符号理論家のための量子削除訂正符号入門

野崎 隆之 [1,2]　　萩原学 [3]

[1] 山口大学 大学院創成科学研究科 理学系学域
[2] 山口大学 時間学研究所

[3] 千葉大学大学院理学研究院

電子情報通信学会ソサイエティ大会
2024/9/12

§1. はじめに (講演者（野崎）の思い)

講演者 (野崎) は古典符号理論家

§1. はじめに (講演者（野崎）の思い)

講演者 (野崎) は古典符号理論家

- 量子符号は最近流行っている

§1. はじめに (講演者（野崎）の思い)

講演者 (野崎) は古典符号理論家

- 量子符号は最近流行っている
  $\Rightarrow$ どうにかして参入したい！

§1. はじめに (講演者（野崎）の思い)

講演者 (野崎) は古典符号理論家

- 量子符号は最近流行っている
  $\Rightarrow$ どうにかして参入したい！
- 量子符号は取っ付きづらい

§1. はじめに (講演者（野崎）の思い)

講演者 (野崎) は古典符号理論家

- 量子符号は最近流行っている
  $\Rightarrow$ どうにかして参入したい！
- 量子符号は取っ付きづらい
  $\Rightarrow$ (古典) 符号理論家に理解しやすい符号はないか？

§1. はじめに (講演者（野崎）の思い)

講演者 (野崎) は古典符号理論家

- 量子符号は最近流行っている
  ⇒ どうにかして参入したい！
- 量子符号は取っ付きづらい
  ⇒ (古典) 符号理論家に理解しやすい符号はないか？

問い

(古典) 符号理論家にとって

- 参入しやすく
- 理解しやすい

量子符号はあるか？

§1. はじめに (量子削除訂正符号)

答え

ある！ 量子削除訂正符号.

§1. はじめに (量子削除訂正符号)

答え

ある！ 量子削除訂正符号.

量子削除訂正符号は...

- 2020 年に初めて構成された
  $\Rightarrow$ 多くの研究課題が残っている！
- いくつかの量子削除符号は，古典符号の知識でほぼ理解できる

§1. はじめに (量子削除訂正符号)

答え

ある！ 量子削除訂正符号.

量子削除訂正符号は...

- 2020 年に初めて構成された
  $\Rightarrow$ 多くの研究課題が残っている！
- いくつかの量子削除符号は，古典符号の知識でほぼ理解できる

今日のテーマ

古典符号の知識でほぼ理解できる
「量子 RS 符号に基づく量子削除訂正符号」[H2023]
を紹介する

[H2023] M. Hagiwara, "Quantum deletion codes derived from quantum Reed-Solomon codes," arXiv preprint arXiv:2306.13399, 2023.

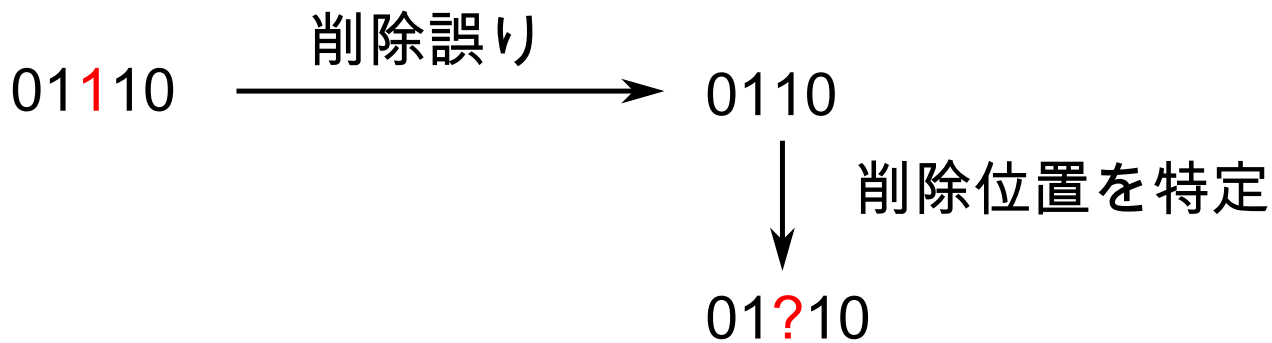
§1. はじめに (話の流れ)

