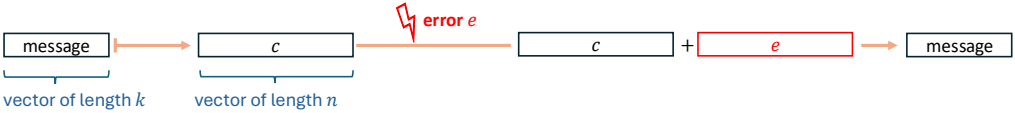
Linearised Chinese Remainder Codes

Philippe Gaborit, **Camille Garnier**, Olivier Ruatta

Introduction

Linear code

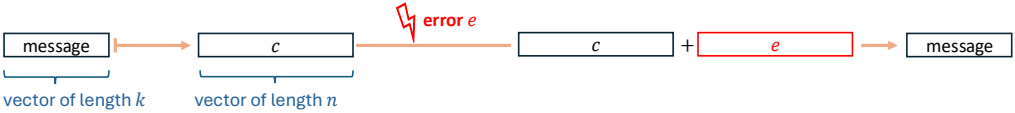
A **linear code** of dimension k and length n is a vector subspace of dimension k of $\mathbb{F}_q^n$.



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:

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

$\hookrightarrow$ Example: $\mathscr{B} = \{1, \alpha, \alpha^2\}$ a $\mathbb{F}_3$-basis of $\mathbb{F}_{3^3}$, $\boldsymbol{w} = (1 + 2\alpha, \ 0, \ 1 + 2\alpha + \alpha^2, \ 1 + 2\alpha)$:

$$\text{Mat}_{\mathscr{B}}(\boldsymbol{v}) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{ and } \text{supp}(\boldsymbol{w}) = < 1 + 2\alpha, \alpha^2 >_{\mathbb{F}_3} .$$

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:

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

$\hookrightarrow$ Example: $\mathscr{B} = \{1, \alpha, \alpha^2\}$ a $\mathbb{F}_3$-basis of $\mathbb{F}_{3^3}$, $\boldsymbol{w} = (1 + 2\alpha, \ 0, \ 1 + 2\alpha + \alpha^2, \ 1 + 2\alpha)$:

$$\text{Mat}_{\mathscr{B}}(\boldsymbol{v}) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{ and } \text{supp}(\boldsymbol{w}) = < 1 + 2\alpha, \alpha^2 >_{\mathbb{F}_3} .$$

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.

$\hookrightarrow$ Example: $w_R(\boldsymbol{w}) = 2$.

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:

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

$\hookrightarrow$ Example: $\mathscr{B} = \{1, \alpha, \alpha^2\}$ a $\mathbb{F}_3$-basis of $\mathbb{F}_{3^3}$, $\boldsymbol{w} = (1 + 2\alpha, \ 0, \ 1 + 2\alpha + \alpha^2, \ 1 + 2\alpha)$:

$$\text{Mat}_{\mathscr{B}}(\boldsymbol{v}) = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 0 & 2 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \text{ and } \text{supp}(\boldsymbol{w}) = < 1 + 2\alpha, \alpha^2 >_{\mathbb{F}_3} .$$

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.

$\hookrightarrow$ Example: $w_R(\boldsymbol{w}) = 2$.

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.

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.

Chinese remainder codes: codes in Hamming metric, using the Chinese remainder theorem on polynomials or integers to encode messages.

1. Chinese Remainder Theorem for linearised polynomials
2. q-CRT codes
3. A special case and its decoding algorithm

1. Chinese Remainder Theorem for linearised polynomials
2. q-CRT codes
3. A special case and its decoding algorithm

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.**

$\hookrightarrow$ Example: $X^{q^2} + X \in \mathbb{F}_{q^m}\langle X^q \rangle$.

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.**

$\hookrightarrow$ Example: $X^{q^2} + X \in \mathbb{F}_{q^m}\langle X^q\rangle$.

