A geometric interpretation of minimal codes

Gianira N. Alfarano
Joint work with M. Borello, A. Neri, A. Ravagnani

De Cifris, Schola Latina Seminars
17th May 2021

University of Zurich[UZH]

Overview

Contents

General Transmission in One Slide

- **Source**: the person/device which transmits something
- **Channel**: the *way* by which information is transmitted
- **Receiver**: the person/device which receives what the source sent

General Transmission in One Slide

- **Source**: the person/device which transmits something
- **Channel**: the *way* by which information is transmitted
- **Receiver**: the person/device which receives what the source sent

General Transmission in One Slide

- **Source**: the person/device which transmits something
- **Channel**: the *way* by which information is transmitted
- **Receiver**: the person/device which receives what the source sent

Safety is achieved by using **Error-Correcting Codes**

General Transmission in One Slide

- **Source**: the person/device which transmits something
- **Channel**: the *way* by which information is transmitted
- **Receiver**: the person/device which receives what the source sent

Safety is achieved by using **Error-Correcting Codes**

Contents

Linear codes

- $\mathbb{F}_q$ finite field of q elements, q prime power
- k, n positive integers, with $k \leq n$
- An injective map $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$, called **encoding map**

Definition

A linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$.

- n is the **length** of $\mathcal{C}$.
- k is the **dimension** of $\mathcal{C}$.

$\mathcal{C}$ is an $[n, k]_q$ code.

- The elements of $\mathcal{C}$ are called **codewords**.

Linear codes

- $\mathbb{F}_q$ finite field of q elements, q prime power
- k, n positive integers, with $k \leq n$
- An injective map $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$, called **encoding map**

Definition

A linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$.

- n is the **length** of $\mathcal{C}$.
- k is the **dimension** of $\mathcal{C}$.

$\mathcal{C}$ is an $[n, k]_q$ code.

- The elements of $\mathcal{C}$ are called **codewords**.

- The **Hamming distance** on $\mathbb{F}_q^n$:

$$\mathrm{d_H}(x, y) = |\{i \mid x_i \neq y_i\}|$$

Definition (Minimum distance of a code)

$$d := \mathrm{d_H}(\mathcal{C}) = \min\{\mathrm{d_H}(x, y) \mid x, y \in \mathcal{C}, x \neq y\}.$$

Linear codes

- $\mathbb{F}_q$ finite field of q elements, q prime power
- k, n positive integers, with $k \leq n$
- An injective map $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$, called **encoding map**

Definition

A linear code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$.

- n is the **length** of $\mathcal{C}$.
- k is the **dimension** of $\mathcal{C}$.

$\mathcal{C}$ is an $[n, k, d]_q$ code.

- The elements of $\mathcal{C}$ are called **codewords**.

- The **Hamming distance** on $\mathbb{F}_q^n$:

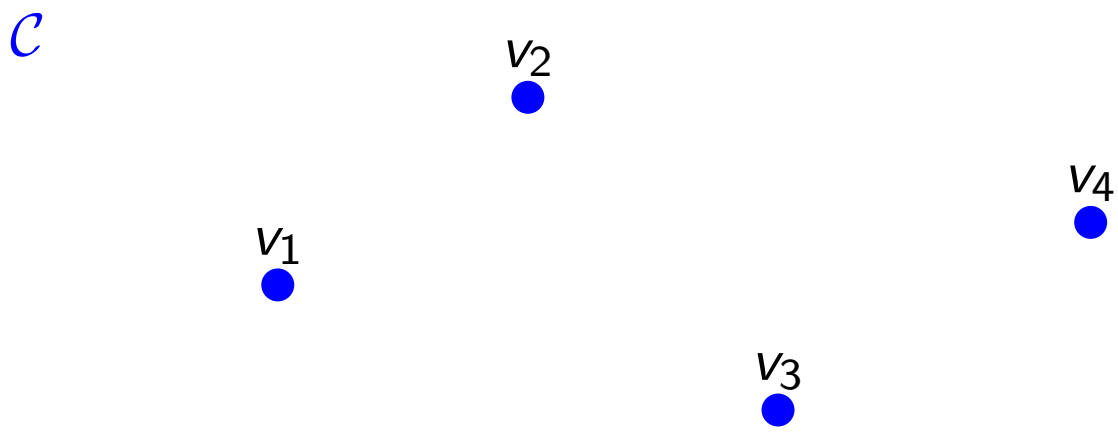
$$\mathrm{d_H}(x, y) = |\{i \mid x_i \neq y_i\}|$$

Definition (Minimum distance of a code)

$$d := \mathrm{d_H}(\mathcal{C}) = \min\{\mathrm{d_H}(x, y) \mid x, y \in \mathcal{C}, x \neq y\}.$$