§2. （古典）削除誤りと消失誤り

削除誤り

送信系列のシンボルが空列に変化する誤り

削除位置がわかれば，消失誤りとみなせる
$\Rightarrow$ (消失訂正符号) + (削除位置検出法) $\rightarrow$ (削除訂正符号)



§2. （古典）線形符号

(n, k) 線形符号

- パリティ検査行列 $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$ で定義される符号

$$\{\boldsymbol{x} \in \mathbb{F}_q^n \mid \mathbf{H}\boldsymbol{x}^T = \mathbf{0}^T\}$$

- 最小距離 d の符号は $d-1$ 個の消失を訂正可能

(n, k) リードソロモン (RS) 符号 C_{RS}

- 符号長 $n = q-1$．$\alpha : \mathbb{F}_q$ の原始元．

$$\mathbf{H} = (\alpha^{(i-1)(j-1)})_{i,j} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k-1} & \alpha^{2(n-k-1)} & \cdots & \alpha^{(n-1)(n-k-1)} \end{pmatrix}$$

- 最小距離 $d = n-k+1$

§2. （古典）2元展開による2元符号の構成

- $\mathbb{F}_{2^m}$ の元は，長さ m の $\mathbb{F}_2$ 上の系列（ブロック）で表現可能
- $\mathbb{F}_{2^m}$ 上の (n,k)RS 符号 C_{RS} は，
  $\mathbb{F}_2$ 上の (nm,km) 符号 $\mathcal{B}(C_{\mathrm{RS}})$ に変換可能
- $\mathcal{B}(C_{\mathrm{RS}})$ は消失を含むブロックが $n-k$ 個以下なら訂正可能

原始多項式 x^3+x+1．自己直交基底 $\{\alpha,\alpha^2,\alpha^4\}$ による変換

$\mathbb{F}_{2^3}$	0	1	α	α^2	α^3	α^4	α^5	α^6
$\mathbb{F}_2^3$	000	111	100	010	101	001	011	110

$0,\alpha^5,\alpha^3,\alpha^2,\alpha^6,\alpha,\alpha^4$ —二元展開→ 000 011 101 010 100 100 001

↓ 消失

$0,?,\alpha^3,\alpha^2,?,\alpha,\alpha^4$ ← 000 ??1 101 010 ?00 100 001

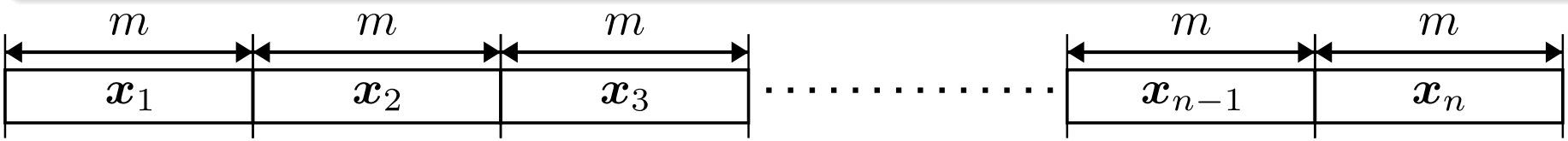
§2. （古典）削除ブロック検出マーカ

仮定 :二元系列に t 個以下の削除が生じる

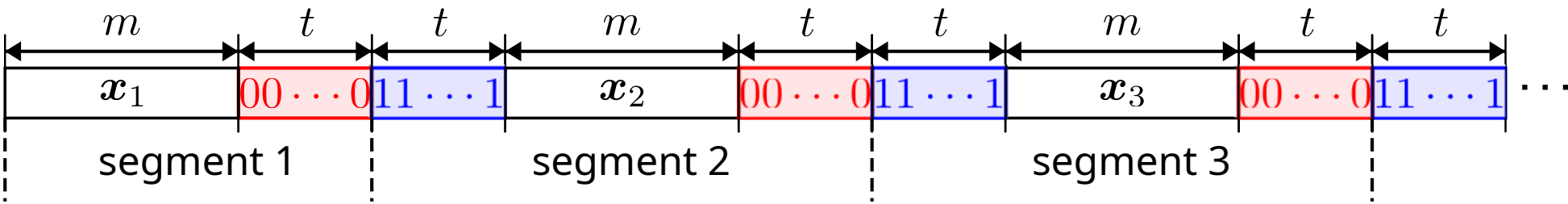
削除ブロック検出マーカ

各ブロックの末尾に以下のマーカを挿入

$$\underbrace{00\cdots0}_{t}\underbrace{11\cdots1}_{t} = \mathbf{0}^{(t)}\mathbf{1}^{(t)}$$



