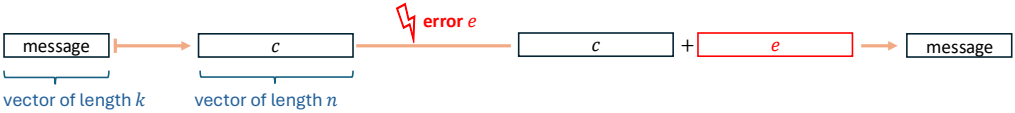
Linearised Chinese Remainder Codes

Camille Garnier
work with Olivier Ruatta and Philippe Gaborit

Introduction

Linear code

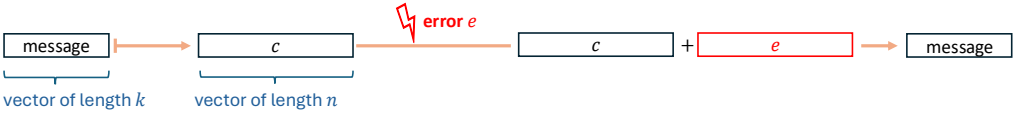
A **linear code** of dimension k and length n is a vector subspace of dimension k of $\mathbb{F}_q^n$.



Introduction

Linear code

A **linear code** of dimension k and length n is a vector subspace of dimension k of $\mathbb{F}_q^n$.



Classical metric for codes: Hamming metric.

Rank metric

Support in rank metric

If $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$, the **support of $\boldsymbol{v}$ in rank metric** is the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$ spanned by its coefficients:

$$\text{supp}(\boldsymbol{v}) = < v_1, \ \ldots \ , v_n >_{\mathbb{F}_q} .$$

Rank metric

Support in rank metric

If $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$, the **support of $\boldsymbol{v}$ in rank metric** is the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$ spanned by its coefficients:

$$\mathrm{supp}(\boldsymbol{v}) = < v_1, \ \ldots \ , v_n >_{\mathbb{F}_q} .$$

Rank weight

If $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$, the **rank weight** of $\boldsymbol{v}$, denoted $w_R(\boldsymbol{v})$, is the dimension of its support.

Remark : $w_R(\boldsymbol{v}) = \mathrm{rank}(\mathrm{Mat}_{\mathscr{B}}(\boldsymbol{v}))$, for every $\mathscr{B}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$.

Rank metric

Support in rank metric

If $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$, the **support of $\boldsymbol{v}$ in rank metric** is the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$ spanned by its coefficients:

$$\text{supp}(\boldsymbol{v}) = < v_1, \ \ldots \ , v_n >_{\mathbb{F}_q} .$$

Rank weight

If $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$, the **rank weight** of $\boldsymbol{v}$, denoted $w_R(\boldsymbol{v})$, is the dimension of its support.

Remark : $w_R(\boldsymbol{v}) = \text{rank}(\text{Mat}_{\mathscr{B}}(\boldsymbol{v}))$, for every $\mathscr{B}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$.

Rank metric

The map $\begin{array}{rcl} d_R : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n & \to & \mathbb{N} \\ (v, w) & \mapsto & w_R(v - w) \end{array}$ is called **rank distance.**

Rank metric code

A **rank metric code** of length n is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$ equipped with the rank metric.

Sum-rank metric

Ambient space for the sum rank metric: $\mathbb{F} := \mathbb{F}_{q^m}^{n_1} \times \mathbb{F}_{q^m}^{n_2} \times \cdots \times \mathbb{F}_{q^m}^{n_l}$.

Sum-rank weight

If $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l) \in \mathbb{F}$, the **sum-rank weight of $\boldsymbol{x}$** is $w_{SR}(\boldsymbol{x}) = \sum_{i=1}^{l} w_R(\boldsymbol{x}_i)$.

Sum-rank metric

Ambient space for the sum rank metric: $\mathbb{F} := \mathbb{F}_{q^m}^{n_1} \times \mathbb{F}_{q^m}^{n_2} \times \cdots \times \mathbb{F}_{q^m}^{n_l}$.

Sum-rank weight

If $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l) \in \mathbb{F}$, the **sum-rank weight of $\boldsymbol{x}$** is $w_{SR}(\boldsymbol{x}) = \sum_{i=1}^{l} w_R(\boldsymbol{x}_i)$.

Sum-Rank metric

The map $\begin{array}{rccc} d_R : & \mathbb{F} \times \mathbb{F} & \to & \mathbb{N} \\ & (v, w) & \mapsto & w_{SR}(v - w) \end{array}$ is called **sum-rank distance.**

Sum-rank metric

Ambient space for the sum rank metric: $\mathbb{F} := \mathbb{F}_{q^m}^{n_1} \times \mathbb{F}_{q^m}^{n_2} \times \cdots \times \mathbb{F}_{q^m}^{n_l}$.

Sum-rank weight

If $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l) \in \mathbb{F}$, the **sum-rank weight of $\boldsymbol{x}$** is $w_{SR}(\boldsymbol{x}) = \sum_{i=1}^{l} w_R(\boldsymbol{x}_i)$.

Sum-Rank metric

The map $\begin{array}{rccc} d_R : \mathbb{F} \times \mathbb{F} & \to & \mathbb{N} \\ (v, w) & \mapsto & w_{SR}(v - w) \end{array}$ is called **sum-rank distance.**

Sum-rank metric code

A **sum-rank metric code** is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}$ equipped with the sum-rank metric.

Sum-rank metric

Ambient space for the sum rank metric: $\mathbb{F} := \mathbb{F}_{q^m}^{n_1} \times \mathbb{F}_{q^m}^{n_2} \times \cdots \times \mathbb{F}_{q^m}^{n_l}$.

Sum-rank weight

If $\boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l) \in \mathbb{F}$, the **sum-rank weight of $\boldsymbol{x}$** is $w_{SR}(\boldsymbol{x}) = \sum_{i=1}^{l} w_R(\boldsymbol{x}_i)$.

Sum-Rank metric

The map $\begin{array}{rccc} d_R : \mathbb{F} \times \mathbb{F} & \to & \mathbb{N} \\ (v, w) & \mapsto & w_{SR}(v - w) \end{array}$ is called **sum-rank distance.**

Sum-rank metric code

A **sum-rank metric code** is an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}$ equipped with the sum-rank metric.

Remark: Both a generalization of the Hamming metric and the rank metric.

Introduction

2 families of codes in rank metric with a decoding algorithm :

- LRPC codes
- Gabidulin codes.

Introduction

2 families of codes in rank metric with a decoding algorithm :

- LRPC codes
- Gabidulin codes.

We introduce a new family: the q-CRT codes.

Introduction

2 families of codes in rank metric with a decoding algorithm :

- LRPC codes
- Gabidulin codes.

We introduce a new family: the q-CRT codes.

- Different parameter constraints than those of Gabidulin codes.
- Decoding algorithm for special cases.
- Codes in rank metric, also adapted for the sum rank-metric: good mix to extend the notion of local decodability in these metrics.

