

Rate-Optimal Streaming Codes over Small Finite Fields for Burst/Random Erasure Channels

Takayuki Nozaki

Yamaguchi University

June 27th, 2023

ISIT2023

Introduction

Low latency and reliable packet communications are required in various applications.

- Vehicle-to-Vehicle communication
- Real-time applications

Introduction

Low latency and reliable packet communications are required in various applications.

- Vehicle-to-Vehicle communication
- Real-time applications

A solution for this problem is streaming code

Streaming code [Martinian-Sundberg-2004]

Erasur correcting code satisfying **decoding delay constraint**

Topic of this talk

Construction of streaming codes

Channel Model

(a, b, w) -sliding window erasure (SWE) channel

Packet erasure channel with random and burst erasures

- w : width of window
- Each window contains $\leq a$ random erasures or a burst erasure of length $\leq b$

Example of Erasure Pattern: $a = 2$, $b = 4$, $w = 5$

Transmitted Packets



Received Packets



Burst erasure of length 4

Channel Model

(a, b, w) -sliding window erasure (SWE) channel

Packet erasure channel with random and burst erasures

- w : width of window
- Each window contains $\leq a$ random erasures or a burst erasure of length $\leq b$

Example of Erasure Pattern: $a = 2$, $b = 4$, $w = 5$

Transmitted Packets



Received Packets



Burst erasure of length 3

Channel Model

(a, b, w) -sliding window erasure (SWE) channel

Packet erasure channel with random and burst erasures

- w : width of window
- Each window contains $\leq a$ random erasures or a burst erasure of length $\leq b$

Example of Erasure Pattern: $a = 2$, $b = 4$, $w = 5$

Transmitted Packets



Received Packets



Burst erasure of length 2

Channel Model

(a, b, w) -sliding window erasure (SWE) channel

Packet erasure channel with random and burst erasures

- w : width of window
- Each window contains $\leq a$ random erasures or a burst erasure of length $\leq b$

Example of Erasure Pattern: $a = 2$, $b = 4$, $w = 5$

Transmitted Packets



Received Packets



Random erasure of size 2

Channel Model

(a, b, w) -sliding window erasure (SWE) channel

Packet erasure channel with random and burst erasures

- w : width of window
- Each window contains $\leq a$ random erasures or a burst erasure of length $\leq b$

Example of Erasure Pattern: $a = 2$, $b = 4$, $w = 5$

Transmitted Packets



Received Packets



Random erasure of size 1

Channel Model

(a, b, w) -sliding window erasure (SWE) channel

Packet erasure channel with random and burst erasures

- w : width of window
- Each window contains $\leq a$ random erasures or a burst erasure of length $\leq b$

Example of Erasure Pattern: $a = 2$, $b = 4$, $w = 5$

Transmitted Packets



Received Packets



Random erasure of size 2

Decoding Delay Constraint

Streaming codes impose the τ -decoding delay constraint on the decoder. Packet x_i must be recovered from received packets $y_1, y_2, \dots, y_{i+\tau}$

$(a, b, w; \tau)$ delay-constrained sliding-window (DCSW) model

- (a, b, w) -SWE channel
- τ -decoding delay (DD) constraint

Optimal rate of streaming code for $(a, b, w; \tau)$ DCSW model [Badr-2017]

$$\tau_{\text{eff}} := \min\{w - 1, \tau\}$$

$$R \leq \frac{\tau_{\text{eff}} - a + 1}{\tau_{\text{eff}} - a + b + 1}$$

The streaming codes achieving this equality are called **rate-optimal**.

In this talk,

We construct rate-optimal streaming codes for $(a, b, w; \tau)$ DCSW model.

Related Works

Rate Optimal Streaming Codes for $(a, b, w; \tau)$ DCSW model

Paper	Order of GF	Condition of Parameter	Explicit
[Fong-2019]	$2\binom{\tau+1}{a}$	Arbitrary feasible param.	No
[Krishnan-2020]	$\bar{\tau}^2$	Arbitrary feasible param.	No
[Krishnan-2020]	$\bar{\tau}$	$b - a = 1$	No
[Krishnan-2020]	$\bar{\tau}$	$(\tau + a + 1) \geq 2b \geq 4a$	Yes
[Krishnan-2020]	$\left(\frac{a}{b}\tau\right)$	$a \mid b \mid (\tau + 1 + b + a)$	Yes
[Ramkumar-2020]	$\bar{\tau}$	$\gcd(b, \tau + 1 - a) \geq a$	Yes
[Ramkumar-2020]	$\bar{\tau}$	$[\tau + 1 \geq a + b] \wedge [a \mid b]$	Yes
[Ramkumar-2020]	$\bar{\tau}$	$[\tau + 1 \geq a + b] \wedge [a \mid (b + 1)]$	Yes
[Domanovitz-2022]	$\bar{\tau}^2$	Arbitrary feasible param.	Yes
[Bhatnagar-2022]	$\bar{\tau}$	$\tau \geq w + b - a - 1$	Yes
This work	$\bar{\tau}$	Arbitrary feasible param.	Yes

