Galois geometries contributing to coding theory

Leo Storme

Ghent University
Dept. of Pure Mathematics and Computer Algebra
Krijgslaan 281 - S22
9000 Ghent
Belgium

Thurnau, April 15, 2010

Outline

OUTLINE

LINEAR CODES

- q = prime number,
- **Prime fields**: $\mathbb{F}_q = \{1, \ldots, q\} \pmod{q}$,
- **Finite fields (Galois fields):** $\mathbb{F}_q$: q prime power,
- **Linear** $[n, k, d]$**-code** C **over** $\mathbb{F}_q$ is:
  - k-dimensional subspace of $V(n, q)$,
  - *minimum distance* d = minimal number of positions in which two distinct codewords differ.

LINEAR CODES

- **Generator matrix of $[n, k, d]$-code C**

$$G = (g_1 \cdots g_n)$$

  - $G = (k \times n)$ matrix of rank k,
  - rows of G form basis of C,
  - codeword of C = linear combination of rows of G.

Linear codes

- **Parity check matrix H for C**
  - $(n-k) \times n$ matrix of rank $n-k$,
  - $c \in C \Leftrightarrow c \cdot H^T = \bar{0}$.

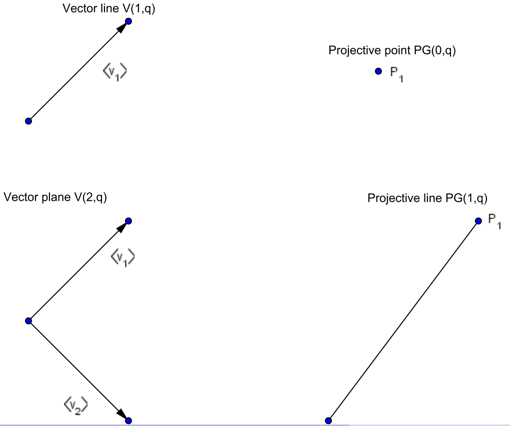
REMARK

Remark: For linear $[n, k, d]$-code C, n, k, d do not change when column g_i in generator matrix

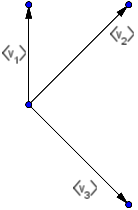
$$G = (g_1 \cdots g_n)$$

is replaced by non-zero scalar multiple.

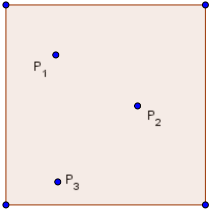
From vector space to projective space

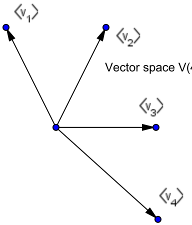


Vector space V(3,q)

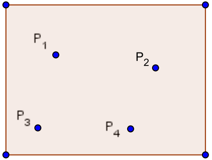


Projective plane PG(2,q)





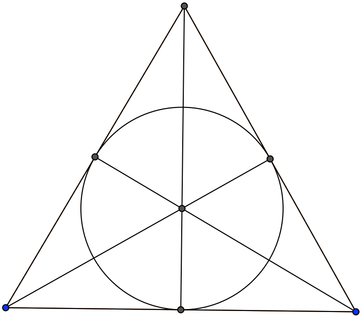
Vector space V(4,q)



Projective 3-space PG(3,q)

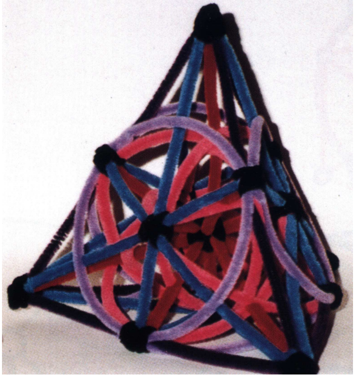
THE FANO PLANE $\mathrm{PG}(2,2)$

From $V(3,2)$ to $\mathrm{PG}(2,2)$



$\mathrm{PG}(3,2)$

From $V(4,2)$ to $\mathrm{PG}(3,2)$



OUTLINE

Griesmer bound and minihypers

Question: Given

- dimension k,
- minimal distance d,

find minimal length n of $[n, k, d]$-code over $\mathbb{F}_q$.