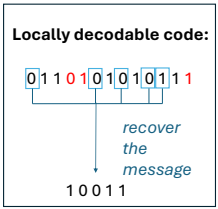
Introduction

2 families of codes in rank metric with a decoding algorithm :

- LRPC codes
- Gabidulin codes.

We introduce a new family: the q-CRT codes.

- Different parameter constraints than those of Gabidulin codes.
- Decoding algorithm for special cases.
- Codes in rank metric, also adapted for the sum rank-metric: good mix to extend the notion of local decodability in these metrics.



Introduction

$f_1, \dots, f_s \in \mathbb{F}_q[x]$ two by two coprime.

Consider $\begin{array}{rcl} \varphi : \mathbb{F}_q[x] & \to & \frac{\mathbb{F}_q[x]}{<f_1>} \times \cdots \times \frac{\mathbb{F}_q[x]}{<f_s>} \\ P & \mapsto & (\pi_1(P), \dots, \pi_s(P)) \end{array}$, where $\pi_i(P) = P \mod f_i$.

Chinese Remainder Theorem Code (CRT code)

The **Chinese Remainder Theorem Code** over $\mathbb{F}_q[x]$ associated to $f_1, \dots, f_s$ of dimension k is the set $\varphi(\mathbb{F}_q[x]_{<k})$.

[1] *On Polynomial Remainder Codes*, Jiun-Hung Yu and Hans-Andrea Loeliger, In: CoRR, 2012.

Introduction

$f_1, \dots, f_s \in \mathbb{F}_q[x]$ two by two coprime.

Consider $\begin{array}{rcl} \varphi : \mathbb{F}_q[x] & \to & \frac{\mathbb{F}_q[x]}{<f_1>} \times \cdots \times \frac{\mathbb{F}_q[x]}{<f_s>} \\ P & \mapsto & (\pi_1(P), \dots, \pi_s(P)) \end{array}$, where $\pi_i(P) = P \mod f_i$.

Chinese Remainder Theorem Code (CRT code)

The **Chinese Remainder Theorem Code** over $\mathbb{F}_q[x]$ associated to $f_1, \dots, f_s$ of dimension k is the set $\varphi(\mathbb{F}_q[x]_{<k})$.

Hamming metric: decoding algorithm based on key equations [1].

[1] *On Polynomial Remainder Codes*, Jiun-Hung Yu and Hans-Andrea Loeliger, In: CoRR, 2012.

Linearised polynomials [Ore33]

Linearised polynomials

The set $\mathbb{F}_{q^m}\langle X^q \rangle = \left\{ A(X) = \sum_{i=0}^{d_A} a_i X^{q^i},\ a_i \in \mathbb{F}_{q^m}, d_A \in \mathbb{N} \right\}$ is the set of **linearised polynomials,** or q-**polynomials.**

Linearised polynomials [Ore33]

Linearised polynomials

The set $\mathbb{F}_{q^m}\langle X^q\rangle = \left\{ A(X) = \sum_{i=0}^{d_A} a_i X^{q^i},\ a_i \in \mathbb{F}_{q^m}, d_A \in \mathbb{N} \right\}$ is the set of **linearised polynomials,** or q-**polynomials.**

- If $P \in \mathbb{F}_{q^m}\langle X^q\rangle$, $\zeta \longmapsto P(\zeta)$ is a $\mathbb{F}_q$-linear map.

Linearised polynomials [Ore33]

Linearised polynomials

The set $\mathbb{F}_{q^m}\langle X^q\rangle = \left\{ A(X) = \sum_{i=0}^{d_A} a_i X^{q^i},\ a_i \in \mathbb{F}_{q^m}, d_A \in \mathbb{N} \right\}$ is the set of **linearised polynomials,** or q-**polynomials.**

- If $P \in \mathbb{F}_{q^m}\langle X^q\rangle$, $\zeta \longmapsto P(\zeta)$ is a $\mathbb{F}_q$-linear map.
- Product of $A, B \in \mathbb{F}_{q^m}\langle X^q\rangle$: $(A \circ B)(X) = A(B(X)) \in \mathbb{F}_{q^m}\langle X^q\rangle$.

The set $(\mathbb{F}_{q^m}\langle X^q\rangle, +, \circ)$ is a non-commutative $\mathbb{F}_{q^m}$-algebra.

Linearised polynomials [Ore33]

Linearised polynomials

The set $\mathbb{F}_{q^m}\langle X^q\rangle = \left\{ A(X) = \sum_{i=0}^{d_A} a_i X^{q^i},\ a_i \in \mathbb{F}_{q^m}, d_A \in \mathbb{N} \right\}$ is the set of **linearised polynomials,** or q-**polynomials.**

- If $P \in \mathbb{F}_{q^m}\langle X^q\rangle$, $\zeta \longmapsto P(\zeta)$ is a $\mathbb{F}_q$-linear map.
- Product of $A, B \in \mathbb{F}_{q^m}\langle X^q\rangle$: $(A \circ B)(X) = A(B(X)) \in \mathbb{F}_{q^m}\langle X^q\rangle$.

The set $(\mathbb{F}_{q^m}\langle X^q\rangle, +, \circ)$ is a non-commutative $\mathbb{F}_{q^m}$-algebra.

Proposition

The set of linearised polynomials is a right euclidean ring.

There exists algorithms to compute (left) LCM, (right) GCD and Bézout relations.

Chinese Remainder Theorem and its lifting (with 2 polynomials)

$F := (f_1, f_2) \in (\mathbb{F}_{q^m}\langle X^q \rangle)^2$, $n := \deg_q(f_1) + \deg_q(f_2)$.
Suppose f_1 and f_2 are coprime (i.e. $f_1 \wedge_r f_2 = X$).

Theorem

Denote $\pi_i(P)$ the rest of P of the right division by f_i. The map

$$\begin{array}{rcl} \varphi_F : \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<f_1 \vee_l f_2>} & \to & \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<f_1>} \times \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<f_2>} \\ P & \mapsto & (\pi_1(P), \pi_2(P)) \end{array}$$

is an isomorphism.

Chinese Remainder Theorem and its lifting (with 2 polynomials)

$F := (f_1, f_2) \in (\mathbb{F}_{q^m}\langle X^q\rangle)^2$, $n := \deg_q(f_1) + \deg_q(f_2)$.
Suppose f_1 and f_2 are coprime (i.e. $f_1 \wedge_r f_2 = X$).

Theorem

Denote $\pi_i(P)$ the rest of P of the right division by f_i. The map

$$\begin{array}{rccc} \varphi_F : & \frac{\mathbb{F}_{q^m}\langle X^q\rangle}{<f_1 \vee_l f_2>} & \to & \frac{\mathbb{F}_{q^m}\langle X^q\rangle}{<f_1>} \times \frac{\mathbb{F}_{q^m}\langle X^q\rangle}{<f_2>} \\ & P & \mapsto & (\pi_1(P), \pi_2(P)) \end{array}$$

is an isomorphism.

Let S_1 and S_2 such that $S_1 \circ f_1 + S_2 \circ f_2 = X$.