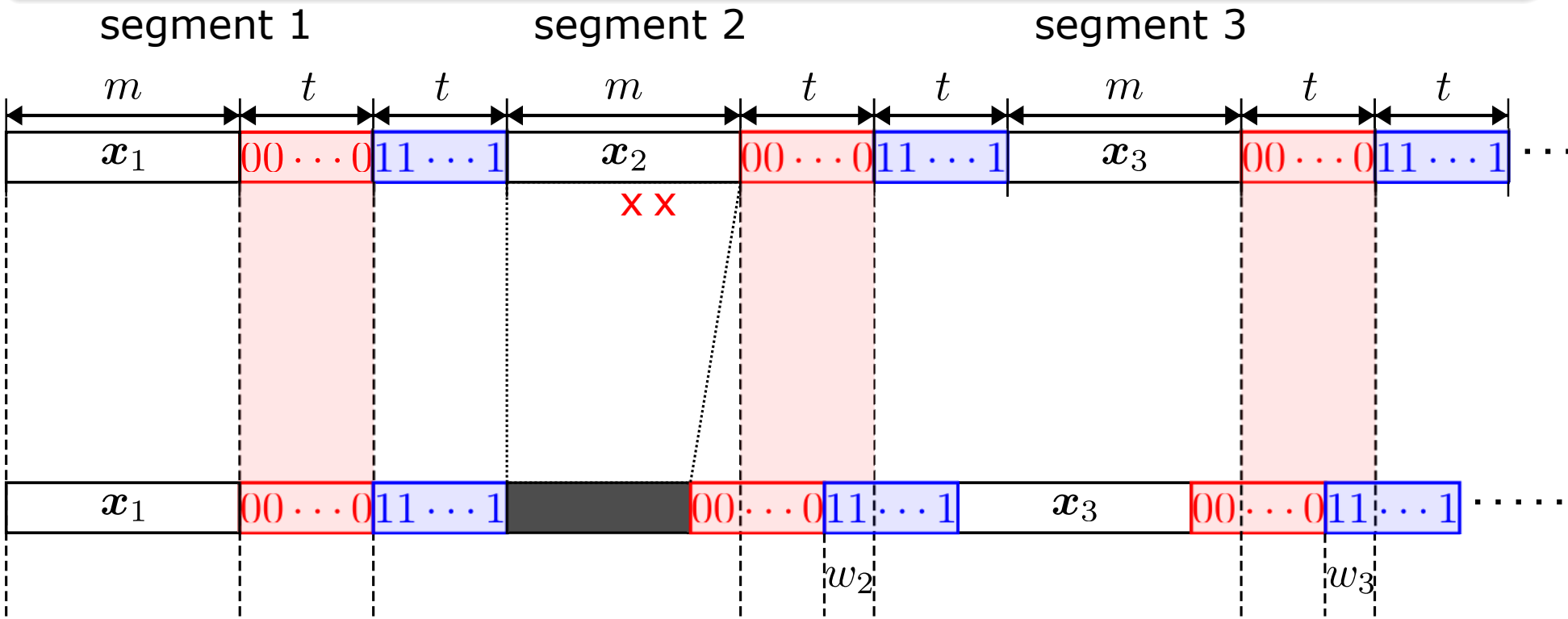
⇓ マーカ挿入



§2. （古典）削除ブロック検出法

$w_i :=$ (第 i セグメントに流入した 1 の個数)
$=$ (第 i セグメントまでに生じた削除数)

$w_{i-1} < w_i \iff$ 第 i セグメントに削除が生じた



§2. （古典）RS 符号による t 削除訂正符号

t 削除訂正符号 C'

