On Linear Codes with Random Multiplier Vectors and the Maximum Trace Dimension Property

Márton Erdélyi, Pál Hegedüs, Sándor Z. Kiss and Gábor P. Nagy

Budapest University of Technology and Economics (Hungary)
University of Szeged (Hungary)

Combinatorics Seminar Szeged
February 16, 2024

Outline

1. Subfield subcodes and trace codes
2. Random codes in McEliece cryptosystems
3. The Maximum Trace Dimension property

Outline

1. Subfield subcodes and trace codes
2. Random codes in McEliece cryptosystems
3. The Maximum Trace Dimension property

Threshold decoding of linear codes

- A linear code C is a linear subspace of $\mathbb{F}_q^n$.
- Length, dimension, generator matrix, parity-check matrix.
- Hamming weight, Hamming distance.

Threshold Decoding Problem

Given linear code $C \leq \mathbb{F}_q^n$, vector $\boldsymbol{y} \in \mathbb{F}_q^n$, and integer t. Find a decomposition

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

such that $\boldsymbol{x} \in C$, $\boldsymbol{e} \in \mathbb{F}_q^n$, and $\mathrm{wt}(\boldsymbol{e}) \leq t$.

- Minimum distance, $d \geq 2t + 1$.
- Singleton bound $n + 1 \geq d + k$, Singleton defect, MDS codes.

Theorem (Berlekamp, McEliece, van Tilborg 1978)

The binary threshold decoding problem is NP-compete.

Threshold decoding of linear codes

- A linear code C is a linear subspace of $\mathbb{F}_q^n$.
- Length, dimension, generator matrix, parity-check matrix.
- Hamming weight, Hamming distance.

Threshold Decoding Problem

Given linear code $C \leq \mathbb{F}_q^n$, vector $\boldsymbol{y} \in \mathbb{F}_q^n$, and integer t. Find a decomposition

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

such that $\boldsymbol{x} \in C$, $\boldsymbol{e} \in \mathbb{F}_q^n$, and $\mathrm{wt}(\boldsymbol{e}) \leq t$.

- Minimum distance, $d \geq 2t + 1$.
- Singleton bound $n + 1 \geq d + k$, Singleton defect, MDS codes.

Theorem (Berlekamp, McEliece, van Tilborg 1978)

The binary threshold decoding problem is NP-compete.

Threshold decoding of linear codes

- A linear code C is a linear subspace of $\mathbb{F}_q^n$.
- Length, dimension, generator matrix, parity-check matrix.
- Hamming weight, Hamming distance.

Threshold Decoding Problem

Given linear code $C \leq \mathbb{F}_q^n$, vector $\boldsymbol{y} \in \mathbb{F}_q^n$, and integer t. Find a decomposition

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

such that $\boldsymbol{x} \in C$, $\boldsymbol{e} \in \mathbb{F}_q^n$, and $\mathrm{wt}(\boldsymbol{e}) \leq t$.

- Minimum distance, $d \geq 2t + 1$.
- Singleton bound $n + 1 \geq d + k$, Singleton defect, MDS codes.

Theorem (Berlekamp, McEliece, van Tilborg 1978)

The binary threshold decoding problem is NP-compete.

Threshold decoding of linear codes

- A linear code C is a linear subspace of $\mathbb{F}_q^n$.
- Length, dimension, generator matrix, parity-check matrix.
- Hamming weight, Hamming distance.

Threshold Decoding Problem

Given linear code $C \leq \mathbb{F}_q^n$, vector $\boldsymbol{y} \in \mathbb{F}_q^n$, and integer t. Find a decomposition

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

such that $\boldsymbol{x} \in C$, $\boldsymbol{e} \in \mathbb{F}_q^n$, and $\mathrm{wt}(\boldsymbol{e}) \leq t$.

- Minimum distance, $d \geq 2t + 1$.
- Singleton bound $n + 1 \geq d + k$, Singleton defect, MDS codes.

Theorem (Berlekamp, McEliece, van Tilborg 1978)

The binary threshold decoding problem is NP-compete.

Threshold decoding of linear codes

- A linear code C is a linear subspace of $\mathbb{F}_q^n$.
- Length, dimension, generator matrix, parity-check matrix.
- Hamming weight, Hamming distance.

Threshold Decoding Problem

Given linear code $C \leq \mathbb{F}_q^n$, vector $\boldsymbol{y} \in \mathbb{F}_q^n$, and integer t. Find a decomposition

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

such that $\boldsymbol{x} \in C$, $\boldsymbol{e} \in \mathbb{F}_q^n$, and $\mathrm{wt}(\boldsymbol{e}) \leq t$.

- Minimum distance, $d \geq 2t + 1$.
- Singleton bound $n + 1 \geq d + k$, Singleton defect, MDS codes.

Theorem (Berlekamp, McEliece, van Tilborg 1978)

The binary threshold decoding problem is NP-compete.

Threshold decoding of linear codes

- A linear code C is a linear subspace of $\mathbb{F}_q^n$.
- Length, dimension, generator matrix, parity-check matrix.
- Hamming weight, Hamming distance.

