An introduction to codes from finite projective planes

Geertrui Van de Voorde

University of Canterbury

Codes from Desarguesian projective planes

Conics and hyperovals

KM-arcs

Blocking sets

- A: Incidence matrix of $\mathrm{PG}(2,q)$, $q = p^h$, p prime:
  - rows=lines of $\mathrm{PG}(2,q)$
  - columns=points of $\mathrm{PG}(2,q)$
  - with entry

$$a_{ij} = \begin{cases} 1 & \text{if point } j \text{ belongs to line } i, \\ 0 & \text{otherwise.} \end{cases}$$

- $\mathrm{C}_1(2,q)$: row span of A
- Generated over $\mathbb{F}_p$.

The code $\mathrm{C}_1(2, q)$, $q = p^h$ has:

- Length $n = q^2 + q + 1$,

The code $C_1(2, q)$, $q = p^h$ has:

- Length $n = q^2 + q + 1$,
- Dimension: $\binom{p+1}{2}^h + 1$ (Hamada/Goethals-Delsarte)

The code $\mathrm{C}_1(2, q)$, $q = p^h$ has:

- Length $n = q^2 + q + 1$,
- Dimension: $\binom{p+1}{2}^h + 1$ (Hamada/Goethals-Delsarte)
- Distance d=minimum weight =? .

$\rightsquigarrow$ *blocking sets*.

DEFINITION

The dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$:

Set of vectors v with $v.c = 0$ for all $c \in \mathcal{C}$.

DEFINITION

The dual code $\mathcal{C}^{\perp}$ of $\mathcal{C}$:

Set of vectors v with $v.c = 0$ for all $c \in \mathcal{C}$.

For $C_1(2, q)^{\perp}$:

- Length $n = q^2 + q + 1$,
- Dimension: $q^2 + q + 1 - (\binom{p+1}{2}^h + 1)$
- Distance $d = ?$.

$\rightsquigarrow$ sets without tangents.

DEFINITION

The dual code $\mathcal{C}^\perp$ of $\mathcal{C}$:

Set of vectors v with $v.c = 0$ for all $c \in \mathcal{C}$.

For $C_1(2,q)^\perp$:

- Length $n = q^2 + q + 1$,
- Dimension: $q^2 + q + 1 - (\binom{p+1}{2}^h + 1)$
- Distance $d = ?$.

$\rightsquigarrow$ sets without tangents.

The dual code

Observation

- If G is a generator matrix for $\mathcal{C}$, then $vG^t = 0$ for all $v \in \mathcal{C}^\perp$.

OBSERVATION

- If G is a generator matrix for C, then $vG^t = 0$ for all $v \in \mathrm{C}^\perp$.
- A matrix H such that $cH^t = 0$ for all $c \in C$ is is called a parity check matrix for C.

THE DUAL CODE

OBSERVATION

- If G is a generator matrix for C, then $vG^t = 0$ for all $v \in \mathrm{C}^\perp$.
- A matrix H such that $cH^t = 0$ for all $c \in C$ is is called a parity check matrix for C.
- Parity check matrix of C=generator matrix of $\mathrm{C}^\perp$ and vice versa.

Definition

A *conic* in $\mathrm{PG}(2, q)$ is a set of points whose coordinates (x_0, y_0, z_0) satisfy a homogeneous quadratic equation.

DEFINITION

A *conic* in $\mathrm{PG}(2, q)$ is a set of points whose coordinates (x_0, y_0, z_0) satisfy a homogeneous quadratic equation.

EXAMPLE

The set of points (x, y, z) with $y^2 = xz$ is a conic.

$$\{(1, t, t^2) : t \in \mathbb{K}\} \cup \{(0, 0, 1)\}$$

THEOREM

In $\mathrm{PG}(2, \mathbb{K})$, all non-empty irreducible conics are projectively equivalent to

$$\{(1, t, t^2) : t \in \mathbb{K}\} \cup \{(0, 0, 1)\}.$$

THEOREM

In $\mathrm{PG}(2, \mathbb{K})$, all non-empty irreducible conics are projectively equivalent to

$$\{(1, t, t^2) : t \in \mathbb{K}\} \cup \{(0, 0, 1)\}.$$

OBSERVATION

$$\{(1, t, t^2) : t \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$$

has $q + 1$ points; so every non-degenerate conic in $\mathrm{PG}(2, q)$ has $q + 1$ points.

- Every line meets an irreducible conic in either 0, 1 or 2 points.
- Every point lies on a unique tangent line to an irreducible conic.

Definition

An oval is a set of points S no three of which lie on a line and such that every point lies on a unique tangent line to the oval.

DEFINITION

An oval is a set of points S no three of which lie on a line and such that every point lies on a unique tangent line to the oval.

In $\mathrm{PG}(2, q)$: an oval has $q + 1$ points.

Every non-singular conic is an oval; but is every oval in $\mathrm{PG}(2, q)$ a conic?

Every non-singular conic is an oval; but is every oval in $\mathrm{PG}(2, q)$ a conic?

MR0054979 (14,1008d) Reviewed

Järnefelt, G.; Kustaanheimo, Paul

An observation on finite geometries. *Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949*, pp. 166–182. *Johan Grundt Tanums Forlag, Oslo,* 1952.

48.0X

Review PDF | Clipboard | Series | Chapter | Make Link

In a geometry with coordinates from a field with a prime number of elements, p, the axioms of incidence will of course be satisfied. It is observed here that the quadratic form $x^2 - ky^2$ with k a quadratic non-residue may be used to define a metric. Certain axioms of congruence are satisfied if this metric is used. It is conjectured that in a plane with $p^2 + p + 1$ points a set of $p + 1$ points, no three on a line, will form a quadric. The reviewer finds this conjecture implausible.

Reviewed by Marshall Hall Jr.

THEOREM (SEGRE 1955)

Every set of $q+1$ *points in* $\mathrm{PG}(2,q)$, *q odd, such that no three are collinear, is the set of points on a conic.*

OVALS AND CONICS

MR0071034 (17,72g) Reviewed
Segre, Beniamino
Ovals in a finite projective plane.
Canadian J. Math. 7 (1955), 414–416.
48.0X
Review PDF | Clipboard | Journal | Article | Make Link

In a finite projective plane with $n+1$ points on a line there can be at most $n+2$ points with the property that no three are on a line and if n is odd there can be at most $n+1$ with this property. If n is even and we have $n+1$ points, no three on a line, then there exists a further point which can be adjoined to these giving $n+2$ points, no three on a line. In a Desarguesian plane a non-degenerate conic contains $n+1$ points, no three on a line. If, when n is odd, we call $n+1$ points, no three on a line, an oval, then it was conjectured by Järnefelt and Kustaanheimo [Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, Tanum, 1952, pp. 166–182; MR0054979] that in a Desarguesian plane of odd order n, an oval is necessarily a conic. This conjecture is shown to be true in this paper. The method of proof is ingenious. We may take three points of the oval to be $A_1:(1,0,0)$, $A_2:(0,1,0)$, and $A_3:(0,0,1)$ and if $P(a_1,a_2,a_3)$ is a further point on the oval and $x_2=\lambda_1 x_3$, $x_3=\lambda_2 x_1$, $x_1=\lambda_3 x_2$ are the three secants PA_1,PA_2,PA_3, then immediately $\lambda_1\lambda_2\lambda_3=1$. Since the product of all non-zero elements in the field is -1, it will follow that for the tangents at A_1,A_2,A_3 that $x_2=k_1x_3$, $x_3=k_2x_1$, $x_1=k_3x_2$ we will have $k_1k_2k_3=-1$. From this the inscribed triangle and its circumscribed triangle are perspective with respect to the center $(1,k_1k_2,-k_2)$. It follows generally that every inscribed triangle and its circumscribed triangle are perspective. Using this relation on the triangles formed from P,A_1,A_2, and A_3, we find that the coordinates of P satisfy a quadratic equation which becomes $x_2x_3+x_3x_1+x_1x_2=0$ if we take C as $(1,1,1)$, as we may. [The fact that this conjecture seemed implausible to the reviewer seems to have been at least a partial incentive to the author to undertake this work. It would be very gratifying if further expressions of doubt were as fruitful.]