C: $\mathbb{F}_{2^m}$ 上の $(n, n-t)$RS 符号を二元展開した符号

$$C' := \{\boldsymbol{x}_1\mathbf{0}^{(t)}\mathbf{1}^{(t)}\boldsymbol{x}_2\mathbf{0}^{(t)}\mathbf{1}^{(t)}\cdots\boldsymbol{x}_n\mathbf{0}^{(t)}\mathbf{1}^{(t)} \mid \boldsymbol{x}_1\boldsymbol{x}_2\cdots\boldsymbol{x}_n \in C\}$$

復号法

1. $w_1, w_2, \ldots w_n$ を計算する
2. $w_{i-1} = w_i$ ならば，$\boldsymbol{x}_i$ を抜き出し，$\boldsymbol{y}_i = \boldsymbol{x}_i$ とする．
   $w_{i-1} < w_i$ ならば，$\boldsymbol{y}_i =?$ とする．
3. $\boldsymbol{y}_1\boldsymbol{y}_2\cdots\boldsymbol{y}_n$ に $\mathcal{B}(C_{\mathrm{RS}})$ の消失訂正法を適用する

§3. 量子符号の準備 (表記)

ケット $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

ブラ $\langle 0| = |0\rangle^\dagger = \begin{pmatrix} 1 & 0 \end{pmatrix}$ $\langle 1| = |1\rangle^\dagger = \begin{pmatrix} 0 & 1 \end{pmatrix}$

$\boldsymbol{x} = x_1 x_2 \cdots x_n \in \mathbb{F}_2^n$ **に対して**

$$|\boldsymbol{x}\rangle = |x_1 x_2 \cdots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \in \mathbb{C}^{2^n}$$
$$\langle \boldsymbol{x}| = \langle x_1 x_2 \cdots x_n| = \langle x_1| \otimes \langle x_2| \otimes \cdots \otimes \langle x_n|$$

クロネッカー積： $\mathbf{A} = (a_{i,j}) \in \mathbb{C}^{n_1 \times m_1}, \mathbf{B} = \mathbb{C}^{n_2 \times m_2}$

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{1,1}\mathbf{B} & \cdots & a_{1,n_1}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m_1,1}\mathbf{B} & \cdots & a_{m_1,n_1}\mathbf{B} \end{pmatrix} \in \mathbb{C}^{n_1 n_2 \times m_1 m_2}$$

§3. 量子符号の準備 (量子ビット)

量子ビット :次数 2 の密度行列

次数 d の密度行列：$\mathbb{C}$ 上の $d \times d$ 行列 ρ

- 対角和が 1：$\mathrm{tr}(\rho) = 1$
- 半正定値：ρ の全ての固有値が 0 以上
- 自己随伴（エルミート行列）：$\rho^\dagger = \rho$

純粋状態

ある $a|0\rangle + b|1\rangle$ $(a, b \in \mathbb{C},\ |a|^2 + |b|^2 = 1)$ によって

$$\rho = (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)^\dagger$$

と表現できるとき，ρ を純粋状態と呼ぶ.
ρ のかわりに $a|0\rangle + b|1\rangle$ と書く.

(c.f.) 混合状態：純粋状態でないもの

§3. 量子符号の準備 (n 個の量子ビットからなる量子系)

次数 2^n の密度行列で表現される

- ρ が混合状態（および純粋状態）のとき

$$\rho = \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n} \rho_{\boldsymbol{x},\boldsymbol{y}} \left|\boldsymbol{x}\right\rangle \left\langle\boldsymbol{y}\right|, \qquad (\rho_{\boldsymbol{x},\boldsymbol{y}} \in \mathbb{C})$$

- ρ が純粋状態のとき

$$\sum_{\boldsymbol{x}\in\mathbb{F}_2^n} a_{\boldsymbol{x}} \left|\boldsymbol{x}\right\rangle$$

§3. 量子符号の準備 (射影測定)

- 測定値は確率的に得られる
- 測定前後で状態が変わる

射影測定：自己随伴行列の集合 $\{\mathbf{P}_0, \mathbf{P}_1, \dots\}$ で規定される

$$\mathbf{P}_i \mathbf{P}_j = \mathbf{P}_i \mathbb{I}[i = j], \qquad \sum_i \mathbf{P}_i = \mathbf{I}$$

