Improvement of stabilizer-based entanglement distillation protocols by encoding operators

2006 J. Phys. A: Math. Gen. 39 4273

(http://iopscience.iop.org/0305-4470/39/16/013)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **39** (2006) 4273–4290 doi:10.1088/0305-4470/39/16/013

Improvement of stabilizer-based entanglement distillation protocols by encoding operators

Shun Watanabe, Ryutaroh Matsumoto and Tomohiko Uyematsu

Department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo 152-8552, Japan

E-mail: shun-wata@it.ss.titech.ac.jp, ryutaroh@it.ss.titech.ac.jp and uematsu@it.ss.titech.ac.jp

Received 7 November 2005
Published 31 March 2006
Online at stacks.iop.org/JPhysA/39/4273

Abstract

This paper presents a method for enumerating all encoding operators in the Clifford group for a given stabilizer. Furthermore, we classify encoding operators into the equivalence classes such that EDPs (entanglement distillation protocols) constructed from encoding operators in the same equivalence class have the same performance. By this classification, for a given parameter, the number of candidates for good EDPs is significantly reduced. As a result, we find the best EDP among EDPs constructed from [[4, 2]] stabilizer codes. This EDP has a better performance than previously known EDPs over a wide range of fidelity.

PACS numbers: 03.67.Mn, 03.67.Pp

1. Introduction

In various methods in quantum communication, we have to share a maximally entangled state. Bennett *et al* [3] proposed the entanglement distillation protocol (EDP), which is a scheme for sharing a maximally entangled state by spatially separated two parties with local operations and classical communication. Classical communication in EDPs can be either one way or two way, and two-way EDPs can distil more entanglement than one-way EDPs.

In [1, 15, 16, 20], the stabilizer-based EDP is proposed, which is constructed from the quantum stabilizer code, and is the generalization of the CSS code based EDP [25]. By using an $[[n, k]]$ stabilizer code, we can construct EDPs that distil k Bell states from n Bell states. The recurrence protocol [4] and the QPA protocol [9] are special cases of stabilizer-based EDPs, which are constructed from [[2, 1]] stabilizer codes [20, section 4].

By now, we arbitrarily choose one of many encoding operators with a stabilizer-based EDP. However, in construction of EDPs from quantum stabilizers, choice of encoding operators for stabilizer codes make large differences in performance of constructed EDPs. Even though there exist infinitely many encoding operators for a given quantum stabilizer, we cannot implement

all encoding operators efficiently. The reason is as follows. Any unitary operator can be approximated by using only elementary operators, the Hadamard operator, the phase operator, the controlled not operator and the $\frac{\pi}{8}$ operator. However in general, most unitary operators require exponentially many elementary operators to be approximated in high accuracy [21, section 4.5].

The Clifford group is the set of unitary operators generated by the Hadamard operator, the phase operator and the controlled not operator. In particular, each element in the Clifford group that acts on n qubits is a product of at most $O(n^2)$ generators [11, 12, 14]. Thus, for a given stabilizer, encoding operators in the Clifford group are efficiently implementable. It is also known that quantum computation by operators in the Clifford group can be efficiently simulated on a classical computer (Gottesman–Knill theorem) [13].

There is another method to construct two-way EDPs, which is the permutation-based EDP [7]. Permutation-based EDPs utilize local operations chosen from the Clifford group, and it is known that choices of local operations make difference in performances of permutation-based EDPs. When encoding operators of stabilizer-based EDPs are restricted to operators in the Clifford group, the classes of stabilizer-based EDPs and permutation-based EDPs are equivalent [18]. Elements of the Clifford group are described in terms of symplectic geometry, which enable us to enumerate all local operations for permutation-based EDPs [8, 17].

In this paper, we construct a method for enumerating all encoding operators in the Clifford group for a given stabilizer. Furthermore, we classify encoding operators into the equivalence classes such that EDPs constructed from encoding operators in the same equivalence class have the same performance. Such a classification has not been considered for either the stabilizer-based EDP or the permutation-based EDP until now. By this classification, for given parameters, the number of candidates for good EDPs is significantly reduced. For example, in the case of EDPs constructed from the $[[4, 2]]$ stabilizer code, the number of candidates is reduced by $1/12288$. It took one week to find the best EDP among EDPs constructed from the $[[4, 2]]$ stabilizer code with computer search, so we would have needed about 200 years to find the best EDP without our result.

As a result, we find the best EDP over wide range of fidelity among EDPs constructed from the $[[4, 2]]$ stabilizer code. This EDP has a better performance than previously known EDPs over wide range of fidelity.

