Error-correcting pairs for a public-key cryptosystem

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

[1] INRIA Rocquencourt - SECRET Team

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

IICMA 2015
The 3rd IndoMS International Conference on Mathematics and Its Applications

Depok, Indonesia, 3 November 2015

Public-key cryptography (PKC)

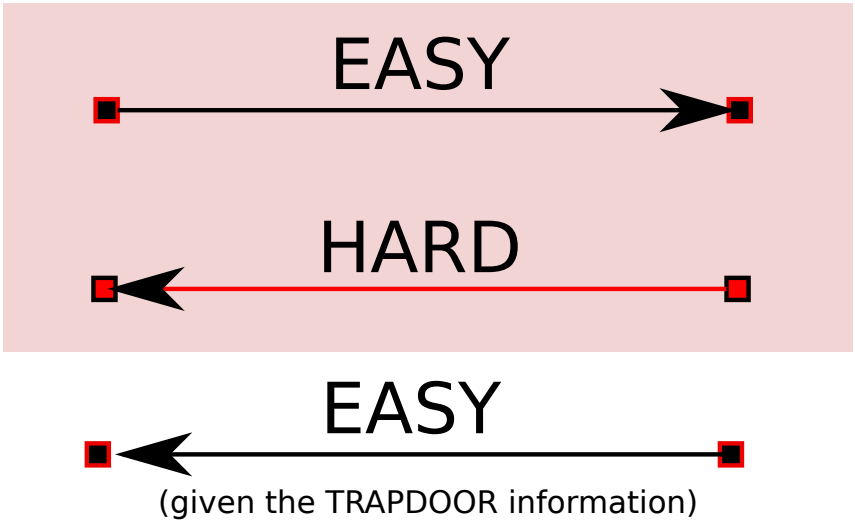
- Diffie and Hellman in 1976 in the public domain
- Ellis in 1970 for secret service, not made public until 1997
- advantage with respect to symmetric-key cryptography
- no exchange of secret key between sender and receiver

One-way function

- At the heart of any public-key cryptosystem is a
- one-way function
- a function $y = f(x)$ that is
- easy to evaluate but
- for which it is computationally infeasible, one hopes
- to find the inverse $x = f^{-1}(y)$

- Example
- differentiation a function is easy
- integrating a function is difficult

Public Key Cryptography



One-Way function

Trapdoor one-way function

Integer factorization

- $x = (p, q)$ is a pair of distinct prime numbers
- $y = pq$ is its product
- proposed by Cocks in 1973 in secret service
- Rivest-Shamir-Adleman (RSA) in 1978 in public domain
- based on the hardness of factorizing integers

Discrete logarithm

- G is a group (written multiplicatively)
- with $a \in G$ and x an integer
- $y = a^x$
- proposed by Williamson in 1974 in secret service
- Diffie-Hellman in 1974 and 1976 in public domain
- based on difficulty of finding discrete logarithms in a finite field

Most PKC are based on Number-theoretic problems

Most PKC are based on Number-theoretic problems

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

RSA

DSA

ECC

ECDSA

HECC

Most PKC are based on Number-theoretic problems

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

RSA

DSA

ECC

ECDSA

HECC

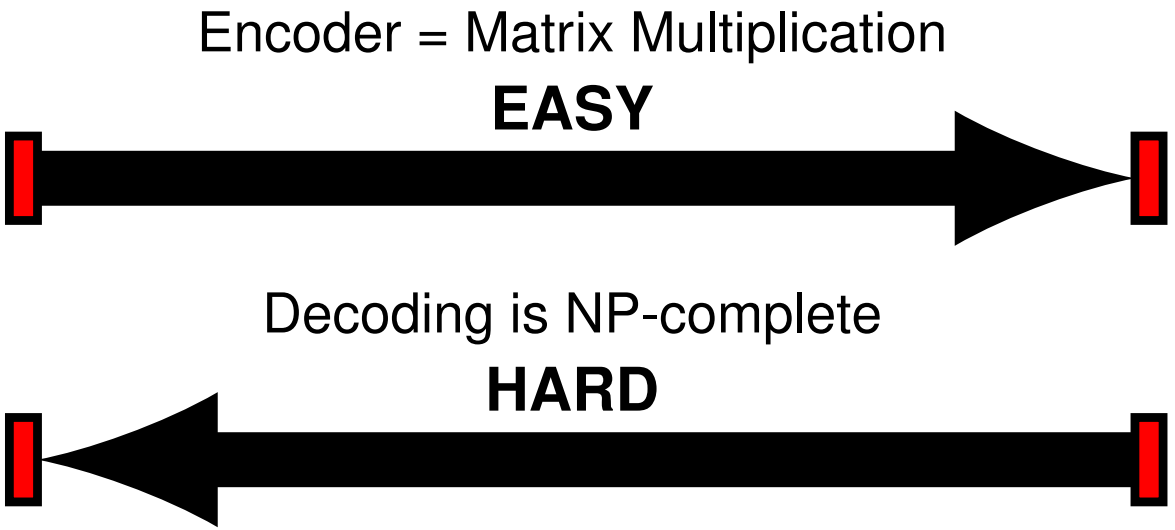
Code-based Cryptography is a powerful alternative