Reviewed by Marshall Hall Jr.

Definition

A (planar) arc is a set of points in a projective plane, no three of which are collinear.

Side note: arcs and MDS codes

Definition

An arc is a set of points in a projective space in general position (no n points contained in an $n-2$-space).

Folklore theorem

Arcs and MDS codes (codes meeting the Singleton bound) are equivalent objects

Side note: arcs and MDS codes

Take coordinates for points of arc as columns of a parity-check matrix.

Example

$(1,0,0),(1,1,1),(1,2,4),(1,3,4),(1,4,1),(0,0,1)$ is an arc of $\mathrm{PG}(2,5)$.

Let $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{bmatrix}$

Then H is a parity check matrix for a code with

- $n = 6$
- $k = 3$
- $d = 4$

Side note: arcs and MDS codes

Take coordinates for points of arc as columns of a parity-check matrix.

Example

$(1,0,0),(1,1,1),(1,2,4),(1,3,4),(1,4,1),(0,0,1)$ is an arc of $\mathrm{PG}(2,5)$.

Let $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{bmatrix}$

Then H is a parity check matrix for a code with

- $n = 6$
- $k = 3$
- $d = 4$
- So the Singleton bound gives $d = 4 \leq n - k + 1 = 4$: MDS code
- Reed-Solomon code

Side note: arcs and MDS codes

Take coordinates for points of arc as columns of a parity-check matrix.

Example

$(1, 0, 0), (1, 1, 1), (1, 2, 4), (1, 3, 4), (1, 4, 1), (0, 0, 1)$ is an arc of $\mathrm{PG}(2, 5)$.

Let $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{bmatrix}$

Then H is a parity check matrix for a code with

- $n = 6$
- $k = 3$
- $d = 4$
- So the Singleton bound gives $d = 4 \leq n - k + 1 = 4$: MDS code
- Reed-Solomon code

Why is $d = 4$?

Side note: arcs and MDS codes

Standard lemma

A matrix H is a parity check matrix for a code with distance d if and only if all sets of $d-1$ columns are linearly independent and there are d dependent columns.

Side note: arcs and MDS codes

Standard lemma

A matrix H is a parity check matrix for a code with distance d if and only if all sets of $d - 1$ columns are linearly independent and there are d dependent columns.

Open Problem

MDS Conjecture: An arc of $\mathrm{PG}(k-1, q)$, with $k \leq q$, has size at most $q + 1$,

Side note: arcs and MDS codes

Standard lemma

A matrix H is a parity check matrix for a code with distance d if and only if all sets of $d-1$ columns are linearly independent and there are d dependent columns.

Open Problem

MDS Conjecture: An arc of $\mathrm{PG}(k-1, q)$, with $k \leq q$, has size at most $q+1$, unless q is even and $k=3$ or $k=q-1$, in which case it has size at most $q+2$.

A linear MDS code of dimension k over $\mathbb{F}_q$ has length at most $q+1$

Side note: arcs and MDS codes

Standard lemma

A matrix H is a parity check matrix for a code with distance d if and only if all sets of $d-1$ columns are linearly independent and there are d dependent columns.

Open Problem

MDS Conjecture: An arc of $\mathrm{PG}(k-1, q)$, with $k \leq q$, has size at most $q+1$, unless q is even and $k=3$ or $k=q-1$, in which case it has size at most $q+2$.
A linear MDS code of dimension k over $\mathbb{F}_q$ has length at most $q+1$ unless q is even and $k=3$ or $k=q-1$, in which case it has length at most $q+2$.

- The MDS conjecture is true for q prime (S. Ball 2012).

BACK TO ARCS IN $\mathrm{PG}(2, q)$

An arc in $\mathrm{PG}(2, q)$ is a set of points no three of which are collinear. Let $\mathcal{A}$ be an arc in $\mathrm{PG}(2, q)$, then

$$|\mathcal{A}| \leq q + 2.$$

LEMMA (BOSE (1947))

Let $\mathcal{A}$ be an arc in $\mathrm{PG}(2, q)$, q odd, then

$$|\mathcal{A}| \leq q + 1.$$

DEFINITION

An arc in $\mathrm{PG}(2, q)$, q even, containing $q + 2$ points is called a hyperoval.

DEFINITION

An arc in $\mathrm{PG}(2, q)$, q even, containing $q + 2$ points is called a hyperoval.

Every line meets a hyperoval in 0 or 2 points.

DEFINITION

An arc in $\mathrm{PG}(2, q)$, q even, containing $q + 2$ points is called a hyperoval.

Every line meets a hyperoval in 0 or 2 points.

EXAMPLE

The set

$$\{(1, t, t^2) : t \in \mathbb{F}_{2^h}\} \cup \{(0, 0, 1\} \cup \{0, 1, 0)\}$$

is a hyperoval.

DEFINITION

An arc in $\mathrm{PG}(2, q)$, q even, containing $q + 2$ points is called a hyperoval.

Every line meets a hyperoval in 0 or 2 points.

EXAMPLE

The set

$$\{(1, t, t^2) : t \in \mathbb{F}_{2^h}\} \cup \{(0, 0, 1\} \cup \{0, 1, 0)\}$$

is a hyperoval.
More generally, for even q, every conic has a *nucleus* in $\mathrm{PG}(2, q)$ and forms a hyperoval. These hyperovals are the regular hyperovals.

OBSERVATION

Not every hyperoval is a regular hyperoval.

Bill Cherowitzo's Hyperoval Page

Introduction | Table of Contents | Bibliography | Table of Known Hyperovals | Open Problems | Glossary | Search Index | Exit

Known Hyperovals in PG(2,2^h)

Name	O-Polynomial	Field Restriction	Section Comments	Properties
Hyperconic	$f(x) = x^2$	None	Section 2	Available
Translation	$f(x) = x^{2^i}$ $(i,h) = 1$	None	Section 2	
Segre	$f(x) = x^6$	h odd	Section 2	
Glynn I	$f(x) = x^{3\sigma + 4}$	h odd	Section 2	
Glynn II	$f(x) = x^{\sigma + \gamma}$	h odd	Section 2	
Payne	$f(x) = x^{1/6}+x^{1/2}+x^{5/6}$	h odd	Section 3	
Cherowitzo	$f(x) = x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$	h odd	Section 3	
Subiaco	see comments	None	Section 3	
Adelaide	see comments	h even	Section 3	
Penttila-O'Keefe	see comments	h = 5	Section 4	

$$\gamma^4 \equiv \sigma^2 \equiv 2 \bmod (2^h-1)$$

THE DUAL CODE OF $C_1(2, q)$

- Rows of generator matrix of $C_1(2, q)$: lines of $PG(2, q)$

THE DUAL CODE OF $C_1(2, q)$

- Rows of generator matrix of $C_1(2, q)$: lines of $PG(2, q)$
- Generator matrix=parity check matrix of $C_1(2, q)^\perp$.
- $c \in C_1(2, q)^\perp \iff c.\ell = 0$ for all lines of $PG(2, q)$

The dual code of $\mathrm{C}_1(2, q)$

- Rows of generator matrix of $\mathrm{C}_1(2, q)$: lines of $\mathrm{PG}(2, q)$
- Generator matrix=parity check matrix of $\mathrm{C}_1(2, q)^\perp$.
- $c \in \mathrm{C}_1(2, q)^\perp \iff c.\ell = 0$ for all lines of $\mathrm{PG}(2, q)$
- Codeword of $\mathrm{C}_1(2, q)^\perp$ corresponds to a set of points such that every line contains 0 or at least 2 of them

The dual code of $C_1(2, q)$

- Rows of generator matrix of $C_1(2, q)$: lines of $PG(2, q)$
- Generator matrix=parity check matrix of $C_1(2, q)^\perp$.
- $c \in C_1(2, q)^\perp \iff c.\ell = 0$ for all lines of $PG(2, q)$
- Codeword of $C_1(2, q)^\perp$ corresponds to a set of points such that every line contains 0 or at least 2 of them
- This is a set without tangents.