Threshold Decoding Problem

Given linear code $C \leq \mathbb{F}_q^n$, vector $\boldsymbol{y} \in \mathbb{F}_q^n$, and integer t. Find a decomposition

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

such that $\boldsymbol{x} \in C$, $\boldsymbol{e} \in \mathbb{F}_q^n$, and $\mathrm{wt}(\boldsymbol{e}) \leq t$.

- Minimum distance, $d \geq 2t + 1$.
- Singleton bound $n + 1 \geq d + k$, Singleton defect, MDS codes.

Theorem (Berlekamp, McEliece, van Tilborg 1978)

The binary threshold decoding problem is NP-compete.

Threshold decoding of linear codes

- A linear code C is a linear subspace of $\mathbb{F}_q^n$.
- Length, dimension, generator matrix, parity-check matrix.
- Hamming weight, Hamming distance.

Threshold Decoding Problem

Given linear code $C \leq \mathbb{F}_q^n$, vector $\boldsymbol{y} \in \mathbb{F}_q^n$, and integer t. Find a decomposition

$$\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$$

such that $\boldsymbol{x} \in C$, $\boldsymbol{e} \in \mathbb{F}_q^n$, and $\mathrm{wt}(\boldsymbol{e}) \leq t$.

- Minimum distance, $d \geq 2t + 1$.
- Singleton bound $n + 1 \geq d + k$, Singleton defect, MDS codes.

Theorem (Berlekamp, McEliece, van Tilborg 1978)

The binary threshold decoding problem is NP-compete.

Generalized Reed-Solomon codes

Definition: RS and GRS codes

- Let q be a prime power, and $0 \leq k \leq n \leq q$ integers,
- Let $\alpha_1, \ldots, \alpha_n$ be **distinct** elements of $\mathbb{F}_q$, and $v_1, \ldots, v_n$ be **nonzero** elements of $\mathbb{F}_q$.
- Write $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\boldsymbol{v} = (v_1, \ldots, v_n)$.

We define the following linear codes over $\mathbb{F}_q$:

$$\mathbf{RS}_k(\boldsymbol{\alpha}) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid \deg(f) < k\}$$

$$\mathbf{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \mid \deg(f) < k\}$$

- $d = n + 1 - k$, GRS codes are MDS.
- Efficient **threshold decoding algorithms** with $t = \lfloor \frac{n-k}{2} \rfloor$.

Generalized Reed-Solomon codes

Definition: RS and GRS codes

- Let q be a prime power, and $0 \le k \le n \le q$ integers,
- Let $\alpha_1, \ldots, \alpha_n$ be **distinct** elements of $\mathbb{F}_q$, and $v_1, \ldots, v_n$ be **nonzero** elements of $\mathbb{F}_q$.
- Write $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\boldsymbol{v} = (v_1, \ldots, v_n)$.

We define the following linear codes over $\mathbb{F}_q$:

$$\mathbf{RS}_k(\boldsymbol{\alpha}) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid \deg(f) < k\}$$
$$\mathbf{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \mid \deg(f) < k\}$$

- $d = n + 1 - k$, GRS codes are MDS.
- Efficient **threshold decoding algorithms** with $t = \lfloor \frac{n-k}{2} \rfloor$.

Generalized Reed-Solomon codes

Definition: RS and GRS codes

- Let q be a prime power, and $0 \leq k \leq n \leq q$ integers,
- Let $\alpha_1, \ldots, \alpha_n$ be **distinct** elements of $\mathbb{F}_q$, and $v_1, \ldots, v_n$ be **nonzero** elements of $\mathbb{F}_q$.
- Write $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\boldsymbol{v} = (v_1, \ldots, v_n)$.

We define the following linear codes over $\mathbb{F}_q$:

$$\mathbf{RS}_k(\boldsymbol{\alpha}) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid \deg(f) < k\}$$

$$\mathbf{GRS}_k(\boldsymbol{\alpha}, \boldsymbol{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \mid \deg(f) < k\}$$

- $d = n + 1 - k$, GRS codes are MDS.
- Efficient **threshold decoding algorithms** with $t = \lfloor \frac{n-k}{2} \rfloor$.

Generalized Reed-Solomon codes

Definition: RS and GRS codes

- Let q be a prime power, and $0 \leq k \leq n \leq q$ integers,
- Let $\alpha_1, \ldots, \alpha_n$ be **distinct** elements of $\mathbb{F}_q$, and $v_1, \ldots, v_n$ be **nonzero** elements of $\mathbb{F}_q$.
- Write $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\mathbf{v} = (v_1, \ldots, v_n)$.

We define the following linear codes over $\mathbb{F}_q$:

$$\mathbf{RS}_k(\boldsymbol{\alpha}) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid \deg(f) < k\}$$

$$\mathbf{GRS}_k(\boldsymbol{\alpha}, \mathbf{v}) = \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \mid \deg(f) < k\}$$

- $d = n + 1 - k$, GRS codes are MDS.
- Efficient **threshold decoding algorithms** with $t = \lfloor \frac{n-k}{2} \rfloor$.

Trace codes and subfield subcodes

- The **trace map** of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

- We define $\mathrm{Tr}(\boldsymbol{x})$ for vectors **entry-by-entry.**
- Let C be a q^m-ary $[n, k, d]$-code.

