IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2023EAP1168

Publicized:2024/07/30

This advance publication article will be replaced by the finalized version after proofreading.

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

Multiple-Insertion-Correcting Non-Binary Quantum Codes and Decoding Algorithm

Ken NAKAMURA[†a)], ***Nonmember and*** **Takayuki NOZAKI**[†,††b)], ***Senior Member***

SUMMARY This paper investigates non-binary quantum codes correcting multiple insertion errors. This paper provides an insertion-correcting procedure of the deletion-correcting non-binary codes constructed by Matsumoto and Hagiwara. By giving the procedure, we present multiple-insertion-correcting non-binary quantum codes.

key words: *Decoding Algorithm, Insertion Error, Non-Binary Codes, Quantum Codes*

1. Introduction

Insertion and deletion errors have been introduced as a quantum synchronization error model in a quantum communication channel [1]. In classical coding theory, Levenshtein [2] proved that any classical code correcting t deletion errors can also correct s deletion and insertion errors. In other words, any classical code correcting t deletion errors can also correct t insertion errors. Shibayama and Hagiwara [3] showed that any quantum code correcting single deletion error can correct single insertion error under the modified Knill-Laflamme conditions by Shibayama and Ouyang [4]. However, it is an open problem whether t-deletion-correcting quantum codes can correct t insertion errors. Similar to the author of [5], we expect this statement to be true. A study of an insertion-correcting procedure for deletion-correcting quantum codes helps to show it.

Nakayama and Hagiwara [6] provided the first single-deletion-correcting binary quantum code and a decoder. Hagiwara [7] presented the first single-insertion-correcting binary quantum code by showing an insertion-correcting procedure of the single-deletion-correcting code [8]. Moreover, Shibayama and Hagiwara [9] gave multiple-deletion-correcting binary quantum codes. Matsumoto and Hagiwara [10] provided multiple-deletion-correcting non-binary quantum codes. However, multiple-insertion-correcting non-binary quantum codes have not been given yet.

The aim of our study is to provide multiple-insertion-correcting non-binary quantum codes. This paper presents multiple-insertion-correcting non-binary quantum codes by showing an insertion-correcting procedure of the multiple-deletion-correcting non-binary quantum codes [10]. Additionally, to show the insertion-correcting procedure, this paper shows an algorithm to make an index set such that includes the indices of all inserted symbols and its cardinality is at most twice the number of insertions.

The rest of the paper is organized as follows. Section 2 introduces the notations used throughout the paper. Moreover, Section 2 gives error models and deletion-correcting non-binary quantum codes given in [10]. Section 3 provides an algorithm to make an index set that includes the indices of all inserted symbols and its cardinality is at most twice the number of insertions. Section 4 presents a multiple insertion error correcting algorithm of the multiple-deletion-correcting non-binary quantum codes [10]. Section 5 concludes the paper.

2. Preliminary

This section gives the notations used throughout the paper. Moreover, this section introduces error models and deletion-correcting non-binary quantum codes [10]. To introduce the codes, we define a monotonically increasing periodic sequence, which can locate all deletion indices.

2.1 Notations

Let $\mathbb{Z}$, $\mathbb{Z}^+$, and $\mathbb{C}$ be the sets of all integers, positive integers, and complex numbers, respectively. For $a, b \in \mathbb{Z}$, define $[\![a, b]\!] := \{i \in \mathbb{Z} \mid a \leq i \leq b\}$. Moreover, define $[\![b]\!] := [\![0, b]\!]$. In particular, $\mathbb{Z}_l = \{0, 1, ..., l-1\}$ represents the set of l-adic symbols. Let $|P|$ be the cardinality of a set P. For $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, $a\%b$ stands for the remainder when a divided by b.

For $\boldsymbol{x} = (x_i) \in \mathbb{Z}_l^n$ and $P = \{p_1, p_2, ..., p_t\} \subseteq [\![1, n]\!]$ with $p_1 < p_2 < \cdots < p_t$, define $\boldsymbol{x}_P := (x_{p_1}, x_{p_2}, ..., x_{p_t})$. To simplify the notation, we write a vector $\boldsymbol{x} = (x_1, x_2, ..., x_n)$ as a sequence $x_1 x_2 ... x_n$. For example, for $\boldsymbol{x} = 0120 \in \mathbb{Z}_3^4$, we have $\boldsymbol{x}_{[\![1,3]\!]} = 012$ and $\boldsymbol{x}_{\{1,4\}} = 00$.

Let $\mathcal{H}_l$ be the complex vector space of dimension l. For $s \in \mathbb{Z}_l$, let $|s\rangle \in \mathcal{H}_l$ be a column vector whose only the $(s+1)$th component is 1 and the other components are 0, and $\langle\mu|$ the adjoint of a vector $|\mu\rangle \in \mathcal{H}_l$.