THE DUAL CODE OF $C_1(2, q)$

- Rows of generator matrix of $C_1(2, q)$: lines of $PG(2, q)$
- Generator matrix=parity check matrix of $C_1(2, q)^\perp$.
- $c \in C_1(2, q)^\perp \iff c.\ell = 0$ for all lines of $PG(2, q)$
- Codeword of $C_1(2, q)^\perp$ corresponds to a set of points such that every line contains 0 or at least 2 of them
- This is a set without tangents.

COROLLARY

The minimum weight for $C_1(2, q)^\perp$ is at least $q + 2$.

- If q is even, a codeword corresponds to a set S of points that every line intersects S in an even number of points.
- A hyperoval is a set of $q + 2$ points, no three collinear.
- Hyperovals in $\mathrm{PG}(2, q)$ exist iff q is even.

COROLLARY

The minimum weight of $\mathrm{C}_1(2, q)^{\perp}$, q even is $q + 2$.

The dual code of $C_1(2, q)$

- If q is even, a codeword corresponds to a set S of points that every line intersects S in an even number of points.
- A hyperoval is a set of $q + 2$ points, no three collinear.
- Hyperovals in $\mathrm{PG}(2, q)$ exist iff q is even.

Corollary

The minimum weight of $C_1(2, q)^{\perp}$, q even is $q + 2$.

The dual code of $C_1(2, q)$

Sets without tangents

- Every codeword of $C_1^{\perp}$ gives rise to a set without tangents, but not vice versa.

THE DUAL CODE OF $C_1(2, q)$

SETS WITHOUT TANGENTS

- Every codeword of $C_1^\perp$ gives rise to a set without tangents, but not vice versa.
- If q is odd: smallest size of set without tangents not known
- Lower bound (Blokhuis - Seress -Wilbrink 1991) $q + \frac{1}{4}\sqrt{2q} + 2$ points
- Example of size $2p - 2$ for p prime.

- The minimum weight of $C_1(2, p)^\perp$, p prime, is $2p$.

THE DUAL CODE OF $\mathrm{C}_1(2, q)$

SETS WITHOUT TANGENTS

- Every codeword of $\mathrm{C}_1^\perp$ gives rise to a set without tangents, but not vice versa.
- If q is odd: smallest size of set without tangents not known
- Lower bound (Blokhuis - Seress -Wilbrink 1991) $q + \frac{1}{4}\sqrt{2q} + 2$ points
- Example of size $2p - 2$ for p prime.

- The minimum weight of $\mathrm{C}_1(2, p)^\perp$, p prime, is $2p$.
- The minimum weight of $\mathrm{C}_1(2, q)^\perp$, q odd, non-prime???

Further codewords of $C_1(2, q)$, q even

Recall

The minimum weight of $\mathrm{C}_1(2, q)^{\perp}$, q even is $q + 2$. Every line meets the support of a codeword in an even number of points, so the weight of each codeword is even.

Further codewords of $C_1(2, q)$, q even

Recall

The minimum weight of $\mathrm{C}_1(2, q)^\perp$, q even is $q + 2$. Every line meets the support of a codeword in an even number of points, so the weight of each codeword is even.

Is there a codeword of weight $q + 4$?

FURTHER CODEWORDS OF $C_1(2,q)$, q EVEN

RECALL

The minimum weight of $\mathrm{C}_1(2,q)^\perp$, q even is $q+2$. Every line meets the support of a codeword in an even number of points, so the weight of each codeword is even.

Is there a codeword of weight $q+4$?

LEMMA

The support of a codeword of weight $q+4$ is necessarily a set of size $q+4$ such that every line meets in $0, 2$ or 4 points.

$\rightsquigarrow$ KM-arcs.

Math. Proc. Camb. Phil. Soc. (1990), **108**, 445 445
Printed in Great Britain

On $(q+t)$-arcs of type $(0, 2, t)$ in a desarguesian plane of order q

BY GÁBOR KORCHMÁROS

Department of Mathematics, University of Basilicata, 85100 *Potenza, Italy*

AND FRANCESCO MAZZOCCA

Department of Mathematics and its Applications, University of Napoli,
via Mezzocannone 8, 80134 *Napoli, Italy*

(*Received* 13 *December* 1989; *revised* 2 *March* 1990)

1. *Introduction*

This paper is concerned with certain point-sets T in a projective plane PG$(2,q)$ over GF(q) which have only three characters with respect to the lines. We assume throughout this paper that for any line l of π

$$|T \cap l| = \begin{cases} 0 \\ 2 \\ t, t \neq 0, 2 \end{cases} \tag{1·1}$$

where
$$|T| = q + t. \tag{1·2}$$

It is easily seen that if $t = 1$ then T is a $(q+1)$-arc, i.e. an oval; otherwise T is a $(q+t, t)$-arc of type $(0, 2, t)$. Therefore $(q+t, t)$-arcs of type $(0, 2, t)$ appear to be a generalization of ovals and there are interesting connections between ovals and $(q+t, t)$-arcs of type $(0, 2, t)$ from various points of view. Our purpose is to investigate

Basic properties

Theorem (Korchmáros-Mazzocca, Gács-Weiner)

If $\mathcal{A}$ is a KM-arc of type t in $\mathrm{PG}(2, q)$, $2 \leq t < q$, then

- q is even;
- t is a divisor of q.

THEOREM (KORCHMÁROS-MAZZOCCA, GÁCS-WEINER)

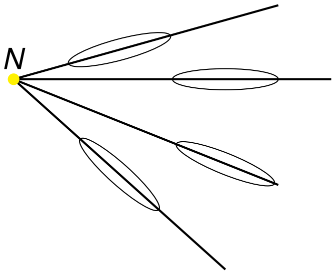
If $\mathcal{A}$ is a KM-arc of type t in $\mathrm{PG}(2, q)$, $2 \leq t < q$, then

- q is even;
- t is a divisor of q.

If $t > 2$, then

- there are $\frac{q}{t} + 1$ different t-secants to $\mathcal{A}$, and they are concurrent.

The common point of the t-secants is called the t-nucleus.



A KM-ARC OF TYPE $q/2$

EXAMPLE (*)

Let Tr: $\mathbb{F}_q \to \mathbb{F}_2 : x \mapsto x + x^2 + x^4 + \cdots + x^{q/2}$

A KM-ARC OF TYPE $q/2$

EXAMPLE (*)

Let $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_2 : x \mapsto x + x^2 + x^4 + \cdots + x^{q/2}$

$$\begin{aligned} S_0 &= \{(1,0,x) \mid \mathrm{Tr}(x) = 0\} \\ S_1 &= \{(1,1,y) \mid \mathrm{Tr}(y) = 1\} \\ S_\infty &= \{(0,1,z) \mid \mathrm{Tr}(z) = 0\} \end{aligned}$$

Then, $S_0 \cup S_1 \cup S_\infty$ is a KM-arc of type $q/2$. Its $q/2$-secants are $Y = 0$, $X + Y = 0$ and $X = 0$. The $q/2$-nucleus is $(0,0,1)$.

