Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon Codes.

Ilaria Zappatore
a joint work with Eleonora Guerrini
LIRMM, Montpellier

Journées Nationales de Calcul Formel 2019
CIRM, Luminy.

Table of contents

Polynomial linear system solving

Polynomial linear system

Fixed a finite field $\mathbb{F}_q$, $m \geq n \geq 1$, we consider the problem of solving a **full rank consistent polynomial linear system**

$$A(x)\mathbf{y}(x) = b(x)$$

$$\begin{pmatrix} a_{1,1}(x) & a_{1,2}(x) & \dots & a_{1,n}(x) \\ a_{2,1}(x) & a_{2,2}(x) & \dots & a_{2,n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ a_{m,1}(x) & a_{m,2}(x) & \dots & a_{m,n}(x) \end{pmatrix} \begin{pmatrix} y_1(x) \\ y_2(x) \\ \vdots \\ y_n(x) \end{pmatrix} = \begin{pmatrix} b_1(x) \\ b_2(x) \\ \vdots \\ b_m(x) \end{pmatrix}$$

where,

- $A(x)$ is a **full rank** $m \times n$ matrix whose entries are polynomials in $\mathbb{F}_q[x]$,
- $b(x)$ is an m-th vector of polynomials in $\mathbb{F}_q[x]$.

Polynomial linear system

Fixed a finite field $\mathbb{F}_q$, $m \geq n \geq 1$, we consider the problem of solving a **full rank consistent polynomial linear system**

$$A(x)\mathbf{y}(x) = b(x)$$

There is a **unique rational solution**

$$\boldsymbol{y}(x) := \frac{\boldsymbol{f}(x)}{g(x)} = \begin{pmatrix} \frac{f_1(x)}{g(x)} \\ \frac{f_2(x)}{g(x)} \\ \vdots \\ \frac{f_n(x)}{g(x)} \end{pmatrix}$$

where $g(x)$ is the monic **least common denominator** and

$$\text{GCD}(\mathbf{f}, g) = \text{GCD}(\text{GCD}_i(f_i), g) = 1. \quad (1)$$

Our aim is to find the polynomials $\boldsymbol{f}$ and g such that

$$A(x)\mathbf{f}(x) = g(x)b(x).$$

Polynomial linear system

Fixed a finite field $\mathbb{F}_q$, $m \geq n \geq 1$, we consider the problem of solving a **full rank consistent polynomial linear system**

$$A(x)\frac{\boldsymbol{f}(x)}{g(x)} = b(x)$$

There is a **unique rational solution**

$$\boldsymbol{y}(x) := \frac{\boldsymbol{f}(x)}{g(x)} = \begin{pmatrix} \frac{f_1(x)}{g(x)} \\ \frac{f_2(x)}{g(x)} \\ \vdots \\ \frac{f_n(x)}{g(x)} \end{pmatrix}$$

where $g(x)$ is the monic **least common denominator** and

$$\mathrm{GCD}(\mathbf{f}, g) = \mathrm{GCD}(\mathrm{GCD}_i(f_i), g) = 1. \tag{1}$$

Our aim is to find the polynomials $\boldsymbol{f}$ and g such that

$$A(x)\mathbf{f}(x) = g(x)b(x).$$

Evaluation/Interpolation

Fix $L \geq df + dg + 1$ distinct **evaluation points** $\{\alpha_1, \alpha_2, \ldots, \alpha_L\}$, where

- $df \geq \max_{1 \leq i \leq n} \deg(f_i)$,
- $dg \geq \deg(g)$.

we can **uniquely** reconstruct f and g by

- **evaluating** the polynomial matrix $A(x)$ and $b(x)$ at α_l, $1 \leq l \leq L$

Evaluation/Interpolation

Fix $L \geq df + dg + 1$ distinct **evaluation points** $\{\alpha_1, \alpha_2, \ldots, \alpha_L\}$, where

- $df \geq \max_{1 \leq i \leq n} \deg(f_i)$,
- $dg \geq \deg(g)$.

we can **uniquely** reconstruct f and g by

- **evaluating** the polynomial matrix $A(x)$ and $b(x)$ at α_l, $1 \leq l \leq L$
- **solving** the evaluating system

$$\left[A(\alpha_l) \begin{pmatrix} \varphi_1(\alpha_l) \\ \varphi_2(\alpha_l) \\ \vdots \\ \varphi_n(\alpha_l) \end{pmatrix} - \psi(\alpha_l) b(\alpha_l) = 0 \right]_{l \in \{1,\ldots,L\}}$$

Evaluation/Interpolation

Fix $L \geq df + dg + 1$ distinct **evaluation points** $\{\alpha_1, \alpha_2, \ldots, \alpha_L\}$, where

- $df \geq \max_{1 \leq i \leq n} \deg(f_i)$,
- $dg \geq \deg(g)$.