($\bar{\tau}$ represents the integer satisfying $\bar{\tau} \geq \tau$ and $\bar{\tau} = p^m$)

Construbtion of This Work

- The code construction in this work is influenced by [Krishman-2020] and [Domanovitz-2022].
- These constructions **locally** use the property of $\text{GF}(\bar{\tau}^2)$
(Almost parts use the property of $\text{GF}(\bar{\tau})$)

Contribution of this work

- By designing parity check matrix,
 - we give the **explicit** construction of the streaming code
 - we give an **efficient encoding algorithm** for the code
- By using companion matrix, we reduce the order of finite field.
- We give an **efficient decoding** algorithm for the code.

Settings of Parameters

In the $(a, b, w; \tau)$ DCSW model, it is sufficient to consider only the case

- $a \leq b$
- $w = \tau + 1$

Reasons:

- If $a > b$, the problem is reduced to the case $a = b$
(a : number of random erasures, b : length of burst erasure)
- Optimal code for $(a, b, \tau + 1; \tau)$ DCSW model is also optimal for $w \neq \tau + 1$ cases

Optimal rate of $(a, b, w; \tau)$ -DCSW model

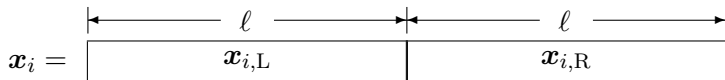
$$\frac{\tau_{\text{eff}} - a + 1}{\tau_{\text{eff}} - a + b + 1} \quad \tau_{\text{eff}} := \min\{w - 1, \tau\}$$

Sub-packet Division

$\mathbf{x}_i \in \mathbb{F}_q^{2\ell}$: i th transmitted packet ($q = 2^m$, $q > \tau$)

Sub-packet Division

We divide each packet into two sub-packets



Parity Check Matrix of Proposed Code

Example: $a = 5, b = 8, \tau = 13, w = 14$ ($\delta := b - a$)

$$\mathbf{H} = \left(\begin{array}{c|cccccccc|cccc}
 \begin{array}{cccccccc}
 \mathbf{J} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{J} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{J} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0}
 \end{array} &
 \begin{array}{cccc}
 \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}
 \end{array} &
 \begin{array}{cccc}
 \mathbf{J} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{J} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{J} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{J}
 \end{array} \\
 \hline
 \begin{array}{cccc}
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I}
 \end{array} &
 \begin{array}{ccc}
 \mathbf{0} & \mathbf{0} & \mathbf{I} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0}
 \end{array} \\
 \hline
 \begin{array}{cccc}
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0}
 \end{array} &
 \begin{array}{ccc}
 \mathbf{0} & \mathbf{0} & \mathbf{I} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0} \\
 \mathbf{0} & \mathbf{0} & \mathbf{0}
 \end{array}
 \end{array} \right)$$

Dimensions: τ (total width), b (width of top-left block), $\delta + 1$ (width of top-right block), δ (height of top-right block), a (height of bottom blocks), $\tau - a + 1$ (width of bottom-left block), b (width of bottom-right block).

Note: Any $t \times t$ sub-matrix of Cauchy matrix \mathbf{C} is non-singular

$$\mathbf{C} \otimes \mathbf{I} = \begin{pmatrix} c_{1,1} \mathbf{I} & c_{1,2} \mathbf{I} & \cdots & c_{1,\tau+a+1} \mathbf{I} \\ c_{2,1} \mathbf{I} & c_{2,2} \mathbf{I} & \cdots & c_{2,\tau+a+1} \mathbf{I} \\ \vdots & \vdots & \ddots & \vdots \\ c_{a,1} \mathbf{I} & c_{a,2} \mathbf{I} & \cdots & c_{a,\tau+a+1} \mathbf{I} \end{pmatrix}$$

