Linear codes arising from geometrical structures

Geertrui Van de Voorde

Academy Contact Forum "Coding Theory and Cryptography III"
September 25, 2009
Brussels

Outline

Outline

Error correcting codes: Motivation

Without Coding Theory:

$$\begin{array}{ccc} \text{Message} & \xrightarrow{\text{Noisy Channel}} & \text{received message} \\ 0 & \longrightarrow & 0 \\ 0 & \leadsto & 1 \end{array}$$

Error correcting codes: Motivation

With coding theory:

$$\text{Message} \quad : \quad \text{NO} = 0$$

Error correcting codes: Motivation

With coding theory:

$$\begin{array}{rcl} \text{Message} & : & \text{NO} = 0 \\ & \downarrow & \textit{Encoding} \\ \text{Codeword} & : & 000 \end{array}$$

Error correcting codes: Motivation

With coding theory:

$$
\begin{array}{rcl}
\text{Message} & : & \text{NO} = 0 \\
 & \downarrow & \textit{Encoding} \\
\text{Codeword} & : & 000 \\
 & \downarrow & \textit{Noisy Channel} \\
 & \rightsquigarrow & \\
\text{Vector} & : & 010
\end{array}
$$

Error correcting codes: Motivation

With coding theory:

Message	:	NO $=$ 0
	$\downarrow$	*Encoding*
Codeword	:	000
	$\downarrow$	*Noisy Channel*
	$\rightsquigarrow$	
Vector	:	010
	$\downarrow$	*Decoding*
Decoded message	:	$010 \cong 000 =$ NO.

Error correcting codes: Definitions

- A linear code of length n and dimension k, over the alphabet $\mathbb{F}_q$, is a k-dimensional subspace C of $V(n, q)$.

Error correcting codes: Definitions

- A linear code of length n and dimension k, over the alphabet $\mathbb{F}_q$, is a k-dimensional subspace C of $V(n, q)$.
- Codeword: vector of C.

ERROR CORRECTING CODES: DEFINITIONS

- A linear code of length n and dimension k, over the alphabet $\mathbb{F}_q$, is a k-dimensional subspace $\mathcal{C}$ of $V(n,q)$.
- Codeword: vector of $\mathcal{C}$.
- A linear $[n,k,d]$-code $\mathcal{C}$ can be defined
  - by a generator matrix G of the subspace $\mathcal{C}$ ($G : k \times n$-matrix)
  - by a parity check matrix H: $x \in \mathcal{C} \iff x.H^T = 0$. ($H : (n-k) \times n$-matrix)

Error correcting codes: Definitions

- A linear code of length n and dimension k, over the alphabet $\mathbb{F}_q$, is a k-dimensional subspace C of $V(n,q)$.
- Codeword: vector of C.
- A linear $[n,k,d]$-code C can be defined
  - by a generator matrix G of the subspace C ($G : k \times n$-matrix)
  - by a parity check matrix H: $x \in \mathrm{C} \iff x.H^T = 0$. ($H : (n-k) \times n$-matrix)
- Encoding: Message: Vector v of $V(k,q) \mapsto v.G$: codeword in $V(n,q)$.

ERROR CORRECTING CODES: DEFINITIONS

- (Hamming) distance $d(c, c')$: Number of positions in which the codewords c and c' differ .
- Minimum distance $d(\mathrm{C})$: $\min\{d(c, c') | c \neq c' \in \mathrm{C}\}$.

Error correcting codes: Definitions

- (Hamming) distance $d(c, c')$: Number of positions in which the codewords c and c' differ .
- Minimum distance $d(\mathrm{C})$: $\min\{d(c, c') | c \neq c' \in \mathrm{C}\}$.
- Weight of c: Number of non-zero positions in $c = d(c, 0)$.
- Minimum weight of C: $\min\{wt(c) | c \neq 0 \in \mathrm{C}\}$.

Properties of a linear error-correcting code

Easy to check

For a linear code C:

- Minimum weight of C=minimum distance of C.
- Minimum distance determines the number of errors that can be corrected (by using nearest-neighbour-decoding).

THE DUAL CODE

The dual code $\mathrm{C}^{\perp}$ of C:
Set of vectors v with $v.c = 0$ for all $c \in \mathrm{C}$.

THE DUAL CODE

The dual code $\mathrm{C}^\perp$ of C:
Set of vectors v with $v.c = 0$ for all $c \in \mathrm{C}$.

Parity check matrix of C=generator matrix of $\mathrm{C}^\perp$ and vice versa.

