A characterization of MDS codes that have an Error Correcting Pair

I. Márquez-Corbella [1] R. Pellikaan [2]

[1] INRIA Rocquencourt - SECRET Team

[3] Dept. of Mathematics and Computing Science, Eindhoven University of Technology

Applications of Computer Algebra (ACA 2015)

Session: Computational aspects and mathematical methods for finite fields and their applications in information theory

23, July 2015

1 Prerequisites

- MDS codes
- Star Product
- GRS codes

2 Error-Correcting Pairs

- Decoding algorithm for GRS - ECP
- Applications in Code-Based Cryptography

3 Main Result

- Puncturing, shortening and gluing
- Main Theorem
- Second Proof

4 Conclusion

NOTATION AND PREREQUISITES

- $\mathbb{F}_q$: Finite field with q elements.
- An $[n,k]_q$ **linear code** $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$
- The **Hamming weight** of $\mathbf{x} \in \mathbb{F}_q^n$ is $\mathrm{w}_H(\mathbf{x})$.

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ we will denote by:

$n(\mathcal{C})$: Length , $k(\mathcal{C})$: Dimension and $d(\mathcal{C})$: Minimum distance

NOTATION AND PREREQUISITES

- $\mathbb{F}_q$: Finite field with q elements.
- An $[n,k]_q$ **linear code** $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$
- The **Hamming weight** of $\mathbf{x} \in \mathbb{F}_q^n$ is $w_H(\mathbf{x})$.

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ we will denote by:

$n(\mathcal{C})$: Length , $k(\mathcal{C})$: Dimension and $d(\mathcal{C})$: Minimum distance

MDS CODES - SINGLETON BOUND

$$d(\mathcal{C}) \leq n(\mathcal{C}) - k(\mathcal{C}) + 1$$

If the equality holds $\Longrightarrow$ $\mathcal{C}$ is an **MDS code**

NOTATION AND PREREQUISITES

- $\mathbb{F}_q$: Finite field with q elements.
- An $[n,k]_q$ **linear code** $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$
- The **Hamming weight** of $\mathbf{x} \in \mathbb{F}_q^n$ is $w_H(\mathbf{x})$.

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ we will denote by:

$n(\mathcal{C})$: Length , $k(\mathcal{C})$: Dimension and $d(\mathcal{C})$: Minimum distance

MDS CODES - SINGLETON BOUND

$$d(\mathcal{C}) \leq n(\mathcal{C}) - k(\mathcal{C}) + 1$$

If the equality holds $\Longrightarrow$ $\mathcal{C}$ is an **MDS code**

EXAMPLES

1. The **zero code** of length n (i.e. the $[n, 0, n+1]$ linear code) and **its dual** (i.e. $\mathbb{F}_q^n$ which has parameters $[n, n, 1]$).
2. The $[n, 1, n]$ **repetition code** over $\mathbb{F}_q$
3. The **(Extended/Generalized) Reed-Solomon codes**

Star Product

Given two vectors $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ we denote by $\mathbf{a} * \mathbf{b}$ the **componentwise product**:

$$\mathbf{a} * \mathbf{b} = (a_1 b_1, \ldots, a_n b_n)$$

Star Product

Given two vectors $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ we denote by $\mathbf{a} * \mathbf{b}$ the **componentwise product**:

$$\mathbf{a} * \mathbf{b} = (a_1 b_1, \ldots, a_n b_n)$$

Star Product of Codes

Let A and B be $\mathbb{F}_q$-codes of length n.
The **star product code** denoted by $A * B$ is:

$$A * B = \langle \{ \mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B \} \rangle$$

When $B = A$, then $A * A$ is called the **square** of A and is denoted by A^2

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i.

GENERALIZED REED-SOLOMON CODES

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i.

Polynomial Vector Space:

$$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$$

GENERALIZED REED-SOLOMON CODES

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i.

Polynomial Vector Space: $L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$

L_k is a vector space of dimension k over $\mathbb{F}_q$

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i.

Polynomial Vector Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$

L_k is a vector space of dimension k over $\mathbb{F}_q$

A basis for L_k is $\left\{1, X, X^2, \ldots, X^{k-1}\right\}$

Generalized Reed-Solomon codes

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i.

Polynomial Vector Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$

L_k is a vector space of dimension k over $\mathbb{F}_q$

A basis for L_k is $\left\{1, X, X^2, \ldots, X^{k-1}\right\}$

Evaluation Map:

$$\begin{array}{rccl} \mathrm{ev}_{\mathbf{a},\mathbf{b}} & L_k & \longrightarrow & \mathbb{F}_q^n \\ & f(X) & \longmapsto & \mathbf{b} * f(\mathbf{a}) \\ & & & = (b_1 f(a_1), \ldots, b_n f(a_n)) \end{array}$$

GENERALIZED REED-SOLOMON CODES

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$.
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i.

Polynomial Vector Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$

L_k is a vector space of dimension k over $\mathbb{F}_q$

A basis for L_k is $\left\{1, X, X^2, \ldots, X^{k-1}\right\}$

Evaluation Map:

$$\begin{array}{rcl} \mathrm{ev}_{\mathbf{a},\mathbf{b}} \quad L_k & \longrightarrow & \mathbb{F}_q^n \\ f(X) & \longmapsto & \mathbf{b} * f(\mathbf{a}) \\ & & = (b_1 f(a_1), \ldots, b_n f(a_n)) \end{array}$$

THE GENERALIZED REED-SOLOMON CODE (GRS)

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f) \mid f \in L_k \right\}$$

GENERALIZED REED-SOLOMON CODES

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. $\Longrightarrow$ **code locators**
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i.

Polynomial Vector Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$

L_k is a vector space of dimension k over $\mathbb{F}_q$

A basis for L_k is $\left\{1, X, X^2, \ldots, X^{k-1}\right\}$

Evaluation Map:

$$\begin{array}{rcl} \mathrm{ev}_{\mathbf{a},\mathbf{b}} \quad L_k & \longrightarrow & \mathbb{F}_q^n \\ f(X) & \longmapsto & \mathbf{b} * f(\mathbf{a}) \\ & & = (b_1 f(a_1), \ldots, b_n f(a_n)) \end{array}$$

THE GENERALIZED REED-SOLOMON CODE (GRS)

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f) \mid f \in L_k \right\}$$

GENERALIZED REED-SOLOMON CODES

- n, k nonnegative integers such that $1 \leq k \leq n \leq q$.
- $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ with $a_i \neq a_j$ for all $i \neq j$. $\Longrightarrow$ **code locators**
- $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ with $b_i \neq 0$ for all i. $\Longrightarrow$ **column multipliers**

Polynomial Vector Space:

$L_k = \{f(X) \in \mathbb{F}_q[X] \mid \deg(f) < k\}$

L_k is a vector space of dimension k over $\mathbb{F}_q$

A basis for L_k is $\left\{1, X, X^2, \ldots, X^{k-1}\right\}$

Evaluation Map:

$$\begin{array}{rcl} \mathrm{ev}_{\mathbf{a},\mathbf{b}} \quad L_k & \longrightarrow & \mathbb{F}_q^n \\ f(X) & \longmapsto & \mathbf{b} * f(\mathbf{a}) \\ & & = (b_1 f(a_1), \ldots, b_n f(a_n)) \end{array}$$

THE GENERALIZED REED-SOLOMON CODE (GRS)

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) = \left\{ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f) \mid f \in L_k \right\}$$

Properties of GRS codes

Proposition: Parameters of GRS codes

The $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is an $[n, k]_q$ code with minimum distance $d = n - k + 1$

Properties of GRS codes

Proposition: Parameters of GRS codes

The $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is an $[n, k]_q$ code with minimum distance $d = n - k + 1$

$$\mathcal{C} \text{ is } \mathbf{MDS} \iff \mathcal{C}^{\perp} \text{ is } \mathbf{MDS}$$

Properties of GRS codes

Proposition: Parameters of GRS codes

The $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is an $[n, k]_q$ code with minimum distance $d = n - k + 1$

$$\mathcal{C} \text{ is } \mathbf{MDS} \iff \mathcal{C}^{\perp} \text{ is } \mathbf{MDS}$$

Proposition: The dual code of a GRS code is a GRS code

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{b}')$$

Canonical Generator matrix for GRS

Canonical Generator matrix for GRS

One basis for L_k is $\left\{1, X, X^2, \ldots, X^{k-1}\right\}$

Canonical Generator matrix for GRS

One basis for L_k is $\{1, X, X^2, \ldots, X^{k-1}\}$

Thus, $\{\mathrm{ev}_{\mathbf{a},\mathbf{b}}(1), \mathrm{ev}_{\mathbf{a},\mathbf{b}}(X), \mathrm{ev}_{\mathbf{a},\mathbf{b}}(X^2), \ldots \mathrm{ev}_{\mathbf{a},\mathbf{b}}(X^{k-1})\}$ gives a generator matrix for $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$

Canonical Generator matrix for GRS

One basis for L_k is $\{1, X, X^2, \ldots, X^{k-1}\}$

Thus, $\{\mathrm{ev}_{\mathbf{a},\mathbf{b}}(1), \mathrm{ev}_{\mathbf{a},\mathbf{b}}(X), \mathrm{ev}_{\mathbf{a},\mathbf{b}}(X^2), \ldots \mathrm{ev}_{\mathbf{a},\mathbf{b}}(X^{k-1})\}$ gives a generator matrix for $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \ldots & a_n^{k-1} \end{pmatrix} \begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix}$$

$$= \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ b_1 a_1 & b_2 a_2 & \ldots & b_n a_n \\ b_1 a_1^2 & b_2 a_2^2 & \ldots & b_n a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{k-1} & b_2 a_2^{k-1} & \ldots & b_n a_n^{k-1} \end{pmatrix} = \begin{pmatrix} \mathbf{b} * \mathbf{1} \\ \mathbf{b} * \mathbf{a} \\ \mathbf{b} * \mathbf{a}^2 \\ \vdots \\ \mathbf{b} * \mathbf{a}^{k-1} \end{pmatrix} \in \mathbb{F}_q^{k \times n}$$

Error-correcting pairs (ECP)

Error-correcting pairs (ECP)

Let:

- $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code. and

R. Pellikaan

On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.

A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

Error-correcting pairs (ECP)

Error-correcting pairs (ECP)

Let:

- $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code.

and

- A be an $[n, K(A)]_{q^m}$ code
- B be an $[n, K(B)]_{q^m}$ code

R. Pellikaan

On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.

A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

ERROR-CORRECTING PAIRS (ECP)

ERROR-CORRECTING PAIRS (ECP)

Let:

- $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code.

and

- A be an $[n, K(A)]_{q^m}$ code
- B be an $[n, K(B)]_{q^m}$ code

(A, B) is a ***t*-ECP** for $\mathcal{C}$ if the following properties hold:

- E.1 $(A * B) \perp \mathcal{C}$.
- E.2 $K(A) > t$.
- E.3 $d(B^{\perp}) > t$.
- E.4 $d(A) + d(\mathcal{C}) > n$.