Let $\mathrm{tr}(A)$ be the trace of a matrix A. For two matrices $A = (a_{i,j})$ and B, the tensor product $A \otimes B$ is defined as

[†]The authors are with Dept. of Informatics, Division of Fundamental Sciences, Graduate School of Sciences and Technology for Innovation, Yamaguchi University, 1677-1, Yoshida, Yamaguchi-shi, Yamaguchi, 753-8512, JAPAN
[††]The author is with The Research Institute for Time Studies, Yamaguchi University
a) E-mail: d027vbu@yamaguchi-u.ac.jp
b) E-mail: tnozaki@yamaguchi-u.ac.jp

$$A \otimes B := \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1}B & a_{m,2}B & \cdots & a_{m,n}B \end{pmatrix},$$

where A is an $m \times n$ matrix. In particular, $A^{\otimes n}$ denotes $\underbrace{A \otimes A \otimes \cdots \otimes A}_{n \text{ times}}$. For $\boldsymbol{x} = (x_i) \in \mathbb{Z}_l^n$, define $|\boldsymbol{x}\rangle := |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$. The set of all density matrices of quantum states represented by n l-adic qudits is denoted by $S(\mathcal{H}_l^{\otimes n})$. When $\rho \in S(\mathcal{H}_l^{\otimes n})$ is pure, there exists a vector $|\mu\rangle \in \mathcal{H}_l^{\otimes n}$ such that $\rho = |\mu\rangle\langle\mu|$. Then, we denote ρ by $|\mu\rangle$.

2.2 Error Models

For $\boldsymbol{x} = (x_i) \in \mathbb{Z}_l^n$, $t \in \mathbb{Z}^+$, and a set of *deletion indices* $P \subseteq [\![1, n]\!]$ with $|P| = t \leq n$, define t deletion errors $D_P : \mathbb{Z}_l^n \to \mathbb{Z}_l^{(n-t)}$ at P as $D_P(\boldsymbol{x}) = \boldsymbol{x}_{[\![1,n]\!]\setminus P}$. For example, $D_{\{2\}}(0120) = 020$. For $\boldsymbol{x} \in \mathbb{Z}_l^n$, $t \in \mathbb{Z}^+$, and a set of *insertion indices* $P \subset [\![1, n+t]\!]$ with $|P| = t$, define the set of sequences inserting t symbols at position P to $\boldsymbol{x}$ by $B_P(\boldsymbol{x})$, i.e., $B_P(\boldsymbol{x}) := \{\boldsymbol{y} \in \mathbb{Z}_l^{(n+t)} \mid D_P(\boldsymbol{y}) = \boldsymbol{x}\}$. For example, if $l = 3$, $B_{\{4\}}(0120) = \{01200, 01210, 01220\}$. Then, t insertion errors at P is a change from $\boldsymbol{x}$ to $z \in B_P(\boldsymbol{x})$.

In the erasure channel, some transmitted symbols can become the erasure symbol ?. For example, when the transmitted sequence is 012012, the received sequence can become 0?201?. Now, we are able to regard erasures as the errors whose indices are known to the receiver. Hence, we also regard the erasure model as the model where the receiver gets the received sequence $D_P(\boldsymbol{x})$ with deletion errors and knows the indices P of the deletions.

For $\rho = \sum_{\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z}_l^n} c_{\boldsymbol{x},\boldsymbol{y}} |\boldsymbol{x}\rangle\langle\boldsymbol{y}| \in S(\mathcal{H}_l^{\otimes n})$ and $p \in [\![1, n]\!]$, the *partial trace* $\mathrm{Tr}_p : S(\mathcal{H}_l^{\otimes n}) \to S\left(\mathcal{H}_l^{\otimes(n-1)}\right)$ is defined as

$$\mathrm{Tr}_p(\rho) = \sum_{\substack{\boldsymbol{x}=(x_i)\in\mathbb{Z}_l^n \\ \boldsymbol{y}=(y_i)\in\mathbb{Z}_l^n}} c_{\boldsymbol{x},\boldsymbol{y}} \mathrm{tr}(|x_p\rangle\langle y_p|) \left|D_{\{p\}}(\boldsymbol{x})\right\rangle \left\langle D_{\{p\}}(\boldsymbol{y})\right|.$$

Then, for $\rho \in S(\mathcal{H}_l^{\otimes n})$ and a set of deletion indices $P = \{p_1, p_2, ..., p_t\} \subseteq [\![1, n]\!]$ with $p_1 < p_2 < \cdots < p_t$, define t deletion errors $\mathcal{D}_P : S(\mathcal{H}_l^{\otimes n}) \to S\left(\mathcal{H}_l^{\otimes(n-t)}\right)$ at P as

$$\mathcal{D}_P(\rho) = \mathrm{Tr}_{p_1} \circ \mathrm{Tr}_{p_2} \circ \cdots \circ \mathrm{Tr}_{p_t}(\rho),$$

where $f \circ g$ is the composition of the maps f and g. In a similar way to $B_P(\boldsymbol{x})$, for $\rho \in S(\mathcal{H}_l^{\otimes n})$, $t \in \mathbb{Z}^+$, and $P \subset [\![1, n+t]\!]$ with $|P| = t$, define

$$\mathcal{B}_P(\rho) := \left\{\sigma \in S\left(\mathcal{H}_l^{\otimes(n+t)}\right) \mid \mathcal{D}_P(\sigma) = \rho\right\}.$$

Then, t insertion errors at P is a change from ρ to $\rho' \in \mathcal{B}_P(\rho)$. If ρ is pure, $\rho' \in \mathcal{B}_P(\rho)$ is denoted by the following.