Proposition

Let $P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<n}$. Denote by $\pi_3(\cdot)$ the remainder of the right division by $f_1 \vee_l f_2$.
Then

$$\pi_3(\pi_2(P) \circ S_1 \circ f_1 + \pi_1(P) \circ S_2 \circ f_2) = P.$$

Why we need more hypothesis for the lifting with more than two polynomials

Even if f_1, f_2 and f_3 are two by two coprime, then $f_1 \vee_l f_2$ is not always coprime with f_3.

$\hookrightarrow$ Example: ζ and $\xi \in \mathbb{F}_{q^m}$ $\mathbb{F}_q$-independent.
$f_1 = X^q - \zeta^{q-1}X$, $f_2 = X^q - \xi^{q-1}X$ and $f_3 = X^q - (\zeta + \xi)^{q-1}X$.
$\zeta \in \ker(f_1)$, $\xi \in \ker(f_2)$, $\zeta + \xi \in \ker(f_1 \vee_l f_2)$ and therefore $f_3 = X^q - (\zeta + \xi)^{q-1}X$ divides $f_1 \vee_l f_2$ on the right.

Why we need more hypothesis for the lifting with more than two polynomials

Even if f_1, f_2 and f_3 are two by two coprime, then $f_1 \vee_l f_2$ is not always coprime with f_3.

$\hookrightarrow$ Example: ζ and $\xi \in \mathbb{F}_{q^m}$ $\mathbb{F}_q$-independent.
$f_1 = X^q - \zeta^{q-1}X$, $f_2 = X^q - \xi^{q-1}X$ and $f_3 = X^q - (\zeta + \xi)^{q-1}X$.
$\zeta \in \ker(f_1)$, $\xi \in \ker(f_2)$, $\zeta + \xi \in \ker(f_1 \vee_l f_2)$ and therefore $f_3 = X^q - (\zeta + \xi)^{q-1}X$ divides $f_1 \vee_l f_2$ on the right.

We need to suppose that f_3 is coprime with $f_1 \vee_l f_2$.

Chinese Remainder Theorem and its lifting (with more than two polynomials)

$F := (f_1, \ldots, f_s) \in (\mathbb{F}_{q^m}\langle X^q \rangle)^s$, $n := \sum_{i=1}^{s} \deg_q(f_i)$.
Suppose that **for all $i \in \{1, \cdots, s\}$ $f_i \wedge_r (\vee_{j \neq i} f_j) = X$.**

Theorem

The map

$$\begin{array}{rccc} \varphi_F : & \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<\vee_{i=1}^{s} f_i>} & \to & \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<f_1>} \times \cdots \times \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<f_s>} \\ & P & \mapsto & (\pi_1(P), \ldots, \pi_s(P)) \end{array}$$

is an isomorphism.

Chinese Remainder Theorem and its lifting (with more than two polynomials)

$F := (f_1, \ldots, f_s) \in (\mathbb{F}_{q^m}\langle X^q\rangle)^s$, $n := \sum_{i=1}^{s} \deg_q(f_i)$.
Suppose that **for all $i \in \{1, \cdots, s\}$ $f_i \wedge_r (\vee_{j\neq i} f_j) = X$.**

Theorem

The map

$$\begin{array}{rccc} \varphi_F : & \frac{\mathbb{F}_{q^m}\langle X^q\rangle}{<\vee_{i=1}^{s} f_i>} & \to & \frac{\mathbb{F}_{q^m}\langle X^q\rangle}{<f_1>} \times \cdots \times \frac{\mathbb{F}_{q^m}\langle X^q\rangle}{<f_s>} \\ & P & \mapsto & (\pi_1(P), \ldots, \pi_s(P)) \end{array}$$

is an isomorphism.

Let $S_{1,i}$ and $S_{2,i}$ such that $S_{1,i} \circ \left(\vee_{j\neq i} f_j \right) + S_{2,i} \circ f_i = X$.

Proposition (Gaborit, **G.**, Ruatta)

Let $P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<n}$. Denote $\pi(\cdot)$ the remainder of the remainder division by $\vee_{i=1}^{s} f_i$.

We have $P = \pi\left(\sum_{i=1}^{s} \pi_i(P) \circ S_{1,i} \circ \vee_{j\neq i} f_j \right)$.

q-CRT codes (Gaborit, **G**., Ruatta)

$k < n$, $A \in \mathbb{F}_{q^m}\langle X^q \rangle$ (such that $\deg_q(A) + k < n$). Denote $\alpha = \deg_q(A)$.

- $\varphi_F : P \mapsto (\pi_1(P), \ldots, \pi_s(P))$
- $M_A : P \longmapsto P \circ A$

q-CRT codes (Gaborit, **G**., Ruatta)

$k < n$, $A \in \mathbb{F}_{q^m}\langle X^q \rangle$ (such that $\deg_q(A) + k < n$). Denote $\alpha = \deg_q(A)$.

- $\varphi_F : P \mapsto (\pi_1(P), \ldots, \pi_s(P))$
- $M_A : P \longmapsto P \circ A$

q-Chinese Remainder Theorem code

The **q-Chinese Remainder Theorem code** associated to k, A and $F = (f_1, \cdots, f_s)$, of **dimension k** and **length n**, is $\mathcal{C} = (\varphi_F \circ M_A)(\mathbb{F}_{q^m}\langle X^q \rangle_{<k})$.

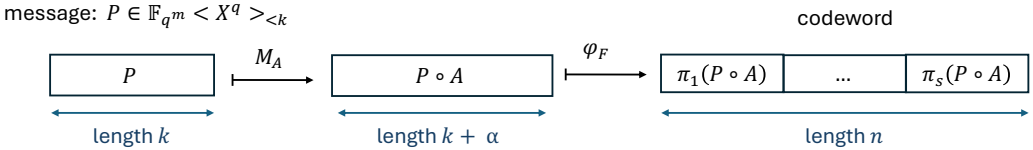
q-CRT codes (Gaborit, **G**., Ruatta)

$k < n$, $A \in \mathbb{F}_{q^m}\langle X^q \rangle$ (such that $\deg_q(A) + k < n$). Denote $\alpha = \deg_q(A)$.

- $\varphi_F : P \mapsto (\pi_1(P), \ldots, \pi_s(P))$
- $M_A : P \longmapsto P \circ A$

q-Chinese Remainder Theorem code

The **q-Chinese Remainder Theorem code** associated to k, A and $F = (f_1, \cdots, f_s)$, of **dimension k** and **length n**, is $\mathcal{C} = (\varphi_F \circ M_A)(\mathbb{F}_{q^m}\langle X^q \rangle_{<k})$.



Role of A

Role of A = control of the minimum distance.

Example: If $P = X$, and $A = X$, $\varphi_F(P \circ A) = (X, \ldots, X) \longrightarrow$ codeword of rank 1.

Role of A

Role of A = control of the minimum distance.

Example: If $P = X$, and $A = X$, $\varphi_F(P \circ A) = (X, \ldots, X) \longrightarrow$ codeword of rank 1.

Remark: We must have $\deg_q(A) + k < n$ to recover exactly $P \circ A$ when we lift $\varphi_F(P \circ A)$.