Result: Griesmer (lower) bound

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = g_q(k, d).$$

Minihypers and Griesmer bound

Equivalence: (Hamada and Helleseth)

Griesmer (lower) bound
equivalent with
minihypers in finite projective spaces

DEFINITION

DEFINITION

$\{f, m; k-1, q\}$-minihyper F is:

- set of f points in $\mathrm{PG}(k-1, q)$,
- F intersects every $(k-2)$-dimensional space in at least m points.

(m-fold blocking sets with respect to the hyperplanes of $\mathrm{PG}(k-1, q)$)

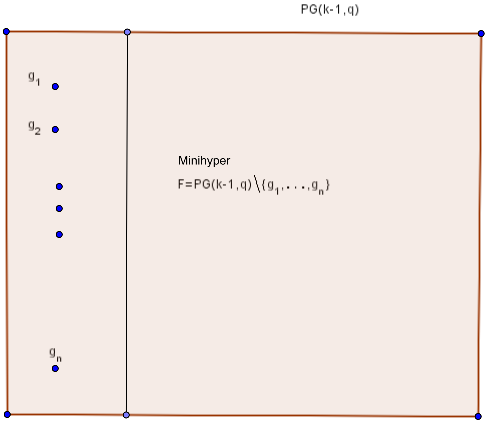
MINIHYPERS AND GRIESMER BOUND

- Let C = $[g_q(k,d),k,d]$-code over $\mathbb{F}_q$.
- If generator matrix

$$G = (g_1 \cdots g_n),$$

minihyper = $\mathrm{PG}(k-1,q) \setminus \{g_1,\ldots,g_n\}$.

Minihypers and Griesmer bound



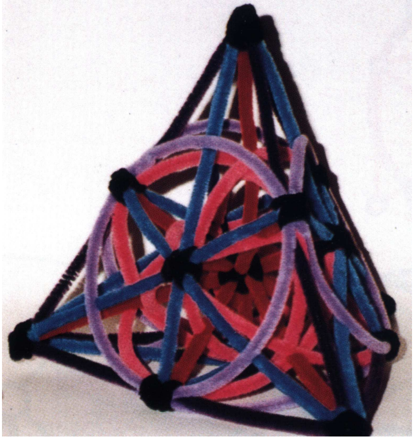
EXAMPLE

Example: Griesmer [8,4,4]-code over $\mathbb{F}_2$

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

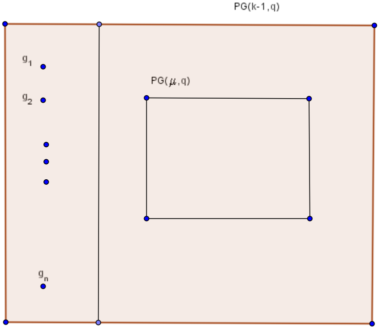
minihyper = $PG(3,2) \setminus$ {columns of G} = plane ($X_0 = 0$).

CORRESPONDING MINIHYPER



Other examples

Example 1. Subspace PG(μ, q) in PG$(k-1, q)$ = minihyper of $[n = (q^k - q^{\mu+1})/(q-1), k, q^{k-1} - q^{\mu}]$-code (McDonald code).



Bose-Burton theorem

Theorem (Bose-Burton)

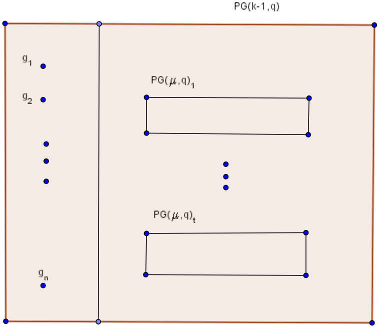
A minihyper consisting of $|PG(\mu, q)|$ points intersecting every hyperplane in at least $|PG(\mu - 1, q)|$ points is equal to a μ-dimensional space $PG(\mu, q)$.

RAJ CHANDRA BOSE

R.C. Bose and R.C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the McDonald codes. *J. Combin. Theory*, 1:96-104, 1966.

Other examples

Example 2. $t < q$ pairwise disjoint subspaces PG$(\mu, q)_i$, $i = 1, \ldots, t$, in PG$(k-1, q)$ = minihyper of $[n = (q^k - 1)/(q-1) - t(q^{\mu+1} - 1)/(q-1), k, q^{k-1} - tq^{\mu}]$-code.



