Ilaria Zappatore
INRIA Saclay, équipe GRACE

Simultaneous Rational Function Reconstruction and applications to Algebraic Coding Theory

PolSys-SpecFun Seminar
February 19, 2021

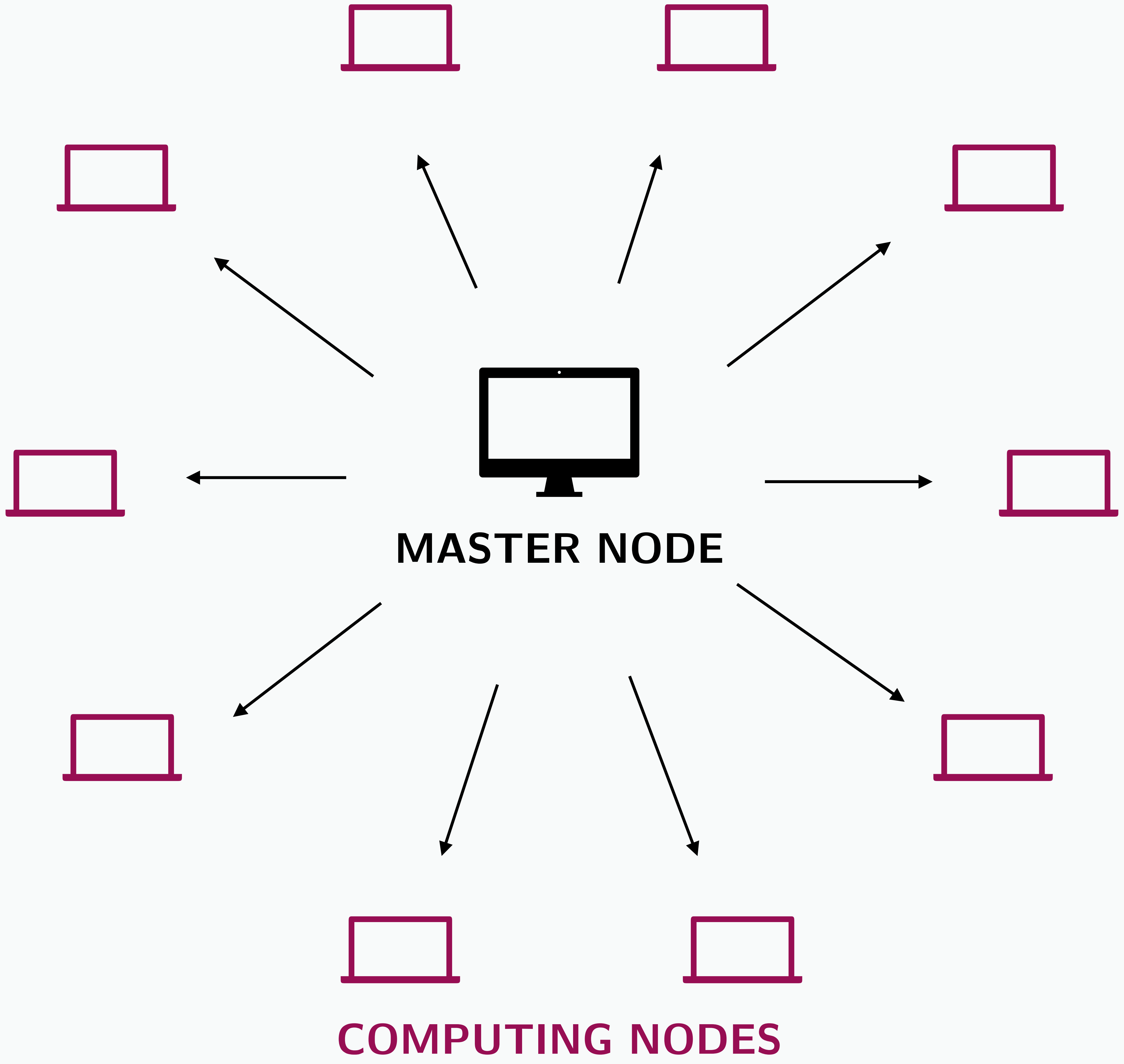
Starting Point

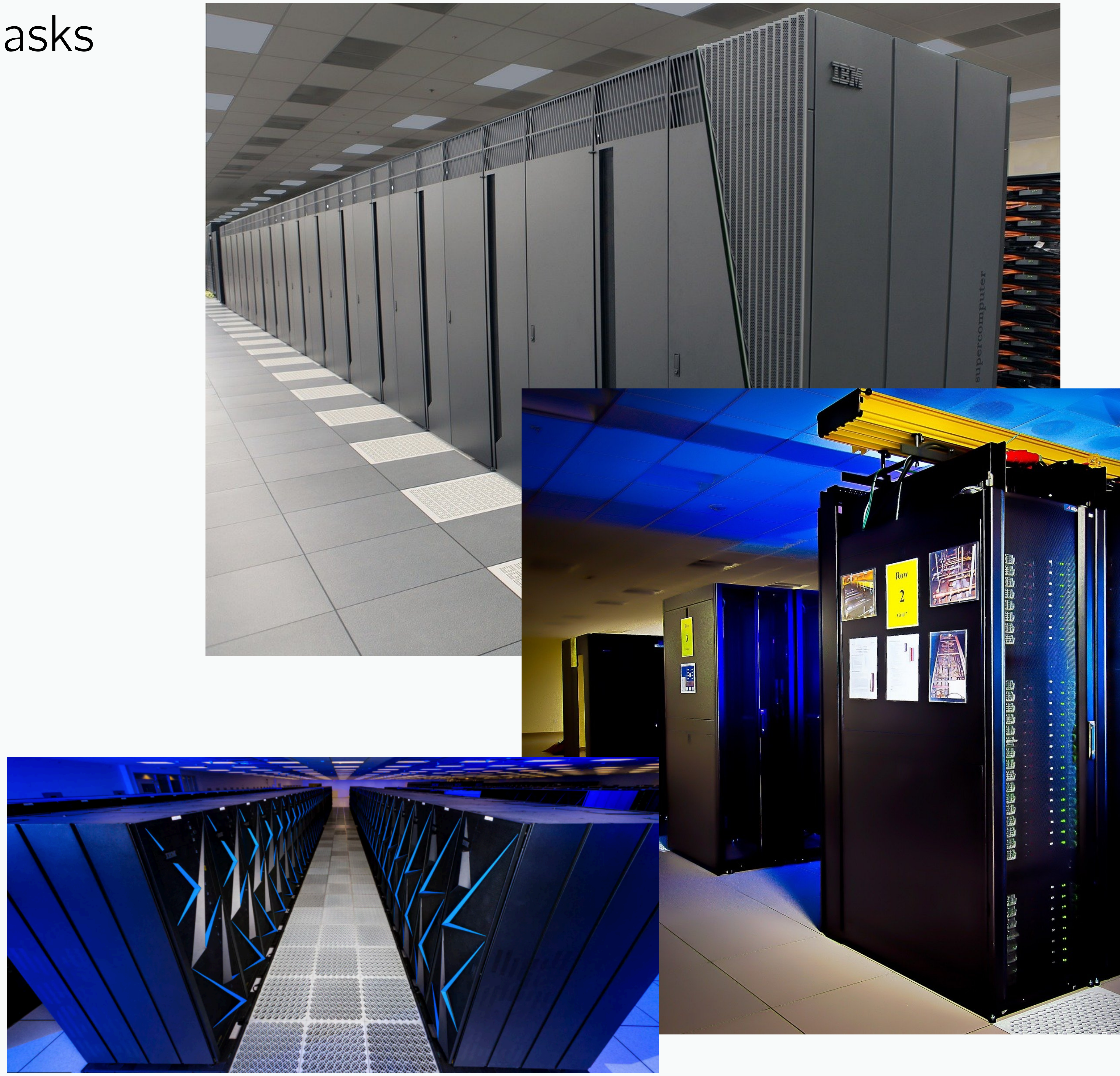
Overview & Motivations

PolSys-SpecFun Seminar
February 19, 2021

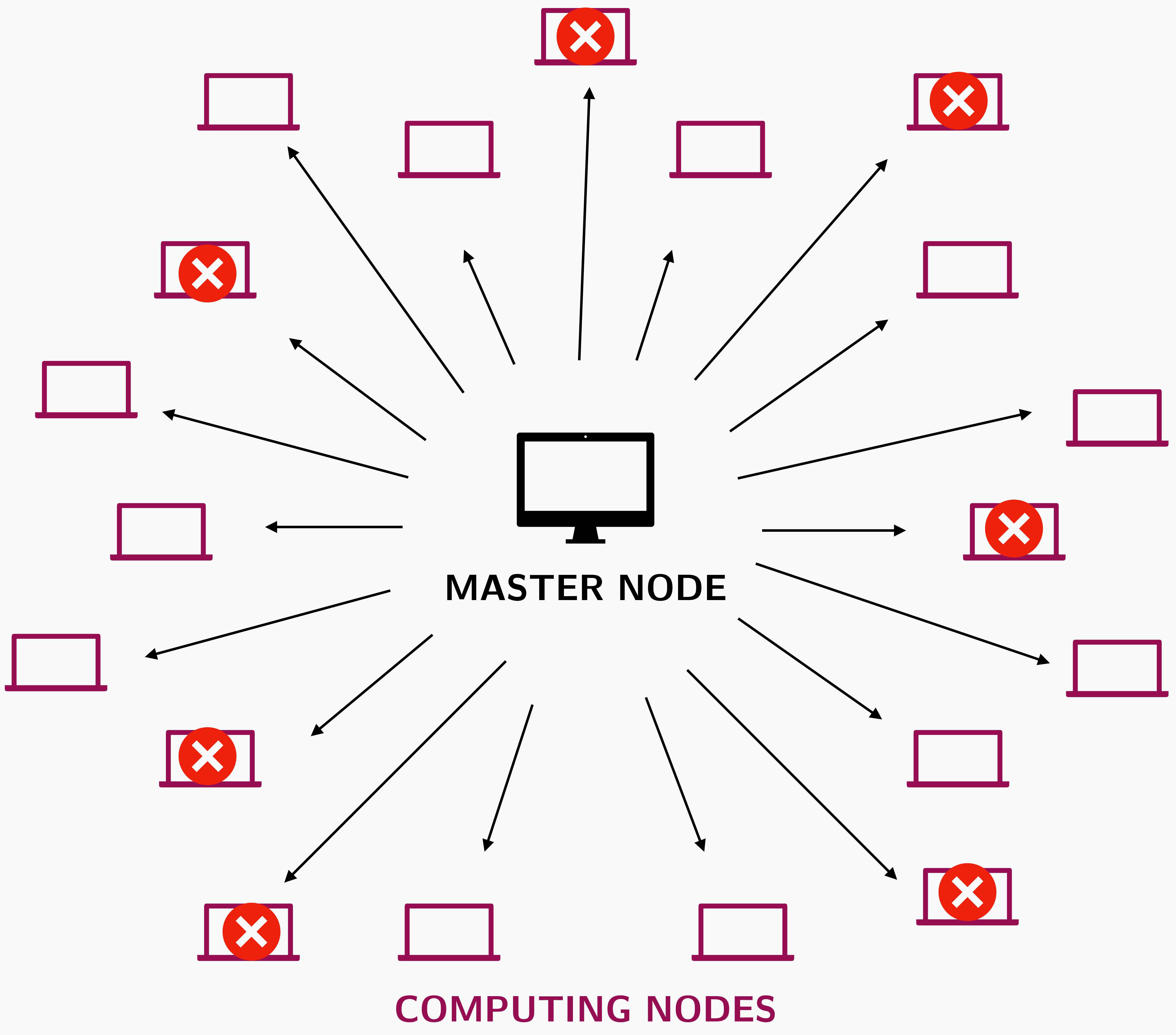
High Performance Computing Technologies

Goal: provide high performances and complete heavy tasks





Fault tolerant algorithms



The **more the number of system components** grows
the **more the failures** of computing nodes becomes **relevant**
(3,5 faults per day)
[DI, GUO, PERSHEY, SNIR, CAPPELLO, 2019], [LIU, CHEN, 2018]

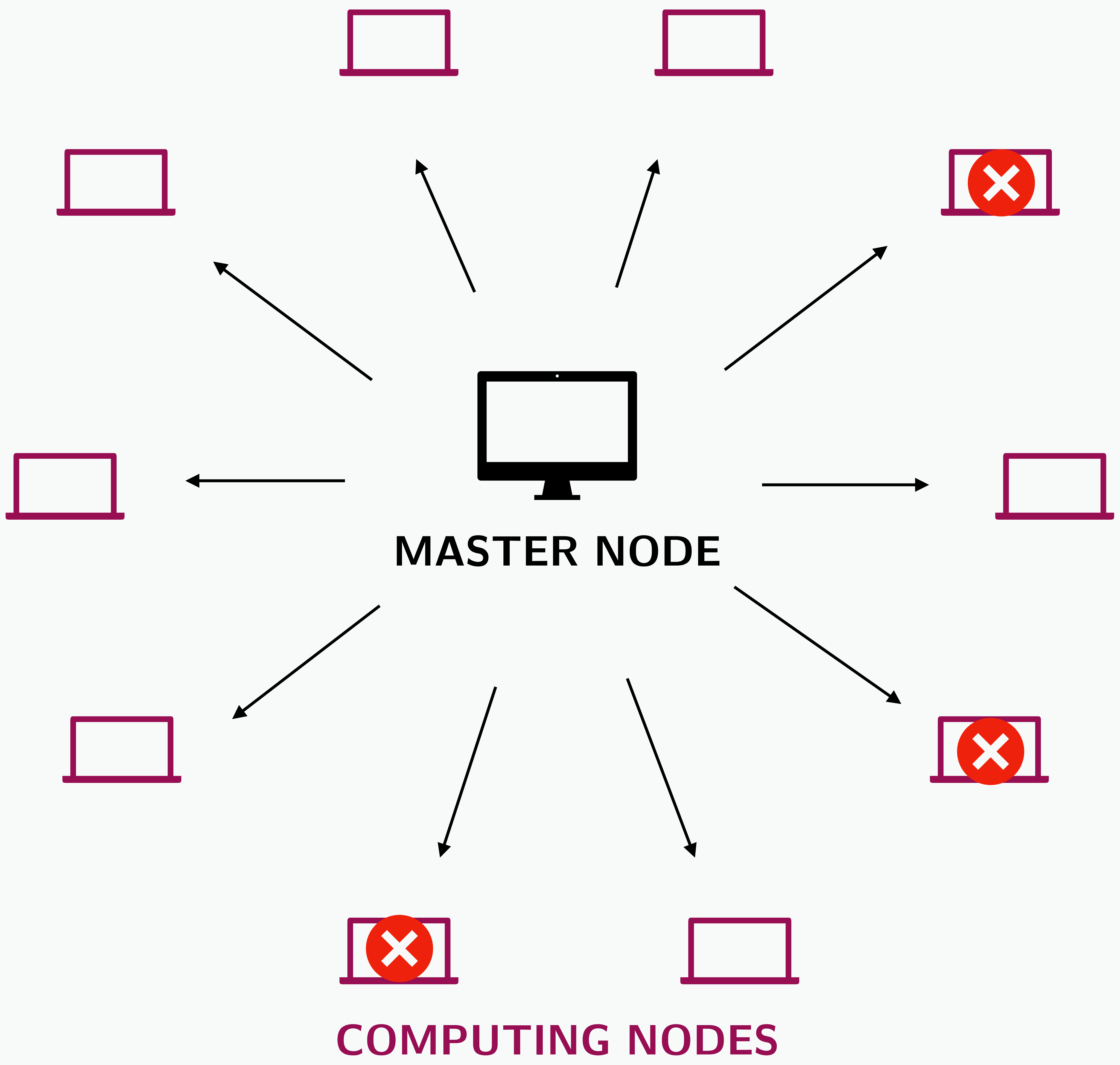
↓

construct **fault tolerant** algorithms

↓

detect/correct faults

Algorithm-based fault tolerant techniques (ABFT)



