Probabilistic Analysis of LLL-based decoder of Interleaved Chinese Remainder Codes

Matteo Abbondati, Eleonora Guerrini,
Romain Lebreton

JC2 - Najac 20/10/2023

LIRMM

Table of contents

Chinese Remainder Codes

Interleaving

Decoding algorithm for ICR codes

Our result

Bonus Track...Not just ICR codes

Outline

Chinese Remainder Codes

Interleaving

Decoding algorithm for ICR codes

Our result

Bonus Track...Not just ICR codes

Chinese Remainder Theorem $N = \prod_{i=1}^{n} p_i$

$$\begin{aligned} \mathbb{Z}_N &\longrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_n} \\ a &\longmapsto ([a]_{p_1}, \ldots, [a]_{p_n}) \end{aligned}$$

Chinese Remainder Theorem & Redundancy

Chinese Remainder Theorem $N = \prod_{i=1}^{n} p_i$

$$\begin{aligned} \mathbb{Z}_N &\longrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_n} \\ a &\longmapsto ([a]_{p_1}, \ldots, [a]_{p_n}) \end{aligned}$$

Redundancy

If we know that $0 \leq a < K < N \Rightarrow$
$([a]_{p_1}, \ldots, [a]_{p_n})$ has redundant information

Chinese Remainder Theorem & Redundancy

Chinese Remainder Theorem $N = \prod_{i=1}^{n} p_i$

$$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_n}$$
$$a \longmapsto ([a]_{p_1}, \ldots, [a]_{p_n})$$

Redundancy

If we know that $0 \leq a < K < N \Rightarrow$
$([a]_{p_1}, \ldots, [a]_{p_n})$ has redundant information

Example

$$N = 3 \cdot 5 \cdot 7 = 105$$
$$K = 3 \cdot 5 = 15$$
$$a = 6 \leftrightsquigarrow (0, 1, 6) \in \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

Chinese Remainder Theorem & Redundancy

Chinese Remainder Theorem $N = \prod_{i=1}^{n} p_i$

$$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_n}$$
$$a \longmapsto ([a]_{p_1}, \ldots, [a]_{p_n})$$

Redundancy

If we know that $0 \leq a < K < N \Rightarrow$ $([a]_{p_1}, \ldots, [a]_{p_n})$ has redundant information

Example

$$N = 3 \cdot 5 \cdot 7 = 105$$
$$K = 3 \cdot 5 = 15$$
$$a = 6 \leftrightsquigarrow (0, 1, 6) \in \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

6 is the only integer $a \in [0, 14]$ with

$$\begin{cases} [a]_3 = 0 \\ [a]_5 = 1 \end{cases}$$

Chinese Remainder Theorem & Redundancy

Chinese Remainder Theorem $N = \prod_{i=1}^{n} p_i$

$$\mathbb{Z}_N \longrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_n}$$
$$a \longmapsto ([a]_{p_1}, \ldots, [a]_{p_n})$$

Redundancy

If we know that $0 \leq a < K < N \Rightarrow$
$([a]_{p_1}, \ldots, [a]_{p_n})$ has redundant information

Example

$$N = 3 \cdot 5 \cdot 7 = 105$$
$$K = 3 \cdot 5 = 15$$
$$a = 6 \leftrightsquigarrow (0, 1, 6) \in \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

6 is the only integer
$a \in [0, 14]$ with
$$\begin{cases} [a]_3 = 0 \\ [a]_5 = 1 \end{cases}$$

Chinese Remainder code

Let $p_1 < \ldots < p_n$, let $k < n$ thus $K = \prod_{i=1}^{k} p_i < N = \prod_{i=1}^{n} p_i$.

$$\mathcal{C} = CR(N, K) := \{([C]_{p_1}, \ldots, [C]_{p_n}) : 0 \leq C < K\}$$

Evaluation - Interpolation codes

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

Polyalphabetic code? Different metric!

$$CR(N, K) := \pi_{p_1} \times \ldots \times \pi_{p_n}([0, K)) \subseteq \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_n}$$

Weighted Distance

$\Lambda_{r,c} = \prod_{i:r_i \neq c_i} p_i$ Error locator, $d_{r,c} = \log_2(\Lambda_{r,c}) = \sum_{i:r_i \neq c_i} \log_2(p_i)$