This paper is organized as follows. In section 2, we review the stabilizer code and the stabilizer-based EDP. In section 3, we show our main theorems. In section 4, we show the best EDP found by using our main theorems.

2. Preliminaries

In this section, we review the stabilizer code, the encoding operator of the stabilizer code, the construction of entanglement distillation protocols (EDPs) from stabilizer codes and previously known results about two-way EDPs and the Clifford group. To make our argument general, we use the p-dimensional Hilbert space (qudit) instead of the two-dimensional space (qubit).

2.1. Stabilizer code

In this section, we review the non-binary generalization [19, 23] of the stabilizer code [5, 6, 10].

Let $\mathcal{H}$ be the p-dimensional complex linear spaces with an orthonormal basis $\{|0\rangle, \ldots, |p-1\rangle\}$, where p is a prime number. We define two matrices X and Z by

$$X|\mathrm{i}\rangle = |\mathrm{i}+1 \bmod p\rangle, \qquad Z|\mathrm{i}\rangle = \omega^i|\mathrm{i}\rangle$$

with a complex primitive pth root ω of 1. The matrices X and Z have the following relation:

$$ZX = \omega XZ. \tag{1}$$

Let $\mathbf{Z}_p = \{0, \ldots, p-1\}$ with addition and multiplication taken modulo p, and $\mathbf{Z}_p^n$ be the n-dimensional vector space over $\mathbf{Z}_p$. For a vector $\vec{a} = (a_1, \ldots, a_n \mid b_1, \ldots, b_n) \in \mathbf{Z}_p^{2n}$, let

$$\mathsf{XZ}^n(\vec{a}) = X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n}.$$

Note that eigenvalues of $X^{a_i} Z^{b_i}$ are powers of ω for $p \geqslant 3$, and $\{\pm 1, \pm \mathbf{i}\}$ for $p = 2$, where $\mathbf{i}$ is the imaginary unit. For a vector $\vec{c} = (c_1, \ldots, c_n) \in \mathbf{Z}_p^n$, we denote

$$|\vec{c}\rangle = |c_1\rangle \otimes \cdots \otimes |c_n\rangle.$$

Definition 1. *Let*

$$\mathcal{P}_n = \left\{ \omega^i \mathsf{XZ}^n(\vec{a}) \,\middle|\, i \in \mathbf{Z}_p, \vec{a} \in \mathbf{Z}_p^{2n} \right\} \tag{2}$$

for $p \geqslant 3$, and

$$\mathcal{P}_n = \left\{ \mu \mathsf{XZ}^n(\vec{a}) \,\middle|\, \mu \in \{\pm 1, \pm \mathbf{i}\}, \vec{a} \in \mathbf{Z}_p^{2n} \right\}$$

for $p = 2$, and let S be a commutative subgroup of $\mathcal{P}_n$. The group $\mathcal{P}_n$ is called the Pauli group and the subgroup S is called a stabilizer.

Suppose that $\{\mathsf{XZ}^n(\vec{\xi}_1), \ldots, \mathsf{XZ}^n(\vec{\xi}_{n-k})$ (and possibly some power of ωI_{p^n} for $p \geqslant 3$ and some power of $\mathbf{i} I_{p^n}$ for $p = 2$) $\}$ is a generating set of the group S, where $\vec{\xi}_1, \ldots, \vec{\xi}_{n-k}$ are linearly independent over $\mathbf{Z}_p$. From now, we fix a generating set of S as $\vec{\xi}_1, \ldots, \vec{\xi}_{n-k}$.

A stabilizer code Q is a joint eigenspace of S in $\mathcal{H}^{\otimes n}$. There are many joint eigenspaces of S and we can distinguish an eigenspace by its eigenvalue of $\mathsf{XZ}^n(\vec{\xi}_i)$ for $i = 1, \ldots, n-k$. Hereafter we fix a joint eigenspace $Q(\vec{0})$ of S and suppose that $Q(\vec{0})$ belongs to the eigenvalue λ_i of $\mathsf{XZ}^n(\vec{\xi}_i)$ for $i = 1, \ldots, n-k$. Note that $\lambda_i \in \{\omega^a \mid a \in \mathbf{Z}_p\}$ for $p \geqslant 3$, and $\lambda_i \in \{\pm 1, \pm \mathbf{i}\}$ for $p = 2$. For a vector $\vec{x} = (x_1, \ldots, x_{n-k}) \in \mathbf{Z}_p^{n-k}$, we denote $Q(\vec{x})$ as a joint eigenspace that belongs to the eigenvalue $\lambda_i \omega^{x_i}$ of $\mathsf{XZ}^n(\vec{\xi}_i)$ for $i = 1, \ldots, n-k$.