Algorithm-based fault tolerant techniques (ABFT)
[HUANG, ABRAHAM, 1984]

↓

exploits the **algorithm's characteristics**
to design a **fault tolerant algorithm**

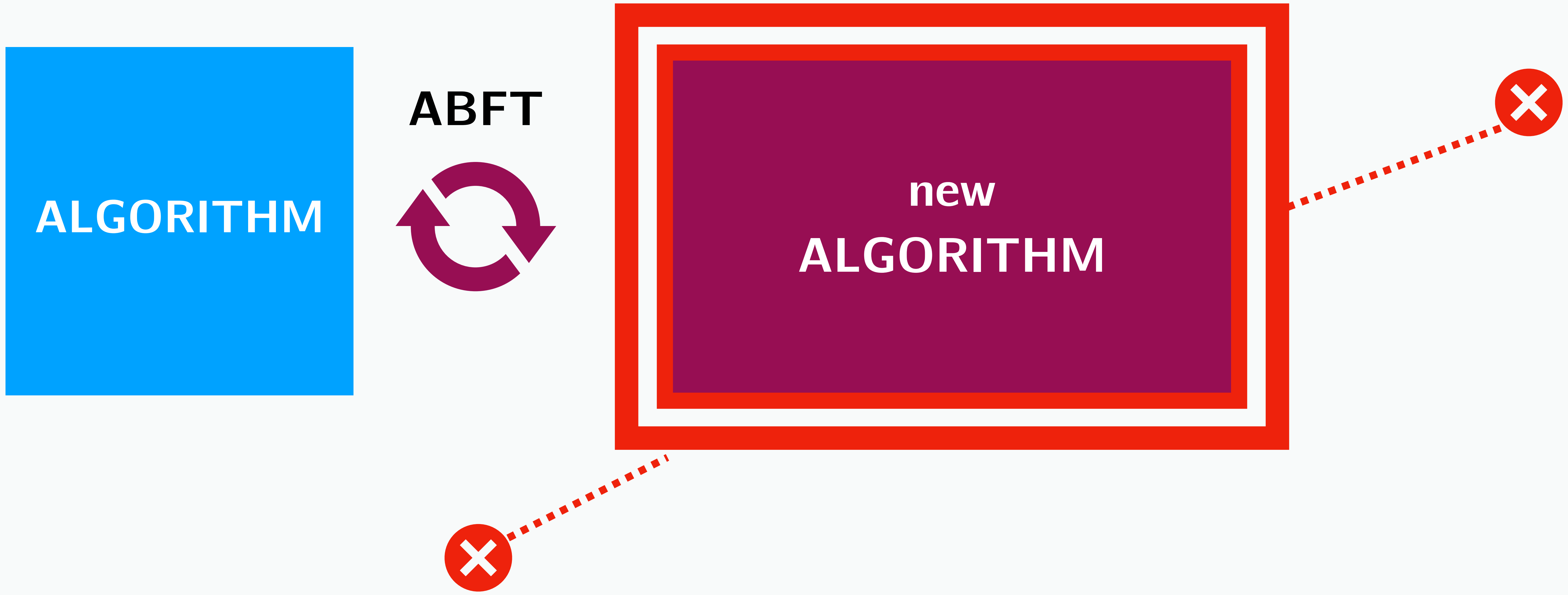
↓

Goal: detect/correct computational errors (faults)

Algorithm-based fault tolerant techniques (ABFT)

[HUANG, ABRAHAM, 1984]

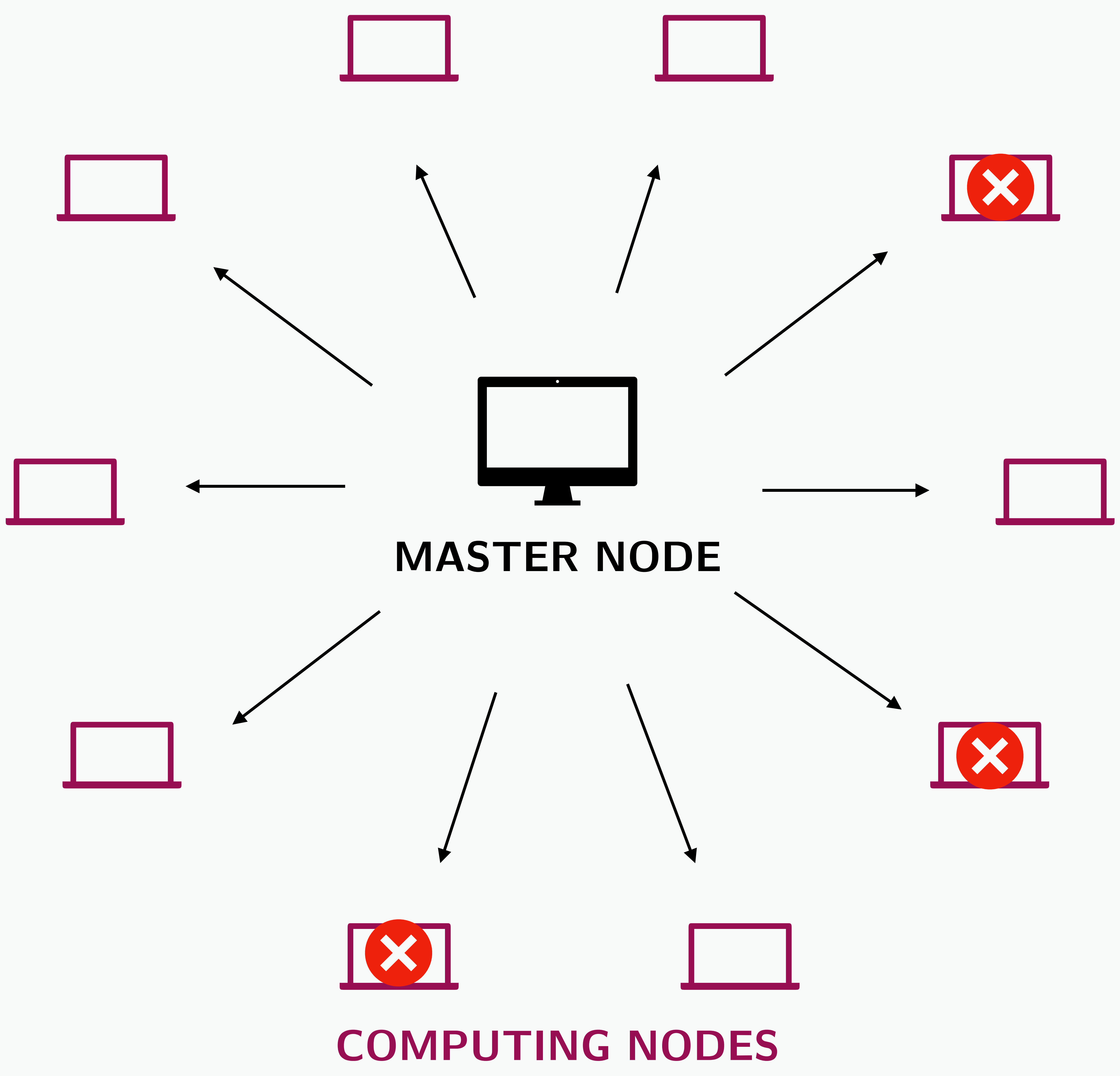
Goal: detect/correct computational errors (faults)



- **adding redundancy** (encoding)
- modify the algorithm, work on encoding data ⟵ robust to errors (faults)

error correcting codes

High Performance Computing Technologies



Algorithm-based fault tolerant techniques (ABFT)
[HUANG, ABRAHAM, 1984]

↓

exploits the **algorithm's characteristics**
to design a **fault tolerant algorithm**

↓

Goal: detect/correct computational errors (faults)

ABFT for Polynomial Linear System Solving by Evaluation-Interpolation

[BOYER, KALTOFEN, 2014]
[KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]
[GUERRINI, LEBRETON, Z., 2019]
[GUERRINI, LEBRETON, Z., 2021]

: publication   : submitted paper

Take a look inside

PolSys-SpecFun Seminar
February 19, 2021

Polynomial Linear System Solving by Evaluation-Interpolation

Polynomial Linear System Solving

$$\underbrace{\begin{pmatrix} a_{1,1}(x) & a_{1,2}(x) & \dots & a_{1,n}(x) \\ a_{2,1}(x) & a_{2,2}(x) & \dots & a_{2,n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}(x) & a_{n,2}(x) & \dots & a_{n,n}(x) \end{pmatrix}}_{A(x)} \underbrace{\begin{pmatrix} y_1(x) \\ y_2(x) \\ \vdots \\ y_n(x) \end{pmatrix}}_{\boldsymbol{y}(x)} = \underbrace{\begin{pmatrix} b_1(x) \\ b_2(x) \\ \vdots \\ b_n(x) \end{pmatrix}}_{\boldsymbol{b}(x)}$$

Polynomial Linear System Solving by Evaluation-Interpolation

Polynomial Linear System Solving

$$\underbrace{\begin{pmatrix} a_{1,1}(x) & a_{1,2}(x) & \dots & a_{1,n}(x) \\ a_{2,1}(x) & a_{2,2}(x) & \dots & a_{2,n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}(x) & a_{n,2}(x) & \dots & a_{n,n}(x) \end{pmatrix}}_{A(x)} \underbrace{\begin{pmatrix} \frac{v_1(x)}{d(x)} \\ \vdots \\ \frac{v_n(x)}{d(x)} \end{pmatrix}}_{\boldsymbol{y}(x)} = \underbrace{\begin{pmatrix} b_1(x) \\ b_2(x) \\ \vdots \\ b_n(x) \end{pmatrix}}_{\boldsymbol{b}(x)}$$

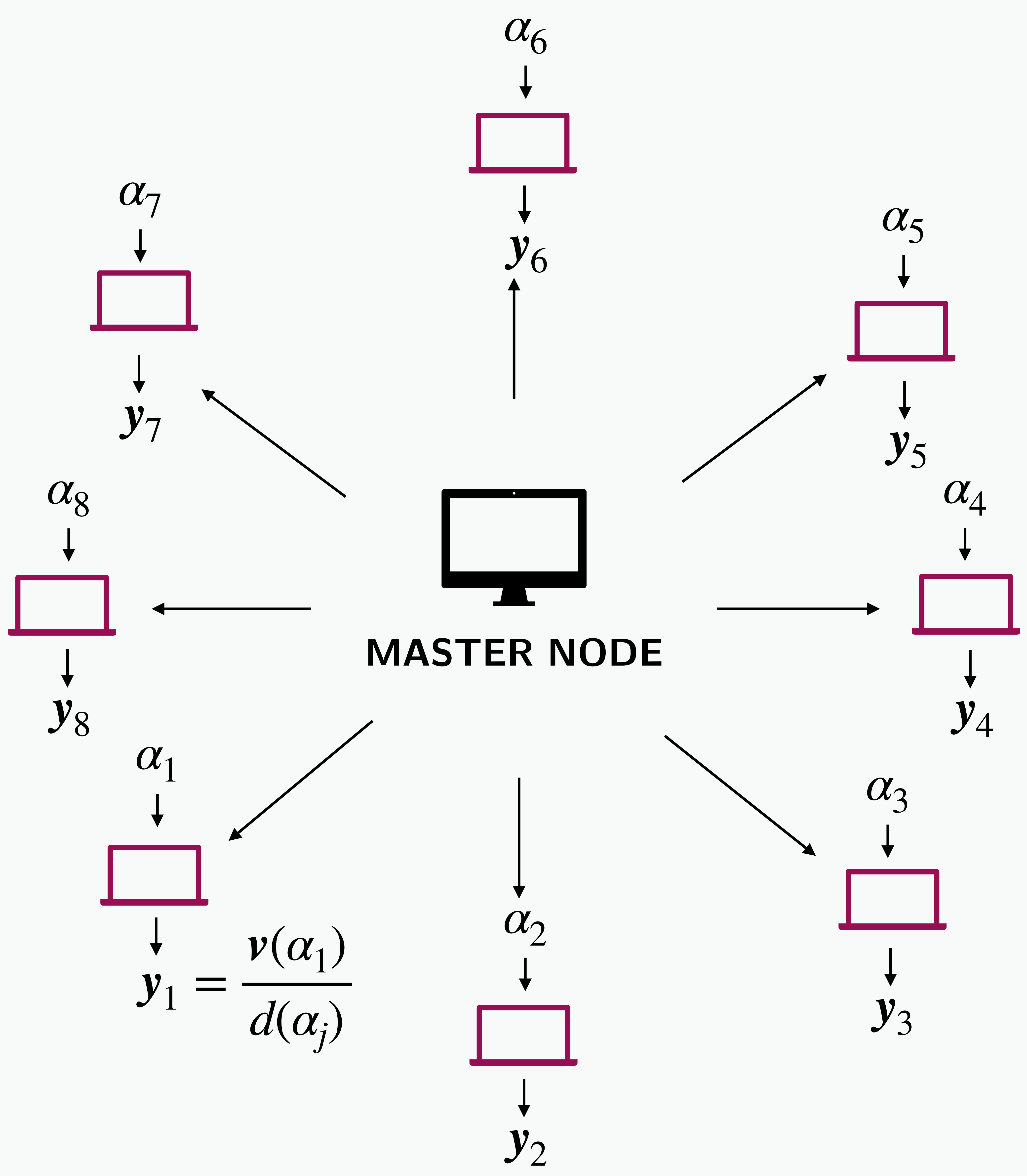
Polynomial Linear System Solving by Evaluation-Interpolation

Polynomial Linear System Solving

$$\underbrace{\begin{pmatrix} a_{1,1}(x) & a_{1,2}(x) & \dots & a_{1,n}(x) \\ a_{2,1}(x) & a_{2,2}(x) & \dots & a_{2,n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}(x) & a_{n,2}(x) & \dots & a_{n,n}(x) \end{pmatrix}}_{A(x)} \underbrace{\begin{pmatrix} \frac{v_1(x)}{d(x)} \\ \vdots \\ \frac{v_n(x)}{d(x)} \end{pmatrix}}_{\boldsymbol{y}(x)} = \underbrace{\begin{pmatrix} b_1(x) \\ b_2(x) \\ \vdots \\ b_n(x) \end{pmatrix}}_{\boldsymbol{b}(x)}$$