A KM-ARC OF TYPE $q/2$

EXAMPLE (*)

Let $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_2 : x \mapsto x + x^2 + x^4 + \cdots + x^{q/2}$

$$\begin{aligned} S_0 &= \{(1,0,x) \mid \mathrm{Tr}(x) = 0\} \\ S_1 &= \{(1,1,y) \mid \mathrm{Tr}(y) = 1\} \\ S_\infty &= \{(0,1,z) \mid \mathrm{Tr}(z) = 0\} \end{aligned}$$

Then, $S_0 \cup S_1 \cup S_\infty$ is a KM-arc of type $q/2$. Its $q/2$-secants are $Y = 0$, $X + Y = 0$ and $X = 0$. The $q/2$-nucleus is $(0,0,1)$.

THEOREM (DE BOECK–VDV 2015)

A set of $q + q/2$ points in $\mathrm{PG}(2,q)$ such that every line meets in $0, 2$ or $q/2$ points is equivalent to example (*).

A KM-arc of type $q/2$

Example (*)

Let $\mathrm{Tr}\colon \mathbb{F}_q \to \mathbb{F}_2 : x \mapsto x + x^2 + x^4 + \cdots + x^{q/2}$

$$\begin{aligned} S_0 &= \{(1,0,x) \mid \mathrm{Tr}(x) = 0\} \\ S_1 &= \{(1,1,y) \mid \mathrm{Tr}(y) = 1\} \\ S_\infty &= \{(0,1,z) \mid \mathrm{Tr}(z) = 0\} \end{aligned}$$

Then, $S_0 \cup S_1 \cup S_\infty$ is a KM-arc of type $q/2$. Its $q/2$-secants are $Y = 0$, $X + Y = 0$ and $X = 0$. The $q/2$-nucleus is $(0, 0, 1)$.

Theorem (De Boeck–VdV 2015)

A set of $q + q/2$ points in $\mathrm{PG}(2, q)$ such that every line meets in $0, 2$ or $q/2$ points is equivalent to example (*). It is necessarily a translation KM-arc.

OVERVIEW: INFINITE FAMILIES OF KM-ARCS OF TYPE 2^i IN $\mathrm{PG}(2, 2^h)$ FOR

(A) $h - i \mid h$ (Korchmáros–Mazzocca, Gács–Weiner)

(B) $h - i + 1 \mid h$ (Gács–Weiner; iterative construction)

OVERVIEW: INFINITE FAMILIES OF KM-ARCS OF TYPE 2^i IN $PG(2, 2^h)$ FOR

(A) $h - i \mid h$ (Korchmáros–Mazzocca, Gács–Weiner)

(B) $h - i + 1 \mid h$ (Gács–Weiner; iterative construction)

(C) $i = h - 2$ (Vandendriessche, De Boeck-VdV 2015)

(D) $i = h - 3$ (De Boeck-VdV 2017)

(E) $i = h - 4$ for some h (De Boeck-VdV 2017)

(F) $i = 1$ Hyperovals

A CONJECTURE

THEOREM (GÁCS-WEINER)

A KM-arc of type t in $\mathrm{PG}(2, q)$ determines a Vandermonde set on each of its t-secants.

THEOREM (GÁCS-WEINER)

A KM-arc of type t in $\mathrm{PG}(2,q)$ determines a Vandermonde set on each of its t-secants.

DEFINITION

$T = \{y_1, \ldots, y_n\} \subseteq \mathbb{F}_q$ is a Vandermonde set if $\sum_{i=0}^{n} y_i^k = 0$ for all $k = 0, \ldots, n-2$.

A conjecture

Theorem (Gács-Weiner)

A KM-arc of type t in $\mathrm{PG}(2, q)$ determines a Vandermonde set on each of its t-secants.

Definition

$T = \{y_1, \ldots, y_n\} \subseteq \mathbb{F}_q$ is a Vandermonde set if $\sum_{i=0}^{n} y_i^k = 0$ for all $k = 0, \ldots, n-2$.

Conjecture (Vandendriessche)

A KM-arc of type t in $\mathrm{PG}(2, q)$ together with its nucleus determines an $\mathbb{F}_2$-linear set on each of its t-secants.

If there is a line L such that the subgroup of the pointwise stabiliser of L stabilising A acts transitively on the points of A outside L, then A is a translation KM-arc with translation line L.

THEOREM (DE BOECK–VDV 2015)

Translation KM-arcs of type 2^i in $\mathrm{PG}(2, 2^h)$ and i-clubs of rank h in $\mathrm{PG}(1, 2^h)$ are equivalent objects.

If there is a line L such that the subgroup of the pointwise stabiliser of L stabilising A acts transitively on the points of A outside L, then A is a translation KM-arc with translation line L.

THEOREM (DE BOECK–VDV 2015)

Translation KM-arcs of type 2^i in $\mathrm{PG}(2, 2^h)$ and i-clubs of rank h in $\mathrm{PG}(1, 2^h)$ are equivalent objects.

- Via i-clubs: examples of type 2^i, with $i = h - 1$, $i = h - 2$, $h - i | h$, $h - i + 1 | h$.
- No 2-club in $\mathrm{PG}(2, 32)$, but there is a KM-arc of type 4 in $\mathrm{PG}(2, 32)$ and $\mathrm{PG}(2, 64)$.

DE BOECK–VDV 20??

If there are only points of weight 1 and 2, then the number of points of weight 2 is contained in

$[q-2\sqrt{q}+1, q+2\sqrt{q}+1] \cup \{2q, 2q+1, 2q+2, 3q, 3q+1, q^2+1\}$.

In particular, there are no $\mathbb{F}_q$-linear 2-clubs in $\mathrm{PG}(1, q^5)$.

History

- Origins in game theory (J. Von Neumann – O. Morgenstern 1944)
- M. Richardson (1956), J. Di Paola (1966), A.A. Bruen (1970)

ON FINITE PROJECTIVE GAMES

MOSES RICHARDSON[1]

1. **Preliminaries on simple games.** Let $N=\{1, 2, \cdots, n\}$ be a finite set of n elements termed *players*. Let $\mathfrak{N}$ be the class of all subsets S of N; the elements S of $\mathfrak{N}$ are termed *coalitions*. If $\mathcal{S}\subset\mathfrak{N}$, let $\mathcal{S}^+$ denote the class of all supersets of elements of $\mathcal{S}$, and $\mathcal{S}^*$ the class of all complements of elements of $\mathcal{S}$; in symbols, $\mathcal{S}^+=[X\in\mathfrak{N}\mid X\supset S$ for some $S\in\mathcal{S}]$, $\mathcal{S}^*=[X\in\mathfrak{N}\mid N-X\in\mathcal{S}]$. By a *simple game* is meant an ordered pair $G=(N, \mathcal{W})$ where $\mathcal{W}\subset\mathfrak{N}$ satisfies (1) $\mathcal{W}=\mathcal{W}^+$, (2) $\mathcal{W}\cap\mathcal{W}^*=0$. The elements of $\mathcal{W}$ are termed *winning coalitions*. The elements of $\mathcal{L}=\mathfrak{N}-\mathcal{W}$ are termed *losing coalitions*. The elements of $\mathcal{B}=\mathcal{L}\cap\mathcal{L}^*$ are termed *blocking coalitions*. A simple game[2] is termed

- M. Richardson. On finite projective games. *Proc. Amer. Math. Soc.* 7, 458–465, 1956.

