Algebraic techniques in finite geometry: a case study

J. De Beule   A. Gács

Department of Pure Mathematics and Computer Algebra
Ghent University

January 29, 2007 / University College Dublin

Directions of a pointset in $\mathrm{AG}(2,q)$ and blocking sets of $\mathrm{PG}(2,q)$

Definition

Suppose that X is a set of points in $\mathrm{AG}(2,q)$. An element $m \in \mathrm{GF}(q)$ is called a *direction* determined by X if it is the slope of a line meeting X in at least two points.

Finite Generalized Quadrangles

A finite generalized quadrangle (GQ) is a point-line geometry $\mathcal{S} = \mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ such that

(i) Each point is incident with $1+t$ lines ($t \geqslant 1$) and two distinct points are incident with at most one line.

(ii) Each line is incident with $1+s$ points ($s \geqslant 1$) and two distinct lines are incident with at most one point.

(iii) If x is a point and L is a line not incident with x, then there is a unique pair $(y, M) \in \mathcal{P} \times \mathcal{B}$ for which $x \mathrm{~I~} M \mathrm{~I~} y \mathrm{~I~} L$.

The parabolic quadric $Q(4,q)$: a finite classical generalized quadrangle of order q.

Finite Generalized Quadrangles

A finite generalized quadrangle (GQ) is a point-line geometry $\mathcal{S} = \mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ such that

(i) Each point is incident with $1+t$ lines $(t \geqslant 1)$ and two distinct points are incident with at most one line.

(ii) Each line is incident with $1+s$ points $(s \geqslant 1)$ and two distinct lines are incident with at most one point.

(iii) If x is a point and L is a line not incident with x, then there is a unique pair $(y, M) \in \mathcal{P} \times \mathcal{B}$ for which $x \mathrm{~I~} M \mathrm{~I~} y \mathrm{~I~} L$.

The parabolic quadric $\mathrm{Q}(4,q)$: a finite classical generalized quadrangle of order q.

Ovoids and partial ovoids

Definition

An *ovoid* of a GQ $\mathcal{S}$ is a set $\mathcal{O}$ of points of $\mathcal{S}$ such that every line of $\mathcal{S}$ contains exactly one point of $\mathcal{O}$.

Definition

A *partial ovoid* of a GQ $\mathcal{S}$ is a set $\mathcal{O}$ of points of $\mathcal{S}$ such that every line of $\mathcal{S}$ contains at most one point of $\mathcal{S}$. A partial ovoid is *maximal* if it cannot be extended to a larger partial ovoid.

We call "partial ovoids" also "arcs".

Ovoids and partial ovoids

Definition

An *ovoid* of a GQ $\mathcal{S}$ is a set $\mathcal{O}$ of points of $\mathcal{S}$ such that every line of $\mathcal{S}$ contains exactly one point of $\mathcal{O}$.

Definition

A *partial ovoid* of a GQ $\mathcal{S}$ is a set $\mathcal{O}$ of points of $\mathcal{S}$ such that every line of $\mathcal{S}$ contains at most one point of $\mathcal{S}$. A partial ovoid is *maximal* if it cannot be extended to a larger partial ovoid.

We call "partial ovoids" also "arcs".

Existence

- $Q(4, q)$ has always ovoids.
- partial ovoids of size q^2 can always be extended to an ovoid
- We are interested in partial ovoids of size $q^2 - 1$ ...
- ...which exist for $q = 3, 5, 7, 11$ and which do not exist for $q = 9$.
- When q is even, maximal partial ovoids of size $q^2 - 1$ do not exist.

Theorem

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a GQ of order (s, t). Any $(st - \rho)$-arc of $\mathcal{S}$ with $0 \leq \rho < \frac{t}{s}$ is contained in an uniquely defined ovoid of $\mathcal{S}$.