Theorem 1 (Fact 2.6 of [11]): Consider a quantum state $\rho = \sum_{\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z}_l^n} c_{\boldsymbol{x},\boldsymbol{y}} |\boldsymbol{x}\rangle\langle\boldsymbol{y}| \in S(\mathcal{H}_l^{\otimes n})$ and a permutation τ on $[\![1, n]\!]$. By abuse of notation, we define the *index permutation* $\tau(\rho) \in S(\mathcal{H}_l^{\otimes n})$ for ρ by

$$\tau(\rho) := \sum_{\substack{\boldsymbol{x}=(x_i)\in\mathbb{Z}_l^n \\ \boldsymbol{y}=(y_i)\in\mathbb{Z}_l^n}} c_{\boldsymbol{x},\boldsymbol{y}} \left|x_{\tau(1)} \cdots x_{\tau(n)}\right\rangle \left\langle y_{\tau(1)} \cdots y_{\tau(n)}\right|.$$

In addition, for $t, n \in \mathbb{Z}^+$ and $P = \{p_1, p_2, ..., p_t\} \subset [\![1, n+t]\!]$ with $p_1 < p_2 < \cdots < p_t$, let τ_P be the permutation on $[\![1, n+t]\!]$ such that $\tau_P(i) = p_i$ for $i \in [\![1, t]\!]$ and $j < k \Rightarrow \tau_P(j) < \tau_P(k)$ for $j, k \in [\![t+1, n+t]\!]$. Then, if $\rho \in S(\mathcal{H}_l^{\otimes n})$ is pure, any quantum state $\rho' \in \mathcal{B}_P(\rho)$ is denoted by $\rho' = \tau_P(\sigma \otimes \rho)$ for some $\sigma \in S(\mathcal{H}_l^{\otimes t})$.

Similar to the classical erasure model, s quantum erasures on P is regarded to as an error model where the receiver gets $\mathcal{D}_P(\rho)$ and knows P.

2.3 Monotonically Increasing Periodic Sequence [10]

The sequence repeating the symbols from 0 to t such as $012\cdots t012\cdots t01\cdots$ is denoted by $\boldsymbol{m} \in \mathbb{Z}_{(t+1)}^n$. More precisely, $\boldsymbol{m} = (m_i)$ satisfies $m_i = (i-1)\%(t+1)$. We call $\boldsymbol{m}$ the *monotonically increasing periodic sequence* on $\mathbb{Z}_{(t+1)}^n$. For example, if $t = 2$ and $n = 7$, $\boldsymbol{m} = 0120120$.

The sequence $\boldsymbol{m} \in \mathbb{Z}_{(t+1)}^n$ can locate t deletion indices as the following procedure [10]. For at most t deletion errors D_P, define $\boldsymbol{y} = (y_i) := D_P(\boldsymbol{m})$. Let $k = \min\{j \mid y_j \geq y_{j+1}\}$. The set $\mathbb{Z}_{(t+1)} \setminus \{y_1, ..., y_k\}$ is the set of all the deleted symbols on $\boldsymbol{m}_{[\![1,t+1]\!]}$. Hence, from $\mathbb{Z}_{(t+1)} \setminus \{y_1, ..., y_k\}$, we get all the deletion indices on $[\![1, t+1]\!]$. Repeat the procedure above from y_{k+1} until the rightmost component in $\boldsymbol{y}$ and we get all the deletion indices.

2.4 Deletion-Correcting Non-binary Quantum Codes [10]

This section introduces deletion-correcting non-binary quantum codes Q' given in [10]. Let $Q \subset \mathcal{H}_l^{\otimes n}$ be a t erasure-correcting quantum code. Define the map $\eta_i : \mathcal{H}_l \to \mathcal{H}_{l(t+1)}$ by $\eta_i : |j\rangle \mapsto |j(t+1)+i\rangle$. Conversion from $|\phi\rangle \in Q$ to $|\psi\rangle \in Q' \subset \mathcal{H}_{l(t+1)}^{\otimes n}$ is defined as apply $\eta_{(i-1)\%(t+1)}$ to the ith physical system of $|\phi\rangle$ for all $i \in [\![1, n]\!]$.

In general, if a message is pure (resp. mixed), the corresponding codeword is also pure (resp. mixed). In this paper, suppose that both messages and codewords are pure.

Example 1: The *Shor code* $Q_S \subset \mathcal{H}_2^{\otimes 9}$ [12] is a 2-erasure-correcting quantum code. This example gives a 2-deletion-correcting quantum code $Q'_S \subset \mathcal{H}_6^{\otimes 9}$ based on the Shor code. By the Shor code, a message $|\mu\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{H}_2^{\otimes 1}$ is encoded to

$$|\phi\rangle = \alpha\left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)^{\otimes 3} + \beta\left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)^{\otimes 3} \in Q_S,$$

where $\alpha, \beta \in \mathbb{C}$. By applying $\eta_{(i-1)\%3}$ to the ith qudit of $|\phi\rangle$

for all $i \in [\![1,9]\!]$, we get a codeword

$$|\psi\rangle = \alpha\left(\frac{|012\rangle + |345\rangle}{\sqrt{2}}\right)^{\otimes 3} + \beta\left(\frac{|012\rangle - |345\rangle}{\sqrt{2}}\right)^{\otimes 3} \in Q'_S.$$