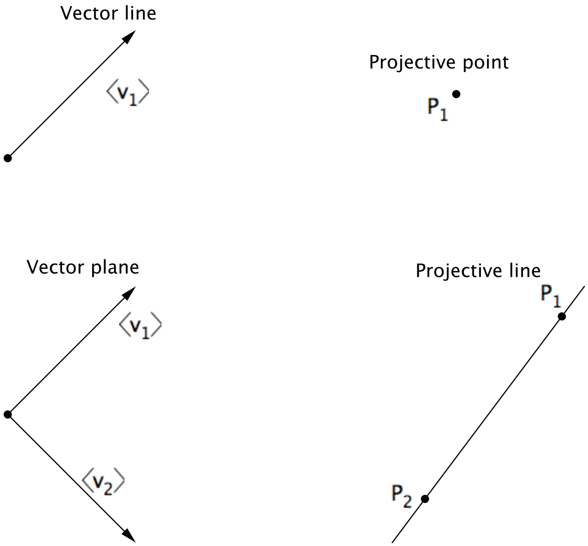
Outline

Projective spaces

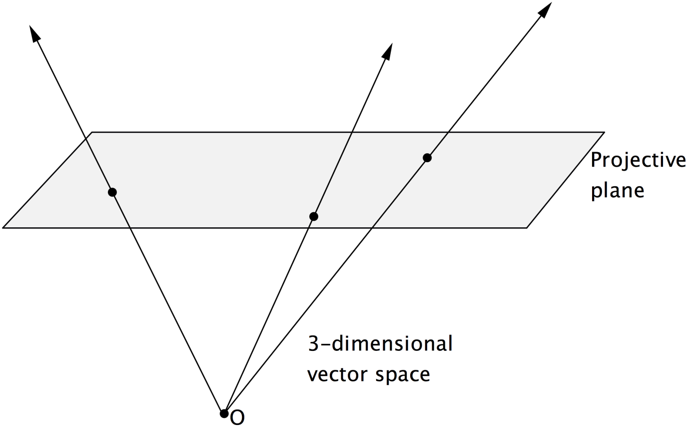
Notation

V: Vector space
$\mathrm{PG}(V)$: Corresponding projective space.

From vector space to projective space



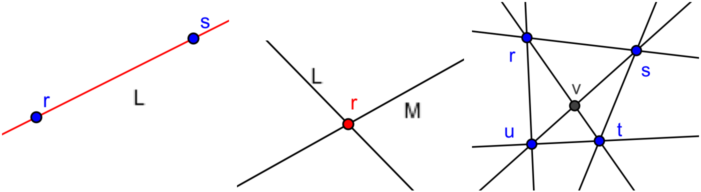
From vector space to projective space



The projective dimension of a projective space is the dimension of the corresponding vector space minus 1

Projective planes

Points, lines and three axioms



(a) $\forall r \neq s \; \exists! L$ (b) $\forall L \neq M \; \exists! r$ (c) $\exists r, s, t, u$

Projective planes over a finite field

Definition

The order of a projective plane is the number of points on a line minus 1.

The order of $\mathrm{PG}(2, q)$ is q, so a line contains $q + 1$ points, and there are $q + 1$ lines through a point.

Existence of a projective plane of order n

$\mathrm{PG}(2, q)$ is an example of a projective plane of order $q = p^h$, p prime.

- Are there projective planes of order n, where n is not a prime power?

THE EXISTENCE OF A PROJECTIVE PLANE OF ORDER n

THEOREM [BRUCK, CHOWLA, RYSER (1949)]

Let n be the order of a projective plane, where $n \equiv 1$ *or* 2 mod 4, then n is the sum of two squares.

The existence of a projective plane of order n

Theorem [Bruck, Chowla, Ryser (1949)]

Let n be the order of a projective plane, where $n \equiv 1 or\ 2 \mod 4$, then n is the sum of two squares.

This theorem rules out projective planes of orders 6 and 14.

THE EXISTENCE OF A PROJECTIVE PLANE OF ORDER n

Does a projective plane of order 10 exist?

The existence of a projective plane of order n

Does a projective plane of order 10 exist?

The answer was found using coding theory.