Definition 2. *For two vectors $\vec{x} = (a_1, \ldots, a_n \mid b_1, \ldots, b_n)$ and $\vec{y} = (c_1, \ldots, c_n \mid d_1, \ldots, d_n)$, the symplectic inner product is defined by*

$$\langle \vec{x}, \vec{y} \rangle = \sum_{i=1}^{n} b_i c_i - a_i d_i.$$

Definition 3. *The linear space $\mathbf{Z}_p^{2n}$ with symplectic inner product defined in definition 2 is called the symplectic space.*

Suppose that we sent $|\varphi\rangle \in Q(\vec{0})$, and received $\mathsf{XZ}^n(\vec{e})|\varphi\rangle$. We can tell which eigenspace of S contains the state $\mathsf{XZ}^n(\vec{e})|\varphi\rangle$ by measuring an observable whose eigenspaces are the same as those of $\mathsf{XZ}^n(\vec{\xi}_i)$. Then the measurement outcome always indicates that the measured state $\mathsf{XZ}^n(\vec{e})|\varphi\rangle$ belonging to the eigenspace that belongs to eigenvalue $\lambda_i \omega^{\langle \vec{\xi}_i, \vec{e} \rangle}$.

2.2. Encoding operator

In this section, we review encoding operators of stabilizer codes. An encoding operator of a stabilizer code is a unitary matrix that maps the canonical basis of $\mathcal{H}^{\otimes n}$ to joint eigenvectors of a stabilizer S.

Definition 4. *Let $\mathcal{H}^n(\vec{e})$ be the subspace of $\mathcal{H}^{\otimes n}$ such that $\mathcal{H}^n(\vec{e})$ is spanned by*

$$\left\{|\vec{e}\rangle \otimes |\vec{x}\rangle \;\middle|\; \vec{x} \in \mathbf{Z}_p^k\right\},$$

where $\vec{e} = (e_1, \ldots, e_{n-k}) \in \mathbf{Z}_p^{n-k}$.

Let $\left\{|\vartheta(\vec{e}, \vec{x})\rangle \;\middle|\; \vec{x} \in \mathbf{Z}_p^k\right\}$ be an orthonormal basis of $Q(\vec{e})$.

Definition 5. *An encoding operator U of a stabilizer code is a unitary operator on $\mathcal{H}^{\otimes n}$ that maps an orthonormal basis of $\mathcal{H}(\vec{e})$ to an orthonormal basis of $Q(\vec{e})$ for all $\vec{e} \in \mathbf{Z}_p^{n-k}$, i.e.,*

$$U : \mathcal{H}(\vec{e}) \ni |\vec{e}\rangle \otimes |\vec{x}\rangle \mapsto |\vartheta(\vec{e}, \vec{x})\rangle \in Q(\vec{e})$$

for $\vec{e} \in \mathbf{Z}_p^{n-k}$ and $\vec{x} \in \mathbf{Z}_p^k$.

Note that a state $\sum_{\vec{x}\in\mathbf{Z}_p^k} \alpha_{\vec{x}}|\vec{x}\rangle$ of $\mathcal{H}^{\otimes k}$ is encoded into

$$\sum_{\vec{x}\in\mathbf{Z}_p^k} \alpha_{\vec{x}}|\vartheta(\vec{e}, \vec{x})\rangle$$

by U with ancilla qudits $|e\rangle$.

2.3. stabilizer-based EDP

In this section, we review the stabilizer-based EDP. We define the following maximally entangled states in $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$ by

$$|\beta^n(\vec{v})\rangle = I_{p^n} \otimes \mathsf{XZ}^n(\vec{v}) \frac{1}{\sqrt{p^n}} \sum_{i=0}^{p^n-1} |i_A\rangle \otimes |i_B\rangle,$$

where $\vec{v} \in \mathbf{Z}_p^{2n}$.