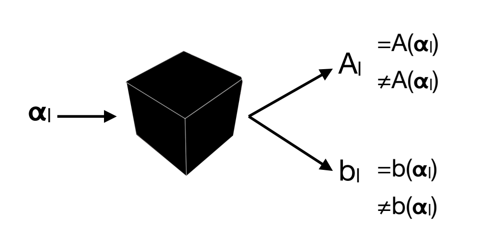
we can **uniquely** reconstruct f and g by

- **evaluating** the polynomial matrix $A(x)$ and $b(x)$ at α_l, $1 \leq l \leq L$
- **solving** the evaluating system

$$\left[A(\alpha_l) \begin{pmatrix} \varphi_1(\alpha_l) \\ \varphi_2(\alpha_l) \\ \vdots \\ \varphi_n(\alpha_l) \end{pmatrix} - \psi(\alpha_l) b(\alpha_l) = 0 \right]_{l \in \{1,\ldots,L\}}$$

- **interpolating** from the evaluated solution the parametric one.

Polynomial linear system solving with errors



Erroneous evaluation

An evaluation point α_l is **erroneous** if

$$A_l \boldsymbol{f}(\alpha_l) \neq g(\alpha_l) b_l$$

$E := |\{l \mid A_l \boldsymbol{f}(\alpha_l) \neq g(\alpha_l) b_l\}|.$

Since A_l is **full rank**[1] for any l,

$$A_l \boldsymbol{f}(\alpha_l) \neq g(\alpha_l) b_l \Longrightarrow A_l \neq A(\alpha_l) \text{ or/and } b_l \neq b(\alpha_l).$$

[1]We omit the rank drops study.

Polynomial linear system solving with errors

How many evaluation points?

[BK14] and [Kal+17] proved that with

$$L \geq L_{BK} := df + dg + 2e + 1$$

evaluation points, it is possible to **uniquely reconstruct** $\boldsymbol{f}$ and g.

- $df \geq \max_{1 \leq i \leq n} \deg(f_i)$,
- $dg \geq \deg(g)$,
- $e \geq |E| := |\{l \mid A_l \boldsymbol{f}(\alpha_l) \neq g(\alpha_l) b_l\}|$

Polynomial linear system solving with errors

Main idea

- For any correct evaluations we have

$$A_l \boldsymbol{f}(\alpha_l) = g(\alpha_l) b_l$$

Polynomial linear system solving with errors

Main idea

- For any correct evaluations we have

$$A_l \boldsymbol{f}(\alpha_l) = g(\alpha_l) b_l$$

- let Λ be the **error locator polynomial**,

$$\Lambda := \prod_{l \in E} (x - \alpha_l),$$

  that is monic and has degree $deg(\Lambda) \leq e$;

Main idea

- For any correct evaluations we have

$$A_l \boldsymbol{f}(\alpha_l) = g(\alpha_l) b_l$$

- let Λ be the **error locator polynomial**,

$$\Lambda := \prod_{l \in E} (x - \alpha_l),$$

  that is monic and has degree $deg(\Lambda) \leq e$;
- we put for any $l \in \{1, \ldots, L\}$,

$$A^l \underbrace{\boldsymbol{f}(\alpha_l)\Lambda(\alpha_l)}_{\boldsymbol{\varphi}(\alpha_l)} = \underbrace{g(\alpha_l)\Lambda(\alpha_l)}_{\psi(\alpha_l)} b^l$$

  where $deg(\boldsymbol{\varphi}) \leq df + e$ and $deg(\psi) \leq dg + e$.

