of type 1 are represented by elements $e \in \mathrm{GF}(q^4)$, for which $e^{q^2+1} = 1$.
- Lines of type 2 are represented by elements $d \in \mathrm{GF}(q^4)$, for which $\gamma d^{q^3+q} - \gamma^{-1} d^{q^2+1} + 1 = 0$, $\gamma = \Gamma^{1-q}$, $\Gamma^{q^2-1} = -1$.

UNIVERSITEIT GENT

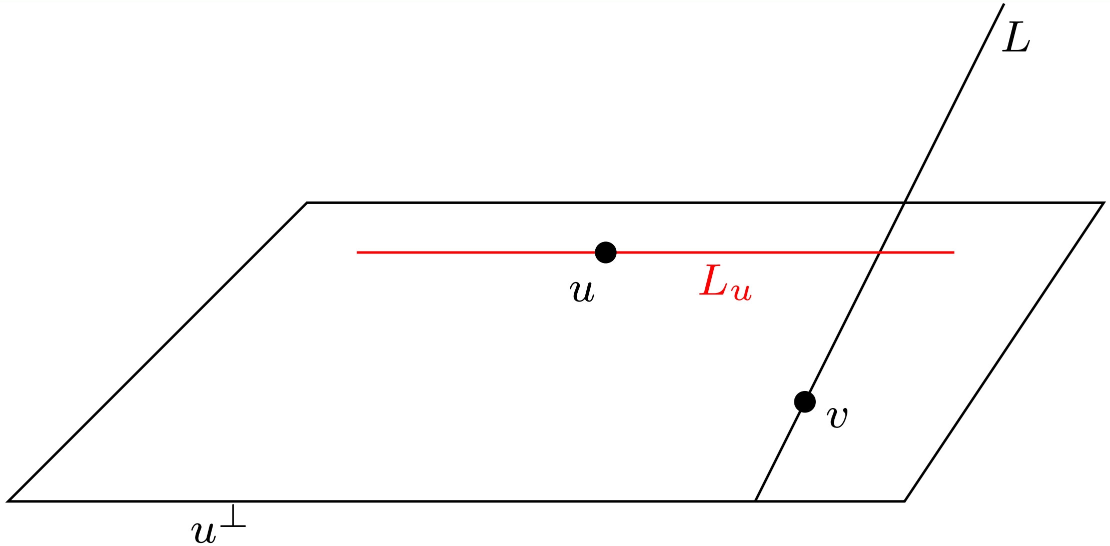
Visualizing the proof



Visualizing the proof



Visualizing the proof



The computation

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

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

UNIVERSITEIT GENT

The computation II

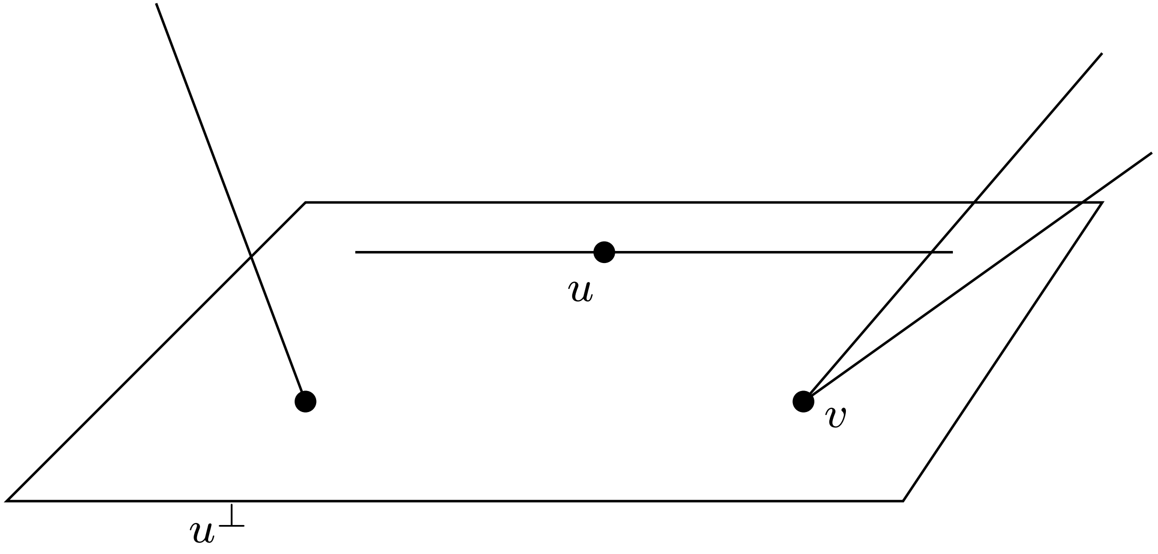
The polynomial

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

has $q^3 + q^2 + q + 1$ roots (all points u) and has degree only q^2. Hence, $|\mathcal{D}| = 0 \mod p$ and $|\mathcal{E}| = 1 \mod p$, since $|\mathcal{D}| + |\mathcal{E}| = q^2 + 1$.

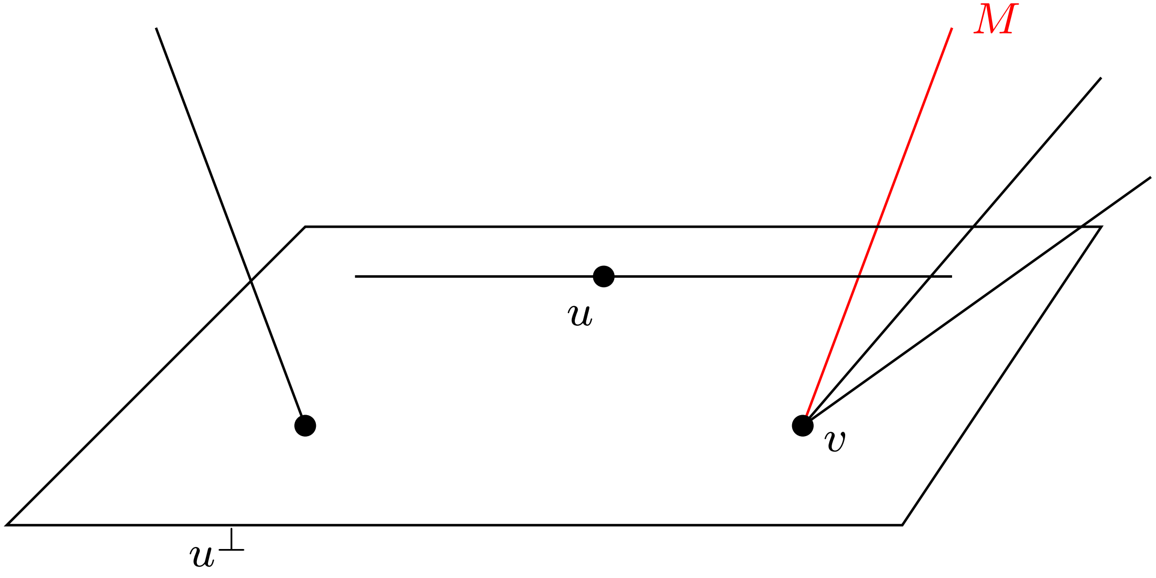
Repeating for the new situation?

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



Repeating for the new situation?

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



Adding negative lines

- The multiple line is a line of $\mathrm{W}(3,q)$, give it weigth -1.
- We consider the polynomial

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

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

UNIVERSITEIT GENT

The intersection numbers

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

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

UNIVERSITEIT GENT

More geometry

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

- $|\alpha \cap \mathcal{B}| = 1 \mod q$ if $m \notin \alpha$
- $|\alpha \cap \mathcal{B}| = 2 \mod q$ if $m \in \alpha$

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

UNIVERSITEIT GENT

A calculation

Suppose that α is a 3-space of $\mathrm{PG}(4,q)$. 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

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

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

UNIVERSITEIT GENT

Another calculation

These two equations imply

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

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

UNIVERSITEIT GENT

The end

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

UNIVERSITEIT GENT