Outline

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

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

Codes from Desarguesian projective planes

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

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

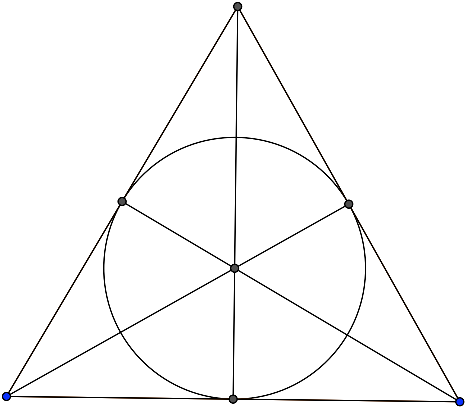
- Generator matrix=incidence matrix of $\mathrm{PG}(2, q)$.
- Generated over $\mathbb{F}_p$.

Notation: $\mathrm{C}_1(2, q)$

The smallest projective plane: PG$(2, 2)$

The projective plane of order 2, the Fano plane, has:

- $q + 1 = 2 + 1 = 3$ points on a line,
- 3 lines through a point.



Code of $\mathrm{PG}(2, 2)$

The incidence matrix of $\mathrm{PG}(2, 2)$ is equal to:

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The codewords are:

$$
\begin{array}{lcccccccc}
\bar{0} & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\bar{1} & = & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\bar{a}_1 & = & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
\bar{a}_2 & = & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
\bar{a}_3 & = & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
\bar{a}_4 & = & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
\bar{a}_5 & = & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
\bar{a}_6 & = & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
\bar{a}_7 & = & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
\bar{b}_1 & = & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
\bar{b}_2 & = & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
\bar{b}_3 & = & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
\bar{b}_4 & = & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
\bar{b}_5 & = & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
\bar{b}_6 & = & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
\bar{b}_7 & = & 0 & 1 & 0 & 1 & 1 & 1 & 0
\end{array}
$$

A GAP IN THE WEIGHT ENUMERATOR

Incidence vector of a line:
codeword of weight $q+1$.

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

A GAP IN THE WEIGHT ENUMERATOR

Incidence vector of a line:
codeword of weight $q+1$.

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

- We exclude all codewords with weight in

$$]q+1, 2q[$$

in the code $\mathrm{C}_1(2,q)$ of points and lines of $\mathrm{PG}(2,q)$, using blocking sets in $\mathrm{PG}(2,q)$.

Blocking sets in $\mathrm{PG}(2, q)$

Definition

A blocking set of $\mathrm{PG}(2, q)$ is a set B of points such that every line contains at least one of the points of B. (The set B 'blocks' all lines of the projective plane.)

Blocking sets in PG$(2, q)$

Definition

A blocking set of PG$(2, q)$ is a set B of points such that every line contains at least one of the points of B. (The set B 'blocks' all lines of the projective plane.)

Definitions

Minimal blocking set B: B has no proper subset that is still a blocking set.

Blocking sets in $\mathrm{PG}(2, q)$

Definition

A blocking set of $\mathrm{PG}(2, q)$ is a set B of points such that every line contains at least one of the points of B. (The set B 'blocks' all lines of the projective plane.)

Definitions

Minimal blocking set B: B has no proper subset that is still a blocking set.

Small blocking set B: $|B| < 3(q+1)/2$.

THE LINK WITH BLOCKING SETS

THEOREM [LAVRAUW, STORME, VDV (2008)]

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

THE LINK WITH BLOCKING SETS

THEOREM [LAVRAUW, STORME, VDV (2008)]

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

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.

COROLLARIES OF THE LINK WITH BLOCKING SETS

THEOREM [BOSE, 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

Theorem [Bose, 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.

Corollaries of the link with blocking sets

Theorem [Bose, 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.

This result was first obtained by Assmus and 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 $]p + 1, 2p[$.

This result was already obtained by Chouinard and by McGuire and Ward for $]p + 1, 3(p + 1)/2[$.

THE LINK WITH BLOCKING SETS CONTINUED

We can prove more:

THEOREM [LAVRAUW, STORME, SZIKLAI, VDV (2009)]

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

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

THEOREM [LAVRAUW, STORME, SZIKLAI, 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

THEOREM [LAVRAUW, STORME, SZIKLAI, VDV (2009)]

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

As a corollary:

THEOREM [LAVRAUW, STORME, SZIKLAI, VDV(2009)]

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

EXTENSIONS TO LARGER DIMENSIONS

$\mathrm{C}_k(n,q)$: Generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$.

Extensions to larger dimensions

$C_k(n, q)$: Generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n, q)$.

Similar results:

- M. Lavrauw, L. Storme, G. VdV: On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n, q)$ and its dual.
  Finite Fields Appl. **20** (2008), 1020–1038.
- M. Lavrauw, L. Storme, P. Sziklai, G. VdV: An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $\mathrm{PG}(n, q)$.
  J. Combin. Theory Ser. A **116** (2009), 996–1001.