Definition

- The subfield subcode of C is

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n$$

- The trace code of C is

$$\mathrm{Tr}(C) = \{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{x}) \mid \boldsymbol{x} \in C\}.$$

Theorem (Delsartes 1975)

$$\mathrm{Tr}(C^\perp) = (C|_{\mathbb{F}_q})^\perp.$$

Trace codes and subfield subcodes

- The **trace map** of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

- We define $\mathrm{Tr}(\boldsymbol{x})$ for vectors **entry-by-entry.**
- Let C be a q^m-ary $[n, k, d]$-code.

Definition

- The subfield subcode of C is
- The trace code of C is

Theorem (Delsartes 1975)

$$\mathrm{Tr}(C^\perp) = (C|_{\mathbb{F}_q})^\perp.$$

Trace codes and subfield subcodes

- The **trace map** of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

- We define $\mathrm{Tr}(\boldsymbol{x})$ for vectors **entry-by-entry.**
- Let C be a q^m-ary $[n, k, d]$-code.

Definition

- The **subfield subcode** of C is

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n.$$

- The **trace code** of C is

$$\mathrm{Tr}(C) = \{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{x}) \mid \boldsymbol{x} \in C\}.$$

Theorem (Delsartes 1975)

$$\mathrm{Tr}(C^{\perp}) = (C|_{\mathbb{F}_q})^{\perp}.$$

Trace codes and subfield subcodes

- The **trace map** of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

- We define $\mathrm{Tr}(\boldsymbol{x})$ for vectors **entry-by-entry.**
- Let C be a q^m-ary $[n, k, d]$-code.

Definition

- The **subfield subcode** of C is

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n.$$

- The **trace code** of C is

$$\mathrm{Tr}(C) = \{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{x}) \mid \boldsymbol{x} \in C\}.$$

Theorem (Delsartes 1975)

$$\mathrm{Tr}(C^\perp) = (C|_{\mathbb{F}_q})^\perp.$$

- The **trace map** of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

- We define $\mathrm{Tr}(\boldsymbol{x})$ for vectors **entry-by-entry.**
- Let C be a q^m-ary $[n, k, d]$-code.

Definition

- The **subfield subcode** of C is

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n.$$

- The **trace code** of C is

$$\mathrm{Tr}(C) = \{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{x}) \mid \boldsymbol{x} \in C\}.$$

Theorem (Delsartes 1975)

$$\mathrm{Tr}(C^\perp) = (C|_{\mathbb{F}_q})^\perp.$$

Trace codes and subfield subcodes

- The **trace map** of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

- We define $\mathrm{Tr}(\boldsymbol{x})$ for vectors **entry-by-entry.**
- Let C be a q^m-ary $[n, k, d]$-code.

Definition

- The **subfield subcode** of C is

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n.$$

- The **trace code** of C is

$$\mathrm{Tr}(C) = \{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{x}) \mid \boldsymbol{x} \in C\}.$$

Theorem (Delsartes 1975)

$$\mathrm{Tr}(C^\perp) = (C|_{\mathbb{F}_q})^\perp.$$

Trace codes and subfield subcodes

- The **trace map** of the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \cdots + x^{q^{m-1}}.$$

- We define $\mathrm{Tr}(\boldsymbol{x})$ for vectors **entry-by-entry.**
- Let C be a q^m-ary $[n, k, d]$-code.

Definition

- The **subfield subcode** of C is

$$C|_{\mathbb{F}_q} = C \cap \mathbb{F}_q^n.$$

- The **trace code** of C is

$$\mathrm{Tr}(C) = \{\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\boldsymbol{x}) \mid \boldsymbol{x} \in C\}.$$

Theorem (Delsartes 1975)

$$\mathrm{Tr}(C^\perp) = (C|_{\mathbb{F}_q})^\perp.$$

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^{\perp}$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^\perp$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^\perp$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^\perp$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^\perp$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^{\perp}$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^{\perp}$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^{\perp}$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Parameters of trace codes and subfield subcodes

- *Length* is n.
- The *minimum distance* of $C|_{\mathbb{F}_q}$ is at least d.
- The *dual minimum distance* of $\mathrm{Tr}(C)$ is at least $d^{\perp}$.
- *Threshold decoding algorithms* keep working for $C|_{\mathbb{F}_q}$.

Open problem: The true dimension of subfield subcodes

We know:

- $\dim(\mathrm{Tr}(C)) \leq mk$.
- $\dim(C|_{\mathbb{F}_q}) \geq n - mk$.

- Partial results on some classes of subfield subcodes.
- See Véron (1998-2005) and Byrne et al. (2023) on the parameters of Trace Goppa Codes.

Alternant codes and Goppa codes

Definition: Alternant codes

Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries and $\boldsymbol{v} = (v_1, \dots, v_n) \in (\mathbb{F}^*_{q^m})^n$ a vector with **nonzero** entries. An alternant code of degree t is a code of the form

$$\mathscr{A}_t(\alpha, \boldsymbol{v}) = (\mathbf{GRS}_t(\alpha, \boldsymbol{v})^\perp)|_{\mathbb{F}_q} = \mathrm{Tr}(\mathbf{GRS}_t(\alpha, \boldsymbol{v}))^\perp.$$

- **Efficient decoding algorithms** with threshold $\lfloor t/2 \rfloor$.