R. Pellikaan

On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.

A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

ERROR-CORRECTING PAIRS (ECP)

ERROR-CORRECTING PAIRS (ECP)

Let:

- $\mathcal{C}$ be an $[n, K(\mathcal{C})]_q$ code.

and

- A be an $[n, K(A)]_{q^m}$ code
- B be an $[n, K(B)]_{q^m}$ code

(A, B) is a ***t*-ECP** for $\mathcal{C}$ if the following properties hold:

- E.1 $(A * B) \perp \mathcal{C}$.
- E.2 $K(A) > t$.
- E.3 $d(B^{\perp}) > t$.
- E.4 $d(A) + d(\mathcal{C}) > n$.

An $[n, k]_q$ code which has a t-ECP over $\mathbb{F}_{q^m}$ has an efficient decoding algorithm.

R. Pellikaan

On decoding by error location and dependent sets of error positions.
Discrete Math., 106–107: 369–381 (1992).

R. Kötter.

A unified description of an error locating procedure for linear codes.
In Proceedings of Algebraic and Combinatorial Coding Theory, 113–117. Voneshta Voda (1992).

An efficient decoding algorithm for GRS codes

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \Longrightarrow \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

An efficient decoding algorithm for GRS codes

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \Longrightarrow \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

Consider the codes

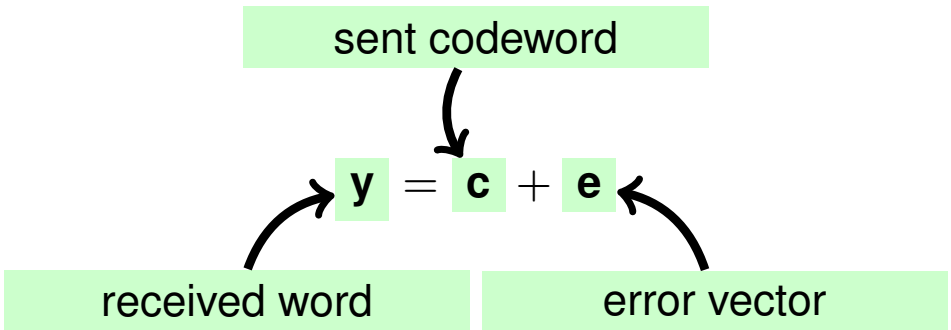
$\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})$

An efficient decoding algorithm for GRS codes

Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \Longrightarrow \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

Consider the codes

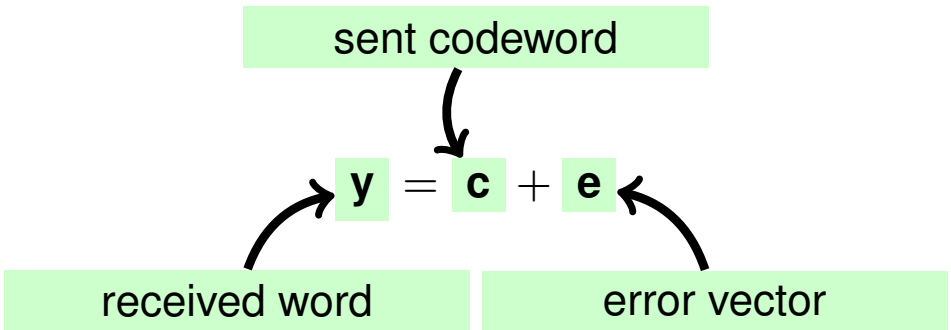
$\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})$



Let $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d}) \Longrightarrow \mathcal{C}^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp})$

Consider the codes

$\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})$



Define:

$$K_{\mathbf{y}} = \left\{ \mathbf{a} \in \mathcal{A} \mid \langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = 0 \text{ , for all } \mathbf{b} \in \mathcal{B} \right\}$$

An efficient decoding algorithm for GRS codes

$$K_y = K_e ?$$

$K_y = K_e$?

Take notice that:

$$\mathcal{A} * \mathcal{B} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})$$

An efficient decoding algorithm for GRS codes

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \end{aligned}$$

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) \end{aligned}$$

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle$$

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{c} + \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{c} + \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \underbrace{\langle \mathbf{c}, \mathbf{a} * \mathbf{b} \rangle}_{=0} + \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

$K_y = K_e$?

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

Or equivalently, $K_{\mathbf{y}} = K_{\mathbf{e}}$

$K_y = K_e$?

YES, since $\mathcal{A} * \mathcal{B} = \mathcal{C}^{\perp}$

Take notice that:

$$\begin{aligned} \mathcal{A} * \mathcal{B} &= \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp}) * \mathrm{GRS}_{t}(\mathbf{c}, \mathbf{1}) \\ &= \mathrm{GRS}_{2t}(\mathbf{c}, \mathbf{d}^{\perp}) \\ &= \mathrm{GRS}_{n-k}(\mathbf{c}, \mathbf{d}^{\perp}) = \mathcal{C}^{\perp} \end{aligned}$$

Thus, for all $\mathbf{a} \in \mathcal{A}$ and $\mathbf{b} \in \mathcal{B}$

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle$$

Or equivalently, $K_{\mathbf{y}} = K_{\mathbf{e}}$

There exists a nonzero $a \in K_y$?

There exists a nonzero $a \in K_y$?

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t+1$, i.e.

$f \in L_{t+1}$

There exists a nonzero $\mathbf{a} \in K_y$?

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t+1$, i.e. $f \in L_{t+1}$

$$\mathbf{a} = \mathbf{d}^{\perp} * f(\mathbf{c}) = \mathrm{ev}_{\mathbf{c},\mathbf{d}^{\perp}}(f) \in \mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$$

There exists a nonzero $\mathbf{a} \in K_y$?

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t+1$, i.e. $f \in L_{t+1}$

$$\mathbf{a} = \mathbf{d}^{\perp} * f(\mathbf{c}) = \mathrm{ev}_{\mathbf{c},\mathbf{d}^{\perp}}(f) \in \mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$$

Moreover, $\mathbf{a} * \mathbf{e} = \mathbf{0}$. Thus $\mathbf{a} \in K_{\mathbf{y}}$

There exists a nonzero $\mathbf{a} \in K_y$?

YES, since $K(\mathcal{A}) > t$

We define $f(X) = \prod_{i \in \mathrm{supp}(\mathbf{e})} (X - c_i) \implies \deg(f) = t < t+1$, i.e. $f \in L_{t+1}$

$$\mathbf{a} = \mathbf{d}^{\perp} * f(\mathbf{c}) = \mathrm{ev}_{\mathbf{c},\mathbf{d}^{\perp}}(f) \in \mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$$

Moreover, $\mathbf{a} * \mathbf{e} = \mathbf{0}$. Thus $\mathbf{a} \in K_{\mathbf{y}}$

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \Longrightarrow \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \Longrightarrow \operatorname{supp}(\mathbf{e}) \subseteq \overline{\operatorname{supp}(\mathbf{a})}$?

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \implies \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \Longrightarrow \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \implies \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

But $\mathrm{w}_H(\mathbf{e} * \mathbf{a}) \leq \mathrm{w}_H(\mathbf{e}) < t < d(\mathcal{B}^{\perp})$

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \Longrightarrow \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \implies \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

But $\mathrm{w}_H(\mathbf{e} * \mathbf{a}) \leq \mathrm{w}_H(\mathbf{e}) < t < d(\mathcal{B}^{\perp})$
Thus $\mathbf{e} * \mathbf{a} = \mathbf{0}$, i.e.

$$\mathrm{supp}(\mathbf{e}) \subseteq \{1, \ldots, n\} - \mathrm{supp}(\mathbf{a}) = \overline{\mathrm{supp}(\mathbf{a})}$$

Let $\mathbf{a} \in K_{\mathbf{y}}$, $\mathbf{a} \neq \mathbf{0} \Longrightarrow \mathrm{supp}(\mathbf{e}) \subseteq \overline{\mathrm{supp}(\mathbf{a})}$?

YES, since $d(\mathcal{B}^{\perp}) > t$

Indeed,

$$0 = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e} * \mathbf{a}, \mathbf{b} \rangle \implies \mathbf{e} * \mathbf{a} \in \mathcal{B}^{\perp}$$

But $\mathrm{w}_H(\mathbf{e} * \mathbf{a}) \leq \mathrm{w}_H(\mathbf{e}) < t < d(\mathcal{B}^{\perp})$
Thus $\mathbf{e} * \mathbf{a} = \mathbf{0}$, i.e.

$$\mathrm{supp}(\mathbf{e}) \subseteq \{1, \ldots, n\} - \mathrm{supp}(\mathbf{a}) = \overline{\mathrm{supp}(\mathbf{a})}$$

An efficient decoding algorithm for GRS codes

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If $w_H(\mathbf{e}) \leq t$, then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\operatorname{supp}(\mathbf{a})}$$

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If $w_H(\mathbf{e}) \leq t$, then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\text{supp}(\mathbf{a})}$$

Is the solution unique?

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If $w_H(\mathbf{e}) \leq t$, then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\text{supp}(\mathbf{a})}$$

Is the solution unique?

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system.

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If $w_H(\mathbf{e}) \leq t$, then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\operatorname{supp}(\mathbf{a})}$$

Is the solution unique?

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system. Then,

$$\langle \mathbf{e}_1, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}_2, \mathbf{a} * \mathbf{b} \rangle \text{ with } \begin{cases} \operatorname{supp}(\mathbf{e}_1) \subseteq \overline{\operatorname{supp}(\mathbf{a})} \\ \operatorname{supp}(\mathbf{e}_2) \subseteq \overline{\operatorname{supp}(\mathbf{a})} \end{cases}$$

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If $w_H(\mathbf{e}) \leq t$, then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\text{supp}(\mathbf{a})}$$

Is the solution unique?

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system. Then,

$$\langle \mathbf{e}_1, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}_2, \mathbf{a} * \mathbf{b} \rangle \text{ with } \begin{cases} \text{supp}(\mathbf{e}_1) \subseteq \overline{\text{supp}(\mathbf{a})} \\ \text{supp}(\mathbf{e}_2) \subseteq \overline{\text{supp}(\mathbf{a})} \end{cases}$$

Then $\mathbf{e}_1 - \mathbf{e}_2 \in \mathcal{C}$, but

$$w_H(\mathbf{e}_1 - \mathbf{e}_2) \leq n - |\text{supp}(\mathbf{a})| \leq d(\mathcal{C}) - 1$$

which **contradicts** the minimality of $d(\mathcal{C})$.

Let $\mathbf{a} \in K_{\mathbf{y}}$ such that $\mathbf{a} \neq 0$.
If $\mathrm{w}_H(\mathbf{e}) \leq t$, then $\mathbf{e}$ is a solution of:

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle \quad \text{for all } \mathbf{b} \in \mathcal{B} \text{ with } e_j \neq 0 \text{ for all } j \in \overline{\mathrm{supp}(\mathbf{a})}$$

Is the solution unique?

