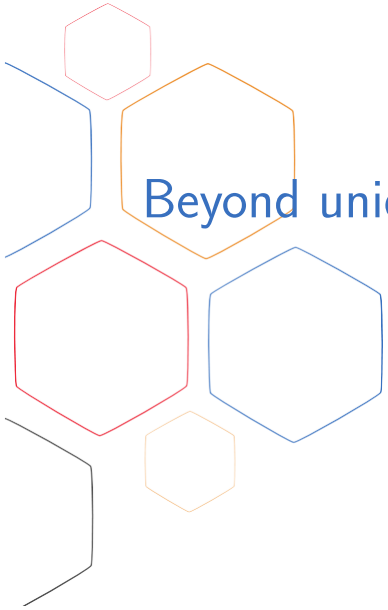


LIRMM

Beyond unique error correction capability with computer algebra

Eleonora Guerrini

12/02/2026

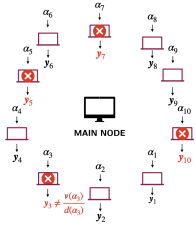
cnrs

Table of Contents

Outline

(Algebraic) Error correcting codes: What for?

* Recover faulty transmitted data
* Distributed Data Storage
* Fault Tolerant Algorithms (FTA)

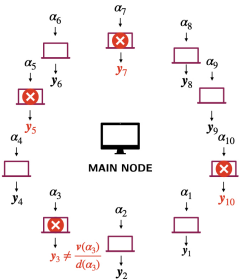


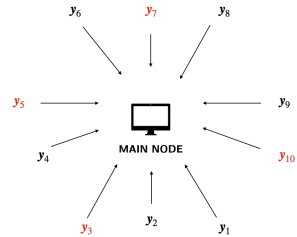
Core of this presentation

* How much we can decode ? $\rightsquigarrow$
* How efficiently we can do it ? $\rightsquigarrow$
* Fault Tolerant Algorithms (FTA)

* Bounds and combinatorial arguments
* Structured algebraic codes
* Go beyond the worst case radius: Algorithms and analysis

Find $\boldsymbol{y}(x) = (y_1, \ldots, y_l)$ s.t. $A(x)\boldsymbol{y}(x) = \boldsymbol{b}(x)$





- ⊙ *(Evaluation)* Node j evaluates A and $\boldsymbol{b}$ in α_j.
- ⊙ *(Pointwise solving)* Compute $\boldsymbol{y}_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j) = \frac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$, for any j.
- ∗ Errors can occur: $\boldsymbol{y} \rightsquigarrow \left(\frac{\boldsymbol{v}(\alpha_1)}{d(\alpha_1)}, \ldots, \frac{\boldsymbol{v}(\alpha_L)}{d(\alpha_L)}\right) + \Xi$
- ◇ *(Interpolation with errors)* Find $(\boldsymbol{v}, d) \in \mathbb{F}_q[x]^{(n+1)\times 1}$, with $N > \deg(\boldsymbol{v}) := \max_{1\le i\le n}\{\deg(v_i)\}$ and $D > \deg(d)$.

Good codes and decoding strategies

Definition (Reed Solomon codes, Reed, Solomon, 1960)

In $\mathbb{F}_q$, fix a set $\{\alpha_1, \ldots, \alpha_n\}$ of distinct points. A Reed Solomon code $RS(n,k)$:

$$RS(n,k) = \{(f(\alpha_1), \ldots, f(\alpha_n)) | f \in \mathbb{F}_q[x],\ deg(f) \leq k-1\}$$

- MDS $dim(C) = n - k + 1$ [unique decoding]
- List-decodable
- Good Interleaving performances
- Fast Decoding methods, relying on recent computer algebra algorithms
- Suitable for polynomial linear system solving

Decoding of RS codes can be solved via Rational Reconstruction (RR).