Recent improvement

Theorem [A. Gács, T. Szőnyi, Zs. Weiner (20??)]

A codeword c in $\mathrm{C}_1(2, q)$, $q = p^h$, 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 $h > 2$.

Back to the axiomatic projective planes

The incidence matrix A of a projective plane of order n satisfies:

$$A.A^T = n.I + J = A^T.A,$$

with J the all-one matrix.

The Bruck-Chowla-Ryser theorem

They proved that: if an $(n^2+n+1)\times(n^2+n+1)$-matrix A satifies this condition and if $n \equiv 1 \text{ or } 2 \mod 4$, then n is the sum of two squares.

METHOD

- Lam, Swierz and Thiel studied the binary code generated by the incidence matrix of a putative plane of order 10.

THE PROJECTIVE PLANE OF ORDER 10

METHOD

- Lam, Swierz and Thiel studied the binary code generated by the incidence matrix of a putative plane of order 10.
- Weight enumerator is determined by the number A_i of codewords with weight i, for $i = 12, 15, 16$.

THE PROJECTIVE PLANE OF ORDER 10

METHOD

- Lam, Swierz and Thiel studied the binary code generated by the incidence matrix of a putative plane of order 10.
- Weight enumerator is determined by the number A_i of codewords with weight i, for $i = 12, 15, 16$.
- A (lengthy!) computer calculation shows that $A_{12} = A_{15} = A_{16} = 0$.

The projective plane of order 10

Method

- Lam, Swierz and Thiel studied the binary code generated by the incidence matrix of a putative plane of order 10.
- Weight enumerator is determined by the number A_i of codewords with weight i, for $i = 12, 15, 16$.
- A (lengthy!) computer calculation shows that $A_{12} = A_{15} = A_{16} = 0$.
- There is no projective plane of order 10.

OUTLINE

Quadrics: definition

Every homogeneous quadratic polynomial $f(X_0, \ldots, X_N)$ in $N + 1$ variables defines a quadric $\mathcal{Q}(N, q)$ of $\mathrm{PG}(N, q)$.

Quadrics: definition

Every homogeneous quadratic polynomial $f(X_0, \ldots, X_N)$ in $N + 1$ variables defines a quadric $\mathcal{Q}(N, q)$ of $\mathrm{PG}(N, q)$.

There are 3 kinds of non-singular quadrics:

- Elliptic quadrics $\mathcal{Q}^-(2n + 1, q)$: equivalent to $X_0X_1 + \cdots + X_{2n-2}X_{2n-1} + f(X_{2n}, X_{2n+1}) = 0$ where f is an irreducible homogeneous polynomial of degree 2.
- Hyperbolic quadrics $\mathcal{Q}^+(2n + 1, q)$: equivalent to $X_0X_1 + \cdots + X_{2n-2}X_{2n-1} + X_{2n}X_{2n+1} = 0$.
- Parabolic quadrics $\mathcal{Q}(2n, q)$: equivalent to $X_0X_1 + \cdots + X_{2n-2}X_{2n-1} + X_{2n}^2 = 0$.

Generators

We denote the largest dimensional spaces contained in a quadric by the *generators*.

Quadric	dimension generator
$\mathcal{Q}^-(2n+1,q)$	$n-1$
$\mathcal{Q}(2n,q)$	$n-1$
$\mathcal{Q}^+(2n+1,q)$	n

Blocking sets and ovoids of Quadrics

Blocking set of $\mathcal{Q}$: set of points meeting every generator.
Ovoid of $\mathcal{Q}$: set of points meeting every generator in exactly one point.

Ovoids of a hyperbolic quadric

- The number of points on a hyperbolic quadric is $(q^n + 1)(q^{n+1} - 1)/(q - 1)$.
- The size of an ovoid of $\mathcal{Q}^+(2n + 1, q)$ is $q^n + 1$.

Ovoids of a hyperbolic quadric

- The number of points on a hyperbolic quadric is $(q^n + 1)(q^{n+1} - 1)/(q - 1)$.
- The size of an ovoid of $\mathcal{Q}^+(2n + 1, q)$ is $q^n + 1$.

Do ovoids of a hyperbolic quadric exist?