YES, since

$$d(\mathcal{A}) + d(\mathcal{C}) > n$$

Suppose that $\mathbf{e}_1$ and $\mathbf{e}_2$ are solutions of the above system. Then,

$$\langle \mathbf{e}_1, \mathbf{a} * \mathbf{b} \rangle = \langle \mathbf{e}_2, \mathbf{a} * \mathbf{b} \rangle \text{ with } \begin{cases} \mathrm{supp}(\mathbf{e}_1) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \\ \mathrm{supp}(\mathbf{e}_2) \subseteq \overline{\mathrm{supp}(\mathbf{a})} \end{cases}$$

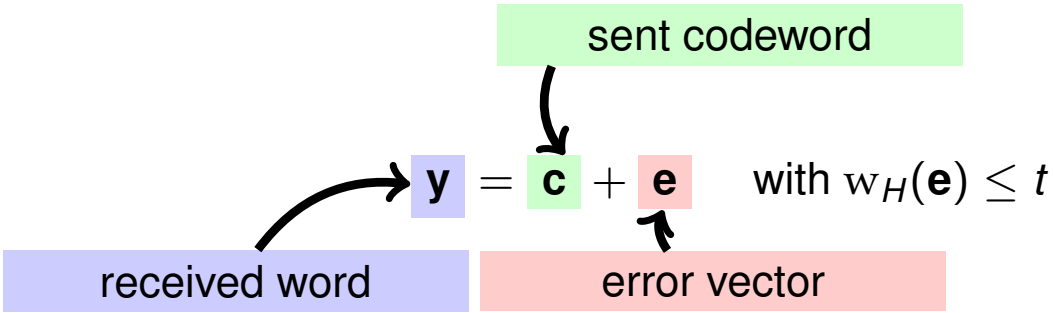
Then $\mathbf{e}_1 - \mathbf{e}_2 \in \mathcal{C}$, but

$$\mathrm{w}_H(\mathbf{e}_1 - \mathbf{e}_2) \leq n - |\mathrm{supp}(\mathbf{a})| \leq d(\mathcal{C}) - 1$$

which **contradicts** the minimality of $d(\mathcal{C})$.

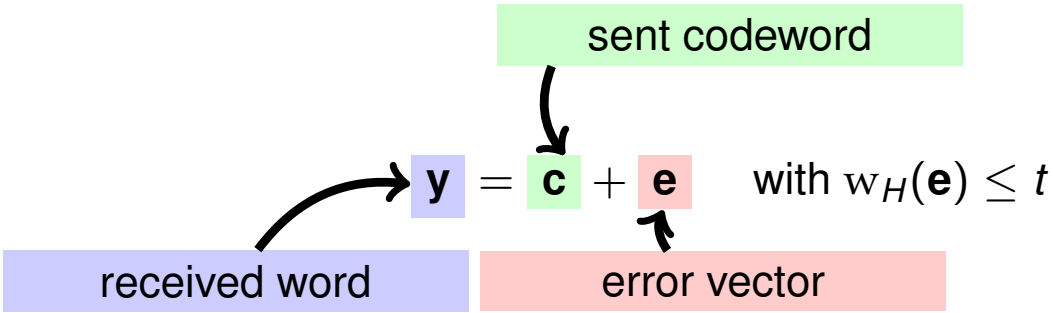
Error-correcting pairs (ECP)

Let $(\mathcal{A}, \mathcal{B})$ be a t-ECP for $\mathcal{C}$.



Error-correcting pairs (ECP)

Let $(\mathcal{A}, \mathcal{B})$ be a t-ECP for $\mathcal{C}$.

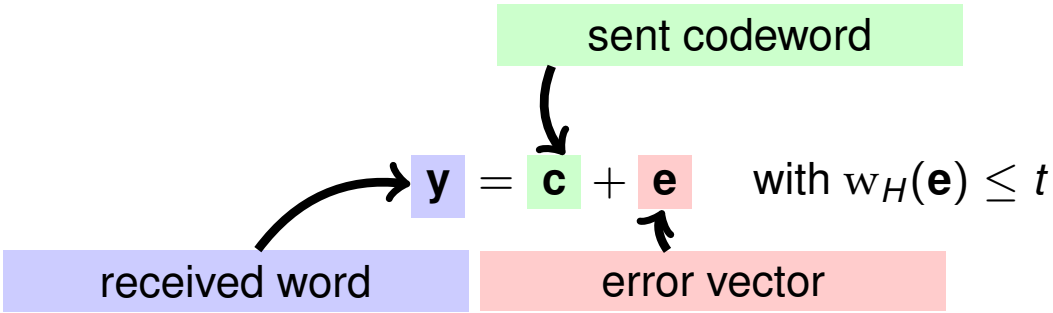


1. There exists $\mathbf{a} \in \mathcal{A}$, $\mathbf{a} \neq \mathbf{0}$ such that

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = 0 \text{ for all } \mathbf{b} \in \mathcal{B} \tag{1}$$

Error-correcting pairs (ECP)

Let $(\mathcal{A}, \mathcal{B})$ be a t-ECP for $\mathcal{C}$.



1. There exists $\mathbf{a} \in \mathcal{A}$, $\mathbf{a} \neq \mathbf{0}$ such that

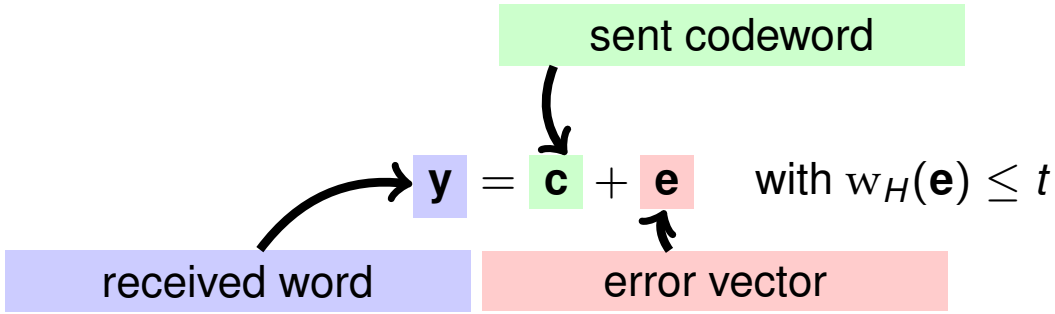
$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = 0 \text{ for all } \mathbf{b} \in \mathcal{B} \tag{1}$$

2. For every solution $\mathbf{a} \in \mathcal{A}$ of (1) we have that:

$$\mathbf{a} * \mathbf{e} = \mathbf{0}$$

Error-correcting pairs (ECP)

Let $(\mathcal{A}, \mathcal{B})$ be a t-ECP for $\mathcal{C}$.



1. There exists $\mathbf{a} \in \mathcal{A}$, $\mathbf{a} \neq \mathbf{0}$ such that

$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = 0 \text{ for all } \mathbf{b} \in \mathcal{B} \tag{1}$$

2. For every solution $\mathbf{a} \in \mathcal{A}$ of (1) we have that:

$$\mathbf{a} * \mathbf{e} = \mathbf{0}$$

3. Since $d(\mathcal{A}) + d(\mathcal{C}) \geq n$. Then, $\mathbf{e}$ is the **unique** solution of:

$$\langle \mathbf{e}, \mathbf{a} * \mathbf{b} \rangle = \mathbf{0} \text{ with } \mathbf{e} * \mathbf{a} = 0 \text{ for all } \mathbf{b} \in \mathcal{B}$$

Error-correcting pairs (ECP)

➜ t-ECP for Generalized Reed-Solomon (GRS) codes

I. Duursma

Decoding codes from curves and cyclic codes.
Ph.D thesis, Eindhoven University of Technology (1993)

I. Duursma, R. Kötter.

Error-locating pairs for cyclic codes.
IEEE Trans. Inform. Theory, Vol.40, 1108–1121 (1994)

Error-correcting pairs (ECP)

➜ t-ECP for Generalized Reed-Solomon (GRS) codes

Let $\mathcal{D}$ be a code that has $(\mathcal{A}, \mathcal{B})$ as t-ECP and suppose that $\mathcal{C} \subseteq \mathcal{D}$. Then $(\mathcal{A}, \mathcal{B})$ is also a t-ECP for $\mathcal{C}$.

In particular **subcodes of GRS** codes have a t-ECP

- ➜ t-ECP for Alternant codes
- ➜ t-ECP for Goppa codes

I. Duursma

Decoding codes from curves and cyclic codes.
Ph.D thesis, Eindhoven University of Technology (1993)

I. Duursma, R. Kötter.

Error-locating pairs for cyclic codes.
IEEE Trans. Inform. Theory, Vol.40, 1108–1121 (1994)

Error-correcting pairs (ECP)

➜ t-ECP for Generalized Reed-Solomon (GRS) codes

> Let $\mathcal{D}$ be a code that has $(\mathcal{A}, \mathcal{B})$ as t-ECP and suppose that $\mathcal{C} \subseteq \mathcal{D}$. Then $(\mathcal{A}, \mathcal{B})$ is also a t-ECP for $\mathcal{C}$.

In particular **subcodes of GRS** codes have a t-ECP

- ➜ t-ECP for Alternant codes
- ➜ t-ECP for Goppa codes

➜ t-ECP for Algebraic-Geometric (AG) codes

I. Duursma

Decoding codes from curves and cyclic codes.
Ph.D thesis, Eindhoven University of Technology (1993)

I. Duursma, R. Kötter.

Error-locating pairs for cyclic codes.
IEEE Trans. Inform. Theory, Vol.40, 1108–1121 (1994)

Error-correcting pairs (ECP)

➜ t-ECP for Generalized Reed-Solomon (GRS) codes

> Let $\mathcal{D}$ be a code that has $(\mathcal{A}, \mathcal{B})$ as t-ECP and suppose that $\mathcal{C} \subseteq \mathcal{D}$. Then $(\mathcal{A}, \mathcal{B})$ is also a t-ECP for $\mathcal{C}$.