Suppose that Alice and Bob share a mixed state $\rho \in \mathcal{S}\left(\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}\right)$, where $\mathcal{S}\left(\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}\right)$ is the set of density operators on $\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n}$. The goal of an entanglement distillation protocol is to extract as many pairs of particles with state close to $|\beta^1(\vec{0})\rangle$ as possible from n pairs of particles in the state ρ, where

$$|\beta^1(\vec{0})\rangle = \frac{1}{\sqrt{p}} \sum_{i=0}^{p-1} |i_A\rangle \otimes |i_B\rangle.$$

For $\vec{\xi}_i = (a_1, \ldots, a_n \mid b_1, \ldots, b_n)$, we define $\vec{\xi}_i^{\star} = (a_1, -b_1, \ldots, a_n, -b_n)$. Since the complex conjugate of ω is ω^{-1}, we can see that $\mathsf{XZ}^n(\vec{\xi}_i^{\star})$ is the component-wise complex conjugated matrix of $\mathsf{XZ}^n(\vec{\xi}_i)$. Let $S^{\star}$ be the subgroup of $\mathcal{P}_n$ generated by $\{\mathsf{XZ}^n(\vec{\xi}_1^{\star}), \ldots, \mathsf{XZ}^n(\vec{\xi}_{n-k}^{\star})\}$. Easy computation shows that $S^{\star}$ is again commutative. So we can consider joint eigenspaces of $S^{\star}$. There exists a joint eigenspace $Q^{\star}(\vec{x})$ of $S^{\star}$ whose eigenvalue of $\mathsf{XZ}^n(\vec{\xi}_i^{\star})$ is $\bar{\lambda}_i\omega^{-x_i}$, where $\bar{\lambda}_i$ is the complex conjugate of λ_i. For a state

$$|\varphi\rangle = \alpha_0|0\rangle + \cdots + \alpha_{p^n-1}|p^n - 1\rangle \in \mathcal{H}^{\otimes n},$$

we define

$$\overline{|\varphi\rangle} = \bar{\alpha}_0|0\rangle + \cdots + \bar{\alpha}_{p^n-1}|p^n - 1\rangle,$$

where $\bar{\alpha}_i$ is the complex conjugate of α_i.

With those notation, our protocol is executed as follows.

(i) Alice measures an observable corresponding to $\mathsf{XZ}^n(\vec{\xi}_i^{\star})$ for each i, and let $\bar{\lambda}_i\omega^{-a_i}$ be the eigenvalue of an eigenspace of $S^{\star}$ containing the state after measurement. In what follows we refer to $(a_1, \ldots, a_{n-k}) \in \mathbf{Z}_p^{n-k}$ as a *measurement outcome*.

(ii) Bob measures an observable corresponding to $\mathsf{XZ}^n(\vec{\xi}_i)$ for each i, and let $\lambda_i\omega^{b_i}$ be the eigenvalue of an eigenspace of S containing the state after measurement. In what follows we also refer to $(b_1, \ldots, b_{n-k}) \in \mathbf{Z}_p^{n-k}$ as a *measurement outcome*.

(iii) Alice sends $(a_1, \ldots, a_{n-k})$ to Bob.

(iv) If the difference of measurement outcomes $(b_1-a_1, \ldots, b_{n-k}-a_{n-k}) \notin T$ for a previously specified set $T \subset \mathbf{Z}_p^{n-k}$, then they abort the protocol.

(v) Bob performs the error correction process according to $a_1, \ldots, a_{n-k}$ as follows: Bob finds a matrix $M \in \mathcal{P}_n$ such that $MQ(\vec{b}) = Q(\vec{a})$. There are many matrices M with $MQ(\vec{b}) = Q(\vec{a})$, and Bob chooses M providing the highest fidelity among those matrices. See [20] for details. He applies M to his particles.

(vi) Alice and Bob apply the inverse of encoding operators $\overline{U}^*$ and U^* of the quantum stabilizer codes respectively, where U^* is the adjoint operator of the encoding operator U and $\overline{U}^*$ is the component-wise complex conjugate operator of U^*. We stress that Alice applies $\overline{U}^*$ instead of U^* [16, 20].

(vii) Alice and Bob discard $n-k$ ancilla qudits.

Note that, when we start with the state $|\beta^n(\vec{u})\rangle$, the state becomes

$$(I_{p^n} \otimes \mathsf{XZ}^n(\vec{u})) \sum_{\vec{x}\in\mathbf{Z}_p^k} \overline{|\vartheta(\vec{a},\vec{x})\rangle} \otimes |\vartheta(\vec{a},\vec{x})\rangle \tag{3}$$

after step (i) [20, proof of lemma 1].

2.4. Clifford group

Definition 6. *Let $\mathcal{U}_n$ be the set of all unitary operators on $\mathcal{H}^{\otimes n}$, and $N(\mathcal{P}_n)$ be the normalizer of $\mathcal{P}_n$ in $\mathcal{U}_n$, i.e.,*

$$N(\mathcal{P}_n) = \{U \mid U \in \mathcal{U}_n, UMU^* \in \mathcal{P}_n \forall M \in \mathcal{P}_n\},$$

which is called the Clifford group, where U^* is the adjoint operator of U.