Code based cryptography

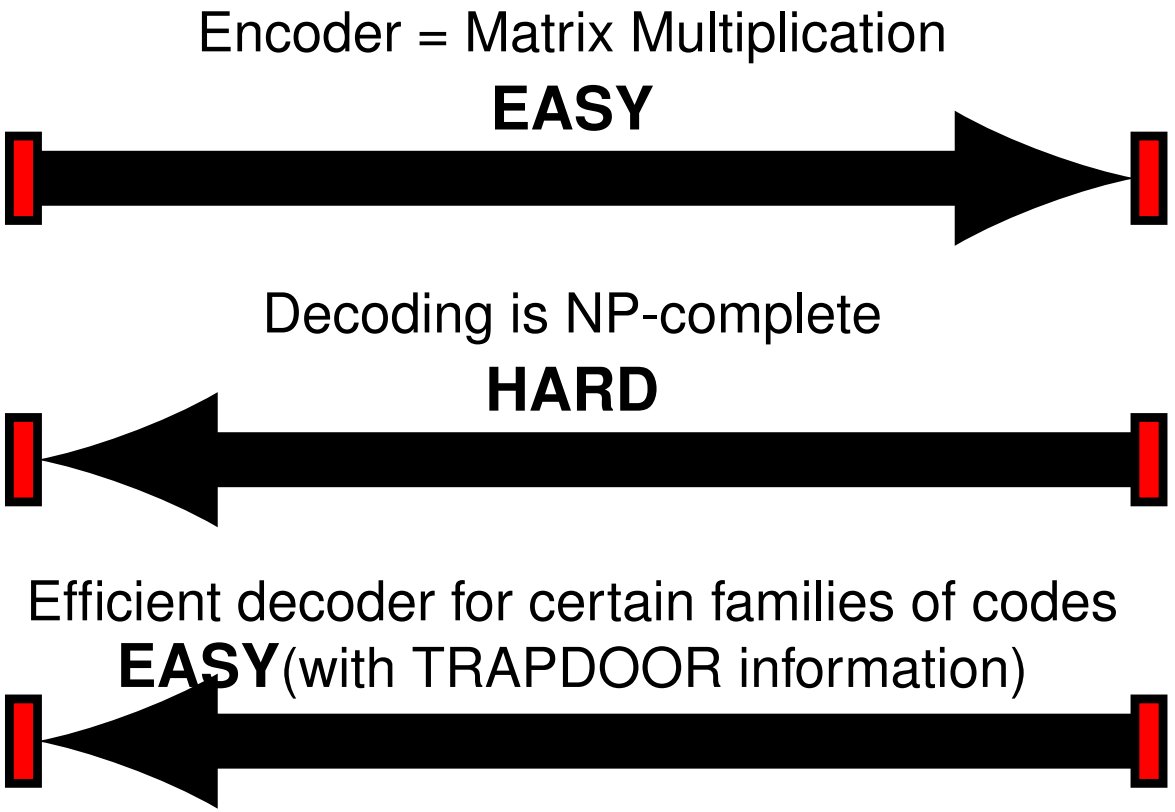
- $h_1, \ldots, h_n$ is a given n-tuple of vectors in $\mathbb{F}_q^r$
- x is an n-tuple of elements in $\mathbb{F}_q$
- $y = \sum_{j=1}^{n} x_j h_j$
- proposed by McEliece in 1978
- based on the difficulty of decoding error-correcting codes
- it is NP complete

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:

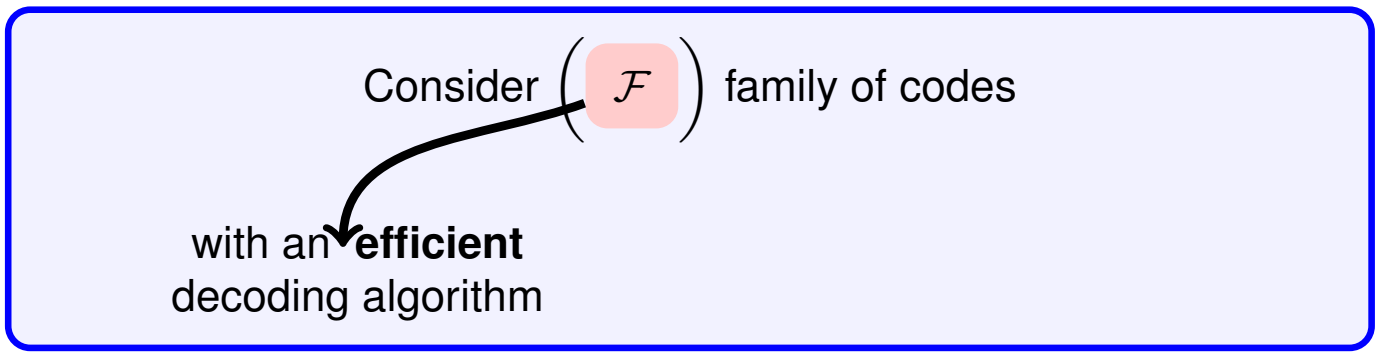
- Large key size.