Polynomial linear system solving with errors

Theorem [BK14]

Assume that

- the number of **erroneous evaluations** is $\leq e$,
- the number of the **correct evaluations** for which A_l is full rank is $\geq df + dg + e + 1$

Let $(\varphi_{min}, \psi_{min})$ be a solution of

$$\begin{cases} A_1 \varphi(\alpha_1) - \psi(\alpha_1) b_1 = 0 \\ \vdots \\ A_L \varphi(\alpha_L) - \psi(\alpha_L) b_L = 0 \end{cases}$$

where ψ_{min} is scaled to have leading coefficient 1 in x and it has minimal degree of all such solutions. Then

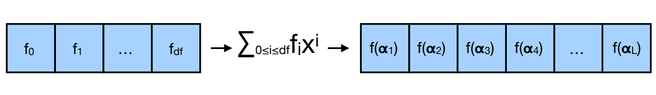
$$\varphi_{min} = \Lambda f, \psi_{min} = \Lambda g$$

Let $\mathbb{F}_q$ be a finite field. Fixed:

- $df < L \le q$,
- L **evaluation points**, $\{\alpha_1, \ldots, \alpha_L\}$,

The **Reed Solomon Code** of **length** L and **dimension** $df + 1$ is the set

$$RS_q := \{(f(\alpha_1), \ldots, f(\alpha_L)) \mid f \in \mathbb{F}_q[x], deg(f) \le df\}.$$



The Reed Solomon code is **Maximum Distance Separable** (MDS), i.e. it matches the Singleton bound. Its **error correction capability** is

$$e_{RS} \le \frac{L - df - 1}{2}$$

Polynomial linear system solving with errors

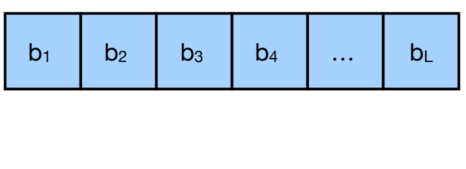
The [BK14] method is a **generalization** of the **Berlekamp-Welch decoding** for **Reed Solomon** codes.

If $m = n = 1$, $A = I_1$, g constant polynomial 1,

Recover the solution of the polynomial linear system

$$\updownarrow$$

Decoding of Reed Solomon code



Polynomial linear system solving with errors

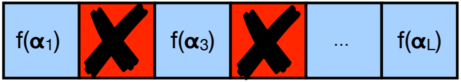
The [BK14] method is a **generalization** of the **Berlekamp-Welch decoding** for **Reed Solomon** codes.

If $m = n = 1$, $A = I_1$, g constant polynomial 1,

Recover the solution of the polynomial linear system

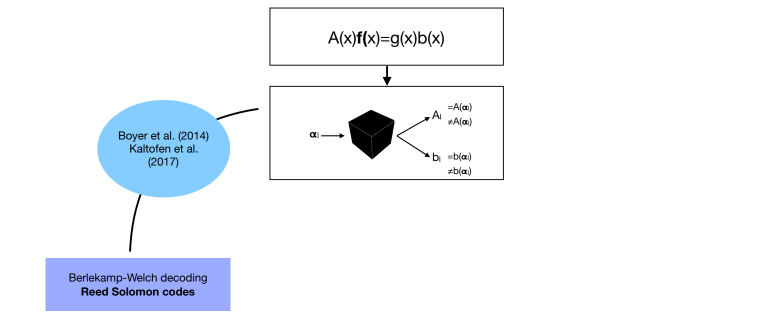
$\updownarrow$

Decoding of Reed Solomon code



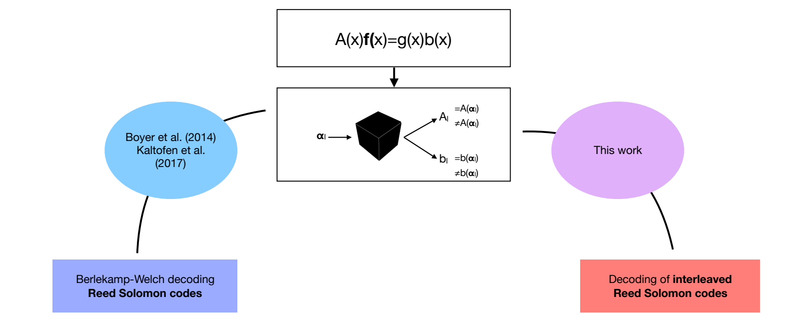
Generalization of the decoding of interleaved RS codes

Our approach



Our purpose is to reconstruct the solution using a technique, inspired by the [BKY03] decoding of **interleaved RS codes**.

