The polynomial method in Galois geometries

Leo Storme

Ghent University
Dept. of Mathematics
Krijgslaan 281 - Building S22
9000 Ghent
Belgium

Lille, June 25, 2013
1. **Galois geometries**
   - 1. Affine spaces
   - 2. Projective spaces

2. **Blocking sets**
   - Linear blocking set
   - Multiple blocking sets in PG(2, q)
   - Multiple blocking sets and algebraic curves
   - Characterization result
Finite fields

- $q = \text{prime number.}$
  - **Prime fields** $\mathbb{F}_q = \{0, 1, \ldots, q - 1\} \pmod{q}$.
  - Binary field $\mathbb{F}_2 = \{0, 1\}$.
  - Ternary field $\mathbb{F}_3 = \{0, 1, 2\} = \{-1, 0, 1\}$.

- **Finite fields** $\mathbb{F}_q$: $q$ prime power.
### Affine Space $\text{AG}(n, q)$

- $V(n, q) = n$-dimensional vector space over $\mathbb{F}_q$.
- $\text{AG}(n, q) = V(n, q)$ plus parallelism.
- $k$-dimensional affine subspace = (translate) of $k$-dimensional vector space.
Let $\Pi_k$ be $k$-dimensional vector space of $V(n, q)$.

$\Pi_k + b$, for $b \in V(n, q)$, are the affine $k$-subspaces parallel to $\Pi_k$.

Two parallel affine $k$-subspaces are disjoint or equal.

Parallelism leads to partitions of $AG(n, q)$ into (parallel) affine $k$-subspaces.
AFFINE PLANE $AG(2, 3)$ OF ORDER 3
From $V(3, q)$ to $PG(2, q)$

Vector line $V(1, q)$

Vector plane $V(2, q)$

Projective point $PG(0, q)$

Projective line $PG(1, q)$

Leo Storme

Polynomial method in Galois geometries
FROM $V(3, q)$ TO $PG(2, q)$
THE FANO PLANE PG(2, 2)
THE PLANE $PG(2, 3)$
FROM $V(4,q)$ TO $\text{PG}(3,q)$

Vector line $V(1,q)$

Vector plane $V(2,q)$

Projective point $\text{PG}(0,q)$

Projective line $\text{PG}(1,q)$

Leo Storme

Polynomial method in Galois geometries
FROM $V(4, q)$ TO $PG(3, q)$

**Vector space $V(3, q)$**

**Vector space $V(4, q)$**

**Projective plane $PG(2, q)$**

**Projective 3-space $PG(3, q)$**
PG(3, 2)
FROM $V(n + 1, q)$ TO $PG(n, q)$

1. From $V(1, q)$ to $PG(0, q)$ (projective point),
2. From $V(2, q)$ to $PG(1, q)$ (projective line),
3. ... 
4. From $V(i + 1, q)$ to $PG(i, q)$ ($i$-dimensional projective subspace),
5. ... 
6. From $V(n, q)$ to $PG(n - 1, q)$ ($(n - 1)$-dimensional subspace = hyperplane),
7. From $V(n + 1, q)$ to $PG(n, q)$ ($n$-dimensional space).
Link between affine and projective spaces

\[ \text{AG}(n, q) = \text{PG}(n, q) \text{ minus one hyperplane (the hyperplane at infinity).} \]
LINK BETWEEN AG(2, 3) AND PG(2, 3)
1. **Galois Geometries**
   - 1. Affine spaces
   - 2. Projective spaces

2. **Blocking Sets**
   - Linear blocking set
   - Multiple blocking sets in $\text{PG}(2, q)$
   - Multiple blocking sets and algebraic curves
   - Characterization result
**Definition and Example**

**Definition**

*Blocking set* $B$ in $\text{PG}(2, q)$ is set of points, intersecting every line in at least one point.

**Example**

Line $L$ in $\text{PG}(2, q)$.
**EXAMPLE**

![Diagram of Galois geometries and blocking sets](image)

- Linear blocking set
- Multiple blocking sets in $\text{PG}(2, q)$
- Multiple blocking sets and algebraic curves
- Characterization result

**Galois geometries**

**Blocking sets**

Leo Storme

Polynomial method in Galois geometries
**Definition**

Point $r$ of blocking set $B$ in $\text{PG}(2, q)$ is *essential* if $B \setminus \{r\}$ is no longer blocking set.