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

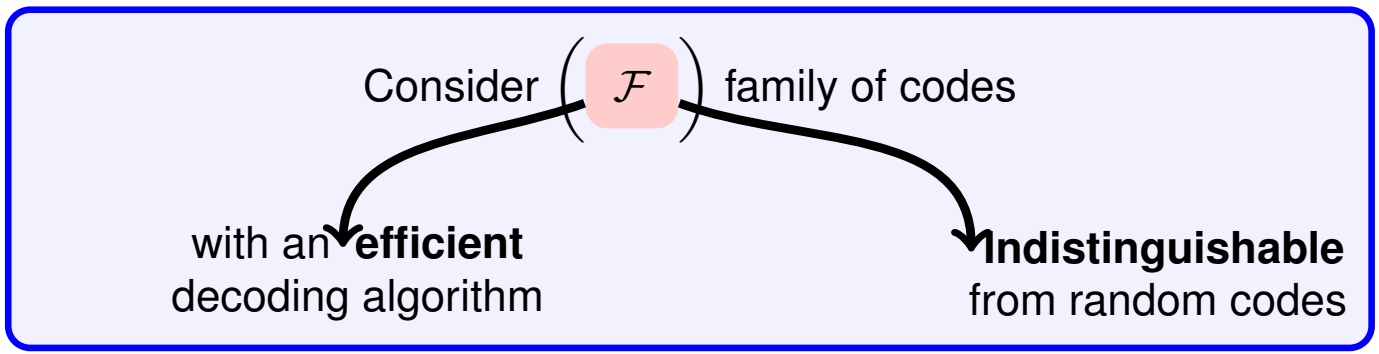
The McEliece Cryptosystem

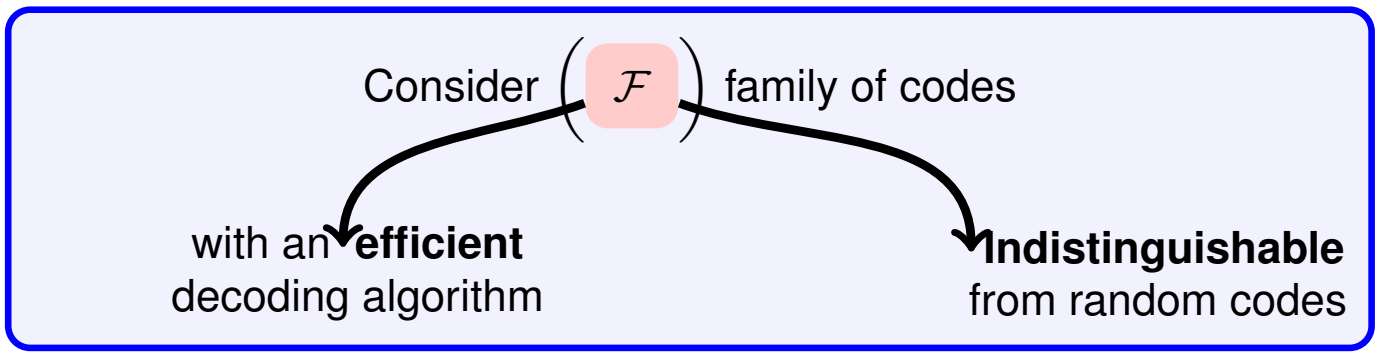
Consider $\left(\mathcal{F} \right)$ family of codes

The McEliece Cryptosystem



The McEliece Cryptosystem





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 $\mathbf{m}$.

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

Inner product and dual code

The inner product on $\mathbb{F}_q^n$ is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$$

This inner product is bilinear, symmetric and non-degenerate

For an $[n, k]_q$ code C we define the dual or orthogonal code $C^\perp$ as

$$C^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{c} \in C \}$$

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

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:

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

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 $d = n - k + 1$

$\mathcal{C}$ is **MDS** $\iff$ $\mathcal{C}^{\perp}$ is **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 $\left\{1, X, X^2, \ldots, X^{k-1}\right\}$

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

Canonical Generator matrix for GRS

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

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

$$
\begin{aligned}
G &= \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_1 & a_2 & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \ldots & a_n^{k-1} \end{pmatrix} \begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix} \\
&= \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ b_1 a_1 & b_2 a_2 & \ldots & b_n a_n \\ b_1 a_1^2 & b_2 a_2^2 & \ldots & b_n a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ b_1 a_1^{k-1} & b_2 a_2^{k-1} & \ldots & b_n a_n^{k-1} \end{pmatrix} = \begin{pmatrix} \mathbf{b} * \mathbf{1} \\ \mathbf{b} * \mathbf{a} \\ \mathbf{b} * \mathbf{a}^2 \\ \vdots \\ \mathbf{b} * \mathbf{a}^{k-1} \end{pmatrix} \in \mathbb{F}_q^{k \times n}
\end{aligned}
$$