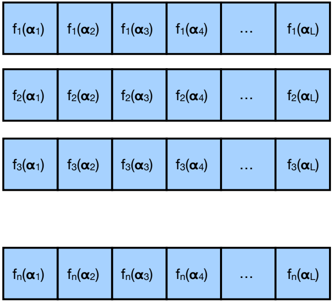
Our approach



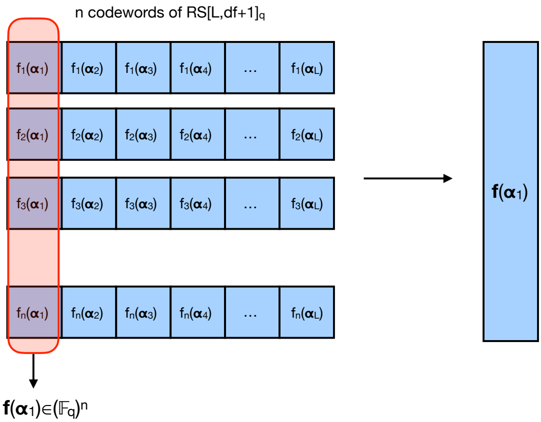
Our purpose is to reconstruct the solution using a technique, inspired by the [BKY03] decoding of **interleaved RS codes**.

Interleaved RS codes

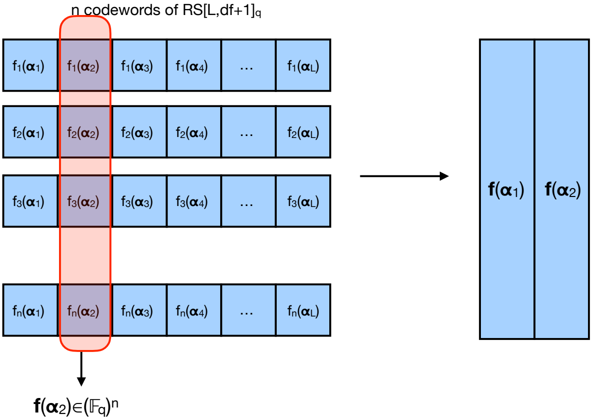
n codewords of $RS[L,df+1]_q$



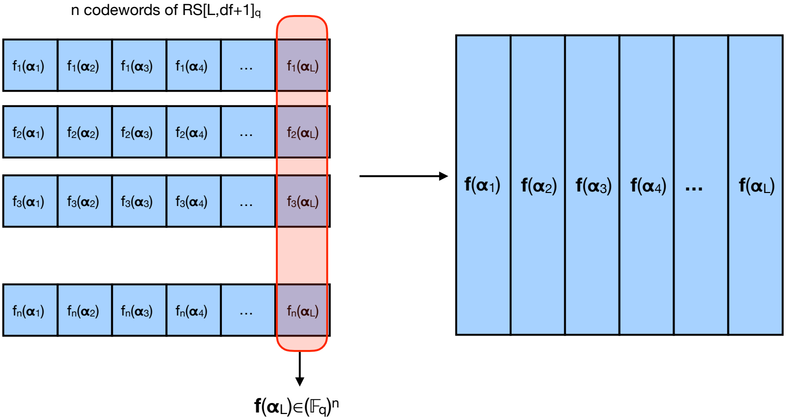
Interleaved RS codes



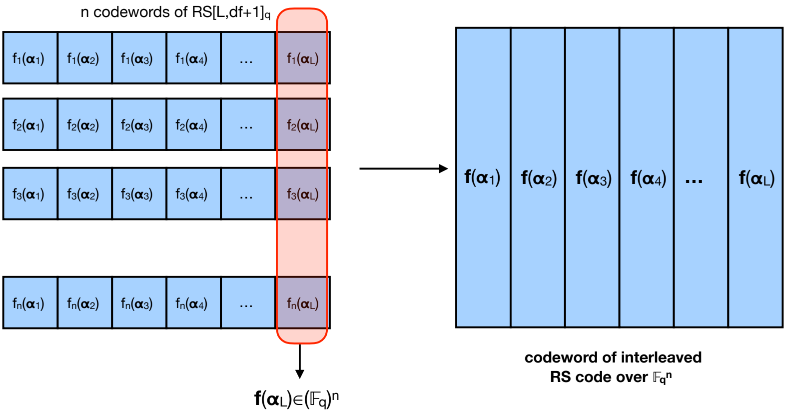
Interleaved RS codes



Interleaved RS codes



Interleaved RS codes



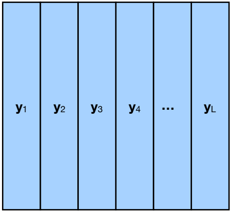
Decoding interleaved Reed Solomon codes

An instance of the **Simultaneous Polynomial Reconstruction** (SPR) is $(\boldsymbol{y}_l)_{1\leq l\leq L} = (y_{il})_{\substack{1\leq i\leq n \\ 1\leq l\leq L}}$ such that there exist

- $E \subset \{1, \ldots, L\}$,
- polynomials $(f_1, \ldots, f_r)$, with $\deg(f_i) \leq df$