The unitary operators in the Clifford group $N(\mathcal{P}_n)$ are decomposed into products of the elementary operators, where elementary operators for $p = 2$ are the Hadamard operator, the phase operator and the controlled not operator [11, 14], and the elementary operators for $p > 2$ are the p-dimensional discrete Fourier transform operator, the sum operator, the p-dimensional phase operator and the S operator [12]. The required number of the elementary operators to represent an operator in the Clifford group is at most $O(n^2)$.

3. Construction of encoding operators

In this section, we present a method to enumerate all encoding operators in the Clifford group for a given stabilizer (definitions 10 and 11). Then, we show relations between Bell states and encoded Bell states (lemma 5, corollary 2, and corollary 3). Then, we classify encoding operators into equivalence classes such that EDPs constructed from encoding operators in the same equivalence class have the same performances (definition 13, theorems 3 and 4). Finally, we show the method to enumerate all equivalence classes (theorem 5).

3.1. Construction method

For a given stabilizer S, we define $\mathcal{M}(S)$ as the set of all encoding operators, which maps the subspace $\mathcal{H}(\vec{e})$ to the subspace $Q(\vec{e})$ for all $\vec{e} \in \mathbf{Z}_p^{n-k}$ (see definition 5).

Definition 7. *Let $\mathcal{M}_{\mathrm{cl}}(S)$ be the subset of $\mathcal{M}(S)$ defined by*

$$\mathcal{M}_{\mathrm{cl}}(S) = \mathcal{M}(S) \cap N(\mathcal{P}_n).$$

$\mathcal{M}_{\mathrm{cl}}(S)$ is the set of all encoding operators that are contained in the Clifford group. The goal of this section is to present a method for enumerating all elements of $\mathcal{M}_{\mathrm{cl}}(S)$. Although the method for enumerating all elements of the Clifford group is known [8, 17], the method for enumerating all elements of $\mathcal{M}_{\mathrm{cl}}(S)$ for a given stabilizer S is not known.

Definition 8. *Let $\{\vec{x}_1, \ldots, \vec{x}_n, \vec{y}_1, \ldots, \vec{y}_n\}$ be a basis of a symplectic space $\mathbf{Z}_p^{2n}$. If $\vec{x}_i$ and $\vec{y}_i$ satisfy*

$$\langle \vec{x}_i, \vec{y}_j \rangle = \delta_{ij}, \qquad \langle \vec{x}_i, \vec{x}_j \rangle = 0, \qquad \langle \vec{y}_i, \vec{y}_j \rangle = 0$$

for all i and j, then the basis $\{\vec{x}_1, \ldots, \vec{x}_n, \vec{y}_1, \ldots, \vec{y}_n\}$ is called a hyperbolic basis.

Lemma 1. *If $\vec{\xi}_1, \ldots, \vec{\xi}_{n-k}$ are mutually orthogonal with respect to the symplectic inner product, then there exists vectors $\vec{\xi}_{n-k+1}, \ldots, \vec{\xi}_n$ and $\vec{\eta}_1, \ldots, \vec{\eta}_n$ such that*

$$\langle \vec{\xi}_i, \vec{\eta}_j \rangle = \delta_{ij}, \qquad \langle \vec{\xi}_i, \vec{\xi}_j \rangle = 0, \qquad \langle \vec{\eta}_i, \vec{\eta}_j \rangle = 0, \tag{4}$$

i.e., $\{\vec{\xi}_1, \ldots, \vec{\xi}_n, \vec{\eta}_1, \ldots, \vec{\eta}_n\}$ form a hyperbolic basis of $\mathbf{Z}_p^{2n}$.

Proof. The assertion of this lemma follows from a standard fact in symplectic geometry [22, 2]. □

Lemma 2. *Let C be the linear subspace of $\mathbf{Z}_p^{2n}$ spanned by $\vec{\xi}_1, \ldots, \vec{\xi}_{n-k}$, and $C^\perp$ be the orthogonal space of C with respect to the symplectic inner product. Let $C_{\max}$ be the linear subspace of $\mathbf{Z}_p^{2n}$ spanned by $\vec{\xi}_1, \ldots, \vec{\xi}_n$. Then,*

$$C_{\max} = C_{\max}^\perp, \qquad C \subseteq C_{\max} \subseteq C^\perp,$$

and $C^\perp$ is spanned by $\vec{\xi}_1, \ldots, \vec{\xi}_n, \vec{\eta}_{n-k+1}, \ldots, \vec{\eta}_n$.

