IEICE TRANS. FUNDAMENTALS, VOL.E104–A, NO.12 DECEMBER 2021

INVITED SURVEY PAPER

A Survey of Quantum Error Correction

Ryutaroh MATSUMOTO †,††a), *Senior Member and* **Manabu HAGIWARA**†††, *Member*

SUMMARY This paper surveys development of quantum error correction. With the familiarity with conventional coding theory and tensor product in multi-linear algebra, this paper can be read in a self-contained manner.

key words: *error correction, quantum information*

1. Introduction

Recently, quantum computation has attracted renewed attention, as several larger scale quantum computers have been reported, e.g. [1]. Fault-tolerant quantum computation (FTQC) [2] is considered indispensable with realization of large-scale quantum computers. FTQC performs computation on codewords in a quantum error-correcting code (QECC) without decoding them to their original information.

The quantum error correction can be divided into two major categories, one is transmission of classical information (sequence of bits) and the other is that of quantum information. FTQC relies on the latter, as memory of a quantum computer consists of quantum information. This review also focuses on the latter. We assume that the readers are familiar with the theory of conventional error correction and elementary algebra. In particular, knowledge on the tensor products is assumed. With that familiarity, this can be read in a self-contained manner. Although a minimum review of quantum information is included in this survey, we can still recommend [3] as a good introductory textbook on quantum information.

The conventional error-correcting code corrects errors on classical information by adding redundancy to the original. Such addition of redundancy was thought to be impossible by the quantum no-cloning theorem [4], neither does the quantum error correction. However, Shor disproved that naive belief by explicitly providing an example of QECC [5], which sparked much research attention on QECC, and many constructions of QECC were proposed at that time. Among them, the important classes of QECC are so-called Calderbank-Shor-Steane (CSS) code [6], [7] and the stabilizer code [8]–[10]. CSS code is a special case of the stabilizer code. This review focuses mainly on the stabilizer code. An important contribution in [8], [9] is translation between QECC and linear spaces over finite fields, which enables use of research results in the conventional ECC. Those results were later extended to nonbinary QECC [11]–[13].

Quantum teleportation reproduce the quantum information possessed by a sender at receiver's place, just by transmission of classical information, while the original quantum information at the sender's place is destroyed when the teleportation succeeds [14]. The trick enabling the quantum teleportation is sharing of so-called quantum entanglement between the sender and the receiver. Quantum teleportation can be interpreted as transmission of quantum information at the cost of shared quantum entanglement. Actually, later it was shown that shared quantum entanglement can be converted to transmission of quantum information [15]. Along this line, the entanglement-assisted quantum error-correcting code (EAQECC) was proposed [16], [17], which enable transmission of more quantum information at the cost of shared quantum entanglement. We will review the connections between EAQECCs and linear spaces over finite fields along the line in [18].

Sparse representations have influenced a wide range of academic fields, including signal processing [19], astronomy [20], mathematics [21], brain science [22], etc. Of course, quantum error-correcting codes are also being influenced to be no exception. Sparsity has been introduced in coding theory since the 1960s and is known as low-density [23]. It was in 1999 that low-density (sparsity) was introduced to quantum error-correcting codes [24].

Quantum error-correcting codes also appear in cryptography. They were used as a tool to prove the security of quantum key distribution (QKD) [25]. It was also used as an instance of quantum secret sharing protocol [26], [27]. As the number of variations of quantum error-correcting codes increases and the number of correctable error models increases, we can expect new applications, including cryptography, to expand.

This paper is organized as follows: Section 2 introduces necessary notations and concepts. Section 3 introduces a general framework of quantum error correction not limited the stabilizer codes. Section 4 introduces the stabilizer codes. Section 5 reveals the connection between the stabilizer and linear spaces over finite fields. Section 6 covers entangle-

Manuscript received February 17, 2021.
Manuscript revised May 20, 2021.
Manuscript publicized June 18, 2021.

†The author is with Department of Information and Communications Engineering, Tokyo Institute of Technology, Tokyo, 152-8550 Japan.
††The author is with Department of Mathematical Sciences, Aalborg University, Aalborg, Denmark.
†††The author is with Department of Mathematics and Informatics, Graduate School of Science, Chiba University, Chiba-shi, 263-0022 Japan.
a) E-mail: ryutaroh@ict.e.titech.ac.jp

DOI: 10.1587/transfun.2021EAI0001

ment assistance and asymmetric quantum errors. Section 7 provides further connections between quantum error correction and conventional error correction. Section 8 is devoted to quantum low-density parity check (LDPC) codes that are codes constructed from a view point of sparsity. Section 9 introduces quantum deletion errors, a related open problem and a conjecture.

2. Preliminaries

2.1 Quantum States

By a **quantum system**, we mean some physical object on which we can make (at least theoretically) a measurement. In quantum physics, a Hilbert space $\mathcal{H}$ is associated with a quantum system. In this paper we always assume $\dim \mathcal{H} < \infty$, which implies that $\mathcal{H}$ is isometric to the $(\dim \mathcal{H})$-dimentional complex linear space. We identify $\mathcal{H}$ with the underlying quantum system. A state of $\mathcal{H}$ is expressed by a density matrix ρ on $\mathcal{H}$, where ρ is a complex Hermitian matrix with nonnegative eigenvalues and $\mathrm{tr}\rho = 1$. We denote the set of density matrices on $\mathcal{H}$ by $\mathcal{S}(\mathcal{H})$. A state $\rho \in \mathcal{S}(\mathcal{H})$ is called of level ℓ if $\dim \mathcal{H} = \ell$. In particular, the state is called a qubit if it is of level 2. When $\mathrm{rank}\rho = 1$, the state ρ has a vectorial expression $\rho = |\varphi\rangle\langle\varphi|$, where $|\varphi\rangle$ is a complex column vector of length one in $\mathcal{H}$. and $\langle\varphi|$ its complex conjugate (row vector). $|\varphi\rangle$ is called ket-phi and a unique way of expressing a column vector. $\langle\varphi|$ is bra-phi. A quantum state that can be expressed by a vector $|\varphi\rangle$ is called a pure state, otherwise it is called a mixed state. In this paper, we mostly use the pure state.

2.2 Evolution of Quantum States

A quantum system $\mathcal{H}$'s evolution without measurements or interactions with its surrounding environment is expressed by a unitary matrix U on $\mathcal{H}$. A mixed state ρ evolves to $U\rho U^*$ by U, where U^* denotes the conjugate transpose of U. A pure state $|\varphi\rangle$ evolves to $U|\varphi\rangle$ by U. In this survey, a unitary matrix U often corresponds to decoding operation or an error caused by a quantum communication channel.

2.3 Projective Measurement

In this paper, we focus on a special kind of quantum measurement, which can be expressed as an orthogonal decomposition of $\mathcal{H}$, or a Hermitian matrix A on $\mathcal{H}$. We call A observable on $\mathcal{H}$. Let λ_i be an eigenvalue of A with multiplicity, and P_i the projection onto the eigenspace belonging to λ_i. Note that $\mathrm{rank}P_i$ = the multiplicity of λ_i. The spectral decomposition A is given by

$$A = \sum_i \lambda_i P_i.$$

When a quantum measurement is expressed by A, each outcome is mapped to λ_i (or i). When a state if $|\varphi\rangle$ before measuring A, the probability of getting a measurement outcome λ_i is $\|P_i|\varphi\rangle\|^2$, and the state changes to $P_i|\varphi\rangle/\|P_i|\varphi\rangle\|$.

2.4 Composite System Consisting of Multiple Quantum Systems

Suppose that there are m quantum systems $\mathcal{H}_1, \ldots, \mathcal{H}_m$. When the state of $\mathcal{H}_i$ is $|\varphi_i\rangle$ for $i = 1, \ldots, m$, the state of composite system is expressed by the tensor product $|\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_m\rangle$. The Hilbert space corresponding to the composite system is $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m$.

When we apply some manipulations on $\mathcal{H}_i$ expressed by unitary matrices U_i $(i = 1, \ldots, m)$, the manipulation on the composite system is expressed by the tensor product $U_1 \otimes \cdots \otimes U_m$.

When we measure observables A_i on $\mathcal{H}_i$, the observable the composite system is expressed by the tensor product $A_1 \otimes \cdots \otimes A_m$.

A quantum state $|\varphi\rangle$ in $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m$ is said to be **entangled** if $|\varphi\rangle$ cannot be written as $|\varphi_1\rangle \otimes \cdots \otimes |\varphi_m\rangle$ for any $|\varphi_i\rangle \in \mathcal{H}_i$ for $i = 1, \ldots, m$.

2.5 Mathematical Model of a Quantum Communication Channel

When we know that a quantum system is in state $|\varphi_i\rangle$ with a probability p_i $(i = 1, \ldots, m)$, the state is expressed as

$$p_1|\varphi_1\rangle\langle\varphi_1| + \cdots + p_m|\varphi_m\rangle\langle\varphi_m|,$$

which is a density matrix. Outputs from a conventional communication channel is probabilistic and random, and is typically expressed as a probability distribution, and a conventional communication channel is typically modeled by a conditional probability distribution. On the other hand, a density matrix can capture the above kind of probabilistic outputs. Because of that, a quantum communication channel is typically modeled as a mapping Γ from density matrices to density matrices. It is known that Γ corresponds to a quantum communication channel if and only if Γ preserves traces of matrices and is completely positive.

