A Finite Geometry Construction for MDPC-Codes

Master Thesis

Jessica Bariffi

September 21, 2020

Table of Contents

1. Introduction
2. Coding Theory
   - Basics
   - MDPC-Codes
3. Finite Geometry
4. Projective Bundles
5. Construction

Introduction

Motivation

- Code-based cryptography $\longrightarrow$ quantum-secure cryptosystems.

Motivation

- Code-based cryptography $\longrightarrow$ quantum-secure cryptosystems.
- McEliece cryptosystem.

Motivation

- Code-based cryptography $\longrightarrow$ quantum-secure cryptosystems.
- McEliece cryptosystem.
    - Goppa codes

Motivation

- Code-based cryptography $\longrightarrow$ quantum-secure cryptosystems.
- McEliece cryptosystem.
  - Goppa codes
  - Low-density parity-check (LDPC) codes

Motivation

- Code-based cryptography $\longrightarrow$ quantum-secure cryptosystems.
- McEliece cryptosystem.
    - Goppa codes
    - Low-density parity-check (LDPC) codes
    - Moderate-density parity-check (MDPC) codes

Goal

- Many constructions (mainly random) exist for MDPC codes

Goal

- Many constructions (mainly random) exist for MDPC codes
- Error-correction performance for random codes is asymptotic

Goal

- Many constructions (mainly random) exist for MDPC codes
- Error-correction performance for random codes is asymptotic
- Give a construction of MDPC codes optimizing the error-correction performance after one round of the bit-flipping decoding algorithm

Coding Theory

Linear Codes

Let $GF(q)$ denote the finite field of q elements, q is a prime power.

Definition

A q*-ary linear code* C of length n and dimension k is a k-dimensional linear subspace of $GF(q)^n$.

Remarks

- We denote C as $[n, k]_q$—linear code.

Linear Codes

Let $GF(q)$ denote the finite field of q elements, q is a prime power.

Definition

A *q-ary linear code* C of length n and dimension k is a k-dimensional linear subspace of $GF(q)^n$.

Remarks

- We denote C as $[n,k]_q-$linear code.
- A codeword $c \in C$ is a vector of length n over a finite field $GF(q)$.

Dual Code

Definition

Let C be an $[n,k]_q-$linear code. Its *dual code* $C^\perp$ is given by

$$C^\perp = \{x \in GF(q)^n \,|\, x \cdot c^\top = 0, \forall c \in C\}.$$

Representation of linear codes

Definition

Let C be an $[n,k]_q-$ linear code. A *generator matrix* for C is a $(k \times n)$ matrix whose rows are formed from any k linearly independent vectors of C. Similarly we define a matrix $H \in GF(q)^{(n-k)\times n}$, the *parity check matrix* of C, to be the generator matrix of the dual code $C^{\perp}$.

Remarks:

- It holds that $H \cdot G^{\top} = 0$.

Representation of linear codes

Definition

Let C be an $[n,k]_q-$ linear code. A *generator matrix* for C is a $(k \times n)$ matrix whose rows are formed from any k linearly independent vectors of C. Similarly we define a matrix $H \in GF(q)^{(n-k)\times n}$, the *parity check matrix* of C, to be the generator matrix of the dual code $C^\perp$.

Remarks:

- It holds that $H \cdot G^\top = 0$.
- $C = \ker H = \{c \in GF(q)^n \mid Hc^\top = 0\}$.

Minimum Distance

Definition

Let x and y be two vectors of $GF(q)^n$. The *Hamming distance* $d(x, y)$ is the number of positions in which x and y differ, i.e.

$$d(x, y) = |\{i \in \{1, \ldots, n\} \mid x_i \neq y_i\}|.$$

The *minimum distance* of a code C, denoted $d(C)$, is the smallest possible Hamming distance two codewords c and $\tilde{c}$ of C,

$$d(C) := \min\{d(c, \tilde{c}) \mid c, \tilde{c} \in C, c \neq \tilde{c}\}.$$

Minimum Distance

Definition

Let x and y be two vectors of $GF(q)^n$. The *Hamming distance* $d(x, y)$ is the number of positions in which x and y differ, i.e.

$$d(x,y) = |\{i \in \{1,\dots,n\} \mid x_i \neq y_i\}| .$$

The *minimum distance* of a code C, denoted $d(C)$, is the smallest possible Hamming distance two codewords c and $\tilde{c}$ of C,

$$d(C) := \min\{d(c,\tilde{c}) \mid c, \tilde{c} \in C, c \neq \tilde{c}\}.$$

Example
$C = \{(0,0,0,0),(0,0,1,1),(1,1,0,0),(1,1,1,1)\}$

Minimum Distance

Definition

Let x and y be two vectors of $GF(q)^n$. The *Hamming distance* $d(x,y)$ is the number of positions in which x and y differ, i.e.

$$d(x,y) = \left|\{i \in \{1,\ldots,n\} \mid x_i \neq y_i\}\right|.$$

The *minimum distance* of a code C, denoted $d(C)$, is the smallest possible Hamming distance two codewords c and $\tilde{c}$ of C,

$$d(C) := \min\{d(c,\tilde{c}) \mid c, \tilde{c} \in C, c \neq \tilde{c}\}.$$

Example

$C = \{(0,0,0,0),(0,0,1,1),(1,1,0,0),(1,1,1,1)\}$

- possible distances between two words: 2 or 4.

Minimum Distance

Definition

Let x and y be two vectors of $GF(q)^n$. The *Hamming distance* $d(x, y)$ is the number of positions in which x and y differ, i.e.

$$d(x, y) = |\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}| .$$

The *minimum distance* of a code C, denoted $d(C)$, is the smallest possible Hamming distance two codewords c and $\tilde{c}$ of C,

$$d(C) := \min\{d(c, \tilde{c}) \mid c, \tilde{c} \in C, c \neq \tilde{c}\}.$$

Example

$C = \{(0, 0, 0, 0), (0, 0, 1, 1), (1, 1, 0, 0), (1, 1, 1, 1)\}$

- possible distances between two words: 2 or 4.
- $d(C) = 2$

Weight

Definition

The weight of a vector $x = (x_1, \ldots, x_n) \in GF(q)^n$ is the the number of non-zero positions of x, i.e. $wt(x) = |\{i = 1, \ldots, n | x_i \neq 0\}|$.

Weight

Definition

The weight of a vector $x = (x_1, \ldots, x_n) \in GF(q)^n$ is the the number of non-zero positions of x, i.e. $wt(x) = |\{i = 1, \ldots, n | x_i \neq 0\}|$.

Remark

If every row x of a matrix H has a constant weight $wt(x) = w$ then we say that H has *row-weight* w.

MDPC-Codes: Background

- Introduction of LDPC-codes in 1963 by Robert Gallager ([2]).

MDPC-Codes: Background

- Introduction of LDPC-codes in 1963 by Robert Gallager ([2]).
- Advantage: high error-correction performance.

MDPC-Codes: Background

- Introduction of LDPC-codes in 1963 by Robert Gallager ([2]).
- Advantage: high error-correction performance.
- Problem: due to the low-weight of the dual codewords, some variants of the McEliece cryptosystem can be attacked.