もとの状態が ρ の場合，

- 測定値 i を得る確率

$$\mathrm{tr}(\mathbf{P}_i \rho)$$

- 測定後の状態

$$\frac{\mathbf{P}_i \rho \mathbf{P}_i^\dagger}{\mathrm{tr}(\mathbf{P}_i \rho)}$$

§3. 量子符号の準備 (射影測定：例)

元の状態 $a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$

射影測定

$$\mathbf{P}_0 = |0\rangle\langle 0| \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbf{P}_1 = |1\rangle\langle 1| \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

測定値	確率	測定後の状態
0	$\lvert a_{00}\rvert^2 + \lvert a_{01}\rvert^2$	$\dfrac{a_{00}\lvert 00\rangle + a_{01}\lvert 01\rangle}{\lvert a_{00}\rvert^2 + \lvert a_{01}\rvert^2}$
1	$\lvert a_{10}\rvert^2 + \lvert a_{11}\rvert^2$	$\dfrac{a_{10}\lvert 10\rangle + a_{11}\lvert 11\rangle}{\lvert a_{10}\rvert^2 + \lvert a_{11}\rvert^2}$

§4. CSS 符号と量子 RS 符号 (CSS 符号)

CSS 符号 $\mathrm{CSS}(C_1, C_2)$

- 2 つの古典 2 元線形符号 C_1, C_2 から構成される量子符号
  (n, k_1) 線形符号 C_1，(n, k_2) 線形符号 C_2 $(C_2 \subset C_1)$
- $\min\{d_{\min}(C_1), d_{\min}(C_2^{\perp})\} - 1$ 個までの量子消失誤りを訂正可能

類別

$$(\boldsymbol{x}_1, \boldsymbol{x}_2 \in C_1) \quad \boldsymbol{x}_1 \sim \boldsymbol{x}_2 \overset{\text{def}}{\iff} \boldsymbol{x}_1 - \boldsymbol{x}_2 \in C_2$$

$C_1/\sim$ の完全代表系：$\{\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_K\}$ $\quad (K = 2^{k_1 - k_2})$

$$|\boldsymbol{\psi}_i + C_2\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{\boldsymbol{y} \in C_2} |\boldsymbol{\psi}_i + \boldsymbol{y}\rangle$$

CSS 符号

$$\sum_{i=1}^{K} \alpha_i \, |\boldsymbol{\psi}_i + C_2\rangle \qquad (\alpha_i \in \mathbb{C}, \textstyle\sum_{i=1}^{K} |\alpha_i|^2 = 1)$$

§4. CSS 符号と量子 RS 符号 (量子 RS 符号)

量子 RS 符号 $\mathrm{CSS}(\mathcal{B}(C_1), \mathcal{B}(C_2))$

- 2 つの古典 RS 符号から構成される量子符号
  (n, k_1)RS 符号 C_1，(n, k_2)RS 符号 C_2 $(C_2 \subset C_1)$
- 量子消失誤りを含むブロックが $\min\{n - k_1, k_2\}$ 以下ならば復号可能

構成法

1. C_1, C_2 を二元展開して $\mathcal{B}(C_1), \mathcal{B}(C_2)$ にする
2. $\mathcal{B}(C_1), \mathcal{B}(C_2)$ で CSS 符号をつくる

ブロック

符号化で得られた mn 個の量子ビットを，m 個ごとに分けて，n 個のブロックをつくる

§5. 量子 RS 符号に基づく量子削除訂正符号 (削除誤り)

(古典) i 番目のビットへの削除誤り

(誤り前) $$\boldsymbol{x} = x_1 x_2 \dots x_{i-1} \underline{x_i} x_{i+1} \dots x_n$$

(誤り後) $$\boldsymbol{x}_{\neg i} = x_1 x_2 \dots x_{i-1} x_{i+1} \dots x_n$$

(量子) i 番目の量子系への削除誤り

(誤り前) $$\rho = \sum_{\boldsymbol{x},\boldsymbol{y} \in \mathbb{F}_2^n} \rho_{\boldsymbol{x},\boldsymbol{y}} \left|\boldsymbol{x}\right\rangle \left\langle \boldsymbol{y}\right|$$