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

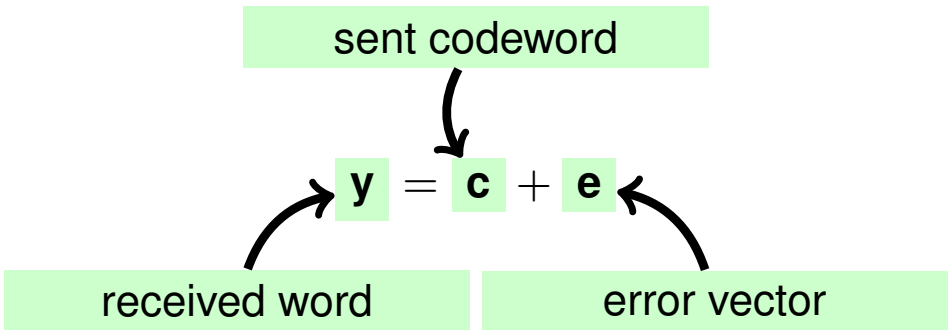
Consider the codes

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

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

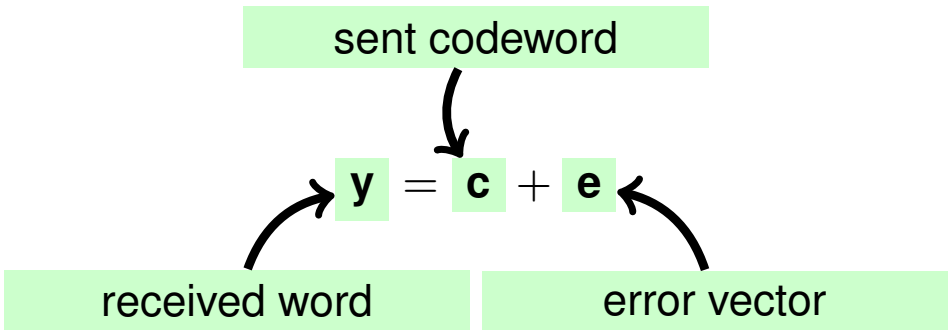
$\mathcal{A} = \mathrm{GRS}_{t+1}(\mathbf{c}, \mathbf{d}^{\perp})$ and $\mathcal{B} = \mathrm{GRS}_t(\mathbf{c}, \mathbf{1})$



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:

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

$K_y = K_e$**?**

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 $\mathbf{a} \in K_{\mathbf{y}}$

AN EFFICIENT DECODING ALGORITHM FOR GRS CODES

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

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

Indeed,

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

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 $w_H(\mathbf{e}) \leq t$, 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?

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,

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

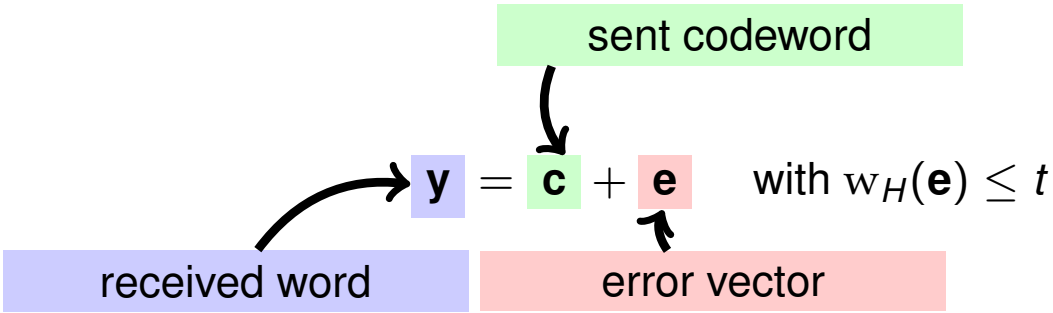
Then $\mathbf{e}_1 - \mathbf{e}_2 \in \mathcal{C}$, but

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

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

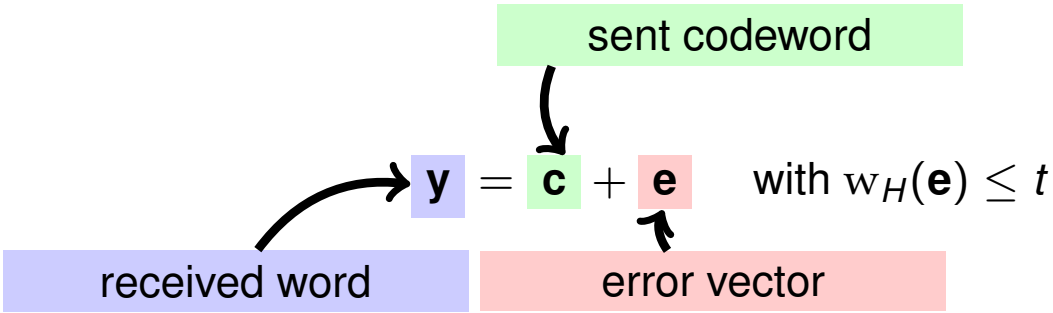
Error-correcting pairs (ECP)

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 $\mathcal{C}$.