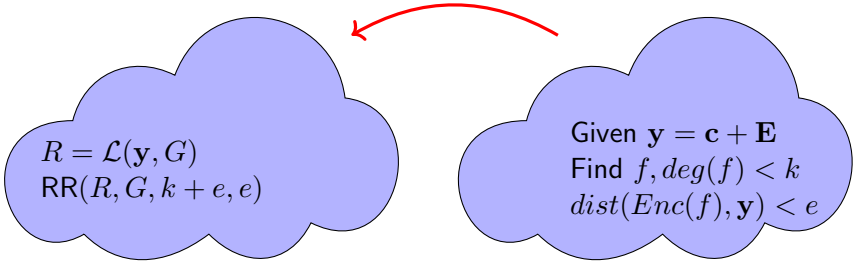
Rational Reconstruction (RR)

Rational Reconstruction is a main tool for decoding

(RR): Given $R, G \in \mathbb{F}_q[x]$, bounds N, M on the desired solution, find (v, d) s.t. :
$v = R \times d \mod G, deg(d) < M, deg(v) < N$

- Performed via Extended Euclidian Algorithm
- different G, different algorithms
  - $G = \prod(x - \alpha_i) \rightsquigarrow$ Cauchy Interpolation
  - $G = x^m \rightsquigarrow$ Padé Approximation
- Condition on the existence of a solution (via linear algebra).
  What about the uniqueness ?

Rational Reconstruction as Decoding



Rational Reconstruction

- Input: $R, G \in \mathbb{F}_q[x]$
- $deg(v) < N, deg(d) < D$
- Output: $v, d \in \mathbb{F}_q[x]$
  - $v = d \times R \mod G$

Decoding

- Input: $\mathbf{y} = (y_1, \ldots, y_n)$
- $G = \prod_{i=1}^{n}(x - \alpha_i), e, k$
- Output: $f \in \mathbb{F}_q[x]$, $deg(f) \leq k - 1$
  - $dist(Enc_{RS}(f), \mathbf{y}) \leq e$

Cauchy Interpolation for Decoding

Cauchy Int. is a particular case of Rational Reconstruction (RR)

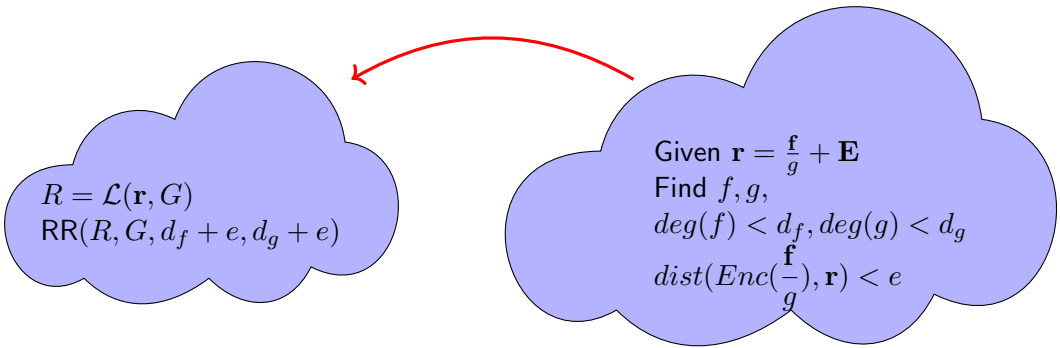
(RR): Given $R, G \in \mathbb{F}_q[x]$, bounds N, M on the desired degrees solution, find (v, d)
$v = R \times d \mod G, deg(d) < M, deg(v) < N$

Note that if $(v, G) = 1$, then $\frac{v}{d} = R \mod G$

Decoding Reed Solomon codes: Set $G = \prod_i^n (x - \alpha_i)$

* Find $\psi, \phi \in \mathbb{F}_q[x]$ s.t. $\mathcal{L}(\mathbf{y}, \alpha_i)\psi = \phi \mod G$
* $\deg(G) = k + 2e - 1$, $M = e$, $N = k + e$,
* Set $\Lambda = \prod_{i \in E}(x - \alpha_i)$, the error locator polynomial
* $(\Lambda, \Lambda \times f)$ solution ✓
* uniqueness due to $\deg(G) = k + 2e - 1$✓