ON FINITE PROJECTIVE GAMES

MOSES RICHARDSON[1]

1. **Preliminaries on simple games.** Let $N=\{1, 2, \cdots, n\}$ be a finite set of n elements termed *players*. Let $\mathfrak{N}$ be the class of all subsets S of N; the elements S of $\mathfrak{N}$ are termed *coalitions*. If $\mathcal{S}\subset\mathfrak{N}$, let $\mathcal{S}^+$ denote the class of all supersets of elements of $\mathcal{S}$, and $\mathcal{S}^*$ the class of all complements of elements of $\mathcal{S}$; in symbols, $\mathcal{S}^+=[X\in\mathfrak{N} \mid X\supset S$ for some $S\in\mathcal{S}]$, $\mathcal{S}^*=[X\in\mathfrak{N} \mid N-X\in\mathcal{S}]$. By a *simple game* is meant an ordered pair $G=(N, \mathcal{W})$ where $\mathcal{W}\subset\mathfrak{N}$ satisfies (1) $\mathcal{W}=\mathcal{W}^+$, (2) $\mathcal{W}\cap\mathcal{W}^*=0$. The elements of $\mathcal{W}$ are termed *winning coalitions*. The elements of $\mathcal{L}=\mathfrak{N}-\mathcal{W}$ are termed *losing coalitions*. The elements of $\mathcal{B}=\mathcal{L}\cap\mathcal{L}^*$ are termed *blocking coalitions*. A simple game[2] is termed

- M. Richardson. On finite projective games. *Proc. Amer. Math. Soc.* 7, 458–465, 1956.
- Subsets of a set of players are called coalitions. Winning coalitions can force a decision. A blocking coalition can block every decision: it contains at least one player of each winning coalition.

Blocking sets: definition

Definition for projective planes

A set of points B in a projective plane Π such that every line of Π contains at least 1 point of B is a blocking set.

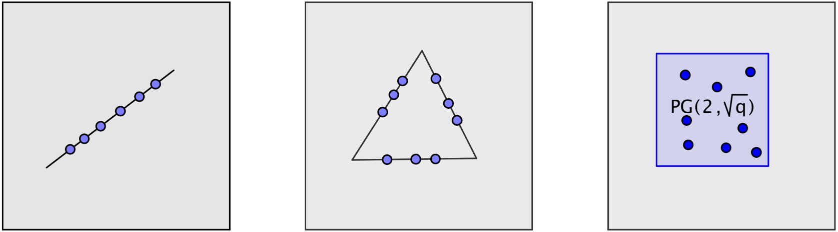
DEFINITION FOR PROJECTIVE PLANES

A set of points B in a projective plane Π such that every line of Π contains at least 1 point of B is a blocking set.

MINIMAL BLOCKING SETS

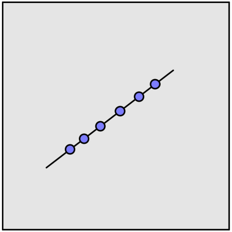
A blocking set B in Π is called minimal if no proper subset of B is a blocking set.

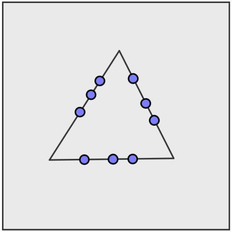
Examples in PG$(2, q)$

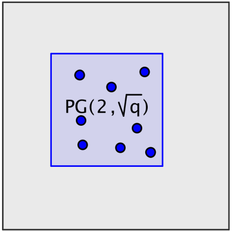


A line: $q + 1$ points

EXAMPLES IN PG$(2, q)$

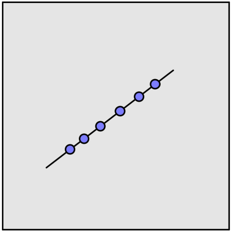


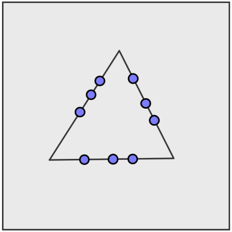


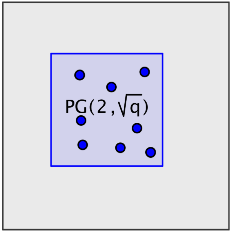


A line: $q + 1$ points
A projective triangle in PG$(2, q)$, q odd: $3(q + 1)/2$ well-chosen points on a triangle

Examples in PG$(2, q)$

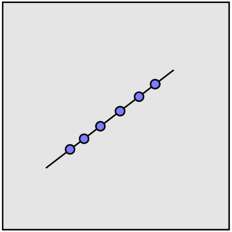
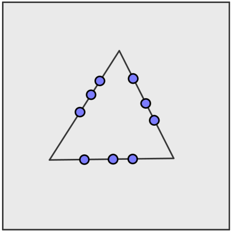
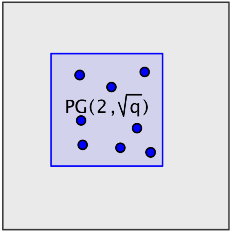






A line: $q + 1$ points
A projective triangle in PG$(2, q)$, q odd: $3(q + 1)/2$ well-chosen points on a triangle
A Baer subplane PG$(2, \sqrt{q})$, q square: $q + \sqrt{q} + 1$ points.

Examples in PG$(2, q)$

A line: $q + 1$ points

A projective triangle in PG$(2, q)$, q odd: $3(q + 1)/2$ well-chosen points on a triangle

A Baer subplane PG$(2, \sqrt{q})$, q square: $q + \sqrt{q} + 1$ points.

Trivial blocking sets

A blocking set B in PG$(2, q)$ is called trivial if it contains a line.

Small blocking sets

A blocking set B in PG$(2, q)$ is called small if $|B| < 3(q + 1)/2$.

A (trivial) lower bound

A (trivial) lower bound

Theorem (R.C. Bose, R.H. Burton (1966))

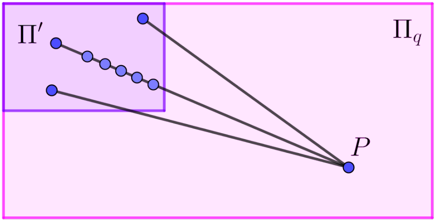
If B is a blocking set in a projective plane of order q, then $|B| \geq q + 1$ and $|B| = q + 1$ if and only if B is a line.

THEOREM (A. BRUEN)

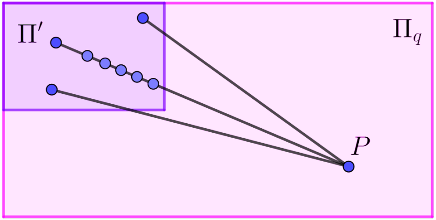
Let B be a non-trivial blocking set in a projective plane Π of order q. Then $|B| \geq q + \sqrt{q} + 1$ and equality holds if and only if B is a Baer subplane.

THEOREM (A. BRUEN)

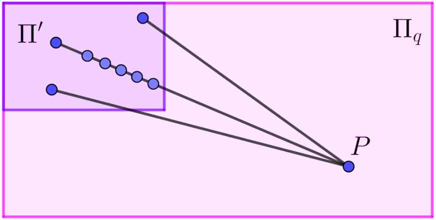
Let B be a non-trivial blocking set in a projective plane Π of order q. Then $|B| \geq q + \sqrt{q} + 1$ and equality holds if and only if B is a Baer subplane.