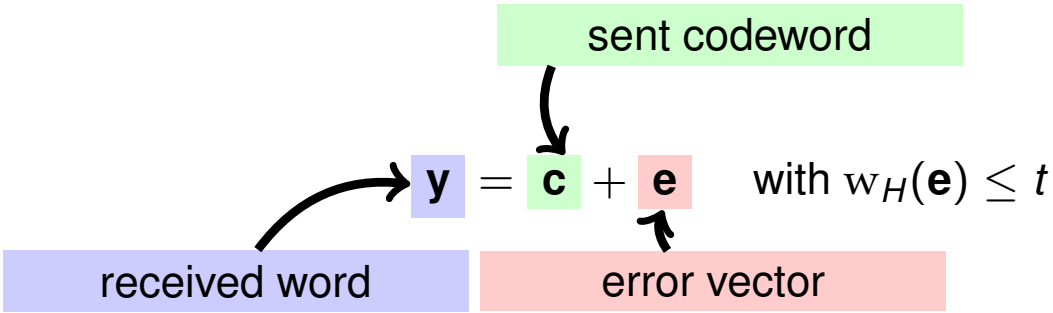


1. There exists $\mathbf{a} \in \mathcal{A}$, $\mathbf{a} \neq \mathbf{0}$ such that

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

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

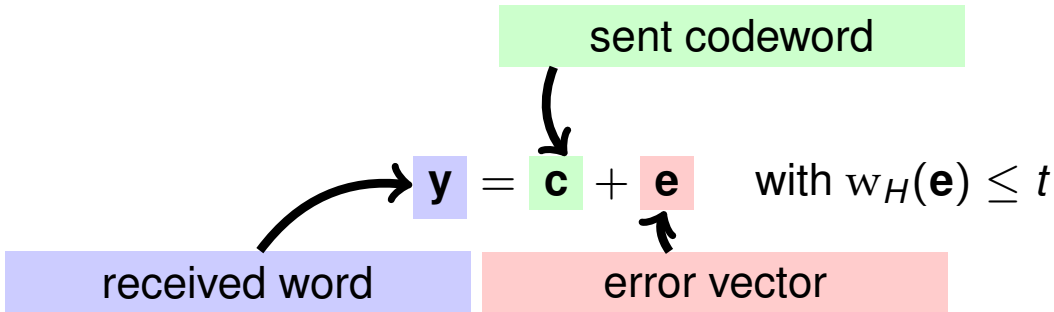
$$\langle \mathbf{y}, \mathbf{a} * \mathbf{b} \rangle = 0 \text{ for all } \mathbf{b} \in \mathcal{B} \tag{1}$$

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

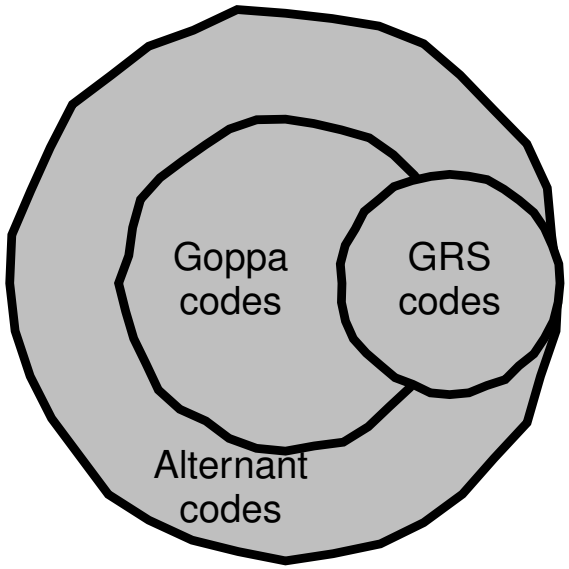
Decoding codes from curves and cyclic codes.
Ph.D thesis, Eindhoven University of Technology (1993)

I. Duursma, R. Kötter.

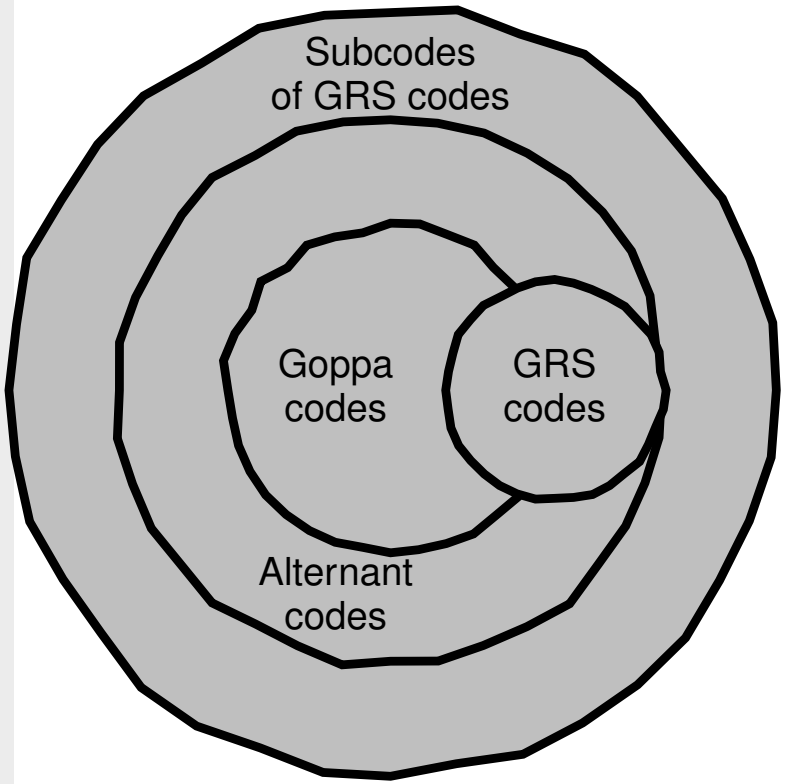
Error-locating pairs for cyclic codes.
IEEE Trans. Inform. Theory, Vol.40, 1108–1121 (1994)