**Definition**

Blocking set $B$ is *minimal* if all of its points are essential.

**Example**

Line $L$ of $\text{PG}(2, q)$ is minimal blocking set $B$ of size $q + 1$. 
**Definition**

*Non-trivial* blocking set $B$ in $\text{PG}(2, q)$ does not contain a line.

**Example:** Baer subplane $\text{PG}(2, \sqrt{q})$ in $\text{PG}(2, q)$, $q$ square.

**Notation:** $q + r(q) + 1 = \text{size of smallest non-trivial blocking set in PG}(2, q)$.

- (Blokhuis) $r(q) = (q + 1)/2$ for $q > 2$ prime,
- (Bruen) $r(q) = \sqrt{q}$ for $q$ square,
- (Blokhuis) $r(q) = q^{2/3}$ for $q$ cube power.
Consider $\text{PG}(2, q)$, $q = p^h$, $p$ prime, $h \geq 1$.
- $\mathbb{F}_q$ has $\mathbb{F}_{p^e}$, $e | h$, as subfield.
- $\text{PG}(h/e, p^e)$ is naturally embedded subgeometry of $\text{PG}(h/e, q)$.
- Project $\text{PG}(h/e, p^e)$ onto plane $\text{PG}(2, q)$.
- Projection $B$ is (linear) blocking set of $\text{PG}(2, q)$. 
Galois geometries
Blocking sets

Linear blocking set
Multiple blocking sets in $\text{PG}(2, q)$
Multiple blocking sets and algebraic curves
Characterization result

Leo Storme
Polynomial method in Galois geometries
PARTICULAR PROPERTIES OF LINEAR BLOCKING SETS

- Line intersects $B$ in $1 \pmod{p^e}$ points.
- If line $L$ shares $1 + p^e$ points with $B$, then $L \cap B = \text{PG}(1, p^e)$.

**Theorem (Sziklai and Szőnyi)**

Let $B$ be minimal blocking set in $\text{PG}(2, q)$, $q = p^h$, $p$ prime, $h \geq 1$, with $|B| < q + (q + 3)/2$. Then

- $B$ intersects every line in $1 \pmod{p^e}$ points, for some $e|h$,
- If $e$ is the maximal integer with this property, then $e|h$, and if line $L$ shares $1 + p^e$ points with $B$, then $L \cap B = \text{PG}(1, p^e)$.
DEFINITIONS

**Definition**
- **$t$-Fold blocking set $B$ in PG$(2, q)$**: intersects every line in at least $t$ points.
- **Minimal $t$-fold blocking set**: no proper subset is still $t$-fold blocking set.
EXAMPLES

- Union of $t$ pairwise disjoint Baer subplanes $\text{PG}(2, \sqrt{q})$ in $\text{PG}(2, q)$, $q$ square.
- (Polverino and Storme) Union of disjoint Baer subplane $\text{PG}(2, \sqrt{q})$ and projected subgeometry $\text{PG}(3, q^{1/3})$ in $\text{PG}(2, q)$, when $q$ is 6-th power.
- Union of two disjoint linear non-trivial blocking sets.
Galois geometries

Blocking sets

Linear blocking set

Multiple blocking sets in $\text{PG}(2, q)$

Multiple blocking sets and algebraic curves

Characterization result

Leo Storme

Polynomial method in Galois geometries
Galois geometries

Blocking sets

Linear blocking set

Multiple blocking sets in $\text{PG}(2, q)$

Multiple blocking sets and algebraic curves

Characterization result

Leo Storme

Polynomial method in Galois geometries
**Setting for Rédei-polynomial**

- $B = t$-fold blocking set in $\text{PG}(2, q)$ of size $t(q + 1) + c$, with $t + c < q$.
- $P$ point of $B$.
- Line $\ell = t$-secant of $B$ through $P$.
- Homogeneous coordinates $(X : Y : Z)$ such that
  - $P = (0 : 1 : 0) = (\infty)$,
  - $\ell : Z = 0$,
  - $B \cap \ell = \{(1 : -y_j : 0) || j = 1, \ldots, t - 1\} \cup \{(0 : 1 : 0)\}$. 