Existence

- $Q(4,q)$ has always ovoids.
- partial ovoids of size q^2 can always be extended to an ovoid
- We are interested in partial ovoids of size q^2-1 ...
- ...which exist for $q = 3, 5, 7, 11$ and which do not exist for $q = 9$.
- When q is even, maximal partial ovoids of size q^2-1 do not exist.

Theorem

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a GQ of order (s,t). Any $(st-\rho)$-arc of $\mathcal{S}$ with $0 \leq \rho < \frac{t}{s}$ is contained in an uniquely defined ovoid of $\mathcal{S}$.

Existence

- $Q(4, q)$ has always ovoids.
- partial ovoids of size q^2 can always be extended to an ovoid
- We are interested in partial ovoids of size $q^2 - 1$ ...
- ...which exist for $q = 3, 5, 7, 11$ and which do not exist for $q = 9$.
- When q is even, maximal partial ovoids of size $q^2 - 1$ do not exist.

Theorem

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a GQ of order (s, t). Any $(st - \rho)$-arc of $\mathcal{S}$ with $0 \leq \rho < \frac{t}{s}$ is contained in an uniquely defined ovoid of $\mathcal{S}$.

Existence

- $\mathrm{Q}(4,q)$ has always ovoids.
- partial ovoids of size q^2 can always be extended to an ovoid
- We are interested in partial ovoids of size $q^2-1\ldots$
- $\ldots$which exist for $q=3,5,7,11$ and which do not exist for $q=9$.
- When q is even, maximal partial ovoids of size q^2-1 do not exist.

Theorem

Let $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ be a GQ of order (s,t). Any $(st-\rho)$-arc of $\mathcal{S}$ with $0\leq\rho<\frac{t}{s}$ is contained in an uniquely defined ovoid of $\mathcal{S}$.

Existence

- $\mathrm{Q}(4,q)$ has always ovoids.
- partial ovoids of size q^2 can always be extended to an ovoid
- We are interested in partial ovoids of size $q^2-1\dots$
- $\dots$which exist for $q=3,5,7,11$ and which do not exist for $q=9$.
- When q is even, maximal partial ovoids of size q^2-1 do not exist.

Theorem

Let $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ be a GQ of order (s,t). Any $(st-\rho)$-arc of $\mathcal{S}$ with $0\le\rho<\frac{t}{s}$ is contained in an uniquely defined ovoid of $\mathcal{S}$.

Existence

- $\mathrm{Q}(4,q)$ has always ovoids.
- partial ovoids of size q^2 can always be extended to an ovoid
- We are interested in partial ovoids of size $q^2-1\ldots$
- $\ldots$which exist for $q=3,5,7,11$ and which do not exist for $q=9$.
- When q is even, maximal partial ovoids of size q^2-1 do not exist.

Theorem

Let $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ be a GQ of order (s,t). Any $(st-\rho)$-arc of $\mathcal{S}$ with $0\leq\rho<\frac{t}{s}$ is contained in an uniquely defined ovoid of $\mathcal{S}$.

Property of (q^2-1)-arcs

Theorem

Let $\mathcal{S}=(\mathcal{P},\mathcal{B},\mathrm{I})$ be a GQ of order (s,t). Let $\mathcal{K}$ be a maximal partial ovoid of size $st-\frac{t}{s}$ of $\mathcal{S}$. Let $\mathcal{B}'$ be the set of lines incident with no point of $\mathcal{K}$, and let $\mathcal{P}'$ be the set of points on at least one line of $\mathcal{B}'$ and let I' be the restriction of I to points of $\mathcal{P}'$ and lines of $\mathcal{B}'$. Then $\mathcal{S}'=(\mathcal{P}',\mathcal{B}',\mathrm{I}')$ is a subquadrangle of order $(s,\rho=\frac{t}{s})$.

Corollary

Suppose that $\mathcal{O}$ is a maximal (q^2-1)-arc of $\mathrm{Q}(4,q)$, then the lines of $\mathrm{Q}(4,q)$ not meeting $\mathcal{O}$ are the lines of a hyperbolic quadric $\mathrm{Q}^+(3,q)\subset\mathrm{Q}(4,Q)$.