Error Correction and Detection Capability

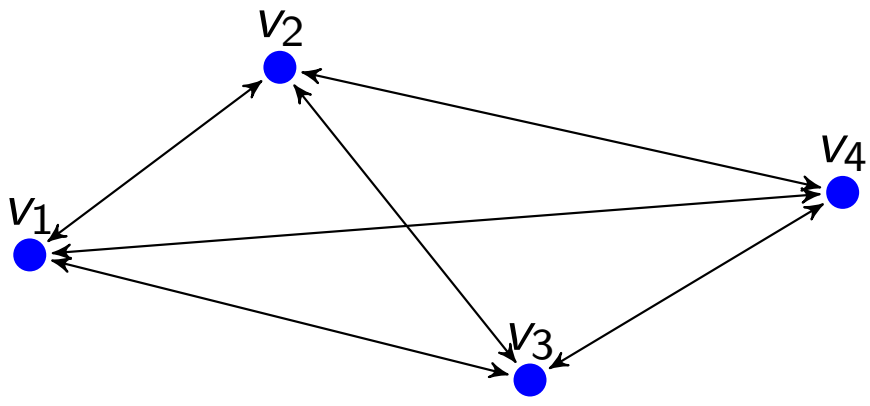
Given a code $\mathcal{C}$



Error Correction and Detection Capability

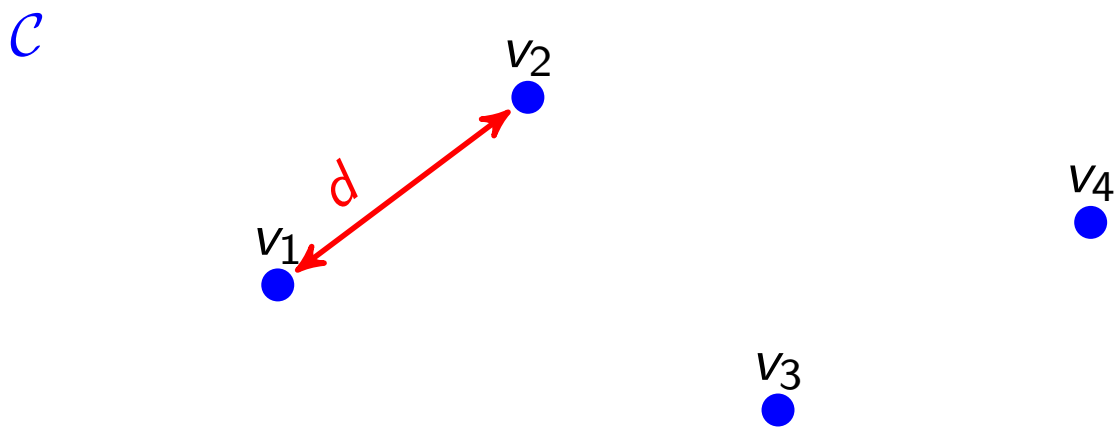
Given a code $\mathcal{C}$

$\mathcal{C}$



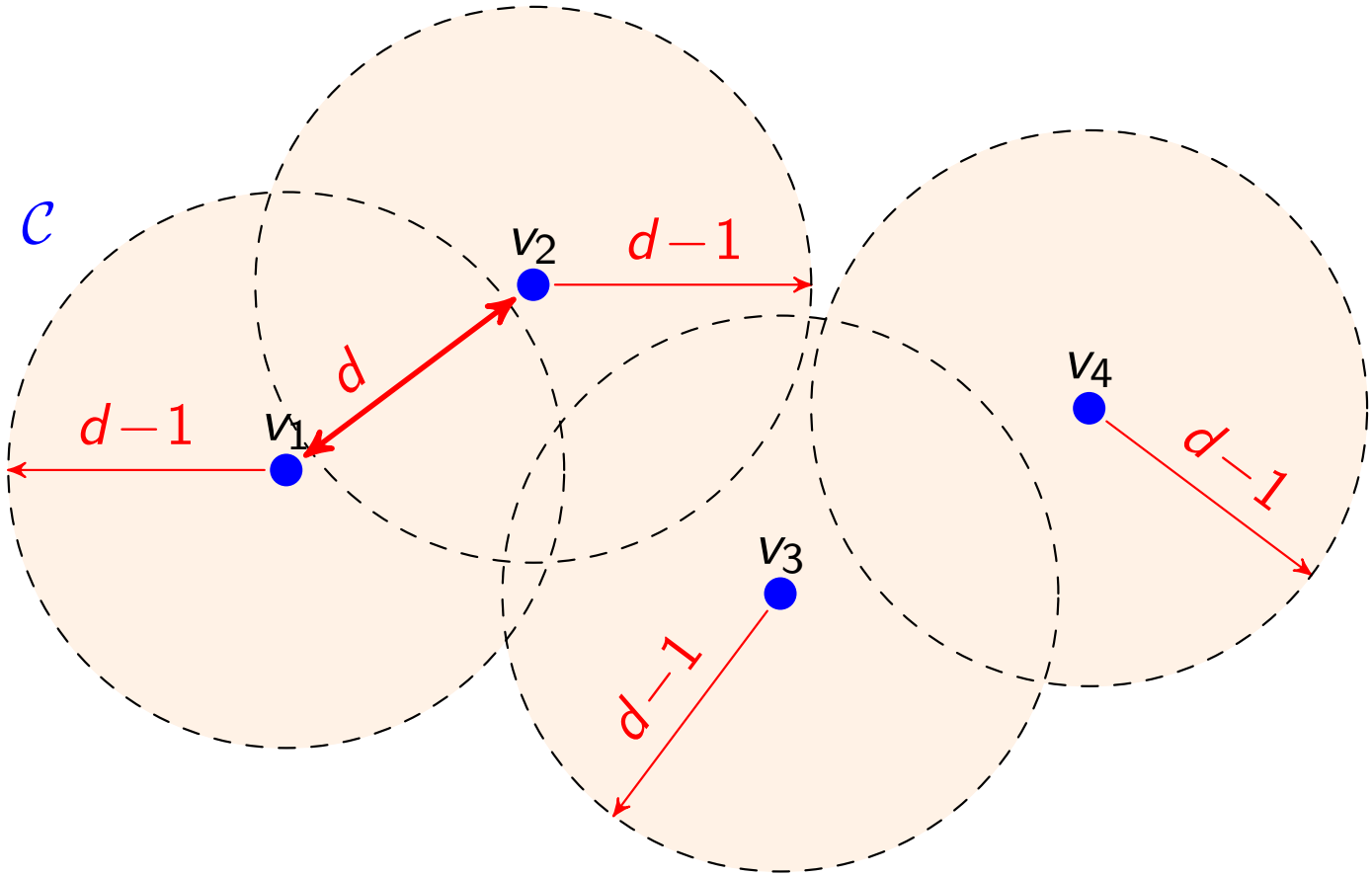
Error Correction and Detection Capability