Parity Check Matrix of Proposed Code

Example: $a = 5, b = 8, \tau = 13, w = 14$ ($\delta := b - a$)

$$\mathbf{H} = \begin{pmatrix}
 \begin{array}{cccccccc|cccc}
 \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} \\
 \hline
 & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{I} \\
 & & & & & & & & & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O}
 \end{array}
 \end{pmatrix}$$

$\mathbf{C} \otimes \mathbf{I}$

τ (width of top row), b (width of first δ columns), $\delta + 1$ (width of last δ columns), δ (height of top δ rows), a (height of bottom a rows), $\tau - a + 1$ (width of left part of bottom rows), b (width of right part of bottom rows)

\mathbf{H} satisfies optimal rate

code length $n := \tau - a + b + 1$, dimension $k := n - b = \tau - a + 1$

Optimal rate of DCSW model

$$\frac{\tau_{\text{eff}} - a + 1}{\tau_{\text{eff}} - a + b + 1} \quad \tau_{\text{eff}} := \min\{w - 1, \tau\}$$

Encoding Algorithm for Proposed Code

Decide parity packets $\mathbf{p}_1, \mathbf{p}_2, \dots, \mathbf{p}_b$ from source packets $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k$

$$\mathbf{H} \begin{pmatrix} \mathbf{U} \\ \mathbf{P} \end{pmatrix} = \mathbf{O}_{2n \times \ell}.$$

$$\mathbf{U} = \begin{pmatrix} \mathbf{u}_{1,L} \\ \mathbf{u}_{1,R} \\ \mathbf{u}_{2,L} \\ \mathbf{u}_{2,R} \\ \vdots \\ \mathbf{u}_{k,L} \\ \mathbf{u}_{k,R} \end{pmatrix}, \quad \mathbf{P} = \begin{pmatrix} \mathbf{p}_{1,L} \\ \mathbf{p}_{1,R} \\ \mathbf{p}_{2,L} \\ \mathbf{p}_{2,R} \\ \vdots \\ \mathbf{p}_{b,L} \\ \mathbf{p}_{b,R} \end{pmatrix}$$

Examples of Decoding for Proposed Code (Burst 1)

Example: $a = 5, b = 8, \tau = 13, w = 14$ (Burst erasure in 1–8)

$$\mathbf{H} = \begin{pmatrix}
 \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} \\
 \hline
 & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{I} \\
 & & & & & & & & & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 \hline
 ? & ? & ? & ? & ? & ? & ? & ? & ? & ! & ! & ! & ! & ! & ! & - & - & -
 \end{pmatrix}$$

$\mathbf{C} \otimes \mathbf{I}$

Decoding of \mathbf{x}_1 :

- From the property of SWE channel, $\mathbf{x}_9, \mathbf{x}_{10}, \dots, \mathbf{x}_{14}$ are correctly received (!)
- By the τ -DD constraint, $\mathbf{x}_{15}, \mathbf{x}_{16}, \mathbf{x}_{17}$ have not been received (-)

From constraint of 1st row

$$\begin{pmatrix} \mathbf{x}_{1,L} \\ \mathbf{x}_{1,R} \end{pmatrix} = \mathbf{J}^{-1} \begin{pmatrix} \mathbf{x}_{9,L} \\ \mathbf{x}_{9,R} \end{pmatrix} + \begin{pmatrix} \mathbf{x}_{14,L} \\ \mathbf{x}_{14,R} \end{pmatrix}$$

Examples of Decoding for Proposed Code (Burst 2)

Example: $a = 5, b = 8, \tau = 13, w = 14$ (Burst erasure in 3–10)

$$\mathbf{H} = \begin{pmatrix}
 \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} \\
 \hline
 & & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{I} \\
 & & & & & & & & & & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 \hline
 \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{?} & \mathbf{?} & \mathbf{?} & \mathbf{?} & \mathbf{?} & \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{!} & \mathbf{!}
 \end{pmatrix}$$

Decoding of $\mathbf{x}_4, \mathbf{x}_5, \dots, \mathbf{x}_8$

- From the property of SWE channel, \mathbf{x}_{17} is correctly received (!)