CHARACTERIZATION RESULT

THEOREM (GOVAERTS AND STORME)

For q odd prime and $1 \leq t \leq (q+1)/2$, $[n = (q^k - 1)/(q-1) - t(q^{\mu+1} - 1)/(q-1), k, q^{k-1} - tq^{\mu}]$-code C: minihyper is union of t pairwise disjoint $PG(\mu, q)$.

OTHER CHARACTERIZATION RESULTS

- Minihypers involving subspaces of different dimension:
  - Hamada, Helleseth, and Maekawa: ϵ_0 points, ϵ_1 lines, ..., ϵ_{k-2} PG$(k-2, q)$, where $\sum_{i=0}^{k-2} \epsilon_i < \sqrt{q} + 1$,
  - De Beule, Metsch, and Storme: improvements to Hamada, Helleseth, and Maekawa.
    For q prime, $\sum_{i=0}^{k-2} \epsilon_i < (q+1)/2$.
- Minihypers involving subgeometries over $\mathbb{F}_{\sqrt{q}}$ in PG$(k-1, q)$, q square:
  - Govaerts and Storme,
  - De Beule, Hallez, Metsch, and Storme.

Outline

Well-known extendability result

Theorem

Every linear binary $[n, k, d]$-code C, d odd, is extendable to linear binary $[n+1, k, d+1]$-code.

Hill-Lizak result

Theorem (Hill and Lizak)

Let C be linear $[n, k, d]$-code over $\mathbb{F}_q$, with $\gcd(d, q) = 1$ and with all weights congruent to 0 or $d \pmod q$. Then C can be extended to $[n+1, k, d+1]$-code all of whose weights are congruent to 0 or $d+1 \pmod q$.

Proof: Subcode of all codewords of weight congruent to 0 $\pmod q$ is linear subcode C_0 of dimension $k-1$. If G_0 defines C_0 and

$$G = \left(\frac{x}{G_0} \right),$$

then

Hill-Lizak result

$$\hat{G} = \left(\begin{array}{c|c} x & 1 \\ \hline & 0 \\ G_0 & \vdots \\ & 0 \end{array} \right)$$

defines C. $\square$

Geometrical counterpart of Landjev

Definition

Multiset K in $\mathrm{PG}(k-1,q)$ is $(n,w;k-1,q)$-*multiarc* or $(n,w;k-1,q)$-*arc* if

1. sum of all weights of points of K is n,
2. hyperplane H of $\mathrm{PG}(k-1,q)$ contains at most w (weighted) points of K and some hyperplane H_0 contains w (weighted) points of K.

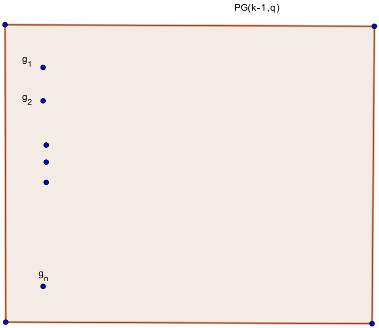
LINEAR CODES AND MULTIARCS

- Let C = $[n, k, d]$-code over $\mathbb{F}_q$.
- If generator matrix

$$G = (g_1 \cdots g_n),$$

then $\{g_1, \ldots, g_n\}$ = $(n, w = n - d; k - 1, q)$-multiarc.

LINEAR CODES AND MULTIARCS



Geometrical counterpart of Landjev

- C linear $[n, k, d]$-code over $\mathbb{F}_q$, $\gcd(d, q) = 1$ and with all weights congruent to 0 or $d \pmod q$. Then C can be extended to $[n+1, k, d+1]$-code all of whose weight are congruent to 0 or $d+1 \pmod q$.
- K =$(n, w; k-1, q)$-multiarc with $\gcd(n-w, q) = 1$ and intersection size of K with all hyperplanes congruent to n or $w \pmod q$. Then K can be extended to $(n+1, w; k-1, q)$-multiarc.

Geometrical counterpart of Landjev

Proof: Hyperplanes H containing $n \pmod q$ points of K form dual blocking set $\tilde{B}$ with respect to codimension 2 subspaces of $\mathrm{PG}(k-1, q)$. Also

$$\tilde{B} = \frac{q^{k-1}-1}{q-1}.$$

By dual of Bose-Burton, $\tilde{B}$ consists of all hyperplanes through particular point P.
This point P extends K to $(n+1, w; k-1, q)$-multiarc. $\square$

Blocking sets in PG$(2, q)$

Definition

Blocking set B in PG$(2, q)$: intersects every line in at least one point.