MDPC-Codes: Background

- Introduction of LDPC-codes in 1963 by Robert Gallager ([2]).
- Advantage: high error-correction performance.
- Problem: due to the low-weight of the dual codewords, some variants of the McEliece cryptosystem can be attacked.
- Extension of LDPC-codes by increasing the row-weight $\longrightarrow$ MDPC-codes.

MDPC-Codes

Definition

A *moderate density parity-check code*, or simply MDPC-code, is a binary linear code of length n with a parity-check matrix whose row weight is $\mathcal{O}(\sqrt{n})$. If the weight of every column is v and the weight of every row is w we say the MDPC-code is *of type* (v, w).

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:
  - Check if y is already a codeword, i.e when $H \cdot y^\top = 0$. If so, then no error occured.
    If not, proceed as follows:

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:
  - Check if y is already a codeword, i.e when $H \cdot y^\top = 0$. If so, then no error occured.
    If not, proceed as follows:
  - For each column j of H compute the number of non-zero entries n_j.

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:
  - Check if y is already a codeword, i.e when $H \cdot y^\top = 0$. If so, then no error occured.
    If not, proceed as follows:
  - For each column j of H compute the number of non-zero entries n_j.
  - Compute for each j of H the number of unsatisfied check equations $u_j = \left|\left\{i \in \{1, \ldots, r\} \,\middle|\, h_{ij} = 1, \sum_l h_{il} y_l = 1 \pmod 2\right\}\right|$.

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:
  - Check if y is already a codeword, i.e when $H \cdot y^\top = 0$. If so, then no error occured.
    If not, proceed as follows:
  - For each column j of H compute the number of non-zero entries n_j.
  - Compute for each j of H the number of unsatisfied check equations $u_j = \left|\left\{i \in \{1, \ldots, r\} \mid h_{ij} = 1, \sum_l h_{il} y_l = 1 \pmod 2\right\}\right|$.
  - If $u_j > n_j/2$, then flip y_j.

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:
  - Check if y is already a codeword, i.e when $H \cdot y^\top = 0$. If so, then no error occured.
    If not, proceed as follows:
  - For each column j of H compute the number of non-zero entries n_j.
  - Compute for each j of H the number of unsatisfied check equations $u_j = \left|\left\{i \in \{1, \ldots, r\} \,|\, h_{ij} = 1, \sum_l h_{il} y_l = 1 \pmod 2\right\}\right|$.
  - If $u_j > n_j/2$, then flip y_j.
  - Compute the syndrome $s = H \cdot y^\top$.

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:
  - Check if y is already a codeword, i.e when $H \cdot y^\top = 0$. If so, then no error occured.
    If not, proceed as follows:
  - For each column j of H compute the number of non-zero entries n_j.
  - Compute for each j of H the number of unsatisfied check equations $u_j = \left|\left\{i \in \{1, \ldots, r\} \,|\, h_{ij} = 1, \sum_l h_{il} y_l = 1 \pmod 2\right\}\right|$.
  - If $u_j > n_j/2$, then flip y_j.
  - Compute the syndrome $s = H \cdot y^\top$.
- Stops if syndrome is zero or if the maximal number of iterations $b_{\max}$ is reached.

The Bit-Flipping Decoding Algorithm

- Inputs: Parity-check matrix H, received word y.
- Output: Decoded word.
- Algorithm:
    - Check if y is already a codeword, i.e when $H \cdot y^\top = 0$. If so, then no error occured.
      If not, proceed as follows:
    - For each column j of H compute the number of non-zero entries n_j.
    - Compute for each j of H the number of unsatisfied check equations $u_j = \left|\left\{i \in \{1, \ldots, r\} \,\middle|\, h_{ij} = 1, \sum_l h_{il} y_l = 1 \pmod 2\right\}\right|$.
    - If $u_j > n_j/2$, then flip y_j.
    - Compute the syndrome $s = H \cdot y^\top$.
- Stops if syndrome is zero or if the maximal number of iterations $b_{\max}$ is reached.
- Complexity: $\mathcal{O}(nwb_{\max})$

Maximum Column Intersection

Definition

Let $H = (h_{ij})_{\substack{1\leq i\leq r\\ 1\leq j\leq n}}$ be a binary matrix. The *intersection number* of two different columns j and j' of H is equal to the number of rows i for which $h_{ij} = h_{ij'} = 1$. The *maximum column intersection*, denoted s_H, of H is equal to the maximum intersection number of two distinct columns of H.

Maximum Column Intersection

Definition

Let $H = (h_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}}$ be a binary matrix. The *intersection number* of two different columns j and j' of H is equal to the number of rows i for which $h_{ij} = h_{ij'} = 1$. The *maximum column intersection*, denoted s_H, of H is equal to the maximum intersection number of two distinct columns of H.

Example

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

Maximum Column Intersection

Definition

Let $H = (h_{ij})_{\substack{1 \le i \le r \\ 1 \le j \le n}}$ be a binary matrix. The *intersection number* of two different columns j and j' of H is equal to the number of rows i for which $h_{ij} = h_{ij'} = 1$. The *maximum column intersection*, denoted s_H, of H is equal to the maximum intersection number of two distinct columns of H.

Example

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

For any two distinct columns the intersection number is 0, 1 or 2.

Maximum Column Intersection

Definition

Let $H = (h_{ij})_{\substack{1 \le i \le r \\ 1 \le j \le n}}$ be a binary matrix. The *intersection number* of two different columns j and j' of H is equal to the number of rows i for which $h_{ij} = h_{ij'} = 1$. The *maximum column intersection*, denoted s_H, of H is equal to the maximum intersection number of two distinct columns of H.

Example

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

For any two distinct columns the intersection number is 0, 1 or 2.

Then $s_H = 2$.

Error-Correction Capacity

Proposition, [5]

Let C be an MDPC-Code of type (v, w) with parity-check matrix $H = (h_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}}$. Let s_H be the maximum column intersection with respect to the parity check matrix H. Performing one round of the bit-flipping decoding algorithm based on the matrix H one can correct all errors of weight at most $\lfloor \frac{v}{2s_H} \rfloor$.

Error-Correction Capacity

Proposition, [5]

Let C be an MDPC-Code of type (v, w) with parity-check matrix $H = (h_{ij})_{\substack{1 \le i \le r \\ 1 \le j \le n}}$. Let s_H be the maximum column intersection with respect to the parity check matrix H. Performing one round of the bit-flipping decoding algorithm based on the matrix H one can correct all errors of weight at most $\lfloor \frac{v}{2s_H} \rfloor$.

Remarks:

Error-Correction Capacity

Proposition, [5]

Let C be an MDPC-Code of type (v, w) with parity-check matrix $H = (h_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}}$. Let s_H be the maximum column intersection with respect to the parity check matrix H. Performing one round of the bit-flipping decoding algorithm based on the matrix H one can correct all errors of weight at most $\lfloor \frac{v}{2s_H} \rfloor$.

Remarks:

- The smaller s_H, the bigger the amount of errors that can be corrected.