When we have a quantum channel from $\mathcal{H}$ to $\mathcal{K}$ and use it n times, the state change is generally expressed by a mapping from $\mathcal{S}(\mathcal{H}^{\otimes n})$ to $\mathcal{S}(\mathcal{K}^{\otimes n})$. But under some mild assumption (e.g. each channel use interacts with an independent surrounding environment), the mapping has the form $\Gamma^{\otimes} : \mathcal{S}(\mathcal{H}^{\otimes n}) \to \mathcal{S}(\mathcal{K}^{\otimes n})$, where $\Gamma : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{K})$. In such a case the quantum channel is said to be **memoryless**. In the following, we always assume that quantum channels are memoryless.

3. General Quantum Error Correction

3.1 Basic Framework

Information transmission over quantum channels can roughly be divided in two categories: One is transmission

of quantum information, and the other is that of classical information (bits). In this paper we focus on the former. Transmission of quantum information includes that of quantum entanglement and mixed states. But they can be reduced to the problem of transmitting pure states [28]. So we consider transmission of pure states.

Let $\mathcal{H}_\ell$ be a ℓ-dimensional complex linear space with an orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |\ell-1\rangle\}$. We will consider encoding a pure state in $\mathcal{H}_\ell^{\otimes k}$ to a pure state in $\mathcal{H}_\ell^{\otimes n}$. Such a quantum error-correcting code (quantum code) is called an $[[n,k]]_\ell$ code. It corresponds to an $[n,k]_\ell$ code in the conventional coding theory.

3.2 Fidelity

When we transmit digital information, decoded message can be either the same as the original or different. The difference between the decoded message and the original one is considered to be a decoding failure.

On the other hand, if quantum information $|\varphi\rangle$ is sent, and the decoded information $|\psi\rangle$ is close to $|\varphi\rangle$, then the probability distributions of measurement outcomes of $|\varphi\rangle$ and $|\psi\rangle$ are similar. Therefore, it is reasonable to consider the closeness of $|\varphi\rangle$ and $|\psi\rangle$, and to regard decoded $|\psi\rangle$ close to the original $|\varphi\rangle$ as decoding success.

The fidelity between $|\varphi\rangle$ and $|\psi\rangle$ is defined as $\langle\varphi|\psi\rangle$. It takes values between 0 and 1. The fidelity is the probability of recognizing $|\psi\rangle$ as $|\varphi\rangle$ by measuring the observable $|\varphi\rangle\langle\varphi|$, where outcome 1 corresponds to $|\varphi\rangle$.

Recall that probabilistic change of quantum state can be expressed as a mixed state ρ (density matrix). When the decoded state is ρ, its fidelity with the original $|\varphi\rangle$ is defined as $\langle\varphi|\rho|\varphi\rangle$. It is also the probability of recognizing ρ as $|\varphi\rangle$ by measuring the observable $|\varphi\rangle\langle\varphi|$. Clearly, the higher fidelity is better.

3.3 Finite Set of Quantum Errors

Even for a single quantum system $\mathcal{H}_\ell$, there are the infinite number of possible quantum errors, because the number of unitary matrices on $\mathcal{H}_\ell$ is infinite. This is contrasting to the fact that there are only $\ell-1$ additive errors on $\{0, 1, \ldots, \ell-1\}$, which corresponds to $\mathcal{H}_\ell$.

However, if a certain finite set of unitary matrices can be corrected as quantum errors, then the fidelity of quantum error correction over a memoryless quantum channel is ensured to be high [29]. We will not dig into the detail of this discretization of quantum errors. The finite set of unitary matrices to be corrected will be shown in the next section.

4. Stabilizer Formalism

4.1 Codebooks Defined by a Stabilizer

Let ω be a complex number such that $\omega^\ell = 1$ and $\omega^0, \omega^1, \ldots, \omega^{\ell-1}$ are different, e.g. $\exp(2\pi\sqrt{-1}/\ell)$. We define two unitary matrices changing $|i\rangle$ as $X_\ell|i\rangle = |i+1 \bmod \ell\rangle$ and $Z_\omega|i\rangle = \omega^i|i\rangle$ for $i = 0, \ldots, \ell-1$. These matrices X_ℓ and Z_ω are called Pauli matrices. By straightforward computation we can see $X_\ell^\ell = Z_\omega^\ell = I_{\ell\times\ell}$, where $I_{\ell\times\ell}$ denotes the $\ell\times\ell$ identity matrix.

Example 1: Consider $\ell = 2$. Then $\omega = -1$ and

$$X_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z_{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Consider a set E of unitary matrices consisting of $\omega^i X_\ell^{a_1} Z_\omega^{b_1} \otimes \cdots \otimes X_\ell^{a_n} Z_\omega^{b_n}$ for $i, a_j, b_j \in \{0, \ldots, \ell-1\}$ for $j = 1, \ldots, n$. E is a non-commutative finite group with matrix multiplication as its group operation. The non-commutativity of matrices in E will play an important role in the development of quantum error correction. It will be shown as Corollary 3.

Lemma 2:

$$(X_\ell^a Z_\omega^b)(X_\ell^{a'} Z_\omega^{b'}) = \omega^{a'b-ab'}(X_\ell^{a'} Z_\omega^{b'})(X_\ell^a Z_\omega^b).$$

Proof. We have

$$\begin{aligned}(X_\ell^a Z_\omega^b)(X_\ell^{a'} Z_\omega^{b'})|i\rangle &= \omega^{ib'+(i+a')b}|i+a+a' \bmod \ell\rangle,\\ (X_\ell^{a'} Z_\omega^{b'})(X_\ell^a Z_\omega^b)|i\rangle &= \omega^{ib+(i+a)b'}|i+a+a' \bmod \ell\rangle.\end{aligned}$$

Comparing the above two equations shows the lemma. □

We will consider the non-commutative relation between two matrices in E. To do this, we need to introduce so-called the symplectic inner product in $\mathbf{Z}_\ell^n$, where $\mathbf{Z}_\ell = \{0, 1, \ldots, \ell-1\}$ whose addition, subtraction, multiplication and division are considered modulo ℓ. $\mathbf{Z}_\ell$ is a finite commutative ring. For $\vec{a} = (a_1, \ldots, a_n)$, $\vec{b} = (b_1, \ldots, b_n) \in \mathbf{Z}_\ell^n$, by $(\vec{a}|\vec{b})$ we denote $(a_1, \ldots, a_n, b_1, \ldots, b_n) \in \mathbf{Z}_\ell^{2n}$. The symplectic inner product between $(\vec{a}|\vec{b}), (\vec{a}'|\vec{b}') \in \mathbf{Z}_\ell^{2n}$ is defined by

$$\langle(\vec{a}|\vec{b}), (\vec{a}'|\vec{b}')\rangle_{\mathrm{s}} = \langle\vec{a}, \vec{b}'\rangle_{\mathrm{E}} - \langle\vec{a}', \vec{b}\rangle_{\mathrm{E}},$$

where $\langle\cdot,\cdot\rangle_{\mathrm{E}}$ denotes the standard Euclidean inner product. The symplectic inner product is alternative in the sense that

$$\langle(\vec{a}|\vec{b}), (\vec{a}'|\vec{b}')\rangle_{\mathrm{s}} = -\langle(\vec{a}'|\vec{b}'), (\vec{a}|\vec{b})\rangle_{\mathrm{s}},$$

which means

$$\langle(\vec{a}|\vec{b}), (\vec{a}|\vec{b})\rangle_{\mathrm{s}} = 0$$

all $(\vec{a}|\vec{b}) \in \mathbf{Z}_\ell^{2n}$.

For $\vec{a}, \vec{b} \in \mathbf{Z}_\ell^n$ define $X_\ell(\vec{a}) = X_\ell^{a_1} \otimes \cdots \otimes X_\ell^{a_n}$ and $Z_\omega(\vec{b}) = Z_\omega^{b_1} \otimes \cdots \otimes Z_\omega^{b_n}$. This means $X_\ell(\vec{a})Z_\omega(\vec{b}) = X_\ell^{a_1} Z_\omega^{b_1} \otimes \cdots \otimes X_\ell^{a_n} Z_\omega^{b_n}$.

By using those notations and Lemma 2, we can easily see

Corollary 3:

$$\begin{aligned}&X_\ell(\vec{a})Z_\omega(\vec{b})X_\ell(\vec{a}')Z_\omega(\vec{b}')\\ &= \omega^{-\langle(\vec{a}|\vec{b}),(\vec{a}'|\vec{b}')\rangle_{\mathrm{s}}} X_\ell(\vec{a}')Z_\omega(\vec{b}')X_\ell(\vec{a})Z_\omega(\vec{b}).\end{aligned}$$

This characterizes the non-commutative relationship in E.

Let S be a commutative subgroup of E. We call a commutative subgroup of E as **stabilizer**.