Definition: Goppa codes

Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries, and $g \in \mathbb{F}_{q^m}(X)$ of degree t such that $g(\alpha_i) \neq 0$ for all $i = 1, \dots, n$. The Goppa code associated to (g, α) is defined as

$$\Gamma(g; \alpha) = \mathscr{A}_t(\alpha, (g(\alpha_1)^{-1}, \dots, g(\alpha_n)^{-1})).$$

- $\Gamma(g; \alpha) = \Gamma(g^2; \alpha)$ holds for $q = 2$ and square-free $g(X)$.
- **Efficient decoding algorithms** with threshold t.

Alternant codes and Goppa codes

Definition: Alternant codes

Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries and $\mathbf{v} = (v_1, \ldots, v_n) \in (\mathbb{F}^*_{q^m})^n$ a vector with **nonzero** entries. An alternant code of degree t is a code of the form

$$\mathscr{A}_t(\alpha, \mathbf{v}) = (\mathbf{GRS}_t(\alpha, \mathbf{v})^{\perp})|_{\mathbb{F}_q} = \mathrm{Tr}(\mathbf{GRS}_t(\alpha, \mathbf{v}))^{\perp}.$$

- **Efficient decoding algorithms** with threshold $\lfloor t/2 \rfloor$.

Definition: Goppa codes

Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries, and $g \in \mathbb{F}_{q^m}(X)$ of degree t such that $g(\alpha_i) \neq 0$ for all $i = 1, \ldots, n$. The Goppa code associated to (g, α) is defined as

$$\Gamma(g; \alpha) = \mathscr{A}_t(\alpha, (g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1})).$$

- $\Gamma(g; \alpha) = \Gamma(g^2; \alpha)$ holds for $q = 2$ and square-free $g(X)$.
- **Efficient decoding algorithms** with threshold t.

Alternant codes and Goppa codes

Definition: Alternant codes

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries and $\boldsymbol{v} = (v_1, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$ a vector with **nonzero** entries. An alternant code of degree t is a code of the form

$$\mathscr{A}_t(\boldsymbol{\alpha}, \boldsymbol{v}) = (\mathbf{GRS}_t(\boldsymbol{\alpha}, \boldsymbol{v})^\perp)|_{\mathbb{F}_q} = \mathrm{Tr}(\mathbf{GRS}_t(\boldsymbol{\alpha}, \boldsymbol{v}))^\perp.$$

- **Efficient decoding algorithms** with threshold $\lfloor t/2 \rfloor$.

Definition: Goppa codes

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries, and $g \in \mathbb{F}_{q^m}(X)$ of degree t such that $g(\alpha_i) \neq 0$ for all $i = 1, \ldots, n$. The Goppa code associated to (g, α) is defined as

$$\Gamma(g; \boldsymbol{\alpha}) = \mathscr{A}_t(\boldsymbol{\alpha}, (g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1})).$$

- $\Gamma(g; \alpha) = \Gamma(g^2; \alpha)$ holds for $q = 2$ and square-free $g(X)$.
- **Efficient decoding algorithms** with threshold t.

Alternant codes and Goppa codes

Definition: Alternant codes

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries and $\boldsymbol{v} = (v_1, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$ a vector with **nonzero** entries. An alternant code of degree t is a code of the form

$$\mathscr{A}_t(\boldsymbol{\alpha}, \boldsymbol{v}) = (\mathbf{GRS}_t(\boldsymbol{\alpha}, \boldsymbol{v})^\perp)|_{\mathbb{F}_q} = \mathrm{Tr}(\mathbf{GRS}_t(\boldsymbol{\alpha}, \boldsymbol{v}))^\perp.$$

- **Efficient decoding algorithms** with threshold $\lfloor t/2 \rfloor$.

Definition: Goppa codes

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries, and $g \in \mathbb{F}_{q^m}(X)$ of degree t such that $g(\alpha_i) \neq 0$ for all $i = 1, \ldots, n$. The Goppa code associated to $(g, \boldsymbol{\alpha})$ is defined as

$$\Gamma(g; \boldsymbol{\alpha}) = \mathscr{A}_t(\boldsymbol{\alpha}, (g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1})).$$

- $\Gamma(g; \boldsymbol{\alpha}) = \Gamma(g^2; \boldsymbol{\alpha})$ holds for $q = 2$ and square-free $g(X)$.
- **Efficient decoding algorithms** with threshold t.

Alternant codes and Goppa codes

Definition: Alternant codes

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries and $\boldsymbol{v} = (v_1, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$ a vector with **nonzero** entries. An alternant code of degree t is a code of the form

$$\mathscr{A}_t(\boldsymbol{\alpha}, \boldsymbol{v}) = (\mathbf{GRS}_t(\boldsymbol{\alpha}, \boldsymbol{v})^\perp)|_{\mathbb{F}_q} = \mathrm{Tr}(\mathbf{GRS}_t(\boldsymbol{\alpha}, \boldsymbol{v}))^\perp.$$

- **Efficient decoding algorithms** with threshold $\lfloor t/2 \rfloor$.