Role of A

Role of A = control of the minimum distance.

Example: If $P = X$, and $A = X$, $\varphi_F(P \circ A) = (X, \dots, X) \longrightarrow$ codeword of rank 1.

Remark: We must have $\deg_q(A) + k < n$ to recover exactly $P \circ A$ when we lift $\varphi_F(P \circ A)$.

Denote $w_R(A)$ the dimension of the $\mathbb{F}_q$-space spanned by the coefficients of A.

Conjecture (Gaborit, G., Ruatta)

Suppose that for all $i \in \{1, \dots, s\}$, $f_i \in \mathbb{F}_q\langle X^q \rangle$, and that $\deg_q(A) \leqslant min(\deg_q(f_i))$. Then the minimum distance of $\mathcal{C}$ is $w_R(A)$, if for every $P \in \mathbb{F}_{q^m}\langle X^q \rangle$ $\dim(\mathrm{supp}(P \circ A)) \geqslant w_R(A)$

Link with Gabidulin Codes

$(g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$ $\mathbb{F}_q$-linearly independent over $\mathbb{F}_{q^m}$.

Suppose $f_i := X^q - g_i^{q-1} X \in \mathbb{F}_{q^m}\langle X^q \rangle$ for all $i \in \{1, \dots, n\}$.

Let $A \in \mathbb{F}_{q^m}\langle X^q \rangle$, corresponding to an inversible map.

Link with Gabidulin Codes

$(g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$ $\mathbb{F}_q$-linearly independent over $\mathbb{F}_{q^m}$.

Suppose $f_i := X^q - g_i^{q-1}X \in \mathbb{F}_{q^m}\langle X^q \rangle$ for all $i \in \{1, \dots, n\}$.

Let $A \in \mathbb{F}_{q^m}\langle X^q \rangle$, corresponding to an inversible map.

The code $\mathcal{C}$ is the image of $\mathbb{F}_{q^m}\langle X^q \rangle_{<k}$ by the application

$$\begin{array}{rcl} \mathbb{F}_{q^m}\langle X^q \rangle & \to & \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<f_1>} \times \cdots \times \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{<f_n>} \\ P & \mapsto & (P \circ A \mod f_1, \dots, P \circ A \mod f_n) = (g_1^{-1}(P \circ A)(g_1)X, \dots, g_n^{-1}(P \circ A)(g_n)X). \end{array}$$

Proposition (Gaborit, G., Ruatta)

$$\begin{aligned} \mathcal{C} &= \{(g_1^{-1}(P \circ A)(g_1), \dots, g_n^{-1}(P \circ A)(g_n)),\ P \in \mathbb{F}_{q^m}\langle X^q \rangle_{<k}\} \\ &= \{c \cdot \mathrm{Diag}(g_1^{-1}, \dots, g_n^{-1}),\ c \in \mathrm{Gab}_k(A(g_1), \dots, A(g_n))\} \\ &= \mathrm{Gab}_k(A(g_1), \dots, A(g_n)) \cdot \mathrm{Diag}(g_1^{-1}, \dots, g_n^{-1}). \end{aligned}$$

A simple example

Example:

- Ambient space: $\mathbb{F}_{q^m} = \mathbb{F}_{q^4}$
- $A = a_0X + a_1X^q + a_2X^{q^2}$
- $f_1 = X^{q^3}$, $f_2 = X^{q^4} - X$

A simple example

Example:

- Ambient space: $\mathbb{F}_{q^m} = \mathbb{F}_{q^4}$
- $A = a_0X + a_1X^q + a_2X^{q^2}$
- $f_1 = X^{q^3}$, $f_2 = X^{q^4} - X$

Bézout relation: $X^{q^3} \circ X^q - (X^{q^4} - X) \circ X = X$.

A simple example

Example:

- Ambient space: $\mathbb{F}_{q^m} = \mathbb{F}_{q^4}$
- $A = a_0X + a_1X^q + a_2X^{q^2}$
- $f_1 = X^{q^3}$, $f_2 = X^{q^4} - X$

Bézout relation: $X^{q^3} \circ X^q - (X^{q^4} - X) \circ X = X$.

Let $P \in \mathbb{F}_{q^4}\langle X^q \rangle_{<4}$ $(k = 4)$.

- Division of $P \circ A$ by f_1 : projection of $P \circ A$ on $\mathbb{F}_{q^m}\langle X^q \rangle_{<3}$.
- Division of $P \circ A$ by f_2 : replacing of X^{q^4} by X in the expression of $P \circ A$.

A simple example

Example:

- Ambient space: $\mathbb{F}_{q^m} = \mathbb{F}_{q^4}$
- $A = a_0X + a_1X^q + a_2X^{q^2}$
- $f_1 = X^{q^3}$, $f_2 = X^{q^4} - X$

Bézout relation: $X^{q^3} \circ X^q - (X^{q^4} - X) \circ X = X$.

Let $P \in \mathbb{F}_{q^4}\langle X^q \rangle_{<4}$ $(k = 4)$.

- Division of $P \circ A$ by f_1 : projection of $P \circ A$ on $\mathbb{F}_{q^m}\langle X^q \rangle_{<3}$.
- Division of $P \circ A$ by f_2 : replacing of X^{q^4} by X in the expression of $P \circ A$.

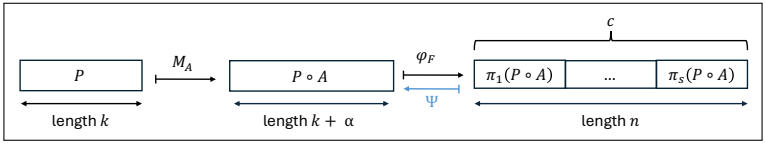
Generator matrix :

$$\left[\begin{array}{cccc|cccc} a_0 & a_1 & a_2 & & a_0 & a_1 & a_2 & 0 \\ 0 & a_0^q & a_1^q & & 0 & a_0^q & a_1^q & a_2^q \\ 0 & 0 & a_0^{q^2} & & a_2^{q^2} & 0 & a_0^{q^2} & a_1^{q^2} \\ 0 & 0 & 0 & & a_1^{q^3} & a_2^{q^3} & 0 & a_0^{q^3} \end{array}\right]$$

A special case: moduli with coefficients in $\mathbb{F}_q$

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.

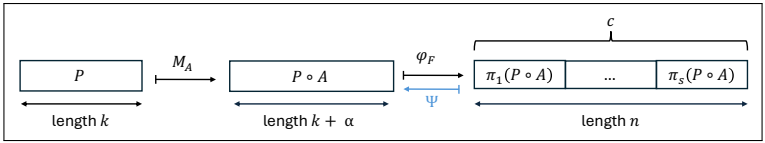
Denote Ψ the lifting of the Chinese Remainder Theorem.



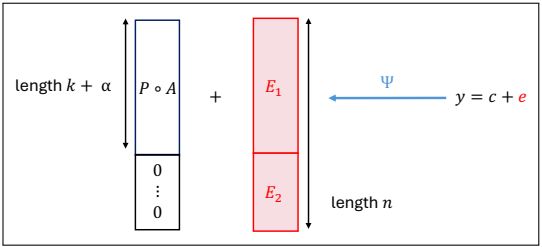
A special case: moduli with coefficients in $\mathbb{F}_q$

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_q\langle X^q \rangle$.