The following is a t-deletion-correcting procedure [10] of Q'. Let $|\mu\rangle \in \mathcal{H}_{l_0}^{\otimes n_0}$ and $|\psi\rangle \in Q' \subset \mathcal{H}_{l(t+1)}^{\otimes n}$ be the message and its corresponding codeword, respectively. For $n' \in [\![n-t, n-1]\!]$, assume that the receiver receives $\rho = \mathcal{D}_P(|\psi\rangle\langle\psi|) \in S(\mathcal{H}_{l(t+1)}^{\otimes n'})$ and knows the number n' of qudits of ρ without destroying ρ. Perform a projective measurement corresponding to $\{M_0, M_1, ..., M_t\}$ on each qudit in ρ, where

$$M_k := \sum_{j \in [l-1]} |j(t+1)+k\rangle\langle j(t+1)+k| \tag{1}$$

for $k \in \mathbb{Z}_{(t+1)}$. Let ρ' be the quantum state after the measurement and $\boldsymbol{y} = (y_i) \in \mathbb{Z}_{(t+1)}^{n'}$ the sequence such that y_i is the measured outcome of the ith qudit of ρ. Then, for $\boldsymbol{m} \in \mathbb{Z}_{(t+1)}^n$, $\boldsymbol{y} = D_P(\boldsymbol{m})$ and $\rho' = \mathcal{D}_P(|\psi\rangle\langle\psi|)$ hold. Since $|P| = n - n' \leq t$, we locate P by the locating procedure in Section 2.3. Hence, since $\mathcal{D}_P$ can be regarded to as at most t erasures, we get $|\mu\rangle$ by applying a t-erasure-correcting procedure of Q.

3. Algorithm for Finding a Set Containing Insertion Indices

Now, we will consider an insertion locating procedure for $\boldsymbol{m} \in \mathbb{Z}_{(t+1)}^n$. However, it is difficult to locate insertion indices P from a sequence $\boldsymbol{z} \in B_P(\boldsymbol{m})$, because we cannot uniquely detect the insertion indices. For example, if $\boldsymbol{m} = 012$ and $\boldsymbol{z} = 0012$, since $0012 \in B_{\{1\}}(012) \cap B_{\{2\}}(012)$, we cannot choose $P = \{1\}$ or $P = \{2\}$. Hence, we give a procedure that compose a set $\overline{P}$ satisfying

$$P \subseteq \overline{P}, \tag{2}$$

$$|\overline{P}| \leq 2|P|. \tag{3}$$

By $\overline{P}$, we get $\boldsymbol{w} = D_{\overline{P}}(\boldsymbol{z})$. Then, $\boldsymbol{w}$ satisfies $\boldsymbol{w} = D_{P'}(\boldsymbol{m}^{(t)})$, where $|P'| \leq t$. In words, $D_{\overline{P}}$ converts t insertion errors for $\boldsymbol{m}$ to at most t deletion errors for $\boldsymbol{m}$. For example, for $\boldsymbol{m} = 012$ and $\boldsymbol{z} = 0012$, if we can set $\overline{P} = \{1, 2\}$, $D_{\overline{P}}$ changes from 0012 to $12 = D_{\{1\}}(012)$.

3.1 Procedure and Example

The following definition gives notations used in this section.

Definition 1: For $\boldsymbol{x} = (x_i) \in \mathbb{Z}_l^n$, let $J_s(\boldsymbol{x})$ be the set of indices of a symbol $s \in \mathbb{Z}_l$, i.e., $J_s(\boldsymbol{x}) := \{i \in [\![1,n]\!] \mid x_i = s\}$. Then, we define $N(\boldsymbol{x}|s) := |J_s(\boldsymbol{x})|$ and denote the ith smallest element of $J_s(\boldsymbol{x})$ by $J_s(\boldsymbol{x}|i)$. For convergence, we define $J_s(\boldsymbol{x}|0) := 0$ and $J_s(\boldsymbol{x}|N(\boldsymbol{x}|s)+1) := n+1$.

Example 2: Suppose $\boldsymbol{x} = 02120102012 \in \mathbb{Z}_3^{11}$. We get $J_1(\boldsymbol{x}) = \{3, 6, 10\}$ and $N(\boldsymbol{x}|1) = 3$. Moreover, we have

$$J_1(\boldsymbol{x}|0) = 0, \quad J_1(\boldsymbol{x}|1) = 3, \quad J_1(\boldsymbol{x}|2) = 6,$$
$$J_1(\boldsymbol{x}|3) = 10, \quad J_1(\boldsymbol{x}|4) = 12.$$

Then, for $P \subset [\![1, n+t']\!]$ with $|P| = t' \leq t$, the following procedure derives $\overline{P}$ satisfying Eqs. (2) and (3).

Procedure 1:
Input: $\boldsymbol{m} \in \mathbb{Z}_{(t+1)}^n$, $\boldsymbol{z} = (z_i) \in B_P(\boldsymbol{m})$
Output: $\overline{P} \subset [\![1, n+t']\!]$

1. Select a *marker* a satisfying

$$N(\boldsymbol{z}|a) = \left\lceil \frac{n-a}{t+1} \right\rceil, \tag{4}$$

where $\lceil x \rceil$ is the smallest integer greater than or equal to a real number x. Define $e := \lceil (n-a)/(t+1) \rceil$.