- $\mathcal{Q}^+(3, q)$: ✓

Ovoids of a hyperbolic quadric

- The number of points on a hyperbolic quadric is $(q^n + 1)(q^{n+1} - 1)/(q - 1)$.
- The size of an ovoid of $\mathcal{Q}^+(2n + 1, q)$ is $q^n + 1$.

Do ovoids of a hyperbolic quadric exist?

- $\mathcal{Q}^+(3, q)$: ✓
- $\mathcal{Q}^+(5, q)$: ✓

Ovoids of a hyperbolic quadric

- The number of points on a hyperbolic quadric is $(q^n + 1)(q^{n+1} - 1)/(q - 1)$.
- The size of an ovoid of $\mathcal{Q}^+(2n + 1, q)$ is $q^n + 1$.

Do ovoids of a hyperbolic quadric exist?

- $\mathcal{Q}^+(3, q)$: ✓
- $\mathcal{Q}^+(5, q)$: ✓
- $\mathcal{Q}^+(7, q)$, q even or $q = 0$ or $2 \mod 3$: ✓

Ovoids of a hyperbolic quadric

- The number of points on a hyperbolic quadric is $(q^n+1)(q^{n+1}-1)/(q-1)$.
- The size of an ovoid of $\mathcal{Q}^+(2n+1,q)$ is q^n+1.

Do ovoids of a hyperbolic quadric exist?

- $\mathcal{Q}^+(3,q)$: ✓
- $\mathcal{Q}^+(5,q)$: ✓
- $\mathcal{Q}^+(7,q)$, q even or $q = 0$ or $2 \mod 3$: ✓
- $\mathcal{Q}^+(2n+1,2)$, $n \geq 4$: ✗

Ovoids of a hyperbolic quadric

- The number of points on a hyperbolic quadric is $(q^n+1)(q^{n+1}-1)/(q-1)$.
- The size of an ovoid of $\mathcal{Q}^+(2n+1,q)$ is q^n+1.

Do ovoids of a hyperbolic quadric exist?

- $\mathcal{Q}^+(3,q)$: ✓
- $\mathcal{Q}^+(5,q)$: ✓
- $\mathcal{Q}^+(7,q)$, q even or $q = 0$ or $2 \mod 3$: ✓
- $\mathcal{Q}^+(2n+1,2)$, $n \geq 4$: ✗
- $\mathcal{Q}^+(2n+1,3)$, $n \geq 4$: ✗
- What about the other cases?

Ovoids of a hyperbolic quadric

- The number of points on a hyperbolic quadric is $(q^n + 1)(q^{n+1} - 1)/(q - 1)$.
- The size of an ovoid of $\mathcal{Q}^+(2n+1, q)$ is $q^n + 1$.

Do ovoids of a hyperbolic quadric exist?

- $\mathcal{Q}^+(3, q)$: ✓
- $\mathcal{Q}^+(5, q)$: ✓
- $\mathcal{Q}^+(7, q)$, q even or $q = 0$ or $2 \mod 3$: ✓
- $\mathcal{Q}^+(2n+1, 2)$, $n \geq 4$: ✗
- $\mathcal{Q}^+(2n+1, 3)$, $n \geq 4$: ✗
- What about the other cases?

The non-existence of ovoids in some particular hyperbolic quadrics was shown using ideas from coding theory.

A partition of the incidence matrix of points and hyperplanes

Points of $\mathcal{Q}^+(2n+1, q)$: $P_1, \ldots, P_s$.
Other points of $\mathrm{PG}(2n+1, q)$: $P_{s+1}, \ldots, P_m$.

A PARTITION OF THE INCIDENCE MATRIX OF POINTS AND HYPERPLANES

Points of $\mathcal{Q}^+(2n+1,q)$: $P_1,\ldots,P_s$.
Other points of $\mathrm{PG}(2n+1,q)$: $P_{s+1},\ldots,P_m$.
Tangent hyperplane at P_i: H_i.
Other hyperplanes: $H_{s+1},\ldots,H_n$.

A partition of the incidence matrix of points and hyperplanes

Points of $\mathcal{Q}^+(2n+1, q)$: $P_1, \dots, P_s$.
Other points of $\mathrm{PG}(2n+1, q)$: $P_{s+1}, \dots, P_m$.
Tangent hyperplane at P_i: H_i.
Other hyperplanes: $H_{s+1}, \dots, H_n$.
Incidence matrix:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}.$$

A partition of the incidence matrix of points and hyperplanes

Points of $\mathcal{Q}^+(2n+1,q)$: $P_1,\ldots,P_s$.
Other points of $\mathrm{PG}(2n+1,q)$: $P_{s+1},\ldots,P_m$.
Tangent hyperplane at P_i: H_i.
Other hyperplanes: $H_{s+1},\ldots,H_n$.
Incidence matrix:

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}.$$

Condition for the existence of an ovoid of $\mathcal{Q}^+(2n+1,q)$

p-rank $A_{11} \geq q^n + 1$.