Given a code $\mathcal{C}$ with distance $d = d(\mathcal{C})$



Error Correction and Detection Capability

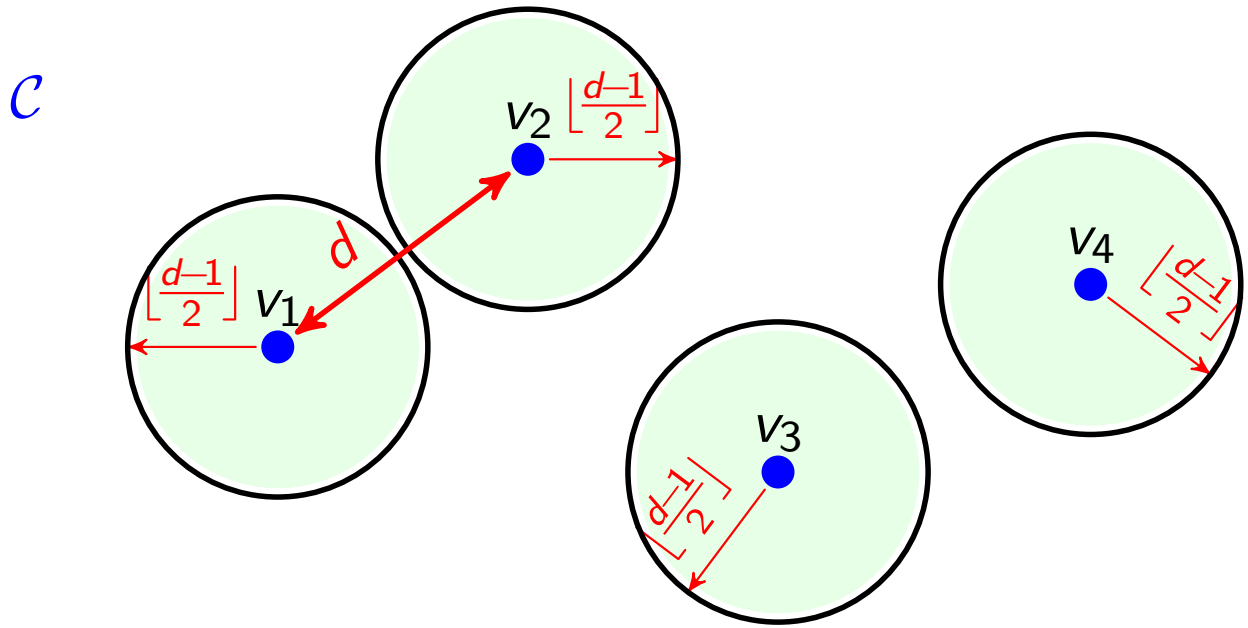
Given a code $\mathcal{C}$ with distance $d = d(\mathcal{C})$



- we can detect at most $d-1$ errors

Error Correction and Detection Capability

Given a code $\mathcal{C}$ with distance $d = d(\mathcal{C})$



- we can detect at most $d - 1$ errors
- and correct at most $\lfloor \frac{d-1}{2} \rfloor$ errors

Linear Codes

For any $v \in \mathbb{F}_q^n$,

- the **support** of v is $\mathrm{supp}(v) = \{i : v_i \neq 0\}$.
- the **Hamming weight** of v is $\mathrm{wt_H}(v) = |\mathrm{supp}(v)| = \mathrm{d_H}(v, 0)$.

Linear Codes

For any $v \in \mathbb{F}_q^n$,

- the **support** of v is $\mathrm{supp}(v) = \{i : v_i \neq 0\}$.
- the **Hamming weight** of v is $\mathrm{wt_H}(v) = |\mathrm{supp}(v)| = \mathrm{d_H}(v, 0)$.

Let $\mathcal{C}$ be an $[n, k, d]_q$ code.

- The minimum distance d is equal to the **minimum weight**

$$d = \min\{\mathrm{wt_H}(c) \mid c \in \mathcal{C} \setminus \{0\}\}.$$

Linear Codes

For any $v \in \mathbb{F}_q^n$,

- the **support** of v is $\mathrm{supp}(v) = \{i : v_i \neq 0\}$.
- the **Hamming weight** of v is $\mathrm{wt_H}(v) = |\mathrm{supp}(v)| = \mathrm{d_H}(v, 0)$.

Let $\mathcal{C}$ be an $[n, k, d]_q$ code.

- The minimum distance d is equal to the **minimum weight**

$$d = \min\{\mathrm{wt_H}(c) \mid c \in \mathcal{C} \setminus \{0\}\}.$$

- Singleton bound: $d \leq n - k + 1$.
- **MDS code**: $d = n - k + 1$

Generator and parity-check matrix

1. $\mathcal{C}$ possesses a **generator matrix** $G \in \mathbb{F}_q^{k \times n}$:

$$\mathcal{C} = \{vG \mid v \in \mathbb{F}_q^k\},$$

i.e. the rows of G form a **basis** of $\mathcal{C}$.

Generator and parity-check matrix

1. $\mathcal{C}$ possesses a **generator matrix** $G \in \mathbb{F}_q^{k \times n}$:

$$\mathcal{C} = \{vG \mid v \in \mathbb{F}_q^k\},$$

   i.e. the rows of G form a **basis** of $\mathcal{C}$.

2. $\mathcal{C}$ possesses a **parity-check matrix** $H \in \mathbb{F}_q^{(n-k) \times n}$:

$$\mathcal{C} = \{u \in \mathbb{F}_q^n \mid Hu^\top = 0\}.$$

Definition

Let $\mathcal{C}$ be a code and H a parity-check matrix for $\mathcal{C}$. The code generated by H is called **dual** code of $\mathcal{C}$ and it is denoted by $\mathcal{C}^\perp$.

Equivalence of codes

Definition

Let $\mathcal{G}$ be the group of automorphism of $\mathbb{F}_q^n$ generated by the permutations of coordinates and by the multiplication of any coordinate by a nonzero element of $\mathbb{F}_q$. Two linear codes $\mathcal{C}$ and $\mathcal{C}'$ are (monomially) **equivalent** of there is $\sigma \in \mathcal{G}$ such that $\mathcal{C}' = \sigma(\mathcal{C})$.