Example 4: For $\ell = n = 2$, we have $E = \{\pm X_2^{a_1} Z_{-1}^{b_1} \otimes X_2^{a_2} Z_{-1}^{b_2} \mid i, a_1, a_2, b_1, b_2 \in \{0,1\}\}$. A commutative subgroup S can be $S = \{I_{2\times2} \otimes I_{2\times2}, X_2 \otimes X_2, Z_{-1} \otimes Z_{-1}, X_2 Z_{-1} \otimes X_2 Z_{-1}\}$.

We will consider a simultaneous (or joint) eigenspace of all matrices in S. Let $|\varphi\rangle \in \mathcal{H}_\ell^{\otimes n}$ be an eigenvector belonging to eigenvalues λ_M for all $M \in E$. For an indexed set $\Lambda = \{\lambda_M \mid M \in E\}$, we can define an eigenspace belonging to Λ, as $\{|\varphi\rangle \mid |\varphi\rangle$ is an eigenvector belonging to eigenvalues λ_M for $M \in S\}$.

Example 5: Continued from the last example. Non-identity matrices in S has two eigenvalues ±1. There are four possible combinations of eigenvalues of 4 matrices in S, namely, $(\lambda_{I_{2\times2}\otimes I_{2\times2}}, \lambda_{X_2\otimes X_2}, \lambda_{Z_{-1}\otimes Z_{-1}}, \lambda_{X_2Z_{-1}\otimes X_2Z_{-1}})$ can be one of $(1,1,1,1)$, $(1,-1,1,-1)$, $(1,1,-1,-1)$ and $(1,-1,-1,1)$. Since $\mathcal{H}_2^{\otimes2}$ has dimension 4, each eigenspace has dimension $1 = 4/4$. The tuple $(1,1,1,1)$ of eigenvalues has $(|00\rangle + |11\rangle)/\sqrt{2}$ as its eigenvector, $(1,-1,1,-1)$ has $(|00\rangle - |11\rangle)/\sqrt{2}$, $(1,1,-1,-1)$ has $(|01\rangle + |10\rangle)/\sqrt{2}$, and $(1,-1,-1,1)$ has $(|01\rangle - |10\rangle)/\sqrt{2}$.

By an **eigenspace** of a stabilizer S, we mean a simultaneous eigenspace as seen in the last example. We will use an eigenspace as a **codebook** for protecting quantum information.

4.2 Dimension of Codebooks

The dimension of a codebook determines how much quantum information can be encoded into a codebook. So we would like to choose the eigenspace with the largest dimension. We will shortly see that every eigenspace has the same dimension by Proposition 6.

From the last example, we see that every eigenspace has the same dimension. We will show that this property always holds.

Proposition 6: Let Q_1 and Q_2 be eigenspaces of a stabilizer S. Then there always exists a unitary matrix M such that $MQ_1 = Q_2$, which implies $\dim Q_1 = \dim Q_2$.

Proof is given in Appendix A.2.

We would like to know the dimension of eigenspaces. Since all of them have the same dimension and eigenspaces of a unitary matrix in E orthogonally decompose the entire space $\mathcal{H}_\ell^{\otimes n}$, the desired dimension can be computed if we can count the number of eigenspaces defined by S. To count them, the next example gives a hint.

Example 7: Continued from the last example. The eigenspace belonging to $(\lambda_{I_{2\times2}\otimes I_{2\times2}}, \lambda_{X_2\otimes X_2}, \lambda_{Z_{-1}\otimes Z_{-1}}, \lambda_{X_2Z_{-1}\otimes X_2Z_{-1}}) = (1,1,1,1)$ is moved to that to $(1,1,-1,-1)$ by $X_2 \otimes I_{2\times2}$, that to $(1,-1,1,-1)$ by $Z_{-1} \otimes I_{2\times2}$, and that to $(1,-1,-1,1)$ by $X_2Z_{-1} \otimes I_{2\times2}$. This demonstrates Proposition 6.

On the other hand, $X_2 \otimes X_2$, $Z_{-1} \otimes Z_{-1}$ or $X_2Z_{-1} \otimes X_2Z_{-1}$ does not exchange eigenspaces. We will show a necessary and sufficient condition for a matrix $M \in E$ does not move an eigenspace of S to another one.

The last example indicates that some matrices in E moves an eigenspace to another one, while other matrices in E keep it. We will see which matrices in E move eigenspaces.

Lemma 8: For $M \in E$ and an eigenspace Q of S, MQ is also an eigenspace of S. Let $S' = \{M \in E \mid MN = NM$ for all $N \in S\}$. For an eigenspace Q of a stabilizer S and a matrix $M \in E$, $MQ = Q$ if and only if $M \in S'$.

Proof is given in Appendix A.1.

Example 9: For $S = \{X_2 \otimes X_2, Z_{-1} \otimes Z_{-1}, X_2Z_{-1} \otimes X_2Z_{-1}, I_{2\times2} \otimes I_{2\times2}\}$, S' is $\{\pm X_2 \otimes X_2, \pm Z_{-1} \otimes Z_{-1}, \pm X_2Z_{-1} \otimes X_2Z_{-1}, \pm I_{2\times2} \otimes I_{2\times2}\}$. Note that $-I_{2\times2} \otimes I_{2\times2}$ changes every vector in $\mathcal{H}_2^{\otimes2}$, but does not move an eigenspace of S to another one. In general, a matrix $M \in S'$ may change vectors in $\mathcal{H}_\ell^{\otimes n}$.

Fix an eigenspace Q of S. Then, by Proposition 6, the set of all eigenspace of S is $\{MQ \mid M \in E\}$. By Lemma 8, the number of spaces in $\{MQ \mid M \in E\}$ is equal to the number of cosets in E/S'. Therefore,

Proposition 10: Every eigenspace of S has dimension

$$\frac{\ell^n}{|E/S'|}.$$

By Proposition 10, in terms of the amount of quantum information in a codebook, every eigenspace of S is equally useful. On the other hand, we have not examined their error correction/detection capabilities. We will see it in the next subsections.

4.3 Detectable Errors

We consider to detect and correct errors in E. Since $\{MQ \mid M \in E\}$ is an orthogonal decomposition of $\mathcal{H}_\ell^{\otimes n}$, we can make a projective quantum measurement corresponding to the decomposition. By making such a measurement on a received quantum codeword, the quantum state after this measurement belongs to one of spaces in $\{MQ \mid M \in E\}$, and the receiver knows which space contains the quantum state from the measurement outcome. A receiver detects an error if the eigenspace containing the received state is different from the original eigenspace used by a sender. By Lemma 8, we immediately obtain:

Proposition 11: An error $M \in E$ can be detected by the above procedure if and only if $M \notin S'$.

In the rest of this survey, by $\overline{S}$ we denote the commutative subgroup of E generated by $\omega I_{\ell\times\ell}^{\otimes n}$ and S.

Example 12: Previous examples of the stabilizer is unsuitable for illustrating error detection/correction procedures. Let $n = 2$, $\ell = 2$ and $S = \{I_{2\times2} \otimes I_{2\times2}, Z_{-1} \otimes Z_{-1}\}$. Then $\overline{S} = \{\pm I_{2\times2} \otimes I_{2\times2}, \pm Z_{-1} \otimes Z_{-1}\}$, and $S' = \overline{S} \cup \{\pm Z_{-1} \otimes I_{2\times2},$

$\pm I_{2\times 2} \otimes Z_{-1}$, $\pm X_2 \otimes X_2$, $\pm X_2 Z_{-1} \otimes X_2$, $\pm X_2 \otimes X_2 Z_{-1}$, $\pm X_2 Z_{-1} \otimes X_2 Z_{-1}\}$. $|E/S'| = 2$ and there are two eigenspaces whose dimensions are $\dim \mathcal{H}_2^{\otimes 2}/|E/S'| = 2$ by Proposition 10. Call those eigenspaces by Q_1 and Q_2. Orthonormal bases of Q_1 and Q_2 can be $\{|00\rangle, |11\rangle\}$, and $\{|01\rangle, |10\rangle\}$, respectively. A codeword in Q_1 can be written as $\alpha|00\rangle + \beta|11\rangle$.

We have $E \setminus S' = \{\pm X_2 \otimes I_{2\times 2}, \pm I_{2\times 2} \otimes X_2\}$, which can be detectable by Q_1 and Q_2. Since $X_2|0\rangle = |1\rangle$, $X_2|1\rangle = |0\rangle$, this quantum code can be viewed as a quantum version of the conventional $[2, 1]$ repetition code $\{00, 11\}$ that can detect single error.

4.4 Correctable Errors

We will investigate correctable errors. Fix an eigenspace Q of a stabilizer S and its quantum codeword $|\varphi\rangle \in Q$. For any $M \in S$, since $|\varphi\rangle$ is an eigenvector of M, $|\varphi\rangle$ and $M|\varphi\rangle$ correspond to the same quantum state.

4.4.1 Set of Errors with No Effect

For any $M \in \overline{S}$, since $|\varphi\rangle$ is an eigenvector of M, $|\varphi\rangle$ and $M|\varphi\rangle$ correspond to the same quantum state. Any errors in $\overline{S}$ have no effect and there is no need for correcting them. We need to clarify which errors have no effect.