Property of (q^2-1)-arcs

Theorem

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a GQ of order (s,t). Let $\mathcal{K}$ be a maximal partial ovoid of size $st - \frac{t}{s}$ of $\mathcal{S}$. Let $\mathcal{B}'$ be the set of lines incident with no point of $\mathcal{K}$, and let $\mathcal{P}'$ be the set of points on at least one line of $\mathcal{B}'$ and let I' be the restriction of I to points of $\mathcal{P}'$ and lines of $\mathcal{B}'$. Then $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathrm{I}')$ is a subquadrangle of order $(s, \rho = \frac{t}{s})$.

Corollary

Suppose that $\mathcal{O}$ is a maximal (q^2-1)-arc of $\mathrm{Q}(4,q)$, then the lines of $\mathrm{Q}(4,q)$ not meeting $\mathcal{O}$ are the lines of a hyperbolic quadric $\mathrm{Q}^+(3,q) \subset \mathrm{Q}(4,Q)$.

The GQ $T_2(\mathcal{C})$

Definition

An oval of $\mathrm{PG}(2, q)$ is a set of $q + 1$ points $\mathcal{C}$, such that no three points of $\mathcal{C}$ are collinear.

Let $\mathcal{C}$ be an oval of $\mathrm{PG}(2, q)$ and embed $\mathrm{PG}(2, q)$ as a hyperplane in $\mathrm{PG}(3, q)$. We denote this hyperplane with π_∞.
Define points as

(i) the points of $\mathrm{PG}(3, q) \setminus \mathrm{PG}(2, q)$,
(ii) the hyperplanes π of $\mathrm{PG}(3, q)$ for which $|\pi \cap \mathcal{C}| = 1$, and
(iii) one new symbol (∞).

Lines are defined as

(a) the lines of $\mathrm{PG}(3, q)$ which are not contained in $\mathrm{PG}(2, q)$ and meet $\mathcal{C}$ (necessarily in a unique point), and
(b) the points of $\mathcal{C}$.

The GQ $T_2(\mathcal{C})$

Definition

An oval of $\mathrm{PG}(2,q)$ is a set of $q+1$ points $\mathcal{C}$, such that no three points of $\mathcal{C}$ are collinear.

Let $\mathcal{C}$ be an oval of $\mathrm{PG}(2,q)$ and embed $\mathrm{PG}(2,q)$ as a hyperplane in $\mathrm{PG}(3,q)$. We denote this hyperplane with π_∞. Define points as

(i) the points of $\mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$,
(ii) the hyperplanes π of $\mathrm{PG}(3,q)$ for which $|\pi \cap \mathcal{C}| = 1$, and
(iii) one new symbol (∞).

Lines are defined as

(a) the lines of $\mathrm{PG}(3,q)$ which are not contained in $\mathrm{PG}(2,q)$ and meet $\mathcal{C}$ (necessarily in a unique point), and
(b) the points of $\mathcal{C}$.

$T_2(\mathcal{C})$ and $\mathrm{Q}(4,q)$

Theorem

When $\mathcal{C}$ is a conic of $\mathrm{PG}(2,q)$, $T_2(\mathcal{C}) \cong \mathrm{Q}(4,q)$.

Theorem

All ovals of $\mathrm{PG}(2,q)$ are conics, when q is odd.

Corollary

When q is odd, $T_2(\mathcal{C}) \cong \mathrm{Q}(4,q)$.

Suppose now that q is odd and $\mathcal{O}$ is a partial ovoid of $\mathrm{Q}(4,q) \cong T_2(\mathcal{C})$. We may assume that $(\infty) \in \mathcal{O}$.
If $\mathcal{O}$ has size k, then $\mathcal{O} = \{(\infty)\} \cup U$, where U is a set of $k-1$ points of type (i).