Trivial example: Line.

Definition

Non-trivial blocking set in PG$(2, q)$: contains no line.

Blocking sets in PG$(2, q)$

$q + r(q) + 1$ = size of smallest non-trivial blocking set in PG$(2, q)$.

- (Blokhuis) $r(q) = (q + 1)/2$ for $q > 2$ prime,
- (Bruen) $r(q) = \sqrt{q} + 1$ for q square,
- (Polverino) $r(q) = q^{2/3} + q^{1/3} + 1$ for q cube power.

IMPROVED RESULTS

THEOREM (LANDJEV AND ROUSSEVA)

Let $\mathcal{K}$ be $(n, w; k-1, q)$-arc, $q = p^s$, with spectrum $(a_i)_{i \geq 0}$. Let $w \not\equiv n \pmod{q}$ and

$$\sum_{i \not\equiv w \pmod{q}} a_i < q^{k-2} + q^{k-3} + \cdots + 1 + q^{k-3} \cdot r(q), \qquad (1)$$

where $q + r(q) + 1$ is minimal size of non-trivial blocking set of $PG(2, q)$. Then $\mathcal{K}$ is extendable to $(n+1, w; k-1, q)$-arc.

Improved results

Theorem

Let C be non-extendable $[n,k,d]$-code over $\mathbb{F}_q$, $q=p^s$, with $\gcd(d,q)=1$. If $(A_i)_{i\geq 0}$ is the spectrum of C, then $\sum_{i\not\equiv 0,d \pmod q} A_i \geq q^{k-3}\cdot r(q)$, where $q+r(q)+1$ is minimal size of non-trivial blocking set of $PG(2,q)$.

IMPROVED RESULTS

Let C be $[n, k, d]$-code over $\mathbb{F}_q$ with $k \geq 3$ and with $\gcd(d, q) = 1$, and with spectrum $(A_i)_{i \geq 0}$.
Define

$$\Phi_0 = \frac{1}{q-1} \sum_{q|i, i \neq 0} A_i, \quad \Phi_1 = \frac{1}{q-1} \sum_{i \not\equiv 0, d \pmod q} A_i.$$

The pair (Φ_0, Φ_1) is the *diversity* of C.
Theorem of Hill and Lizak states that every linear code with $\Phi_1 = 0$ is extendable.

IMPROVED RESULTS

THEOREM (MARUTA)

Let $q \geq 5$ be odd prime power and let $k \geq 3$. For linear $[n, k, d]$-code C over $\mathbb{F}_q$ with $d \equiv -2 \pmod q$ and with diversity (Φ_0, Φ_1) such that $A_i = 0$ for all $i \not\equiv 0, -1, -2 \pmod q$, the following results are equivalent:

1. *C is extendable.*
2. $(\Phi_0, \Phi_1) \in \{(v_{k-1}, 0), (v_{k-1}, 2q^{k-2}), (v_{k-1} + (\rho - 2)q^{k-2}, 2q^{k-2})\} \cup \{(v_{k-1} + iq^{k-2}, (q-2i)2^{k-2} \mid i = 1, \ldots, \rho - 1\}$*, where* $\rho = (q+1)/2$.

Furthermore, if 1. and 2. are valid and if $(\Phi_0, \Phi_1) \neq (v_{k-1} + (\rho - 2)q^{k-2}, 2q^{k-2})$, then C is doubly extendable.

OUTLINE

DEFINITION

DEFINITION

Let C be linear $[n, k, d]$-code over $\mathbb{F}_q$. The *covering radius* of C is smallest integer R such that every n-tuple in $\mathbb{F}_q^n$ lies at Hamming distance at most R from codeword in C.

THEOREM

Let C be linear $[n, k, d]$-code over $\mathbb{F}_q$ with parity check matrix

$$H = (h_1 \cdots h_n).$$

Then covering radius of C is equal to R if and only if every $(n-k)$-tuple over $\mathbb{F}_q$ can be written as linear combination of at most R columns of H.