In particular **subcodes of GRS** codes have a t-ECP

- ➜ t-ECP for Alternant codes
- ➜ t-ECP for Goppa codes

➜ t-ECP for Algebraic-Geometric (AG) codes

➜ t-ECP for Cyclic codes

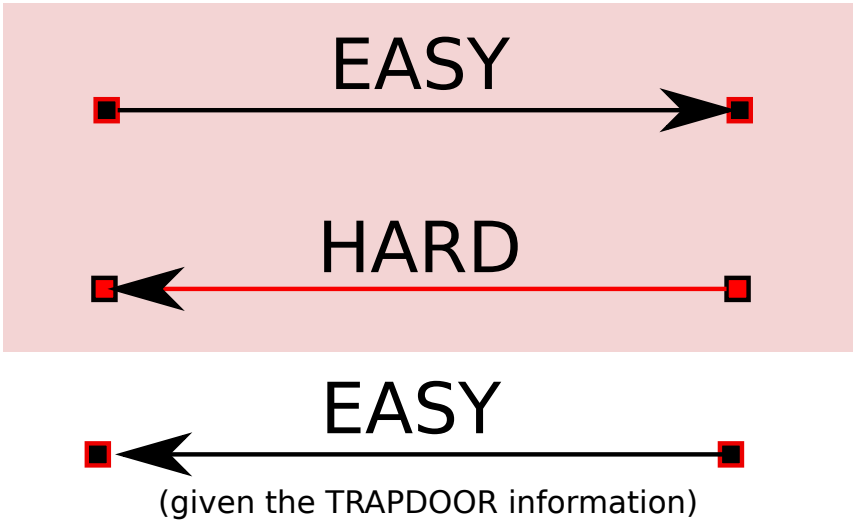
I. Duursma

Decoding codes from curves and cyclic codes.
Ph.D thesis, Eindhoven University of Technology (1993)

I. Duursma, R. Kötter.

Error-locating pairs for cyclic codes.
IEEE Trans. Inform. Theory, Vol.40, 1108–1121 (1994)

Public Key Cryptography



One-Way function

Trapdoor one-way function

Preparing for the Cryptopocalypse

Most PKC are based on Number-theoretic problems

Preparing for the Cryptopocalypse

Most PKC are based on Number-theoretic problems

➜ It can be attacked in polynomial time using **Shor's algorithm**

RSA
DSA
ECC
ECDSA
HECC

Preparing for the Cryptopocalypse

Most PKC are based on Number-theoretic problems

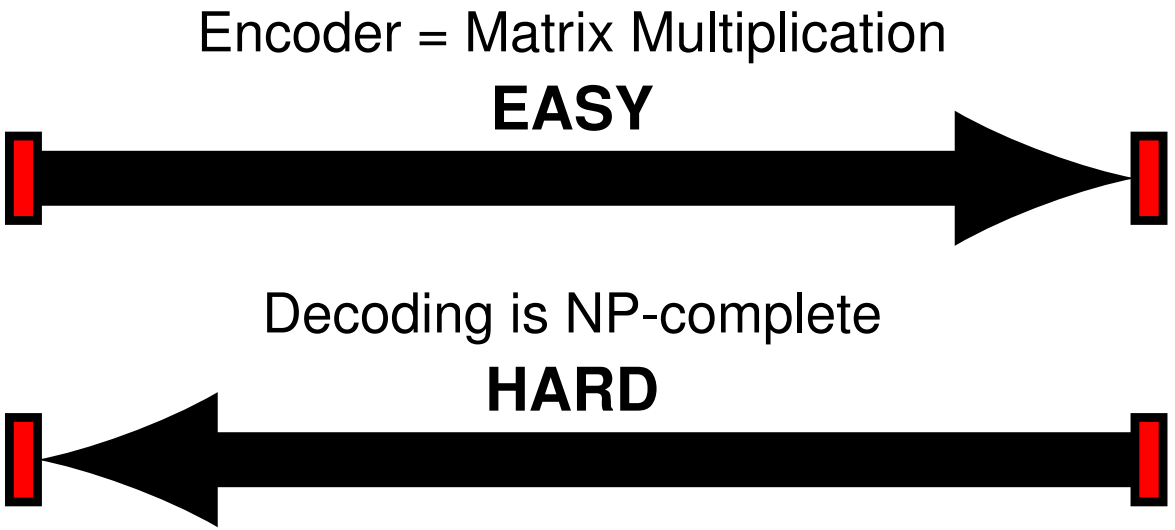
➜ It can be attacked in polynomial time using **Shor's algorithm**

RSA
DSA
ECC
ECDSA
HECC

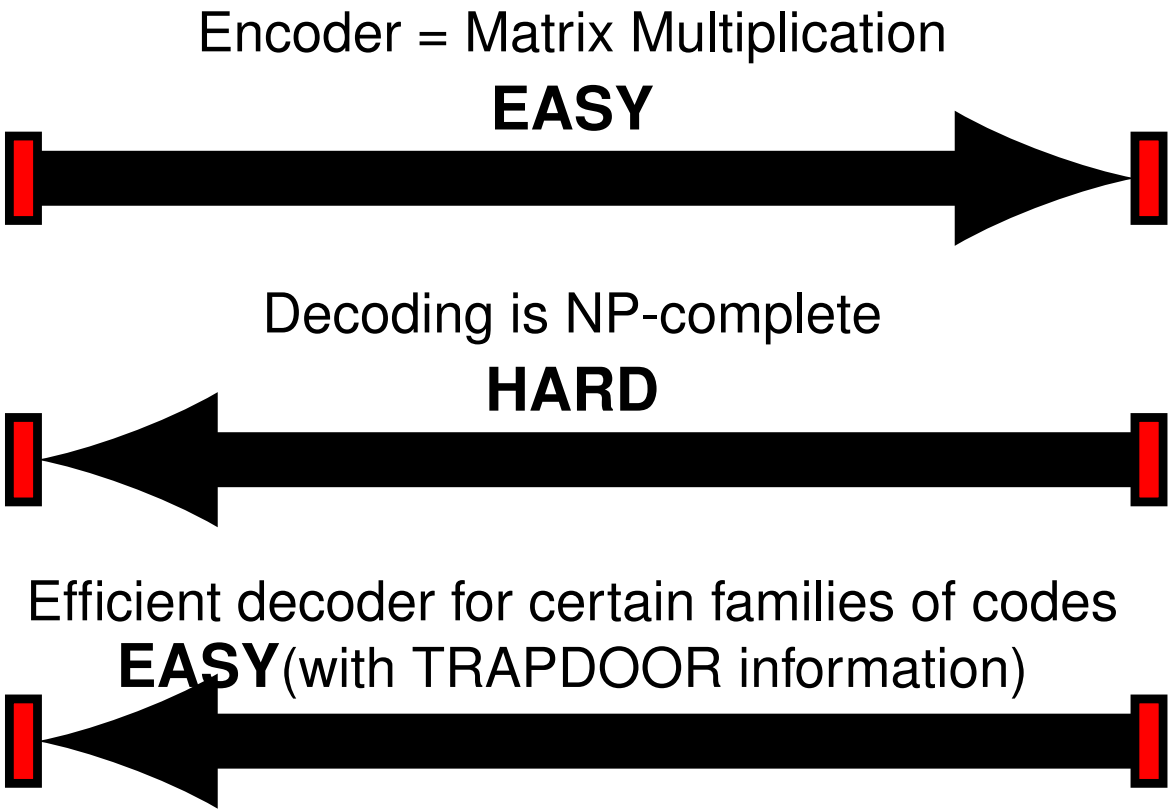
Code-based Cryptography is a powerful alternative

Trapdoor one-way functions - Decoder

Trapdoor one-way functions - Decoder



Trapdoor one-way functions - Decoder



McEliece cryptosystem

➜ McEliece introduced the first PKC based on Error-Correcting Codes in 1978.

Advantages:

- Fast encryption (matrix-vector multiplication) and decryption functions.
- Interesting candidate for post-quantum cryptography.

Drawback:

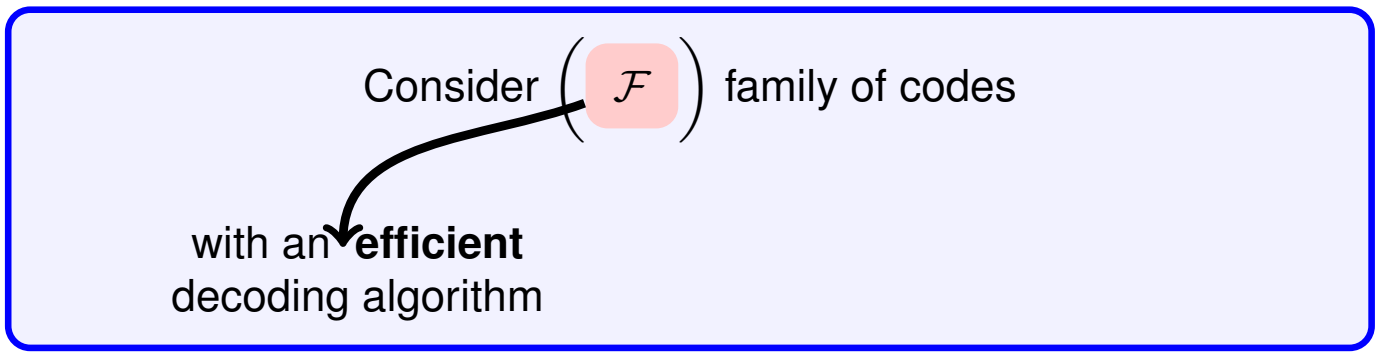
- Large key size.

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

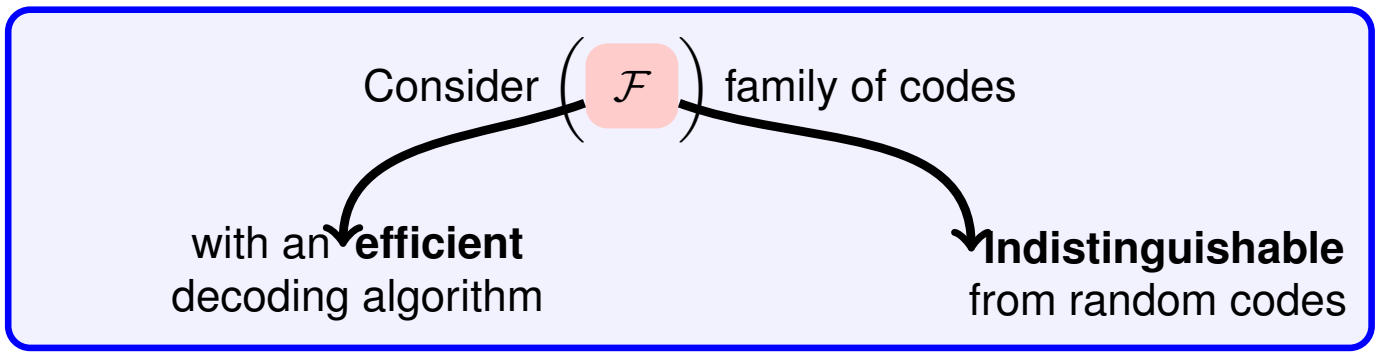
The McEliece Cryptosystem

Consider $\left(\mathcal{F} \right)$ family of codes

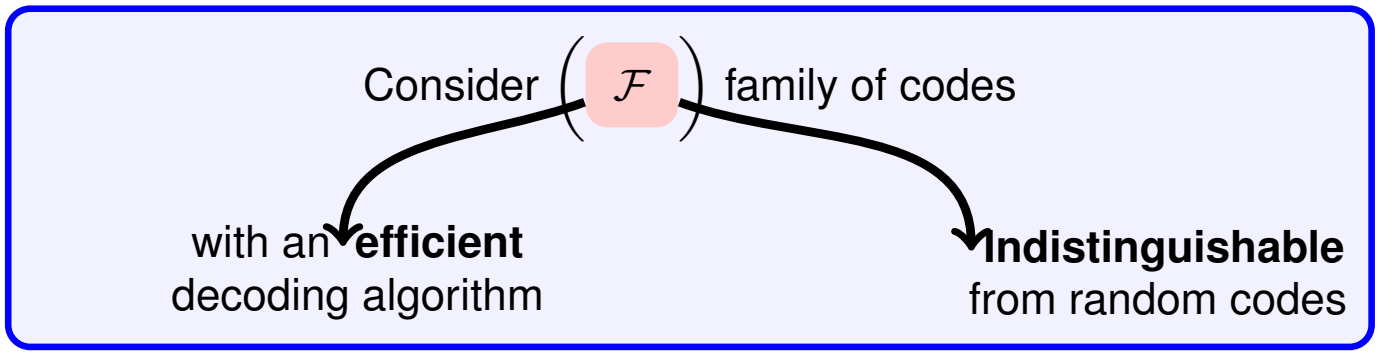
The McEliece Cryptosystem



The McEliece Cryptosystem



The McEliece Cryptosystem



Key Generation Algorithm:

- $G \in \mathbb{F}_q^{k \times n}$ a **generator matrix** for $\mathcal{C} \in \mathcal{F}$
- $\mathcal{A}_{\mathcal{C}}$ an **"Efficient" decoding algorithm** for $\mathcal{C}$ which corrects up to t **errors**.