Denote Ψ the lifting of the Chinese Remainder Theorem.



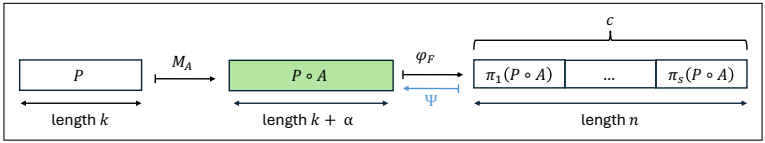
$\boldsymbol{e} \in \mathbb{F}_{q^m}^n$, $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$.
$\boldsymbol{E} := \Psi(\boldsymbol{e})$, and $Y := \Psi(\boldsymbol{y})$.



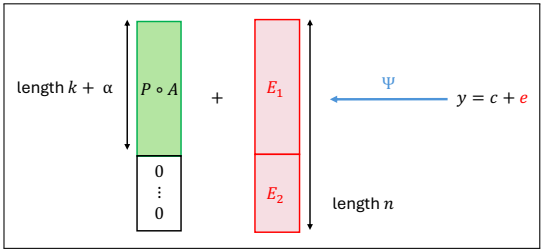
A special case: moduli with coefficients in $\mathbb{F}_q$

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.

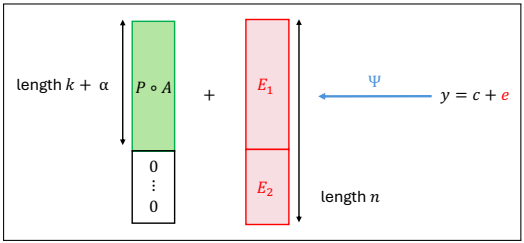
Denote Ψ the lifting of the Chinese Remainder Theorem.



$\boldsymbol{e} \in \mathbb{F}_{q^m}^n$, $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$.
$\boldsymbol{E} := \Psi(\boldsymbol{e})$, and $Y := \Psi(\boldsymbol{y})$.

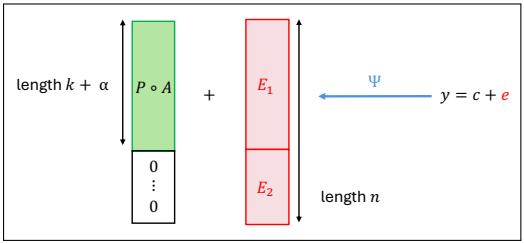


Computing the support of the lifting of the error



We immediately deduce E_2 from the second block.

Computing the support of the lifting of the error



We immediately deduce E_2 from the second block.

$\downarrow$(property of rank metric codes)

We can then use E_2 to deduce $\mathrm{supp}(E)$.

Computing the support of the lifting of the error

Suppose $\boldsymbol{e} \sim \mathcal{U}$.
Let $r \in \{1, \dots, \min(m, n - \alpha - k)\}$.

Proposition (Gaborit, G., Ruatta)

Knowing that $w_R(E) = r$, we have $\mathrm{supp}(E_2) = \mathrm{supp}(E)$ with probability

$$q^{r(k+\alpha)} \prod_{i=0}^{r-1} \frac{(q^{n-k-\alpha} - q^i)}{(q^n - q^i)}.$$

Computing the support of the lifting of the error

Suppose $\boldsymbol{e} \sim \mathcal{U}$.
Let $r \in \{1, \dots, \min(m, n - \alpha - k)\}$.

Proposition (Gaborit, G., Ruatta)

Knowing that $w_R(E) = r$, we have $\mathrm{supp}(E_2) = \mathrm{supp}(E)$ with probability

$$q^{r(k+\alpha)} \prod_{i=0}^{r-1} \frac{(q^{n-k-\alpha} - q^i)}{(q^n - q^i)}.$$

Number of matrices with coefficients in $\mathbb{F}_q$ of size $n \times m$ of rank r :

$$\prod_{i=0}^{r-1} \frac{(q^m - q^i)(q^n - q^i)}{q^r - q^i}.$$

Computing the support of the lifting of the error

Suppose $\boldsymbol{e} \sim \mathcal{U}$.
Let $r \in \{1, \dots, \min(m, n-\alpha-k)\}$.

Proposition (Gaborit, G., Ruatta)

Knowing that $w_R(E) = r$, we have $\mathrm{supp}(E_2) = \mathrm{supp}(E)$ with probability

$$q^{r(k+\alpha)} \prod_{i=0}^{r-1} \frac{(q^{n-k-\alpha} - q^i)}{(q^n - q^i)}.$$

Number of matrices with coefficients in $\mathbb{F}_q$ of size $n \times m$ of rank r :

$$\prod_{i=0}^{r-1} \frac{(q^m - q^i)(q^n - q^i)}{q^r - q^i}.$$

This probability decreases when r increases.

Computing the support of the lifting of the error

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.

Proposition (Gaborit, G., Ruatta)

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e).$$

Therefore, if $\boldsymbol{w_R(e) \leqslant r}$, then $\boldsymbol{w_R(E) \leqslant r}$.

Computing the support of the lifting of the error

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.

Proposition (Gaborit, G., Ruatta)

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e).$$

Therefore, if $\boldsymbol{w_R(e) \leqslant r}$, **then** $\boldsymbol{w_R(E) \leqslant r}$.

If $w_R(\boldsymbol{e}) \leqslant r \leqslant n - \alpha - k$, the probability that $\mathrm{supp}(E_2) = \mathrm{supp}(E)$ is lower bounded by

$$q^{r(k+\alpha)} \prod_{i=0}^{r-1} \frac{(q^{n-k-\alpha} - q^i)}{(q^n - q^i)}.$$

Computing the support of the lifting of the error

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.

Proposition (Gaborit, G., Ruatta)

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e).$$

Therefore, if $\boldsymbol{w_R(e) \leqslant r}$**, then** $\boldsymbol{w_R(E) \leqslant r}$**.**

If $w_R(\boldsymbol{e}) \leqslant r \leqslant n - \alpha - k$, the probability that $\mathrm{supp}(E_2) = \mathrm{supp}(E)$ is lower bounded by

$$q^{r(k+\alpha)} \prod_{i=0}^{r-1} \frac{(q^{n-k-\alpha} - q^i)}{(q^n - q^i)}.$$

$\hookrightarrow$ **We recover the support of the lifting of the error using only the second block, with high probability.**

Computing the support of the lifting of the error

Proposition (Gaborit, G., Ruatta)

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e).$$

Computing the support of the lifting of the error

Proposition (Gaborit, G., Ruatta)

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e).$$

Proof: We use the fact that:

- If $g \in \mathbb{F}_{q^m}\langle X^q \rangle$ and $f \in \mathbb{F}_q\langle X^q \rangle$ are such that $\mathrm{supp}(g) \subset S$, with S a $\mathbb{F}_q$ vector subspace of $\mathbb{F}_{q^m}$, then $\mathrm{supp}(g \circ f) \subset S$.
- If $g \in \mathbb{F}_{q^m}\langle X^q \rangle$, and $f \in \mathbb{F}_q\langle X^q \rangle$, $\mathrm{supp}(\pi(g)) \subset \mathrm{supp}(g)$, where $\pi(g)$ is the remainder in the right division by f.