Since the light blue part is non-singular, these are recoverable

Examples of Decoding for Proposed Code (Burst 3)

Example: $a = 5, b = 8, \tau = 13, w = 14$ (Burst erasure in 9–16)

$$\mathbf{H} = \left(\begin{array}{cccccccc|cccccccc}
 \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} \\
 \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{J} & \mathbf{O} \\
 \hline
 & & & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{I} \\
 & & & & & & & & & & & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & & & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 & & & & & & & & & & & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\
 \hline
 & & & & & & & & & & & ? & ? & ? & ? & ? & ? & ? & ? & \mathbf{I} \\
 \hline
 ! & ! & ! & ! & ! & ! & ! & ! & ! & ? & ? & ? & ? & ? & ? & ? & ? & ? & !
 \end{array} \right)$$

Principle of Decoding

Theorem 1

$$\left(\begin{array}{c|ccc} \mathbf{J} + a_{1,1}\mathbf{I} & a_{1,2}\mathbf{I} & \cdots & a_{1,t}\mathbf{I} \\ \hline a_{2,1}\mathbf{I} & a_{2,2}\mathbf{I} & \cdots & a_{2,t}\mathbf{I} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t,1}\mathbf{I} & a_{t,2}\mathbf{I} & \cdots & a_{t,t}\mathbf{I} \end{array} \right)$$

is non-singular if and only if

$$\begin{pmatrix} a_{2,2} & \cdots & a_{2,t} \\ \vdots & \ddots & \vdots \\ a_{t,2} & \cdots & a_{t,t} \end{pmatrix}$$

is non-singular

[Note] Light blue part in the previous slide satisfies the condition

Examples of Decoding for Proposed Code (Random 1)

Example $a = 5, b = 8, \tau = 13, w = 14$

$$\mathbf{H} = \left(\begin{array}{cccccccccccccccc|cccc}
 \text{J} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{I} & \text{O} & \text{O} & \text{O} & \text{O} & \text{J} & \text{O} & \text{O} & \text{O} \\
 \text{O} & \text{J} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{I} & \text{O} & \text{O} & \text{O} & \text{O} & \text{J} & \text{O} & \text{O} \\
 \text{O} & \text{O} & \text{J} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{I} & \text{O} & \text{O} & \text{O} & \text{O} & \text{J} & \text{O} \\
 \hline
 & & & & & & & & & & \text{O} & \text{O} & \text{O} & \text{O} & \text{I} & \text{O} & \text{O} & \text{I} \\
 \hline
 & & & & & & & & & & \text{I} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} \\
 & & & & \text{C} \otimes \text{I} & & & & & & \text{O} & \text{I} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} \\
 & & & & & & & & & & \text{O} & \text{O} & \text{I} & \text{O} & \text{O} & \text{O} & \text{O} & \text{O} \\
 & & & & & & & & & & \text{O} & \text{O} & \text{O} & \text{I} & \text{O} & \text{O} & \text{O} & \text{O} \\
 \hline
 ? & ! & ! & ! & ? & ! & ? & ! & ? & ! & ? & ! & ! & ! & ! & - & - & -
 \end{array} \right)$$

From Theorem 1, light blue part is non-singular

Examples of Decoding for Proposed Code (Random 2)

Example: $a = 5, b = 8, \tau = 13, w = 14$

$\mathbf{H} =$

J	O	O	O	O	O	O	O	I	O	O	O	O	J	O	O	O
O	J	O	O	O	O	O	O	O	I	O	O	O	O	J	O	O
O	O	J	O	O	O	O	O	O	O	I	O	O	O	O	J	O
									O	O	O	O	I	O	O	I
									I	O	O	O	O	O	O	O
									O	I	O	O	O	O	O	O
									O	O	I	O	O	O	O	O
									O	O	O	I	O	O	O	O

C \otimes I

? ! ! ! ? ! ? ! ? ! ! ! ! ! - - -

- 1 By the lower 4 rows, recover except x_{14}
- 2 By the 1st row, recover x_{14}

Low-Complexity Decoding Algorithm

Decoding algorithm needs to solve \mathbf{X} of the following equation

Question: Can we efficiently solve the following equation?

(In a naive algorithm, we need to use augmented matrix with $2t$ rows)

$$\begin{pmatrix} \mathbf{J} + a_{1,1}\mathbf{I} & a_{1,2}\mathbf{I} & \cdots & a_{1,t}\mathbf{I} \\ a_{2,1}\mathbf{I} & a_{2,2}\mathbf{I} & \cdots & a_{2,t}\mathbf{I} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t,1}\mathbf{I} & a_{t,2}\mathbf{I} & \cdots & a_{t,t}\mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{x}_{1,L} \\ \mathbf{x}_{1,R} \\ \mathbf{x}_{2,L} \\ \mathbf{x}_{2,R} \\ \vdots \\ \mathbf{x}_{t,L} \\ \mathbf{x}_{t,R} \end{pmatrix} = \begin{pmatrix} \mathbf{b}_{1,L} \\ \mathbf{b}_{1,R} \\ \mathbf{b}_{2,L} \\ \mathbf{b}_{2,R} \\ \vdots \\ \mathbf{b}_{t,L} \\ \mathbf{b}_{t,R} \end{pmatrix}$$

Low-Complexity Decoding Algorithm

Decoding algorithm needs to solve \mathbf{X} of the following equation

Question: Can we efficiently solve the following equation?