Equivalence of codes

Definition

Let $\mathcal{G}$ be the group of automorphism of $\mathbb{F}_q^n$ generated by the permutations of coordinates and by the multiplication of any coordinate by a nonzero element of $\mathbb{F}_q$. Two linear codes $\mathcal{C}$ and $\mathcal{C}'$ are (monomially) **equivalent** of there is $\sigma \in \mathcal{G}$ such that $\mathcal{C}' = \sigma(\mathcal{C})$.

Definition

An $[n, k, d]_q$ code $\mathcal{C}$ is **nondegenerate** if there is no $i \in \{1, \ldots, n\}$ with $c_i = 0$ for all $c \in \mathcal{C}$.

Contents

Projective Space

Let $\mathrm{PG}(k-1,q)$ be the **projective space** $(\mathbb{F}_q^k \setminus \{0\})/\sim$, where

$$u \sim v \iff \exists\, \lambda \in \mathbb{F}_q^* \text{ s.t. } u = \lambda v.$$

Projective Space

Let $\mathrm{PG}(k-1,q)$ be the **projective space** $(\mathbb{F}_q^k \setminus \{0\})/\sim$, where

$$u \sim v \iff \exists\, \lambda \in \mathbb{F}_q^* \text{ s.t. } u = \lambda v.$$

	$\mathbb{F}_q^k$	$\mathrm{PG}(k-1,q)$
	dim. 1	dim. 0 (*Points*)
	dim. 2	dim. 1 (*Lines*)
	$\vdots$	$\vdots$
	dim. $k-1$	dim. $k-2$ (*Hyperplanes*)

Examples

$\mathrm{PG}(1,3)$: the **projective line** over $\mathbb{F}_3$

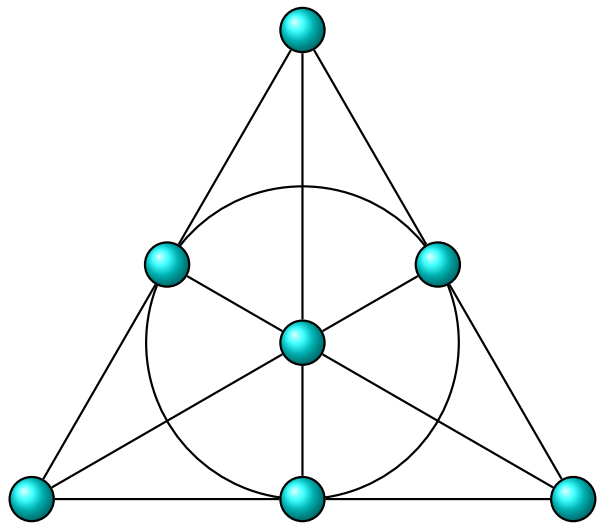
- Start with
  $\mathbb{F}_3^2 \setminus \{(0,0)\} = \{(1,0),(2,0),(0,1),(0,2),(1,1),(2,2),(1,2),(2,1)\}$.
- Identify multiples: $\mathrm{PG}(1,3) = \{(1:0),(0:1),(1:1),(1:2)\}$

In general

$$|\mathrm{PG}(k-1,q)| = \frac{q^k-1}{q-1}.$$

Examples

$\mathrm{PG}(2,2)$: the **Fano plane**



Generator matrix

- Let $G \in F_q^{k \times n}$ be a generator matrix of a linear code $\mathcal{C}$, then

$$\mathcal{C} = \{vG \mid v \in \mathbb{F}_q^k\}.$$

- The Hamming weight of a codeword vG is equal to the number of columns of G which are not orthogonal to v (with respect to the standard inner product).

Example

Let $\mathcal{C}$ be the $[6, 3]_2$ code generated by

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

The codeword $(1, 1, 1)G$ has weight 3 as the first 3 columns of G are not orthogonal to $(1, 1, 1)$ (indeed $(1, 1, 1)G = (1, 1, 1, 0, 0, 0)$).

Generator matrix

Let $\mathcal{M}$ denote the set of columns of G, i.e. $\mathcal{M}$ is a subset of $\mathbb{F}_q^k$

Remark

Let $\mathcal{B}$ be the standard basis of $\mathbb{F}_q^n$. We can write

$$\mathcal{M} = \{Gy^t : y \in \mathcal{B}\}$$

$$\Rightarrow \mathrm{wt}(vG) = n - |\mathcal{M} \cap v^{\perp}|,$$

where $v^{\perp} = \{u \in \mathbb{F}_q^k, u \cdot v = 0\}$

Example

Let $\mathcal{C}$ be the $[6,3]_2$ code of the previous example:
$\mathcal{M} := \{(1,0,0),(0,1,0),(0,0,1),(0,1,1),(1,0,1),(1,1,0)\}$
$\mathrm{wt}((1,1,0)G) = 6 - |\{(0,0,1),(1,0,1),(1,1,0)\}| = 3.$

Projective Systems

Let $\mathrm{PG}(k-1,q)$ be the projective space over $\mathbb{F}_q$ with $\mathbb{F}_q^k$ as underlying vector space.

Projective Systems

Let $\mathrm{PG}(k-1,q)$ be the projective space over $\mathbb{F}_q$ with $\mathbb{F}_q^k$ as underlying vector space.

Definition

A projective $(n,k,d)_q$ system is a finite multiset $\mathcal{P}$ of n points in $\mathrm{PG}(k-1,q)$ that does not lie in any (projective) hyperplane Π.

$$d = n - \max\{|\mathcal{P} \cap \Pi| : \Pi \subset \mathrm{PG}(k-1,q), \dim(\Pi) = k-2\}.$$

Projective Systems

Let $\mathrm{PG}(k-1,q)$ be the projective space over $\mathbb{F}_q$ with $\mathbb{F}_q^k$ as underlying vector space.