The existence of an ovoid of $\mathcal{Q}^+(2n+1, q)$

p-rank A= dimension of the code of points and hyperplanes in $\mathrm{PG}(n, q)$ (known).

THE EXISTENCE OF AN OVOID OF $\mathcal{Q}^+(2n+1,q)$

p-rank A= dimension of the code of points and hyperplanes in $\mathrm{PG}(n,q)$ (known).

p-rank A_{11} can be calculated in a similar way

The existence of an ovoid of $\mathcal{Q}^+(2n+1, q)$

p-rank A= dimension of the code of points and hyperplanes in $\mathrm{PG}(n, q)$ (known).

p-rank A_{11} can be calculated in a similar way

p-rank $A_{11} \geq q^n + 1$ gives a contradiction in some cases.

Theorem [A. Blokhuis, E. Moorhouse (1995)]

There are no ovoids in $\mathcal{Q}^+(9, 2^e), \mathcal{Q}^+(9, 3^e), \mathcal{Q}^+(11, 5^e), \mathcal{Q}^+(11, 7^e)$.

The code of points and lines of $\mathcal{Q}(4, q)$

$\mathrm{C}(\mathcal{Q}(4, q))$: code generated by incidence matrix of points and lines of $\mathcal{Q}(4, q)$.

The code of points and lines of $\mathcal{Q}(4, q)$

$\mathrm{C}(\mathcal{Q}(4, q))$: code generated by incidence matrix of points and lines of $\mathcal{Q}(4, q)$.

$\mathrm{C}(\mathcal{Q}(4, q))$: subcode of $\mathrm{C}_1(4, q)$ $\rightarrow$ e.g. no codewords with weight in $]q+1, 2q[$ if q is prime.

THE DUAL CODE $C(\mathcal{Q}(4, q))^\perp$

Codeword c of $C(\mathcal{Q}(4, q))^\perp$, q even, corresponds to a set S of points such that every line contains an even number of points of S.

The dual code $C(\mathcal{Q}(4,q))^\perp$

Codeword c of $C(\mathcal{Q}(4,q))^\perp$, q even, corresponds to a set S of points such that every line contains an even number of points of S.

Codewords of minimum weight

Trivial lower bound: $d \geq q+2$.

Theorem [J.L. Kim, K. Mellinger, L. Storme (2007)]

Let $c \in C(\mathcal{Q}(4,q))^\perp$:

- $wt(c) \geq 2q+2$ if q is even (sharp)
- $wt(c) \geq \frac{(q+1)\sqrt{q}}{2}$ if q is odd.

Codewords of large weight

Codeword c of $\mathrm{C}(\mathcal{Q}(4, q))^{\perp}$, q even, corresponds to a set S of points such that every line contains an even number of points of S.

A line of $\mathcal{Q}(4, q)$, q even, contains an odd number of points of $\mathcal{Q}(4, q)$.

Codewords of large weight

Codeword c of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, corresponds to a set S of points such that every line contains an even number of points of S.

A line of $\mathcal{Q}(4,q)$, q even, contains an odd number of points of $\mathcal{Q}(4,q)$.

Observation

The complement of a codeword c of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, determines a set S of points such that every line of $\mathcal{Q}(4,q)$ contains an odd number of points of S.

Codewords of large weight

Codeword c of $\mathrm{C}(\mathcal{Q}(4,q))^{\perp}$, q even, corresponds to a set S of points such that every line contains an even number of points of S.

A line of $\mathcal{Q}(4,q)$, q even, contains an odd number of points of $\mathcal{Q}(4,q)$.

Observation

The complement of a codeword c of $\mathrm{C}(\mathcal{Q}(4,q))^{\perp}$, q even, determines a set S of points such that every line of $\mathcal{Q}(4,q)$ contains an odd number of points of S.

Corollary

The complement of a codeword of $\mathrm{C}(\mathcal{Q}(4,q))^{\perp}$, q even, is a blocking set of $\mathcal{Q}(4,q)$.

CODEWORDS OF LARGE WEIGHT

NOTATION: B= COMPLEMENT OF A CODEWORD c

If every line contains exactly one point of B: B is an ovoid of $\mathcal{Q}(4, q)$. Ovoids of $\mathcal{Q}(4, q)$ have $q^2 + 1$ points.