Generalisation for Rational Recovering (with Errors)



Cauchy Interpolation for Rational Recovering with Errors

Extension : Reconstruct $\frac{f}{g}$ from $r_i = \begin{cases} \frac{f(\alpha_i)}{g(\alpha_i)} \text{ or} \\ \text{erroneous value for } i \in E \end{cases}$

$\deg(f) < k, deg(g) < D$

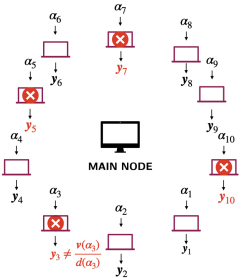
Given $(r_1, \ldots, r_n) \in \mathbb{F}_q$, Set $G = \prod_i^n (x - \alpha_i)$

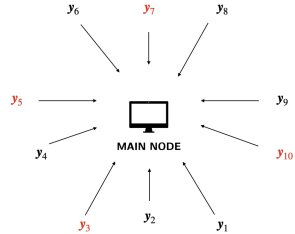
* Find $\psi, \phi \in \mathbb{F}_q[x]$ s.t. $\mathcal{L}(r, \alpha_i)\psi = \phi \mod G$
* $\deg(G) = k + D + 2e - 1$, $M = e + D$, $N = k + e$,
* Set $\Lambda = \prod_{i \in E}(x - \alpha_i)$, $(\Lambda \times g, \Lambda \times f)$ solution ✓
* uniqueness due to $\deg(G) = D + k + 2e - 1$✓

[Boyer,Kaltofen SNC'14,Kaltofen, Pernet et al.,ISSAC'17,ISSAC'19]

Outline

Application : Faulty Interpolation Evaluation Algorithm





* (BK'18,KPZ'19) Faulty Polynomial Linear System Solving

  Given $A(x) \in (\mathbb{F}[x])^{n \times \ell}$

  * Find $\mathbf{y}$ s.t. $A(x)\mathbf{y} = \mathbf{b}(\mathbf{x})$
  * Key equation : vectorial RR + bound on e
  * Bounds optimized with degrees of $A(x)$ and $b(x)$

Vectorial Rational Recovering with Errors I

Behind the Recovering Algorithm

* $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j) \rightsquigarrow \psi = \varphi R_i \mod \prod_{j=1}^{n}(x-\alpha_j)$
* Set $\Lambda = \prod_{i\in E}(x-\alpha_i)$, $(\Lambda \times d, \Lambda \times \boldsymbol{v})$ solution
* $\deg(\varphi_i) < N+\tau$, $\deg(\psi) < D+\tau$.
* Uniqueness by algebraic arguments: $n = N + D + 2e$ ✓
* Decoding Algorithm $\rightsquigarrow$
  - ⊙ Pointwise Evaluation and Lin Syst solving over $\mathbb{F}_q$
  - ◇ Find an element of the kernel of the associated matrix
  - * Thanks to uniqueness results, any solution leads to $\frac{\Lambda\times\boldsymbol{v}}{\Lambda\times d} \rightsquigarrow \frac{\boldsymbol{v}}{d}$

[Boyer,Kaltofen SNC'14,Kaltofen, Pernet and al.,ISSAC'17,ISSAC'19]

Outline

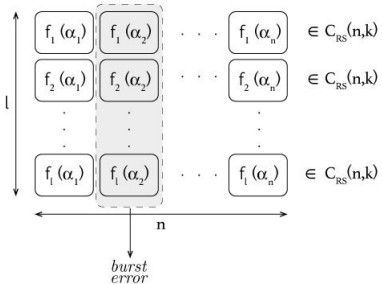
Beyond unique decoding guaranteed

Unique Decoding of Reed Solomon codes by RR can be extended to:

List Decoding	(Guruswami and Sudan, IEEE TIT'99)
Power Decoding	(Rosenkilde IEEE TIT'15)
Interleaving codes	(Bleichenbacher,Kiayas and al.ICALP'03)

Goal: Extend Interleaving decoders to Ractional vectors recovering with errors

Collaborative Decoding beyond $\frac{n-k}{2}$



$$M_{Y,N+\tau,D+\tau} = \left(\begin{array}{ccc|c} \mathcal{V}_{L,N+\tau} & & & -D_1\mathcal{V}_{L,D+\tau} \\ & \ddots & & \vdots \\ & & \mathcal{V}_{L,N+\tau} & -D_n\mathcal{V}_{L,D+\tau} \end{array} \right)$$

* Collaborative decoding: $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
* Error Model : $e = |\{i \in [1,\ldots,n] | \exists j,\ f_j(\alpha_i) \neq y_{ij}\}|$
* Can correct with high probability $e \leq \frac{l(n-k)}{l+1}$ (comparing to $e \leq \frac{(n-k)}{2}$)

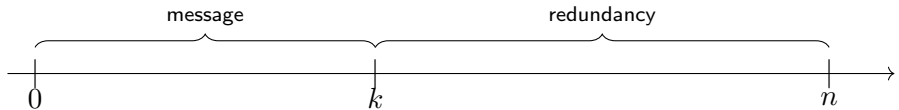
The power of Interleaving

k bits message $\xmapsto{n-k \text{ redundant bits}}$ n bits codeword

Bleichenbacher, Kiayas ICALP'03 and Schmidt, Sidorenko and al. IEEE-TIT'13

The power of Interleaving

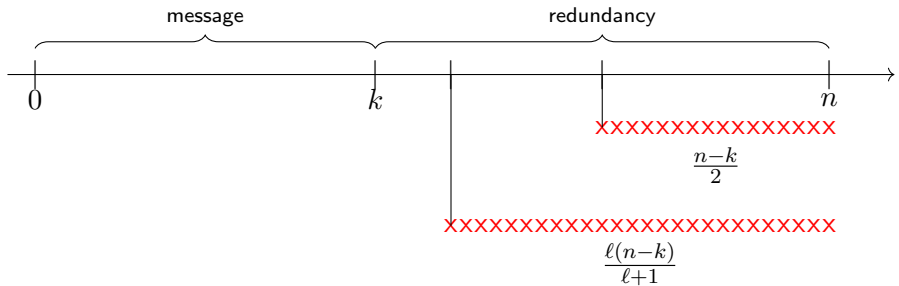
k bits message $\xmapsto{n-k \text{ redundant bits}}$ n bits codeword



Bleichenbacher, Kiayas ICALP'03 and Schmidt, Sidorenko and al. IEEE-TIT'13

The power of Interleaving

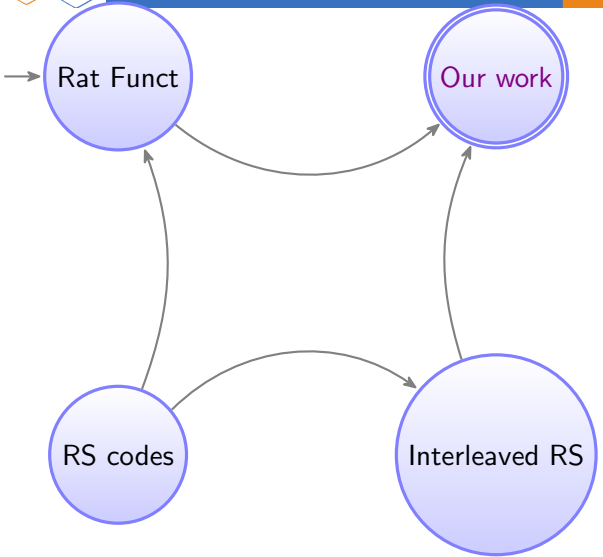
k bits message $\xmapsto{n-k \text{ redundant bits}}$ n bits codeword