Reed Solomon codes	Chinese Remainder codes
Linear	Not Linear
monoalphabetic	polyalphabetic
Hamming metric	Weighted distance
MDS: $d = n - k + 1$	$d > \log_2\left(\frac{N}{K}\right)$

Outline

Chinese Remainder Codes

Interleaving

Decoding algorithm for ICR codes

Our result

Bonus Track...Not just ICR codes

Interleaving

Burst Errors Channels

$$\ldots \left| c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} \right| c_{2,1}, c_{2,2}, c_{2,3}, c_{2,4}, c_{2,5} \left| c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} \right| \ldots$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\ldots \left| c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} \right| c_{2,1}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} \left| c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} \right| \ldots$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\dots \left| \underline{c_{1,1}}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} \right| c_{2,1}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} \left| c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} \right| \dots$$

$$\dots \left| c_{1,1} \right.$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\ldots \left| c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} \right| \underline{c_{2,1}}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} \left| c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} \right| \ldots$$

$$\ldots \left| c_{1,1}, c_{2,1} \right.$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\ldots \left| c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} \right| c_{2,1}, \xcancel{c_{2,2}}, \xcancel{c_{2,3}}, \xcancel{c_{2,4}}, c_{2,5} \left| \underline{c_{3,1}}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} \right| \ldots$$

$$\ldots \left| c_{1,1}, c_{2,1}, c_{3,1} \right.$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\dots \left| c_{1,1}, \underline{c_{1,2}}, c_{1,3}, c_{1,4}, c_{1,5} \right| c_{2,1}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} \left| c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} \right| \dots$$

$$\dots \left| c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2} \right.$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\ldots \left| c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} \right| c_{2,1}, \underline{\cancel{c_{2,2}}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} \left| c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} \right| \ldots$$

$$\ldots \left| c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2}, c_{2,2} \right.$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\ldots | c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} | c_{2,1}, c_{2,2}, c_{2,3}, c_{2,4}, c_{2,5} | c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} | \ldots$$

$$\ldots | c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2}, c_{2,2}, c_{3,2}, c_{1,3}, c_{2,3}, c_{3,3}, c_{1,4}, c_{2,4}, c_{3,4}, c_{1,5}, c_{2,5}, c_{3,5} | \ldots$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\dots | c_{1,1}, c_{1,2}, \bigcirc\!\!\!\!\!c_{1,3}, c_{1,4}, c_{1,5} | c_{2,1}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} | c_{3,1}, c_{3,2}, \bigcirc\!\!\!\!\!c_{3,3}, c_{3,4}, c_{3,5} | \dots$$

$$\dots | c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2}, c_{2,2}, c_{3,2}, \cancel{c_{1,3}}, \cancel{c_{2,3}}, \cancel{c_{3,3}}, c_{1,4}, c_{2,4}, c_{3,4}, c_{1,5}, c_{2,5}, c_{3,5} | \dots$$

$$I_\ell(\mathcal{C}) = \left\{ \begin{pmatrix} \cdots & \vec{c}_1 & \cdots \\ \cdots & \vec{c}_2 & \cdots \\ & \vdots & \\ \cdots & \vec{c}_\ell & \cdots \end{pmatrix} : \vec{c}_i \in \mathcal{C} \right\}$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\dots |c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5}|c_{2,1}, c_{2,2}, c_{2,3}, c_{2,4}, c_{2,5}|c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5}| \dots$$

$$\dots |c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2}, c_{2,2}, c_{3,2}, c_{1,3}, c_{2,3}, c_{3,3}, c_{1,4}, c_{2,4}, c_{3,4}, c_{1,5}, c_{2,5}, c_{3,5}| \dots$$

$$I_\ell(\mathcal{C}) = \left\{ \begin{pmatrix} \cdots & \vec{c}_1 & \cdots \\ \cdots & \vec{c}_2 & \cdots \\ & \vdots & \\ \cdots & \vec{c}_\ell & \cdots \end{pmatrix} : \vec{c}_i \in \mathcal{C} \right\}$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\ldots \,|c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5}|c_{2,1}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5}|c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5}|\,\ldots$$