Proof. The assertion of this lemma follows from the property of a hyperbolic basis. □

Definition 9. *For $p = 2$, we define $\mu(\vec{\xi}_i), \mu(\vec{\eta}_i) \in \{\pm 1, \pm \mathbf{i}\}$ for each $\mathsf{XZ}^n(\vec{\xi}_i), \mathsf{XZ}^n(\vec{\eta}_i)$ as follows, where $\mathbf{i}$ is the imaginary unit. For a vector $\vec{\xi}_i = (a_1, \ldots, a_n \mid b_1, \ldots, b_n)$, we define $m(\vec{\xi}_i) = |\{i \mid a_i = b_i = 1\}|$, i.e., the number of XZ s in $\mathsf{XZ}^n(\vec{\xi}_i)$. We define $\mu(\vec{\xi}_i)$ as*

$$\mu(\vec{\xi}_j) = \mathbf{i}^{m(\vec{\xi}_i)}.$$

$\mu(\vec{\eta}_i)$ is defined in the same way.

For example, in case of $n = 4$ and $\mathsf{XZ}^4(\vec{\xi}_j) = X \otimes XZ \otimes XZ \otimes XZ$, $\mu(\vec{\xi}_j) = -\mathbf{i}$. In case of $n = 3$ and $\mathsf{XZ}^3(\vec{\xi}_j) = XZ \otimes I_2 \otimes XZ$, $\mu(\vec{\xi}_j) = -1$. We need $\mu(\vec{\xi}_j)$ so that $(\mu(\vec{\xi}_j)\mathsf{XZ}^n(\vec{\xi}_j))^2 = I_{2^n}$. For $p \geqslant 3$, we do not need $\mu(\vec{\xi}_j)$ and $\mu(\vec{\eta}_j)$.

Definition 10. *Let $S_{\max}$ be the subgroup of $\mathcal{P}_n$ generated by $\{\mathsf{XZ}^n(\vec{x}) \mid \vec{x} \in C_{\max}\}$. Let $Q_{\min}(\vec{0})$ be the stabilizer code defined by $S_{\max}$ contained in $Q(\vec{0})$. We have* $\dim Q_{\min}(\vec{0}) = 1$. *Let $|\psi(\vec{0})\rangle \in Q_{\min}(\vec{0})$ be a state vector of unit norm.*

Let

$$\widetilde{\mathsf{X}}^n(\vec{f}_i) = \theta_x(\vec{f}_i)\mathsf{XZ}^n(\vec{\eta}_i), \tag{5}$$

$$\widetilde{\mathsf{Z}}^n(\vec{f}_i) = \theta_z(\vec{f}_i)\mathsf{XZ}^n(\vec{\xi}_i) \tag{6}$$

for $p \geqslant 3$, *and*

$$\widetilde{\mathsf{X}}^n(\vec{f}_i) = \theta_x(\vec{f}_i)\mu(\vec{\eta}_i)\mathsf{XZ}^n(\vec{\eta}_i), \tag{7}$$

$$\widetilde{\mathsf{Z}}^n(\vec{f}_i) = \theta_z(\vec{f}_i)\mu(\vec{\xi}_i)\mathsf{XZ}^n(\vec{\xi}_i) \tag{8}$$

for $p = 2$, *where* $\vec{f}_i$ *is a vector such that the ith element is 1 and the other elements are* 0, $\theta_x(\cdot)$ *is an arbitrary power of* ω, *and we choose* $\theta_z(\cdot)$ *so that* $\widetilde{\mathsf{Z}}^n(\vec{f}_i)|\psi(\vec{0})\rangle = |\psi(\vec{0})\rangle$ *for* $i = 1, \ldots, n$.

Let

$$\widetilde{\mathsf{X}}^n(\vec{u}) = \prod_{i=1}^{n} (\widetilde{\mathsf{X}}(\vec{f}_i))^{u_i} \tag{9}$$

$$\widetilde{\mathsf{Z}}^n(\vec{v}) = \prod_{i=1}^{n} (\widetilde{\mathsf{Z}}(\vec{f}_i))^{v_i} \tag{10}$$

for $\vec{u} = (u_1, \ldots, u_n) \in \mathbf{Z}_p^n$ *and* $\vec{v} = (v_1, \ldots, v_n) \in \mathbf{Z}_p^n$.