$$\begin{cases} \boldsymbol{y}_l = \boldsymbol{f}(\alpha_l) & l \notin E \\ \boldsymbol{y}_l \neq \boldsymbol{f}(\alpha_l) & l \in E \end{cases}$$

The solution of the SPR is the tuple $\boldsymbol{f} = (f_1, \ldots, f_n) \in (\mathbb{F}_q[x])^n$



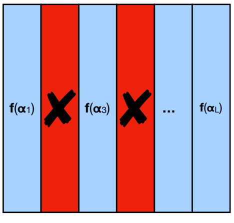
Decoding interleaved Reed Solomon codes

An instance of the **Simultaneous Polynomial Reconstruction** (SPR) is $(\boldsymbol{y}_l)_{1 \leq l \leq L} = (y_{il})_{\substack{1 \leq i \leq n \\ 1 \leq l \leq L}}$ such that there exist

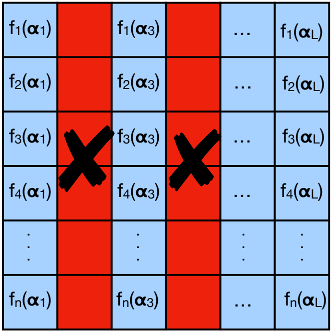
- $E \subset \{1, \ldots, L\}$,
- polynomials $(f_1, \ldots, f_r)$, with $\deg(f_i) \leq df$

$$\begin{cases} \boldsymbol{y}_l = \boldsymbol{f}(\alpha_l) & l \notin E \\ \boldsymbol{y}_l \neq \boldsymbol{f}(\alpha_l) & l \in E \end{cases}$$

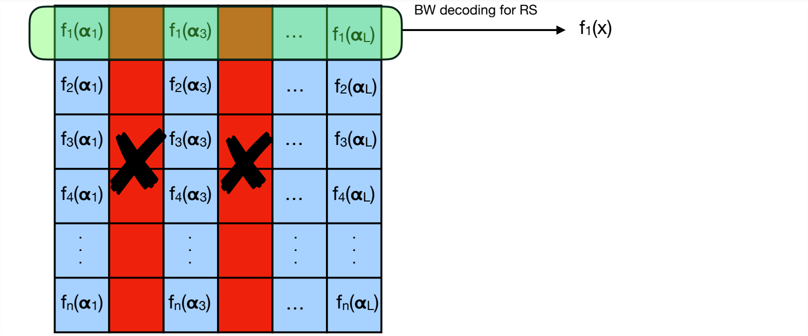
The solution of the SPR is the tuple $\boldsymbol{f} = (f_1, \ldots, f_n) \in (\mathbb{F}_q[x])^n$