2. For $i \in [\![e]\!]$, define

$$S_{\boldsymbol{m}}(i) := [\![J_a(\boldsymbol{m}, i)+1, J_a(\boldsymbol{m}, i+1)-1]\!],$$
$$S_{\boldsymbol{z}}(i) := [\![J_a(\boldsymbol{z}, i)+1, J_a(\boldsymbol{z}, i+1)-1]\!].$$

Then, for $i \in [\![e]\!]$, set

$$T_i = \{s \in \mathbb{Z}_{(t+1)} \mid N(\boldsymbol{m}_{S_{\boldsymbol{m}}(i)}|s) < N(\boldsymbol{z}_{S_{\boldsymbol{z}}(i)}|s)\}.$$

3. Get $\overline{P}$ as follows:

$$\overline{P} = \bigcup_{i \in [e]} \{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\} \tag{5}$$

Example 3: Assume that $\boldsymbol{m} = 012012012 \in \mathbb{Z}_3^9$ and $\boldsymbol{z} = 02120102012 \in B_{\{2,7\}}(\boldsymbol{m})$. Then, $t' = 2$.

1. By the following calculation, select $a = 1$:

$$N(\boldsymbol{z}|0) = 4, \quad N(\boldsymbol{z}|1) = 3, \quad N(\boldsymbol{z}|2) = 4,$$
$$\left\lceil \frac{n-0}{t+1} \right\rceil = 3, \quad \left\lceil \frac{n-1}{t+1} \right\rceil = 3, \quad \left\lceil \frac{n-2}{t+1} \right\rceil = 3.$$

2. Note that $e = 3$. Since

$$S_{\boldsymbol{m}}(0) = [\![1,1]\!], \quad S_{\boldsymbol{z}}(0) = [\![1,2]\!],$$
$$S_{\boldsymbol{m}}(1) = [\![3,4]\!], \quad S_{\boldsymbol{z}}(1) = [\![4,5]\!],$$
$$S_{\boldsymbol{m}}(2) = [\![6,7]\!], \quad S_{\boldsymbol{z}}(2) = [\![7,9]\!],$$
$$S_{\boldsymbol{m}}(3) = [\![9,9]\!], \quad S_{\boldsymbol{z}}(3) = [\![11,11]\!],$$

we get

$$\boldsymbol{m}_{S_{\boldsymbol{m}}(0)} = 0, \quad \boldsymbol{z}_{S_{\boldsymbol{z}}(0)} = 02,$$
$$\boldsymbol{m}_{S_{\boldsymbol{m}}(1)} = 20, \quad \boldsymbol{z}_{S_{\boldsymbol{z}}(1)} = 20,$$
$$\boldsymbol{m}_{S_{\boldsymbol{m}}(2)} = 20, \quad \boldsymbol{z}_{S_{\boldsymbol{z}}(2)} = 020,$$
$$\boldsymbol{m}_{S_{\boldsymbol{m}}(3)} = 2, \quad \boldsymbol{z}_{S_{\boldsymbol{z}}(3)} = 2.$$

Hence, we have $T_0 = \{2\}$, $T_1 = \emptyset$, $T_2 = \{0\}$, and $T_3 = \emptyset$.

3. From the above, we get

$$\{j \in S_{\boldsymbol{z}}(0) \mid z_j \in T_0\} = \{2\},$$
$$\{j \in S_{\boldsymbol{z}}(1) \mid z_j \in T_1\} = \emptyset,$$
$$\{j \in S_{\boldsymbol{z}}(2) \mid z_j \in T_2\} = \{7, 9\},$$

$$\{j \in S_{\boldsymbol{z}}(3) \mid z_j \in T_1\} = \emptyset.$$

Hence, get $\overline{P} = \{2\} \cup \emptyset \cup \{7, 9\} \cup \emptyset = \{2, 7, 9\}$.

Recall $P = \{2, 7\}$. Here, $P \subseteq \overline{P}$ and $|\overline{P}| \leq 2|P|$ holds. Hence, $\overline{P}$ satisfies Eqs. (2) and (3).

3.2 Justification

Theorem 2: The set $\overline{P}$ of Procedure 1 satisfies Eqs. (2) and (3).

proof: Define $U := \{z_i \mid i \in P\}$. In words, U is the set of symbols inserted to $\boldsymbol{m}$. We have $t \geq |P| \geq |U|$. Hence, $\mathbb{Z}_{(t+1)} \setminus U \neq \emptyset$ holds. Then, $a \in \mathbb{Z}_{(t+1)} \setminus U$ satisfies $N(\boldsymbol{z}|a) = N(\boldsymbol{m}|a)$. Since $N(\boldsymbol{m}|a) = \lceil (n-a)/(t+1) \rceil$, step 1 finds $a \in \mathbb{Z}_{(t+1)} \setminus U$. For all $j \in P \cap S_{\boldsymbol{z}}(i)$, $N(\boldsymbol{m}_{S_{\boldsymbol{m}}(i)}|z_j) < N(\boldsymbol{z}_{S_{\boldsymbol{z}}(i)}|z_j)$ holds. Hence, $T_i = \{z_j \mid j \in P \cap S_{\boldsymbol{z}}(i)\}$. In words, T_i is the set of symbols inserted to $\boldsymbol{m}_{S_{\boldsymbol{m}}(i)}$. Because $P \cap S_{\boldsymbol{z}}(i) \subseteq \{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\}$ and Eq. (5), we get

$$\bigcup_{i \in [\![e]\!]} (P \cap S_{\boldsymbol{z}}(i)) \subseteq \bigcup_{i \in [\![e]\!]} \{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\} = \overline{P}. \quad (6)$$

Note that $\bigcup_{i \in [\![e]\!]} S_{\boldsymbol{z}}(i) = [\![1, n{+}t']\!] \setminus \{j \in [\![1, n{+}t']\!] \mid z_j = a\}$ and $\{j \in [\![1, n+t']\!] \mid z_j = a\} \cap P = \emptyset$. Hence, we have

$$\bigcup_{i \in [\![e]\!]} (P \cap S_{\boldsymbol{z}}(i)) = P \cap \bigcup_{i \in [\![e]\!]} S_{\boldsymbol{z}}(i) = P. \quad (7)$$

Combining Eqs. (6) and (7), we obtain Eq. (2).