Uniqueness no more possible without accepting failure

Bleichenbacher, Kiayas ICALP'03 and Schmidt, Sidorenko and al. IEEE-TIT'13

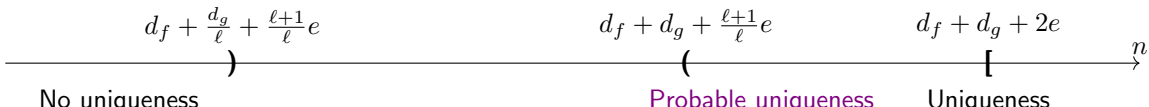
Applying Collaborative Decoding to FTA



Result on number of evaluation points

$$\ell n = \ell(d_f + d_g - 1) + (\ell + 1)e$$

- $d_f \geq \deg(f) := \max_{1 \leq i \leq n} \deg(f_i)$, (equivalent of k)
- $d_g = \deg(g)$,
- e is the number of erroneous evaluations.
  - $e = |E| = |\{l \in \{1, \ldots, \ell\} \mid A_l \boldsymbol{f}(\alpha_l) \neq g(\alpha_l)\boldsymbol{b}_l\}|$.



[G. and Lebreton and al ISIT'19,ISSAC'20-21-24]

Idea of the proof -replacing $2e$ by $\frac{\ell}{\ell+1}$-

Scenario

$E = \{i \in [1, \ldots, n] | \exists j,\ \frac{f_j(\alpha_i)}{g(\alpha_i)} \neq y_{ij}\}$.

We can correct with high probability $E \leq \frac{l(n-k)}{l+1}$

Goal: show that for (ψ, φ_i) s.t. $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$

- ◇ There is a specific solution of type $(\Lambda g, \Lambda f_1, \ldots, \Lambda f_n)$
  - ◇ Give a partition on $E = \cup_{i=1}^{\ell} I_i$, such that $|I_i| \leq \frac{E}{\ell}$
  - ◇ Construct a solution according to E
- ∗ Prove that almost all solution are of the type $(\Lambda g, \Lambda f_1, \ldots, \Lambda f_n)$
  - ∗ Use of Probabilistic argument on the rank of the kernel of the associated matrix (leads to $\frac{d_g+|E|}{q}$)

Our result

Theorem

Let $e_{max} := \frac{\ell}{\ell+1}(n - d_f - d_g + 1)$. *If* $e < e_{max}$ *then* $\forall(\varphi, \psi_1, \ldots, \psi_\ell)$ *solutions of the "Simultaneous Rational Function Reconstruction" problem, the vector of rational functions*

$$\left(\frac{\psi_1}{\varphi}, \ldots, \frac{\psi_\ell}{\varphi}\right)$$

is unique with probability at least

$$\mathbb{P}_u(e) \geq 1 - \frac{1}{q-1}\frac{1}{q^{(\ell+1)(e_{max}-e)}}$$

[Abbondati and G. and Lebreton ISSAC'24-JSC'26]

Main ideas of the Proof

Remark that

$\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$ is equivalent to $\psi_i = \varphi R_i \mod \prod_{j=1}^{n}(x - \alpha_j)$

* $\psi_i = \varphi R_i \mod \prod_{j=1}^{n}(x - \alpha_j)$ is equivalent to $\psi_i' = \varphi' R_i \mod \Lambda$
* Decoding failure is upper bounded by the probability of finding $(\psi_i', \varphi') \neq 0$
* Counting elements here gives a better upper bound than the previous approach