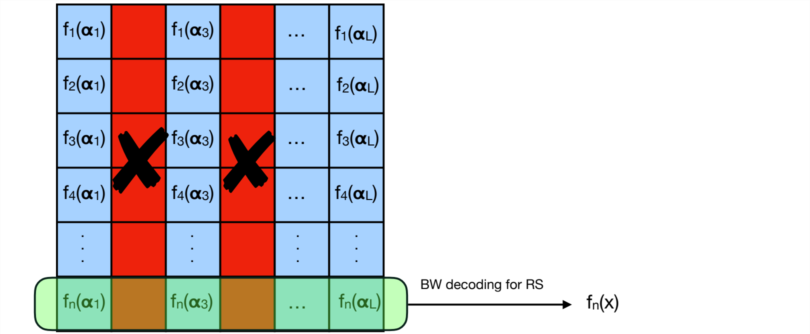
Decoding interleaved RS codes



Decoding interleaved RS codes



Decoding interleaved RS codes



In this way,

- recover $\boldsymbol{f} = (f_1, \ldots, f_n) \in (\mathbb{F}_q[x])^n$,
- correct up to $\frac{L-df-1}{2}$ errors (MDS).

Decoding interleaved RS codes

Theorem [BKY03]

Given $(y_{il})_{\substack{1\le i\le n\\1\le l\le L}} \in (\mathbb{F}_q)^{nL}$ where $e \le |E| = \frac{n(L-df-1)}{n+1}$

Probabilistic assumptions

Assume that for any $i \in \{1, \ldots, n\}$,

- $l \in E$, y_{il} are **uniformly distributed** over $\mathbb{F}_q$,
- $l \notin E$, $y_{il} = f_i(\alpha_l)$ and $f_1, \ldots, f_n$ are **uniformly distributed** over the vector space of polynomials of $\mathbb{F}_q[x]$ of degree at most df;

The linear system,

$$\begin{cases} [m_1(\alpha_l) = y_{1l}\Lambda(\alpha_l)]_{1\le l\le L} \\ \ldots \\ [m_r(\alpha_l) = y_{nl}\Lambda(\alpha_l)]_{1\le l\le L} \end{cases} \tag{2}$$

admits at most one solution with probability at least $1 - e/q$.

Decoding interleaved RS codes

Theorem [BMS04]

Given $(y_{il})_{\substack{1\leq i\leq n\\ 1\leq l\leq L}} \in (\mathbb{F}_q)^{nL}$ where $e := |E| = \frac{n(L-df-1)}{n+1}$

Probabilistic assumptions

Assume that for any $i \in \{1,\ldots,n\}$,

- $l \in E$, y_{il} are **uniformly distributed** over $\mathbb{F}_q$,
- $l \notin E$, $y_{il} = f_i(\alpha_l)$,

The linear system,

$$\begin{cases} [m_1(\alpha_l) = y_{1l}\Lambda(\alpha_l)]_{1\leq l\leq L} \\ \ldots \\ [m_r(\alpha_l) = y_{nl}\Lambda(\alpha_l)]_{1\leq l\leq L} \end{cases} \tag{3}$$

admits at most one solution with probability at least $1 - \frac{exp(1/(q^{r-2}))}{q}$.

Decoding interleaved RS codes

If $n \geq 1$ then,

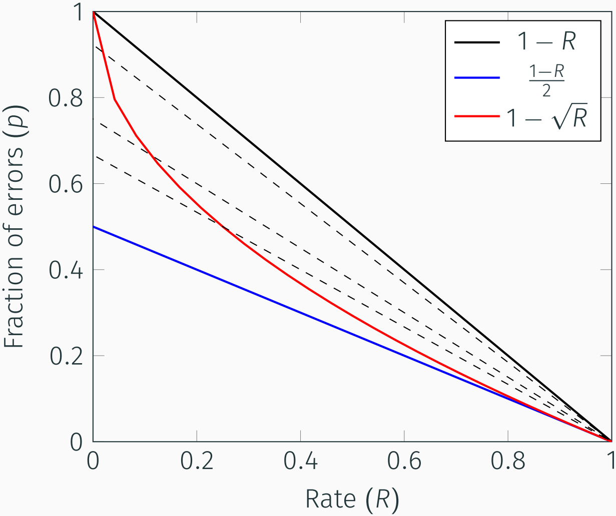
probabilistic assumptions		
$\downarrow$		
$\frac{n(L-df-1)}{n+1}$	$\geq$	$\frac{L-df-1}{2}$
$\downarrow$		$\downarrow$
unique decoding		**unique** decoding
error probability $\mathcal{O}(1/q)$		

Under some **probabilistic assumptions** it is possible to decode **beyond the unique decoding bound**.