Definition

A projective $(n,k,d)_q$ system is a finite multiset $\mathcal{P}$ of n points in $\mathrm{PG}(k-1,q)$ that does not lie in any (projective) hyperplane Π.

$$d = n - \max\{|\mathcal{P} \cap \Pi| : \Pi \subset \mathrm{PG}(k-1,q), \dim(\Pi) = k-2\}.$$

Two projective $(n,k,d)_q$ systems $\mathcal{P}, \mathcal{P}'$ are called *equivalent* if there exists $\varphi \in \mathrm{PGL}(k,q)$ such that $\varphi(\mathcal{P}) = \mathcal{P}'$, which preserves multiplicities.

Projective Systems

Let $\mathrm{PG}(k-1,q)$ be the projective space over $\mathbb{F}_q$ with $\mathbb{F}_q^k$ as underlying vector space.

Definition

A projective $(n,k,d)_q$ system is a finite multiset $\mathcal{P}$ of n points in $\mathrm{PG}(k-1,q)$ that does not lie in any (projective) hyperplane Π.

$$d = n - \max\{|\mathcal{P} \cap \Pi| : \Pi \subset \mathrm{PG}(k-1,q), \dim(\Pi) = k-2\}.$$

Two projective $(n,k,d)_q$ systems $\mathcal{P}, \mathcal{P}'$ are called *equivalent* if there exists $\varphi \in \mathrm{PGL}(k,q)$ such that $\varphi(\mathcal{P}) = \mathcal{P}'$, which preserves multiplicities.

Transform metric properties of codes in geometric properties of projective systems.

Correspondence Codes-Projective Systems

Theorem

There is a one-to-one correspondence between the set of equivalence classes of nondegenerate $[n, k, d]_q$ codes and the set of equivalence classes of projective $(n, k, d)_q$ systems.

Explanation: Consider an $[n, k, d]_q$ code $\mathcal{C}$ with generator matrix $G = (g_{i,j})$.

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

Correspondence Codes-Projective Systems

Theorem

There is a one-to-one correspondence between the set of equivalence classes of nondegenerate $[n, k, d]_q$ codes and the set of equivalence classes of projective $(n, k, d)_q$ systems.

Explanation: Consider an $[n, k, d]_q$ code $\mathcal{C}$ with generator matrix $G = (g_{i,j})$. A basis for $\mathcal{C}$ is given by the rows of G.

$$\begin{array}{cc} \rightarrow & \\ \rightarrow & \\ & \\ \rightarrow & \end{array} \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

Correspondence Codes-Projective Systems

Theorem

There is a one-to-one correspondence between the set of equivalence classes of nondegenerate $[n, k, d]_q$ codes and the set of equivalence classes of projective $(n, k, d)_q$ systems.

Explanation: Consider an $[n, k]_q$ code $\mathcal{C}$ with generator matrix $G = (g_{i,j})$. A basis for $\mathcal{C}$ is given by the rows of G.

$$\begin{array}{cccc} \downarrow & \downarrow & & \downarrow \\ \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix} \end{array}$$

We can instead consider the set $\mathcal{P}$ given by the columns as projective points in $\mathrm{PG}(k-1, q)$.

Correspondence Codes-Projective Systems

Theorem

There is a one-to-one correspondence between the set of equivalence classes of nondegenerate $[n, k, d]_q$ codes and the set of equivalence classes of projective $(n, k, d)_q$ systems.

Explanation:

$$\begin{pmatrix} \downarrow & \downarrow & & \downarrow \\ g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

For any nonzero vector $u = (u_1, u_2, \ldots, u_k)$ in $\mathbb{F}_q^k$, the hyperplane

$$u_1x_1 + u_2x_2 + \cdots + u_kx_k = 0$$

contains $|\mathcal{P}| - w$ points of $\mathcal{P}$ if and only if the codeword uG has weight w.

Important Reference

M.A. Tsfasman and S.G. Vladut. "Algebraic-geometric codes", vol. 58 of Mathematics and its Applications (Soviet Series). Kluwer Academic Publishers Group, 1991.

Contents

Minimal codewords and minimal codes

Definition

Let $\mathcal{C}$ be an $[n, k]_q$ code. A codeword $c \in \mathcal{C}$ is **minimal** if for every $c' \in C$

$$\mathrm{supp}(c') \subseteq \mathrm{supp}(c) \Longleftrightarrow c' = \lambda c$$

for some $\lambda \in \mathbb{F}_q$.

Definition

A linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is **minimal** if all its codewords are minimal.

Why are minimal codes interesting?

- Minimal codewords were first studied by Massey ('93). He proposed an application to Secret Sharing Schemes:
- Supports of minimal codewords of the dual of a code were used to define an access structure to a secret.

Why are minimal codes interesting?

- Minimal codewords were first studied by Massey ('93). He proposed an application to Secret Sharing Schemes:
- Supports of minimal codewords of the dual of a code were used to define an access structure to a secret.
- Finding minimal codewords of a given code is in general a difficult task.
- Designing codes whose codewords are all minimal could be easier.

Why are minimal codes interesting?

- Minimal codewords were first studied by Massey ('93). He proposed an application to Secret Sharing Schemes:
- Supports of minimal codewords of the dual of a code were used to define an access structure to a secret.
- Finding minimal codewords of a given code is in general a difficult task.
- Designing codes whose codewords are all minimal could be easier.
- Really interesting from a combinatorial point of view
- Supports of the nonzero codewords form an antichain with respect to "$\subseteq$"
- They have strong geometric properties.

Threshold Secret Sharing Scheme

Definition

Let k and n be positive integers, $k \leq n$. A (k, n)-**threshold scheme** is a method of sharing a secret s among a set of n participants in such a way that any k participants can compute the value of the secret, but no group of $k - 1$ (or fewer) can do so.