Error-Correction Capacity

Proposition, [5]

Let C be an MDPC-Code of type (v, w) with parity-check matrix $H = (h_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}}$. Let s_H be the maximum column intersection with respect to the parity check matrix H. Performing one round of the bit-flipping decoding algorithm based on the matrix H one can correct all errors of weight at most $\lfloor \frac{v}{2s_H} \rfloor$.

Remarks:

- The smaller s_H, the bigger the amount of errors that can be corrected.
- **Goal**: Give a construction of MDPC-codes with a small maximum column intersection.

Finite Geometry

Incidence Structure

Definition

An *incidence structure* is a triple $S = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, consisting of a set of points $\mathcal{P}$, a set of lines $\mathcal{L}$ that is distinct from the set of points, and an incidence relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$ between the points and the lines.

Incidence Structure

Definition

An *incidence structure* is a triple $S = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, consisting of a set of points $\mathcal{P}$, a set of lines $\mathcal{L}$ that is distinct from the set of points, and an incidence relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$ between the points and the lines.

Example

$\mathcal{P} = \{a, b, c, d\}$, $\mathcal{L} = \{l = \{a, b\}, m = \{b, c\}, n = \{c, d\}, o = \{a, d\}\}$.

Incidence Structure

Definition

An *incidence structure* is a triple $S = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, consisting of a set of points $\mathcal{P}$, a set of lines $\mathcal{L}$ that is distinct from the set of points, and an incidence relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$ between the points and the lines.

Example

$\mathcal{P} = \{a, b, c, d\}$, $\mathcal{L} = \{l = \{a, b\}, m = \{b, c\}, n = \{c, d\}, o = \{a, d\}\}$.

- A point $P \in \mathcal{P}$ is incident to a line $L \in \mathcal{L}$ if and only if $P \in L$.

Incidence Structure

Definition

An *incidence structure* is a triple $S = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, consisting of a set of points $\mathcal{P}$, a set of lines $\mathcal{L}$ that is distinct from the set of points, and an incidence relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$ between the points and the lines.

Example

$\mathcal{P} = \{a, b, c, d\}$, $\mathcal{L} = \{l = \{a, b\}, m = \{b, c\}, n = \{c, d\}, o = \{a, d\}\}$.

- A point $P \in \mathcal{P}$ is incident to a line $L \in \mathcal{L}$ if and only if $P \in L$.
- The point a is incident to line l and o.

Incidence Matrix

Definition

Let S be an incidence structure of n points and m lines. An *incidence matrix* $A = (a_{ij})$ is an $(n \times m)$ matrix defined by

$$a_{ij} = \begin{cases} 0, & \text{if point } p_i \text{ does not lie on line } l_j \\ 1, & \text{if point } p_i \text{ lies on line } l_j. \end{cases}$$

Incidence Matrix

Definition

Let S be an incidence structure of n points and m lines. An *incidence matrix* $A = (a_{ij})$ is an $(n \times m)$ matrix defined by

$$a_{ij} = \begin{cases} 0, & \text{if point } p_i \text{ does not lie on line } l_j \\ 1, & \text{if point } p_i \text{ lies on line } l_j. \end{cases}$$

Example
$\mathcal{P} = \{a, b, c, d\}$, $\mathcal{L} = \{l = \{a, b\}, m = \{b, c\}, n = \{c, d\}, o = \{a, d\}\}$.

Incidence Matrix

Definition

Let S be an incidence structure of n points and m lines. An *incidence matrix* $A = (a_{ij})$ is an $(n \times m)$ matrix defined by

$$a_{ij} = \begin{cases} 0, & \text{if point } p_i \text{ does not lie on line } l_j \\ 1, & \text{if point } p_i \text{ lies on line } l_j. \end{cases}$$

Example

$\mathcal{P} = \{a, b, c, d\}$, $\mathcal{L} = \{l = \{a, b\}, m = \{b, c\}, n = \{c, d\}, o = \{a, d\}\}$.

- $$A = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} l & m & n & o \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Projective plane

Definition

A *projective plane* is an incidence structure Π of points and lines satisfying the following properties

(P1) Any two distinct points are incident with exactly one line,

(P2) Any two distinct lines are incident with exactly one point,

(P3) There are four points such that no three of them are collinear.

Projective plane

Definition

A *projective plane* is an incidence structure Π of points and lines satisfying the following properties

(P1) Any two distinct points are incident with exactly one line,

(P2) Any two distinct lines are incident with exactly one point,

(P3) There are four points such that no three of them are collinear.

Remark:

Projective plane

Definition

A *projective plane* is an incidence structure Π of points and lines satisfying the following properties

(P1) Any two distinct points are incident with exactly one line,

(P2) Any two distinct lines are incident with exactly one point,

(P3) There are four points such that no three of them are collinear.

Remark:

- A *finite projective plane* is a projective plane of finitely many points and lines.

Projective Plane

Number of points incident to a line

Every point in a finite projective plane is incident to a constant $q + 1$ lines. Dually every line passes through a constant $q + 1$ points.

The number q is called the order of a projective plane.

Projective Plane

Number of points incident to a line

Every point in a finite projective plane is incident to a constant $q+1$ lines. Dually every line passes through a constant $q+1$ points.

The number q is called the order of a projective plane.

Projective Plane

Number of points incident to a line

Every point in a finite projective plane is incident to a constant $q+1$ lines. Dually every line passes through a constant $q+1$ points.

The number q is called the order of a projective plane.

Total number of points and lines

In a finite projective plane of order q there are q^2+q+1 points and q^2+q+1 lines.

Desarguesian Plane

A projective plane that can be constructed from a three-dimensional vector space over a field K is called a *Desarguesian plane*. We denote it by $PG(2, K)$.

Desarguesian Plane

A projective plane that can be constructed from a three-dimensional vector space over a field K is called a *Desarguesian plane*. We denote it by $PG(2, K)$.

Desarguesian plane $PG(2, q)$ over $GF(q)$:

Desarguesian Plane

A projective plane that can be constructed from a three-dimensional vector space over a field K is called a *Desarguesian plane*. We denote it by $PG(2, K)$.

Desarguesian plane $PG(2, q)$ over $GF(q)$:

- Identified with the equivalence classes of $GF(q)^3\backslash\{0\}/_\sim$, where:

$$(x, y, z) \sim (\lambda x, \lambda y, \lambda z) \text{ for } \lambda \in GF(q)\backslash\{0\}.$$

Desarguesian Plane

A projective plane that can be constructed from a three-dimensional vector space over a field K is called a *Desarguesian plane*. We denote it by $PG(2, K)$.

Desarguesian plane $PG(2, q)$ over $GF(q)$:

- Identified with the equivalence classes of $GF(q)^3 \backslash \{0\}/_\sim$, where:

$$(x, y, z) \sim (\lambda x, \lambda y, \lambda z) \text{ for } \lambda \in GF(q) \backslash \{0\}.$$

- For a given point $P = [x, y, z]$ the set of lines passing through P is given by

$$\langle a, b, c \rangle := \{[a, b, c] \in PG(2, q) \mid ax + by + cz = 0\}.$$

Desarguesian Plane

Example: Fano Plane $PG(2,2)$

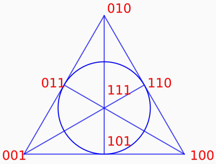
- Consists of $2^2 + 2 + 1 = 7$ points and 7 lines.