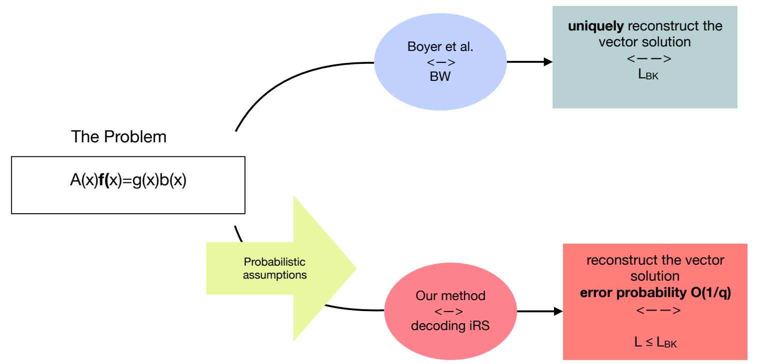
Decoding interleaved RS codes

If $n \geq 1$ then,

$$\frac{n(1-R)}{n+1} \geq \frac{1-R}{2}$$

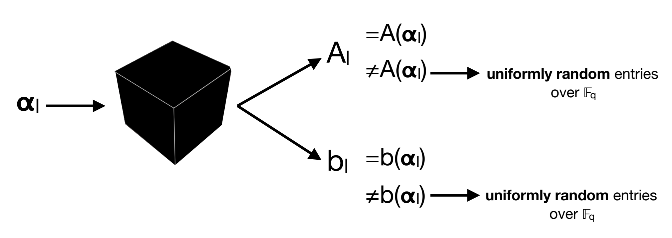


Our scenario



We focus on the square case $m = n$.

Our scenario



We fix $L := \frac{n(df+e+1)+dg+e}{n}$ evaluation points, where

- $df \geq \deg(f) := \max_{1\leq i\leq n} \deg(f_i)$,
- $dg = \deg(g)$,
- e is a bound on the number of erroneous evaluations

$$e \geq |E| := |\{l \in \{1,\ldots,L\} \mid A_l \boldsymbol{f}(\alpha_l) \neq g(\alpha_l) b_l\}|.$$

Generalization of the decoding of interleaved RS codes

For any $l \in \{1, \ldots, L\}$ we study the homogeneous linear systems

$$A_l \boldsymbol{\gamma}_l - \sigma_l b_l = 0$$

Since A_l is full rank, the kernel is one-dimensional. Let $(\boldsymbol{\gamma}_l, \sigma_l) = (\gamma_{l1}, \ldots, \gamma_{ln}, \sigma_l)$ be the generator of the kernel, then

$$\mathbf{y}_l := \frac{\boldsymbol{\gamma}_l}{\sigma_l} = \begin{cases} = \frac{f(\alpha_l)}{g(\alpha_l)} & l \notin E \\ \neq \frac{f(\alpha_l)}{g(\alpha_l)} & l \in E \text{ uniformly random} \end{cases}$$

Generalization of the decoding of interleaved RS codes

Now, we consider the key equations

$$\begin{cases} \boldsymbol{\varphi}(\alpha_1) - \boldsymbol{y}_1 \psi(\alpha_1) = 0 \\ \dots \\ \boldsymbol{\varphi}(\alpha_L) - \boldsymbol{y}_L \psi(\alpha_L) = 0 \end{cases} \tag{4}$$

- $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_n) \in (\mathbb{F}_q[x])^n$ and $\deg(\varphi_i) \leq df + e$,
- $\psi \in \mathbb{F}_q[x]$, $\deg(\psi) \leq dg + e$.