Public Key: $\mathcal{K}_{\text{pub}} = (G, t)$
Private Key: $\mathcal{K}_{\text{secret}} = (\mathcal{A}_{\mathcal{C}})$

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\text{ENCRYPT}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

where $\mathbf{e}$ is a random error vector of weight at most t.

Encryption Algorithm:

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

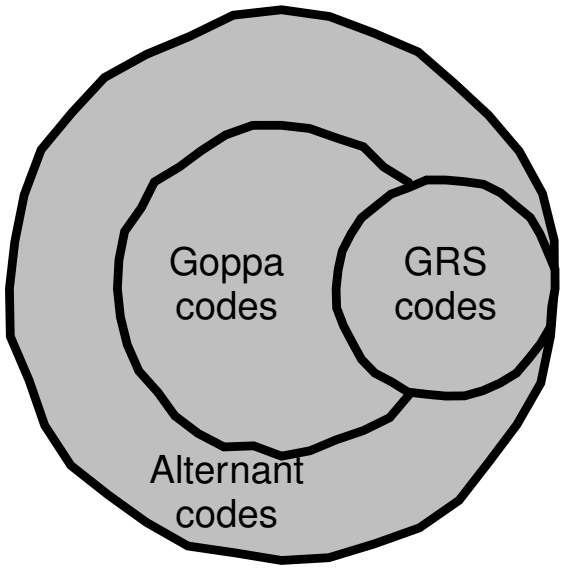
$$\text{ENCRYPT}(\mathbf{m}) = \mathbf{m}G + \mathbf{e} = \mathbf{y}$$

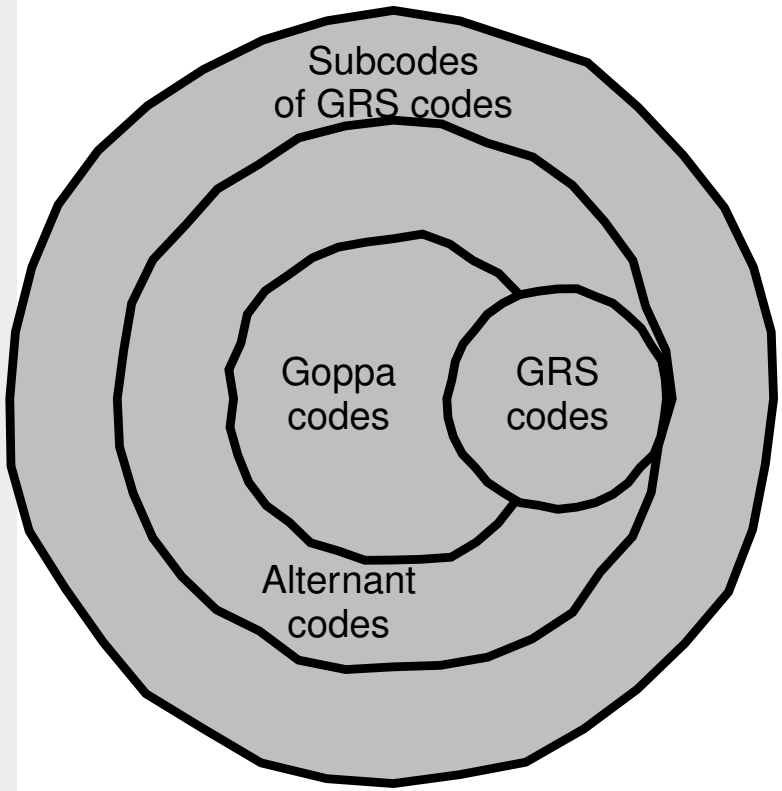
where $\mathbf{e}$ is a random error vector of weight at most t.

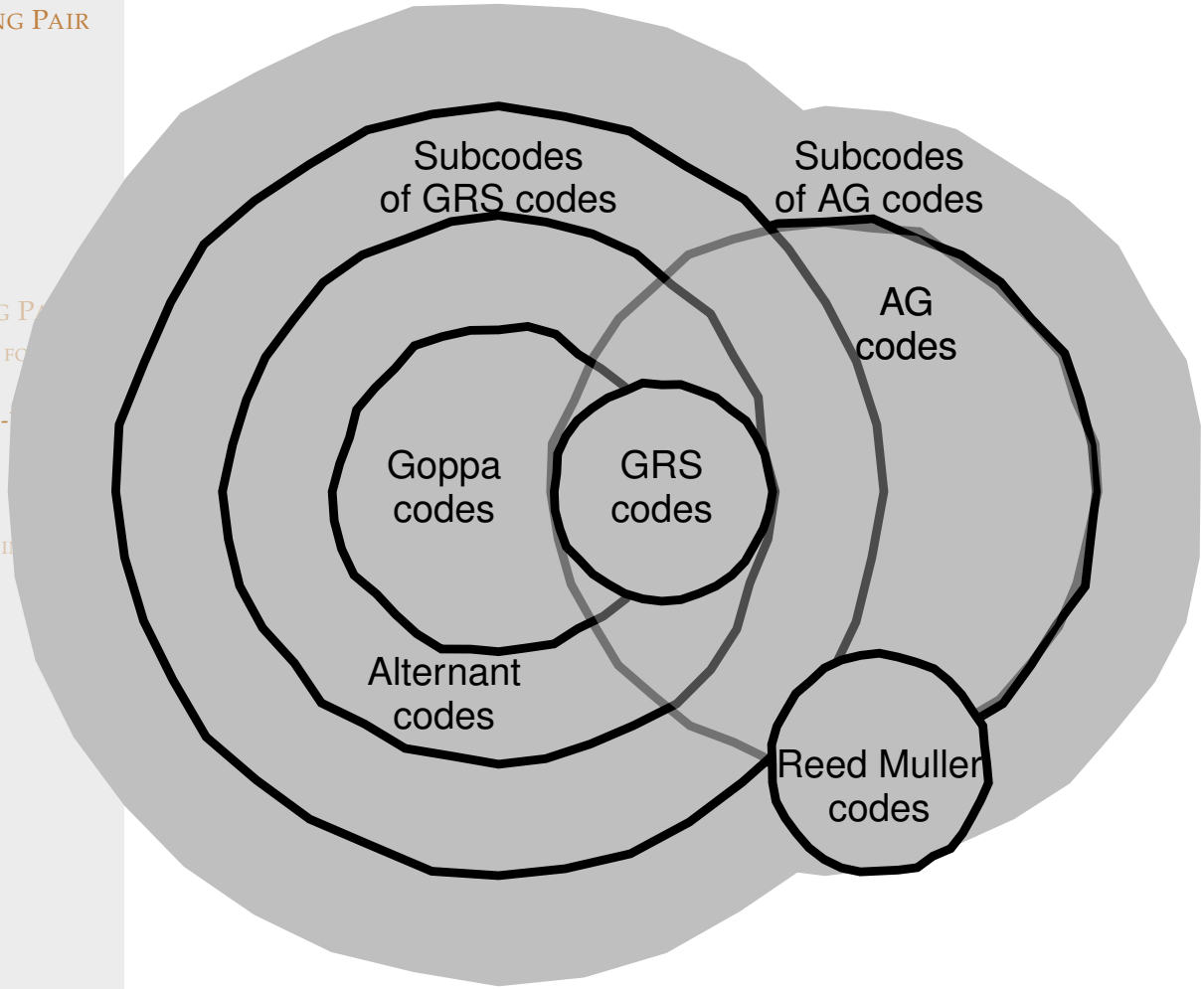
Decryption Algorithm:

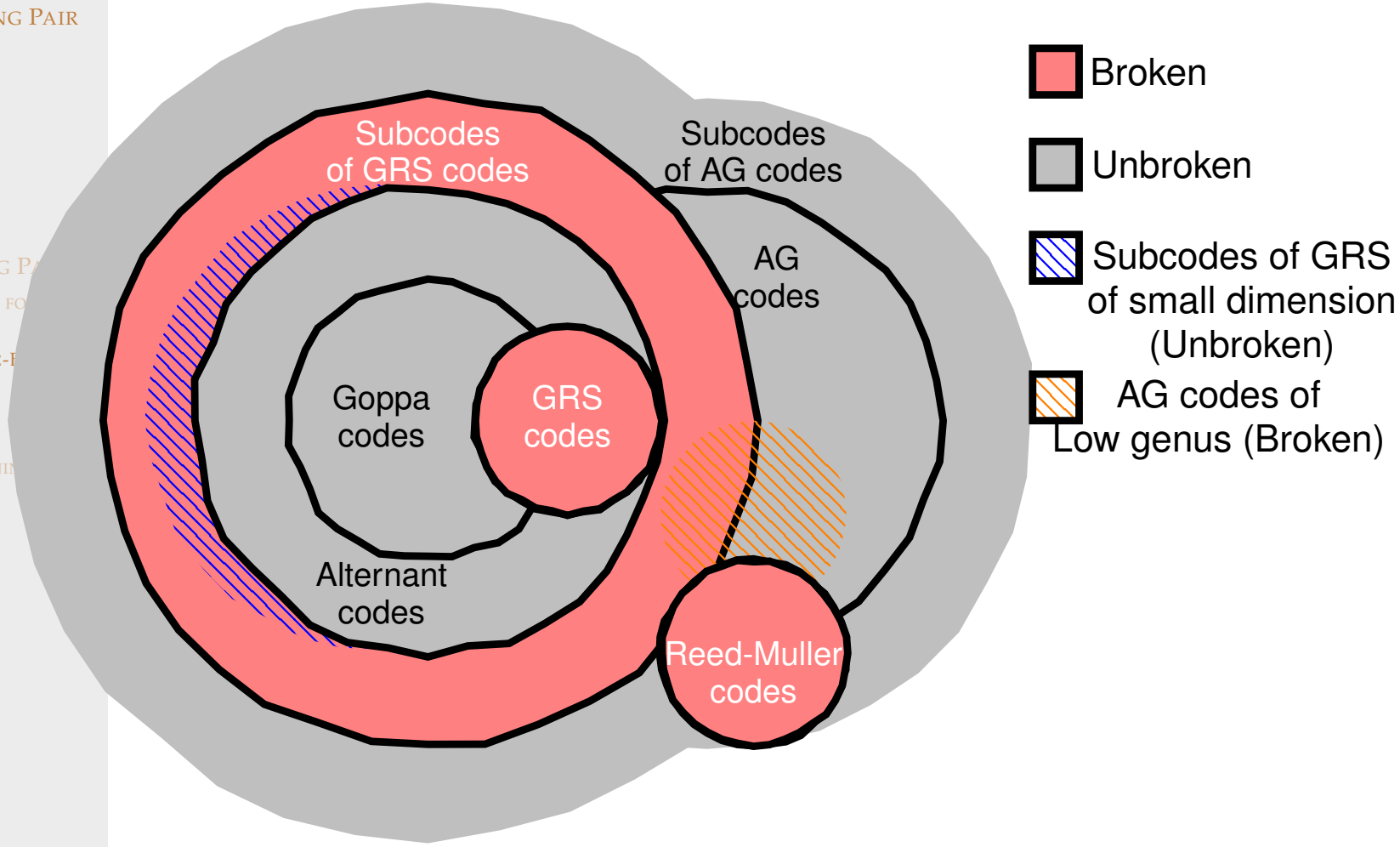
Using $\mathcal{K}_{secret}$, the receiver obtain $\mathbf{m}$.