Overview

	Previously	Our work
IRS [1]	$t < \frac{\ell}{\ell+1}(n - d_f + 1) \quad \mathbb{P}_f \leq \frac{1}{q-1}\frac{1}{q^{(\ell+1)(e_{max}-e)}}$	
SRFR [2]	$e < \frac{\ell}{\ell+1}(n - d_f - d_g + 1)$ $\mathbb{P}_f \leq \frac{d_g+e}{q}$	$e < \frac{\ell}{\ell+1}(n - d_f - d_g + 1)$ $\mathbb{P}_f \leq \frac{1}{q-1}\frac{1}{q^{(\ell+1)(e_{max}-e)}}$

SRFR Simultaneous Rational Function Reconstruction

[1] Schmidt, Sidorenko et al. IEEE TIT'09

[2] G., Lebreton et al ISIT'19 and Abbondati, G. et al. '24 and '25

..extension on the moduli

Multipoint-Multiprecision Approach

Idea : Since $(f_1/g(\alpha_1), \ldots, f_l/g(\alpha_n)) \rightsquigarrow r_k = f_k/g_k \bmod \prod_{i=1}^{n}(x-\alpha_j)$, compute $r_j(x) = \boldsymbol{f}(x)/g(x) \bmod (x-\alpha_j)^{\ell_j}$

Previous Model

- $|\{\alpha_1, \ldots, \alpha_n\}| = deg \prod(x-\alpha_j)$
- Hyp : $g(\alpha_i) \neq 0$ or large char field

[G., Lebreton et al. JSC'22]

- $r_j(x) = \boldsymbol{f}(x)/g(x) \bmod (x-\alpha_j)^{\ell_j}$ for a $\ell_j > 1$
- Handle poles by modifying the key equation

Multiprecision approach: uniqueness

No error
$\sum_{j=1}^{\delta} \ell_j \geq N + D - 1$

Unique Decoding
$\sum_{j=1}^{\delta} \ell_j \geq (N + \hat{\tau}) + D + \hat{\tau} - 1$

Interleaving
$L \geq N + D - 1 + 2\hat{\tau}_v + \lceil \frac{\hat{\tau}_r}{n} \rceil + \hat{\tau}_r$

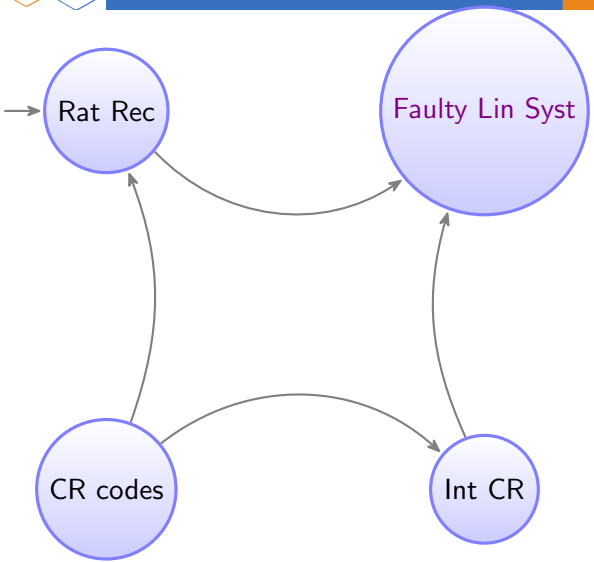
$$E := \{j | (x - \alpha_j)^{v_j} \boldsymbol{f}(x) \neq r_j(x) g(x) \, mod (x - \alpha_j)^{\ell_j}\}$$

Two type of errors :

- Valuation errors $E_v := \{j |\, v_j \neq min(val_{\alpha_j}(g), \ell_j)\}$ and $\hat{\tau}_v \geq |E_v|$
- Evaluation errors $E_r := \{j |\, j \in E \cap (v_j = val_{\alpha_j}(g))\}$ and $\mathrm{tr} \geq |E_r|$

Fix $\hat{\tau}_v := \sum_{j=1}^{\tau_v} \ell_j$ and $\hat{\tau}_r := \sum_{j=1}^{\tau_r} \ell_j$.
Unique decoding for all error in E_v and almost errors in E_r : $\leq \frac{(D+\hat{\tau})}{q}\}$