$$\ldots \,|c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2}, c_{2,2}, c_{3,2}, \cancel{c_{1,3}}, \cancel{c_{2,3}}, \cancel{c_{3,3}}, c_{1,4}, c_{2,4}, c_{3,4}, c_{1,5}, c_{2,5}, c_{3,5}|\,\ldots$$

$$I_\ell(\mathcal{C}) = \left\{ \begin{pmatrix} \cdots & \vec{c}_1 & \cdots \\ \cdots & \vec{c}_2 & \cdots \\ & \vdots & \\ \cdots & \vec{c}_\ell & \cdots \end{pmatrix} : \vec{c}_i \in \mathcal{C} \right\}$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\ldots | c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} | c_{2,1}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} | c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} | \ldots$$

$$\ldots | c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2}, c_{2,2}, c_{3,2}, \cancel{c_{1,3}}, \cancel{c_{2,3}}, \cancel{c_{3,3}}, c_{1,4}, c_{2,4}, c_{3,4}, c_{1,5}, c_{2,5}, c_{3,5} | \ldots$$

$$I_\ell(\mathcal{C}) = \left\{ \begin{pmatrix} \vec{c}_1 & \cdots \\ \vec{c}_2 & \cdots \\ \vdots & \\ \vec{c}_\ell & \cdots \end{pmatrix} : \vec{c}_i \in \mathcal{C} \right\}$$

Interleaving

Burst Errors Channels (length bursts $\ell \approx 3$)

$$\dots | c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5} | c_{2,1}, \cancel{c_{2,2}}, \cancel{c_{2,3}}, \cancel{c_{2,4}}, c_{2,5} | c_{3,1}, c_{3,2}, c_{3,3}, c_{3,4}, c_{3,5} | \dots$$

$$\dots | c_{1,1}, c_{2,1}, c_{3,1}, c_{1,2}, c_{2,2}, c_{3,2}, \cancel{c_{1,3}}, \cancel{c_{2,3}}, \cancel{c_{3,3}}, c_{1,4}, c_{2,4}, c_{3,4}, c_{1,5}, c_{2,5}, c_{3,5} | \dots$$

$$I_\ell(\mathcal{C}) = \left\{ \begin{pmatrix} \dots & \vec{c}_1 & \dots \\ \dots & \vec{c}_2 & \dots \\ & \vdots & \\ \dots & \vec{c}_\ell & \dots \end{pmatrix} : \vec{c}_i \in \mathcal{C} \right\}$$

- Localized errors on common coordinates
- Increases the decoding radius beyond d_u
- Involves a failure probability analysis

Outline

Chinese Remainder Codes

Interleaving

Decoding algorithm for ICR codes

Our result

Bonus Track...Not just ICR codes

Decoding of Interleaved CR codes [LSN13][1]

$0 \le C_i < K$

$$(C_1, \dots, C_\ell) \mapsto \begin{pmatrix} [C_1]_{p_1} & \cdots & [C_1]_{p_n} \\ [C_2]_{p_1} & \cdots & [C_2]_{p_n} \\ & \vdots & \\ [C_\ell]_{p_1} & \cdots & [C_\ell]_{p_n} \end{pmatrix} \xrightarrow[\text{Channel}]{\overbrace{\begin{pmatrix} e_{1,1} & \cdots & e_{1,n} \\ & \vdots & \\ e_{\ell,1} & \cdots & e_{\ell,n} \end{pmatrix}}^{t \text{ columns} \sim \mathcal{U}\left(\mathbb{Z}_{p_i}^{\ell}\right)}} \begin{pmatrix} [R_1]_{p_1} & \cdots & [R_1]_{p_n} \\ [R_2]_{p_1} & \cdots & [R_2]_{p_n} \\ & \vdots & \\ [R_\ell]_{p_1} & \cdots & [R_\ell]_{p_n} \end{pmatrix} \in D_{\boldsymbol{C},\xi_r}$$

$$\Lambda = \prod_{i \in \xi_r} p_i$$

[1] Li, Wenhui, Vladimir Sidorenko, and Johan SR Nielsen. "On decoding interleaved chinese remainder codes." 2013 IEEE International Symposium on Information Theory. IEEE, 2013.