Threshold Secret Sharing Scheme

Definition

Let k and n be positive integers, $k \leq n$. A (k, n)-**threshold scheme** is a method of sharing a secret s among a set of n participants in such a way that any k participants can compute the value of the secret, but no group of $k-1$ (or fewer) can do so.

In a more general situation, we would like to specify exactly which subsets are qualified to recover the secret.

Access Structure

Definition

- The subsets of participants which is qualified to recover the secret are called qualified subsets or **authorized subsets**.
- The collection Γ of all the authorized subsets is called an **access structure**.

Access Structure

Definition

- The subsets of participants which is qualified to recover the secret are called qualified subsets or **authorized subsets**.
- The collection Γ of all the authorized subsets is called an **access structure**.

The subsets in Γ specify those subset of participants that are qualified to compute the secret. If $\mathcal{B} \subseteq P$, then we denote by B the set of shares for the participants in subset $\mathcal{B}$.

Access Structure

Definition

- The subsets of participants which is qualified to recover the secret are called qualified subsets or **authorized subsets**.
- The collection Γ of all the authorized subsets is called an **access structure**.

The subsets in Γ specify those subset of participants that are qualified to compute the secret. If $\mathcal{B} \subseteq P$, then we denote by B the set of shares for the participants in subset $\mathcal{B}$.

Definition

A (k, n)-threshold scheme has access structure $\Gamma = \{\mathcal{B} \subseteq P : |B| \geq k\}$.

Massey's Construction Secret Sharing Scheme

Let $G = (g_0, \ldots, g_{n-1})$ be the generator matrix of an $[n, k, d]_q$-code $\mathcal{C}$.

In the secret sharing scheme based on $\mathcal{C}$, the secret is an element of $\mathbb{F}_q$, which is called the **secret space**, and $n-1$ participants $\{P_1, \ldots, P_{n-1}\}$ and a dealer D are involved. The dealer is a trusted person.

Massey's Construction Secret Sharing Scheme

Let $G = (g_0, \ldots, g_{n-1})$ be the generator matrix of an $[n, k, d]_q$-code $\mathcal{C}$.

In the secret sharing scheme based on $\mathcal{C}$, the secret is an element of $\mathbb{F}_q$, which is called the **secret space**, and $n-1$ participants $\{P_1, \ldots, P_{n-1}\}$ and a dealer D are involved. The dealer is a trusted person.

In order to compute the shares with respect to a secret , the dealer chooses randomly a vector $u = (u_0, \ldots, u_{k-1}) \in \mathbb{F}_q^k$ such that $s = u \cdot g_0$.

Remark

There are $q^k - 1$ vectors in $\mathbb{F}_q^k$ of this form.

Massey's Construction Secret Sharing Scheme

The dealer then treats u as an information vector and computes the corresponding codeword

$$t = (t_0, \ldots, t_{n-1}) = uG$$

and gives t_i to the participant P_i, for $i \in \{1, \ldots, n-1\}$.

Since $t_0 = ug_0 = s$ then $P_{i_1}, \ldots, P_{i_m}$ can recover s if and only if g_0 is a linear combination of $g_{i_1}, \ldots g_{i_m}$.

To find the minimal access sets of the secret sharing scheme based on $\mathcal{C}$, it is sufficient to find the minimal codewords of $\mathcal{C}^{\perp}$ whose first coordinate is 1.

Remark

The access structure of the SSS corresponding to C is specified by the support of minimal codewords in $C^{\perp}$ having 1 as the first component.

Secret sharing scheme

Assume we want to "split" an m-bit secret into m-bit shares for four users A, B, C, D in such a way that $\Gamma = \{\{A, B\}, \{B, C, D\}\}$, but no coalition of users not containing one of these two authorized coalitions as a subset can obtain any information about the secret, for example $\{A, C\}$.

Secret sharing scheme

Assume we want to "split" an m-bit secret into m-bit shares for four users A, B, C, D in such a way that $\Gamma = \{\{A, B\}, \{B, C, D\}\}$, but no coalition of users not containing one of these two authorized coalitions as a subset can obtain any information about the secret, for example $\{A, C\}$.

- Choose $\mathcal{C}$ to be a $[5, 3]_{2^m}$ code, with parity check

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

- Choose the secret to be the first digit of a codeword and give the digits in positions $2, 3, 4$ and 5 to A, B, C, D.
- If $v = (v_1, .., v_5)$ is a the chosen codeword, $Hv^t = 0$, hence $v_1 + v_2 + v_3 = 0$ and $v_2 + v_4 + v_5 = 0$.

Secret sharing scheme

$\Gamma(\mathcal{C})$ is specified by those minimal codewords in the dual code $\mathcal{C}^{\perp}$ whose first component is a 1 in the manner that the set of shares specified by each such minimal codeword in the dual code is the set of shares corresponding to those locations after the first where this minimal codeword is non-zero.

- There are only two minimal codewords in the code $\mathcal{C}^{\perp}$ with 1 as first coordinates:

$$v_1 = (1, 1, 1, 0, 0), \qquad v_2 = (1, 0, 1, 1, 1).$$

- $\Gamma = \{\{v_2, v_3\}, \{v_3, v_4, v_5\}\}$.

First examples of minimal codes

- Any $[n, 1]_q$ code is trivially minimal

First examples of minimal codes

- Any $[n, 1]_q$ code is trivially minimal

- For every $k \in \mathbb{N}$, the $[(q^k - 1)/(q - 1), k]_q$ **simplex code** (dual of the q-ary Hamming code) is minimal.

  Are there shorter codes?

First examples of minimal codes

- Any $[n, 1]_q$ code is trivially minimal

- For every $k \in \mathbb{N}$, the $[(q^k - 1)/(q - 1), k]_q$ **simplex code** (dual of the q-ary Hamming code) is minimal.

  Are there shorter codes?

  Yes!