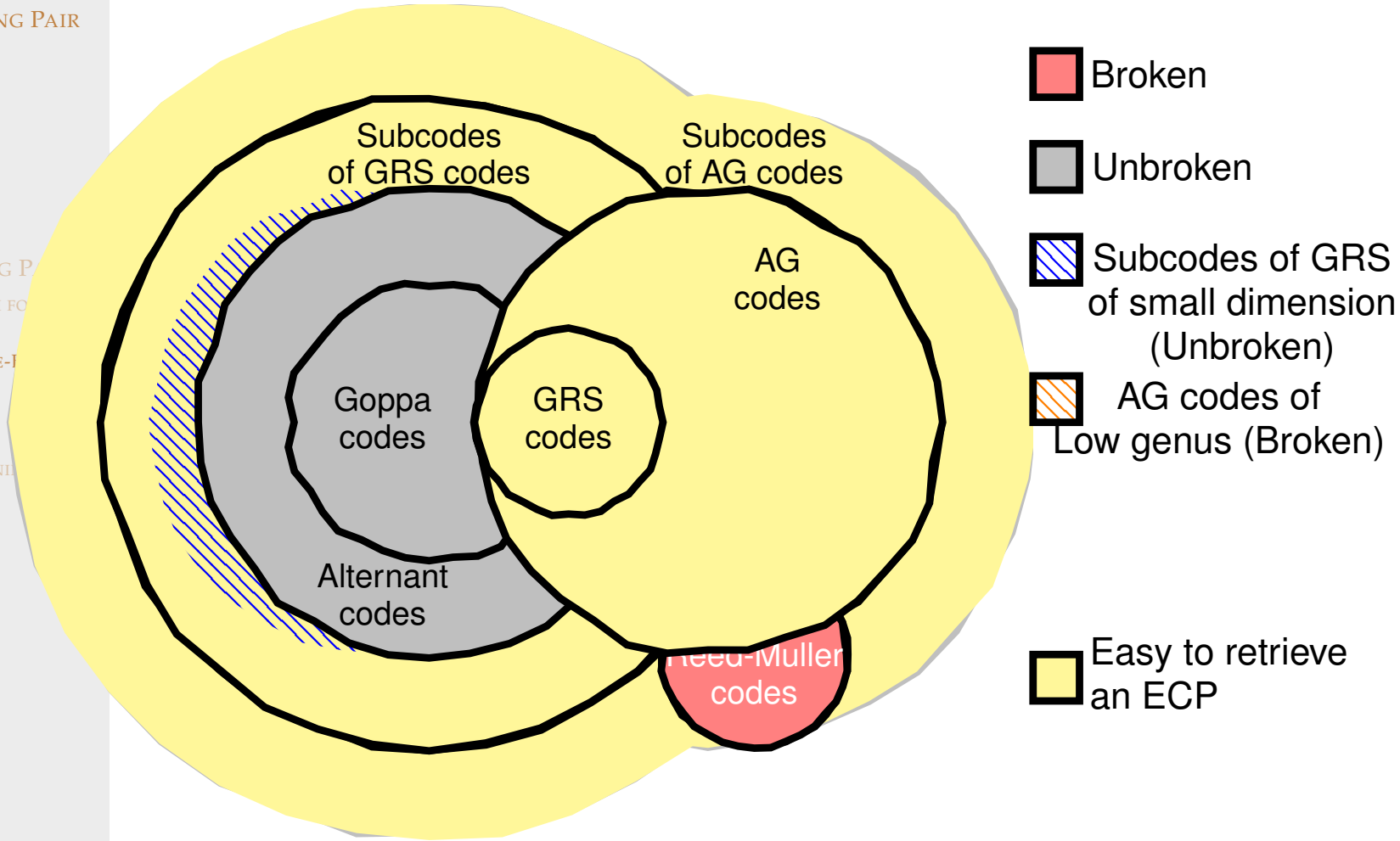
$$\text{DECRYPT}(\mathbf{y}) = \mathcal{A}_{\mathcal{C}}(\mathbf{y}) = \mathbf{m}$$

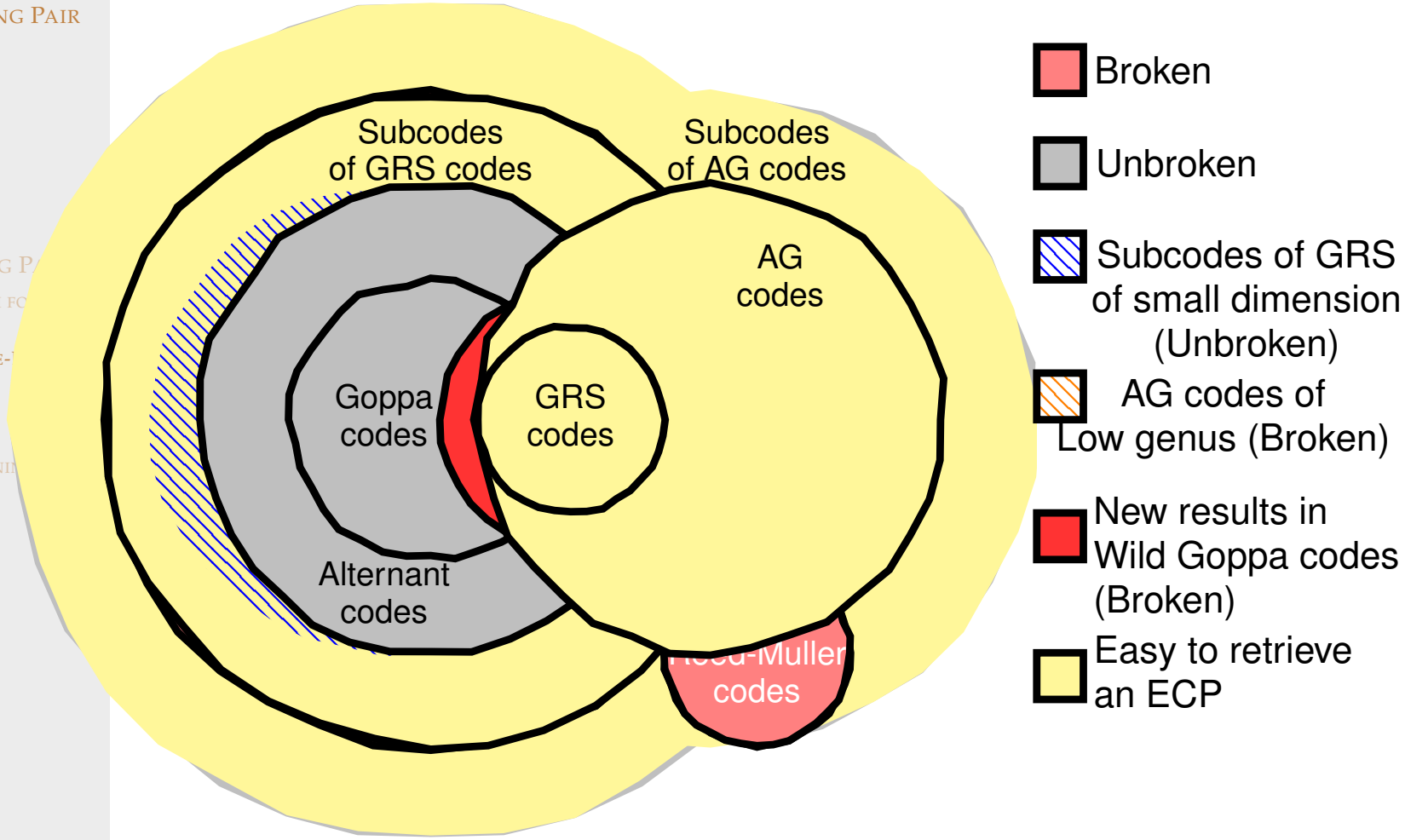












PUNCTURED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code

Punctured code

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$

PUNCTURED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

PUNCTURED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

PUNCTURED CODE $\mathcal{C}_J$

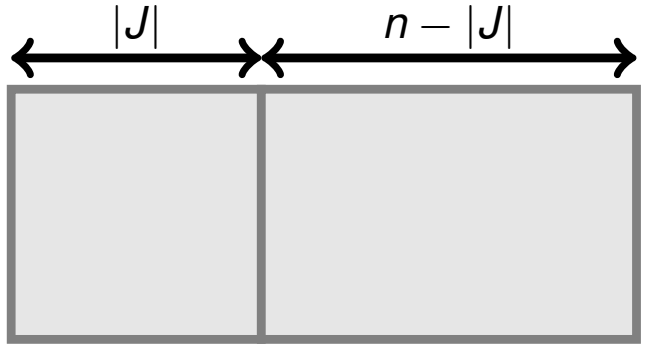
The words of $\mathcal{C}_J$ are codewords of $\mathcal{C}$ restricted to the positions of $\overline{J}$, i.e.

$$\mathcal{C}_J = \{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C}\}$$

PUNCTURED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

$G =$ 

PUNCTURED CODE $\mathcal{C}_J$

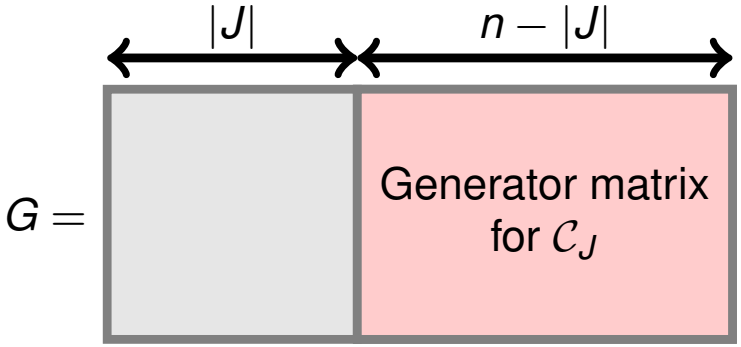
The words of $\mathcal{C}_J$ are codewords of $\mathcal{C}$ restricted to the positions of $\overline{J}$, i.e.