---

**Leo Storme**

**Polynomial method in Galois geometries**
\[ A = \text{affine plane } \text{PG}(2, q) \setminus \ell, \text{ such that } (x, y) = (x : y : 1), \]

\[ B \cap A = \{(a_i, b_i) \mid i = 1, \ldots, tq + c\}. \]

\[ F(U, V) = \prod_{j=1}^{t-1} (V + y_j) \prod_{i=1}^{tq+c} (U + a_i V + b_i). \]

(Rédei-polynomial)

\[ F(U, V) = \sum_{i=0}^{t} F_i(U, V)(U^q - U)^{t-i}(V^q - V)^i, \]

where \( \text{deg}(F_i) \leq \text{deg}(F) - qt. \)
Rédei-polynomial

- Homogeneous part of largest degree and substitute $V = 1$, 

$$f(U) := \left( U + a_i \right)^{tq+c} = \sum_{i=0}^{t} f_i(U) U^{q(t-i)},$$

where $f_i(U) = F_{i0}(U, 1)$, and where $F_{i0}$ is homogeneous part of $F_i(U, V)$ of highest degree.

- Since $B$ is $t$-fold blocking set, $f$ contains factor $U + y$ at least $t - 1$ times, for all $y \in \mathbb{F}_q$.

- So $f$ is divisible by $(U^q - U)^{t-1}$. Dividing by $(U^q - U)^{t-1}$, we obtain excess polynomial

$$\text{ex}(U) = U^q f_0(U) + f_1(U) + (t - 1)Uf_0(U).$$
Rédei polynomial

Excess polynomial

$$\text{ex}(U) = U^q f_0(U) + f_1(U) + (t - 1)Uf_0(U)$$

contains information about lines through $P$ having more than $t$ points of $B$.

**Definition**

Let $\text{ex}(U)$ be excess polynomial of $P$. Let $q = p^n$, $p$ prime. Let $d(U) = \gcd(f_0(U), f_1(U))$. If $e$ is largest integer for which $\text{ex}(U)/d(U)$ is $p^e$-th power, then $e$ is called exponent of $P$. 
Rédei polynomial

**Notation:** $\deg(f) = f^\circ$.

**Theorem (Blokhuis, Storme, Szőnyi)**

Let $f \in \mathbb{F}_q[X]$, $q = p^n$, $p$ prime, be fully reducible, $f(X) = X^q h(X) + g(X)$, where $\gcd(g, h) = 1$. Let $k = \max(g^\circ, h^\circ) < q$. Let $e$ be maximal such that $f$ is $p^e$-th power. Then:
Rédei polynomial

**Theorem (Blokhuis, Storme, Szőnyi)**

1. \( e = n \) and \( k = 0 \);
2. \( e \geq 2n/3 \) and \( k \geq p^e \);
3. \( 2n/3 > e > n/2 \) and \( k \geq p^{n-e/2} - (3/2)p^{n-e} \);
4. \( e = n/2 \) and \( k = p^e \) and \( f(X) = a\text{Tr}(bX + c) + d \) or \( f(X) = a\text{Norm}(bX + c) + d \) for suitable constants \( a, b, c, d \).
5. \( e = n/2 \) and \( k \geq p^e \left[ \frac{1}{4} + \sqrt{(p^e + 1)/2} \right] \);
6. \( n/2 > e > n/3 \) and \( k \geq p^{n/2+e/2} - p^{n-e} - p^e/2 \), or if \( 3e = n + 1 \) and \( p \leq 3 \), then \( k \geq p^e(p^e + 1)/2 \);
7. \( n/3 \geq e > 0 \) and \( k \geq p^e \left[ (p^{n-e} + 1)/(p^e + 1) \right] \);
8. \( e = 0 \) and \( k \geq (q + 1)/2 \);
9. \( e = 0, k = 1 \) and \( f(X) = a(X^q - X) \).
**Lemma**

Let $B$ be minimal $t$-fold blocking set, $|B| = t(q + 1) + c$ and let $P \in B$. Then at least $q - c$ lines through $P$ intersect $B$ in exactly $t$ points.