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

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.**

$\hookrightarrow$ Example: $X^{q^2} + X \in \mathbb{F}_{q^m}\langle X^q\rangle$.

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

$\hookrightarrow$ Example: $X^q \circ aX = a^q X^q \neq aX \circ X^q = aX^q$ if $a \in \mathbb{F}_{q^m} \backslash \mathbb{F}_q$.

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.**

$\hookrightarrow$ Example: $X^{q^2} + X \in \mathbb{F}_{q^m}\langle X^q\rangle$.

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

$\hookrightarrow$ Example: $X^q \circ aX = a^q X^q \neq aX \circ X^q = aX^q$ if $a \in \mathbb{F}_{q^m} \backslash \mathbb{F}_q$.

Proposition

The set of linearised polynomials is a right euclidean ring.

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

Chinese Remainder Theorem and its lifting (with 2 polynomials)

$F := (f_1, f_2) \in (\mathbb{F}_{q^m}\langle X^q \rangle)^2$, $d := \deg_q(f_1) + \deg_q(f_2)$.
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 in 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.

Chinese Remainder Theorem and its lifting (with 2 polynomials)

$F := (f_1, f_2) \in (\mathbb{F}_{q^m}\langle X^q\rangle)^2$, $d := \deg_q(f_1) + \deg_q(f_2)$.
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 in 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 $P \in \mathbb{F}_{q^m}\langle X^q\rangle_{<d}$. Denote by $\pi_3(\cdot)$ the remainder by 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)

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

Theorem

The map

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

is an isomorphism.

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

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

Theorem

The map

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

is an isomorphism.

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

Proposition

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

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

1 Chinese Remainder Theorem for linearised polynomials

2 q-CRT codes

3 A special case and its decoding algorithm

q-CRT codes

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

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

q-CRT codes

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

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

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 d**, is $\mathcal{C} = (\varphi_F \circ M_A)(\mathbb{F}_{q^m}\langle X^q \rangle_{<k})$.

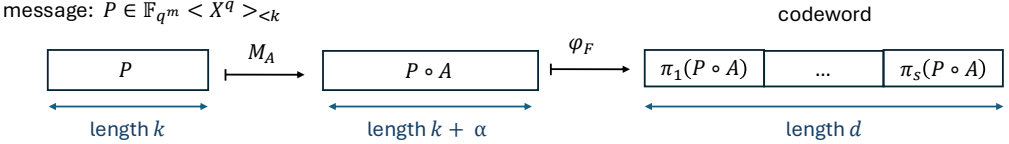
q-CRT codes

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

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

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 d**, is $\mathcal{C} = (\varphi_F \circ M_A)(\mathbb{F}_{q^m}\langle X^q \rangle_{<k})$.



1 Chinese Remainder Theorem for linearised polynomials

2 q-CRT codes

3 A special case and its decoding algorithm

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

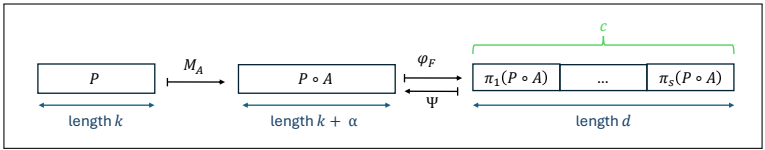
Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.
Ψ the lifting of the Chinese Remainder Theorem. $\alpha := \deg_q(A)$.

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

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.
Ψ the lifting of the Chinese Remainder Theorem. $\alpha := \deg_q(A)$.
$\boldsymbol{c} \in \mathcal{C}$.

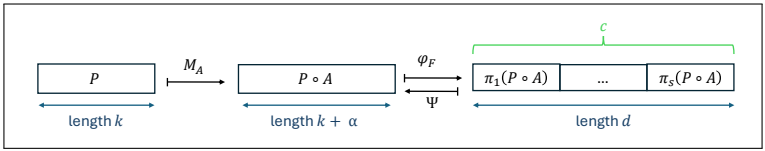
A special case: moduli with coefficients in $\mathbb{F}_q$

Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.
Ψ the lifting of the Chinese Remainder Theorem. $\alpha := \deg_q(A)$.
$\boldsymbol{c} \in \mathcal{C}$.