Codewords of large weight

Notation: B= complement of a codeword c

If every line contains exactly one point of B: B is an ovoid of $\mathcal{Q}(4,q)$. Ovoids of $\mathcal{Q}(4,q)$ have q^2+1 points.

Lemma [V. Pepe, L. Storme, G. VdV (20??)]

Let c be a codeword of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even. Then $wt(c) \leq q^3+q$ and $wt(c) = q^3+q$ iff B is an ovoid.

CODEWORDS OF LARGE WEIGHT

NOTATION: B= COMPLEMENT OF A CODEWORD c

If every line contains exactly one point of B: B is an ovoid of $\mathcal{Q}(4, q)$. Ovoids of $\mathcal{Q}(4, q)$ have $q^2 + 1$ points.

LEMMA [V. PEPE, L. STORME, G. VDV (20??)]

Let c be a codeword of $\mathrm{C}(\mathcal{Q}(4, q))^\perp$, q even. Then $wt(c) \leq q^3 + q$ and $wt(c) = q^3 + q$ iff B is an ovoid.

THEOREM [V. PEPE, L. STORME, G. VDV (20??)]

A blocking set B of $\mathcal{Q}(4, q)$, q even, with $|B| \leq q^2 + q/6$, always contains an ovoid.

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4, q))^{\perp}$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4, q))^{\perp}$ with weight in $[q^3 + 5q/6, q^3 + q[$.

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4,q))^\perp$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4,q))^\perp$ with weight in $[q^3 + 5q/6, q^3 + q[$.

PROOF.

- c: codeword with weight $\geq q^3 + 5q/6$.

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4,q))^\perp$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4,q))^\perp$ with weight in $[q^3 + 5q/6, q^3 + q[$.

PROOF.

- c: codeword with weight $\geq q^3 + 5q/6$.
- B: blocking set of size $\leq q^2 + q/6$

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4,q))^\perp$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4,q))^\perp$ with weight in $[q^3+5q/6, q^3+q[$.

PROOF.

- c: codeword with weight $\geq q^3+5q/6$.
- B: blocking set of size $\leq q^2+q/6$
- B': ovoid contained in B

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4,q))^\perp$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4,q))^\perp$ with weight in $[q^3 + 5q/6, q^3 + q[$.

PROOF.

- c: codeword with weight $\geq q^3 + 5q/6$.
- B: blocking set of size $\leq q^2 + q/6$
- B': ovoid contained in B
- c': vector such that complement of c' is B'

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4,q))^\perp$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4,q))^\perp$ with weight in $[q^3+5q/6, q^3+q[$.

PROOF.

- c: codeword with weight $\geq q^3+5q/6$.
- B: blocking set of size $\leq q^2+q/6$
- B': ovoid contained in B
- c': vector such that complement of c' is B'
- c'= codeword!

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4,q))^\perp$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4,q))^\perp$ with weight in $[q^3 + 5q/6, q^3 + q[$.

PROOF.

- c: codeword with weight $\geq q^3 + 5q/6$.
- B: blocking set of size $\leq q^2 + q/6$
- B': ovoid contained in B
- c': vector such that complement of c' is B'
- c'= codeword!
- $c - c'$ codeword with weight $\leq q/6 < 2q + 2$

A GAP IN THE WEIGHT ENUMERATOR OF $C(\mathcal{Q}(4,q))^\perp$

COROLLARY [V. PEPE, L. STORME, G. VDV (20??)]

There are no codewords in $C(\mathcal{Q}(4,q))^\perp$ with weight in $[q^3+5q/6, q^3+q[$.

PROOF.

- c: codeword with weight $\geq q^3+5q/6$.
- B: blocking set of size $\leq q^2+q/6$
- B': ovoid contained in B
- c': vector such that complement of c' is B'
- c'= codeword!
- $c-c'$ codeword with weight $\leq q/6 < 2q+2$
- $c=c' \Rightarrow wt(c)=q^3+q$.

□

Similar results:

- J.L. Kim, K. Mellinger, L. Storme: Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles. *Des. Codes Cryptogr.* **42** (2007), 73–92.
- V. Pepe, L. Storme, G. Van de Voorde: Small weight codewords in the LDPC codes arising from linear representations of geometries. *J. Combin. Des.* **17** (2009), 1–24.
- V. Pepe, L. Storme, G. Van de Voorde: On codewords in the dual code of classical generalised quadrangles and classical polar spaces. *Discrete Math.*, to appear.