**Proof:**

- Let $P = (0 : 1 : 0)$ and denote by $e$ the exponent of $P$.
- $\text{ex}(U) = U^q h(U) + g(U)$, with $h^o, g^o \leq c$.
- Let $d(U) = \gcd(h(U), g(U))$, then
  $\text{ex}(U)/d(U) = (U^q/p^e h_1(U) + g_1(U))p^e$.
- Number of lines that are not $t$-secants is at most $c + 1$. 
**IMPORTANT LEMMA**

**Lemma**

Let $B$ be minimal $t$-fold blocking set of $\mathbb{PG}(2, q)$ of size $tq + t + c$. Let $P$ be point of exponent $e$. Then

1. $P$ lies on at least $2 + (q - c)/p^e$ lines meeting $B$ in at least $p^e + t$ points;
2. $P$ lies on at least $(q - 3c)/p^e + 4$ distinct $(p^e + t)$-secants to $B$. 

Leo Storme | Polynomial method in Galois geometries
Proof:

- Assume \( d(U) = 1 \).
- \( \text{ex}(U) = (e_1(U))^{p^e} = (U^{q/p^e} h_1(U) + g_1(U))^{p^e} \), with \( g_1^\circ, h_1^\circ \leq c/p^e \).
- Then \( \text{gcd}(e_1(U), e'_1(U)) \) divides \( g_1(U)h'_1(U) - g'_1(U)h_1(U) \), and contains contribution of multiple roots of \( e_1 \).
- \( \text{deg}(g_1(U)h'_1(U) - g'_1(U)h_1(U)) \leq 2c/p^e - 2 \).
- So, \( e_1(U) \) has at least \( (q - c)/p^e + 2 \) distinct roots. At most \( 2c/p^e - 2 \) of them can be multiple roots, hence \( e_1(U) \) has at least \( (q - 3c)/p^e + 4 \) simple roots.
**Setting for Algebraic Curves**

- $B = t$-fold blocking set with $|B| = tq + t + c$, with $c + t < (q + 3)/2$.
- Exponent of any point in $B$ is $e > 0$.
- (so, intuitively, every line intersects $B$ in $t \mod p^e$ points)

**Definition**

Let $\text{ex}(U)$ be excess polynomial of $P$. Let $q = p^n$, $p$ prime. Let $d(U) = \gcd(f_0(U), f_1(U))$. If $e$ is largest integer for which $\text{ex}(U)/d(U)$ is $p^e$-th power, then $e$ is called exponent of $P$. 

Leo Storme

Polynomial method in Galois geometries
Setting for algebraic curves

\[ F(U, V) = \prod_{j=1}^{t-1} (V + y_j) \prod_{i=1}^{tq+c} (U + a_i V + b_i). \]

\[ F(U, V) = (U^q - U)^t F_0(U, V) + (U^q - U)^{t-1} (V^q - V) F_1(U, V) + \cdots + (V^q - V)^t F_t(U, V), \]

where \( \deg(F_i) \leq c + t - 1. \)
Useful lemmas

**Lemma**

If line $Y = -mX - b$ intersects $B \cap A$ in more than $t$ points, then $F_0(b, m) = \ldots = F_t(b, m) = 0$.

**Lemma**

$F_0, \ldots, F_t$ have no common divisor, dependent on $U$. 
THEOREM

For a $t$-fold blocking set $B$ in $PG(2, q)$, where $q = p^h$, $p$ prime, $h \geq 1$, with $|B| = tq + t + c$, $c + t < (q + 3)/2$, intersects every line in $t \pmod{p}$ points.

**Proof:**

- Absolutely irreducible component $H(U, V)$ of $F_0(U, V) / \prod_{j=1}^{t-1} (V + y_j)$, with $\deg(H) = s$.
- $\exists i$ for which $H(U, V) \not\| F_i(U, V)$. 

Leo Storme  
Polynomial method in Galois geometries
THEOREM

(Proof, continued)

- If $H'_U \neq 0$, then $H$ has at least

$$ (q + 1 - t)s - s(s - 1) $$

$\mathbb{F}_q$-rational points (Blokhuis, Pellikaan, Szőnyi).