Definition: Goppa codes

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}$ be a vector with **distinct** entries, and $g \in \mathbb{F}_{q^m}(X)$ of degree t such that $g(\alpha_i) \neq 0$ for all $i = 1, \ldots, n$. The Goppa code associated to $(g, \boldsymbol{\alpha})$ is defined as

$$\Gamma(g; \boldsymbol{\alpha}) = \mathscr{A}_t(\boldsymbol{\alpha}, (g(\alpha_1)^{-1}, \ldots, g(\alpha_n)^{-1})).$$

- $\Gamma(g; \boldsymbol{\alpha}) = \Gamma(g^2; \boldsymbol{\alpha})$ holds for $q = 2$ and square-free $g(X)$.
- **Efficient decoding algorithms** with threshold t.

Outline

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k} | T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n-k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n-k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \dots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \dots, \alpha_n))$.
2. T is a $(n-k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \dots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k} | T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n-k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n-k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n - k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k} | T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n - k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n - k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n - k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n - k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Public key of the classic McEliece scheme

- Known parameters: n, m, t positive integers; $k = n - mt$, $q = 2$.

Randomly generated private key $(g; (\alpha_1, \ldots, \alpha_n))$

1. Monic irreducible polynomial $g(X) \in \mathbb{F}_{2^m}[X]$ of degree t.
2. **Different** elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^m}$.

Computed public key T

1. $H = [I_{n-k}|T]$ is the parity-check matrix of the binary Goppa code $\Gamma(g; (\alpha_1, \ldots, \alpha_n))$.
2. T is a $(n-k) \times k$ binary matrix.

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

Motivation 1: The probability of success

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

The **probability of success** is easy to compute for **(1)** and **(2).**

Classic McEliece NIST Proposal 2020

"Approximately 29% of choices of C have this form, so key generation requires about 3.4 attempts on average [...]"

Problem 1

Why 29%?

Motivation 1: The probability of success

"Las Vegas" TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

The **probability of success** is easy to compute for **(1)** and **(2).**

Classic McEliece NIST Proposal 2020

"Approximately 29% of choices of C have this form, so key generation requires about 3.4 attempts on average [...]"

Problem 1

Why 29%?

Motivation 1: The probability of success

“Las Vegas” TRY-and-REJECT if:

1. random irreducible polynomial g has degree $< t$;
2. random elements $\alpha_1, \ldots, \alpha_n$ are not distinct;
3. the first $mt = n - k$ columns of H are not linearly independent.

The **probability of success** is easy to compute for **(1)** and **(2).**

Classic McEliece NIST Proposal 2020

“Approximately 29% of choices of C have this form, so key generation requires about 3.4 attempts on average [...]”

Problem 1

Why 29%?

Motivation 2: Dimension of random alternant codes

1. The **Goppa Code Distinguishing Problem (GDP)** asks to distinguish efficiently a generator matrix of a Goppa code from a *randomly drawn one.*
2. The dimension of the square of alternant and Goppa codes is an important cryptanalytic tool in GDP.
3. See Faugère et al. (2013) for experimental evidences and Mora, Tillich (2022) for rigorous upper bounds.

Theorem [Mora, Tillich 2022]

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(\alpha, \mathbf{v})^{\perp})^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2).$$

Problem 2

Find $\dim_{\mathbb{F}_q} \mathscr{A}_r(\alpha, \mathbf{v})$ with uniformly random α and $\mathbf{v}$.

Motivation 2: Dimension of random alternant codes

1. The **Goppa Code Distinguishing Problem (GDP)** asks to distinguish efficiently a generator matrix of a Goppa code from a *randomly drawn one.*
2. The dimension of the square of alternant and Goppa codes is an important cryptanalytic tool in GDP.
3. See Faugère et al. (2013) for experimental evidences and Mora, Tillich (2022) for rigorous upper bounds.

Theorem [Mora, Tillich 2022]

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(\alpha, \mathbf{v})^{\perp})^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2).$$

Problem 2

Find $\dim_{\mathbb{F}_q} \mathscr{A}_r(\alpha, \mathbf{v})$ with uniformly random α and $\mathbf{v}$.

Motivation 2: Dimension of random alternant codes

1. The **Goppa Code Distinguishing Problem (GDP)** asks to distinguish efficiently a generator matrix of a Goppa code from a *randomly drawn one.*
2. The dimension of the square of alternant and Goppa codes is an important cryptanalytic tool in GDP.
3. See Faugère et al. (2013) for experimental evidences and Mora, Tillich (2022) for rigorous upper bounds.

Theorem [Mora, Tillich 2022]

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(\alpha, \boldsymbol{v})^{\perp})^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2).$$

Problem 2

Find $\dim_{\mathbb{F}_q} \mathscr{A}_r(\alpha, \boldsymbol{v})$ with uniformly random α and $\boldsymbol{v}$.

Motivation 2: Dimension of random alternant codes

1. The **Goppa Code Distinguishing Problem (GDP)** asks to distinguish efficiently a generator matrix of a Goppa code from a *randomly drawn one.*
2. The dimension of the square of alternant and Goppa codes is an important cryptanalytic tool in GDP.
3. See Faugère et al. (2013) for experimental evidences and Mora, Tillich (2022) for rigorous upper bounds.