We denote the set of indices of symbols inserted to $\boldsymbol{m}_{S_{\boldsymbol{m}}(i)}$ by R_i, i.e., $\boldsymbol{m}_{S_{\boldsymbol{m}}(i)} = D_{R_i}(\boldsymbol{z}_{S_{\boldsymbol{z}}(i)})$. In addition, since $\boldsymbol{m} = 012...t012...t01...$, the number of a symbol s of $S_{\boldsymbol{m}}(i)$ between ith marker and $(i+1)$th marker is at most 1, i.e., $1 \geq N(\boldsymbol{m}_{S_{\boldsymbol{m}}(i)}|s)$. From the above, we get

$$\begin{aligned} 1 \geq N(\boldsymbol{m}_{S_{\boldsymbol{m}}(i)}|s) &= N(D_{R_i}(\boldsymbol{z}_{S_{\boldsymbol{z}}(i)})|s) = N(\boldsymbol{z}_{S_{\boldsymbol{z}}(i) \setminus R_i}|s) \\ &= |\{j \in S_{\boldsymbol{z}}(i) \setminus R_i \mid z_j = s\}| \end{aligned}$$

for any $s \in \mathbb{Z}_{(t+1)}$. Hence,

$$\begin{aligned} |T_i| = \sum_{s \in T_i} 1 &\geq \sum_{s \in T_i} |\{j \in S_{\boldsymbol{z}}(i) \setminus R_i \mid z_j = s\}| \\ &= \left| \bigcup_{s \in T_i} \{j \in S_{\boldsymbol{z}}(i) \setminus R_i \mid z_j = s\} \right| \\ &= \left| \{j \in S_{\boldsymbol{z}}(i) \setminus R_i \mid z_j \in T_i\} \right| \\ &= |\{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\} \setminus R_i| \quad (8) \end{aligned}$$

From the definition of T_i and R_i, $|R_i| \leq |T_i|$ holds. Hence, Eq. (8) yields

$$\begin{aligned} 2|R_i| \geq |R_i| + |T_i| &\geq |R_i| + |\{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\} \setminus R_i| \\ &= |\{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\} \cup R_i| \\ &\geq |\{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\}| \end{aligned}$$

for any $i \in [\![e]\!]$. The family $\{S_{\boldsymbol{z}}(i)\}_{i \in [\![e]\!]}$ is pairwise disjoint, i.e., $S_{\boldsymbol{z}}(i_1) \cap S_{\boldsymbol{z}}(i_2) = \emptyset$ for distinct $i_1, i_2 \in [\![e]\!]$. Moreover, since $R_i \subseteq S_{\boldsymbol{z}}(i)$, $\{R_i\}_{i \in [\![e]\!]}$ is also pairwise disjoint. Similarly, since $\{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\} \subseteq S_{\boldsymbol{z}}(i)$, $\{\{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\}\}_{i \in [\![e]\!]}$ is also pairwise disjoint. Recall that R_i is the set of the indices of symbols inserted to $\boldsymbol{m}_{S_{\boldsymbol{m}}(i)}$, i.e., $\bigcup_{i \in [\![e]\!]} R_i = P$. Therefore, we obtain

$$\begin{aligned} |\overline{P}| &= \left| \bigcup_{i \in [\![e]\!]} \{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\} \right| \\ &= \sum_{i \in [\![e]\!]} |\{j \in S_{\boldsymbol{z}}(i) \mid z_j \in T_i\}| \\ &\leq \sum_{i \in [\![e]\!]} 2|R_i| = 2\left| \bigcup_{i \in [\![e]\!]} R_i \right| = 2|P|. \end{aligned}$$

Thus, we get Eq. (3). □

4. Insertion-Correcting Procedure

This section provides t-insertion-correcting procedure (Procedure 2) of the t-deletion-correcting quantum code Q' [10]. This implies that Q' is a t-insertion-correcting quantum code. Moreover, this section gives an example and justification.

4.1 Procedure and Example

For a pure codeword $|\psi\rangle \in Q' \subset \mathcal{H}_{l(t+1)}^{\otimes n}$ and $P \subset [\![1, n+t']\!]$ with $|P| = t' \leq t$, suppose that the receiver receives $\rho \in \mathcal{B}_P(|\psi\rangle\langle\psi|)$ and knows the number t' of insertions without destroying ρ. Let M_k be the matrix given by Eq. (1), i.e., $M_k = \sum_{j \in [\![l-1]\!]} |j(t+1)+k\rangle\langle j(t+1)+k|$ for $k \in \mathbb{Z}_{(t+1)}$. Let $|\mu\rangle \in \mathcal{H}_{l_0}^{\otimes n_0}$ be the message that becomes $|\psi\rangle \in Q'$ by encoding.