Proposition 13: For a stabilizer S and its eigenspace Q, a unitary matrix M has no effect on every quantum codeword $|\varphi\rangle \in Q$ if and only if $M \in \overline{S}$.

Proof is given in Appendix A.3.

4.4.2 Error Correction Procedure

In order to discuss the set of correctable errors, we need to fix a decoding procedure. We consider the following procedure that extends our previously described detection procedure. Fix a stabilizer S and its codebook $Q \subset \mathcal{H}_\ell^{\otimes n}$. Firstly the decoder makes a projective measurement corresponding to the orthogonal decomposition $\{MQ \mid M \in E\}$ of $\mathcal{H}_\ell^{\otimes n}$. After this measurement, the quantum state belongs to one of eigenspaces in $\{MQ \mid M \in E\}$, and the decoder knows which eigenspace contains the state. Let $M_e Q$ contains the quantum state after this measurement. The decoder's job is to select $M' \in E$ suitably and to apply M' to the quantum state. We will consider how to select M' suitably. By Lemma 8, Any error M in the coset $M_e + S' = \{M + N \mid N \in S'\}$ sends Q to $M_e Q$. Let M_{ML} be the most likely error in the coset $M_e + S'$. Then we should select M' as $M_{\mathrm{ML}}^{-1} = M_{\mathrm{ML}}^*$. What is most likely depends on the statistical property of the channel. Let P be a probability distribution on $\{X_\ell^a Z_\omega^b \mid a, b \in \{0, 1, \ldots, \ell - 1\}\}$. Since we assume the quantum channel is memoryless, for $\vec{a} = (a_1, \ldots, a_n)$, $\vec{b} = (b_1, \ldots, b_n) \in \{0, \ldots, \ell - 1\}^n$, the probability of $X_\ell(\vec{a})Z_\omega(\vec{b})$ can be written as $P(X_\ell^{a_1} Z_\omega^{b_1}) \times \cdots \times P(X_\ell^{a_n} Z_\omega^{b_n})$. Any $M \in E$ can be written as a multiple of $X_\ell(\vec{a})Z_\omega(\vec{b})$ for some $\vec{a}, \vec{b} \in \{0, \ldots, \ell-1\}^n$, and we define the weight $w(M)$ of M as $\sharp\{j \mid (a_j, b_j) \neq (0, 0)\}$. If the probability $P(I_{\ell\times\ell})$ of no error is relatively larger than any other probabilities $P(X_\ell^a Z_\omega^b)$ with $(a, b) \neq (0, 0)$, then we have $w(M_1) < w(M_2) \Rightarrow P(M_1) > P(M_2)$. Therefore, M_{ML} can be selected such that $w(M_{\mathrm{ML}}) \leq w(M)$ for all $M \in M_e + S'$. We have a decoding rule similar to the minimum distance decoding in the conventional coding theory.

4.4.3 Correctable Errors and the Minimum Distance

We define the **minimum distance** of a stabilizer S by

$$d = \min\{w(M) \mid M \in S' \setminus \overline{S}\}.$$

Example 14: Continued from Example 12. We have $S' \setminus \overline{S} = \{\pm Z_{-1} \otimes I_{2\times 2}, \pm I_{2\times 2} \otimes Z_{-1}, \pm X_2 \otimes X_2, \pm X_2 Z_{-1} \otimes X_2, \pm X_2 \otimes X_2 Z_{-1}, \pm X_2 Z_{-1} \otimes X_2 Z_{-1}\}$. Therefore we see that its minimum distance is 1.

Suppose that a quantum codeword was sent and an error M occurred. If $w(M) < d/2$, then we have either $M \in \overline{S}$ or $M \notin S'$. If $M \in \overline{S}$, then M has no effect on every codeword. Our quantum error correction/detection recognizes that the received quantum state belongs to the original codebook, and declares "no error".

If $M \notin S'$, then by Proposition 11 our decoder recognizes that a received state does not belong to the original codebook and existence of error. Then our decoder searches M_{ML} such that $M_{\mathrm{ML}} \in M + S'$ and $w(M_{\mathrm{ML}}) \leq w(M')$ for all $M' \in M + S'$. By the assumption $w(M) < d/2$, M_{ML} must be a multiple of M and applying $M_{\mathrm{ML}}^{-1} = M_{\mathrm{ML}}^*$ to the received quantum state restores the originally sent quantum codeword.

Therefore, we have

Proposition 15: If an error has weight less than half the minimum distance, it can be corrected by the described decoding procedure.

Suppose that $\sharp E/S' = \ell^{n-k}$, then every eigenspace of the stabilizer S has dimension ℓ^k, every codeword belongs to $\mathcal{H}_\ell^{\otimes n}$. Such a quantum code is called an $[[n, k, d]]_\ell$ code, similar to the notation $[n, k, d]_\ell$ code in the conventional coding theory.

5. Description of Stabilizer Codes by Finite Fields

5.1 Prime Dimension

The conventional theory of error-correcting codes is built by linear spaces over finite fields. On the other hand, our explanation uses complex linear spaces, and research results of the conventional coding theory cannot be directly applied. In this section, we explain ways to describe the stabilizers by finite fields. We assume that ℓ is equal to some prime number p. Let $\mathbf{F}_p$ be the finite field with p elements.

For $M = \omega^i X_\ell(\vec{a})Z_\omega(\vec{b}) \in E$ with some $\vec{a}, \vec{b} \in \mathbf{F}_p^n$, define a mapping $f(M)$ from E to $\mathbf{F}_p^{2n}$ by $f(M) = (\vec{a}|\vec{b})$, where $(\vec{a}|\vec{b})$ denotes a concatenated vector of $\vec{a}$ and $\vec{b}$.

Let $C \subseteq \mathbf{F}_p^{2n}$ be an $\mathbf{F}_p$-linear space. Let $S = f^{-1}(C) \subset E$. By construction we have $\overline{S} = S$.

For C, we denote by $C^{\perp_s}$ the symplectic orthogonal space of C, as

$$C^{\perp_s} = \{(\vec{a}|\vec{b}) \mid \langle(\vec{a}|\vec{b}),(\vec{c}|\vec{d})\rangle_s = 0, \forall(\vec{c}|\vec{d}) \in C\}.$$

Then $S' = f^{-1}(C^{\perp_s})$ by Corollary 3, and S is commutative if and only if $C \subset C^{\perp_s}$.

For $(\vec{a}|\vec{b}) = (a_1, \ldots, a_n|b_1, \ldots, b_n) \in \mathbf{F}_p^{2n}$, define the symplectic weight $w_s(\vec{a}|\vec{b}) = \sharp\{i \mid (a_i, b_i) \neq (0,0)\}$. Then, the minimum weight of $S' \setminus \overline{S}$ is equal to $w_s(C^{\perp_s} \setminus C)$.

E/S' is isomorphic to $\mathbf{F}_p^{2n}/C^{\perp_s}$ as commutative groups, and if $\dim C = n - k$ then $\dim \mathbf{F}_p^{2n}/C^{\perp_s} = n - k$ and the dimension of every eigenspace of the stabilizer is p^k, and C gives an $[[n, k, w_s(C^{\perp_s} \setminus C)]]_p$ quantum code.

5.2 Prime Power Dimension

In the last subsection, we have considered the case where $\dim \mathcal{H}_\ell$ is a prime number p. In this subsection we will consider the case where $\dim \mathcal{H}_\ell$ is a prime power p^m ($m \geq 1$).

Since $\mathcal{H}_{p^m}$ is isometric to $\mathcal{H}_p^{\otimes m}$, we can just regard an $[[n, k]]_{p^m}$ quantum code as an $[[nm, km]]_p$ quantum code and use linear spaces in $\mathbf{F}_p^{2mn}$. With such an approach we need to modify the definition of weight. So we will explain another approach.

Let $\{\beta_1, \ldots, \beta_m\}$ be an $\mathbf{F}_p$-basis of $\mathbf{F}_{p^m}$. For $\beta \in \mathbf{F}_{p^m}$, we define the trace map from $\mathbf{F}_{p^m}$ to $\mathbf{F}_p$ by $\mathrm{Tr}(\beta) = \beta + \beta^p + \cdots + \beta^{p^{m-1}}$. Let $\{\gamma_1, \ldots, \gamma_m\}$ be the dual basis of $\{\beta_1, \ldots, \beta_m\}$ with respect to Tr, that is,

$$\mathrm{Tr}(\beta_i\gamma_j) = \delta_{i,j},$$

where $\delta_{i,j}$ is the Kronecker's delta. Since the mapping $(x, y) \in \mathbf{F}_{p^m}^2$ to $\mathrm{Tr}(xy) \in \mathbf{F}_p$ is an $\mathbf{F}_p$-bilinear nondegenerate form, it is well known in algebra that a dual basis always exists.

Example 16: We can choose an $\mathbf{F}_2$-basis of $\mathbf{F}_4$ as $\beta_1 = 1$, $\beta_2 = \alpha$, where $\alpha^2 + \alpha + 1 = 0$. Then its dual basis with respect to the trace is $\gamma_1 = \alpha^2$, $\gamma_2 = 1$.