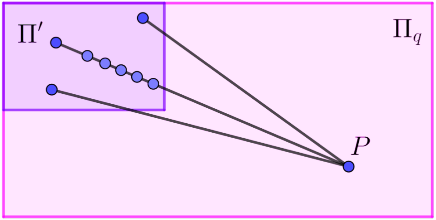
Π_q: projective plane of order q, q square
Π': Baer subplane of Π_q



- P lies on $q+1$ lines of Π_q



- P lies on $q + 1$ lines of Π_q
- At most one of these meets Π' in a line (so contains $\sqrt{q} + 1$ points)



- P lies on $q+1$ lines of Π_q
- At most one of these meets Π' in a line (so contains $\sqrt{q}+1$ points)
- The other at least q points of Π' are connected to P by distinct lines.
- So the points of Π' block all lines of Π

RECALL

A blocking set in $\mathrm{PG}(2, q)$ is *small* if its size is less than $3(q+1)/2$.

RECALL

A blocking set in $\mathrm{PG}(2, q)$ is *small* if its size is less than $3(q+1)/2$.

THEOREM (A. BLOKHUIS (1994))

A small minimal blocking set in $\mathrm{PG}(2, p)$, p prime, is a line.

Recall
A blocking set in $\mathrm{PG}(2, q)$ is *small* if its size is less than $3(q+1)/2$.

Theorem (A. Blokhuis (1994))
A small minimal blocking set in $\mathrm{PG}(2, p)$, p prime, is a line.

Theorem (T. Szőnyi (1997))
A small minimal blocking set in $\mathrm{PG}(2, p^2)$, p prime, is a line or a Baer subplane.

THEOREM (O. POLVERINO(1998))

A small minimal blocking set in $\mathrm{PG}(2, p^3)$*, p prime, is a line or is projectively equivalent to*

$\{(x, x^p, 1) | x \in \mathbb{F}_{p^3}\} \cup \{(x, x^p, 0) | x \in \mathbb{F}_{p^3}\}$ *or*

$\{(x, x + x^p + x^{p^2}, 1) | x \in \mathbb{F}_{p^3}\} \cup \{(x, x + x^p + x^{p^2}, 0) | x \in \mathbb{F}_{p^3}\}$.

THEOREM (O. POLVERINO(1998))

A small minimal blocking set in $\mathrm{PG}(2, p^3)$*, p prime, is a line or is projectively equivalent to*
$\{(x, x^p, 1) | x \in \mathbb{F}_{p^3}\} \cup \{(x, x^p, 0) | x \in \mathbb{F}_{p^3}\}$ *or*
$\{(x, x + x^p + x^{p^2}, 1) | x \in \mathbb{F}_{p^3}\} \cup \{(x, x + x^p + x^{p^2}, 0) | x \in \mathbb{F}_{p^3}\}$.

REMARKS

- Either $p^3 + p^2 + p + 1$ points or $p^3 + p^2 + 1$ points.

THEOREM (O. POLVERINO(1998))

A small minimal blocking set in $\mathrm{PG}(2, p^3)$, *p prime, is a line or is projectively equivalent to*

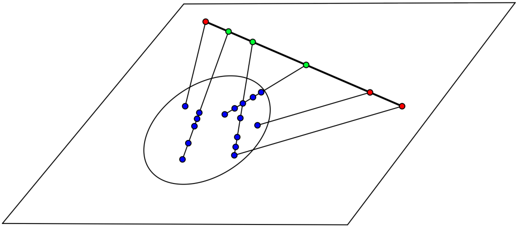
$\{(x, x^p, 1) | x \in \mathbb{F}_{p^3}\} \cup \{(x, x^p, 0) | x \in \mathbb{F}_{p^3}\}$ *or*

$\{(x, x + x^p + x^{p^2}, 1) | x \in \mathbb{F}_{p^3}\} \cup \{(x, x + x^p + x^{p^2}, 0) | x \in \mathbb{F}_{p^3}\}$.

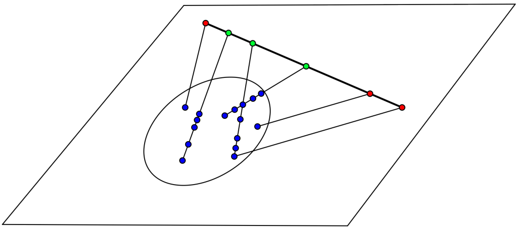
REMARKS

- Either $p^3 + p^2 + p + 1$ points or $p^3 + p^2 + 1$ points.
- of Rédei-type: there is a line with $|B| - p^3$ points of the blocking set B.
- consists of p^3 affine points, together with their determined directions.

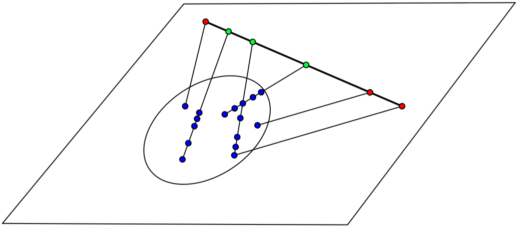
DIRECTIONS DETERMINED BY A POINT SET



DIRECTIONS DETERMINED BY A POINT SET

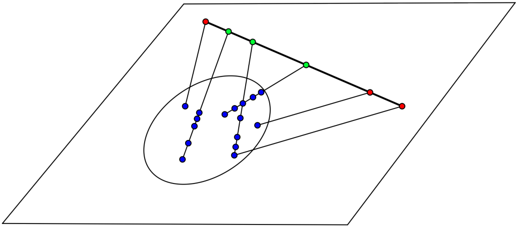


- Take a (blue) point set of size q.



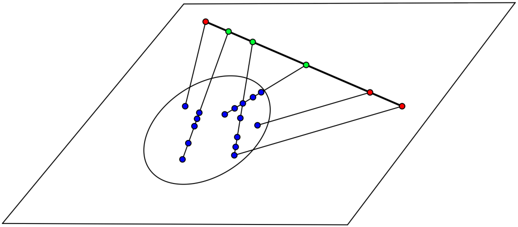
- Take a (blue) point set of size q.
- The green points are the directions determined by the blue point set.

Directions determined by a point set



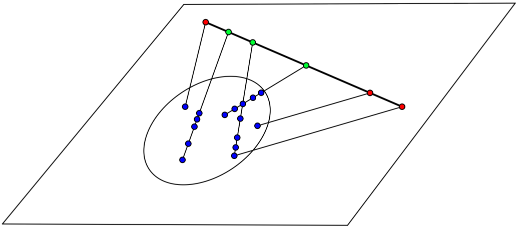
- Take a (blue) point set of size q.
- The green points are the directions determined by the blue point set.
- Each line $\neq L_\infty$ through a red point is a tangent line to the blue point set.

DIRECTIONS DETERMINED BY A POINT SET

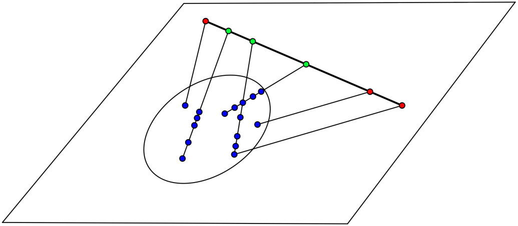


- Take a (blue) point set of size q.
- The green points are the directions determined by the blue point set.
- Each line $\neq L_\infty$ through a red point is a tangent line to the blue point set.
- Union of the blue and green point set is a minimal blocking set.
- If the green set has size $< q/2$, the blocking set is small.