Computing the support of the lifting of the error

Proposition (Gaborit, G., Ruatta)

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e).$$

Proof: We use the fact that:

- If $g \in \mathbb{F}_{q^m}\langle X^q\rangle$ and $f \in \mathbb{F}_q\langle X^q\rangle$ are such that $\mathrm{supp}(g) \subset S$, with S a $\mathbb{F}_q$ vector subspace of $\mathbb{F}_{q^m}$, then $\mathrm{supp}(g \circ f) \subset S$.
- If $g \in \mathbb{F}_{q^m}\langle X^q\rangle$, and $f \in \mathbb{F}_q\langle X^q\rangle$, $\mathrm{supp}(\pi(g)) \subset \mathrm{supp}(g)$, where $\pi(g)$ is the remainder in the right division by f.

We have

$$E = \pi\Big(\sum_{i=1}^{s} \pi_i(e) \circ S_{1,i} \circ \vee_{j\neq i} f_j\Big).$$

Since for all $i \in \{1, \cdots, s\}$, $f_i \in \mathbb{F}_q\langle X^q\rangle$, we have $\vee_{j\neq i} f_j \in \mathbb{F}_q\langle X^q\rangle$, and $S_{1,i} \in \mathbb{F}_q\langle X^q\rangle$. For every $i \in \{1, \cdots, s\}$, we have $\mathrm{supp}(\pi_i(e) \circ S_{1,i} \circ \vee_{j\neq i} f_j) \subset \mathrm{supp}(e)$. Therefore $\mathrm{supp}(E) \subset \mathrm{supp}(e)$.

Computing the lifting of the error

$M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k}) = \{P \circ A,\ P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<k}\} \longrightarrow$ code of length $k+\alpha$ and dimension k over $\mathbb{F}_{q^m}$.

$H \in M_{\alpha\times(k+\alpha)}(\mathbb{F}_{q^m})$ a parity check matrix of $M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k})$.

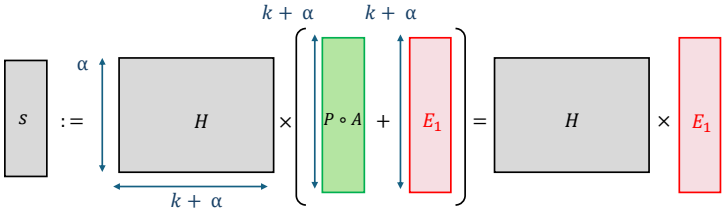
[2] *Low Rank Parity Check Codes: New Decoding Algorithms and Applications to Cryptography*, Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Gilles Zémor, In: IEEE Transactions on Information Theory, 2019.

Computing the lifting of the error

$M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k}) = \{P \circ A,\ P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<k}\} \longrightarrow$ code of length $k+\alpha$ and dimension k over $\mathbb{F}_{q^m}$.

$H \in M_{\alpha\times(k+\alpha)}(\mathbb{F}_{q^m})$ a parity check matrix of $M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k})$.

We compute:



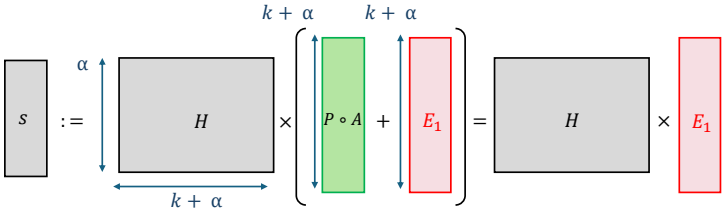
[2] *Low Rank Parity Check Codes: New Decoding Algorithms and Applications to Cryptography*, Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Gilles Zémor, In: IEEE Transactions on Information Theory, 2019.

Computing the lifting of the error

$M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k}) = \{P \circ A,\ P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<k}\} \longrightarrow$ code of length $k+\alpha$ and dimension k over $\mathbb{F}_{q^m}$.

$H \in M_{\alpha\times(k+\alpha)}(\mathbb{F}_{q^m})$ a parity check matrix of $M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k})$.

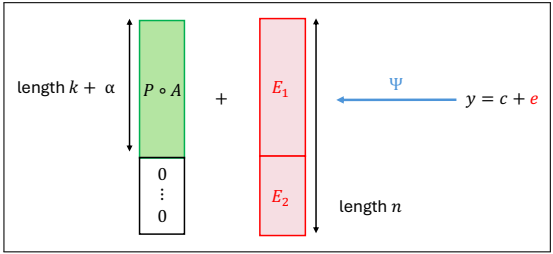
We compute:



We solve the system $s = H \times E_1$, using $\mathrm{supp}(E)$ (as LRPC codes decoding [2]).
$\longrightarrow$ system with $\boldsymbol{r(k+\alpha)}$ **unknows** and $\boldsymbol{m\alpha}$ **equations over** $\mathbb{F}_q$. We can solve it if $\boldsymbol{r < \frac{m\alpha}{k+\alpha}}$.

[2] *Low Rank Parity Check Codes: New Decoding Algorithms and Applications to Cryptography*, Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Gilles Zémor, In: IEEE Transactions on Information Theory, 2019.

Decoding algorithm



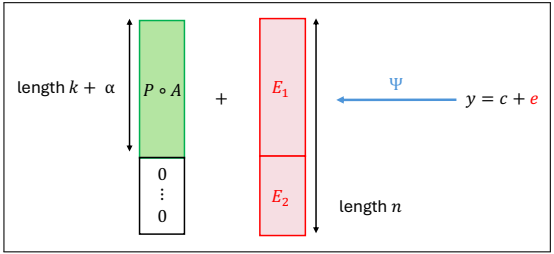
Algorithm Decoding algorithm

Input: $y = c + e$, where $c \in \mathcal{C}$, and $w_r(e) \leqslant \min(\frac{m\alpha}{k+\alpha}, n - k - \alpha)$.

Output: $P \in \mathbb{F}_{q^m}\langle X^q \rangle_k$ such that $y - \varphi_F(P \circ A) \leqslant w_r(e)$, or failure.

1: Compute $Y := \Psi(y) \in \mathbb{F}_{q^m}\langle X^q \rangle$.
2: From Y, deduce E_2, and compute $\mathrm{supp}(E_2)$.
3: Using $\mathrm{supp}(E_2)$, compute E_1 by linear algebra.
4: Deduce $P \circ A$, by computing $Y - E_1 - E_2$.
5: Compute the right division of $P \circ A$ by A.