Desarguesian Plane

Example: Fano Plane $PG(2, 2)$

- Consists of $2^2 + 2 + 1 = 7$ points and 7 lines.

$$\mathcal{P} = \{[1,0,1],[1,1,0],[0,1,1],[1,1,1],\\ [0,0,1],[1,0,0],[0,1,0]\},$$
$$\mathcal{L} = \{\langle 1,0,1\rangle,\langle 1,1,0\rangle,\langle 0,1,1\rangle,\langle 1,1,1\rangle,\\ \langle 0,0,1\rangle,\langle 1,0,0\rangle,\langle 0,1,0\rangle\}.$$



Desarguesian Plane

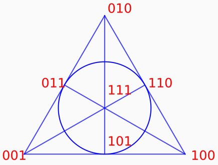
Example: Fano Plane $PG(2,2)$

- Consists of $2^2 + 2 + 1 = 7$ points and 7 lines.

$$\begin{aligned}\mathcal{P} = \{&[1,0,1],[1,1,0],[0,1,1],[1,1,1],\\ &[0,0,1],[1,0,0],[0,1,0]\},\\ \mathcal{L} = \{&\langle 1,0,1\rangle,\langle 1,1,0\rangle,\langle 0,1,1\rangle,\langle 1,1,1\rangle,\\ &\langle 0,0,1\rangle,\langle 1,0,0\rangle,\langle 0,1,0\rangle\}.\end{aligned}$$

- An incidence matrix is given by

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$



Codes from Projective Planes

Late 1950s: constructions of error-correcting codes using projective planes.

- Let $\Pi = PG(2, q)$ of odd order q over $GF(2)$ with incidence matrix H.

Codes from Projective Planes

Late 1950s: constructions of error-correcting codes using projective planes.

- Let $\Pi = PG(2, q)$ of odd order q over $GF(2)$ with incidence matrix H.
- The columns of H correspond to the lines and the rows of H correspond to the points.

Codes from Projective Planes

Late 1950s: constructions of error-correcting codes using projective planes.

- Let $\Pi = PG(2, q)$ of odd order q over $GF(2)$ with incidence matrix H.
- The columns of H correspond to the lines and the rows of H correspond to the points.
- H is an $(q^2 + q + 1) \times (q^2 + q + 1)$ binary matrix of column-weight $v = q + 1 = \mathcal{O}(\sqrt{q^2 + q + 1})$.

Codes from Projective Planes

Late 1950s: constructions of error-correcting codes using projective planes.

- Let $\Pi = PG(2, q)$ of odd order q over $GF(2)$ with incidence matrix H.
- The columns of H correspond to the lines and the rows of H correspond to the points.
- H is an $(q^2 + q + 1) \times (q^2 + q + 1)$ binary matrix of column-weight $v = q + 1 = \mathcal{O}(\sqrt{q^2 + q + 1})$.
- Maximum column intersection $s_H = 1$.

Codes from Projective Planes

Late 1950s: constructions of error-correcting codes using projective planes.

- Let $\Pi = PG(2, q)$ of odd order q over $GF(2)$ with incidence matrix H.
- The columns of H correspond to the lines and the rows of H correspond to the points.
- H is an $(q^2 + q + 1) \times (q^2 + q + 1)$ binary matrix of column-weight $v = q + 1 = \mathcal{O}(\sqrt{q^2 + q + 1})$.
- Maximum column intersection $s_H = 1$.
- Define a binary linear code $C_2(\Pi) = \mathrm{rowspace}(H)$,

Codes from Projective Planes

Late 1950s: constructions of error-correcting codes using projective planes.

- Let $\Pi = PG(2, q)$ of odd order q over $GF(2)$ with incidence matrix H.
- The columns of H correspond to the lines and the rows of H correspond to the points.
- H is an $(q^2 + q + 1) \times (q^2 + q + 1)$ binary matrix of column-weight $v = q + 1 = \mathcal{O}(\sqrt{q^2 + q + 1})$.
- Maximum column intersection $s_H = 1$.
- Define a binary linear code $C_2(\Pi) = \mathrm{rowspace}(H)$,
- $C_2(\Pi)^\perp = \ker(H)$ is a $[q^2 + q + 1, 1]_2-$linear code.

Projective Bundles

Conic

Definition

A *conic* $\mathcal{C}$ of a projective plane Π of order q is a set of points $[x, y, z]$ of Π satisfying a quadratic equation.

- A general quadratic equation is $ax^2 + by^2 + cz^2 + dyz + exz + fxy = 0$, where $a, b, c, d, e, f \in GF(q)$ not all zero. Its associated matrix is $A = \begin{pmatrix} 2a & f & e \\ f & 2b & d \\ e & d & 2c \end{pmatrix}$.

Conic

Definition

A *conic* $\mathcal{C}$ of a projective plane Π of order q is a set of points $[x, y, z]$ of Π satisfying a quadratic equation.

- A general quadratic equation is $ax^2 + by^2 + cz^2 + dyz + exz + fxy = 0$, where $a, b, c, d, e, f \in GF(q)$ not all zero. Its associated matrix is $A = \begin{pmatrix} 2a & f & e \\ f & 2b & d \\ e & d & 2c \end{pmatrix}$.

Conic

Definition

A *conic* $\mathcal{C}$ of a projective plane Π of order q is a set of points $[x, y, z]$ of Π satisfying a quadratic equation.

- A general quadratic equation is $ax^2 + by^2 + cz^2 + dyz + exz + fxy = 0$, where $a, b, c, d, e, f \in GF(q)$ not all zero. Its associated matrix is
$$A = \begin{pmatrix} 2a & f & e \\ f & 2b & d \\ e & d & 2c \end{pmatrix}.$$

Definition

A conic $\mathcal{C}$ is *non-degenerate* if $\det(A) \neq 0$ when q is odd, or if (d, e, f) is non-zero and not contained in $\mathcal{C}$ when q is even.
A *degenerate* conic is a conic which is not non-degenerate.

Conic

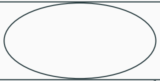
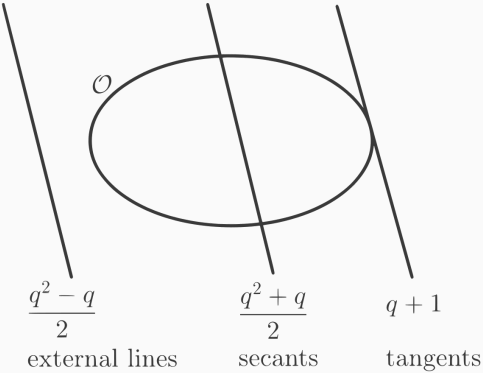
Type of conic	points in $\mathcal{C}$	Diagram
non-degenerate	$q+1$	
repeated line	$q+1$	
two real lines	$2q+1$	
two imaginary lines	1	

Table 1: The four distinct types of conics in $PG(2,q)$.