Evaluation-Interpolation Algorithm

1. **Evaluate** $A(x)$, $\boldsymbol{b}(x)$ in $\{\alpha_1, \dots, \alpha_L\}$, ($A(\alpha_j)$ full rank)
2. **Compute** $y_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j) = \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$,
3. Interpolate $\boldsymbol{y}(x)$ from $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L$



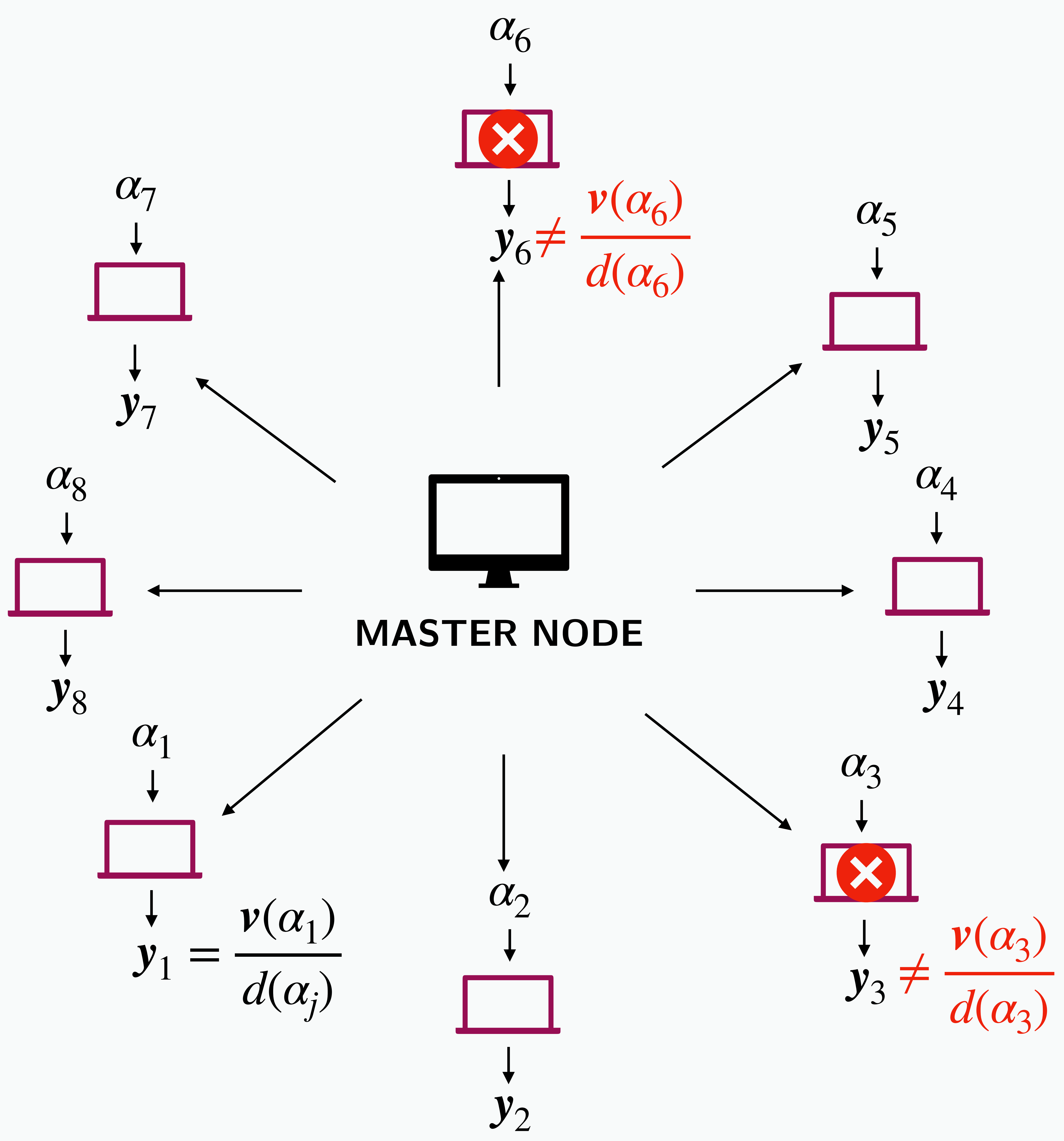
Polynomial Linear System Solving by Evaluation-Interpolation

Polynomial Linear System Solving

$$\underbrace{\begin{pmatrix} a_{1,1}(x) & a_{1,2}(x) & \dots & a_{1,n}(x) \\ a_{2,1}(x) & a_{2,2}(x) & \dots & a_{2,n}(x) \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}(x) & a_{n,2}(x) & \dots & a_{n,n}(x) \end{pmatrix}}_{A(x)} \underbrace{\begin{pmatrix} \frac{v_1(x)}{d(x)} \\ \vdots \\ \frac{v_n(x)}{d(x)} \end{pmatrix}}_{\boldsymbol{y}(x)} = \underbrace{\begin{pmatrix} b_1(x) \\ b_2(x) \\ \vdots \\ b_n(x) \end{pmatrix}}_{\boldsymbol{b}(x)}$$

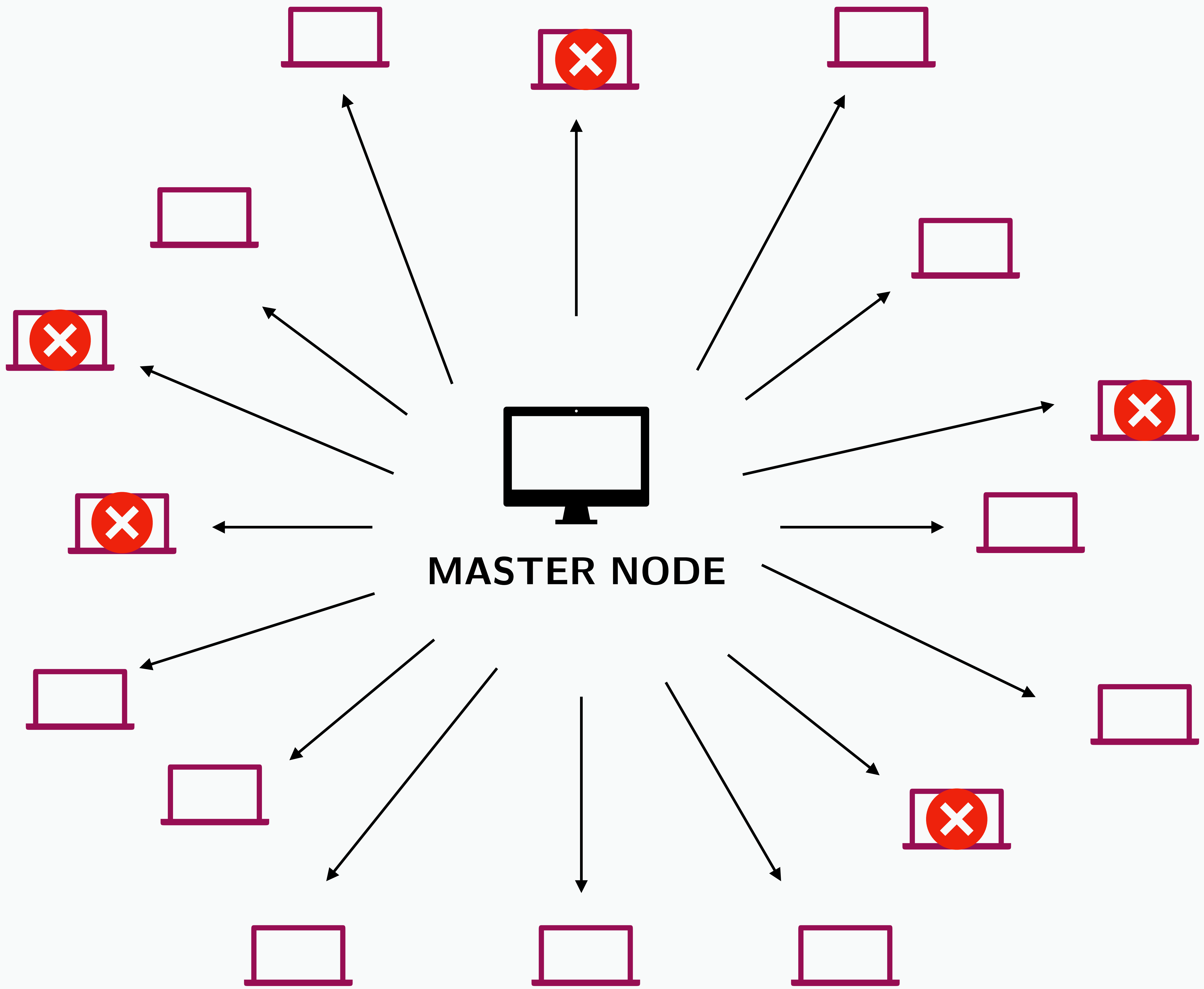
Evaluation-Interpolation Algorithm

1. **Evaluate** $A(x)$, $\boldsymbol{b}(x)$ in $\{\alpha_1, \dots, \alpha_L\}$, ($A(\alpha_j)$ full rank)
2. **Compute** $y_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j) = \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$,
3. Interpolate $\boldsymbol{y}(x)$ from $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L$



ABFT for PLS solving by Evaluation-Interpolation

- **adding** redundancy (encoding), consider many nodes



ABFT for Evaluation-Interpolation Algorithm

1. **Evaluate** $A(x)$, $\boldsymbol{b}(x)$ in many evaluation points
2. **Compute** $\boldsymbol{y}_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j)$

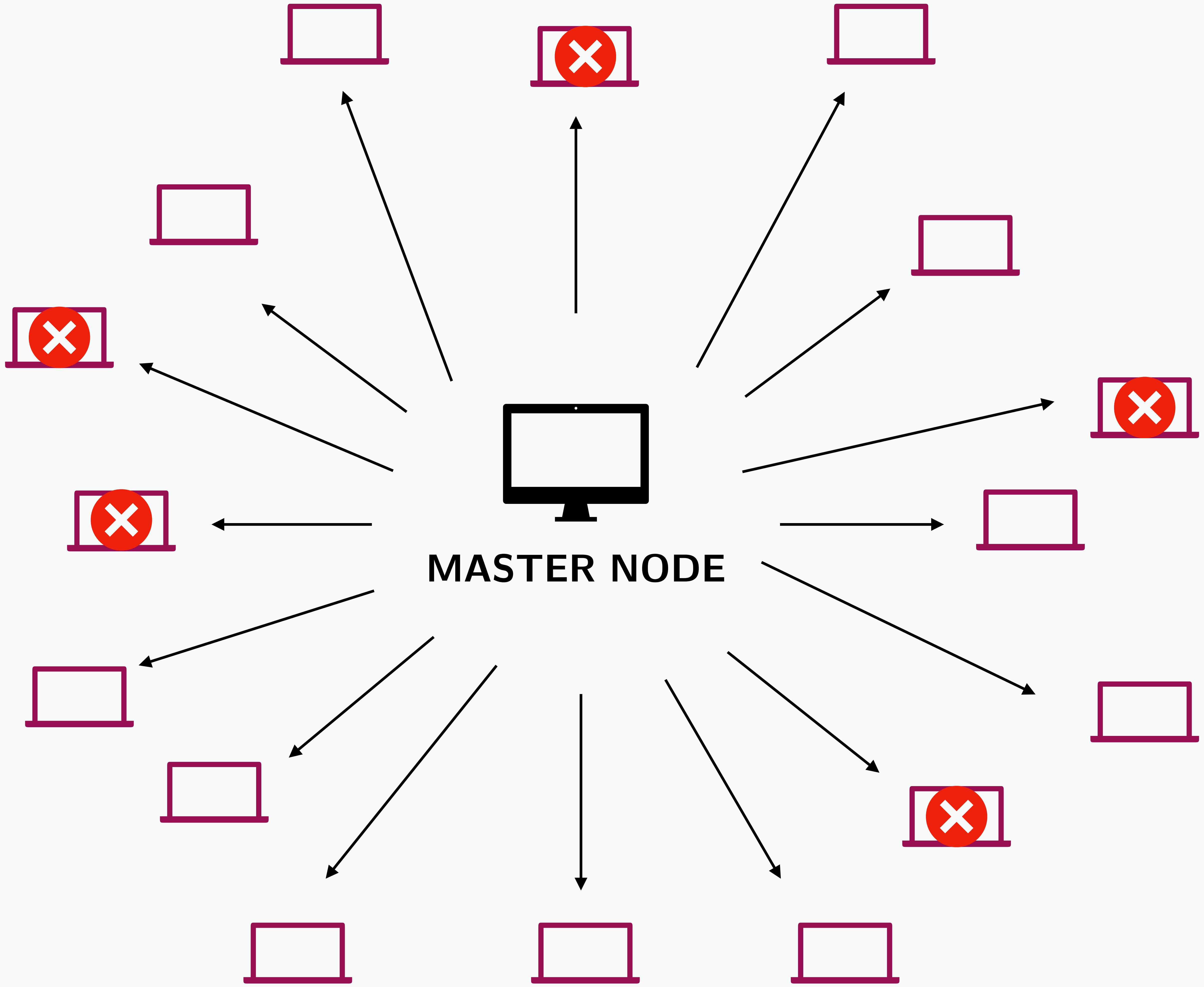
ABFT for PLS solving by Evaluation-Interpolation

- **adding** redundancy (encoding), consider many nodes
- decoding, correcting errors

ABFT for Evaluation-Interpolation Algorithm

1. **Evaluate** $A(x)$, $\boldsymbol{b}(x)$ in many evaluation points
2. **Compute** $\boldsymbol{y}_j = A(\alpha_j)^{-1}\boldsymbol{b}(\alpha_j)$
3. Interpolate $\boldsymbol{y}(x)$ from $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$ where some errors occur

Simultaneous Cauchy Interpolation with Errors



Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation with Errors

Given $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

- $\boldsymbol{y}_j = \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ correct evaluations
- $\boldsymbol{y}_j \neq \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ erroneous evaluations