Let $(\vec{a}|\vec{b}) = (a_1, \ldots, a_m|b_1, \ldots, b_m)$, $(\vec{c}|\vec{d}) = (c_1, \ldots, c_m|d_1, \ldots, d_m) \in \mathbf{F}_p^{2m}$, $A = a_1\beta_1 + \cdots + a_m\beta_m$, $B = b_1\gamma_1 + \cdots + b_m\gamma_m$, $C = c_1\beta_1 + \cdots + c_m\beta_m$, $D = d_1\gamma_1 + \cdots + d_m\gamma_m \in \mathbf{F}_{p^m}$. We have

$$\begin{aligned}
&\langle(\vec{a}|\vec{b}),(\vec{c}|\vec{d})\rangle_s && (1)\\
&= \sum_{i=1}^n a_i d_i - b_i c_i && (2)\\
&= \sum_{i=1}^n a_i d_i \mathrm{Tr}(\beta_i\gamma_i) - b_i c_i \mathrm{Tr}(\beta_i\gamma_i) && (3)\\
&= \sum_{i=1}^n \sum_{j=1}^n a_i d_j \mathrm{Tr}(\beta_i\gamma_j) - b_i c_j \mathrm{Tr}(\beta_i\gamma_j) && (4)\\
&= \mathrm{Tr}(\sum_{i=1}^n a_i\beta_i \sum_{j=1}^n d_j\gamma_j) - \mathrm{Tr}(\sum_{i=1}^n b_i\beta_i \sum_{j=1}^n c_j\gamma_j) && (5)\\
&= \mathrm{Tr}(\sum_{i=1}^n a_i\beta_i \sum_{j=1}^n d_j\gamma_j - \sum_{i=1}^n b_i\beta_i \sum_{j=1}^n c_j\gamma_j) && (6)\\
&= \mathrm{Tr}(AD - BC). && (7)
\end{aligned}$$

For $(\vec{a}|\vec{b}) = (a_1, \ldots, a_n|b_1, \ldots, b_n)$, $(\vec{c}|\vec{d}) = (c_1, \ldots, c_n|d_1, \ldots, d_n) \in \mathbf{F}_{p^m}^{2n}$, by expanding each component of $\vec{a}$ and $\vec{c}$ by $\beta_1, \ldots, \beta_m$ and each component of $\vec{b}$ and $\vec{d}$ by $\gamma_1, \ldots, \gamma_m$, we obtain $(\vec{a}'|\vec{b}') = (a'_{1,1}, \ldots, a'_{n,m}|b'_{1,1}, \ldots, b'_{n,m})$, $(\vec{c}'|\vec{d}') = (c'_{1,1}, \ldots, c'_{n,m}|d'_{1,1}, \ldots, d'_{n,m}) \in \mathbf{F}_p^{2mn}$, where $a_i = a_{i,1}\beta_1 + \cdots + a_{i,m}\beta_m$ and $b_i = b_{i,1}\gamma_1 + \cdots + b_{i,m}\gamma_m$. By Eq. (7), We have

$$\mathrm{Tr}(\langle(\vec{a}|\vec{b}),(\vec{c}|\vec{d})\rangle_s) = \langle(\vec{a}'|\vec{b}'),(\vec{c}'|\vec{d}')\rangle_s$$

Define the left hand side as the trace inner product $\langle(\vec{a}|\vec{b}),(\vec{c}|\vec{d})\rangle_{tr}$, which is a nondegenerate symplectic form. Let $C^{\perp_{tr}}$ be the orthogonal space of C with respect to the above trace inner product. We can see that if C is $\mathbf{F}_{p^m}$-linear then $C^{\perp_{tr}} = C^{\perp_s}$.

Proposition 17: For $C \subset \mathbf{F}_{p^m}^{2n}$ with $\dim C = n - k$, if $C \subset C^{\perp_s}$, then we have an $[[n, k, w_s(C^{\perp_s} \setminus C)]]_{p^m}$ quantum code by expanding vectors in $\mathbf{F}_{p^m}^{2n}$ by $\{\beta_1, \ldots, \beta_m\}$ and $\{\gamma_1, \ldots, \gamma_m\}$

A large drawback in the quantum stabilizer codes is that linear spaces must be self-orthogonal with respect to the trace or symplectic inner product. Removal of this restriction is discussed in the next section.

6. Entanglement Assistance and Asymmetric Errors

Due to the page limitation, proofs in Sects. 6 and 7 cannot be given. Please refer to [18].

6.1 Entanglement Assisted Quantum-Error Correcting Codes

As the quantum teleportation, it is well-known that shared entanglement allows error-free transmission of quantum states. In a similar context, the entanglement-assisted quantum error-correcting code (EAQECC) allows more encoded quantum states by the cost of shared entanglement. Another large advantage of EAQECC is that it can be constructed from any subspace of $\mathbf{F}_q^{2n}$, where q is an arbitrarily fixed prime or prime power. An EAQECC is said to have the minimum distance d if it can detect all errors whose weight less than d. An EAQECC with minimum distance d can correct $(d-1)/2$ errors. The following is known. For the definition of maximally entangled quantum states, please refer to [3].

Proposition 18: Let $C \subseteq \mathbf{F}_q^{2n}$ be an $(n-k)$-dimensional $\mathbf{F}_q$-linear space and $H = (H_X|H_Z)$ a matrix whose row space is C. Let $C' \subseteq \mathbf{F}_q^{2(n+c)}$ be an $\mathbf{F}_q$-linear space such

that its projection to the coordinates $1, 2, \ldots, n, n+c+1, n+c+2, \ldots, 2n+c$ equals C and $C' \subseteq (C')^{\perp_s}$, where c is the minimum required number of maximally entangled quantum states in $\mathcal{H}_q \otimes \mathcal{H}_q$. Then,

$$\begin{aligned} 2c &= \operatorname{rank}\left(H_X H_Z^T - H_Z H_X^T\right) \\ &= \dim_{\mathbf{F}_q} C - \dim_{\mathbf{F}_q}\left(C \cap C^{\perp_s}\right). \end{aligned}$$

The encoding quantum circuit is constructed from C', and it encodes $k+c$ logical qudits in $\mathcal{H}_q^{\otimes k+c}$ into n physical qudits using c maximally entangled pairs. The minimum distance is $d := w_s\left(C^{\perp_s} \setminus (C \cap C^{\perp_s})\right)$. In sum, C provides an $[[n, k+c, d; c]]_q$ EAQECC over the field $\mathbf{F}_q$.

By the notation $[[n, k+c, d; c]]_q$, c denotes the number of maximally entangled pairs in $\mathcal{H}_q^{\otimes 2}$ shared between the sender and the receiver.

Also note that when $C \subseteq C^{\perp_s}$, then we can choose $C' = C$ and the construction reduces to that of the quantum stabilizer code. For details of EAQECC, please refer to [18].

6.2 Asymmetric Errors

When $\ell = p = q = 2$, X_2 corresponds to the quantum bit error and Z_{-1} does to the quantum phase error. It is argued that under some situation, the probabilities of the quantum bit and phase errors are much different [30], [31]. In such a case, it is reasonable to consider asymmetric error detection/correction capability.

Definition 19: For an error $M = \omega^i X_\ell(\vec{a}) Z_\omega(\vec{b}) \in E$, define the bit error weight $w_x(M) = w_H(\vec{a})$ and the phase error weight $w_z(M) = w_H(\vec{b})$, where w_H denotes the usual Hamming weight.

Proposition 20: [32] Notations are the same as Proposition 18. Let $d_x = \min\{w_H(\vec{a}) \mid (\vec{a}|\vec{b}) \in C^{\perp_s} \setminus C\}$, and $d_z = \min\{w_H(\vec{b}) \mid (\vec{a}|\vec{b}) \in C^{\perp_s} \setminus C\}$. Then the EAQECC constructed by C can detect every error whose bit error weight is $< d_x$ and phase error weight $< d_z$, and can correct every error whose bit error weight is $< d_x/2$ and phase error weight $< d_z/2$.

We will not mention the asymmetric errors elsewhere, but all the results can be easily modified to cover asymmetric error detection/correction.

7. Reduction of the Code Construction to the Conventional Coding Theory

7.1 Hermitian Inner Product

Until now, every code construction involves the symplectic or the trace inner product in some form. They are inconvenient when we use the conventional coding theory for quantum code construction. We will introduce the Hermitian inner product in $\mathbf{F}_{q^2}$, which is somewhat similar to the standard Euclidean inner product. For $\vec{x} = (x_1, \ldots, x_n) \in \mathbf{F}_{q^2}^n$, $\vec{x}^q$ denotes $(x_1^q, \ldots, x_n^q)$. For $\vec{x}, \vec{y} \in \mathbf{F}_{q^2}^n$, we define their Hermitian inner product as

$$\langle \vec{x}, \vec{y} \rangle_h = \langle \vec{x}^q, \vec{y} \rangle_E,$$

where $\langle \vec{x}^q, \vec{y} \rangle_E$ denotes the Euclidean inner product. Let $\{\lambda, \lambda^q\}$ be a normal basis of $\mathbf{F}_{q^2}$ over $\mathbf{F}_q$. It is well-known that such a basis always exists.