(誤り後) $$\mathrm{Tr}_i(\rho) = \sum_{\boldsymbol{x},\boldsymbol{y} \in \mathbb{F}_2^n} \rho_{\boldsymbol{x},\boldsymbol{y}} \mathrm{tr}(\left|x_i\right\rangle \left\langle y_i\right|) \left|\boldsymbol{x}_{\neg i}\right\rangle \left\langle \boldsymbol{y}_{\neg i}\right|$$

$$\mathrm{tr}(\left|x\right\rangle \left\langle y\right|) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$$

§5. 量子 RS 符号に基づく量子削除訂正符号 (削除誤り)

$$\rho = \frac{1}{2}\Big(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\Big)$$

$$= \frac{|00\rangle + |11\rangle}{\sqrt{2}}\frac{\langle 00| + \langle 11|}{\sqrt{2}} = \begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix}$$

$$\mathrm{Tr}_2(\rho) = \frac{1}{2}\Big(|0\rangle\langle 0|\,\mathrm{tr}(|0\rangle\langle 0|) + |0\rangle\langle 1|\,\mathrm{tr}(|0\rangle\langle 1|) + |1\rangle\langle 0|\,\mathrm{tr}(|1\rangle\langle 0|) + |1\rangle\langle 1|\,\mathrm{tr}(|1\rangle\langle 1|)\Big)$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

※ 純粋状態も混合状態になる場合がある

§5. 量子 RS 符号に基づく量子削除訂正符号 (符号化)

古典符号の場合 (復習)

C_{RS} : $(n, n-t)$RS 符号

1. 二元展開した RS 符号 $\mathcal{B}(C_{\mathrm{RS}})$ を用いて，符号化

$$\boldsymbol{u} \mapsto \boldsymbol{x}$$

2. 符号語を m ビットごとに区切り，n 個のブロックを作る

$$\boldsymbol{x} \to \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n$$

3. 各ブロックの末尾に $0^{(t)}1^{(t)}$ をつける

$$\boldsymbol{x}_1, 0^{(t)}1^{(t)}, \boldsymbol{x}_2, 0^{(t)}1^{(t)}, \ldots, x_n, 0^{(t)}1^{(t)}$$

§5. 量子 RS 符号に基づく量子削除訂正符号 (符号化)

量子符号の場合

C_1 : $(n, n-t)$RS 符号，C_2 : (n, t) RS 符号 $(C_2 \subseteq C_1)$

1. 量子 RS 符号 $\mathrm{CSS}(\mathcal{B}(C_1), \mathcal{B}(C_2))$ を用いて，符号化

$$\rho \mapsto \sigma$$

2. 量子系を m 個ごとに区切り，n 個のブロックを作る

$$\sigma \to S_1, S_2, \ldots, S_n$$

3. 各ブロックの末尾に $\mathfrak{o}^t\mathfrak{l}^t := |0^{(t)}\rangle\langle 0^{(t)}| \otimes |1^{(t)}\rangle\langle 1^{(t)}|$ をつける

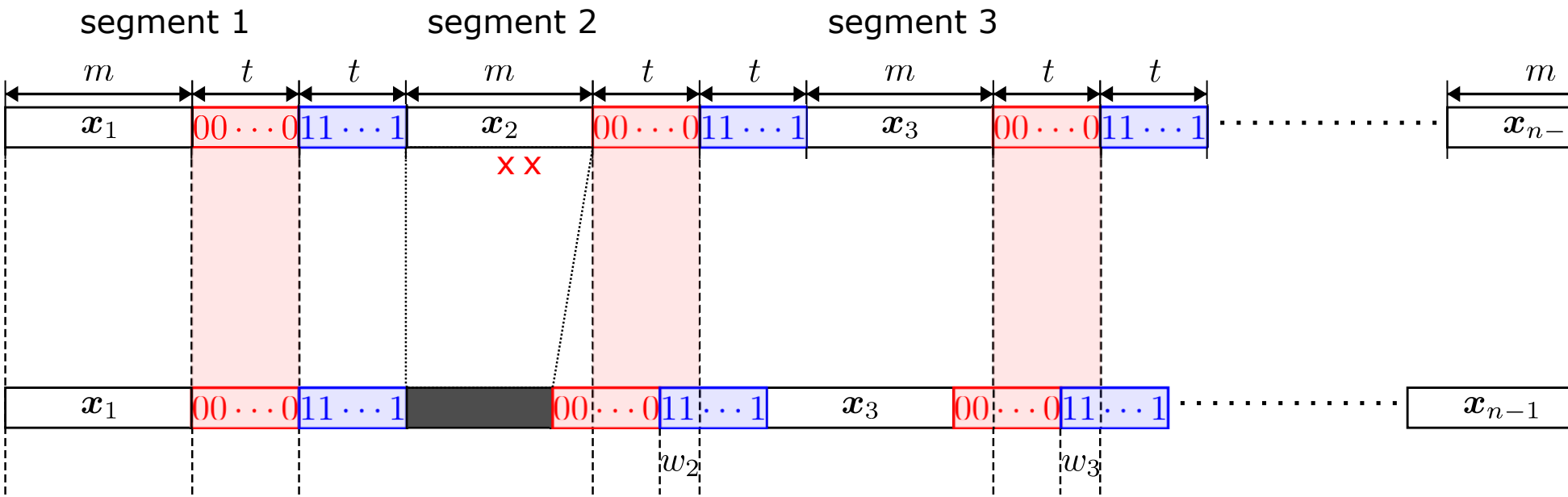
$$S_1, \mathfrak{o}^t\mathfrak{l}^l, S_2, \mathfrak{o}^t\mathfrak{l}^l, \ldots, S_n, \mathfrak{o}^t\mathfrak{l}^l$$