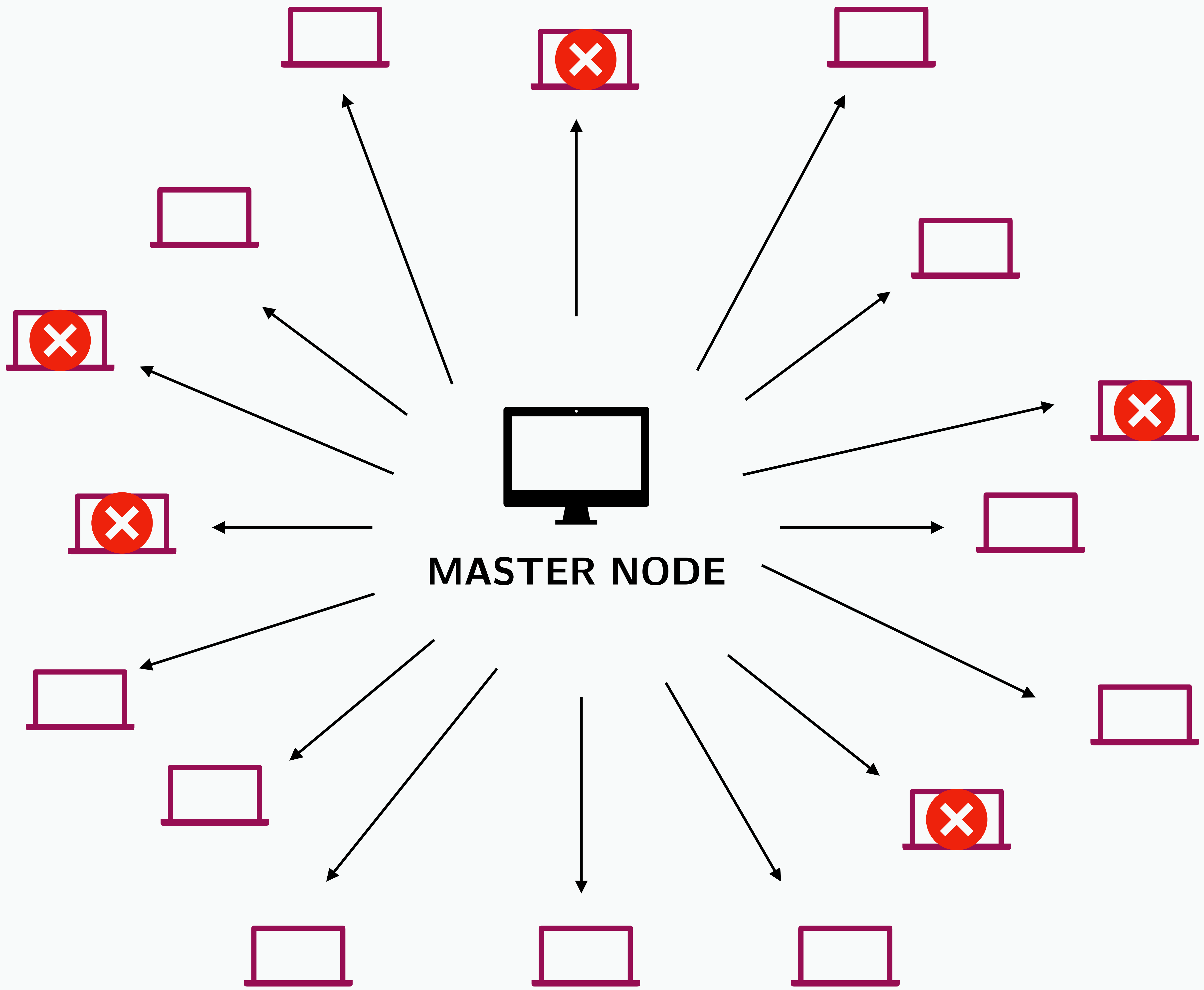
the *degree bounds* $N > \deg(\boldsymbol{v})$, $D > \deg(d)$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $(\boldsymbol{v}(x), d(x)) \longrightarrow \boldsymbol{y}(x)$

Simultaneous Cauchy Interpolation

Simultaneous Rational Function Reconstruction



Two Main Questions

1. How many evaluations (nodes) do we need to uniquely recover $(v(x), d(x))$?

fewer evaluations $\longrightarrow$ fewer computations

2. Can we reduce this number?

Number of Evaluations - Outline of this work

			uniqueness	**uniqueness** ***almost always***
no-errors	$(\boldsymbol{v}(x), d(x))$		Cauchy Interpolation	**[GUERRINI, LEBRETON, Z., 2020]**
	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$		[CABAY, 1971]	?
with errors	$(\boldsymbol{v}(x), d(x))$	d constant $(D = 1)$	Unique Decoding Capability Theorem (IRS codes)	IRS codes [BLEICHENBACHER, KIAYIAS, YUNG, 2003]
		$D > 1$	[BOYER, KALTOFEN, 2014]	**[GUERRINI, LEBRETON, Z., 2019]**
	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$		[KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]	**[GUERRINI, LEBRETON, Z., 2021]**

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $(\underbrace{v_1(x), \ldots, v_n(x)}_{\boldsymbol{v}(x)}, d(x))$ s.t.

- $v_i(\alpha_j) = y_{i,j} d(\alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

↓

Simultaneous Rational Function Reconstruction

→ Vector Generalization **same denominator**

Cauchy Interpolation

Given the evaluations $y_1, \ldots, y_L$

and the *degree bounds* N, D

GOAL: **find** $(v(x), d(x))$ s.t.

- $\frac{v(\alpha_j)}{d(\alpha_j)} = y_j, d(\alpha_j) \neq 0$
- $\deg(v) < N$
- $\deg(d) < D$

↓

Rational Function Reconstruction

If the number of evaluations $L \geq N + D - 1$

↓

Unique solution

$(v_1, d_1), (v_2, d_2)$ **solutions** $\longrightarrow \frac{v_1}{d_1} = \frac{v_2}{d_2}$

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x)}_{\boldsymbol{v}(x)}, d(x))$ s.t.

- $v_i(\alpha_j) = y_{i,j} d(\alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$\longrightarrow$

Vector Generalization
same denominator

Cauchy Interpolation

Given the evaluations $y_1, \ldots, y_L$

and the *degree bounds* N, D

GOAL: **find** $(v(x), d(x))$ s.t.

- $v(\alpha_j) = y_j d(\alpha_j)$
- $\deg(v) < N$
- $\deg(d) < D$

1. Apply the **Cauchy Interpolation** component-wise ($L \geq N + D - 1 \longrightarrow$ **uniqueness**)

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $(\underbrace{v_1(x), \dots, v_n(x)}_{\boldsymbol{v}(x)}, d(x))$ s.t.

- $v_i(\alpha_j) = y_{i,j} d(\alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$\longrightarrow$

Vector Generalization

same denominator

Cauchy Interpolation

Given the evaluations $y_1, \dots, y_L$

and the *degree bounds* N, D

GOAL: **find** $(v(x), d(x))$ s.t.

- $v(\alpha_j) = y_j d(\alpha_j)$
- $\deg(v) < N$
- $\deg(d) < D$

1. Apply the **Cauchy Interpolation** component-wise ($L \geq N + D - 1 \longrightarrow$ **uniqueness**)
2. Use the **common denominator feature** to reduce the number of equations of the related **homogeneous linear system**

$\searrow$ **#equations** = **#unknowns -1** $\longrightarrow$ $L = N + (D-1)/n$

#equations $= nL$, #unknowns $= nN + D$

uniqueness?

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \dots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $(\underbrace{v_1(x), \dots, v_n(x)}_{\boldsymbol{v}(x)}, d(x))$ s.t.

- $v_i(\alpha_j) = y_{i,j} d(\alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

Vector Generalization
same denominator

Cauchy Interpolation

Given the evaluations $y_1, \dots, y_L$

and the *degree bounds* N, D

GOAL: **find** $(v(x), d(x))$ s.t.

- $v(\alpha_j) = y_j d(\alpha_j)$
- $\deg(v) < N$
- $\deg(d) < D$

If we want to recover a solution of a PLS:

- with $L \geq \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\}$ ⟶ **uniqueness** [CABAY, 1971]
- for **specific degree constraints** N, D $\max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} = N + (D-1)/n$ ⟶ **uniqueness** [OLESH, STORJOHANN, 2007]

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x), d(x))}_{\boldsymbol{v}(x)}$ s.t.

- $v_i(\alpha_j) = y_{i,j} d(\alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$\longrightarrow$

Vector Generalization
same denominator

Cauchy Interpolation

Given the evaluations $y_1, \ldots, y_L$

and the *degree bounds* N, D

GOAL: **find** $(v(x), d(x))$ s.t.

- $v(\alpha_j) = y_j d(\alpha_j)$
- $\deg(v) < N$
- $\deg(d) < D$

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = N + (D-1)/n$, **for almost all instances** $\Longrightarrow$ **uniqueness**.

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

Just a hint of the technique...

PolSys-SpecFun Seminar
February 19, 2021

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x), d(x))}_{\boldsymbol{v}(x)}$ s.t.

- $v_i(\alpha_j) = y_{i,j} d(\alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = \deg(\boldsymbol{a}) = N + (D-1)/n$, **for almost all instances** $\Longrightarrow$ **uniqueness**.

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x)}_{\boldsymbol{v}(x)}, d(x))$ s.t.

- $v_i(x) = u_i(x)d(x) \bmod \prod (x - \alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$\boldsymbol{u}(x)$ vector of Lagrange interpolators

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = \deg(\boldsymbol{a}) = N + (D-1)/n$, **for almost all instances** $\Longrightarrow$ **uniqueness**.

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

No-error case

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x), d(x))}_{\boldsymbol{v}(x)}$ s.t.

- $v_i(x) = u_i(x)d(x) \bmod \prod (x - \alpha_j)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$\boldsymbol{u}(x)$ vector of Lagrange interpolators

→ Specific case of

Simultaneous Rational Function Reconstruction

Given two vector of polynomials $\boldsymbol{u}(x), \boldsymbol{a}(x)$

and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x), d(x))}_{\boldsymbol{v}(x)}$ s.t.

- $v_i(x) = u_i(x)d(x) \bmod a_i(x)$
- $\deg(v_i) < N$
- $\deg(d) < D$

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = \deg(\boldsymbol{a}) = N + (D-1)/n$, **for almost all instances** $\Longrightarrow$ **uniqueness**.

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

No-error case

Simultaneous Rational Function Reconstruction

Given two vector of polynomials $\boldsymbol{u}(x), \boldsymbol{a}(x)$ and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x), d(x))}_{\boldsymbol{v}(x)}$ s.t.

- $v_i(x) = u_i(x)d(x) \bmod a_i(x)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$$(\boldsymbol{v}, d)\underbrace{\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \\ -u_1 & -u_2 & \ldots & -u_n \end{pmatrix}}_{R_{\boldsymbol{u}}} = 0 \bmod \underbrace{\langle (0,\ldots,a_i,\ldots 0)\rangle}_{\mathscr{M}} \longleftrightarrow (\boldsymbol{v}, d) \in \mathscr{A}_{R_{\boldsymbol{u}}}$$

$$\mathscr{A}_{R_{\boldsymbol{u}}} = \{\boldsymbol{p} = (p_1(x), \ldots, p_n(x)) \mid \boldsymbol{p}R_{\boldsymbol{u}} = \boldsymbol{0} \bmod \mathscr{M}\}$$

Relation module

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = \deg(\boldsymbol{a}) = N + (D-1)/n$, **for almost all instances** $\Longrightarrow$ **uniqueness**.

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

No-error case

Simultaneous Rational Function Reconstruction

Given two vector of polynomials $\boldsymbol{u}(x), \boldsymbol{a}(x)$ and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x)}_{\boldsymbol{v}(x)}, d(x))$ s.t.

- $v_i(x) = u_i(x)d(x) \bmod a_i(x)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$$(\boldsymbol{v}, d)\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \\ -u_1 & -u_2 & \ldots & -u_n \end{pmatrix} = 0 \bmod \langle (0, \ldots, a_i, \ldots 0) \rangle \longleftrightarrow (\boldsymbol{v}, d) \in \mathscr{A}_{R_u}$$

take the max

$$\underbrace{(\deg(v_1) - N}_{<0}, \ldots, \underbrace{\deg(v_n) - N}_{<0}, \underbrace{\deg(d) - D}_{<0}) \longrightarrow rdeg_{(-N,\ldots,-N,-D)}(\boldsymbol{v}, d) < 0$$

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = \deg(\boldsymbol{a}) = N + (D-1)/n$, **for almost all instances** $\Longrightarrow$ **uniqueness**.

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

No-error case

Simultaneous Rational Function Reconstruction

Given two vector of polynomials $\boldsymbol{u}(x), \boldsymbol{a}(x)$ and the *degree bounds* N, D

GOAL: **find** $(\underbrace{v_1(x), \ldots, v_n(x)}_{\boldsymbol{v}(x)}, d(x))$ s.t.

- $(\boldsymbol{v}, d) \in \mathscr{A}_{R_u}$
- $rdeg_{(-N,\ldots,-N,-D)}(\boldsymbol{v}, d) < 0$

How to prove uniqueness?

- ***Minimal basis*** $\mathscr{B}$ *of* $\mathscr{A}_{R_u}$, for which the $\boldsymbol{s}-$**row degrees are uniquely defined** *(Ordered Weak Popov)*
- **Solution space generated** by **elements of** $\mathscr{B}$ the with **negative** $\boldsymbol{s}-$**row degrees**

↓

$(-N, \ldots, -N, -D)$-**row degrees** of $\mathscr{B}$ of the form $(0,0,\ldots,-1)$

↓

Solution space uniquely generated $\Rightarrow$ **uniqueness**

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = \deg(\boldsymbol{a}) = N + (D-1)/n$, **for almost all instances,** $rdeg_{(-N,\ldots,-N,-D)}(\mathscr{B}) = (0,\ldots,0,-1)$

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

Number of Evaluations - Outline of this work

			uniqueness	uniqueness *almost always*
no-errors	$(v(x), d(x))$		$L = N + D - 1$ Cauchy Interpolation	$L = N + \left\lceil \frac{(D-1)}{n} \right\rceil$
	$A(x)\frac{v(x)}{d(x)} = b(x)$		$L = \max\{\deg(A) + N, \deg(b) + D\}$ [CABAY, 1971]	
with errors	$(v(x), d(x))$	d constant ($D = 1$)	Unique Decoding Capability Theorem (IRS codes)	IRS codes [BLEICHENBACHER, KIAYIAS, YUNG, 2003]
		$D > 0$	[BOYER, KALTOFEN, 2014]	**[GUERRINI, LEBRETON, Z., 2019]**
	$A(x)\frac{v(x)}{d(x)} = b(x)$		[KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]	**[GUERRINI, LEBRETON, Z., 2021]**

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation with Errors

Given $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

- $\boldsymbol{y}_j = \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ correct evaluations
- $\boldsymbol{y}_j \neq \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ erroneous evaluations

the *degree bounds* $N > \deg(\boldsymbol{v})$, $D > \deg(d)$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $(\boldsymbol{v}(x), d(x)) \longrightarrow \boldsymbol{y}(x)$

Interleaved Reed-Solomon codes

Interleaved Reed-Solomon Codes

Let $k \leq n \leq q$ and $\{\alpha_1, \ldots, \alpha_n\}$ distinct *evaluation points,*

$$\mathscr{C}_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \ldots, \boldsymbol{f}(\alpha_n)) \mid \boldsymbol{f} \in \mathbb{F}_q[x]^{l\times 1}, \deg(\boldsymbol{f}) < k\}$$