For $(\vec{a}|\vec{b}), (\vec{c}|\vec{d}) \in \mathbf{F}_q^{2n}$, let $\iota(\vec{a}|\vec{b}) = \lambda\vec{a} + \lambda^q\vec{b} \in \mathbf{F}_{q^2}^n$, then we have

$$\begin{aligned} &\langle \iota(\vec{a}|\vec{b}), \iota(\vec{c}|\vec{d}) \rangle_h - \langle \iota(\vec{c}|\vec{d}), \iota(\vec{a}|\vec{b}) \rangle_h \\ &= (\lambda^{2q} - \lambda^2) \langle (\vec{a}|\vec{b}), (\vec{c}|\vec{d}) \rangle_s \end{aligned}$$

Therefore, we have $\langle (\vec{a}|\vec{b}), (\vec{c}|\vec{d}) \rangle_s = 0$ if and only if $\langle \iota(\vec{a}|\vec{b}), \iota(\vec{c}|\vec{d}) \rangle_h - \langle \iota(\vec{c}|\vec{d}), \iota(\vec{a}|\vec{b}) \rangle_h = 0$. This implies that for $\vec{x}, \vec{y} \in \mathbf{F}_{q^2}^n$, $\langle \vec{x}, \vec{y} \rangle_h = 0 \Rightarrow \langle \iota^{-1}(\vec{x}), \iota^{-1}(\vec{y}) \rangle_s = 0$.

By the relation between the Hermitian and the symplectic inner products, Proposition 18 implies

Proposition 21: Let $C \subseteq \mathbf{F}_{q^2}^n$ be an $(n-k)/2$-dimensional code over $\mathbf{F}_{q^2}$, for suitable integers n and k. Denote by H its generator matrix. Let $C' \subseteq \mathbf{F}_{q^2}^{(n+c)}$ be an $\mathbf{F}_{q^2}$-linear space whose projection to the coordinates $1, 2, \ldots, n$ equals C and satisfies $C' \subseteq (C')^{\perp_h}$, where c is the minimum required number of maximally entangled quantum states in $\mathbf{C}^q \otimes \mathbf{C}^q$. Then,

$$c = \operatorname{rank}(HH^*) = \dim_{\mathbf{F}_{q^2}} C - \dim_{\mathbf{F}_{q^2}}\left(C \cap C^{\perp_h}\right).$$

The encoding quantum circuit is constructed from C', and it encodes $k+c$ logical qudits in $\mathbf{C}^q \otimes \cdots (k+c \text{ times}) \cdots \otimes \mathbf{C}^q$ into n physical qudits using c maximally entangled pairs. The minimum distance is $d := d_H\left(C^{\perp_h} \setminus (C \cap C^{\perp_h})\right)$, where d_H is defined as the minimum Hamming weight of the vectors in the set $C^{\perp_h} \setminus \left(C \cap C^{\perp_h}\right)$. In sum, C provides an $[[n, k+c, d; c]]_q$ EAQECC over the field $\mathbf{F}_q$.

7.2 Euclidean Inner Product

Let $C_1, C_2 \subseteq \mathbf{F}_q^n$, then $C_1 \otimes C_2 = \{(\vec{a}|\vec{b}) \mid \vec{a} \in C_1, \vec{b} \in C_2\} \subset \mathbf{F}_q^{2n}$. $(C_1 \otimes C_2)^{\perp_s} = C_2^{\perp_E} \otimes C_1^{\perp_E}$, where $C_1^{\perp_E}$ is the orthogonal space of C_1 with respect to the standard Euclidean product, and the equality can be seen from comparing their dimentions as linear spaces. By using this relation, Proposition 18 implies

Proposition 22: Let C_1 and C_2 be two linear codes over $\mathbf{F}_q$ included in $\mathbf{F}_q^n$ with respective dimensions k_1 and k_2 and generator matrices H_1 and H_2. Then, the code $C_0 = C_1 \times C_2 \subseteq \mathbf{F}_q^{2n}$ gives rise to an EAQECC which encodes $n - k_1 - k_2 + c$ logical qudits into n physical qudits using the minimum required of maximally entangled pairs c, which is

$$c = \operatorname{rank}(H_1 H_2^T) = \dim_{\mathbf{F}_q} C_1 - \dim_{\mathbf{F}_q}(C_1 \cap C_2^\perp).$$

The minimum distance of the entanglement-assisted quantum code is larger than or equal to

$$d := \min\left\{d_H\left(C_1^{\perp} \setminus (C_2 \cap C_1^{\perp})\right), d_H\left(C_2^{\perp} \setminus (C_1 \cap C_2^{\perp})\right)\right\}.$$

In sum, one gets an $[[n, n-k_1-k_2+c, d; c]]_q$ EAQECC.

8. Quantum LDPC Codes

The history of quantum low-density parity-check (LDPC) codes is well documented in [33], which summarized the results up to 2015, but sufficiently covers the main milestone at the time of writing. It classifies quantum LDPC codes into four classes. These are "Dual-containing CSS codes," "Non-dual-containing CSS codes," "Non-CSS codes," and "Entanglement-assisted (EA) codes." Among these, "Non-dual-containing CSS codes" and "EA codes" are the classes in which codes with high error correction performance have been discovered. In the former, it is mentioned that spatially coupled quasi-cyclic low-density parity-check (SC QC-LDPC) codes [34] and non-binary QC-LDPC code [35], which are subclasses of the former, show performance close to the Hashing bound $1-H(\mathbf{p})$, where $H(\mathbf{p})$ is the entropy of the probability distribution $\mathbf{p} = (1-p_X-p_Y-p_Z, p_X, p_Y, p_Z)$ and p_X, p_Y and p_Z are the error-probabilities of X, Y and Z. In other words, the communication channel is assumed as a Pauli channel. Codes in [34] and [35] are derived from [36]. In the latter case, it is shown that the performance is close to conventional LDPC codes [37]. It is worth mentioning that the first authors of four references [34]–[37] are Japanese researchers.

In this section, we will assume the level of the quantum state to $\ell := 2$. First, we define a quantum LDPC code using the stabilizer formalism. In other words, we define a quantum code Q as the eigenspace of a stabilizer (i.e. commutative subgroup) S of the group E. Any element of E can be represented in the form of $\pm X(\vec{a})Z(\vec{b})$, where $\vec{a}, \vec{b} \in \mathbf{F}_2^n$.

As in conventional coding theory, there is no strict definition of LDPC codes in quantum coding theory. The definition in this paper also only provide a rough frame.

Definition 23: A quantum LDPC code is defined as a pair (Q, H) of a quantum code Q and a generator system H, in the sense of group theory, of a stabilizer S that satisfies the following condition:

For any $\pm X(\vec{a})Z(\vec{b}) \in \mathsf{H}$, $w_{\mathrm{s}}(\vec{a}|\vec{b})$ is small.

The word "small" in the above condition is ambiguous. Therefore it is not strictly defined. This can be said to be a translation of the property called "sparsity" into the stabilizer formalism.

The quantum LDPC codes defined in the stabilizer formalism are classified into two subclasses according to whether the class is called CSS or not. In addition, the CSS code is classified into two subclasses based on whether it is dual-containing or not. Putting them all together, we obtain the three classes "Dual-containing CSS codes," "Non-dual-containing CSS codes," and "Non-CSS codes." Let us introduce the definition of CSS codes.

For the stabilizer S, we write S_X for the set of elements that can be represented as $\pm X(\vec{a})Z(\mathbf{0})$, and S_Z for the set of elements that can be represented as $\pm X(\mathbf{0})Z(\vec{b})$. Here $\vec{a}, \vec{b}, \mathbf{0} \in \mathbf{F}_2^n$, where $\mathbf{0}$ is a vector with all zero entries. If S is generated by the union $S_X \cup S_Z$, then the corresponding quantum code Q is called a CSS code.

The bit sequence a is obtained from $\pm X(a)Z(\mathbf{0})$ of S_X. Let us write C_X' for the set of bit sequences obtained in this way. Similarly, let us define C_Z' from S_Z. Set the dual code, with the standard inner product, of C_X' as C_X and the dual code of C_Z' as C_Z. It turns out that the decoding methods of C_X and C_Z can be applied to the error correction for Q, and the knowledge and the technique of conventional coding theory can be applied to quantum error correction. In particular, when (Q, H) is a quantum CSS-LDPC codes, both C_X and C_Z are conventional LDPC codes.

CSS codes are called "dual-containing CSS codes" when $C_X = C_Z$, otherwise they are called "non-dual-containing CSS codes."

The reason why the performance of non-dual-containing CSS LDPC codes as quantum LDPC codes is better than the other two classes is due to its error correction algorithm and the structure of the stabilizer. In order to correct errors, the error Pauli matrices are estimated by a specific algorithm based on the measurement outcomes made by projective measurements associated to the stabilizer. In quantum LDPC codes, the algorithm is based on the sum-product algorithm, which is a decoding algorithm for conventional LDPC codes. This can be regarded as a calculation to find the error vector from the received word syndrome. The details can be found in [38]. This sum-product algorithm does not work well for non-CSS codes and dual-containing CSS codes, since it is said to be in terms of conventional LDPC codes as "the girth" of the Tanner graph corresponding to these quantum codes cannot exceed 4. In the language of stabilizers, this means that there exist different i and j and the different $\pm X(\vec{a})Z(\vec{b})$ and $\pm X(\vec{c})Z(\vec{d}) \in \mathsf{H}$ such that none of $(a_i, b_i), (c_i, d_i), (a_j, b_j)$ and (c_j, d_j) is $(0, 0)$.