Theorem [Mora, Tillich 2022]

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(\boldsymbol{\alpha}, \mathbf{v})^{\perp})^{\star 2} \leq \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2).$$

Problem 2

Find $\dim_{\mathbb{F}_q} \mathscr{A}_r(\boldsymbol{\alpha}, \mathbf{v})$ with uniformly random $\boldsymbol{\alpha}$ and $\mathbf{v}$.

Motivation 2: Dimension of random alternant codes

1. The **Goppa Code Distinguishing Problem (GDP)** asks to distinguish efficiently a generator matrix of a Goppa code from a *randomly drawn one.*
2. The dimension of the square of alternant and Goppa codes is an important cryptanalytic tool in GDP.
3. See Faugère et al. (2013) for experimental evidences and Mora, Tillich (2022) for rigorous upper bounds.

Theorem [Mora, Tillich 2022]

$$\dim_{\mathbb{F}_q}(\mathscr{A}_r(\alpha, \mathbf{v})^{\perp})^{\star 2} \le \binom{rm+1}{2} - \frac{m}{2}(r-1)(r-2).$$

Problem 2

Find $\dim_{\mathbb{F}_q} \mathscr{A}_r(\alpha, \mathbf{v})$ with uniformly random α and $\mathbf{v}$.

Outline

New codes by multiplier vectors

Definition: New code by a multiplier vector

Let $C \leq \mathbb{F}_q^n$ be a code of length n, and $\boldsymbol{a} = (a_1, \dots, a_n) \in (\mathbb{F}_q^*)^n$ a vector with nonzero entries. We define the code

$$C_{\boldsymbol{a}} = \{(a_1 x_1, \dots, a_n x_n) \mid (x_1, \dots, x_n) \in C\}$$

with multiplier vector $\boldsymbol{a}$.

Definition: Monomially equivalent codes

Two codes $C, D \leq \mathbb{F}_q^n$ are called monomially equivalent, if $D = C_{\boldsymbol{a}}$ for some multiplier vector $\boldsymbol{a} \in (\mathbb{F}_q^*)^n$.

- Monomially equivalent codes have the same parameters.
- $\mathbf{GRS}_k(\alpha, \boldsymbol{v}) = \mathbf{RS}_k(\alpha)_{\boldsymbol{v}}$.

New codes by multiplier vectors

Definition: New code by a multiplier vector

Let $C \leq \mathbb{F}_q^n$ be a code of length n, and $\boldsymbol{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$ a vector with nonzero entries. We define the code

$$C_{\boldsymbol{a}} = \{(a_1 x_1, \ldots, a_n x_n) \mid (x_1, \ldots, x_n) \in C\}$$

with multiplier vector $\boldsymbol{a}$.

Definition: Monomially equivalent codes

Two codes $C, D \leq \mathbb{F}_q^n$ are called monomially equivalent, if $D = C_{\boldsymbol{a}}$ for some multiplier vector $\boldsymbol{a} \in (\mathbb{F}_q^*)^n$.

- Monomially equivalent codes have the same parameters.
- $\mathbf{GRS}_k(\alpha, \boldsymbol{v}) = \mathbf{RS}_k(\alpha)_{\boldsymbol{v}}$.

New codes by multiplier vectors

Definition: New code by a multiplier vector

Let $C \leq \mathbb{F}_q^n$ be a code of length n, and $\boldsymbol{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$ a vector with nonzero entries. We define the code

$$C_{\boldsymbol{a}} = \{(a_1 x_1, \ldots, a_n x_n) \mid (x_1, \ldots, x_n) \in C\}$$

with multiplier vector $\boldsymbol{a}$.

Definition: Monomially equivalent codes

Two codes $C, D \leq \mathbb{F}_q^n$ are called monomially equivalent, if $D = C_{\boldsymbol{a}}$ for some multiplier vector $\boldsymbol{a} \in (\mathbb{F}_q^*)^n$.

- Monomially equivalent codes have the same parameters.
- $\mathbf{GRS}_k(\alpha, \boldsymbol{v}) = \mathbf{RS}_k(\alpha)_{\boldsymbol{v}}$.

New codes by multiplier vectors

Definition: New code by a multiplier vector

Let $C \leq \mathbb{F}_q^n$ be a code of length n, and $\boldsymbol{a} = (a_1, \dots, a_n) \in (\mathbb{F}_q^*)^n$ a vector with nonzero entries. We define the code

$$C_{\boldsymbol{a}} = \{(a_1 x_1, \dots, a_n x_n) \mid (x_1, \dots, x_n) \in C\}$$

with multiplier vector $\boldsymbol{a}$.

Definition: Monomially equivalent codes

Two codes $C, D \leq \mathbb{F}_q^n$ are called monomially equivalent, if $D = C_{\boldsymbol{a}}$ for some multiplier vector $\boldsymbol{a} \in (\mathbb{F}_q^*)^n$.