Non-Degenerate Conic and Lines



The relative positions between lines and a non-degenerate conic.

Definition

Definition

A *projective bundle* $\mathcal{B}$ is a collection of $q^2 + q + 1$ non-degenerate conics in $PG(2, q)$ that are mutually intersecting in a unique point.

Definition

Definition

A *projective bundle* $\mathcal{B}$ is a collection of $q^2 + q + 1$ non-degenerate conics in $PG(2, q)$ that are mutually intersecting in a unique point.

Remarks:

Definition

Definition

A *projective bundle* $\mathcal{B}$ is a collection of $q^2 + q + 1$ non-degenerate conics in $PG(2, q)$ that are mutually intersecting in a unique point.

Remarks:

- Non-degenerate conics of $\mathcal{B}$ can be interpreted as lines in $PG(2, q)$.

Definition

Definition

A *projective bundle* $\mathcal{B}$ is a collection of $q^2 + q + 1$ non-degenerate conics in $PG(2, q)$ that are mutually intersecting in a unique point.

Remarks:

- Non-degenerate conics of $\mathcal{B}$ can be interpreted as lines in $PG(2, q)$.
- The incidence structure of $PG(2, q)$ can be represented by points and non-degenerate conics of $\mathcal{B}$.

Definition

Definition

A *projective bundle* $\mathcal{B}$ is a collection of $q^2 + q + 1$ non-degenerate conics in $PG(2, q)$ that are mutually intersecting in a unique point.

Remarks:

- Non-degenerate conics of $\mathcal{B}$ can be interpreted as lines in $PG(2, q)$.
- The incidence structure of $PG(2, q)$ can be represented by points and non-degenerate conics of $\mathcal{B}$.
- The rows of an incidence matrix are represented by the points and the columns are represented by the non-degenerate conics.

Existence in $PG(2, q)$

David Glynn has studied projective bundles in detail in his Ph.D. thesis from 1978 ([3]).

- He proved the existence of projective bundles in $PG(2, q)$.

Existence in $PG(2, q)$

David Glynn has studied projective bundles in detail in his Ph.D. thesis from 1978 ([3]).

- He proved the existence of projective bundles in $PG(2, q)$.
- Classification of totally three types.

Existence in $PG(2, q)$

David Glynn has studied projective bundles in detail in his Ph.D. thesis from 1978 ([3]).

- He proved the existence of projective bundles in $PG(2, q)$.
- Classification of totally three types.
- Each of the three types exists for an odd prime power q.

Existence in $PG(2,q)$

David Glynn has studied projective bundles in detail in his Ph.D. thesis from 1978 ([3]).

- He proved the existence of projective bundles in $PG(2,q)$.
- Classification of totally three types.
- Each of the three types exists for an odd prime power q.
- Only one of these is a projective bundle also if q is an even prime power.

Algebraic Classification

Due to Singer ([4]).

Identify the points of $PG(2, q)$ with the integers mod $q^2 + q + 1$.

Algebraic Classification

Due to Singer ([4]).

Identify the points of $PG(2,q)$ with the integers mod q^2+q+1.

Definition

If a set D of $q+1$ distinct integers $d_0,\dots,d_q$ has the property that $(d_i-d_j)_{0\le i\ne j\le q}$ are distinct mod q^2+q+1, then D is called a *perfect difference set*.

Algebraic Classification

Due to Singer ([4]).

Identify the points of $PG(2,q)$ with the integers mod q^2+q+1.

Definition

If a set D of $q+1$ distinct integers $d_0,\ldots,d_q$ has the property that $(d_i-d_j)_{0\leq i\neq j\leq q}$ are distinct mod q^2+q+1, then D is called a *perfect difference set*.

Algebraic Classification

Due to Singer ([4]).

Identify the points of $PG(2,q)$ with the integers mod q^2+q+1.

Definition

If a set D of $q+1$ distinct integers $d_0,\dots,d_q$ has the property that $(d_i-d_j)_{0\leq i\neq j\leq q}$ are distinct mod q^2+q+1, then D is called a *perfect difference set*.

Example

For $q=2$, the set $\{0,1,3\}$ of 3 integers is a perfect difference set mod 7, because all the possible differences

$$0-1\equiv\mathbf{6},\ 0-3\equiv\mathbf{4},\ 1-3\equiv\mathbf{5},\ 1-0\equiv\mathbf{1},\ 3-0\equiv\mathbf{3},\ 3-1\equiv\mathbf{2}$$

are distinct mod 7

Algebraic Classification

Construction of a perfect difference set of $q+1$ integers:

- Write d_0 for the point in $PG(2,q)$ identified with 0 and d_1 for the point in $PG(2,q)$ identified with 1.

Algebraic Classification

Construction of a perfect difference set of $q+1$ integers:

- Write d_0 for the point in $PG(2,q)$ identified with 0 and d_1 for the point in $PG(2,q)$ identified with 1.
- Suppose then that the points that are on the same line with d_0 and d_1 are labelled by $d_2, \ldots, d_q$.
  For instance, if $q=2$: $d_0 = 0$, $d_1 = 1$, $d_2 = 3$.

Algebraic Classification

Construction of a perfect difference set of $q+1$ integers:

- Write d_0 for the point in $PG(2,q)$ identified with 0 and d_1 for the point in $PG(2,q)$ identified with 1.
- Suppose then that the points that are on the same line with d_0 and d_1 are labelled by $d_2,\ldots,d_q$.
  For instance, if $q=2$: $d_0=0$, $d_1=1$, $d_2=3$.
- $D=\{d_0,d_1,\ldots,d_q\}$ is a perfect difference set.

Algebraic Classification

Construction of a perfect difference set of $q+1$ integers:

- Write d_0 for the point in $PG(2,q)$ identified with 0 and d_1 for the point in $PG(2,q)$ identified with 1.
- Suppose then that the points that are on the same line with d_0 and d_1 are labelled by $d_2, \ldots, d_q$.
  For instance, if $q = 2$: $d_0 = 0$, $d_1 = 1$, $d_2 = 3$.
- $D = \{d_0, d_1, \ldots, d_q\}$ is a perfect difference set.
- The following array with integers reduced mod q^2+q+1 represents the points and lines of $PG(2,q)$.

$$\begin{array}{cccc} d_0 & d_0+1 & \cdots & d_0+q^2+q \\ d_1 & d_1+1 & \cdots & d_1+q^2+q \\ \vdots & \vdots & \cdots & \vdots \\ d_q & d_q+1 & \cdots & d_q+q^2+q \end{array}$$

Algebraic Classification

Consider the projective plane $PG(2, q)$ of order q.

- Identify the set of points with the integers modulo $q^2 + q + 1$.

Algebraic Classification

Consider the projective plane $PG(2,q)$ of order q.

- Identify the set of points with the integers modulo q^2+q+1.
- The lines are the shifts of a perfect difference set D, i.e.

$$\mathcal{L} = \left\{ \{d_0+i, d_1+i, \ldots, d_q+i\} \,|\, i \in \mathbb{Z}/_{\langle q^2+q+1\rangle} \right\}.$$

Algebraic Classification

Consider the projective plane $PG(2,q)$ of order q.