$$\mathcal{C}_J = \{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C}\}$$

PUNCTURED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J



PUNCTURED CODE $\mathcal{C}_J$

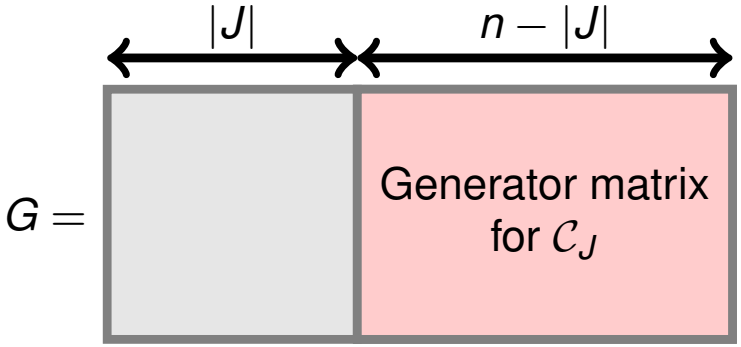
The words of $\mathcal{C}_J$ are codewords of $\mathcal{C}$ restricted to the positions of $\overline{J}$, i.e.

$$\mathcal{C}_J = \{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C}\}$$

PUNCTURED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J



PUNCTURED CODE $\mathcal{C}_J$

The words of $\mathcal{C}_J$ are codewords of $\mathcal{C}$ restricted to the positions of $\overline{J}$, i.e.

$$\mathcal{C}_J = \{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C}\}$$

PARAMETERS OF THE PUNCTURED CODE

The punctured code $\mathcal{C}_J$ is an $[n(\mathcal{C}) - |J|, k(\mathcal{C}_J), d(\mathcal{C}_J)]$ code with:

$$d(\mathcal{C}) - |J| \leq d(\mathcal{C}_J) \leq d(\mathcal{C}) \quad \text{and} \quad k(\mathcal{C}) - |J| \leq k(\mathcal{C}_J) \leq k(\mathcal{C})$$

SHORTENED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

SHORTENED CODE

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

SHORTENED CODE $\mathcal{C}^J$

The words of $\mathcal{C}^J$ are codewords of $\mathcal{C}$ that have a zero in the J-locations, i.e.

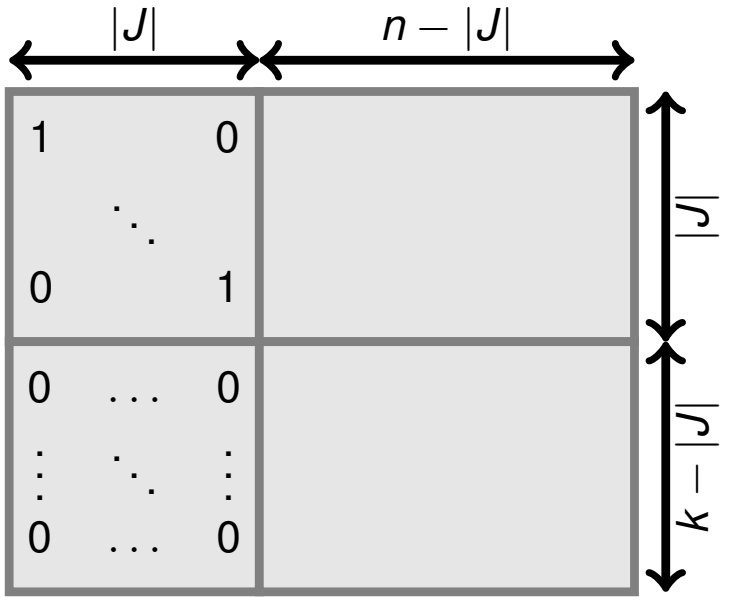
$$\mathcal{C}^J = \left\{ \mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C} \text{ and } c_j = 0 \text{ for all } j \in J \right\}$$

Shortened code

Let:

- $\mathcal{C}$ be an $[n,k]_q$ code
- $(J,\overline{J})$ be a partition of $\{1,\dots,n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

$$G = \left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & \\ \hline 0 & \dots & 0 & \\ \vdots & \ddots & \vdots & \\ 0 & \dots & 0 & \end{array}\right] \begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} |J| \\ \\ \\ \\ \\ k-|J| \end{matrix}$$



Shortened code $\mathcal{C}^J$

The words of $\mathcal{C}^J$ are codewords of $\mathcal{C}$ that have a zero in the J-locations, i.e.

$$\mathcal{C}^J = \{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C} \text{ and } c_j = 0 \text{ for all } j \in J\}$$

Shortened code

Let:

- $\mathcal{C}$ be an $[n,k]_q$ code
- $(J,\overline{J})$ be a partition of $\{1,\ldots,n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

$$G = \left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & \\ \hline 0 & \ldots & 0 & \\ \vdots & \ddots & \vdots & \text{Generator matrix for } \mathcal{C}^J \\ 0 & \ldots & 0 & \end{array}\right) \begin{array}{l} \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{l} |J| \\ \\ \\ \\ \\ k-|J| \end{array}$$

$|J|$ and $n-|J|$ mark the column blocks; $|J|$ and $k-|J|$ mark the row blocks.

Shortened code $\mathcal{C}^J$

The words of $\mathcal{C}^J$ are codewords of $\mathcal{C}$ that have a zero in the J-locations, i.e.

$$\mathcal{C}^J = \left\{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C} \text{ and } c_j = 0 \text{ for all } j \in J\right\}$$

Shortened code

Let:

- $\mathcal{C}$ be an $[n, k]_q$ code
- $(J, \overline{J})$ be a partition of $\{1, \ldots, n\}$
- $\mathbf{x}_J$ the **restriction** of $\mathbf{x} \in \mathbb{F}_q^n$ to the coordinates indexed by J

$$G = \left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & \\ 0 & & 1 & \\ \hline 0 & \ldots & 0 & \\ \vdots & \ddots & \vdots & \text{Generator matrix for } \mathcal{C}^J \\ 0 & \ldots & 0 & \end{array}\right)$$

with $|J|$ columns on the left block, $n - |J|$ columns on the right block, $|J|$ rows on the top block, and $k - |J|$ rows on the bottom block.

Shortened code $\mathcal{C}^J$

The words of $\mathcal{C}^J$ are codewords of $\mathcal{C}$ that have a zero in the J-locations, i.e.

$$\mathcal{C}^J = \{\mathbf{c}_{\overline{J}} \mid \mathbf{c} \in \mathcal{C} \text{ and } c_j = 0 \text{ for all } j \in J\}$$

Parameters of the shortened code

The punctured code $\mathcal{C}^J$ is an $[n(\mathcal{C}) - |J|, k(\mathcal{C}^J), d(\mathcal{C}^J)]$ code with:

$$d(\mathcal{C}) - |J| \leq d(\mathcal{C}^J) \quad \text{and} \quad k(\mathcal{C}) - |J| \leq k(\mathcal{C}^J) \leq k(\mathcal{C})$$

Puncturing and Shortening an MDS code

Lemma 1

Let:

- $\mathcal{C}$ be an **MDS** code
- J be a subset of $\{1, \ldots, n\}$ with $n(\mathcal{C}) - |J| \geq k(\mathcal{C})$

Then:

$\mathcal{C}_J$ and $\mathcal{C}^J$ **are MDS codes**

Puncturing and Shortening an MDS code

Lemma 1

Let:

- $\mathcal{C}$ be an **MDS** code
- J be a subset of $\{1, \ldots, n\}$ with $n(\mathcal{C}) - |J| \geq k(\mathcal{C})$

Then:

$\mathcal{C}_J$ and $\mathcal{C}^J$ **are MDS codes**

$\mathcal{C}_J : [n(\mathcal{C}) - |J|, k(\mathcal{C})]$

PUNCTURING AND SHORTENING AN MDS CODE

LEMMA 1

Let:

- $\mathcal{C}$ be an **MDS** code
- J be a subset of $\{1, \ldots, n\}$ with $n(\mathcal{C}) - |J| \geq k(\mathcal{C})$

Then:

$\mathcal{C}_J$ and $\mathcal{C}^J$ **are MDS codes**

$\mathcal{C}_J : [n(\mathcal{C}) - |J|, k(\mathcal{C})]$

$\mathcal{C}^J : [n(\mathcal{C}) - |J|, k(\mathcal{C}) - |J|]$

Gluing Property

Proposition: The Gluing Property

Let:

- $\mathcal{C}$ be an $[n, k]$ **MDS** code.
- I and J **disjoint** subsets of $\{1, \ldots, n\}$ with $2 \leq k \leq n - |I \cup J| - 2$.

If C_I and C_J are GRS codes. Then, $\mathcal{C}$ is a GRS code.

$2 \leq k(\mathcal{C}) \leq n - |I \cup J| - 2$ IS NECESSARY!!!

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\Longleftrightarrow$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\Longleftrightarrow$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

Well known result:
GRS codes of dimension $r + 1$ can be described as a projective system of points on a **rational normal curve** of degree r in $\mathbb{P}^r(\mathbb{F}_q)$.

$2 \leq k(\mathcal{C}) \leq n - |I \cup J| - 2$ IS NECESSARY!!!

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\Longleftrightarrow$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

Well known result:
GRS codes of dimension $r + 1$ can be described as a projective system of points on a **rational normal curve** of degree r in $\mathbb{P}^r(\mathbb{F}_q)$.

EXAMPLE:

Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two irreducible conics in $\mathbb{P}^2(\mathbb{F}_q)$
(i.e. rational normal curves of degree 2 in $\mathbb{P}^2(\mathbb{F}_q)$).

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\Longleftrightarrow$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

Well known result:
GRS codes of dimension $r+1$ can be described as a projective system of points on a **rational normal curve** of degree r in $\mathbb{P}^r(\mathbb{F}_q)$.

EXAMPLE:

Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two irreducible conics in $\mathbb{P}^2(\mathbb{F}_q)$
(i.e. rational normal curves of degree 2 in $\mathbb{P}^2(\mathbb{F}_q)$).

- **By Bezout's Theorem:** They intersect in at most 4 points.
  We assume that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ intersect in 4 points: P_3, P_4, P_5, P_6

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\iff$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

Well known result:
GRS codes of dimension $r + 1$ can be described as a projective system of points on a **rational normal curve** of degree r in $\mathbb{P}^r(\mathbb{F}_q)$.

EXAMPLE:

Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two irreducible conics in $\mathbb{P}^2(\mathbb{F}_q)$
(i.e. rational normal curves of degree 2 in $\mathbb{P}^2(\mathbb{F}_q)$).