- Monomially equivalent codes have the same parameters.
- $\mathbf{GRS}_k(\alpha, \boldsymbol{v}) = \mathbf{RS}_k(\alpha)_{\boldsymbol{v}}$.

The Maximum Trace Dimension property

Definition: Maximum Trace Dimension property

Let $C \leq \mathbb{F}_{q^m}$ be a linear code of length n and dimension k. We say that C has maximum trace dimension if $mk \leq n$ and

$$\dim(\mathrm{Tr}(C)) = mk.$$

Theorem 1

Let C be an $[n, k, d]_{q^m}$-code and let $h = n + 1 - k - d$ be its Singleton defect. Let P_C denote the **proportion of multiplier vectors $\boldsymbol{a} \in (\mathbb{F}^*_{q^m})^n$** such that the linear code $C_{\boldsymbol{a}}$ has maximum trace dimension. Then

$$P_C \geq 1 - \frac{1 - q^{-m(h+k)}}{(q-1)q^{n-m(h+k)}}. \qquad (1)$$

In particular, if $n \geq m(k+h)$ then $P_C > 0$.

Proof. We use results by Meneghetti, Pellegrini, Sala (2022) on the weight distribution of almost MDS codes. $\square$

The Maximum Trace Dimension property

Definition: Maximum Trace Dimension property

Let $C \leq \mathbb{F}_{q^m}$ be a linear code of length n and dimension k. We say that C has maximum trace dimension if $mk \leq n$ and

$$\dim(\mathrm{Tr}(C)) = mk.$$

Theorem 1

Let C be an $[n, k, d]_{q^m}$-code and let $h = n + 1 - k - d$ be its Singleton defect. Let P_C denote the **proportion of multiplier vectors $\boldsymbol{a} \in (\mathbb{F}^*_{q^m})^n$** such that the linear code $C_{\boldsymbol{a}}$ has maximum trace dimension. Then

$$P_C \geq 1 - \frac{1 - q^{-m(h+k)}}{(q-1)q^{n-m(h+k)}}. \tag{1}$$

In particular, if $n \geq m(k + h)$ then $P_C > 0$.

Proof. We use results by Meneghetti, Pellegrini, Sala (2022) on the weight distribution of almost MDS codes. □

Corollaries

Full support random alternant codes have maximum dimension with very high probability:

Proposition

Assume $n > mk$. The **random alternant code** of length n, degree k, extension degree m over $\mathbb{F}_q$ has dimension $n - mk$ with probability at least

$$1 - \frac{1 - q^{-mk}}{(q-1)q^{n-mk}}. \quad (2)$$

Maximum trace dimension property of AG-codes:

Theorem 2

Let $C = C_L(D, G)$ be a **functional AG code** of length $n = \deg(D)$ over the finite field $\mathbb{F}_{q^m}$, $m > 1$. If $\deg(G) \leq n/m - 1$, then

$$P_C \geq 1 - \frac{1 - q^{-m(\deg(G)+1)}}{(q-1)q^{n-m(\deg(G)+1)}}. \quad (3)$$

Corollaries

Full support random alternant codes have maximum dimension with very high probability:

Proposition

Assume $n > mk$. The **random alternant code** of length n, degree k, extension degree m over $\mathbb{F}_q$ has dimension $n - mk$ with probability at least

$$1 - \frac{1 - q^{-mk}}{(q-1)q^{n-mk}}. \tag{2}$$

Maximum trace dimension property of AG-codes:

Theorem 2

Let $C = C_L(D, G)$ be a **functional AG code** of length $n = \deg(D)$ over the finite field $\mathbb{F}_{q^m}$, $m > 1$. If $\deg(G) \leq n/m - 1$, then

$$P_C \geq 1 - \frac{1 - q^{-m(\deg(G)+1)}}{(q-1)q^{n-m(\deg(G)+1)}}. \tag{3}$$

Maximum trace dimension for $n \leq mk$

Theorem 3

Let C be an $[n, k, d]_{q^m}$-code and let $h = n + 1 - k - d$ be its Singleton defect. Let P'_C denote the **proportion of multiplier vectors $\boldsymbol{a} \in (\mathbb{F}^*_{q^m})^n$** such that

$$\dim(\mathrm{Tr}(C_{\boldsymbol{a}})) \geq n - mh.$$

Then

$$P'_C \geq \frac{q^{mh+1} - q^{mh} - q^{n-mk} + q^{-mk}}{q^{mh+1} - 1}. \tag{4}$$

In particular:

1. If $n \leq m(k + h)$, or equivalently $d \leq n(1 - 1/m) + 1$, then $P'_C > 0$.
2. If C is **MDS** ($h = 0$) then

$$P'_C \geq 1 - \frac{1 - q^{-n}}{(q-1)q^{mk-n}}. \tag{5}$$

Maximum trace dimension for $n \leq mk$

Theorem 3

Let C be an $[n, k, d]_{q^m}$-code and let $h = n + 1 - k - d$ be its Singleton defect. Let P'_C denote the **proportion of multiplier vectors** $\boldsymbol{a} \in (\mathbb{F}^*_{q^m})^n$ such that

$$\dim(\mathrm{Tr}(C_{\boldsymbol{a}})) \geq n - mh.$$

Then

$$P'_C \geq \frac{q^{mh+1} - q^{mh} - q^{n-mk} + q^{-mk}}{q^{mh+1} - 1}. \tag{4}$$