Procedure 2:
Input: $\rho \in \mathcal{B}_P(|\psi\rangle\langle\psi|)$
Output: message $|\mu\rangle \in \mathcal{H}_{l_0}^{\otimes n_0}$

1. Perform a projective measurement corresponding to $\{M_0, M_1, ..., M_t\}$ on each qudit in ρ. Let ρ' be the quantum state after the measurement, and $\boldsymbol{z} = (z_i) \in \mathbb{Z}_{(t+1)}^{(n+t')}$ the sequence such that z_i is the measured outcome of the ith qudit of ρ.
2. Get $\overline{P}$ from $\boldsymbol{z}$ by Procedure 1.
3. Make $\mathcal{D}_{\overline{P}}(\rho')$.
4. By applying the t-deletion-correcting procedure (Sect. 2.4) of Q' to $\mathcal{D}_{\overline{P}}(\rho')$, output $|\mu\rangle$.

Example 4: Let Q'_S be a 2-quantum deletion-correcting quantum code based on the Shor code in Example 1. Assume that $\rho \in \mathcal{B}_{\{2,7\}}(|\psi\rangle\langle\psi|)$ for $|\psi\rangle \in Q'_S$.

1. Perform a projective measurement corresponding to $\{P_0, P_1, P_2\}$ on each qudit in ρ, where

$$P_0 = |0\rangle\langle 0| + |3\rangle\langle 3|, \quad P_1 = |1\rangle\langle 1| + |4\rangle\langle 4|,$$
$$P_2 = |2\rangle\langle 2| + |5\rangle\langle 5|.$$

Then, we have $\boldsymbol{z} = 0z_2 1201 z_7 2012$. The symbols z_2 and

z_7 are the outcomes of inserted qudits. In this example, assume that $z = 02120102012$.
2. Get $\overline{P} = \{2, 7, 9\}$ by Procedure 1 (See Example 3).
3. We make $\mathcal{D}_{\{2,7,9\}}(\rho')$.
4. From Lemma 1, which is given in the next section, $\rho' \in \mathcal{B}_{\{2,7\}}(|\psi\rangle\langle\psi|)$ holds. Hence, since $\mathcal{D}_{\{2,7,9\}}(\rho') = \mathcal{D}_{\{7\}}(|\psi\rangle\langle\psi|)$, we can get the message by applying a 2-deletion-correcting procedure of Q'_S to $\mathcal{D}_{\{2,7,9\}}(\rho')$.

4.2 Justification

This section proves that we can get the message by applying Procedure 2 to the received quantum state. To show it, we give the following lemma.

Lemma 1: Consider z and ρ' in Step 1 of Procedure 2. Then, for $\boldsymbol{m} \in \mathbb{Z}^n_{(t+1)}$, $P \subset [\![1, n+t']\!]$ with $|P| = t'$, and $|\psi\rangle \in Q'$, $z \in B_P(\boldsymbol{m})$ and $\rho' \in \mathcal{B}_P(|\psi\rangle\langle\psi|)$ hold.

proof: Define $A_k := \{j(t+1)+k \mid j \in [\![l-1]\!]\}$ for $k \in \mathbb{Z}_{(t+1)}$. In addition, from Eq. (1), we get $M_k = \sum_{h\in A_k} |h\rangle\langle h|$. Recall since $|\psi\rangle$ is pure, ρ is represented by $\tau_P(\sigma \otimes |\psi\rangle\langle\psi|)$ with $\sigma \in S\big(\mathcal{H}^{\otimes t'}_{l(t+1)}\big)$ from Theorem 1. We denote

$$|\psi\rangle\langle\psi| = \sum_{\boldsymbol{x},\boldsymbol{y}\in\mathbb{Z}^n_{l(t+1)}} c_{\boldsymbol{x},\boldsymbol{y}} |\boldsymbol{x}\rangle\langle\boldsymbol{y}| \in Q'.$$

Then, from the construction (Sect. 2.4) of Q', if $c_{\boldsymbol{x},\boldsymbol{y}} \neq 0$, $\boldsymbol{x} = (x_i), \boldsymbol{y} = (y_i) \in \mathbb{Z}^n_{l(t+1)}$ satisfy $x_i, y_i \in A_{(i-1)\%(t+1)}$ for all $i \in [\![1, n]\!]$. From the above, the outcome of the projective measurement on the ith qudit in $|\psi\rangle\langle\psi|$ is $(i-1)\%(t+1)$ with probability 1, and the quantum state does not change by the measurement. Assume that $\sigma \in S\big(\mathcal{H}^{\otimes t'}_{l(t+1)}\big)$ is represented by

$$\sum_{\substack{\boldsymbol{x}=(x_i)\in\mathbb{Z}^{t'}_{l(t+1)}\\ \boldsymbol{y}=(y_i)\in\mathbb{Z}^{t'}_{l(t+1)}}} c'_{\boldsymbol{x},\boldsymbol{y}} |\boldsymbol{x}\rangle\langle\boldsymbol{y}|.$$