On the other hand, in non-dual-containing CSS codes, SC QC-LDPC codes and non-binary QC-QLDPC codes are constructed as codes that overcome this drawback. With an internal diameter of 6 or more, the accuracy of the sum-product algorithm is improved, which significantly increases the success rate of error correction. As a result, it is evaluated that "at the time of writing, only the SC QC-LDPC codes and the non-binary QC-QLDPC codes are know to perform close to the Hashing bound" at [33].

It is very difficult to achieve both sparsity and commutativity of the generators. To overcome this problem, a method of giving up the commutativity and using EA instead has been proposed [39]. This method has been reported to achieve high performance close to that of conventional LDPC codes [37].

9. Quantum Deletion Codes

In this section, we introduce "deletion error", one of the errors that cannot be represented by Pauli matrices, and discuss codes to correct the error. Let $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n$ be quantum

systems of dimension ℓ. Further, let $\mathcal{H} := \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ and $\mathcal{H}_{\bar{i}} := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_{i-1} \otimes \mathcal{H}_{i+1} \otimes \cdots \otimes \mathcal{H}_n$ be defined. In general, any quantum state $\rho \in \mathcal{H}$ is expressed as

$$\rho = \sum_{\vec{x},\vec{y} \in \{0,\ldots,\ell-1\}^n} a_{\vec{x},\vec{y}} |x_1\rangle\langle y_1| \otimes \cdots \otimes |x_n\rangle\langle y_n|$$

where the coefficients $a_{\vec{x},\vec{y}} \in \mathbb{C}$.

Definition 24: A (single) deletion error $D_i : S(\mathcal{H}) \to S(\mathcal{H}_{\bar{i}})$ for $1 \le i \le n$ is defined as

$$\begin{aligned} D_i(\rho) := \sum_{\vec{x},\vec{y} \in \{0,\ldots,\ell-1\}^n} & a_{\vec{x},\vec{y}} \mathrm{Tr}(|x_i\rangle\langle y_i|) |x_1\rangle\langle y_1| \otimes \\ & \cdots \otimes |x_{i-1}\rangle\langle y_{i-1}| \otimes |x_{i+1}\rangle\langle y_{i+1}| \otimes \\ & \cdots \otimes |x_n\rangle\langle y_n|. \end{aligned}$$

This error is known as the partial trace. In physics, the partial trace gives the state restricted to a subsystem $\mathcal{H}_{\bar{i}}$ of $\mathcal{H}$. In terms of coding theory, this is an operation that gives a shorter subsequence of the codeword.

"Deletion errors" are often confused with "erasure errors" [42]. Here, an erasure error means an error such that its position is known. An erasure error does not change the length, while a deletion error makes the length shorter. The erasure position of the quantum system is assumed to be known, while the deleted position is assumed to be unknown. A code that can correct deletion errors can also correct erasure errors. This is because an erasure error can be converted to a deletion error by deleting the erasure part. From these reasons, it can be understood that deletion error-correction is more difficult than erasure error-correction.

A quantum code that can correct t-(single-)deletion errors is called a t-deletion code. If $t = 1$, the code is called a single deletion code. The first single deletion code was discovered in 2019 [40]. The code is an $[[8,1]]_2$ code. Later, in 2020, $[[4,1]]_2$ code was discovered in [41]. For erasure correction, the following theorem is known, by the way.

Proposition 25 ([42]): There is no single erasure correcting code of length less than 4.

From this theorem and the argument on conversion from erasure errors to deletion errors above, we obtain:

Proposition 26 ([41]): The $[[4,1]]_2$ code, the four qubits code, is the shortest single deletion code.

The four qubits code has the property called PI (Permutation Invariant).

Definition 27: A state $\rho = \sum_{\vec{x},\vec{y} \in \{0,\ldots,\ell-1\}^n} a_{\vec{x},\vec{y}} |x_1\rangle\langle y_1| \otimes \cdots \otimes |x_n\rangle\langle y_n|$ is PI if and only if

$$\rho = \sum_{\vec{x},\vec{y} \in \{0,\ldots,\ell-1\}^n} a_{\vec{x},\vec{y}} |x_{\sigma(1)}\rangle\langle y_{\sigma(1)}| \otimes \cdots \otimes |x_{\sigma(n)}\rangle\langle y_{\sigma(n)}|$$

for any permutation σ on $\{1,2,\ldots,n\}$.

A quantum code Q is PI if and only if any state in Q is PI.

Very recently, three papers on quantum deletion codes are uploaded to the arXiv server [43]–[45] and all the papers discussed PI codes. An issue on PI deletion codes is that the code rate becomes smaller when the code length is increased. Therefore, the following problem should be raised.

Problem 28: Can we construct a single deletion quantum code with its code rate close to 1? Here the code rate is defined as k/n, for the $[[n,k]]_\ell$ code.

The dual error to the deletion error is the insertion error. While the deletion error reduces the quantum systems, the insertion error increases. In conventional coding theory, the following is known.

Proposition 29 ([46]): Let C be a classical code. C is a t-deletion code by the bounded distance decoding (BDD) if and only if C is a t-insertion code by BDD[†].

The following conjecture arises naturally.

Conjecture 30: Let Q be a quantum code. Q is a t-deletion code by some decoding if and only if Q is a t-insertion correction code by some decoding.

This conjecture is unresolved even at $t = 1$. The following is a positive result by an instance.

Proposition 31: [47] The four qubits deletion code can correct single insertion errors. In other words, the four qubits deletion code is the first quantum insertion code.

Acknowledgments

This paper is partially supported by KAKENHI 18H01435. The first author would like to thank Prof. Takayuki Nozaki, Mr. Mamoru Shibata and two anonymous reviewers for reading and pointing out errors in the initial manuscript.

References

[1] F. Arute, et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol.574, pp.505–510, Oct. 2019.
[2] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error rate," SIAM J. Comput., vol.38, no.4, pp.1207–1282, July 2008.
[3] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
[4] W.K. Wootters and W.H. Zurek, "A single quantum cannot be cloned," Nature, vol.299, pp.802–803, 1982.
[5] P.W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A, vol.52, no.4, pp.2493–2496, Oct. 1995.
[6] A.R. Calderbank and P.W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol.54, no.2, pp.1098–1105, Aug. 1996.
[7] A.M. Steane, "Multiple particle interference and quantum error correction," Proc. Roy. Soc. London Ser. A, vol.452, no.1954, pp.2551–2577, Nov. 1996.
[8] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," Phys. Rev. Lett., vol.78, no.3, pp.405–408, Jan. 1997.

[†]The distance is not the Hamming distance but the Levenshtein distance. For details, please refer to [46].