- **By Bezout's Theorem:** They intersect in at most 4 points.
  We assume that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ intersect in 4 points: P_3, P_4, P_5, P_6
- Let $P_1, P_2 \in \mathcal{Q}_1(\mathbb{F}_q) \setminus \mathcal{Q}_2(\mathbb{F}_q)$.

$2 \leq k(\mathcal{C}) \leq n - |I \cup J| - 2$ IS NECESSARY!!!

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\Longleftrightarrow$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

Well known result:
GRS codes of dimension $r+1$ can be described as a projective system of points on a **rational normal curve** of degree r in $\mathbb{P}^r(\mathbb{F}_q)$.

EXAMPLE:

Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two irreducible conics in $\mathbb{P}^2(\mathbb{F}_q)$
(i.e. rational normal curves of degree 2 in $\mathbb{P}^2(\mathbb{F}_q)$).

- **By Bezout's Theorem:** They intersect in at most 4 points.
  We assume that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ intersect in 4 points: P_3, P_4, P_5, P_6
- Let $P_1, P_2 \in \mathcal{Q}_1(\mathbb{F}_q) \setminus \mathcal{Q}_2(\mathbb{F}_q)$.
- Let $P_7, P_8 \in \mathcal{Q}_2(\mathbb{F}_q) \setminus \mathcal{Q}_1(\mathbb{F}_q)$.

$2 \leq k(\mathcal{C}) \leq n - |I \cup J| - 2$ IS NECESSARY!!!

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\Longleftrightarrow$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

Well known result:
GRS codes of dimension $r+1$ can be described as a projective system of points on a **rational normal curve** of degree r in $\mathbb{P}^r(\mathbb{F}_q)$.

EXAMPLE:

Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two irreducible conics in $\mathbb{P}^2(\mathbb{F}_q)$
(i.e. rational normal curves of degree 2 in $\mathbb{P}^2(\mathbb{F}_q)$).

- **By Bezout's Theorem:** They intersect in at most 4 points.
  We assume that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ intersect in 4 points: P_3, P_4, P_5, P_6
- Let $P_1, P_2 \in \mathcal{Q}_1(\mathbb{F}_q) \setminus \mathcal{Q}_2(\mathbb{F}_q)$.
- Let $P_7, P_8 \in \mathcal{Q}_2(\mathbb{F}_q) \setminus \mathcal{Q}_1(\mathbb{F}_q)$.
  We define $\mathcal{C}$ as the [8,3,6] MDS code defined by $\mathcal{P} = (P_1, \ldots, P_8)$

LINEAR CODES VS. PROJECTIVE SYSTEMS

$\mathcal{P} = (P_1, \ldots, P_n)$
Projective System in $\mathbb{P}^r(\mathbb{F}_q)$
with $P_i = (p_{0i} : p_{1i} : \ldots : p_{ri})$

$\iff$

Code defined by
$G_P = \begin{pmatrix} P_1 & \cdots & P_n \end{pmatrix} \in \mathbb{F}_q^{r \times n}$

Well known result:
GRS codes of dimension $r+1$ can be described as a projective system of points on a **rational normal curve** of degree r in $\mathbb{P}^r(\mathbb{F}_q)$.

EXAMPLE:

Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be two irreducible conics in $\mathbb{P}^2(\mathbb{F}_q)$
(i.e. rational normal curves of degree 2 in $\mathbb{P}^2(\mathbb{F}_q)$).

- **By Bezout's Theorem:** They intersect in at most 4 points.
  We assume that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ intersect in 4 points: P_3, P_4, P_5, P_6
- Let $P_1, P_2 \in \mathcal{Q}_1(\mathbb{F}_q) \setminus \mathcal{Q}_2(\mathbb{F}_q)$.
- Let $P_7, P_8 \in \mathcal{Q}_2(\mathbb{F}_q) \setminus \mathcal{Q}_1(\mathbb{F}_q)$.
  We define $\mathcal{C}$ as the [8,3,6] MDS code defined by $\mathcal{P} = (P_1, \ldots, P_8)$
- Let $J_1 = \{1, 2\}$ and $J_2 = \{7, 8\}$.
  $\mathcal{C}_{J_1}$ and $\mathcal{C}_{J_2}$ are GRS codes but $\mathcal{C}$ is not a GRS code.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \left\{ 0, 1, n(\mathcal{C})-1, n(\mathcal{C}) \right\}$ are dealt separately.

   Trivial codes: $\mathbf{0}$ and $\mathbb{F}_q^n = \mathbf{0}^{\perp}$

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.

   Trivial codes: $\mathbf{0}$ and $\mathbb{F}_q^n = \mathbf{0}^\perp$

   Codes: $\mathrm{GRS}_1(\mathbf{a}, \mathbf{b})$ and $\mathrm{GRS}_1(\mathbf{a}, \mathbf{b})^\perp$

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**

THEOREM: [PELLIKAAN (1996)]

If $\mathcal{C}$ is an $[n, n-4, 5]_q$ code with a 2-ECP then $\mathcal{C}$ is a GRS code.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$$\mathcal{C} \text{ is a GRS code}$$

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.
   - Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ code that has a t-ECP.

THEOREM: [PELLIKAAN (1996)]

If $\mathcal{C}$ is an $[n, n-2t, 2t+1]_q$ code and (A, B) is a t-ECP for $\mathcal{C}$.
W.l.o.g. we can assume that:

$$A \text{ is an } [n, t+1, n-t]_q \quad \text{and} \quad B \text{ is an } [n, t, n-t+1]_q$$

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.
   - Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ code that has a t-ECP.
   - We define:
     - ➜ $\mathcal{C}_{J_1}$ with $J_1 = \{n-1, n\}$. By **Lemma 1**: $\mathcal{C}_{J_1}$ is an MDS code with parameters: $[n-2, n-2t, 2(t-1)-1]$
     - ➜ $A_1 = \left(A_{\{n\}}\right)^{\{n-1\}}$. By **Lemma 1**: A_1 is an MDS code
     - ➜ $B_1 = \left(B^{\{n\}}\right)_{\{n-1\}}$. By **Lemma 1:** B_1 is an MDS code

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.
   - Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ code that has a t-ECP.
   - We define:
     - ➜ $\mathcal{C}_{J_1}$ with $J_1 = \{n-1, n\}$. By **Lemma 1**: $\mathcal{C}_{J_1}$ is an MDS code with parameters: $[n-2, n-2t, 2(t-1)-1]$
     - ➜ $A_1 = \left(A_{\{n\}}\right)^{\{n-1\}}$. By **Lemma 1**: A_1 is an MDS code
     - ➜ $B_1 = \left(B^{\{n\}}\right)_{\{n-1\}}$. By **Lemma 1:** B_1 is an MDS code
     - ➜ (A_1, B_1) is a $(t-1)$-ECP for $\mathcal{C}_{J_1}$.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.
   - Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ code that has a t-ECP.
   - We define:
     - ➜ $\mathcal{C}_{J_1}$ with $J_1 = \{n-1, n\}$. By **Lemma 1**: $\mathcal{C}_{J_1}$ is an MDS code with parameters: $[n-2, n-2t, 2(t-1)-1]$
     - ➜ $A_1 = \left(A_{\{n\}}\right)^{\{n-1\}}$. By **Lemma 1**: A_1 is an MDS code
     - ➜ $B_1 = \left(B^{\{n\}}\right)_{\{n-1\}}$. By **Lemma 1:** B_1 is an MDS code
     - ➜ (A_1, B_1) is a $(t-1)$-ECP for $\mathcal{C}_{J_1}$.
       By **Induction hypothesis:** $\mathcal{C}_{J_1}$ is a GRS code.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.
   - Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ code that has a t-ECP.
   - We define:
     - ➜ $\mathcal{C}_{J_1}$ with $J_1 = \{n-1, n\}$. By **Lemma 1**: $\mathcal{C}_{J_1}$ is an MDS code with parameters:

       $$[n-2, n-2t, 2(t-1)-1]$$

       By **Induction hypothesis:** $\mathcal{C}_{J_1}$ is a GRS code.
     - ➜ $\mathcal{C}_{J_2}$ with $J_2 = \{1, 2\}$.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.
   - Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ code that has a t-ECP.
   - We define:
     - ➜ $\mathcal{C}_{J_1}$ with $J_1 = \{n-1, n\}$. By **Lemma 1**: $\mathcal{C}_{J_1}$ is an MDS code with parameters:
       $$[n-2, n-2t, 2(t-1)-1]$$
       By **Induction hypothesis:** $\mathcal{C}_{J_1}$ is a GRS code.
     - ➜ $\mathcal{C}_{J_2}$ with $J_2 = \{1, 2\}$.
       By **Induction hypothesis:** $\mathcal{C}_{J_2}$ is a GRS code.

MAIN THEOREM

MAIN RESULT:

Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ that has a t-ECP. Then,

$\mathcal{C}$ is a GRS code

Sketch of the proof:

1. The cases $k(\mathcal{C}) = \{0, 1, n(\mathcal{C})-1, n(\mathcal{C})\}$ are dealt separately.
2. We proceed by induction on t.
   - For $t = 1$ **Easy to check!**
   - For $t = 2$: **Already proved**
   - **Inductive Step:** We assume the theorem holds for $t' < t$.
   - Let $\mathcal{C}$ be an $[n, n-2t, 2t+1]_q$ code that has a t-ECP.
   - We define:
     - ➜ $\mathcal{C}_{J_1}$ with $J_1 = \{n-1, n\}$. By **Lemma 1**: $\mathcal{C}_{J_1}$ is an MDS code with parameters:
       $$[n-2, n-2t, 2(t-1)-1]$$
       By **Induction hypothesis:** $\mathcal{C}_{J_1}$ is a GRS code.
     - ➜ $\mathcal{C}_{J_2}$ with $J_2 = \{1, 2\}$.
       By **Induction hypothesis:** $\mathcal{C}_{J_2}$ is a GRS code.
   - By **Gluing Property:** $\mathcal{C}$ is a GRS code.

Second Proof - Using recent results of Mirandola-Zémor

Proposition

Let (A, B) be a pair of $\mathbb{F}_q$-linear codes of length n. Then:

$$d(A * B) \leq \max\{1, n - (\dim(A) + \dim(B)) + 2\}$$

(A, B) is a **Product MDS (PMDS)** if the **equality holds**.

Proposition

Let (A, B) be a PMDS pair of $\mathbb{F}_q$-linear code of length n. And assume that:

$$n > \dim(A) + \dim(B) \quad \text{and} \quad \dim(A), \dim(B) \geq 2$$

Then:

$$A, \quad B \quad \text{and} \quad A * B \quad \textbf{are GRS codes}$$

D. Mirandola and G. Zémor

Critical pairs for the Product Singleton Bound.
WCC 2015.

Conclusion

Main result

The class of MDS codes of minimum distance $2t + 1$ that have a t-ECP **coincides** with the class of GRS codes.

Future Question: What about AG codes of genus larger than **Zero**?

Thank you for your attention!