(In a naive algorithm, we need to use augmented matrix with $2t$ rows)

$$\begin{pmatrix} \mathbf{J} + a_{1,1}\mathbf{I} & a_{1,2}\mathbf{I} & \cdots & a_{1,t}\mathbf{I} \\ a_{2,1}\mathbf{I} & a_{2,2}\mathbf{I} & \cdots & a_{2,t}\mathbf{I} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t,1}\mathbf{I} & a_{t,2}\mathbf{I} & \cdots & a_{t,t}\mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{x}_{1,L} \\ \mathbf{x}_{1,R} \\ \mathbf{x}_{2,L} \\ \mathbf{x}_{2,R} \\ \vdots \\ \mathbf{x}_{t,L} \\ \mathbf{x}_{t,R} \end{pmatrix} = \begin{pmatrix} \mathbf{b}_{1,L} \\ \mathbf{b}_{1,R} \\ \mathbf{b}_{2,L} \\ \mathbf{b}_{2,R} \\ \vdots \\ \mathbf{b}_{t,L} \\ \mathbf{b}_{t,R} \end{pmatrix}$$

Answer: It can be solved like as the following problem (matrix of t rows)

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,t} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t,1} & a_{t,2} & \cdots & a_{t,t} \end{pmatrix} \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_t \end{pmatrix} = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_t \end{pmatrix}$$

Low-Complexity Decoding Algorithm

- 1 Construct augmented matrix \mathbf{F}

$$\mathbf{F} = \left(\begin{array}{cccc|cc} a_{1,1} & a_{1,2} & \cdots & a_{1,t} & \mathbf{b}_{1,L} & \mathbf{b}_{1,R} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,t} & \mathbf{b}_{2,L} & \mathbf{b}_{2,R} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{t,1} & a_{t,2} & \cdots & a_{t,t} & \mathbf{b}_{t,L} & \mathbf{b}_{t,R} \end{array} \right).$$

- 2 (Forward Elimination) Apply elementary row operations to \mathbf{F}

$$\left(\begin{array}{cccc|cc} a'_{1,1} & 0 & \cdots & 0 & \mathbf{b}'_{1,L} & \mathbf{b}'_{1,R} \\ a'_{2,1} & \boxed{\phantom{\mathbf{I}}} & & & \mathbf{b}'_{2,L} & \mathbf{b}'_{2,R} \\ \vdots & & \mathbf{I} & & \vdots & \vdots \\ a_{t,1'} & & & & \mathbf{b}'_{t,L} & \mathbf{b}'_{t,R} \end{array} \right).$$

- 3 Derive $\mathbf{x}_{1,L}, \mathbf{x}_{1,R}$ as follows:

$$\begin{pmatrix} \mathbf{x}_{1,L} \\ \mathbf{x}_{1,R} \end{pmatrix} = (f(a'_{1,1}))^{-1} \begin{pmatrix} \beta + a'_{1,1} & 1 \\ 1 & a'_{1,1} \end{pmatrix} \begin{pmatrix} \mathbf{b}'_{1,L} \\ \mathbf{b}'_{1,R} \end{pmatrix}.$$

- 4 (Backward Substitution) Derive $\mathbf{x}_{i,L}, \mathbf{x}_{i,R}$ ($i = 2, \dots, k$) as follows:

$$(\mathbf{x}_{i,L}, \mathbf{x}_{i,R}) = (\mathbf{b}'_{i,L}, \mathbf{b}'_{i,R}) + a'_{i,1}(\mathbf{x}_{1,L}, \mathbf{x}_{1,R}).$$

Conclusion

Construct streaming codes satisfying

- Rate-optimal
- Over $\mathbb{F}_{\bar{\tau}}$ ($\bar{\tau} > \tau$ and $\bar{\tau} = 2^m$)
- Explicit construction

For this code,

- we give an encoding algorithm
- we give a decoding algorithm
- we reduce the complexity of sub-routine of decoding (Theorem 1)