- Identify the set of points with the integers modulo q^2+q+1.
- The lines are the shifts of a perfect difference set D, i.e.

$$\mathcal{L} = \left\{ \{d_0+i, d_1+i, \ldots, d_q+i\} \,|\, i \in \mathbb{Z}/_{\langle q^2+q+1\rangle} \right\}.$$

Algebraic Classification

Consider the projective plane $PG(2, q)$ of order q.

- Identify the set of points with the integers modulo $q^2 + q + 1$.
- The lines are the shifts of a perfect difference set D, i.e.

$$\mathcal{L} = \left\{ \{d_0 + i, d_1 + i, \ldots, d_q + i\} \mid i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle} \right\}.$$

Example

Algebraic Classification

Consider the projective plane $PG(2,q)$ of order q.

- Identify the set of points with the integers modulo q^2+q+1.
- The lines are the shifts of a perfect difference set D, i.e.

$$\mathcal{L} = \left\{ \{d_0+i, d_1+i, \ldots, d_q+i\} \mid i \in \mathbb{Z}/_{\langle q^2+q+1\rangle} \right\}.$$

Example

Algebraic Classification

Consider the projective plane $PG(2, q)$ of order q.

- Identify the set of points with the integers modulo $q^2 + q + 1$.
- The lines are the shifts of a perfect difference set D, i.e.

$$\mathcal{L} = \left\{ \{d_0 + i, d_1 + i, \ldots, d_q + i\} \mid i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle} \right\}.$$

Example

Fano plane $PG(2, 2)$:
$\mathcal{P} = \{0, 1, 2, 3, 4, 5, 6\}$,
$D = \{0, 1, 3\}$,
$\mathcal{L} = \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\},$
$\{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}\}.$

Algebraic Classification

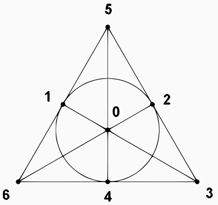
Consider the projective plane $PG(2,q)$ of order q.

- Identify the set of points with the integers modulo q^2+q+1.
- The lines are the shifts of a perfect difference set D, i.e.

$$\mathcal{L} = \left\{ \{d_0+i, d_1+i, \ldots, d_q+i\} \mid i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle} \right\}.$$

Example

Fano plane $PG(2,2)$:
$\mathcal{P} = \{0,1,2,3,4,5,6\}$,
$D = \{0,1,3\}$,
$\mathcal{L} = \{\{0,1,3\},\{1,2,4\},\{2,3,5\},$
$\{3,4,6\},\{4,5,0\},\{5,6,1\},\{6,0,2\}\}$.



Algebraic Classification

Theorem [1]

For $N = q^2 + q + 1$, if $r \in \mathbb{Z}/_{\langle N \rangle}$ is relatively prime to N and $D = \{d_0, \ldots, d_q\}$ a perfect difference set for $PG(2, q)$, then the set $D/r = \{d_0/r, \ldots, d_q/r\}$ is the point set of some curve of degree r.

Notes:

- The order q is an odd prime power and $N = q^2 + q + 1$ is odd too.

Algebraic Classification

Theorem [1]

For $N = q^2 + q + 1$, if $r \in \mathbb{Z}/_{\langle N \rangle}$ is relatively prime to N and $D = \{d_0, \ldots, d_q\}$ a perfect difference set for $PG(2, q)$, then the set $D/r = \{d_0/r, \ldots, d_q/r\}$ is the point set of some curve of degree r.

Notes:

- The order q is an odd prime power and $N = q^2 + q + 1$ is odd too.
- The values $r \in \{-1, 2^{-1}, 2\}$ are always relatively prime to N.

Algebraic Classification

Theorem [1]

For $N = q^2 + q + 1$, if $r \in \mathbb{Z}/_{\langle N \rangle}$ is relatively prime to N and $D = \{d_0, \ldots, d_q\}$ a perfect difference set for $PG(2, q)$, then the set $D/r = \{d_0/r, \ldots, d_q/r\}$ is the point set of some curve of degree r.

Notes:

- The order q is an odd prime power and $N = q^2 + q + 1$ is odd too.
- The values $r \in \{-1, 2^{-1}, 2\}$ are always relatively prime to N.
    1. *Circumscribed bundle:* Image of $-D$ under the cycle $S(i) = i + 1$, for $i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle}$.

Algebraic Classification

Theorem [1]

For $N = q^2 + q + 1$, if $r \in \mathbb{Z}/_{\langle N \rangle}$ is relatively prime to N and $D = \{d_0, \ldots, d_q\}$ a perfect difference set for $PG(2, q)$, then the set $D/r = \{d_0/r, \ldots, d_q/r\}$ is the point set of some curve of degree r.

Notes:

- The order q is an odd prime power and $N = q^2 + q + 1$ is odd too.
- The values $r \in \{-1, 2^{-1}, 2\}$ are always relatively prime to N.
    1. *Circumscribed bundle:* Image of $-D$ under the cycle $S(i) = i + 1$, for $i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle}$.
    2. *Inscribed bundle:* Image of $D/2^{-1} = 2D$ under the cycle $S(i) = i + 1$, for $i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle}$.

Algebraic Classification

Theorem [1]

For $N = q^2 + q + 1$, if $r \in \mathbb{Z}/_{\langle N \rangle}$ is relatively prime to N and $D = \{d_0, \ldots, d_q\}$ a perfect difference set for $PG(2, q)$, then the set $D/r = \{d_0/r, \ldots, d_q/r\}$ is the point set of some curve of degree r.

Notes:

- The order q is an odd prime power and $N = q^2 + q + 1$ is odd too.
- The values $r \in \{-1, 2^{-1}, 2\}$ are always relatively prime to N.
  1. *Circumscribed bundle:* Image of $-D$ under the cycle $S(i) = i + 1$, for $i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle}$.
  2. *Inscribed bundle:* Image of $D/2^{-1} = 2D$ under the cycle $S(i) = i + 1$, for $i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle}$.
  3. *Self-polar bundle:* Image of $D/2$ under the cycle $S(i) = i + 1$, for $i \in \mathbb{Z}/_{\langle q^2+q+1 \rangle}$.

Algebraic Classification

Example

- Consider $PG(2,3)$. A perfect difference set of $q+1=4$ integers modulo $q^2+q+1=13$ is given by $D=\{0,1,3,9\}$.

Algebraic Classification

Example

- Consider $PG(2,3)$. A perfect difference set of $q+1=4$ integers modulo $q^2+q+1=13$ is given by $D=\{0,1,3,9\}$.
- Choose one of the bundles. For instance, $2D=\{0,2,6,5\}$.

Algebraic Classification

Example

- Consider $PG(2,3)$. A perfect difference set of $q+1=4$ integers modulo $q^2+q+1=13$ is given by $D=\{0,1,3,9\}$.
- Choose one of the bundles. For instance, $2D=\{0,2,6,5\}$.
- Hence an inscribed bundle is given by $\mathcal{B}_I=\{\{0+i,2+i,5+i,6+i\}\,|\,i\in\mathbb{Z}/_{\langle 13\rangle}\}$.