Asymptotic performance

Definition (Asymptotically good codes)

A family of codes is said **asymptotically good** if it contains a sequence $C = (\mathcal{C}_1, \mathcal{C}_2, \dots)$ of linear codes, where C_n is an $[n, k_n, d_n]_q$ code such that the rate $R = k_n/n$ and the relative distance $\delta = d_n/n$ of C_n, that is

$$R := \liminf_{n\to\infty} \frac{k_n}{n} \qquad \text{and} \qquad \delta := \liminf_{n\to\infty} \frac{d_n}{n},$$

are both positive.

First bounds

Theorem (Minimal Bound)

For any rate $R = k/n$ such that

$$0 \leq R \leq \frac{1}{2} \log_q \left(\frac{q^2}{q^2 - q + 1} \right),$$

there exists an infinite sequence of $[n, k]_q$ minimal codes.

H. Chabanne, G. Cohen and A. Patey, "Towards secure two-party computation from the wire-tap channel", International Conference on Information Security and Cryptology, 2013.

Theorem

Let $\mathcal{C}$ be an $[n, k, d]_q$ minimal code with $k \geq 2$. Then $d \geq k + q - 2$.

G.N. Alfarano, M. Borello and A. Neri, "A geometric characterization of minimal codes and their asymptotic performance", Advances in Mathematics of Communications, 2019.

G. Cohen, S. Mesnager and A. Patey, "On minimal and quasi-minimal linear codes", IMA International Conference on Cryptography and Coding, 2013.

Asymptotic performances of minimal codes

Theorem

Minimal codes are asymptotically good.

Remark

In this case, the problem reduces to finding, for a fixed q, an infinite family of minimal codes over $\mathbb{F}_q$ whose length is linear in k.

G.N. Alfarano, M. Borello and A. Neri "A geometric characterization of minimal codes and their asymptotic performance", Advances in Mathematics of Communications, 2019.

Geometry of minimal codes

What about the geometric point of view for minimal codes?

Theorem [A., Borello, Neri ('20)]

$$\{\text{Equivalence classes of } [n,k,d]_q \text{ minimal codes}\}$$

$$\updownarrow$$

$$\{\text{Equivalence classes of } \textbf{cutting blocking sets} \text{ in } \mathrm{PG}(k-1,q)\}$$

Cutting blocking sets

Definition

Let $k \in \mathbb{N}$. A set $\mathcal{P}$ in $\mathrm{PG}(k-1,q)$ is called **cutting blocking set** if for every hyperplane Λ in $\mathrm{PG}(k-1,q)$

$$\langle \mathcal{P} \cap \Lambda \rangle = \Lambda.$$

Cutting blocking sets

Definition

Let $k \in \mathbb{N}$. A set $\mathcal{P}$ in $\mathrm{PG}(k-1,q)$ is called **cutting blocking set** if for every hyperplane Λ in $\mathrm{PG}(k-1,q)$

$$\langle \mathcal{P} \cap \Lambda \rangle = \Lambda.$$

- First introduced by Davydov, Giulietti, Marcugini, Pambianco ('11) under the name of **strong blocking sets**.
- Used in coding theory for constructing **covering codes**.
- Héger, Patkós and Takáts used them under the name of **hyperplane generating sets** for constructing (semi)resolving sets.
- Studied by Fancsali and Sziklai ('14) for geometric purposes who called them **generating sets**.
- Reintroduced by Bonini and Borello ('20) for constructing special families of minimal codes.

Bounds

Definition

A t-**fold blocking set** in $\mathrm{PG}(k-1,q)$ is a set of points $\mathcal{P}$ such that for every hyperplane $\Lambda \subseteq \mathrm{PG}(k-1,q)$, it holds:

$$|\Lambda \cap \mathcal{P}| \geq t.$$

Bounds

Definition

A t-**fold blocking set** in $\mathrm{PG}(k-1,q)$ is a set of points $\mathcal{P}$ such that for every hyperplane $\Lambda \subseteq \mathrm{PG}(k-1,q)$, it holds:

$$|\Lambda \cap \mathcal{P}| \geq t.$$

Remark

Cutting blocking sets in $\mathrm{PG}(k-1,q)$ are in particular $(k-1)$-fold blocking sets.

Bounds

Definition

A t-**fold blocking set** in $\mathrm{PG}(k-1,q)$ is a set of points $\mathcal{P}$ such that for every hyperplane $\Lambda \subseteq \mathrm{PG}(k-1,q)$, it holds:

$$|\Lambda \cap \mathcal{P}| \geq t.$$

Remark

Cutting blocking sets in $\mathrm{PG}(k-1,q)$ are in particular $(k-1)$-fold blocking sets.

Theorem (Beutelspacher, '83)

Let $4 \leq k \leq \sqrt{q}+2$ and let $\mathcal{P}$ be a $(k-1)$-fold blocking set in $\mathrm{PG}(k-1,q)$. Then $|\mathcal{P}| \geq (q+1)(k-1)$.

A. Beutelspacher, "On Baer subspaces of finite projective spaces", Mathematische Zeitschrift, 1983.

Bounds

Using algebraic arguments, we proved the following results:

Theorem

Let $\mathcal{C}$ be an $[n, k, d]_q$ minimal code. Then

$$n \geq (q+1)(k-1).$$

Bounds

Using algebraic arguments, we proved the following results:

Theorem

Let $\mathcal{C}$ be an $[n, k, d]_q$ minimal code. Then

$$n \geq (q+1)(k-1).$$

Theorem

Let $\mathcal{C}$ be an $[n, k, d]_q$ minimal code. Then

$$d \geq (q-1)(k-1)+1.$$

G.N. Alfarano, M. Borello, A. Neri, A. Ravagnani. "Three combinatorial perspectives on minimal codes", submitted, 2021.