DIRECTIONS DETERMINED BY A POINT SET



DIRECTIONS DETERMINED BY A POINT SET



- Pointset of size q, not at the line at infinity $Z = 0$ and not determining the 'vertical' direction: $\{(x, f(x), 1) | x \in \mathbb{F}_q\}$.
- Directions determined by a *function f* over a finite field.

THEOREM (S. BALL - A. BLOKHUIS - A. BROUWER - L. STORME - T. SZŐNYI, S. BALL)

Let f be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$, $q = p^h$, for some prime p, and let N be the number of directions determined by f.

THEOREM (S. BALL - A. BLOKHUIS - A. BROUWER - L. STORME - T. SZŐNYI, S. BALL)

Let f be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$, $q = p^h$, for some prime p, and let N be the number of directions determined by f. Let $s = p^e$ be maximal such that any line with a direction determined by f is incident with a multiple s of points of the graph of f. One of the following holds:

THEOREM (S. BALL - A. BLOKHUIS - A. BROUWER - L. STORME - T. SZŐNYI, S. BALL)

Let f be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$, $q = p^h$, for some prime p, and let N be the number of directions determined by f. Let $s = p^e$ be maximal such that any line with a direction determined by f is incident with a multiple s of points of the graph of f. One of the following holds:

(I) $s = 1$ *and* $(q + 3)/2 \leq N \leq q + 1$;

(II) $\mathbb{F}_s$ *is a subfield of* $\mathbb{F}_q$ *and* $q/s + 1 \leq N \leq (q - 1)/(s - 1)$;

(III) $s = q$ *and* $N = 1$.

Moreover, if $s > 2$, then f is an $\mathbb{F}_s$-linear map.

RÉDEI TYPE BLOCKING SETS

- A small minimal blocking set in $\mathrm{PG}(2, p)$, is a line, and hence of Rédei type.

RÉDEI TYPE BLOCKING SETS

- A small minimal blocking set in $\mathrm{PG}(2, p)$, is a line, and hence of Rédei type.
- A small minimal blocking set in $\mathrm{PG}(2, p^2)$, is a line or a Baer subplane, and hence of Rédei type.

RÉDEI TYPE BLOCKING SETS

- A small minimal blocking set in $\mathrm{PG}(2, p)$, is a line, and hence of Rédei type.
- A small minimal blocking set in $\mathrm{PG}(2, p^2)$, is a line or a Baer subplane, and hence of Rédei type.
- A small minimal blocking set in $\mathrm{PG}(2, p^3)$ is of Rédei type.

A CONJECTURE (A. BLOKHUIS)

All small minimal blocking sets of Rédei-type and the smallest minimal blocking set equivalent to
$\{(1, x, \mathrm{Tr}(x))|x \in \mathbb{F}_q\} \cup \{(0, x, \mathrm{Tr}(x))|x \in \mathbb{F}_q\}$.

THEOREM (P. POLITO, O. POLVERINO (1999))

There exists a small minimal blocking set in $\mathrm{PG}(2, p^h)$, *p prime,* $h > 3$, *that is not of Rédei-type.*

THEOREM (P. POLITO, O. POLVERINO (1999))

There exists a small minimal blocking set in $\mathrm{PG}(2, p^h)$*, p prime,* $h > 3$*, that is not of Rédei-type.*

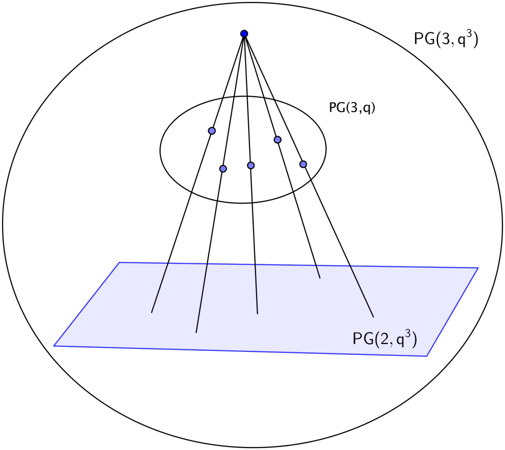
The constructed blocking sets are $\mathbb{F}_p$-linear point sets.

Via projection

(Alternative) definition

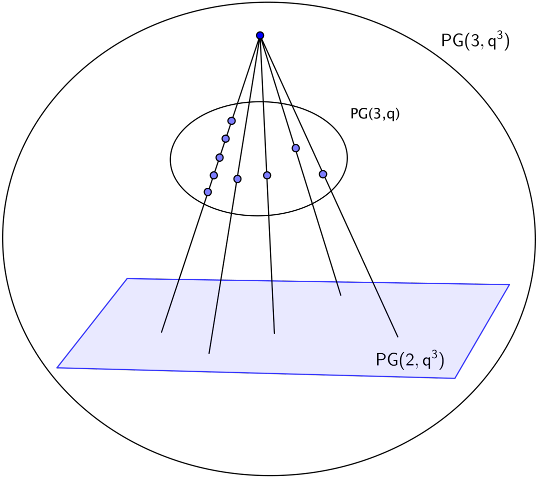
$\mathbb{F}_q$-linear set in $\mathrm{PG}(n, q^t)$: a subgeometry over $\mathbb{F}_q$ ($\cong \mathrm{PG}(n, q)$) or the projection of a subgeometry from a suitable subspace.

VIA PROJECTION: RANK 4 IN $\mathrm{PG}(2, q^3)$



Scattered linear set of rank 4: blocking set of size $q^3 + q^2 + q + 1$.

Via projection: rank 4 in $\mathrm{PG}(2, q^3)$



Linear set or rank 4: blocking set of size $q^3 + q^2 + 1$.

CONJECTURE [P. SZIKLAI ('2008')]

All small minimal blocking sets in $\mathrm{PG}(2, q)$, $q = p^h$, p prime, are $\mathbb{F}_p$-linear sets.

CONJECTURE [P. SZIKLAI ('2008')]

All small minimal blocking sets in $\mathrm{PG}(2,q)$, $q = p^h$, p prime, are $\mathbb{F}_p$-linear sets.

- All blocking sets of Rédei-type are linear sets.
- The linearity conjecture in $\mathrm{PG}(2,p^h)$, p prime, is wide open for $h > 3$.

THE SIZE OF A LINEAR SET OF RANK $k+1$

A linear set L of rank k is the projection of a $\mathrm{PG}(k, q)$, which has $\frac{q^{k+1}-1}{q-1}$ points.

THE SIZE OF A LINEAR SET OF RANK $k+1$

A linear set L of rank k is the projection of a $\mathrm{PG}(k,q)$, which has $\frac{q^{k+1}-1}{q-1}$ points.

So $|L| \leq \frac{q^{k+1}-1}{q-1}$.

Is there a trivial lower bound?

THE SIZE OF A LINEAR SET OF RANK $k+1$

A linear set L of rank k is the projection of a $\mathrm{PG}(k,q)$, which has $\frac{q^{k+1}-1}{q-1}$ points.

So $|L| \leq \frac{q^{k+1}-1}{q-1}$.

Is there a trivial lower bound?

THEOREM (J. DE BEULE AND G. VDV (2018))

For a linear set L in $\mathrm{PG}(1,q^t)$ of rank k:

$$|L| \geq q^{k-1}+1$$

THE SIZE OF A LINEAR SET OF RANK $k+1$

A linear set L of rank k is the projection of a $\mathrm{PG}(k,q)$, which has $\frac{q^{k+1}-1}{q-1}$ points.

So $|L| \leq \frac{q^{k+1}-1}{q-1}$.

Is there a trivial lower bound?