We define our encoding operator U_e *by*

$$U_e : \mathsf{X}^n(\vec{u})|\vec{0}\rangle \mapsto \widetilde{\mathsf{X}}^n(\vec{u})|\psi(\vec{0})\rangle, \tag{11}$$

where $\mathsf{X}^n(\vec{u}) = X^{u_1} \otimes \cdots \otimes X^{u_n}$. *We define* $\mathsf{Z}^n(\vec{u})$ *in a similar manner.*

Remark 1. From lemma 3, we find that equations (9) and (10) are a generalization of encoded $\mathsf{X}^n(\vec{u})$ operator and encoded $\mathsf{Z}^n(\vec{v})$ operator defined in [14].

Remark 2. The construction of the encoding operator depends on the choice of $\vec{\xi}_{n-k+1}, \ldots, \vec{\xi}_n$ and $\vec{\eta}_1, \ldots, \vec{\eta}_n$ that satisfy equation (4), $Q_{\min}(\vec{0}) \subset Q(\vec{0})$, and phase factors $\theta_x(\cdot)$. An example will be given in section 4.

Definition 11. *For a given stabilizer S, we define* $\mathcal{M}_g(S)$ *as the set of encoding operators* U_e *for all choices of* $\vec{\xi}_{n-k+1}, \ldots, \vec{\xi}_n, \vec{\eta}_1, \ldots, \vec{\eta}_n, Q_{\min}(\vec{0}) \subset Q(\vec{0})$, *and* $\theta_x(\cdot)$.

$\mathcal{M}_g(S)$ is the set of all encoding operators that are constructed by the method in definition 10. Next, we show $\mathcal{M}_g(S)$ is equal to $\mathcal{M}_{\mathrm{cl}}(S)$.

Lemma 3. *For* $\widetilde{\mathsf{X}}^n(\vec{s}), \widetilde{\mathsf{Z}}^n(\vec{t})$, U_e *defined by equations (9), (10) and (11), we have*

$$U_e\mathsf{X}^n(\vec{s})U_e^* = \widetilde{\mathsf{X}}^n(\vec{s}) \in \mathcal{P}_n \qquad \forall \vec{s} \in \mathbf{Z}_p^n, \tag{12}$$

$$U_e\mathsf{Z}^n(\vec{t})U_e^* = \widetilde{\mathsf{Z}}^n(\vec{t}) \in \mathcal{P}_n \qquad \forall \vec{t} \in \mathbf{Z}_p^n. \tag{13}$$

Proof. For $\vec{u} \in \mathbf{Z}_p^n$, let $|\varphi(\vec{u})\rangle = U_e|\vec{u}\rangle = \widetilde{\mathsf{X}}^n(\vec{u})|\psi(\vec{0})\rangle$. For $\vec{s} \in \mathbf{Z}_p^n$, we have

$$\begin{aligned} U_e\mathsf{X}(\vec{s})U_e^*|\varphi(\vec{u})\rangle &= U_e\mathsf{X}^n(\vec{s})|\vec{u}\rangle \\ &= U_e|\vec{u}+\vec{s}\rangle \\ &= \widetilde{\mathsf{X}}^n(\vec{u}+\vec{s})|\psi(\vec{0})\rangle \\ &= \widetilde{\mathsf{X}}^n(\vec{s})\widetilde{\mathsf{X}}^n(\vec{u})|\psi(\vec{0})\rangle \\ &= \widetilde{\mathsf{X}}^n(\vec{s})|\varphi(\vec{u})\rangle. \end{aligned}$$

Since $\{|\varphi(\vec{u})\rangle \mid \vec{u} \in \mathbf{Z}_p^n\}$ form an orthonormal basis of $\mathcal{H}^{\otimes n}$, we have

$$U_e \mathsf{X}^n(\vec{s}) U_e^* = \widetilde{\mathsf{X}}^n(\vec{s}) \in \mathcal{P}_n \quad \forall \vec{s} \in \mathbf{Z}_p^n.$$

Next, for $\vec{t} \in \mathsf{Z}_p^n$, we have

$$\begin{aligned} U_e \mathsf{Z}^n(\vec{t}) U_e^* |\varphi(\vec{u})\rangle &= U_e \mathsf{Z}^n(\vec{t}) |\vec{u}\rangle \\ &= \omega^{(\vec{t},\vec{u})} U_e |\vec{u}\rangle \\ &= \omega^{(\vec{t},\vec{u})} \widetilde{\mathsf{X}}^n(\vec{u}) |\psi(\vec{0})\rangle, \end{aligned} \tag{14}$$