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

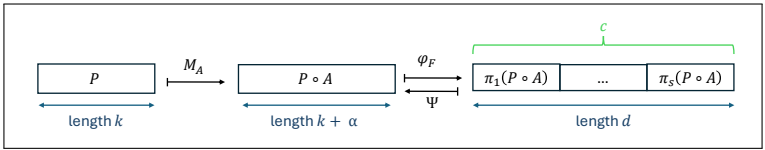
Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.
Ψ the lifting of the Chinese Remainder Theorem. $\alpha := \deg_q(A)$.
$\boldsymbol{c} \in \mathcal{C}$.



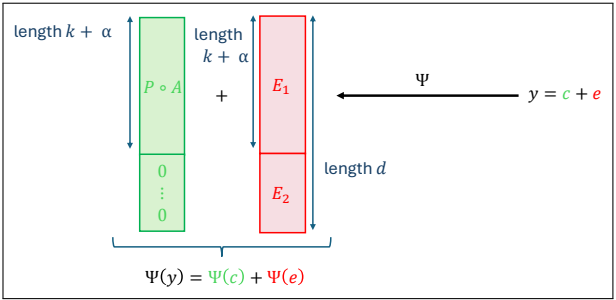
$\boldsymbol{e} \in \mathbb{F}_{q^m}^d$, $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$.
$\boldsymbol{E} := \Psi(\boldsymbol{e})$, and $Y := \Psi(\boldsymbol{y})$.

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

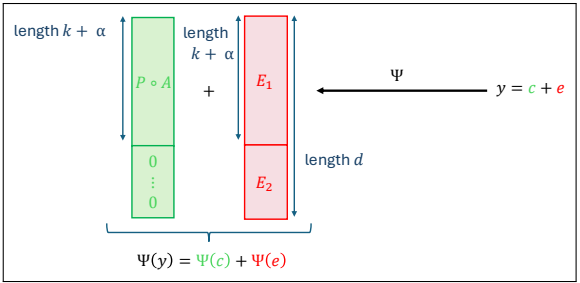
Suppose $F = (f_1, \cdots, f_s) \in \mathbb{F}_{\boldsymbol{q}}\langle X^q \rangle$.
Ψ the lifting of the Chinese Remainder Theorem. $\alpha := \deg_q(A)$.
$\boldsymbol{c} \in \mathcal{C}$.



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



Computing the support of the error



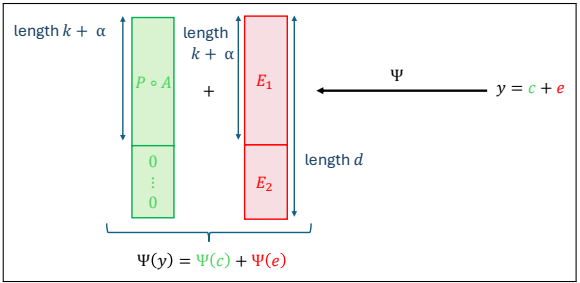
We can use E_2 to deduce $\mathrm{supp}(E)$:
Suppose $\boldsymbol{e} \sim \mathcal{U}$.

Proposition (P.G., C.G., O.R.)

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

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

Computing the support of the error



We can use E_2 to deduce $\mathrm{supp}(E)$:
Suppose $\boldsymbol{e} \sim \mathcal{U}$.

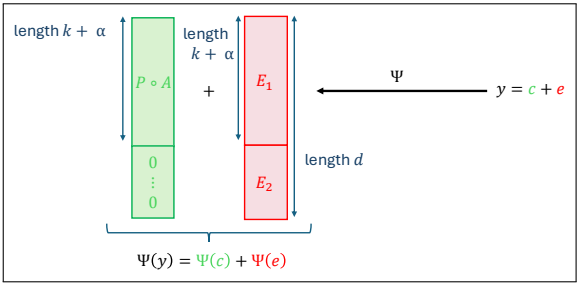
Proposition (P.G., C.G., O.R.)