THEOREM (J. DE BEULE AND G. VDV (2018))

For a linear set L in $\mathrm{PG}(1,q^t)$ of rank k:

$$|L| \geq q^{k-1}+1$$

An $\mathbb{F}_q$-linear set in $\mathrm{PG}(2,q^t)$ of rank $t+1$ contains at least $q^t+q^{t-1}+1$ points.

OBSERVATION

The trace map gives us an example of an $\mathbb{F}_q$-linear set in $\mathrm{PG}(2, q^t)$ of rank $t+1$ of Rédei-type containing $q^t + q^{t-1} + 1$ points.

OBSERVATION

The trace map gives us an example of an $\mathbb{F}_q$-linear set in $\mathrm{PG}(2, q^t)$ of rank $t+1$ of Rédei-type containing $q^t + q^{t-1} + 1$ points.

THEOREM (D. JENA AND G. VDV (2020))

- There exist linear sets of rank t in $\mathrm{PG}(1, q^t)$ of size $q^{t-1} + 1$ not arising from the Trace map,

OBSERVATION

The trace map gives us an example of an $\mathbb{F}_q$-linear set in $\mathrm{PG}(2, q^t)$ of rank $t + 1$ of Rédei-type containing $q^t + q^{t-1} + 1$ points.

THEOREM (D. JENA AND G. VDV (2020))

- There exist linear sets of rank t in $\mathrm{PG}(1, q^t)$ of size $q^{t-1} + 1$ not arising from the Trace map,
- and there exist non-Rédei-type linear blocking sets of size $q^t + q^{t-1} + 1$ in $\mathrm{PG}(2, q^t)$,

The smallest linear (blocking) sets

Observation

The trace map gives us an example of an $\mathbb{F}_q$-linear set in $\mathrm{PG}(2, q^t)$ of rank $t+1$ of Rédei-type containing $q^t + q^{t-1} + 1$ points.

Theorem (D. Jena and G. VdV (2020))

- There exist linear sets of rank t in $\mathrm{PG}(1, q^t)$ of size $q^{t-1} + 1$ not arising from the Trace map,
- and there exist non-Rédei-type linear blocking sets of size $q^t + q^{t-1} + 1$ in $\mathrm{PG}(2, q^t)$,
- where we can specify the weight of the heaviest point.

A gap in the weight enumerator

Incidence vector of a line in a projective plane of order q:
codeword of weight $q + 1$.

Difference of the incidence vectors of two lines:
codeword of weight $2q$.

- Is there anything in between?

THE LINK WITH BLOCKING SETS

THEOREM (M. LAVRAUW, L. STORME, G. VDV (2008))

A codeword $c \in \mathrm{C}_1(2, q)$ *with weight* $< 2q$ *defines a small minimal blocking set in* $\mathrm{PG}(2, q)$.

THE LINK WITH BLOCKING SETS

THEOREM (M. LAVRAUW, L. STORME, G. VDV (2008))

A codeword $c \in \mathrm{C}_1(2,q)$ with weight $< 2q$ defines a small minimal blocking set in $\mathrm{PG}(2,q)$.

i.e: the set of non-zero positions in the codeword c corresponds to a set of points in $\mathrm{PG}(2,q)$ forming a blocking set.

RECALL (R.C. BOSE, R.H. BURTON (1966))

If B is a blocking set in $\mathrm{PG}(2, q)$, then $|B| \geq q + 1$ and $|B| = q + 1$ iff B is a line.

Corollaries of the link with blocking sets

Recall (R.C. Bose, R.H. Burton (1966))

If B is a blocking set in $\mathrm{PG}(2, q)$, then $|B| \geq q + 1$ and $|B| = q + 1$ iff B is a line.

Corollary

The minimum weight of $\mathrm{C}_1(2, q)$ is $q + 1$ and the minimum weight vectors correspond to the incidence vectors of lines.

(first obtained by E. Assmus and J.D. Key)

COROLLARIES OF THE LINK WITH BLOCKING SETS

THEOREM (A. BLOKHUIS (1994))

A small minimal blocking set in $\mathrm{PG}(2, p)$*, p prime, is a line.*

COROLLARIES OF THE LINK WITH BLOCKING SETS

THEOREM (A. BLOKHUIS (1994))

A small minimal blocking set in $\mathrm{PG}(2, p)$*, p prime, is a line.*

COROLLARY

There are no codewords in $\mathrm{C}_1(2, p)$*, p prime, with weight in* $]p + 1, 2p[$.

Corollaries of the link with blocking sets

Theorem (A. Blokhuis (1994))

A small minimal blocking set in $\mathrm{PG}(2, p)$, p prime, is a line.

Corollary

There are no codewords in $\mathrm{C}_1(2, p)$, p prime, with weight in $]p+1, 2p[$.

(first obtained by K. Chouinard and by G. McGuire and H. Ward for $]p+1, 3(p+1)/2[$)

Even stronger:

LEMMA (M. LAVRAUW, L. STORME, P. SZIKLAI, G. VDV (2009))

A codeword $c \in \mathcal{C}_1(2, q)$ with weight $< 2q$ defines a small minimal blocking set, intersecting every other small minimal blocking set in $1 \bmod p$ points.

Results for $C_1(2, q)$, q a prime power

Looking at intersections with linear blocking sets:

Theorem (M. Lavrauw, L. Storme, P. Sziklai, G. VdV (2009))

A small minimal blocking set, intersecting every other small minimal blocking set in 1 *mod p points, is a line.*

Results for $C_1(2, q)$, q a prime power

Looking at intersections with linear blocking sets:

Theorem (M. Lavrauw, L. Storme, P. Sziklai, G. VdV (2009))

A small minimal blocking set, intersecting every other small minimal blocking set in 1 *mod p points, is a line.*

Corollary

There are no codewords in $C_1(2, q)$*, with weight in* $]q + 1, 2q[$*.*

Results for $C_1(2, q)$, q a prime power

Theorem (Fack, Fancsali, Storme, VdV, Winne (2006)

For q prime: a codeword in $C_1(2, p)$ with weight $\leq 2p + \frac{p-1}{2}$ is a linear combination of at most 2 lines, so has weight $p + 1$, $2p$, or $2p + 1$.

Results for $C_1(2, q)$, q a prime power

Theorem (Fack, Fancsali, Storme, VdV, Winne (2006)

For q prime: a codeword in $C_1(2, p)$ with weight $\leq 2p + \frac{p-1}{2}$ is a linear combination of at most 2 lines, so has weight $p + 1$, $2p$, or $2p + 1$.

Bagchi (2012)/De Boeck–Vandendriessche (2014)

There exists a codeword in $C_1(2, p)$ of weigth $3p - 3$ which is not a linear combination of 3 lines.

RESULTS FOR $C_1(2, q)$, q A PRIME POWER

THEOREM (T. SZŐNYI AND ZS. WEINER (2018))

A codeword c in $C_1(2, q)$, $q = p^h$, with weight smaller than $q\sqrt{q} + 1$ is a linear combination of at most $\lceil \frac{wt(c)}{q+1} \rceil$ lines, when q is large and $h \geq 2$.

Open problems

- Prove (or disprove) that every projective plane has prime power order
- Prove (or disprove) that a projective plane of order p prime is Desarguesian
- Find a new hyperoval/classify hyperovals
- Construct a KM-arc of type t for all $t|q$.
- Prove (or disprove) the MDS conjecture
- Determine the minimum weight of $C(2,q)^{\perp}$
- Find the smallest size of a set without tangents in $\mathrm{PG}(2,q)$, q odd
- Prove (or disprove) that a small minimal blocking set in $\mathrm{PG}(2,q)$ is a linear set

Thank you for your attention!