The IRS code is an **MDS code**

the **minimum distance** is $d = n - k + 1$

$(m_{1,0}, \ldots, m_{1,k-1})$ $(m_{2,0}, \ldots, m_{2,k-1})$ $\cdots$ $(m_{l,0}, \ldots, m_{l,k-1})$

$$f_1(x) = \sum_{i=0}^{k-1} m_{1,i}x^i \quad f_2(x) = \sum_{i=0}^{k-1} m_{2,i}x^i \quad \cdots \quad f_l(x) = \sum_{i=0}^{k-1} m_{l,i}x^i \rightarrow \boldsymbol{f}(x) = \begin{pmatrix} f_1(x) \\ f_2(x) \\ \vdots \\ f_l(x) \end{pmatrix}$$

Encoding

$$C = \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \ldots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \ldots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \ldots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \ldots & f_l(\alpha_n) \end{pmatrix}$$

RS codeword

RS codeword

Interleaved Reed-Solomon codeword

Interleaved Reed-Solomon codes

Interleaved Reed-Solomon Codes

Let $k \leq n \leq q$ and $\{\alpha_1, \ldots, \alpha_n\}$ distinct *evaluation points*,

$$\mathscr{C}_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \ldots, \boldsymbol{f}(\alpha_n)) \mid \boldsymbol{f} \in \mathbb{F}_q[x]^{l \times 1}, \deg(\boldsymbol{f}) < k\}$$

The IRS code is an **MDS code**

the **minimum distance** is $d = n - k + 1$

Encoding

Channel

$$C = \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \ldots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \ldots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \ldots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \ldots & f_l(\alpha_n) \end{pmatrix}$$

$$\begin{pmatrix} f_1(\alpha_1) & & & & \\ f_2(\alpha_1) & & & & \\ f_3(\alpha_1) & & & & \\ \vdots & & & & \\ f_l(\alpha_1) & & & & \end{pmatrix}$$

Interleaved Reed-Solomon codes

Interleaved Reed-Solomon Codes

Let $k \leq n \leq q$ and $\{\alpha_1, \ldots, \alpha_n\}$ distinct *evaluation points*,

$$\mathscr{C}_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \ldots, \boldsymbol{f}(\alpha_n)) \mid \boldsymbol{f} \in \mathbb{F}_q[x]^{l\times 1}, \deg(\boldsymbol{f}) < k\}$$

The IRS code is an **MDS code**

the **minimum distance** is $d = n - k + 1$

Encoding

$$C = \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \ldots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \ldots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \ldots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \ldots & f_l(\alpha_n) \end{pmatrix}$$

Channel

$$\begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & & & \\ f_2(\alpha_1) & f_2(\alpha_2) & & & \\ f_3(\alpha_1) & f_3(\alpha_2) & & & \\ \vdots & \vdots & & & \\ f_l(\alpha_1) & f_l(\alpha_2) & & & \end{pmatrix}$$

burst error

Interleaved Reed-Solomon codes

Interleaved Reed-Solomon Codes

Let $k \leq n \leq q$ and $\{\alpha_1, \ldots, \alpha_n\}$ distinct *evaluation points*,

$$\mathscr{C}_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \ldots, \boldsymbol{f}(\alpha_n)) \mid \boldsymbol{f} \in \mathbb{F}_q[x]^{l\times 1}, \deg(\boldsymbol{f}) < k\}$$

The IRS code is an **MDS code**

the **minimum distance** is $d = n - k + 1$

Encoding

$$C = \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \ldots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \ldots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \ldots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \ldots & f_l(\alpha_n) \end{pmatrix}$$

Channel

$$\begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \ldots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \ldots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \ldots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \ldots & f_l(\alpha_n) \end{pmatrix}$$

burst error

Interleaved Reed-Solomon codes

Interleaved Reed-Solomon Codes

Let $k \leq n \leq q$ and $\{\alpha_1, \ldots, \alpha_n\}$ distinct *evaluation points*,

$$\mathscr{C}_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \ldots, \boldsymbol{f}(\alpha_n)) \mid \boldsymbol{f} \in \mathbb{F}_q[x]^{l \times 1}, \deg(\boldsymbol{f}) < k\}$$

Decoding

$$Y = \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \ldots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \ldots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \ldots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \ldots & f_l(\alpha_n) \end{pmatrix}$$

burst error

The IRS code is an **MDS code**

the **minimum distance** is $d = n - k + 1$

Simultaneous Interpolation with Errors

Decoding IRS codes

Given the received matrix with columns $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$

- $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)$ correct evaluations
- $\boldsymbol{y}_j \neq \boldsymbol{f}(\alpha_j)$ erroneous evaluations

the *degree bound* $k > \deg(\boldsymbol{f})$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $\boldsymbol{f}(x)$

Interleaved Reed-Solomon codes

Interleaved Reed-Solomon Codes

Let $k \le n \le q$ and $\{\alpha_1, \dots, \alpha_n\}$ distinct *evaluation points*,

$$\mathscr{C}_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \dots, \boldsymbol{f}(\alpha_n)) \mid \boldsymbol{f} \in \mathbb{F}_q[x]^{l \times 1}, \deg(\boldsymbol{f}) < k\}$$

Decoding

$$Y = \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \dots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \dots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \dots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \dots & f_l(\alpha_n) \end{pmatrix}$$

burst error

this is exactly our starting point!

Simultaneous Interpolation with Errors

The IRS code is an **MDS code**

the **minimum distance** is $d = n - k + 1$

Simultaneous Interpolation with Errors
Decoding IRS codes

Given the received matrix with columns $\boldsymbol{y}_1, \dots, \boldsymbol{y}_n$

- $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)$ correct evaluations
- $\boldsymbol{y}_j \ne \boldsymbol{f}(\alpha_j)$ erroneous evaluations

the *degree bound* $k > \deg(\boldsymbol{f})$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $\boldsymbol{f}(x)$

Interleaved Reed-Solomon codes

Interleaved Reed-Solomon Codes

Let $k \leq n \leq q$ and $\{\alpha_1, \dots, \alpha_n\}$ distinct *evaluation points*,

$$\mathcal{C}_{IRS}(n,k) := \{(\boldsymbol{f}(\alpha_1), \dots, \boldsymbol{f}(\alpha_n)) \mid \boldsymbol{f} \in \mathbb{F}_q[x]^{l \times 1}, \deg(\boldsymbol{f}) < k\}$$

Decoding

this is exactly our starting point!

Simultaneous Interpolation with Errors

$$Y = \begin{pmatrix} f_1(\alpha_1) & f_1(\alpha_2) & f_1(\alpha_3) & \dots & f_1(\alpha_n) \\ f_2(\alpha_1) & f_2(\alpha_2) & f_2(\alpha_3) & \dots & f_2(\alpha_n) \\ f_3(\alpha_1) & f_3(\alpha_2) & f_3(\alpha_3) & \dots & f_3(\alpha_n) \\ \vdots & \vdots & \vdots & \dots & \vdots \\ f_l(\alpha_1) & f_l(\alpha_2) & f_l(\alpha_3) & \dots & f_l(\alpha_n) \end{pmatrix}$$

burst error

The IRS code is an **MDS code**

the **minimum distance** is $d = n - k + 1$

Simultaneous Interpolation with Errors / Decoding IRS codes

Given the received matrix with columns $\boldsymbol{y}_1, \dots, \boldsymbol{y}_n$

- $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)$ correct evaluations
- $\boldsymbol{y}_j \neq \boldsymbol{f}(\alpha_j)$ erroneous evaluations

the *degree bound* $k > \deg(\boldsymbol{f})$

and *an upper bound τ on the number of errors*.

GOAL: **reconstruct** $\boldsymbol{f}(x)$

Simultaneous Cauchy Interpolation

Decoding Interleaved Reed-Solomon codes

Simultaneous Interpolation with Errors

Given the received matrix with columns $\boldsymbol{y}_1, \dots, \boldsymbol{y}_n$

- $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)$ correct evaluations
- $\boldsymbol{y}_j \neq \boldsymbol{f}(\alpha_j)$ erroneous evaluations

the *degree bound* $k > \deg(\boldsymbol{f})$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $\boldsymbol{f}(x)$

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \dots, \boldsymbol{y}_n$

and the *degree bounds* $\tau + k$, $\tau + 1$

GOAL: **find** $\underbrace{(\varphi_1(x), \dots, \varphi_l(x)}_{\boldsymbol{\varphi}(x)}, \psi(x))$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < \tau + k$
- $\deg(\psi) < \tau + 1$

↓

Simultaneous Rational Function Reconstruction

Decoding Interleaved Reed-Solomon codes

Simultaneous Interpolation with Errors

Given the received matrix with columns $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$

- $y_j = f(\alpha_j)$ correct evaluations
- $y_j \neq f(\alpha_j)$ erroneous evaluations

the *degree bound* $k > \deg(f)$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $f(x)$

$(\Lambda(x)f(x), \Lambda(x))$

solution

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$

and the *degree bounds* $\tau + k$, $\tau + 1$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_l(x)}_{\boldsymbol{\varphi}(x)}, \psi(x))$ s.t.

- $\Lambda(\alpha_j)f_i(\alpha_j) = y_{i,j}\Lambda(\alpha_j)$
- $\deg(\Lambda f) < \tau + k$
- $\deg(\Lambda) < \tau + 1$

$$\Lambda(x) = \prod_{\alpha_j \textbf{ erroneous}} (x - \alpha_j)$$

Error Locator Polynomial

roots = erroneous evaluation points

$\deg(\Lambda)$ = nb errors

Decoding Interleaved Reed-Solomon codes

Simultaneous Interpolation with Errors

Given the received matrix with columns $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$

- $\boldsymbol{y}_j = \boldsymbol{f}(\alpha_j)$ correct evaluations
- $\boldsymbol{y}_j \neq \boldsymbol{f}(\alpha_j)$ erroneous evaluations

the *degree bound* $k > \deg(\boldsymbol{f})$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $\boldsymbol{f}(x)$

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$

and the *degree bounds* $\tau + k$, $\tau + 1$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_l(x)}_{\boldsymbol{\varphi}(x)}, \psi(x))$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < \tau + k$
- $\deg(\psi) < \tau + 1$