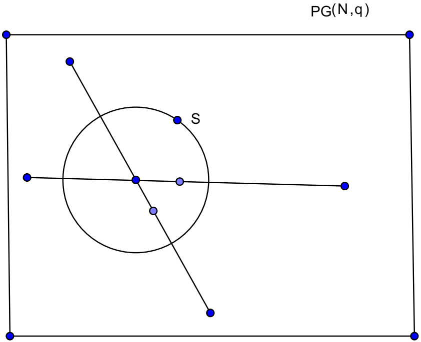
Definition

Definition

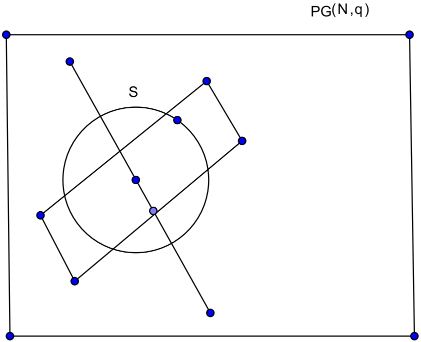
Let S be subset of $\mathrm{PG}(N, q)$. The set S is called ρ-*saturating* when every point P from $\mathrm{PG}(N, q)$ can be written as linear combination of at most $\rho + 1$ points of S.

Covering radius ρ for linear $[n, k, d]$-code equivalent with
$(\rho - 1)$-saturating set in PG$(n - k - 1, q)$

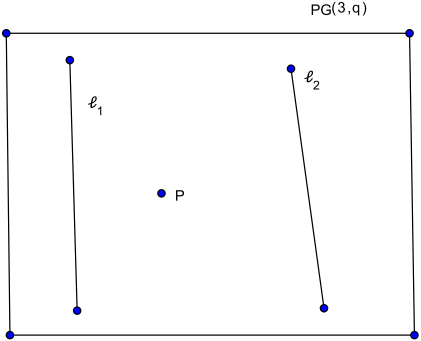
1-SATURATING SETS



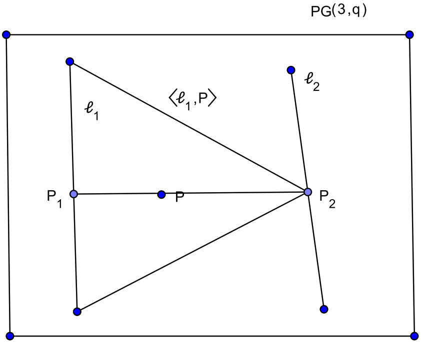
2-SATURATING SETS



1-Saturating set in $PG(3, q)$ of size $2q + 2$



1-Saturating set in $\mathrm{PG}(3, q)$ of size $2q + 2$



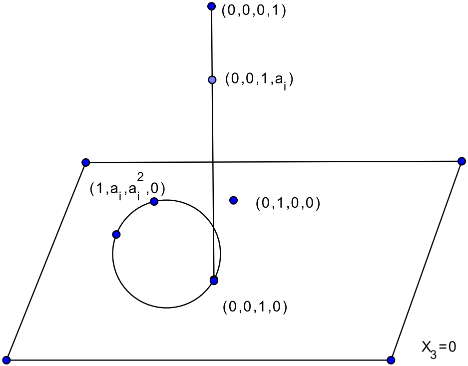
Example of Östergård and Davydov

Let $\mathbb{F}_q = \{a_1 = 0, a_2, \ldots, a_q\}$.

$$H_1 = \left[\begin{array}{ccc|c|cccc} 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ a_1 & \cdots & a_q & 1 & 0 & 0 & \cdots & 0 \\ a_1^2 & \cdots & a_q^2 & 0 & 0 & 1 & \cdots & 1 \\ 0 & \cdots & 0 & 0 & 1 & a_2 & \cdots & a_q \end{array}\right]$$

Columns of H_1 define 1-saturating set of size $2q + 1$ in PG$(3, q)$.