Construction

The Parity-Check Matrix

Let $PG(2,q)$ be of odd order q.

Π: Representation of $PG(2,q)$ with points and lines.

The Parity-Check Matrix

Let $PG(2,q)$ be of odd order q.

Π: Representation of $PG(2,q)$ with points and lines.

Γ: Representation of $PG(2,q)$ with points and non-deg. conics of a projective bundle.

The Parity-Check Matrix

Let $PG(2,q)$ be of odd order q.

Π: Representation of $PG(2,q)$ with points and lines.

Γ: Representation of $PG(2,q)$ with points and non-deg. conics of a projective bundle.

Let H_1 and H_2 be two incidence matrices of Π and Γ.

The Parity-Check Matrix

Let $PG(2,q)$ be of odd order q.

Π: Representation of $PG(2,q)$ with points and lines.

Γ: Representation of $PG(2,q)$ with points and non-deg. conics of a projective bundle.

Let H_1 and H_2 be two incidence matrices of Π and Γ.

Define $H = [H_1|H_2]$ of size $(q^2+q+1) \times 2(q^2+q+1)$.

$$H = \begin{array}{c} \\ p_1 \\ p_2 \\ \vdots \\ p_{q^2+q+1} \end{array} \begin{array}{c} \begin{array}{cccc|cccc} l_1 & l_2 & \dots & l_{q^2+q+1} & c_1 & c_2 & \dots & c_{q^2+q+1} \end{array} \\ \left(\begin{array}{cccc|cccc} & & & & & & & \\ & & & & & & & \\ & & & & & & & \\ & & & & & & & \end{array} \right) \end{array}$$

The Parity-Check Matrix

Example

Consider $PG(2,3)$: identify the points with $\mathbb{Z}/_{\langle 13 \rangle}$.

The Parity-Check Matrix

Example

Consider $PG(2,3)$: identify the points with $\mathbb{Z}/_{\langle 13\rangle}$.

- $\mathcal{P} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$,
  $\mathcal{L} = \left\{\{0+i, 1+i, 3+i, 9+i\} \,|\, i \in \mathbb{Z}/_{\langle 13\rangle}\right\}$

The Parity-Check Matrix

Example

Consider $PG(2,3)$: identify the points with $\mathbb{Z}/_{\langle 13\rangle}$.

- $\mathcal{P} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$,
  $\mathcal{L} = \left\{\{0+i, 1+i, 3+i, 9+i\} \mid i \in \mathbb{Z}/_{\langle 13\rangle}\right\}$
- Inscribed bundle: $\mathcal{B}_I = \{\{0+i, 2+i, 5+i, 6+i\} \mid i \in \mathbb{Z}/_{\langle 13\rangle}\}$.

The Parity-Check Matrix

Example

Consider $PG(2,3)$: identify the points with $\mathbb{Z}/_{\langle 13\rangle}$.

- $\mathcal{P} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$,
  $\mathcal{L} = \big\{\{0+i, 1+i, 3+i, 9+i\} \,|\, i \in \mathbb{Z}/_{\langle 13\rangle}\big\}$
- Inscribed bundle: $\mathcal{B}_I = \{\{0+i, 2+i, 5+i, 6+i\} \,|\, i \in \mathbb{Z}/_{\langle 13\rangle}\}$.

$$\left(\begin{array}{ccccccccccccc|ccccccccccccc}
1&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&1&1&0&0&1&0\\
1&1&0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&1&0&0&1\\
0&1&1&0&0&0&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&1&1&0&0\\
1&0&1&1&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&0\\
0&1&0&1&1&0&0&0&1&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1\\
0&0&1&0&1&1&0&0&0&1&0&0&0&1&0&0&1&0&1&0&0&0&0&0&0&1\\
0&0&0&1&0&1&1&0&0&0&1&0&0&1&1&0&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&1&0&1&1&0&0&0&1&0&0&1&1&0&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&1&0&1&1&0&0&0&1&0&0&1&1&0&0&1&0&1&0&0&0&0\\
1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0&0\\
0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0\\
0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&1&1&0&0&1&0&1&0\\
0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&1&1&0&0&1&0&1
\end{array}\right)$$

MDPC-Code from Planes

Constructed code:

- $C_2(\Pi \sqcup \Gamma)^\perp := \ker(H)$ is binary linear code of length $n = 2(q^2 + q + 1)$ and type $(v, w) = (q + 1, 2(q + 1))$.

MDPC-Code from Planes

Constructed code:

- $C_2(\Pi \sqcup \Gamma)^\perp := \ker(H)$ is binary linear code of length $n = 2(q^2 + q + 1)$ and type $(v, w) = (q + 1, 2(q + 1))$.
- Indeed $v = \mathcal{O}(\sqrt{n})$. Thus, $C_2(\Pi \sqcup \Gamma)^\perp$ is an MDPC-code.

MDPC-Code from Planes

Constructed code:

- $C_2(\Pi \sqcup \Gamma)^\perp := \ker(H)$ is binary linear code of length $n = 2(q^2 + q + 1)$ and type $(v, w) = (q + 1, 2(q + 1))$.
- Indeed $v = \mathcal{O}(\sqrt{n})$. Thus, $C_2(\Pi \sqcup \Gamma)^\perp$ is an MDPC-code.

MDPC-Code from Planes

Constructed code:

- $C_2(\Pi \sqcup \Gamma)^\perp := \ker(H)$ is binary linear code of length $n = 2(q^2 + q + 1)$ and type $(v, w) = (q + 1, 2(q + 1))$.
- Indeed $v = \mathcal{O}(\sqrt{n})$. Thus, $C_2(\Pi \sqcup \Gamma)^\perp$ is an MDPC-code.

Proposition

The dimension of the MDPC-code $C_2(\Pi \sqcup \Gamma)^\perp$ is given by $\dim(C_2(\Pi \sqcup \Gamma)^\perp) = q^2 + q + 2$.

MDPC-Code from Planes

Constructed code:

- $C_2(\Pi \sqcup \Gamma)^\perp := \ker(H)$ is binary linear code of length $n = 2(q^2 + q + 1)$ and type $(v, w) = (q + 1, 2(q + 1))$.
- Indeed $v = \mathcal{O}(\sqrt{n})$. Thus, $C_2(\Pi \sqcup \Gamma)^\perp$ is an MDPC-code.

Proposition

The dimension of the MDPC-code $C_2(\Pi \sqcup \Gamma)^\perp$ is given by $\dim(C_2(\Pi \sqcup \Gamma)^\perp) = q^2 + q + 2$.

MDPC-Code from Planes

Constructed code:

- $C_2(\Pi \sqcup \Gamma)^\perp := \ker(H)$ is binary linear code of length $n = 2(q^2 + q + 1)$ and type $(v, w) = (q + 1, 2(q + 1))$.
- Indeed $v = \mathcal{O}(\sqrt{n})$. Thus, $C_2(\Pi \sqcup \Gamma)^\perp$ is an MDPC-code.