Decoding algorithm



Algorithm Decoding algorithm

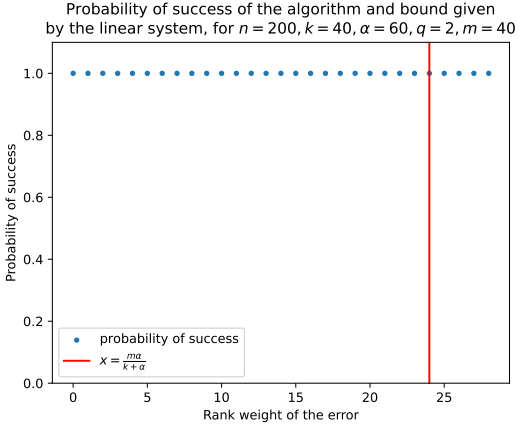
Input: $y = c + e$, where $c \in \mathcal{C}$, and $w_r(e) \leqslant \min(\frac{m\alpha}{k+\alpha}, n-k-\alpha)$.

Output: $P \in \mathbb{F}_{q^m}\langle X^q \rangle_k$ such that $y - \varphi_F(P \circ A) \leqslant w_r(e)$, or failure.

1: Compute $Y := \Psi(y) \in \mathbb{F}_{q^m}\langle X^q \rangle$.
2: From Y, deduce E_2, and compute $\mathrm{supp}(E_2)$.
3: Using $\mathrm{supp}(E_2)$, compute E_1 by linear algebra.
4: Deduce $P \circ A$, by computing $Y - E_1 - E_2$.
5: Compute the right division of $P \circ A$ by A.

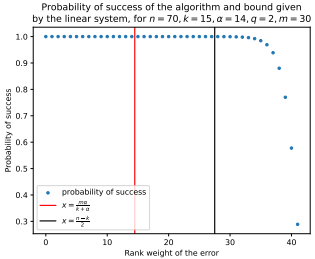
- Polynomial-time algorithm.
- Dominant cost: linear algebra over $\mathbb{F}_q$.
- Can output a codeword even beyond the unique decoding radius.

Success probability

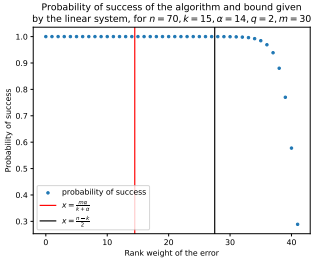


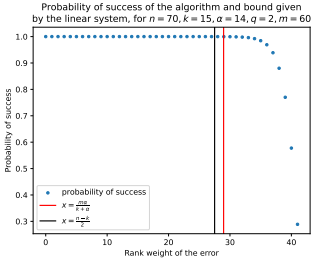
The probability of success is close to one for all rank weights that the algorithm can decode.

Success probability

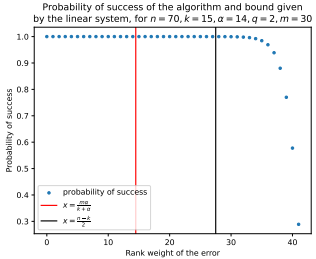


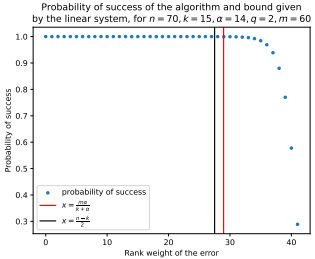
Success probability

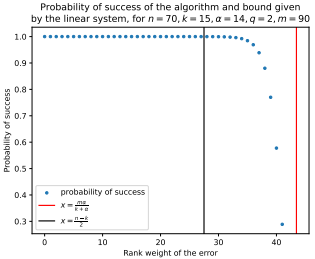




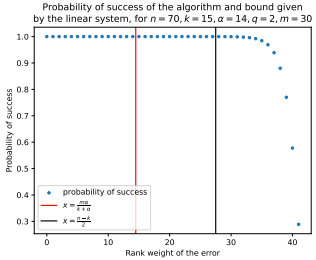
Success probability

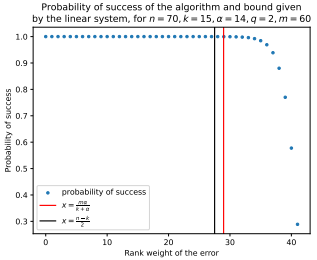


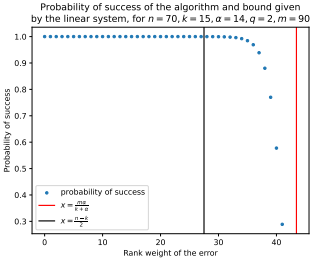




Success probability







$\longrightarrow$ The value of m allows to adjust the bound given by the linear system.

Simple codes

$\mathcal{A} := M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k}) = \{P \circ A,\ P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<k}\}$, $\mathcal{C}$ the q-CRT code associated to $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q\rangle$.

[3] *Identity-Based Encryption from Codes with Rank Metric*, Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, Jean-Pierre Tillich, In: Advances in Cryptology - CRYPTO 2017

Simple codes

$\mathcal{A} := M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k}) = \{P \circ A,\ P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<k}\}$, $\mathcal{C}$ the q-CRT code associated to $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q\rangle$. Consider

$$\begin{array}{rcl} L_n : \mathbb{F}_{q^m}\langle X^q\rangle_{<n} & \to & \mathbb{F}_{q^m}^n \\ \sum_{i=0}^{n-1} p_i X^{q^i} & \mapsto & (p_0, \ldots, p_{n-1}) \end{array}.$$

Denote $\mathcal{A}_0 = L_n(\mathcal{A})$.

[3] *Identity-Based Encryption from Codes with Rank Metric*, Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, Jean-Pierre Tillich, In: Advances in Cryptology - CRYPTO 2017

Simple codes

$\mathcal{A} := M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k}) = \{P \circ A,\ P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<k}\}$, $\mathcal{C}$ the q-CRT code associated to $F = (f_1, \cdots, f_s) \in \mathbb{F}_{q^m}\langle X^q\rangle$. Consider

$$\begin{array}{rcl} L_n : \mathbb{F}_{q^m}\langle X^q\rangle_{<n} & \to & \mathbb{F}_{q^m}^n \\ \sum_{i=0}^{n-1} p_i X^{q^i} & \mapsto & (p_0, \ldots, p_{n-1}) \end{array}.$$

Denote $\mathcal{A}_0 = L_n(\mathcal{A})$.

A generator matrix of $\mathcal{A}_0$: $G = \left(M \mid 0_{k\times(n-(k+\alpha))}\right)$, where $M \in \mathbb{F}_{q^m}^{k\times(k+\alpha)}$(simple code [3]).

[3] *Identity-Based Encryption from Codes with Rank Metric*, Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, Jean-Pierre Tillich, In: Advances in Cryptology - CRYPTO 2017

Simple codes

$\mathcal{A} := M_A(\mathbb{F}_{q^m}\langle X^q\rangle_{<k}) = \{P \circ A,\ P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<k}\}$, $\mathcal{C}$ the q-CRT code associated to $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q\rangle$. Consider

$$\begin{array}{rcl} L_n : \mathbb{F}_{q^m}\langle X^q\rangle_{<n} & \to & \mathbb{F}_{q^m}^n \\ \sum_{i=0}^{n-1} p_i X^{q^i} & \mapsto & (p_0, \ldots, p_{n-1}) \end{array}.$$

Denote $\mathcal{A}_0 = L_n(\mathcal{A})$.