Outline

Introduction

Projective spaces

Codes from projective spaces

Codes and ovoids of quadrics

Functional codes

DEFINITION

DEFINITION

Consider a non-singular quadric $\mathcal{Q}$ of $\mathrm{PG}(N, q)$. Let $\mathcal{Q} = \{P_1, \ldots, P_n\}$. Let $\mathcal{F}$ be the set of all homogeneous quadratic polynomials $f(X_0, \ldots, X_N)$ defined by $N + 1$ variables. The functional code $\mathrm{C}_2(\mathcal{Q})$ is the linear code

$$\mathrm{C}_2(\mathcal{Q}) = \{(f(P_1), \ldots, f(P_n)) || f \in \mathcal{F} \cup \{0\}\}.$$

Definition

Definition

Consider a non-singular quadric $\mathcal{Q}$ of $\mathrm{PG}(N, q)$. Let $\mathcal{Q} = \{P_1, \ldots, P_n\}$. Let $\mathcal{F}$ be the set of all homogeneous quadratic polynomials $f(X_0, \ldots, X_N)$ defined by $N + 1$ variables. The functional code $\mathrm{C}_2(\mathcal{Q})$ is the linear code

$$\mathrm{C}_2(\mathcal{Q}) = \{(f(P_1), \ldots, f(P_n)) || f \in \mathcal{F} \cup \{0\}\}.$$

$n = |\mathcal{Q}|$,

$k = \binom{N+2}{2} - 1$,

$d = ?$

The minimum weight

A codeword of small weight:

- codeword with many zeros
- quadric having a large intersection with $\mathcal{Q}$.

Results

Theorem [F. Edoukou (2007)]

Minimum weight codewords for $C_2(\mathcal{Q})$ in $\mathrm{PG}(3, q)$ and $\mathrm{PG}(4, q)$ correspond to singular quadrics consisting of two hyperplanes.

Results

Theorem [F. Edoukou (2007)]

Minimum weight codewords for $\mathrm{C}_2(\mathcal{Q})$ in $\mathrm{PG}(3, q)$ and $\mathrm{PG}(4, q)$ correspond to singular quadrics consisting of two hyperplanes.

Theorem [F. Edoukou, A. Hallez, F. Rodier, L. Storme (20??)]

- Minimum weight codewords for $\mathrm{C}_2(\mathcal{Q})$ in $\mathrm{PG}(N, q)$ correspond to a singular quadric consisting of two hyperplanes.
- Codewords of small weight: determination of the possibilities for the intersection of quadrics with a set of two hyperplanes.

Small weight codewords in $C_2(\mathcal{Q})$, $\mathcal{Q}$ a hyperbolic quadric $\mathcal{Q}^+(2l+1, q)$

Weight	Number of codewords
$w_1 = q^{2l} - q^{2l-1} - q^l + q^{l-1}$	$\frac{(q^{3l}+q^{2l})(q^{l+1}-1)}{2}$
$w_1 + q^l - q^{l-1}$	$\frac{(q^{2l+1}-q)(q^{l+1}-1)(q^{l-1}+1)}{2(q-1)} +$ $(q^{3l-1} - q^{l-1})(q^{l+2} - q)$
$w_1 + q^l$	$(q^{3l} + q^{2l})(q^{l+1} - 1)(q - 1)$
$w_1 + 2q^l - 2q^{l-1}$	$\frac{q^{2l+1}(q^{l+1}-1)(q^l-1)(q-1)}{4}$
$w_1 + 2q^l - q^{l-1}$	$\frac{(q^{3l-1}-q^{l-1})(q^{l+1}-1)(q^2-q)}{2}$
$w_1 + 2q^l$	$\frac{(q^{3l}+q^{2l})(q^{l+1}-1)(q^2-3q+2)}{4}$

Similar results:

- F.A.B. Edoukou, A. Hallez, F. Rodier, L. Storme: On the small weight codewords of the functional codes $C_2(\mathcal{Q})$, $\mathcal{Q}$ a non-singular quadric.
  J. Pure Appl. Algebra, submitted.
- F.A.B. Edoukou, A. Hallez, F. Rodier, L. Storme: On the small weight codewords of the functional codes $C_h(X)$, X a non-singular hermitian variety.
  Des. Codes Cryptogr., submitted.
- A. Hallez, L. Storme: Functional codes arising from quadric intersections with hermitian varieties.
  Finite Fields Appl., submitted.