Example of Östergård and Davydov

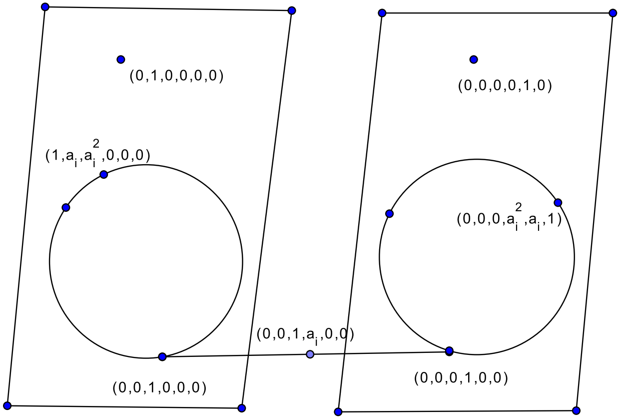


Example of Östergård and Davydov

$$H_2 = \left[\begin{array}{ccc|c|ccc|ccc|c} 1 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ a_1 & \cdots & a_q & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ a_1^2 & \cdots & a_q^2 & 0 & 1 & \cdots & 1 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 & a_2 & \cdots & a_q & a_1^2 & \cdots & a_q^2 & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a_1 & \cdots & a_q & 1 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 & 0 \end{array}\right],$$

Columns of H_2 define 2-saturating set of size $3q + 1$ in $\mathrm{PG}(5, q)$.

Example of Östergård and Davydov



OUTLINE

Linear MDS codes and arcs

Question:
Given

- length n,
- dimension k,

find maximal value of d.
Result: Singleton (upper) bound

$$d \leq n - k + 1.$$

Notation: MDS code = $[n, k, n-k+1]$-code.

ARCS

Equivalence:

Singleton (upper) bound (MDS codes)
equivalent with
***Arcs in finite projective spaces* (Segre)**

DEFINITION

DEFINITION

n-Arc in $\mathrm{PG}(k-1, q)$: set of n points, every k linearly independent.

Example: n-arc in $\mathrm{PG}(2, q)$: n points, no three collinear.

Normal rational curve

Classical example of arc:

$$\{(1, t, \ldots, t^{k-1}) || t \in \mathbb{F}_q\} \cup \{(0, \ldots, 0, 1)\}$$

defines $[q+1, k, d = q+2-k]$-GDRS (**Generalized Doubly-Extended Reed-Solomon**) code with generator matrix

$$G = \begin{pmatrix} 1 & \cdots & 1 & 0 \\ t_1 & \cdots & t_q & 0 \\ \vdots & \vdots & \vdots & \vdots \\ t_1^{k-2} & \cdots & t_q^{k-2} & 0 \\ t_1^{k-1} & \cdots & t_q^{k-1} & 1 \end{pmatrix}$$

CHARACTERIZATION RESULT

THEOREM (SEGRE, THAS)

For

- *q odd prime power,*
- $2 \leq k < \sqrt{q}/4$,

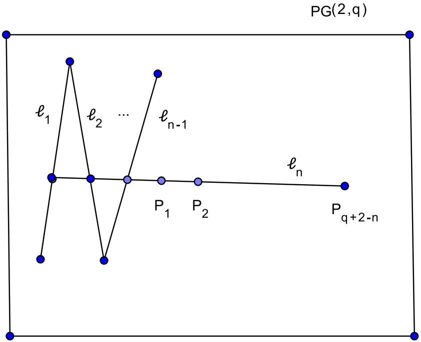
$[n = q + 1, k, d = q + 2 - k]$*-MDS code is GDRS.*

Technique used by Segre and Thas

- n-Arc in $\mathrm{PG}(2, q)$: set of n points, no three collinear.
- Dual n-arc in $\mathrm{PG}(2, q)$: set of n lines, no three concurrent.

Consequence: Point of $\mathrm{PG}(2, q)$ lies on zero, one, or two lines of dual n-arc.

POINTS ON ONE LINE OF DUAL n-ARC



TECHNIQUE USED BY SEGRE AND THAS

THEOREM (SEGRE)

Points of $PG(2,q)$, q odd, belonging to one line of dual n-arc in $PG(2,q)$ belong to algebraic curve Γ of degree $2(q+2-n)$.

If n large (close to $q+1$), then Γ contains $q+1-n$ lines, extending dual n-arc to dual $(q+1)$-arc.

THEOREM (VOLOCH)

For

- *q odd prime,*
- *$2 \leq k < q/45$,*

$[n = q+1, k, d = q+2-k]$-MDS code is GDRS.

Ball result

Theorem (Ball)

For q odd prime, $n \leq q+1$ for every $[n, k, n-k+1]$-MDS code.

Technique: Polynomial techniques

Thank you very much for your attention!