Chinese Reminder codes (CR) for Faulty Linear Systems



[Abbondati,Afflatet and al. ITW'23, Abbondati,G.and al'23]

CR codes and Linear System Solving with Integers

Definition (CR codes)

Given

- $0 < p_1 < p_2 < ... < p_n$, prime numbers
- Let k and $K = \prod_{i=1}^{k} p_i$
- $\mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_n}$

$$CR(P; n, K) = \{([c]_{p_1}, ..., [c]_{p_n}) : c \in \mathbb{N} \text{ et } c < K\}$$

Define $\Lambda = \prod_{i|r_i \neq c_i} p_i$

$N = p_0 p_1 \cdots p_{n-1}$

Evaluation - Interpolation codes

Reed-Solomon codes	Chinese Remainder codes
$f \in \mathbb{F}_q[x]_{<k}$	$C \in [0, K)$
Encoding $\pi_{(x-\alpha_1)} \quad \cdots \quad \pi_{(x-\alpha_n)}$	$\pi_{p_1} \quad \cdots \quad \pi_{p_n}$
$\vec{c} = (f(\alpha_1), \ldots, f(\alpha_n))$	$\vec{c} = ([C]_{p_1}, \ldots, [C]_{p_n})$
Channel $\vec{e} = (e_1, \ldots, e_n)$	$\vec{e} = (e_1, \ldots, e_n)$
$\vec{y} = (y_1, \ldots, y_n) \leftrightarrow R(x) \in \mathbb{F}_q[x]_{<n}$	$\vec{r} = (r_1, \ldots, r_n) \leftrightarrow R \in \mathbb{Z}_N$
Decoding	
$f(x) \in \mathbb{F}_q[x]_{<k}$	$C \in [0, K)$

Extension of Interleaved Rational Numbers codes

$$\Lambda f_i = \Lambda g R_i \mod N \begin{cases} \psi_i = \Lambda f_i \\ \varphi = \Lambda g \end{cases} \psi_i = \varphi R_i \mod N \qquad (\varphi, \psi_1, \ldots, \psi_\ell) \in \mathcal{L} = \begin{pmatrix} 1 & R_1 & \cdots & R_\ell \\ 0 & N & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & N \end{pmatrix} \subseteq \mathbb{Z}^{\ell+1}$$

Abbondati, G. et al ISSAC'24 and JSC'26

Extension of Interleaved Rational Numbers codes

$$\Lambda f_i = \Lambda g R_i \mod N \begin{cases} \psi_i = \Lambda f_i \\ \varphi = \Lambda g \end{cases} \quad \psi_i = \varphi R_i \mod N \qquad (\varphi, \psi_1, \ldots, \psi_\ell) \in \mathcal{L} = \begin{pmatrix} 1 & R_1 & \cdots & R_\ell \\ 0 & N & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & N \end{pmatrix} \subseteq \mathbb{Z}^{\ell+1}$$

$\Lambda \leq 2^\tau$

Short elements of $\mathcal{L}$

$$(\Lambda g, \Lambda f_1, \ldots, \Lambda f_\ell) \in S_R = \{(\varphi, \psi_1, \ldots, \psi_\ell) \in \mathcal{L} : 0 < \varphi < 2^\tau G, |\psi_i| < 2^\tau F\} \subseteq \mathcal{L}$$

LLL

Abbondati, G. et al ISSAC'24 and JSC'26

Perspectives

- Malicious adversary in FTA [work in progress...]
- Codes over ideals for LRC codes [submitted Cavicchioni, G. et al '26]
- Algebraic codes decoding for suitable FTA
- Early Termination (online algorithms for decoding)

[Abbondati, Franzoi,G. Lebreton, in the direction of Brakensiek et al. arxiv'25]

Thank you

- Eleonora Guerrini -

LIRMM - Université de Montpellier