Proposition

The dimension of the MDPC-code $C_2(\Pi \sqcup \Gamma)^\perp$ is given by $\dim(C_2(\Pi \sqcup \Gamma)^\perp) = q^2 + q + 2$.

Theorem

Let d denote the minimum distance of the MDPC-code $C_2(\Pi \sqcup \Gamma)^\perp$. Then the following estimate holds

$$\left\lfloor \frac{2q+4}{3} \right\rfloor + 1 \leq d.$$

Error-correction

Recall:
MDPC-code of length n, column-weight v, parity-check matrix H and max. column intersection $s \implies$ after performing one round of bit-flipping algorithm one can correct errors of weight at most $\lfloor \frac{v}{2s} \rfloor$.

- For $C_2(\Pi \sqcup \Gamma)^{\perp}$ of length $n = 2(q^2 + q + 1)$ and parity-check matrix H we have:

Error-correction

Recall:
MDPC-code of length n, column-weight v, parity-check matrix H and max. column intersection $s \Longrightarrow$ after performing one round of bit-flipping algorithm one can correct errors of weight at most $\lfloor \frac{v}{2s} \rfloor$.

- For $C_2(\Pi \sqcup \Gamma)^{\perp}$ of length $n = 2(q^2 + q + 1)$ and parity-check matrix H we have:
    - column-weight $v = q + 1$.

Error-correction

Recall:
MDPC-code of length n, column-weight v, parity-check matrix H and max. column intersection $s \implies$ after performing one round of bit-flipping algorithm one can correct errors of weight at most $\lfloor \frac{v}{2s} \rfloor$.

- For $C_2(\Pi \sqcup \Gamma)^\perp$ of length $n = 2(q^2 + q + 1)$ and parity-check matrix H we have:
  - column-weight $v = q + 1$.
  - $s_H = 2$.

Error-correction

Recall:
MDPC-code of length n, column-weight v, parity-check matrix H and max. column intersection $s \implies$ after performing one round of bit-flipping algorithm one can correct errors of weight at most $\lfloor \frac{v}{2s} \rfloor$.

- For $C_2(\Pi \sqcup \Gamma)^\perp$ of length $n = 2(q^2 + q + 1)$ and parity-check matrix H we have:
  - column-weight $v = q + 1$.
  - $s_H = 2$.

Error-correction

Recall:
MDPC-code of length n, column-weight v, parity-check matrix H and max. column intersection $s \implies$ after performing one round of bit-flipping algorithm one can correct errors of weight at most $\lfloor \frac{v}{2s} \rfloor$.

- For $C_2(\Pi \sqcup \Gamma)^\perp$ of length $n = 2(q^2 + q + 1)$ and parity-check matrix H we have:
    - column-weight $v = q + 1$.
    - $s_H = 2$.

Theorem

After performing one round of bit-flipping decoding algorithm on a parity-check matrix H of $C_2(\Pi \sqcup \Gamma)^\perp$ we can correct errors of weight up to $\lfloor \frac{q+1}{4} \rfloor$, which is roughly $\sqrt{\frac{n}{32}}$.

Error-correction

q	inscribed bundle	circumscribed bundle	self-polar bundle
5	53.5%	53.5%	53.5%
7	4.2 %	3.9%	3.9%
9	75.9%	75.4%	76.0%
11	43.8%	42.8%	42.1%
13	91.9%	91.3%	90.5%
17	96.0%	96.6%	96.0%
19	91.5%	91.6%	91.3%
23	97.4%	98.0%	97.8%
25	98.9%	98.9%	100%

Table 2: Probability to decode a received word of $\lfloor \frac{q+1}{4} \rfloor + 1$ errors correctly after one round of the bit-flipping decoding algorithm.

Error-correction

q	inscribed bundle	circumscribed bundle	self-polar bundle
5	2.9%	2.9%	2.9%
9	6.1%	5.0%	5.9%
11	4.3%	4.8%	4.8%
13	16.9%	17.5%	17.0%
17	59.4%	58.6%	57.7%
19	45.1%	45.6%	46.6%
23	78.0%	80.1%	77.7%
25	95.8%	95.0%	94.5%

Table 3: Probability to decode a received word of $\lfloor \frac{q+1}{4} \rfloor + 2$ errors correctly after one round of the bit-flipping decoding algorithm.

Thank you for your attention!

Questions?

Algebraic Classification

Example

q	perfect difference set D
2	$\{0, 1, 3\}$
3	$\{0, 1, 3, 9\}$
5	$\{0, 1, 3, 8, 12, 18\}$
7	$\{0, 1, 3, 13, 32, 36, 43, 52\}$
9	$\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\}$

Table 4: Perfect difference sets for some initial values of q.

Minimum Distance

It is rather difficult to compute the minimum distance of $C_2(\Pi \sqcup \Gamma)^{\perp}$.

Estimation:

- Let $S = \{l_1, ..., l_r, c_1, ..., c_s\}$ be an arbitrary but minimal set of linearly dependent columns of H, where l_i are some columns corresponding to lines and c_i some corresponding non-degenerate conics of $PG(2, q)$, then:
  $(\bigcup_{i=1}^{r} l_i) \cup (\bigcup_{i=1}^{s} c_i) = \left(\bigcup_{i<j} l_i \cap l_j\right) \cup \left(\bigcup_{i<j} c_i \cap c_j\right) \cup \left(\bigcup_{i,j} l_i \cap c_j\right)$

Minimum Distance

It is rather difficult to compute the minimum distance of $C_2(\Pi \sqcup \Gamma)^\perp$.

Estimation:

- Let $S = \{l_1, ..., l_r, c_1, ..., c_s\}$ be an arbitrary but minimal set of linearly dependent columns of H, where l_i are some columns corresponding to lines and c_i some corresponding non-degenerate conics of $PG(2, q)$, then:
$$(\bigcup_{i=1}^{r} l_i) \cup (\bigcup_{i=1}^{s} c_i) = \left(\bigcup_{i<j} l_i \cap l_j\right) \cup \left(\bigcup_{i<j} c_i \cap c_j\right) \cup \left(\bigcup_{i,j} l_i \cap c_j\right)$$
- $\lceil \frac{2(q+2)}{3} \rceil \leq d(C_2(\Pi \sqcup \Gamma)^\perp)$.

References i

R. D. Baker, J. M. N. Brown, G. L. Ebert, J. C. Fisher, et al.
Projective bundles.
Bulletin of the Belgian Mathematical Society-Simon Stevin, 1(3):329–336, 1994.

R. Gallager.
Low-density parity-check codes.
IRE Transactions on information theory, 8(1):21–28, 1962.

D. G. Glynn.
Finite projective planes and related combinatorial systems.
PhD thesis, University of Adelaide Adelaide, 1978.

J. Singer.
A theorem in finite projective geometry and some applications to number theory.
Transactions of the American Mathematical Society, 43(3):377–385, 1938.

References ii

J.-P. Tillich.
The decoding failure probability of mdpc codes.
In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 941–945. IEEE, 2018.