Generalization of the decoding of interleaved RS codes

Now, we consider the key equations

$$\begin{cases} \boldsymbol{\varphi}(\alpha_1) - \boldsymbol{y}_1 \psi(\alpha_1) = 0 \\ \dots \\ \boldsymbol{\varphi}(\alpha_L) - \boldsymbol{y}_L \psi(\alpha_L) = 0 \end{cases} \tag{4}$$

- The system has nL equations and $n(df + e + 1) + dg + e + 1 = nL + 1$ unknowns, i.e. the coefficients of $\boldsymbol{\varphi}$ and ψ.
- If the rank of the coefficient matrix is nL, the kernel is one-dimensional and $(\boldsymbol{\varphi}, \psi)$ its generator is

$$\boldsymbol{\varphi} = \Lambda \boldsymbol{f}, \psi = \Lambda g.$$

Generalization of the decoding of interleaved RS codes

Theorem (Guerrini, Z. 2019)

Under the previous assumptions,

$$Pr[\text{rank} < nL] \leq \frac{exp(1 - q^{n-2})}{q}$$

The **error probability** is $\mathcal{O}(1/q)$.

Moreover if $n \geq 1$,

$$L = \frac{n(df + e + 1) + dg + e}{n} \leq df + dg + 2e + 1 = L_{BK}$$

Generalization of the decoding of interleaved RS codes

Data: $(A_l, b_l)_{1 \le l \le L}$ and df, dg, e
Result: (f, g) or `fail`
$L := \lceil \frac{n(df+e+1)+dg+e}{n} \rceil$;
find a basis $\{(\boldsymbol{\gamma}_l, \sigma_l)\}$ of the right kernel of $A_l \boldsymbol{\gamma}_l - \sigma_l b_l = 0$ for $l = 1, \ldots, L$;
$\boldsymbol{y}_l := \frac{\boldsymbol{\gamma}_l}{\sigma_l}$;
construct the key equation (4) and, given M the coefficient matrix;
if $rank(M) == n(df + e + 1) + dg + e$ **then**
  find a basis $\{(\boldsymbol{\varphi}, \psi)\}$ of the right kernel of M;
  $\Lambda := GCD(\boldsymbol{\varphi}, \psi)$;
  $\boldsymbol{f} := \frac{\boldsymbol{\varphi}}{\Lambda}$ and $g := \frac{\psi}{\Lambda}$;
else
  return `fail`
end

Experiments and conclusions

Experiments

We implement our algorithm in `SageMath`.

We apply 100 times our method to solve 100 different polynomial linear systems of size 3 and number of errors 4.

We denote,

- p^* represents the number of times in which the rank is less than nL,
- p the percentage of theoretical error probability of our theorem, $\frac{exp(1-q^{n-2})}{q}$

We obtain the following results:

q	p^*	p
2^5	$0,9\%$	$3,22\%$
2^6	$0,33\%$	$1,58\%$
2^9	$0,16\%$	$0,19\%$

Open Problems

- Study the **rank drops** case,
- better **upper bound** the **error probability**,
- $dg \geq deg(g)$.

Thanks for your attention.

References

Brice Boyer and Erich L. Kaltofen. “Numerical Linear System Solving with Parametric Entries by Error Correction”. In: *Proceedings of the 2014 Symposium on Symbolic-Numeric Computation*. SNC ’14. Shanghai, China: ACM, 2014, pp. 33–38. ISBN: 978-1-4503-2963-7. DOI: 10.1145/2631948.2631956. URL: http://doi.acm.org/10.1145/2631948.2631956.

Daniel Bleichenbacher, Aggelos Kiayias, and Moti Yung. "Decoding of Interleaved Reed Solomon Codes over Noisy Data.". In: *J.C.M. Baeten, J.K. Lenstra, J. Parrow, G.J. Woeginger (eds) Automata, Languages and Programming. ICALP 2003. Lecture Notes in Computer Science*, vol. 2719. Springer, Berlin, Heidelberg., 2003.

A. Brown, L. Minder, and A. Shokrollahi. "Probabilistic decoding of interleaved RS-codes on the q-ary symmetric channel". In: *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.* June 2004, pp. 326–326. DOI: 10.1109/ISIT.2004.1365363.

Erich L. Kaltofen, Clément Pernet, Arne Storjohann, and Cleveland Waddell. "Early Termination in Parametric Linear System Solving and Rational Function Vector Recovery with Error Correction". In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*. ISSAC '17. Kaiserslautern, Germany: ACM, 2017, pp. 237–244. ISBN: 978-1-4503-5064-8. DOI: 10.1145/3087604.3087645. URL: http://doi.acm.org/10.1145/3087604.3087645.