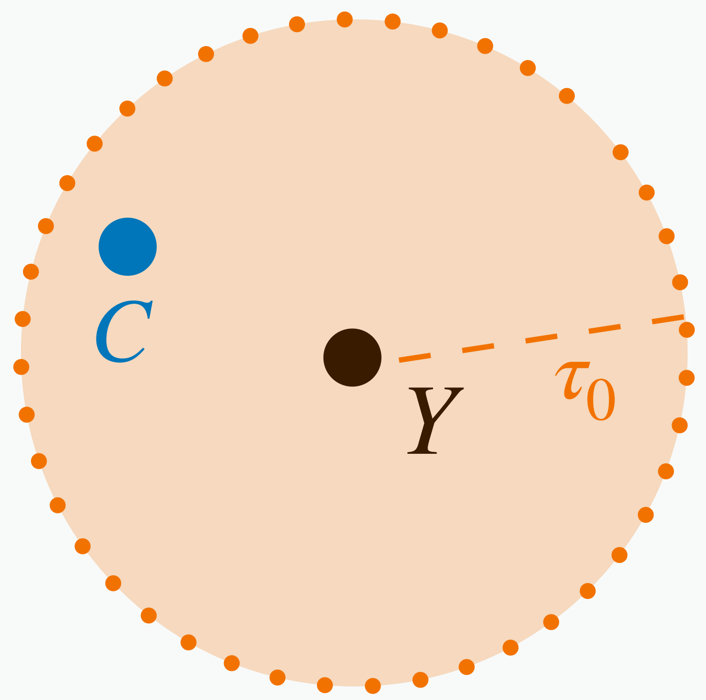
↓

uniqueness

$(\Lambda(x)\boldsymbol{f}(x), \Lambda(x))$

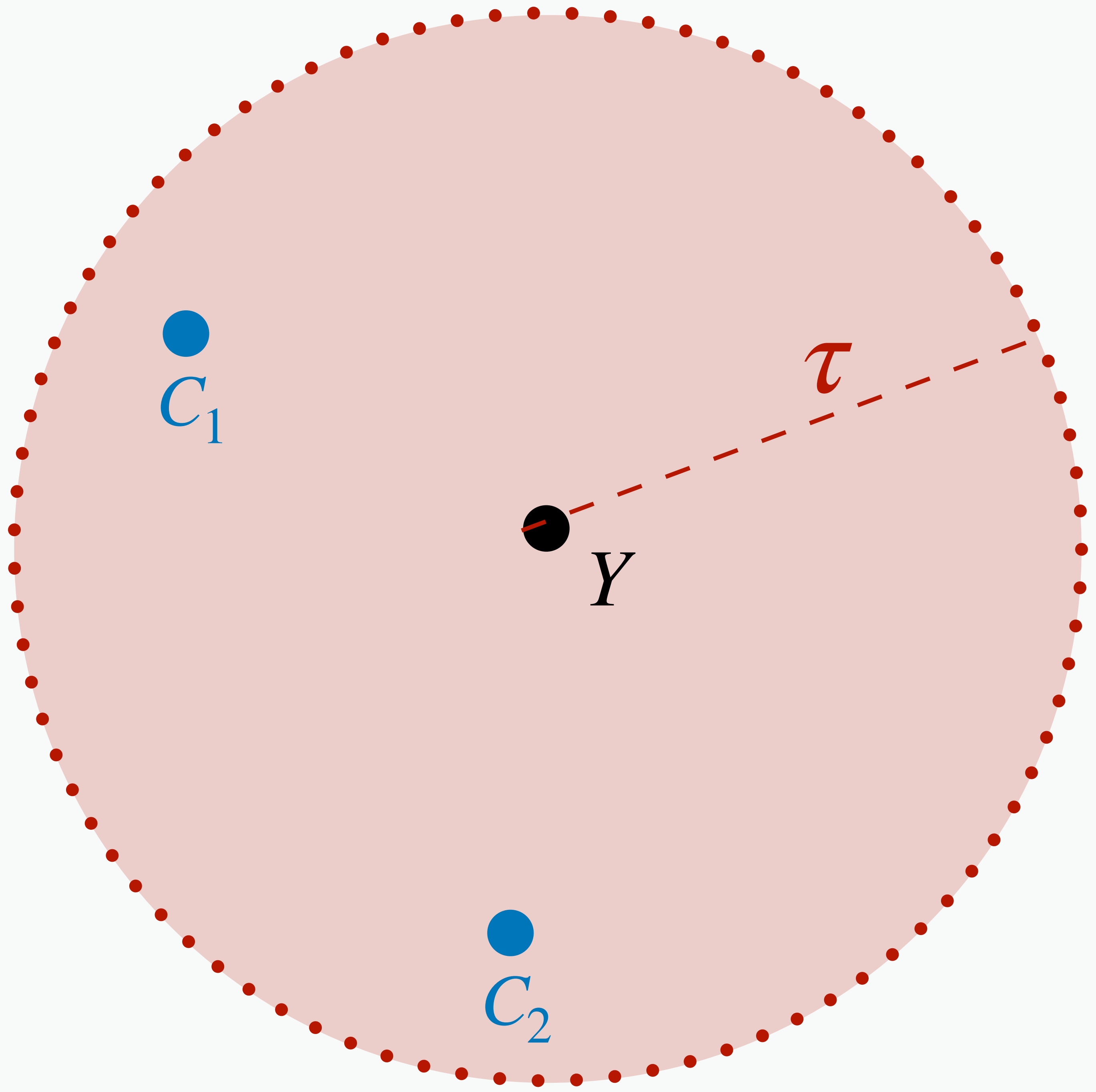
↓

unique decoding



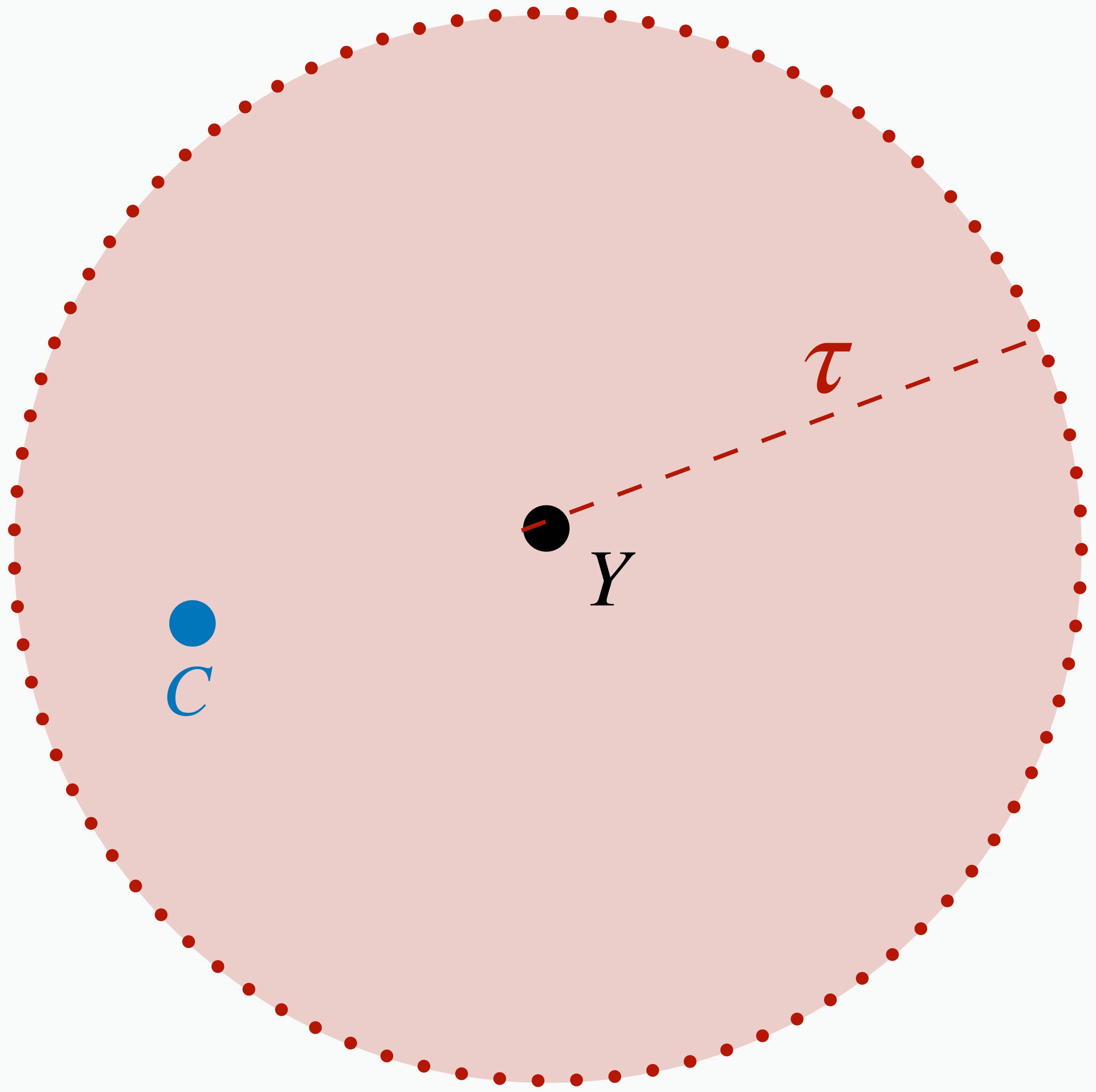
1. Unique decoding Capability

nb errors $\leq \frac{n-k}{2} = \frac{d-1}{2} := \tau_0 \longrightarrow$ unique decoding



1. Unique decoding Capability

nb errors $\leq \frac{n-k}{2} = \frac{d-1}{2} := \tau_0 \longrightarrow$ unique decoding



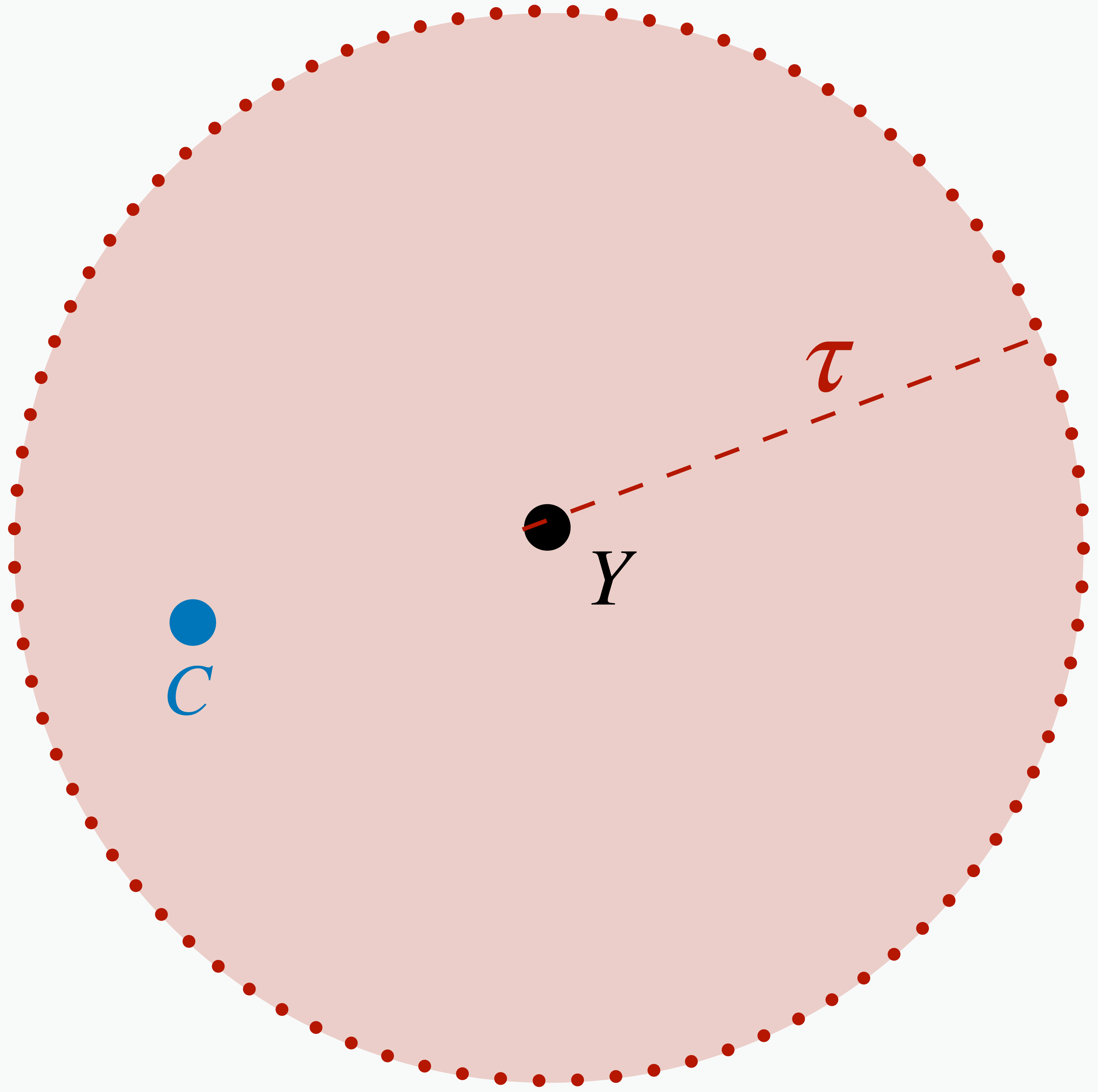
1. Unique decoding Capability

nb errors $\leq \dfrac{n-k}{2} = \dfrac{d-1}{2} := \tau_0 \longrightarrow$ unique decoding

2. [BLEICHENBACHER, KIAYIAS, YUNG, 2003]

nb errors $\leq \dfrac{l(n-k)}{l+1} =: \tau_{IRS} \longrightarrow$ uniqueness for almost all error patterns

The proportion of error patterns leading to non-uniqueness $\leq$ nb errors$/q$



1. Unique decoding Capability

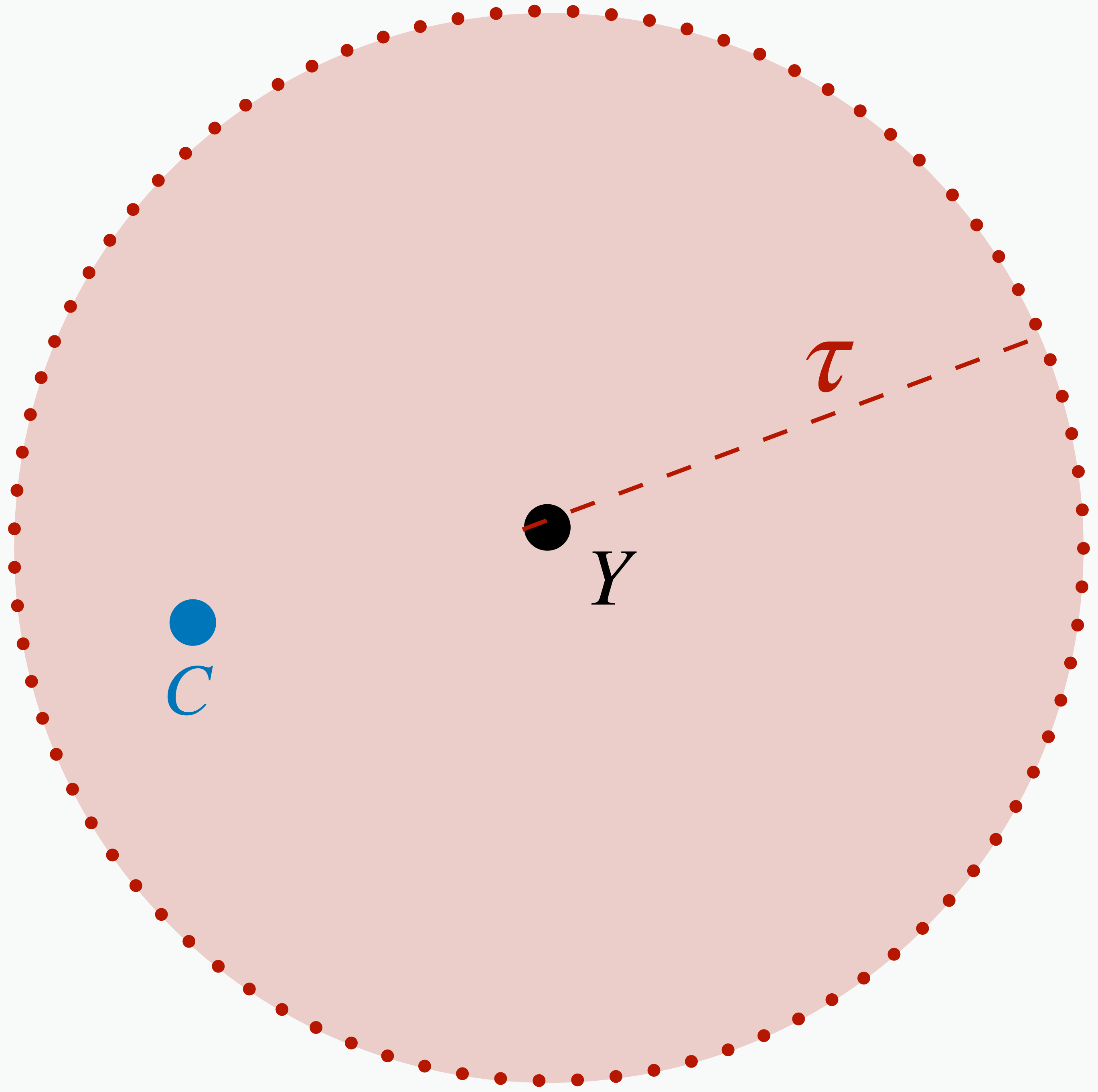
$$\text{nb errors} \leq \frac{n-k}{2} = \frac{d-1}{2} := \tau_0 \longrightarrow \text{unique decoding}$$

2. [BLEICHENBACHER, KIAYIAS, YUNG, 2003]

$$\text{nb errors} \leq \frac{l(n-k)}{l+1} =: \tau_{IRS} \longrightarrow \text{uniqueness for almost all error patterns}$$

The proportion of error patterns leading to non-uniqueness $\leq$ nb errors$/q$

does not depend on errors, $\mathcal{O}(1/q)$
[BROWN, MINDER, SHOKROLLAHI, 2004]
[SCHIMDT, SIDORENKO, BOSSERT, 2009]
[PUCHINGER, ROSENKILDE, 2017]



1. Unique decoding Capability

nb errors $\leq \frac{n-k}{2} = \frac{d-1}{2} := \tau_0 \longrightarrow$ unique decoding

2. [BLEICHENBACHER, KIAYIAS, YUNG, 2003]

nb errors $\leq \frac{l(n-k)}{l+1} =: \tau_{IRS} \longrightarrow$ uniqueness for almost all error patterns

The proportion of error patterns leading to non-uniqueness $\leq$ nb errors$/q$

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n$

and the *degree bounds* $\tau + k$, $\tau + 1$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_l(x), \psi(x))}_{\boldsymbol{\varphi}(x)}$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < \tau + k$
- $\deg(\psi) < \tau + 1$

1. Cauchy Interpolation component-wise (RFR)

$n = \tau + k + \tau \iff$ nb errors $\leq \frac{n-k}{2} =: \tau_0 \longrightarrow$ uniqueness

2. Common denominator feature

$n = k + \left\lceil \frac{\tau}{l} \right\rceil + \tau \iff$ nb errors $\leq \frac{l(n-k)}{l+1} =: \tau_{IRS} \longrightarrow$ uniqueness for almost all error patterns

Simultaneous Cauchy Interpolation with Errors

Simultaneous Interpolation with Errors

Reconstruct a **vector of polynomials** by its evaluations, some erroneous

$\updownarrow$

decoding IRS codes

Simultaneous Cauchy Interpolation with Errors

Reconstruct a **vector of rational functions** by its evaluations, some erroneous