Bounds

Using algebraic arguments, we proved the following results:

Theorem

Let $\mathcal{C}$ be an $[n, k, d]_q$ minimal code. Then

$$n \geq (q+1)(k-1).$$

Theorem

Let $\mathcal{C}$ be an $[n, k, d]_q$ minimal code. Then

$$d \geq (q-1)(k-1)+1.$$

G.N. Alfarano, M. Borello, A. Neri, A. Ravagnani. "Three combinatorial perspectives on minimal codes", submitted, 2021.

Using geometric arguments the same bounds have been shown two weeks ago.

T. Héger, and Z. L. Nagy. "Short minimal codes and covering codes via strong blocking sets in projective spaces", March 2021.

Contents

Rational normal tangent set

Choose $2k-3$ points on the rational normal curve in $\mathrm{PG}(k-1,q)$. The union of the tangent lines in those points is a cutting blocking set, **provided that** $\mathrm{char}(\mathbb{F}_q) \geq k$, $q \geq 2k-3$.

This construction provides a $[(2k-3)(q+1), k]_q$ minimal code.

S. Fancsali, P. Sziklai. "Lines in higgledy-piggledy arrangement", The electronic journal of combinatorics **21**, 2014.

Coding theory remarks

In coding theory it is not enough to have construction of codes for q big.

- Explicitly constructing asymptotically good minimal codes, that are proved to exist.
- Technically, we fix q and send k to infinity together with the code length.

Coding theory remarks

In coding theory it is not enough to have construction of codes for q big.

- Explicitly constructing asymptotically good minimal codes, that are proved to exist.
- Technically, we fix q and send k to infinity together with the code length.
- Problem: find, for a fixed q, an infinite family of minimal codes over $\mathbb{F}_q$ whose length is linear in k.
- Geometrically: Find cutting blocking sets whose cardinality grows linearly in k.

Coding theory remarks

In coding theory it is not enough to have construction of codes for q big.

- Explicitly constructing asymptotically good minimal codes, that are proved to exist.
- Technically, we fix q and send k to infinity together with the code length.
- Problem: find, for a fixed q, an infinite family of minimal codes over $\mathbb{F}_q$ whose length is linear in k.
- Geometrically: Find cutting blocking sets whose cardinality grows linearly in k.
- The previous construction does not address this problem

Tetrahedron

Let $P_1, \ldots, P_k$ be points in $\mathrm{PG}(k-1, q)$ in general position. Consider $\ell_{i,j} = \langle P_i, P_j \rangle$.
Then, the set

$$\mathcal{P} = \cup_{i,j} \ell_{i,j}$$

is a cutting blocking set.

This construction provides a $\left[(q-1)\binom{k}{2} + k, k\right]_q$ minimal code.

G.N. Alfarano, M. Borello, A. Neri. "A geometric characterization of minimal codes and their asymptotic performance", Advances in Mathematics of Communications, 2020.

D. Bartoli, M. Bonini, and B. Gunes. "An inductive construction of minimal codes", Cryptography and Communications, 2021

W. Lu, X. Wu, X. Cao. "The parameters of minimal linear codes", Finite Fields and Their Applications, 2021.

A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco, "Linear nonbinary covering codes and saturating sets in projective spaces", Advances in Mathematics of Communications, 2011.

Construction from spreads

Definition

A line-spread in $\mathrm{PG}(k-1,q)$ is a partition of $\mathrm{PG}(k-1,q)$ in lines (i.e. 1-dimensional projective subspaces).

Every line-spread can be constructed with the field reduction map which sends points of $\mathrm{PG}(t-1,q^2)$ in lines of $\mathrm{PG}(2t-1,q)$.
Let $\gamma \in \mathbb{F}_{q^2}$ be a primitive element and let $M \in \mathbb{F}_q^{2\times 2}$ be the companion matrix of its minimal polynomial over $\mathbb{F}_q$.

$$\mathbb{F}_{q^2} \overset{\phi}{\cong} \mathbb{F}_q[M] = \{0\} \cup \{M^i \mid 1 \leq i \leq q^2-1\}.$$

To a point $P := [u_1 : \cdots : u_t] \in \mathrm{PG}(t-1,q^2)$, we associate the line

$$\{[x\phi(u_1) : \cdots : x\phi(u_t)] \mid x \in \mathrm{PG}(1,q)\}.$$

Construction from spreads

Theorem

Assume $k = 2t$. Let S be a line-spread of $\mathrm{PG}(k-1, q)$. One can choose $\frac{k^2}{4}$ lines from S so that their union is a cutting blocking set.

It is not only an existence, but the proof is **constructive**:
For example: field reduction applied to the $\frac{k^2}{4}$ points given by

$$\{[e_i] \mid 1 \leq i \leq t\} \cup \{[e_i + e_j] \mid 1 \leq i < j \leq t\} \cup \{[e_i + \gamma e_j] \mid 1 \leq i < j \leq t\}.$$

This construction provides a $\left[\frac{k^2}{4}(q+1), k\right]_q$ minimal code.

Summarizing

- Minimal codes are in one-to-one correspondence with cutting blocking sets

Summarizing

- Minimal codes are in one-to-one correspondence with cutting blocking sets
- We aim to construct cutting blocking sets whose size grows linearly with k;

Summarizing

- Minimal codes are in one-to-one correspondence with cutting blocking sets
- We aim to construct cutting blocking sets whose size grows linearly with k;
- We provided a construction of cutting blocking sets using spreads;

Summarizing

- Minimal codes are in one-to-one correspondence with cutting blocking sets
- We aim to construct cutting blocking sets whose size grows linearly with k;
- We provided a construction of cutting blocking sets using spreads;
- This construction produces a short minimal code, for infinitely many dimensions and field sizes;

Summarizing

- Minimal codes are in one-to-one correspondence with cutting blocking sets
- We aim to construct cutting blocking sets whose size grows linearly with k;
- We provided a construction of cutting blocking sets using spreads;
- This construction produces a short minimal code, for infinitely many dimensions and field sizes;
- It works for all those pairs (k, q) for which the construction with the tangent lines to the rational normal curve cannot be used.

Thank you!