§5. 量子 RS 符号に基づく量子削除訂正符号 (復号)

古典符号の場合 (復習)

$\boldsymbol{z} = z_1 z_2 \dots z_{n'}$: 削除後の系列

1. 元々 $\mathbf{0}^{(t)}$ があった位置に対応する $z_{\alpha_i+1} z_{\alpha_i+2} \dots z_{\alpha_i+t}$ に含まれる 1 の個数を w_i とする $(\alpha_i = i(m+2t) - 2t)$
2. $w_{i-1} = w_i$ ならば，$\boldsymbol{x}_i$ を抜き出し，$\boldsymbol{y}_i = \boldsymbol{x}_i$ とする．
   $w_{i-1} < w_i$ ならば，$\boldsymbol{y}_i = ?$ とする．
3. $\boldsymbol{y}_1 \boldsymbol{y}_2 \cdots \boldsymbol{y}_n$ に $\mathcal{B}(C_{\mathrm{RS}})$ の消失訂正法を適用する



§5. 量子 RS 符号に基づく量子削除訂正符号 (復号)

量子符号の場合

$\tau' = q_1, q_2, \ldots, q_{n'}$: 削除後の量子系

1. 元々 $|\mathbf{0}^{(t)}\rangle\langle\mathbf{0}^{(t)}|$ があった位置に対応する $q_{\alpha_i+1}q_{\alpha_i+2}\cdots q_{\alpha_i+t}$ を
   それぞれ $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ で観測し，
   観測値に含まれる 1 の個数を w_i とする $(\alpha_i = i(m+2t) - 2t)$
2. $w_{i-1} = w_i$ ならば，$\boldsymbol{S}_i$ を抜き出し，$\boldsymbol{B}_i = \boldsymbol{S}_i$ とする．
   $w_{i-1} < w_i$ ならば，$\boldsymbol{B}_i$ を消失シンボルにする．
3. $\boldsymbol{B}_1\boldsymbol{B}_2\cdots\boldsymbol{B}_n$ に $\mathrm{CSS}(\mathcal{B}(C_1), \mathcal{B}(C_2))$ の消失訂正法を適用する

注意

0 を $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ で観測すると確率 1 で 0
1 を $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ で観測すると確率 1 で 1

まとめ

古典符号の知識でほぼ理解できる
「量子 RS 符号に基づく量子削除訂正符号」
を紹介した

補遺

- 「量子 RS 符号に基づく量子削除訂正符号」は挿入誤りも訂正可能
- [MH2022] も古典符号の知識から理解しやすい
- [MH2022] は挿入+削除の復号的な誤りも訂正可能

[MH2022] R. Matsumoto, and M. Hagiwara, Constructions of ℓ-Adic t-Deletion-Correcting Quantum Codes, IEICE Trans. Fundamentals, Vol.E105-A, No.3, pp.571-575, March 2022.