Codes with a t-ECP

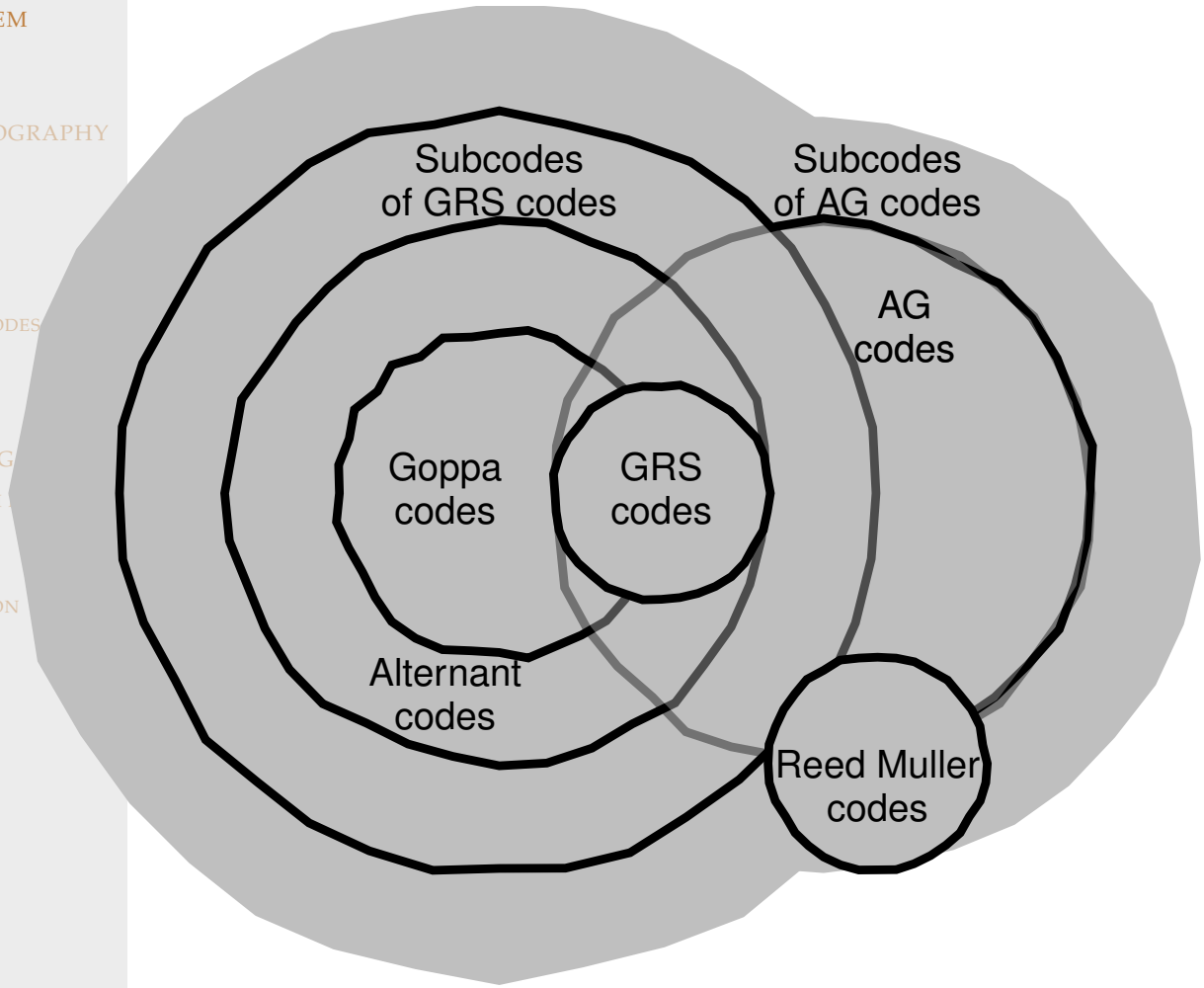
Codes with a t-ECP



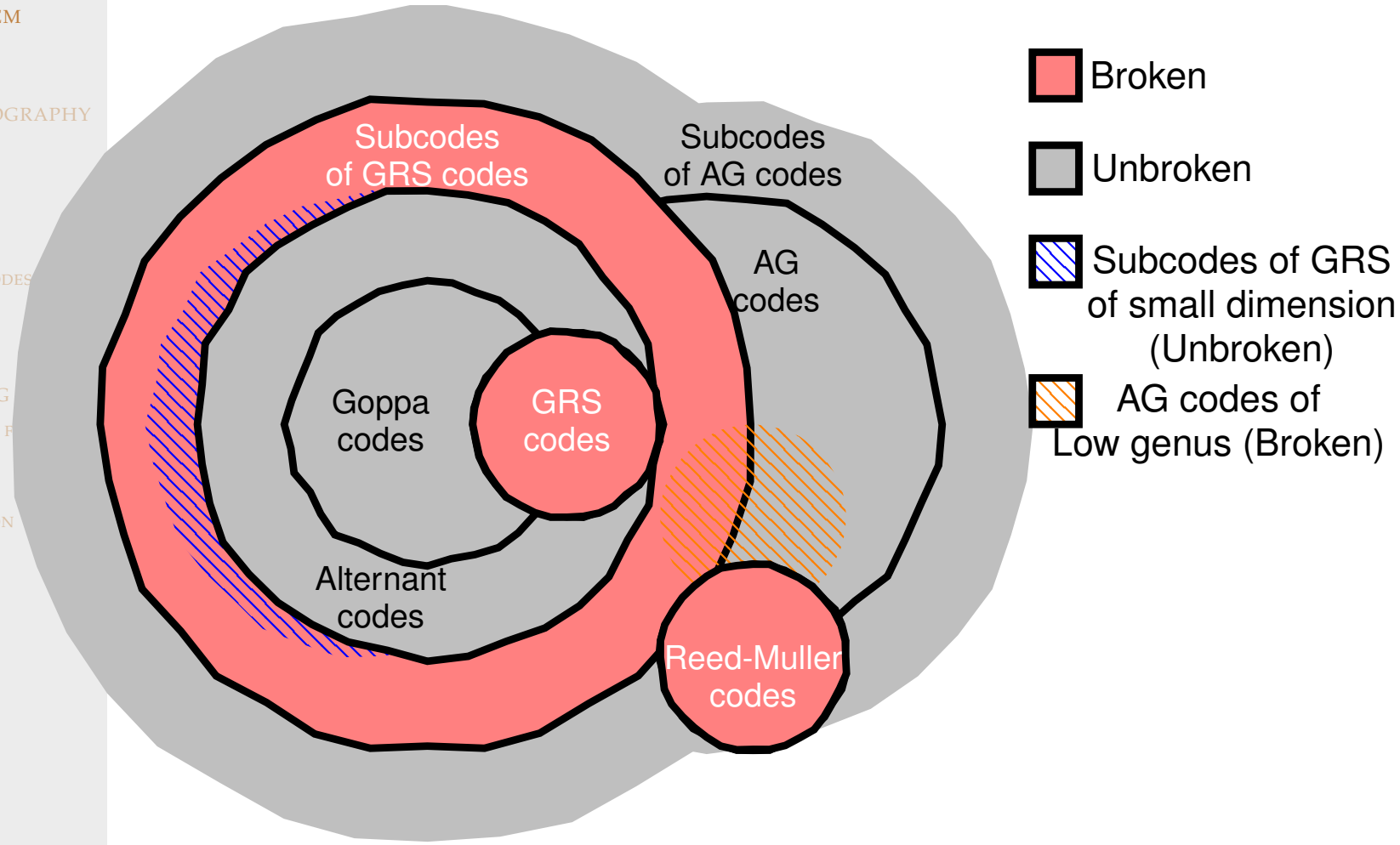
Codes with a t-ECP



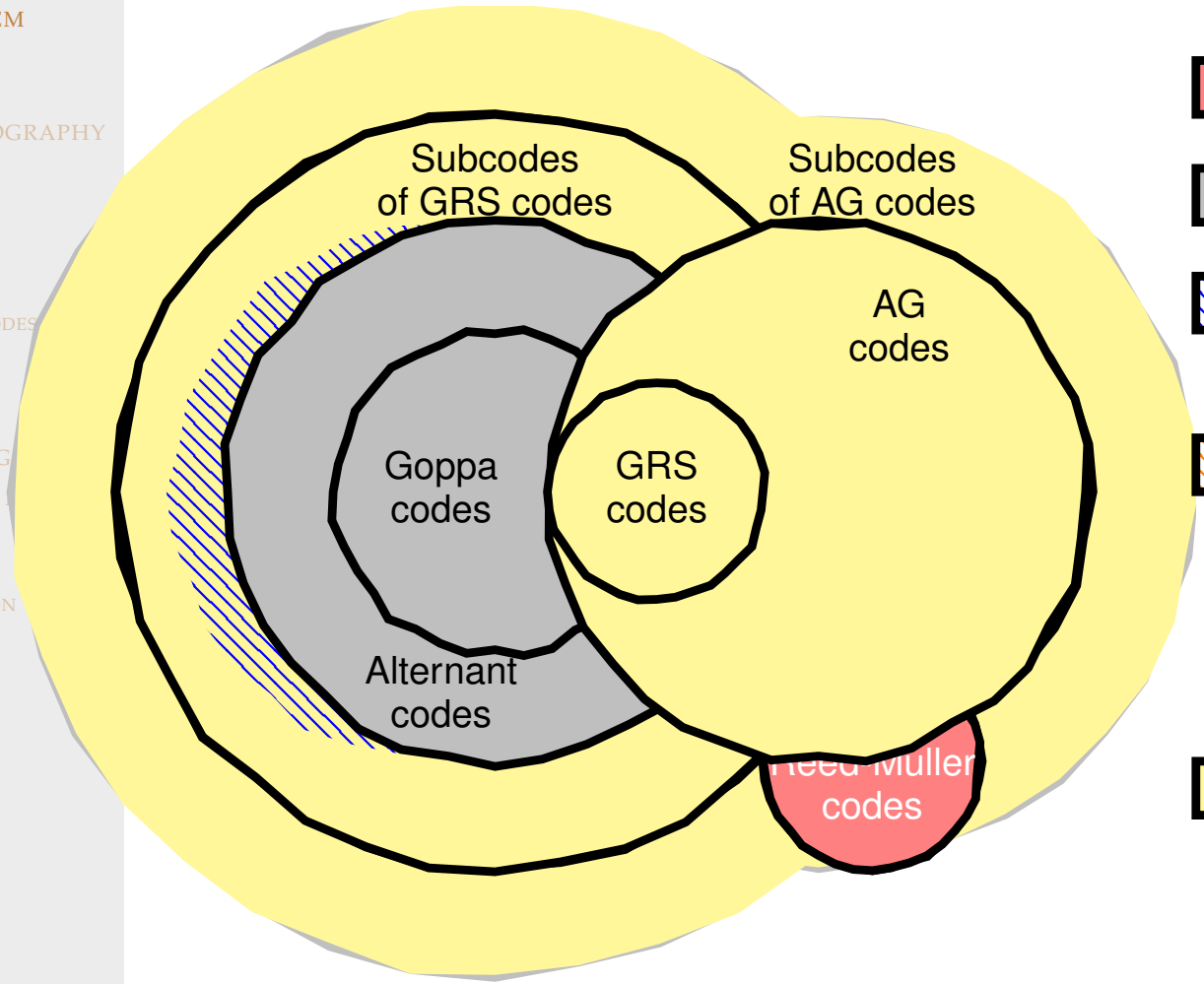
Codes with a t-ECP



Codes with a t-ECP



Codes with a t-ECP



Broken

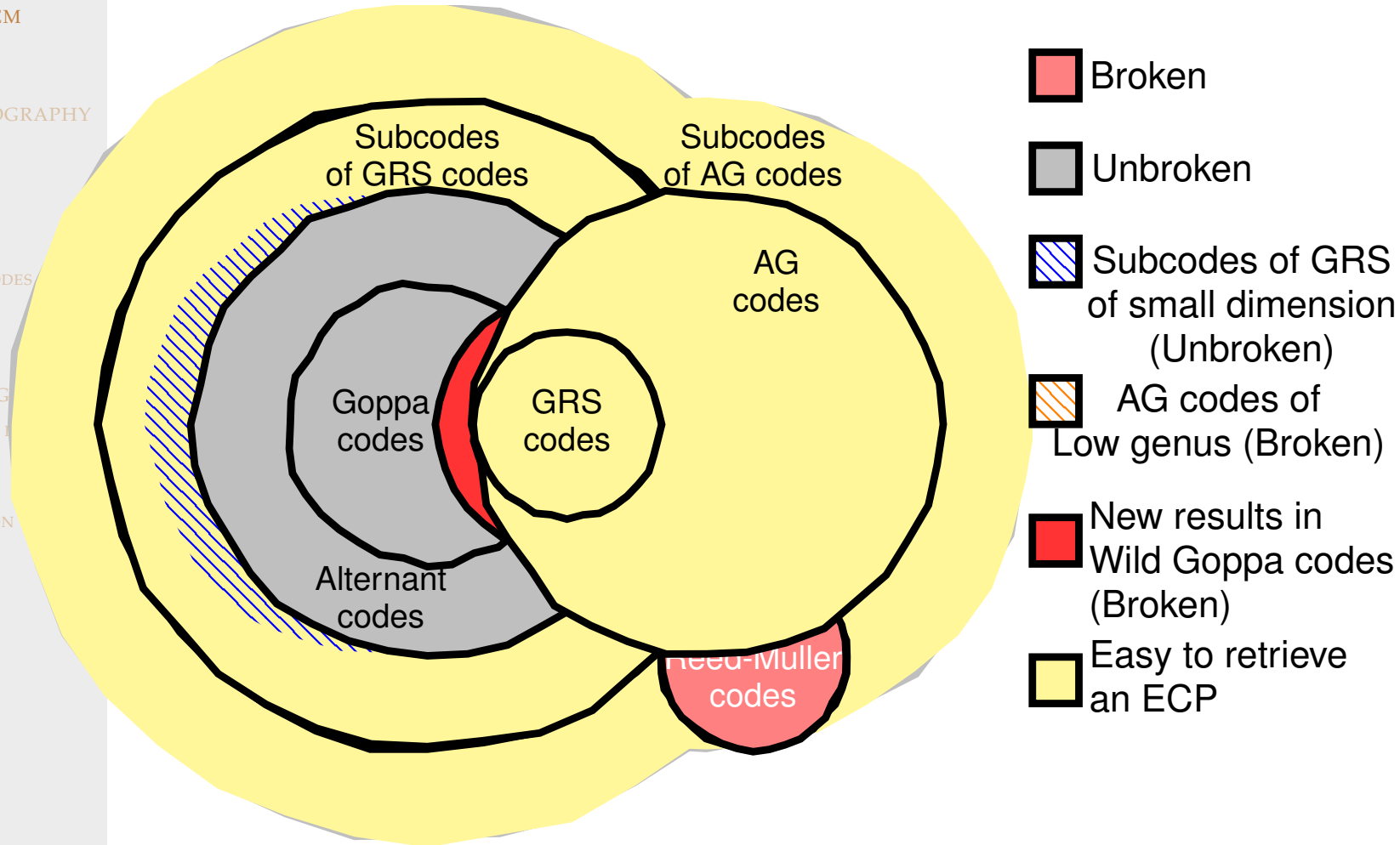
Unbroken

Subcodes of GRS of small dimension (Unbroken)

AG codes of Low genus (Broken)

Easy to retrieve an ECP

Codes with a t-ECP



ECP ONE-WAY FUNCTION

$\mathcal{P}(n, t, q)$ is the collection of pairs (A, B) that satisfy

$$\begin{array}{ll} E.2 \;\; k(A) > & E.5 \;\; d(A^{\perp}) > 1 \\ E.3 \;\; d(B^{\perp}) > t & E.6 \;\; d(A) + 2t > n \end{array}$$

Let

$$C = \mathbb{F}_q^n \cap (A * B)^{\perp}.$$

Then $d(C)$ is at least $2t + 1$ and (A, B) is a t-ECP for C

$\mathcal{F}(n, t, q)$ is the collection of $\mathbb{F}_q$-linear codes of length n and minimum distance $d \geq 2t + 1$

Consider the following map

$$\begin{array}{rccc} \varphi_{(n,t,q)} : & \mathcal{P}(n, t, q) & \longrightarrow & \mathcal{F}(n, t, q) \\ & (A, B) & \longmapsto & C \end{array}$$

The question is whether this map is a one-way function.

Conclusion

Main result

Many known classes of codes
that have have decoding algorithm correcting t-errors
have a t-ECP
and are not suitable for a code based PKC

Future Question: Is the ECP map a one-way function?

Thank you for your attention!