In particular:

1. If $n \leq m(k + h)$, or equivalently $d \leq n(1 - 1/m) + 1$, then $P'_C > 0$.
2. If C is **MDS** ($h = 0$) then

$$P'_C \geq 1 - \frac{1 - q^{-n}}{(q-1)q^{mk-n}}. \tag{5}$$

Maximum trace dimension for $n \leq mk$

Theorem 3

Let C be an $[n,k,d]_{q^m}$-code and let $h = n + 1 - k - d$ be its Singleton defect. Let P'_C denote the **proportion of multiplier vectors $\boldsymbol{a} \in (\mathbb{F}^*_{q^m})^n$** such that

$$\dim(\mathrm{Tr}(C_{\boldsymbol{a}})) \geq n - mh.$$

Then

$$P'_C \geq \frac{q^{mh+1} - q^{mh} - q^{n-mk} + q^{-mk}}{q^{mh+1} - 1}. \tag{4}$$

In particular:

1. If $n \leq m(k+h)$, or equivalently $d \leq n(1 - 1/m) + 1$, then $P'_C > 0$.
2. If C is **MDS** ($h = 0$) then

$$P'_C \geq 1 - \frac{1 - q^{-n}}{(q-1)q^{mk-n}}. \tag{5}$$

Final remarks on the 29%

- Let A be an $n \times n$ matrix over the finite field $\mathbb{F}_q$, whose entries are chosen **uniformly at random.**
- As $n \to \infty$, the **probability** that A has rank n converges very fast to

$$S(q) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{q^i}\right).$$

- $S(q)$ is also called the q-Pochhamer symbol $(1/q; 1/q)_\infty$.
- For $q = 2$, a *good estimate* for $S(2)$ is

$$0.288788095086603.$$

- **Numerical experiments** show that with $q = 2$ and $n = mk$,

$$P_C \approx 0.29$$

holds, if C is Reed-Solomon ($h = 0$) or Hermitian code ($h \approx 2^{m-1}(2^m - 1)$)

Final remarks on the 29%

- Let A be an $n \times n$ matrix over the finite field $\mathbb{F}_q$, whose entries are chosen **uniformly at random.**
- As $n \to \infty$, the **probability** that A has rank n converges very fast to

$$S(q) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{q^i}\right).$$

- $S(q)$ is also called the q-Pochhamer symbol $(1/q; 1/q)_\infty$.
- For $q = 2$, a *good estimate* for $S(2)$ is

$$0.288788095086603.$$

- **Numerical experiments** show that with $q = 2$ and $n = mk$,

$$P_C \approx 0.29$$

holds, if C is Reed-Solomon ($h = 0$) or Hermitian code ($h \approx 2^{m-1}(2^m - 1)$)

Final remarks on the 29%

- Let A be an $n \times n$ matrix over the finite field $\mathbb{F}_q$, whose entries are chosen **uniformly at random.**
- As $n \to \infty$, the **probability** that A has rank n converges very fast to

$$S(q) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{q^i}\right).$$

- $S(q)$ is also called the q-Pochhamer symbol $(1/q; 1/q)_\infty$.
- For $q = 2$, a *good estimate* for $S(2)$ is

$$0.288788095086603.$$

- **Numerical experiments** show that with $q = 2$ and $n = mk$,

$$P_C \approx 0.29$$

holds, if C is Reed-Solomon ($h = 0$) or Hermitian code ($h \approx 2^{m-1}(2^m - 1)$)

Final remarks on the 29%

- Let A be an $n \times n$ matrix over the finite field $\mathbb{F}_q$, whose entries are chosen **uniformly at random.**
- As $n \to \infty$, the **probability** that A has rank n converges very fast to

$$S(q) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{q^i}\right).$$

- $S(q)$ is also called the q-Pochhamer symbol $(1/q; 1/q)_\infty$.
- For $q = 2$, a *good estimate* for $S(2)$ is

$$0.288788095086603.$$

- **Numerical experiments** show that with $q = 2$ and $n = mk$,

$$P_C \approx 0.29$$

holds, if C is Reed-Solomon ($h = 0$) or Hermitian code ($h \approx 2^{m-1}(2^m - 1)$)

Final remarks on the 29%

- Let A be an $n \times n$ matrix over the finite field $\mathbb{F}_q$, whose entries are chosen **uniformly at random.**
- As $n \to \infty$, the **probability** that A has rank n converges very fast to

$$S(q) = \prod_{i=1}^{\infty} \left(1 - \frac{1}{q^i}\right).$$

- $S(q)$ is also called the q-Pochhamer symbol $(1/q; 1/q)_\infty$.
- For $q = 2$, a *good estimate* for $S(2)$ is

$$0.288788095086603.$$

- **Numerical experiments** show that with $q = 2$ and $n = mk$,

$$P_C \approx 0.29$$

holds, if C is Reed-Solomon ($h = 0$) or Hermitian code ($h \approx 2^{m-1}(2^m - 1)$)

THANK YOU FOR YOUR ATTENTION!