Decoding of Interleaved CR codes [LSN13][1]

$0 \le C_i < K$

$$(C_1, \dots, C_\ell) \mapsto \begin{pmatrix} [C_1]_{p_1} & \cdots & [C_1]_{p_n} \\ [C_2]_{p_1} & \cdots & [C_2]_{p_n} \\ & \vdots & \\ [C_\ell]_{p_1} & \cdots & [C_\ell]_{p_n} \end{pmatrix} \overset{\overbrace{\begin{pmatrix} e_{1,1} & \cdots & e_{1,n} \\ & \vdots & \\ e_{\ell,1} & \cdots & e_{\ell,n} \end{pmatrix}}^{t \text{ columns} \sim \mathcal{U}\left(\mathbb{Z}_{p_i}^{\ell}\right)}}{\underset{\Lambda = \prod_{i \in \xi_r} p_i}{\xrightarrow{\text{Channel}}}} \begin{pmatrix} [R_1]_{p_1} & \cdots & [R_1]_{p_n} \\ [R_2]_{p_1} & \cdots & [R_2]_{p_n} \\ & \vdots & \\ [R_\ell]_{p_1} & \cdots & [R_\ell]_{p_n} \end{pmatrix} \in D_{\boldsymbol{C}, \xi_r}$$

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

[1] Li, Wenhui, Vladimir Sidorenko, and Johan SR Nielsen. "On decoding interleaved chinese remainder codes." 2013 IEEE International Symposium on Information Theory. IEEE, 2013.

Decoding of Interleaved CR codes [LSN13][1]

$0 \le C_i < K$

$$(C_1,\ldots,C_\ell) \mapsto \begin{pmatrix} [C_1]_{p_1} & \cdots & [C_1]_{p_n} \\ [C_2]_{p_1} & \cdots & [C_2]_{p_n} \\ & \vdots & \\ [C_\ell]_{p_1} & \cdots & [C_\ell]_{p_n} \end{pmatrix} \overset{\overbrace{\begin{pmatrix} e_{1,1} & \cdots & e_{1,n} \\ & \vdots & \\ e_{\ell,1} & \cdots & e_{\ell,n}\end{pmatrix}}^{t \text{ columns} \sim \mathcal{U}\left(\mathbb{Z}_{p_i}^{\ell}\right)}}{\rightsquigarrow} \begin{pmatrix} [R_1]_{p_1} & \cdots & [R_1]_{p_n} \\ [R_2]_{p_1} & \cdots & [R_2]_{p_n} \\ & \vdots & \\ [R_\ell]_{p_1} & \cdots & [R_\ell]_{p_n} \end{pmatrix} \in D_{\boldsymbol{C},\xi_r}$$

Channel

$$\Lambda = \prod_{i \in \xi_r} p_i$$

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

$\Lambda \le 2^\tau$

Short elements of $\mathcal{L}$

↓

$$(\Lambda, \Lambda C_1, \ldots, \Lambda C_\ell) \in S_R = \{(\varphi, \psi_1, \ldots, \psi_\ell) \in \mathcal{L} : 0 < \varphi < 2^\tau, |\psi_i| < 2^\tau K\} \subseteq \mathcal{L}$$

LLL

[1] Li, Wenhui, Vladimir Sidorenko, and Johan SR Nielsen. "On decoding interleaved chinese remainder codes." 2013 IEEE International Symposium on Information Theory. IEEE, 2013.

Outline

Chinese Remainder Codes

Interleaving

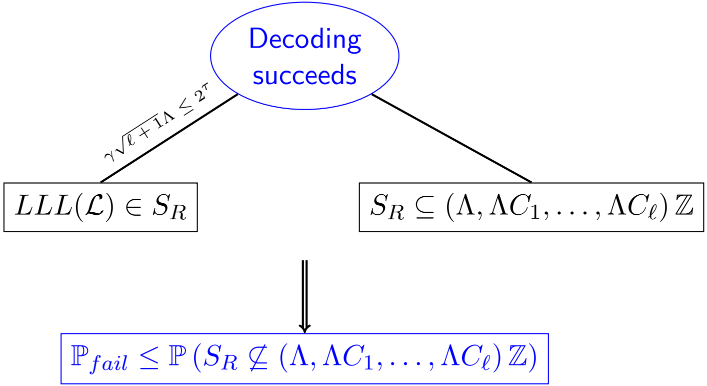
Decoding algorithm for ICR codes

Our result

Bonus Track...Not just ICR codes

Idea of the analysis

$$(\Lambda, \Lambda C_1, \ldots, \Lambda C_\ell) \in S_R = \{(\varphi, \psi_1, \ldots, \psi_\ell) \in \mathcal{L} : 0 < \varphi < 2^\tau, |\psi_i| < 2^\tau K\} \subseteq \mathcal{L}$$