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

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

We have $\mathrm{supp}(E) \subset \mathrm{supp}(\boldsymbol{e})$. Therefore, $w_R(E) \leq w_R(\boldsymbol{e})$.

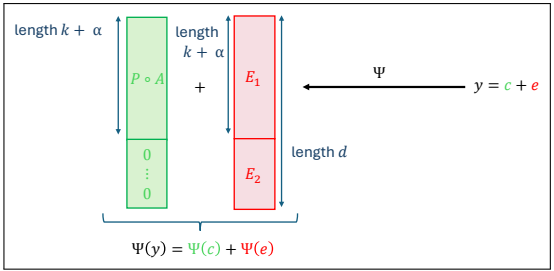
Computing the error



Using $\mathrm{supp}(E)$, we can compute E_1 by solving a linear system, if $r < \frac{m\alpha}{k+\alpha}$. (as LRPC codes decoding[1])

[1] *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, août 2019.

Decoding algorithm

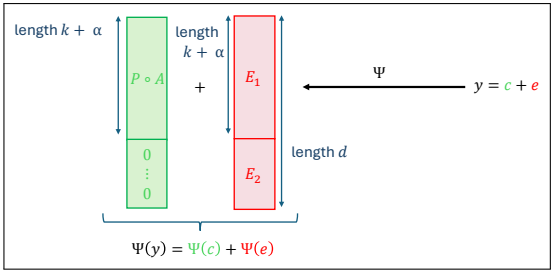


Algorithm Decoding algorithm

Input: $y = c + e$, where $c \in \mathcal{C}$, and $w_R(e) < \frac{m\alpha}{k+\alpha}$.
Output: $P \in \mathbb{F}_{q^m}\langle X^q \rangle_{<k}$ such that $c = P \circ A$, 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



- Polynomial-time algorithm.
- Dominant cost: linear algebra over $\mathbb{F}_q$.

Algorithm Decoding algorithm

Input: $y = c + e$, where $c \in \mathcal{C}$, and $w_R(e) < \frac{m\alpha}{k+\alpha}$.
Output: $P \in \mathbb{F}_{q^m}\langle X^q \rangle_{<k}$ such that $c = P \circ A$, 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.

Conclusion

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

Conclusion

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

Open questions and further work:

- Deterministic decoding algorithm, with key equation.
- Decoding algorithm for the general case.

Conclusion

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

Open questions and further work:

- Deterministic decoding algorithm, with key equation.
- Decoding algorithm for the general case.

Thank you for your attention !

Link with Gabidulin Codes

$(g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$ $\mathbb{F}_q$-linearly independant over $\mathbb{F}_{q^m}$.
$f_i := X^q - g_i^{q-1} X \in \mathbb{F}_{q^m}\langle X^q \rangle$ for all $i \in \{1, \dots, n\}$.

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

$$\begin{array}{rcl} \mathbb{F}_{q^m}\langle X^q \rangle & \to & \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{F_1} \times \cdots \times \frac{\mathbb{F}_{q^m}\langle X^q \rangle}{F_n} \\ P & \mapsto & (P \mod F_1, \dots, P \mod F_n) = (g_1^{-1} P(g_1) X, \dots, g_n^{-1} P(g_n) X). \end{array}$$

Each word $\boldsymbol{c}$ of $\mathcal{C}_{k,F}$ can be written as $c = (g_1^{-1} P(g_1), \dots, g_n^{-1} P(g_n))$, with $P \in \mathbb{F}_{q^m}\langle X^q \rangle_{<k}$.

Proposition

$$\mathcal{C}_{k,F} = \mathrm{Gab}_k(g_1, \dots, g_n)\mathrm{Diag}(g_1^{-1}, \dots, g_n^{-1}).$$