Then, the outcome of the projective measurement on the ith qudit in σ is $z \in \mathbb{Z}_{(t+1)}$ with probability $\sum_{\boldsymbol{x}\in\mathbb{Z}^n_{l(t+1)}: x_i\in A_z} c_{\boldsymbol{x},\boldsymbol{x}}$, and the quantum state changes to another quantum state by the measurement. From the above, the outcomes of the inserted qudits are one of $\mathbb{Z}_{(t+1)}$, and the outcomes of the other qudits are repeated from 0 to t in order, such as $01\cdots t01\cdots t0\cdots$. Hence, for $\boldsymbol{m} \in \mathbb{Z}^n_{(t+1)}$, $\boldsymbol{m} = D_P(z)$ holds. Similarly, $|\psi\rangle\langle\psi| = \mathcal{D}_P(\rho')$ holds. Therefore, z and ρ' satisfy $z \in B_P(\boldsymbol{m})$ and $\rho' \in \mathcal{B}_P(|\psi\rangle\langle\psi|)$. □

Theorem 3: For a message $|\mu\rangle$ and its corresponding codeword $|\psi\rangle \in Q' \subset \mathcal{H}^{\otimes n}_{l(t+1)}$, the quantum state obtained by applying Procedure 2 to $\rho \in \mathcal{B}_P(|\psi\rangle\langle\psi|)$ is $|\mu\rangle$ if $|P| \leq t$.

proof: The sequence z and the quantum state ρ' given in Step 1 satisfy $z \in B_P(\boldsymbol{m})$ and $\rho' \in \mathcal{B}_P(|\psi\rangle\langle\psi|)$ from Lemma 1. Since the set $\overline{P}$ given in Step 2 satisfies Eqs. (2) and (3), there exists the set $P' \subset [\![1, n]\!]$ such that $\mathcal{D}_{\overline{P}}(\rho') = \mathcal{D}_{P'}(|\psi\rangle\langle\psi|)$ and $|P'| = \big|\overline{P}\setminus P\big|$. Hence, in Step 3, ρ' changes to $\mathcal{D}_{\overline{P}}(\rho') = \mathcal{D}_{P'}(|\psi\rangle\langle\psi|)$. Since $|P'| = \big|\overline{P} \setminus P\big| \leq t$, we have $|\mu\rangle$ by applying the t-deletion-correcting procedure of Q' to $\mathcal{D}_{P'}(|\psi\rangle\langle\psi|)$, i.e., in step 4, we get $|\mu\rangle$. Therefore, we obtain $|\mu\rangle$ by applying Procedure 2 to $\rho \in \mathcal{B}_P(|\psi\rangle\langle\psi|)$. □

Theorem 3 states that Procedure 2 is a t-insetion-correcting procedure of Q'.

5. Conclusions

This paper provided an insertion-correcting procedure of the codes constructed by Matsumoto and Hagiwara. By giving the procedure, we presented multiple-insertion-correcting non-binary quantum codes.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number 22K11905. The author also would like to thank the anonymous reviewers for their careful reading and their insightful comments and suggestions.

References

[1] J. Leahy, D. Touchette, and P. Yao, "Quantum insertion-deletion channels," arXiv preprint arXiv:1901.00984, 2019.
[2] V. Levenshtein, "Binary codes capable of correcting deletions, insertions, and reversals," Soviet physics doklady, vol.10, no.8, pp.707–710, 1966.
[3] T. Shibayama and M. Hagiwara, "Equivalence of quantum single insertion and single deletion error-correctabilities, and construction of codes and decoders," 2022 IEEE International Symposium on Information Theory (ISIT), pp.2957–2962, 2022.
[4] T. Shibayama and Y. Ouyang, "The equivalence between correctability of deletions and insertions of separable states in quantum codes," 2021 IEEE Information Theory Workshop (ITW), pp.1–6, IEEE, 2021.
[5] M. Hagiwara, "Introduction to quantum error-correcting codes from the shortest length examples," preprint.
[6] A. Nakayama and M. Hagiwara, "The first quantum error-correcting code for single deletion errors," IEICE Communications Express, vol.9, no.4, pp.100–104, 2020.
[7] M. Hagiwara, "The four qubits deletion code is the first quantum insertion code," IEICE Communications Express, vol.10, no.5, pp.243–247, 2021.
[8] M. Hagiwara and A. Nakayama, "A four-qubits code that is a quantum deletion error-correcting code with the optimal length," 2020 IEEE International Symposium on Information Theory (ISIT), pp.1870–1874, IEEE, 2020.
[9] T. Shibayama and M. Hagiwara, "Permutation-invariant quantum codes for deletion errors," 2021 IEEE International Symposium on Information Theory (ISIT), pp.1493–1498, IEEE, 2021.
[10] R. Matsumoto and M. Hagiwara, "Constructions of l-adic t-deletion-correcting quantum codes," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.105, no.3, pp.571–575, 2022.
[11] T. Shibayama, Construction conditions of quantum error-correcting codes for various types of insertion/deletion errors, Ph.D. thesis, Chiba University, 2022.
[12] P.W. Shor, "Scheme for reducing decoherence in quantum computer memory," Physical review A, vol.52, no.4, pp.R2493–R2496, 1995.

Ken NAKAMURA received B.S. degree from Yamaguchi University in 2023. Since April 2023, he has been currently pursuing the M.S. degree in Department of Informatics, Yamaguchi University. His research interests is insertion/deletion correcting quantum codes.

Takayuki Nozaki received B.E., M.E., and D.E. degrees from Tokyo Institute of Technology in 2008, 2010, and 2012, respectively. He is currently an associate professor at Yamaguchi University. His research interests include error correcting codes and coding theory. He received the Best Paper Award from the IEICE of Japan in 2018. He is a member of IEEE, ACM, AMS, and IPSJ.