Our Result [AAGL][2]

Theorem (Decoding ICR codes)

Set

$$d_{\max} := \frac{\ell}{\ell+1}\left[\log(N) - \log(K) - \log\left(6\gamma\sqrt{\ell+1}\right)\right].$$

Choose $d_t < d_{\max}$, *set* $\tau_t := d_t + \log\left(\gamma\sqrt{\ell+1}\right)$.
Consider $R \sim D_{C,\mathcal{E}_r}$ *such that* $\log \Lambda_r \leq d_t$.
Then the decoding algorithm on random input R *outputs the center codeword* C *of the distribution* $D_{C,\mathcal{E}_r}$, *with a probability of failure* $\mathbb{P}_f$ *upper-bounded by*

$$\mathbb{P}_f \leq 2^{-(\ell+1)(d_{\max}-d_t)} + \exp\left(\frac{n}{p_1^{\ell-1}}\right) - 1.$$

[2] Abbondati, Matteo, et al. "Probabilistic Analysis of LLL-based Decoder of Interleaved Chinese Remainder Codes." ITW 2023-IEEE Information Theory Workshop. 2023.

Outline

Chinese Remainder Codes

Interleaving

Decoding algorithm for ICR codes

Our result

Bonus Track...Not just ICR codes

Rational Extensions of Evaluation-Interpolation Codes [P][3]

Field of fractions of $\mathbb{F}_q[x]$: $\mathbb{F}_q(x)$

RF Codes

$$\mathbb{F}_q(x)$$
$$\cup|$$
$$\left\{ \frac{f}{g} \in \mathbb{F}_q(x) : d^o(f) < d_f, d^o(g) < d_g, \gcd(f,g) = 1 \right\}$$

$$ev_{\alpha_1} \quad \ldots \quad ev_{\alpha_n}$$

$$\vec{c} = \left(\frac{f}{g}(\alpha_1), \ldots, \frac{f}{g}(\alpha_n) \right)$$

Field of fractions of $\mathbb{Z}$: $\mathbb{Q}$

RN Codes

$$\mathbb{Q}$$
$$\cup|$$
$$\left\{ \frac{f}{g} \in \mathbb{Q} : |f| < F, 0 < g < G, \gcd(f,g) = 1 \right\}$$

$$ev_{p_1} \quad \ldots \quad ev_{p_n}$$

$$\vec{c} = ([f]_{p_1}[g]^{-1}_{p_1}, \ldots, [f]_{p_1}[g]^{-1}_{p_n})$$

[3] Pernet, Clément. High performance and reliable algebraic computing. Diss. Université Joseph Fourier, Grenoble 1, 2014.

State of the Art

	Previously	Us
IRN	$\emptyset$	$d < \frac{\ell}{\ell+1}\left[\log(N) - \log(FG) - \log\left(6\gamma\sqrt{\ell+1}\right)\right]$ $\mathbb{P}_f \leq 2^{-(\ell+1)(d_{\max}-d_t)} + \exp\left(\frac{n}{p_1^{\ell-1}}\right) - 1$
IRF	$t < \frac{\ell}{\ell+1}(n - d_f - d_g + 1)$ $\mathbb{P}_f \leq \frac{d_g+t}{q}$ [GLZ][4]	$t < \frac{\ell}{\ell+1}(n - d_f - d_g + 1)$ $\mathbb{P}_f \leq \frac{1}{q}\frac{1}{q^{(\ell+1)(t_{max}-t)}}\exp\left(\frac{t}{q}\right) + \frac{2t}{q^\ell}$

[4] Guerrini, E., Lebreton, R., & Zappatore, I. (2020). Enhancing simultaneous rational function recovery: adaptive error correction capability and new bounds for applications. arXiv preprint arXiv:2003.01793.

Thank you for your attention!