A generator matrix of $\mathcal{A}_0$: $G = \left(M \mid 0_{k\times(n-(k+\alpha))}\right)$, where $M \in \mathbb{F}_{q^m}^{k\times(k+\alpha)}$(simple code [3]).

We have $(L_n \circ \Psi)(\mathcal{C}) = \mathcal{A}_0$, and $L_n \circ \Psi$ is an isometry for the rank metric.
Therefore, $\boldsymbol{\mathcal{C}}$ **is a simple code.**

[3] *Identity-Based Encryption from Codes with Rank Metric*, Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, Jean-Pierre Tillich, In: Advances in Cryptology - CRYPTO 2017

Decoding of a wider class

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{q^l}\langle X^q \rangle$, where $l < m$ is small.

Decoding of a wider class

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{q^l}\langle X^q \rangle$, where $l < m$ is small.
Same decoding algorithm, but **changes in the bound:**

Decoding of a wider class

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{q^l}\langle X^q \rangle$, where $l < m$ is small.

Same decoding algorithm, but **changes in the bound:** Indeed, $\mathrm{supp}(E) \nsubseteq \mathrm{supp}(e)$.

Decoding of a wider class

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{q^l}\langle X^q \rangle$, where $l < m$ is small.
Same decoding algorithm, but **changes in the bound:** Indeed, $\mathrm{supp}(E) \not\subseteq \mathrm{supp}(e)$.

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e) \cdot \mathbb{F}_{q^l},$$

and then

$$\dim(\mathrm{supp}(E)) \leqslant w_r(e) \cdot l.$$

Decoding of a wider class

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{q^l}\langle X^q \rangle$, where $l < m$ is small.
Same decoding algorithm, but **changes in the bound:** Indeed, $\mathrm{supp}(E) \nsubseteq \mathrm{supp}(e)$.

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e) \cdot \mathbb{F}_{q^l},$$

and then

$$\dim(\mathrm{supp}(E)) \leqslant w_r(e) \cdot l.$$

Proposition (Gaborit, G., Ruatta)

Knowing that $w_r(E) = rl$, we have $\mathrm{supp}(E_2) = \mathrm{supp}(E)$ with probability

$$q^{l \cdot r \cdot (k+\alpha)} \prod_{i=0}^{lr-1} \frac{q^{n-(k+\alpha)} - q^i}{q^n - q^i}.$$

Decoding of a wider class

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{q^l}\langle X^q \rangle$, where $l < m$ is small.
Same decoding algorithm, but **changes in the bound:** Indeed, $\mathrm{supp}(E) \nsubseteq \mathrm{supp}(e)$.

We have

$$\mathrm{supp}(E) \subset \mathrm{supp}(e) \cdot \mathbb{F}_{q^l},$$

and then

$$\dim(\mathrm{supp}(E)) \leqslant w_r(e) \cdot l.$$

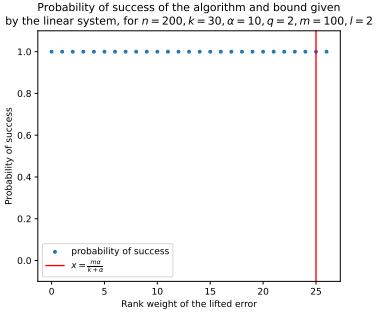
Proposition (Gaborit, G., Ruatta)

Knowing that $w_r(E) = rl$, we have $\mathrm{supp}(E_2) = \mathrm{supp}(E)$ with probability

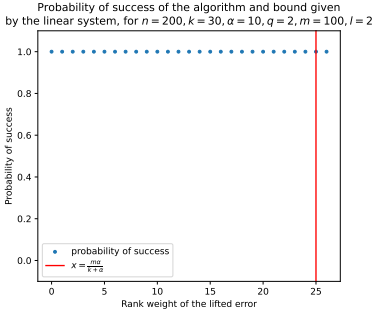
$$q^{l \cdot r \cdot (k+\alpha)} \prod_{i=0}^{lr-1} \frac{q^{n-(k+\alpha)} - q^i}{q^n - q^i}.$$

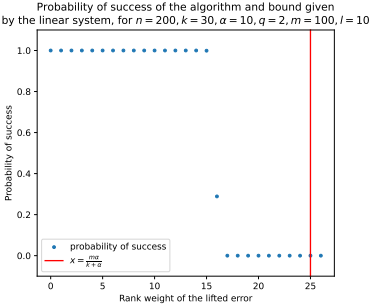
If $w_R(e) \leqslant r$, the probability of success of the decoding algorithm is lower bounded by the one above.

Probability of success on an example

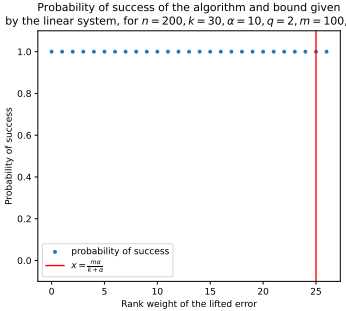


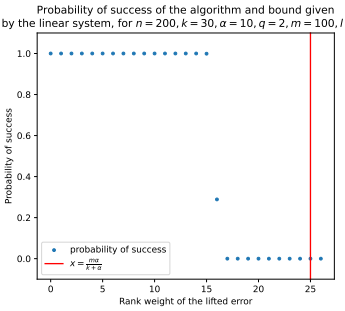
Probability of success on an example

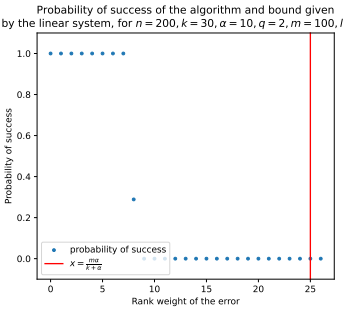




Probability of success on an example







Conclusion

- New family of rank metric codes.
- Based on Chinese Remainder Theorem for linearised polynomials.
- Probabilistic decoding algorithm for special cases, in polynomial time.

Conclusion

- New family of rank metric codes.
- Based on Chinese Remainder Theorem for linearised polynomials.
- Probabilistic decoding algorithm for special cases, in polynomial time.

Open questions and further work:

- Deterministic decoding algorithm, with key equation.
- Decoding algorithm for the general case.
- Study of their local properties: local testability and local decodability (in sum-rank metric, and rank metric).

Conclusion

- New family of rank metric codes.
- Based on Chinese Remainder Theorem for linearised polynomials.
- Probabilistic decoding algorithm for special cases, in polynomial time.

Open questions and further work:

- Deterministic decoding algorithm, with key equation.
- Decoding algorithm for the general case.
- Study of their local properties: local testability and local decodability (in sum-rank metric, and rank metric).

Thank you for your attention !

See `hal-05062636` : "Linearized Polynomial Chinese remainder codes".