↓

Simultaneous Cauchy Interpolation

Number of Evaluations - Outline of this work

			uniqueness	uniqueness *almost always*
no-errors	$(\boldsymbol{v}(x), d(x))$		$L = N + D - 1$ Cauchy Interpolation	$L = N + \left\lceil \frac{(D-1)}{n} \right\rceil$
	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$		$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\}$ [CABAY, 1971]	
with errors	$(\boldsymbol{v}(x), d(x))$	d constant ($D = 1$)	$L = N - 1 + 2\tau$ Unique Decoding Capability Theorem (IRS codes)	$L = N - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$ [BLEICHENBACHER, KIAYIAS, YUNG, 2003]
		$D > 1$	[BOYER, KALTOFEN, 2014]	**[GUERRINI, LEBRETON, Z., 2019]**
	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$		[KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]	**[GUERRINI, LEBRETON, Z., 2021]**

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation with Errors

Given $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

- $\boldsymbol{y}_j = \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ correct evaluations
- $\boldsymbol{y}_j \neq \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ erroneous evaluations

the *degree bounds* $N > \deg(\boldsymbol{v})$, $D > \deg(d)$

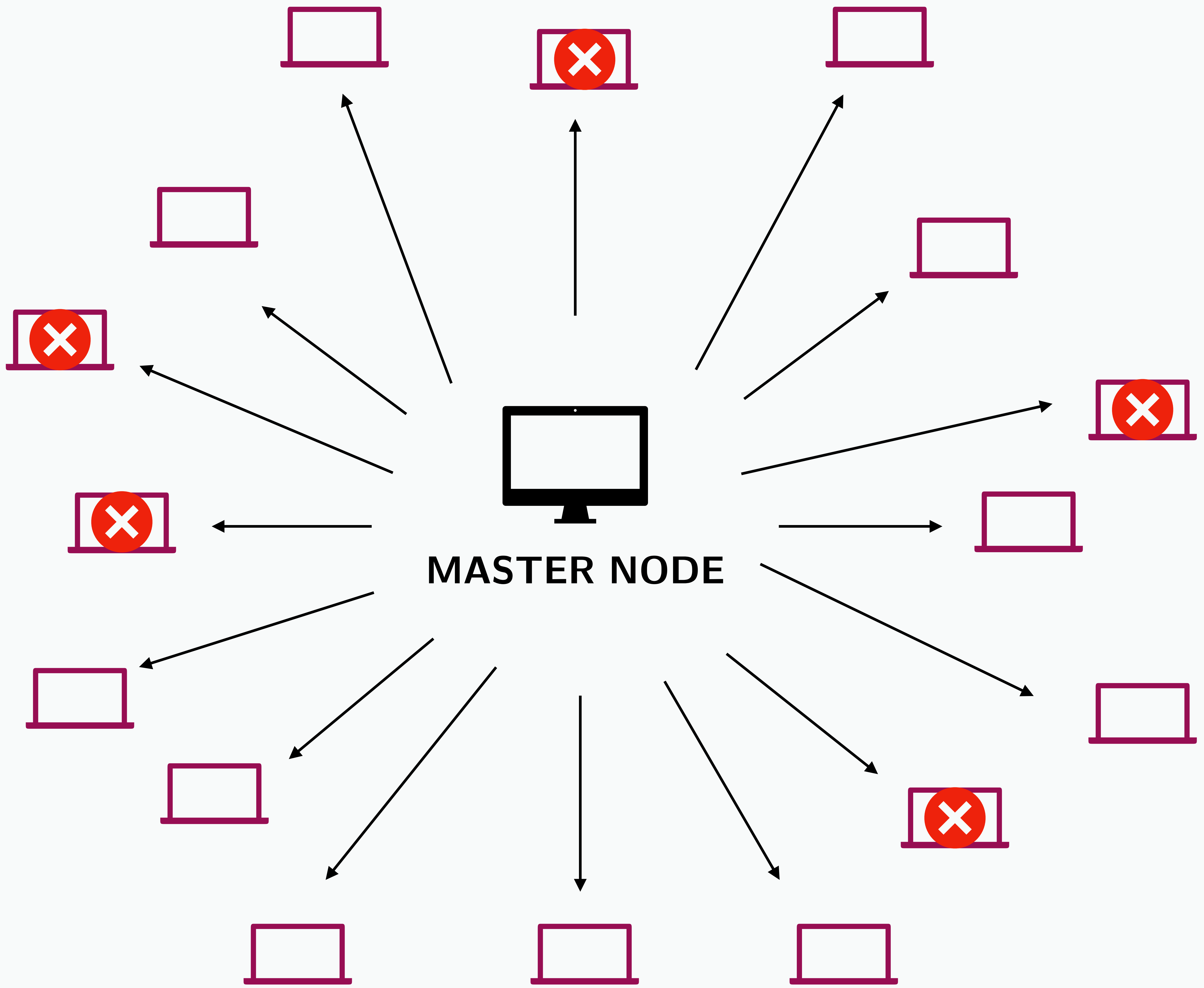
and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $(\boldsymbol{v}(x), d(x)) \longrightarrow \boldsymbol{y}(x)$

↓

Simultaneous Cauchy Interpolation

Simultaneous Rational Function Reconstruction



Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation with Errors

Given $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

- $\boldsymbol{y}_j = \frac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ correct evaluations
- $\boldsymbol{y}_j \neq \frac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ erroneous evaluations

the *degree bounds* $N > \deg(\boldsymbol{v})$, $D > \deg(d)$

and *an upper bound τ on the number of errors*.

GOAL: **reconstruct** $(\boldsymbol{v}(x), d(x)) \longrightarrow \boldsymbol{y}(x)$

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* $N + \tau$, $D + \tau$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_n(x), \psi(x))}_{\boldsymbol{\varphi}(x)}$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < N + \tau$
- $\deg(\psi) < D + \tau$

$(\Lambda(x)\boldsymbol{v}(x), \Lambda(x)d(x))$

solution

$$\Lambda(x) = \prod_{\alpha_j \text{ erroneous}} (x - \alpha_j)$$

Error Locator Polynomial

roots = erroneous evaluation points

$\deg(\Lambda)$ = nb errors

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation with Errors

Given $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

- $\boldsymbol{y}_j = \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ correct evaluations
- $\boldsymbol{y}_j \neq \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ erroneous evaluations

the *degree bounds* $N > \deg(\boldsymbol{v})$, $D > \deg(d)$

and *an upper bound* τ *on the number of errors*.

GOAL: **reconstruct** $(\boldsymbol{v}(x), d(x)) \longrightarrow \boldsymbol{y}(x)$

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* $N + \tau$, $D + \tau$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_n(x), \psi(x))}_{\boldsymbol{\varphi}(x)}$ s.t.

- $\Lambda(\alpha_j)v_i(\alpha_j) = y_{i,j}\Lambda(\alpha_j)$
- $\deg(\Lambda v_i) < N + \tau$
- $\deg(\Lambda d) < D + \tau$

$(\Lambda(x)\boldsymbol{v}(x), \Lambda(x)d(x))$

solution

$$\Lambda(x) = \prod_{\alpha_j \text{ erroneous}} (x - \alpha_j)$$

Error Locator Polynomial

roots = erroneous evaluation points

$\deg(\Lambda)$ = nb errors

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation with Errors

Given $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

- $\boldsymbol{y}_j = \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ correct evaluations
- $\boldsymbol{y}_j \neq \dfrac{\boldsymbol{v}(\alpha_j)}{d(\alpha_j)}$ erroneous evaluations

the *degree bounds* $N > \deg(\boldsymbol{v})$, $D > \deg(d)$

and *an upper bound τ on the number of errors*.

GOAL: **reconstruct** $(\boldsymbol{v}(x), d(x)) \longrightarrow \boldsymbol{y}(x)$

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* $N + \tau$, $D + \tau$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_n(x)}_{\boldsymbol{\varphi}(x)}, \psi(x))$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < N + \tau$
- $\deg(\psi) < D + \tau$

$\downarrow$

uniqueness

$(\Lambda(x)\boldsymbol{v}(x), \Lambda(x)d(x))$

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* $N + \tau$, $D + \tau$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_n(x)}_{\boldsymbol{\varphi}(x)}, \psi(x))$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < N + \tau$
- $\deg(\psi) < D + \tau$

generalizing and re-elaborating the result of [BLEICHENBACHER, KIAYIAS, YUNG, 2003] for IRS codes

1. Cauchy Interpolation component-wise

   $L = N + D + 2\tau - 1 \longrightarrow$ uniqueness

   [BOYER, KALTOFEN, 2014]

2. If we want to recover a solution of a PLS

   $L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau \longrightarrow$ uniqueness

   [CABAY, 1971] ⟶ [KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]

$L = N + D - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau \longrightarrow$ uniqueness for almost all error patterns

If we want to recover a solution of a PLS

$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + \left\lceil \frac{\tau}{n} \right\rceil + \tau \longrightarrow$ uniqueness for almost all error patterns

The proportion of error patterns leading to non-uniqueness $\leq (D + \tau)/q$

Number of Evaluations - Outline of this work

			uniqueness	uniqueness *almost always*
no-errors	$(\boldsymbol{v}(x), d(x))$		$L = N + D - 1$ Cauchy Interpolation	$L = N + \left\lceil \frac{(D-1)}{n} \right\rceil$
no-errors	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$		$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\}$ [CABAY, 1971]	
with errors	$(\boldsymbol{v}(x), d(x))$	d constant $(D = 1)$	$L = N - 1 + 2\tau$ Unique Decoding Capability Theorem (IRS codes)	$L = N - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$ [BLEICHENBACHER, KIAYIAS, YUNG, 2003]
with errors	$(\boldsymbol{v}(x), d(x))$	$D > 1$	$L = N + D - 1 + 2\tau$ [BOYER, KALTOFEN, 2014]	$L = N + D - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$
with errors	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$	$D > 1$	$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau$ [KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]	$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + \left\lceil \frac{\tau}{n} \right\rceil + \tau$

Early Termination

$$\overline{L} = \min\{L_{BK}, L_{KPS}\}$$

- $L_{BK} = N + D + 2\tau - 1,$
- $L_{KPSW} = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau$

$\geq$

$$L_{new} = \min\{L_{GLZ19}, L_{GLZ20}\}$$

- $L_{GLZ19} = N + D - 1 + \tau + \left\lceil \frac{\tau}{n} \right\rceil,$
- $L_{GLZ21} = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + \tau + \left\lceil \frac{\tau}{n} \right\rceil$

All these bounds depend on

- $N \geq \deg(\boldsymbol{v})$
- $D \geq \deg(d)$
- $\tau \geq$ nb errors, e

we don't know these quantities

If N, D, τ are too big compared to $\deg(\boldsymbol{v})$, $\deg(d)$, e ⟶ $\overline{L}$, L_{new} too big compared to the number we really need

EARLY TERMINATION TECHNIQUE [KALTOFEN, PERNET, STORJOHANN, WADDELL, 2017]

GOAL: decrease the number of evaluation points without knowing the real degrees

Early termination strategy

$\deg(\boldsymbol{v})$
$\deg(\boldsymbol{d})$
$\boldsymbol{e}$

$\mathscr{L}$ which depends on
$\deg(\boldsymbol{v}), \deg(d)$, **nb errors** e

solution space

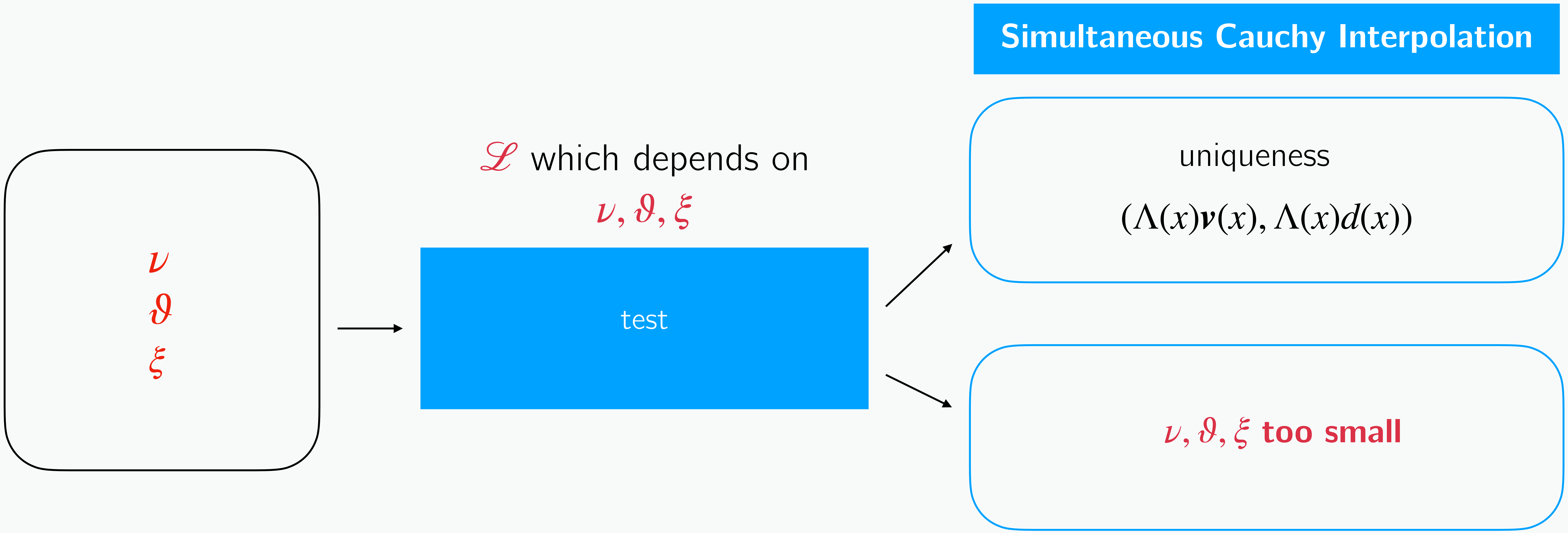
- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < \deg(\boldsymbol{v}) + e + 1$
- $\deg(\psi) < \deg(d) + e + 1$

Simultaneous Cauchy Interpolation

uniqueness

$(\Lambda(x)\boldsymbol{v}(x), \Lambda(x)d(x))$

Early termination strategy



Early termination strategy

ν

ϑ

ξ

$\mathscr{L}$ which depends on ν, ϑ, ξ

test

solution space

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < \nu + \xi$
- $\deg(\psi) < \vartheta + \xi$