- These points all belong to $F_i$, and Bézout's theorem gives

$$ (q + 1 - t)s - s(s - 1) \leq s(c + t - 1). $$

- Gives inequality

$$ c + t + (t + s) \geq q + 3, $$

and as $s \leq c$,

$$ c + t \geq (q + 3)/2. $$
**Theorem**

- If $c + t < (q + 3)/2$, then $H'_U \equiv 0$ for any component $H$.
- All lines intersect $B$ in $t \pmod{p}$ points.

**Theorem**

$t$-Fold blocking set $B$ in $\text{PG}(2, q)$, $q = p^h$, $p$ prime, $h \geq 1$, with $|B| = tq + t + c$, $c + t < (q + 3)/2$, intersects every line in $t \pmod{p}$ points.
Let $B$ be minimal $t$-fold blocking set of $\text{PG}(2, p^{6m})$ of size $t(q + 1) + c$, with $2 \leq t < q^{1/4}/4$, and $c < p^{4m}\sqrt{p}/2$.

**Lemma**

*Point of $B$ has exponent $4m$, $3m$ or $2m$. Moreover, when $e = 3m$, then this point defines dual Baer subline of lines all containing at least $p^{3m} + t$ points of $B$.***
Rédei polynomial theorem (Blokhuis, Storme, Szőnyi)

1. \( e = n \) and \( k = 0 \);
2. \( e \geq 2n/3 \) and \( k \geq p^e \);
3. \( 2n/3 > e > n/2 \) and \( k \geq p^{n-e/2} - (3/2)p^{n-e} \);
4. \( e = n/2 \) and \( k = p^e \) and \( f(X) = a \text{Tr}(bX + c) + d \) or \( f(X) = a \text{Norm}(bX + c) + d \) for suitable constants \( a, b, c, d \).
5. \( e = n/2 \) and \( k \geq p^e \left[ \frac{1}{4} + \sqrt{(p^e + 1)/2} \right] \);
6. \( n/2 > e > n/3 \) and \( k \geq p^{n/2+e/2} - p^{n-e} - p^e/2 \), or if \( 3e = n + 1 \) and \( p \leq 3 \), then \( k \geq p^e(p^e + 1)/2 \);
7. \( n/3 \geq e > 0 \) and \( k \geq p^e [(p^{n-e} + 1)/(p^e + 1)] \);
8. \( e = 0 \) and \( k \geq (q + 1)/2 \);
9. \( e = 0, k = 1 \) and \( f(X) = a(X^q - X) \).
**Definition**

Line containing at least $p^{4m} + t$ points of $B$ is called *very long*, while line meeting $B$ in at least $p^{3m} + t$ points is called *long*.

**Lemma**

*Dual Baer subline of long lines through point of exponent $3m$ is unique.*
**Definition**

If $P$ is point of $t$-fold blocking set $B$ of exponent $3m$ defining dual Baer subline of long lines, and $\ell$ is one of the lines of this dual Baer subline, then we call $P$ special point of $\ell$.

**Lemma**

*If line $\ell$ contains $2t + 1$ special points, Baer subplane contained in $B$.***
Galois geometries
Blocking sets
Linear blocking set
Multiple blocking sets in PG(2, q)
Multiple blocking sets and algebraic curves
Characterization result

Leo Storme
Polynomial method in Galois geometries
If there is Baer subplane $S$ contained in $B$, then $B \setminus S$ is minimal $(t - 1)$-fold blocking set.
From now on, line $\ell$ contains at most $2t$ special points.

**Lemma**

$B$ has at most $c$ points of exponent $3m$.

**Lemma**

There are at most $2t$ points of exponent $4m$. 
Theorem (Blokhuis, Lovász, Storme, Szőnyi)

$t$-Fold blocking set $B$ in $\text{PG}(2, p^{6m})$, $2 \leq t < p^{3m/2}/4$, with $|B| < tp^{6m} + p^{4m}\sqrt{p}/2 + t$, not containing Baer subplane, has size $|B| \geq tp^{6m} + tp^{4m} - O(p^{2m})$. 

Characterization result
Thank you very much for your attention!