[9] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inf. Theory, vol.44, no.4, pp.1369–1387, July 1998.
[10] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," Phys. Rev. A, vol.54, no.3, pp.1862–1868, Sept. 1996.
[11] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," IEEE Trans. Inf. Theory, vol.47, no.7, pp.3065–3072, Nov. 2001.
[12] J. Bierbrauer and Y. Edel, "Quantum twisted codes," J. Combinatorial Designs, vol.8, no.3, pp.174–188, April 2000.
[13] R. Matsumoto and T. Uyematsu, "Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes," IEICE Trans. Fundamentals, vol.E83-A, no.10, pp.1878–1883, Oct. 2000.
[14] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett., vol.70, no.13, pp.1895–1899, March 1993.
[15] I. Devetak, A.W. Harrow, and A.J. Winter, "A resource framework for quantum Shannon theory," IEEE Trans. Inf. Theory, vol.54, no.10, pp.4587–4618, Oct. 2008.
[16] T. Brun, I. Devetak, and M.H. Hsieh, "Correcting quantum errors with entanglement," Science, vol.314, no.5798, pp.436–439, 2006.
[17] M.M. Wilde and T.A. Brun, "Optimal entanglement formulas for entanglement-assisted quantum coding," Phys. Rev. A, vol.77, no.6, article ID 064302, 2008.
[18] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Entanglement-assisted quantum error-correcting codes over arbitrary finite fields," Quantum Inf. Process., vol.18, article ID 116, 2019.
[19] D.L. Donoho, "Compressed sensing," IEEE Trans. Inf. Theory, vol.52, no.4, pp.1289–1306, April 2006.
[20] A. Kazunori, et al., "First M87 event horizon telescope results. III. Data processing and calibration," Astrophys. J. Lett., vol.875, no.1, L3, 2019.
[21] E.J. Candés, J.K. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate measurements," Commun. Pure Appl. Math., vol.59, no.8, pp.1207–1223, 2006.
[22] B. Olshausen, "Sparse coding in brains and machines," Stanfort Talks, 2016, https://talks.stanford.edu/bruno-olshausen-sparse-coding-in-brains-and-machines/
[23] R.G. Gallager, "Low density parity check codes," IRE Trans. Inf. Theory, vol.IT-8, no.1, pp.21–28, Jan. 1962.
[24] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," IEEE Trans. Inf. Theory, vol.50, no.10, pp.2315–2330, Oct. 2004.
[25] P.W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol.85, pp.441–444, July 2000.
[26] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A, vol.59, no.3, pp.1829–1834, 1999.
[27] D. Gottesman, "Theory of quantum secret sharing," Phys. Rev. A, vol.61, no.4, article ID 042311, 2000.
[28] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A, vol.55, no.2, pp.900–911, Feb. 1997.
[29] R. Matsumoto, "Fidelity of a t-error correcting quantum code with more than t errors," Phys. Rev. A, vol.64, no.2, article ID 022314, Aug. 2001.
[30] L. Ioffe and M. Mézard, "Asymmetric quantum error-correcting codes," Phys. Rev. A, vol.75, no.3, article ID 032345, March 2007.
[31] A.M. Steane, "Simple quantum error-correcting codes," Phys. Rev. A, vol.54, no.6, pp.4741–4751, Dec. 1996.
[32] C. Galindo, F. Hernando, R. Matsumoto, and D. Ruano, "Asymmetric entanglement-assisted quantum error-correcting codes and BCH codes," IEEE Access, vol.8, pp.18571–18579, 2020.
[33] Z. Babar, P. Botsinis, D. Alanis, S.X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," IEEE Access, vol.3, pp.2492–2519, 2015.
[34] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, "Spatially coupled quasi-cyclic quantum LDPC codes," Proc. IEEE Int. Symp. Inf. Theory, pp.638–642, Jul./Aug. 2011.
[35] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," IEEE Trans. Inf. Theory, vol.58, no.2, pp.1223–1230, Feb. 2012.
[36] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," Proc. IEEE Int. Symp. Inf. Theory, pp.806–810, June 2007.
[37] Y. Fujiwara, A. Gruner, and P. Vandendriessche, "High-rate quantum lowdensity parity-check codes assisted by reliable qubits," IEEE Trans. Inf. Theory, vol.61, no.4, pp.1860–1878, April 2015.
[38] M. Hagiwara, M.P.C. Fossorier, and H. Imai, "Fixed initialization decoding of LDPC codes over a binary symmetric channel," IEEE Trans. Inf. Theory, vol.58, no.4, pp.2321–2329, April 2012, doi: 10.1109/TIT.2011.2177440.
[39] M.-H. Hsieh, T.A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," Phys. Rev. A, vol.79, no.3, article ID 032340, 2009.
[40] A. Nakayama and M. Hagiwara, "The first quantum error-correcting code for single deletion errors," IEICE Communications Express, 2020, vol.9, no.4, pp.100–104, 2020, (Early 2020/01/22,) Online ISSN 2187-0136, doi: 10.1587/comex.2019XBL0154.
[41] 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), Los Angeles, CA, USA, pp.1870–1874, 2020, doi: 10.1109/ISIT44484.2020.9174339.
[42] M. Grassl, T. Beth, and T. Pellizzari. "Codes for the quantum erasure channel," Phys. Rev. A, vol.56, no.1, pp.33–36, 1997.
[43] Y. Ouyang, "Permutation-invariant quantum coding for quantum deletion channels," arXiv preprint arXiv:2102.02494, 2021.
[44] T. Shibayama and M. Hagiwara, "Permutation-invariant quantum codes for deletion errors," arXiv preprint arXiv:2102.03015, 2021.
[45] R. Matsumoto and M. Hagiwara, "Constructions of ℓ-adic t-deletion-correcting quantum codes," arXiv preprint arXiv:2102.04230, 2021.
[46] V.I. Levenshtein, "Binary codes capable of correcting deletions, insertions, and reversals," Soviet Physics Dokl., vol.10, no.8, pp.707–710, 1966.
[47] M. Hagiwara, "The four qubits deletion code is the first quantum insertion code," IEICE ComEX, Article ID 2020XBL0191, [Advance publication], (Early 2021/02/16,) doi.org/10.1587/comex.2020XBL0191.

Appendix: Proofs

A.1 Proof of Lemma 8

For $N \in S$ and an eigenspace Q of S, let λ_N be the eigenvalue to which Q belongs. For a fixed $M \in E$, let $\omega^z MN = NM$. For every $|\varphi\rangle \in Q$, $NM|\varphi\rangle = \omega^z MN|\varphi\rangle = \omega^z \lambda_N M|\varphi\rangle$, which means that every $M|\varphi\rangle \in MQ$ belongs to the same eigenvalue of $N \in S$, which shows that MQ is also an eigenspace of S.

We also observe that $MQ = Q$ if and only if $z = 0$. In the above argument, by the definition of S', $z = 0$ if and only if $M \in S'$, which shows the second claim of the lemma.

A.2 Proof of Proposition 6

Lemma 32: Matrices in E spans the linear space of all linear matrices on $\mathcal{H}_\ell^{\otimes n}$.

Proof: This can be verified by a straightforward computation, so the proof is omitted.

Proof of Proposition 6: Since every $M \in E$ is unitary, every eigenvector of M is orthogonal to each other. This means that $Q_1 \neq Q_2$ implies $Q_1 \perp Q_2$. By Lemma 8, MQ is also an eigenspace. By Lemma 32, $\{MQ \mid M \in E\}$ linearly spans $\mathcal{H}_\ell^{\otimes n}$. If there were eigenspace Q' not in $\{MQ \mid M \in E\}$, it would contradict with Lemma 8, Lemma 32, or the orthogonality of eigenspaces, which completes the proof.

A.3 Proof of Proposition 13

It is clear that $M \in \overline{S}$ has no effect on every quantum codeword in Q.

We will prove that $M \notin \overline{S}$ implies existence of $|\varphi\rangle \in Q$ such that $M|\varphi\rangle$ is not a multiple of $|\varphi\rangle$. Assume $M \notin S'$, then, by Lemma 8, $M|\varphi\rangle \notin Q$ for all $|\varphi\rangle \in Q$ and clearly $M|\varphi\rangle$ is not a multiple of $|\varphi\rangle$.

Assume $M \notin S' \setminus \overline{S}$. Let S_2 be a commutative subgroup of E generated by M and $\overline{S}$. Then $\dim f(S_2) = 1 + \dim f(\overline{S}) = 1 + \dim f(S)$. This means that there exists eigenspaces Q_2 and Q_3 of S_2 such that Q_2 and Q_3 are strictly contained in Q. Since $\dim Q_2 = \dim Q_3 \leq \dim Q - \ell$, Q_2 and Q_3 can be chosen differently. Let $|\varphi_2\rangle \in Q_2 \setminus Q_3$ and $|\varphi_3\rangle \in Q_3 \setminus Q_2$. Define λ_i as the eigenvalue of $|\varphi_i\rangle$ for the matrix M, and $|\varphi\rangle = (|\varphi_2\rangle + |\varphi_3\rangle)/\sqrt{2}$. By the definition of $|\varphi_2\rangle$ and $|\varphi_3\rangle$, we have $\lambda_2 \neq \lambda_3$, which implies $M|\varphi\rangle$ is not a multiple of $|\varphi\rangle$.

Ryutaroh Matsumoto was born in Nagoya, Japan, on November 29, 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering from Tokyo Institute of Technology, Tokyo, Japan, in 1996, 1998, and 2001, respectively. He was an Assistant Professor from 2001 to 2004, was an Associate Professor from 2004 to 2017 with the Department of Information and Communications Engineering, Tokyo Institute of Technology, Japan, and was an Associate Professor from 2017 to 2020 with the Department of Information and Communication Engineering, Nagoya University, Nagoya, Japan. Since 2020, he has been an Associate Professor with the Department of Information and Communications Engineering, Tokyo Institute of Technology, Japan. In 2011 and 2014, he was as a Velux Visiting Professor with the Department of Mathematical Sciences, Aalborg University, Aalborg, Denmark. His research interests include error-correcting codes, quantum information theory, information theoretic security, and communication theory. Dr. Matsumoto was the recipient of the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He was also the recipient of the Best Paper Awards from IEICE in 2001, 2008, 2011, and 2014.

Manabu Hagiwara was born in Ashikaga, Japan, on July 26, 1974. He received the B.E. degree in mathematics from Chiba University in 1997, and the M.E. and Ph.D. degrees in mathematical science from the University of Tokyo in 1999 and 2002, respectively. From 2002 to 2005 he was a postdoctoral fellow at IIS, the University of Tokyo. From 2005 to 2012 he was a research scientist with National Institute of Advanced Industrial Science and Technology (AIST). From 2011 to 2012 he was a visiting scholar with the University of Hawaii. From 2013 to 2020 he was an associate professor with Chiba University. He was the general co-chair of the International Symposium on Information Theory and its Application 2020 (ISITA2020), Oahu, Hawaii. Currently, he is a full professor with Graduate School of Science, Chiba University. His current research interests include coding theory and combinatorics. Prof. Hagiwara was the recipient of the ComEX Top Downloaded Letter Award, from IEICE, in April 2020.