Simultaneous Cauchy Interpolation

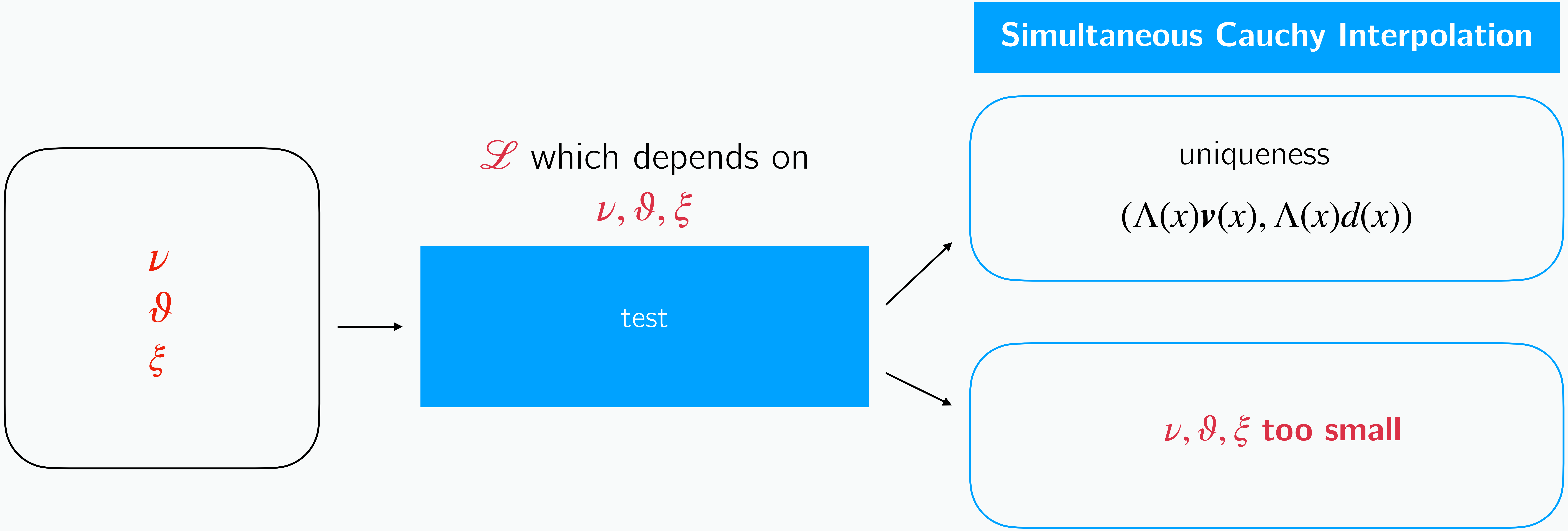
uniqueness

$(\Lambda(x)\boldsymbol{v}(x), \Lambda(x)d(x))$

ν, ϑ, ξ too small

solution space trivial

Early termination strategy



construct an early algorithm which iteratively increments $\mathscr{L}$ until a solution is found

Early termination strategy

ν
ϑ
ξ

$\mathscr{L}_{new} \leq \mathscr{L}$ which depends on ν, ϑ, ξ

test

Simultaneous Cauchy Interpolation

uniqueness **for almost all error patterns**
$(\Lambda(x)\boldsymbol{v}(x), \Lambda(x)d(x))$

ν, ϑ, ξ **too small**

Conclusions & Open Problems

PolSys-SpecFun Seminar

February 19, 2021

Number of Evaluations - Outline of this work

<table>
<tr><th></th><th></th><th></th><th>uniqueness</th><th>uniqueness
almost always</th></tr>
<tr><td rowspan="2">no-errors</td><td colspan="2">$(\boldsymbol{v}(x), d(x))$</td><td>$L = N + D - 1$
Cauchy Interpolation</td><td>$L = N + \left\lceil \frac{(D-1)}{n} \right\rceil$</td></tr>
<tr><td colspan="2">$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$</td><td>$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\}$
[CABAY, 1971]</td><td></td></tr>
<tr><td rowspan="3">with errors</td><td rowspan="2">$(\boldsymbol{v}(x), d(x))$</td><td>$d$ constant
$(D = 1)$</td><td>$L = N - 1 + 2\tau$
Unique Decoding Capability Theorem (IRS codes)</td><td>$L = N - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$
[BLEICHENBACHER, KIAYIAS, YUNG, 2003]</td></tr>
<tr><td rowspan="2">$D > 1$</td><td>$L = N + D - 1 + 2\tau$
[BOYER, KALTOFEN, 2014]</td><td>$L = N + D - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$</td></tr>
<tr><td>$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$</td><td>$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau$
[KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]</td><td>$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + \left\lceil \frac{\tau}{n} \right\rceil + \tau$</td></tr>
</table>

Early termination technique

Publications

International conferences with proceedings

- ***Polynomial Linear System Solving with Errors by Simultaneous Polynomial Reconstruction of Interleaved Reed-Solomon codes.*** E.Guerrini, R.Lebreton, I.Zappatore. *In Proceedings of ISIT'19*, pages 1542-1546. IEEE, 2019
- ***On the Uniqueness of Rational Function Reconstruction.*** E.Guerrini, R.Lebreton, I.Zappatore. *In Proceedings of ISSAC'20.* ACM, 2020

Preprint, work in progress

- ***Polynomial Linear System Solving with Random Errors: new bounds and early termination technique.*** E.Guerrini, R.Lebreton, I.Zappatore. *arXiv:2102.04182*

Perspectives

Improving previous results

- On the uniqueness of the simultaneous rational function reconstruction
- Failure probability of Simultaneous Cauchy Interpolation with Errors

Extending previous results

- Rational Function Codes
- Early termination techniques for decoding error correcting codes
- Multivariate Rational Function Reconstruction

Improving previous results

- On the uniqueness of the simultaneous rational function reconstruction

On the uniqueness of SRFR

Simultaneous Rational Function Reconstruction

Given two vector of polynomials $\boldsymbol{u}(x), \boldsymbol{a}(x)$ and the *degree bounds* N, D

GOAL: **find** $\underbrace{(v_1(x), \ldots, v_n(x), d(x))}_{\boldsymbol{v}(x)}$ s.t.

- $v_i(x) = u_i(x)d(x) \bmod a_i(x)$
- $\deg(v_i) < N$
- $\deg(d) < D$

$$\frac{v_i(x)}{d(x)} = u_i(x) \bmod a_i(x), \gcd(a_i, d) = 1$$

If $L = N + (D-1)/n$, **for almost all instances** $u_i = v_i/d \implies$ **uniqueness?**

Theorem [GUERRINI, LEBRETON, Z., 2020]

If $L = \deg(\boldsymbol{a}) = N + (D-1)/n$, **for almost all instances** $\implies$ **uniqueness**.

If $\mathbb{K} = \mathbb{F}_q$, the **proportion of instances** leading to **non-uniqueness** is $\leq (D-1)/q$

Number of Evaluations - Outline of this work

			uniqueness	**uniqueness** *almost always*
no-errors	$\frac{v(x)}{d(x)}$		$L = N + D - 1$ Cauchy Interpolation	**?** $L = N + \left\lceil \frac{(D-1)}{n} \right\rceil$
	$A(x)\frac{v(x)}{d(x)} = b(x)$		$L = \max\{\deg(A) + N, \deg(b) + D\}$ [CABAY, 1971]	**?** $L = N + \left\lceil \frac{(D-1)}{n} \right\rceil$
with errors	$(v(x), d(x))$	d constant ($D = 1$)	$L = N - 1 + 2\tau$ Unique Decoding Capability Theorem (IRS codes)	$L = N - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$ [BLEICHENBACHER, KIAYIAS, YUNG, 2003]
		$D > 1$	$L = N + D - 1 + 2\tau$ [BOYER, KALTOFEN, 2014]	$L = N + D - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$
	$A(x)\frac{v(x)}{d(x)} = b(x)$		$L = \max\{\deg(A) + N, \deg(b) + D\} + 2\tau$ [KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]	$L = \max\{\deg(A) + N, \deg(b) + D\} + \left\lceil \frac{\tau}{n} \right\rceil + \tau$

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* $N+\tau$, $D+\tau$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_n(x)}_{\boldsymbol{\varphi}(x)}, \psi(x))$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < N+\tau$
- $\deg(\psi) < D+\tau$

↓

uniqueness

$(\Lambda(x)\boldsymbol{v}(x), \Lambda(x)d(x))$

1. Cauchy Interpolation component-wise (RFR)

   $L = N + D + 2\tau - 1 \longrightarrow$ uniqueness

   [BOYER, KALTOFEN, 2014]

2. If we want to recover a solution of a PLS

   $L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau \longrightarrow$ uniqueness

   [CABAY, 1971] ⟶ [KALTOFEN, PERNET, STORJOHANN, WADDEL, 2014]

Common denominator constraint

$$L = N + \left\lceil \frac{D-1+\tau}{n} \right\rceil + \tau \longrightarrow$$

uniqueness

for almost all error patterns

for almost all $\boldsymbol{v}/d$?

Improving previous results

- On the uniqueness of the simultaneous rational function reconstruction
- Failure probability of Simultaneous Cauchy Interpolation with Errors

Number of Evaluations - Outline of this work

			uniqueness	uniqueness *almost always*
no-errors	$(\boldsymbol{v}(x), d(x))$		$L = N + D - 1$ Cauchy Interpolation	$L = N + \left\lceil \frac{(D-1)}{n} \right\rceil$
	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$		$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\}$ [CABAY, 1971]	?
with errors	$(\boldsymbol{v}(x), d(x))$	d constant $(D = 1)$	$L = N - 1 + 2\tau$ Unique Decoding Capability Theorem (IRS codes)	$L = N - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$ [BLEICHENBACHER, KIAYIAS, YUNG, 2003]
		$D > 1$	$L = N + D - 1 + 2\tau$ [BOYER, KALTOFEN, 2014]	$L = N + D - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau$
	$A(x)\frac{\boldsymbol{v}(x)}{d(x)} = \boldsymbol{b}(x)$		$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau$ [KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]	$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + \left\lceil \frac{\tau}{n} \right\rceil + \tau$

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* $N + \tau$, $D + \tau$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_n(x), \psi(x))}_{\boldsymbol{\varphi}(x)}$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < N + \tau$
- $\deg(\psi) < D + \tau$

generalizing and re-elaborating the result of [BLEICHENBACHER, KIAYIAS, YUNG, 2003] for IRS codes

1. Cauchy Interpolation component-wise

   $L = N + D + 2\tau - 1 \longrightarrow$ uniqueness

   [BOYER, KALTOFEN, 2014]

2. If we want to recover a solution of a PLS

   $L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau \longrightarrow$ uniqueness

   [CABAY, 1971] ⟶ [KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]

$L = N + D - 1 + \left\lceil \frac{\tau}{n} \right\rceil + \tau \longrightarrow$ uniqueness for almost all error patterns

If we want to recover a solution of a PLS

$L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + \left\lceil \frac{\tau}{n} \right\rceil + \tau \longrightarrow$ uniqueness for almost all error patterns

The proportion of error patterns leading to non-uniqueness $\leq (D + \tau)/q$

Simultaneous Cauchy Interpolation with Errors

Simultaneous Cauchy Interpolation

Given the vectors $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_L$

and the *degree bounds* $N + \tau$, $D + \tau$

GOAL: **find** $\underbrace{(\varphi_1(x), \ldots, \varphi_n(x), \psi(x))}_{\boldsymbol{\varphi}(x)}$ s.t.

- $\varphi_i(\alpha_j) = y_{i,j}\psi(\alpha_j)$
- $\deg(\varphi_i) < N + \tau$
- $\deg(\psi) < D + \tau$

generalizing and re-elaborating the result of [BLEICHENBACHER, KIAYIAS, YUNG, 2003] for IRS codes

1. Cauchy Interpolation component-wise

   $L = N + D + 2\tau - 1 \longrightarrow$ uniqueness

   [BOYER, KALTOFEN, 2014]

2. If we want to recover a solution of a PLS

   $L = \max\{\deg(A) + N, \deg(\boldsymbol{b}) + D\} + 2\tau \longrightarrow$ uniqueness

   [CABAY, 1971] $\longrightarrow$ [KALTOFEN, PERNET, STORJOHANN, WADDEL, 2017]

$L = N + D - 1 + \left\lceil \frac{\tau}{\ldots} \right\rceil$ … uniqueness … atterns

If we want t…

$L = \max\{\deg$ … eness … error patterns

can we improve this bound?
prove that it does not depend on errors
as IRS?

[BROWN, MINDER, SHOKROLLAHI, 2004]
[SCHMIDT, SIDORENKO, BOSSERT, 2009]
[PUCHINGER, ROSENKILDE, 2017]

The proportion of error patterns leading to non-uniqueness $\leq (D + \tau)/q$

Conclusions & Open Problems

Improving previous results

- On the uniqueness of the simultaneous rational function reconstruction
- Failure probability of Simultaneous Cauchy Interpolation with Errors

Extending previous results

- Rational Function Codes

Simultaneous Cauchy Interpolation with Errors

Simultaneous Interpolation with Errors

Reconstruct a **vector of polynomials** by its evaluations, some erroneous

↕

decoding IRS codes

—

Simultaneous Cauchy Interpolation with Errors

Reconstruct a **vector of rational functions** by its evaluations, some erroneous

↕

decoding specific Interleaved Rational Function codes

[PERNET, 2017]

↓ ↓

🛠 **Simultaneous Cauchy Interpolation**

Conclusions & Open Problems

Rational Function Code [PERNET, 2017]

generalization of Reed-Solomon codes, **non linear**

Let $N, D \leq L \leq q$ and $\{\alpha_1, \ldots, \alpha_L\}$ distinct *evaluation points*,

$$\mathscr{C}_{RF}(n,k) := \left\{ \left(\frac{v(\alpha_1)}{d(\alpha_1)}, \ldots, \frac{v(\alpha_L)}{d(\alpha_L)} \right) \mid \frac{v}{d} \in \mathbb{F}_q(x), \deg(v) < N, \deg(d) < D, d(\alpha_j) \neq 0 \right\}$$

Interleaved Rational Function Code [PERNET, 2017]

the minimum distance $\geq L - (N + D + 2)$

Let $N, D \leq L \leq q$ and $\{\alpha_1, \ldots, \alpha_L\}$ distinct *evaluation points*,

$$\mathscr{C}_{RF}(n,k) := \left\{ \left(\frac{\boldsymbol{v}(\alpha_1)}{\boldsymbol{d}(\alpha_1)}, \ldots, \frac{\boldsymbol{v}(\alpha_L)}{\boldsymbol{d}(\alpha_L)} \right) \mid \frac{\boldsymbol{v}}{\boldsymbol{d}} \in \mathbb{F}_q(x)^{n \times 1}, \deg(v) < N, \deg(d) < D, d_i(\alpha_j) \neq 0 \right\}$$

Improving previous results

- On the uniqueness of the simultaneous rational function reconstruction
- Failure probability of Simultaneous Cauchy Interpolation with Errors

Extending previous results

- Rational Function Codes → determine parameters and other applications
- Early termination techniques for decoding error correcting codes
  [KHONJI, PERNET, ROCH, ROCHE, STALINSKI, 2010]
- Multivariate (Simultaneous) Rational Function Reconstruction
  ↘ coding theory applications, decoding (interleaved) AG codes

Thank you

PolSys-SpecFun Seminar

February 19, 2021