Directions

The set $\mathcal{O}$ is a partial ovoid, this implies that the line determined by two points of U cannot contain a point of $\mathcal{C}$.
So U is a set of points of $\mathrm{AG}(3, q)$ not determining $q + 1$ given directions.
If $|U| = q^2 - 2$, we want to show that U can be extended, so that the corresponding partial ovoid is not maximal. Keep in mind that this is not true for certain values of q
Denote by D the set of directions determined by U, denote by O the set of points $\pi_\infty \setminus D$.

The Rédei polynomial

Choose $\pi_\infty : X_3 = 0$. Set
$U = \{(a_i, b_i, c_i, 1) : i = 1, \ldots, k\} \subset \mathrm{AG}(3,q)$, then
$D = \{(a_i - a_j, b_i - b_j, c_i - c_j, 0) : i \neq j\}$
Define

$$R(X,Y,Z,W) = \prod_{i=1}^{k}(X + a_iY + b_iZ + c_iW)$$

then

$$R(X,Y,Z,W) = X^k + \sum_{i=1}^{k}\sigma_i(Y,Z,W)X^{k-i}$$

with $\sigma_i(X,Y,Z)$ the i-th elementary symmetric polynomial of the set $\{a_iY + b_iZ + c_iW | i = 1 \ldots k\}$.

The Rédei polynomial

Choose $\pi_\infty : X_3 = 0$. Set
$U = \{(a_i, b_i, c_i, 1) : i = 1, \dots, k\} \subset \mathrm{AG}(3, q)$, then
$D = \{(a_i - a_j, b_i - b_j, c_i - c_j, 0) : i \neq j\}$
Define

$$R(X,Y,Z,W) = \prod_{i=1}^{k} (X + a_i Y + b_i Z + c_i W)$$

then

$$R(X,Y,Z,W) = X^k + \sum_{i=1}^{k} \sigma_i(Y,Z,W) X^{k-i}$$

with $\sigma_i(X,Y,Z)$ the i-th elementary symmetric polynomial of the set $\{a_i Y + b_i Z + c_i W | i = 1 \dots k\}$.

The Rédei polynomial

Lemma

For any $x, y, z, w \in GF(q)$, $(y, z, w) \neq (0, 0, 0)$, *the multiplicity of* $-x$ *in the multi-set* $\{ya_i + zb_i + wc_i : i = 1, \ldots, k\}$ *is the same as the number of common points of* U *and the plane* $yX_0 + zX_1 + wX_2 + xX_3 = 0$.

The Rédei polynomial

From now on: $|U| = q^2 - 2$, q odd. We may then assume that $\sum a_i = \sum b_i = \sum c_i = 0$, implying $\sigma_1(X,Y,Z) = 0$.
Consider a line L in π_∞:

$$L : yX_0 + zX_1 + wX_2 = X_3 = 0$$

Suppose that $L \cap O \neq \emptyset$ then
$R(X,y,z,w)(X^2 - \sigma_2(y,z,w)) = (X^q - X)^q$.

The Rédei polynomial

From now on: $|U| = q^2 - 2$, q odd. We may then assume that $\sum a_i = \sum b_i = \sum c_i = 0$, implying $\sigma_1(X,Y,Z) = 0$.
Consider a line L in π_∞:

$$L : yX_0 + zX_1 + wX_2 = X_3 = 0$$

Suppose that $L \cap O \neq \emptyset$ then
$R(X,y,z,w)(X^2 - \sigma_2(y,z,w)) = (X^q - X)^q$.

Relations for σ

Define

$$S_k(Y,Z,W)=\sum_i (a_iY+b_iZ+c_iW)^k$$

Lemma

If the line with equation $yX_0+zX_1+wX_2=X_3=0$ has at least one common point with O, then $S_k(y,z,w)=0$ for odd k and $S_k(y,z,w)=-2\sigma_2^{k/2}(y,z,w)$ for even k.

The main theorem

Theorem

If $|U| = q^2 - 2$, $q = p^h$ and $|O| \geq p + 2$, then U can be extended by two points to a set of q^2 points determining the same directions.