where $(\cdot,\cdot)$ is the standard inner product. From the definition of $\widetilde{\mathsf{Z}}^n(\vec{t})$, we have $\widetilde{\mathsf{Z}}^n(\vec{t})|\psi(\vec{0})\rangle = |\psi(\vec{0})\rangle$. Since $\vec{\xi}_i$ and $\vec{\eta}_j$ satisfy equation (4), we have

$$\begin{aligned} &\mathsf{XZ}^n(\vec{\eta}_i)\mathsf{XZ}^n(\vec{\xi}_j) = \omega^{-1}\mathsf{XZ}^n(\vec{\xi}_j)\mathsf{XZ}^n(\vec{\eta}_i), \\ &\mathsf{XZ}^n(\vec{\xi}_i)\mathsf{XZ}^n(\vec{\xi}_j) = \mathsf{XZ}^n(\vec{\xi}_j)\mathsf{XZ}^n(\vec{\xi}_i), \\ &\mathsf{XZ}^n(\vec{\eta}_i)\mathsf{XZ}^n(\vec{\eta}_j) = \mathsf{XZ}^n(\vec{\eta}_j)\mathsf{XZ}^n(\vec{\eta}_i), \end{aligned}$$

and

$$\widetilde{\mathsf{X}}^n(\vec{u})\widetilde{\mathsf{Z}}^n(\vec{t}) = \omega^{-(\vec{t},\vec{u})}\widetilde{\mathsf{Z}}^n(\vec{t})\widetilde{\mathsf{X}}^n(\vec{u}).$$

Since $\widetilde{\mathsf{Z}}(\vec{t})|\psi(\vec{0})\rangle = |\psi(\vec{0})\rangle$, equation (14) is equal to

$$\begin{aligned} \omega^{(\vec{t},\vec{u})}\widetilde{\mathsf{X}}^n(\vec{u})\widetilde{\mathsf{Z}}^n(\vec{t})|\psi(\vec{0})\rangle &= \omega^{(\vec{t},\vec{u})}\omega^{-(\vec{t},\vec{u})}\widetilde{\mathsf{Z}}^n(\vec{t})\widetilde{\mathsf{X}}^n(\vec{u})|\psi(\vec{0})\rangle \\ &= \widetilde{\mathsf{Z}}^n(\vec{t})|\varphi(\vec{u})\rangle. \end{aligned}$$

Thus, we have

$$U_e \mathsf{Z}^n(\vec{t}) U_e^* = \widetilde{\mathsf{Z}}^n(\vec{t}) \in \mathcal{P}_n \quad \forall \vec{t} \in \mathbf{Z}_p^n.$$

□

Corollary 1. *For any $U_e \in \mathcal{M}_g(S)$, we have $U_e \in N(\mathcal{P}_n)$.*

Proof. Since $\{\mathsf{X}^n(\vec{s})\}$ and $\{\mathsf{Z}^n(\vec{t})\}$ are the generator set of $\mathcal{P}_n$ for $p \geqslant 3$, and $\{\mathsf{X}^n(\vec{s})\}$ and $\{\mathsf{Z}^n(\vec{t})\}$ and $\mathbf{i}I_{p^n}$ are the generator set of $\mathcal{P}_n$ for $p = 2$, from lemma 3, we have $U_e \in N(\mathcal{P}_n)$. □

Lemma 4. *For $U_c \in \mathcal{M}_{\mathrm{cl}}(S)$, there exists $U_e \in \mathcal{M}_g(S)$ such that $U_c = U_e$.*

Proof. We will construct $U_e \in \mathcal{M}_g(S)$ such that $U_e = U_c$. We set $|\psi\rangle$ by

$$|\psi\rangle = U_c|\vec{0}\rangle,$$

and set $\vec{\xi}_{n-k+1}, \ldots, \vec{\xi}_n$ and $\theta_z(\cdot)$ by

$$\widetilde{\mathsf{Z}}^n(\vec{f}_i) = \theta_z(\vec{f}_i)\mathsf{XZ}^n(\vec{\xi}_i) \qquad \text{for } i = 1, \ldots, n-k \tag{15}$$

$$\widetilde{\mathsf{Z}}^n(\vec{f}_i) = \theta_z(\vec{f}_i)\mathsf{XZ}^n(\vec{\xi}_i) = U_c \mathsf{Z}^n(\vec{f}_i) U_c^* \qquad \text{for } i = n-k+1, \ldots, n, \tag{16}$$

for $p \geqslant 3$, and

$$\widetilde{\mathsf{Z}}^n(\vec{f}_j) = \theta_z(\vec{f}_j)\mu(\vec{\xi}_j)\mathsf{XZ}^n(\vec{\xi}_j) \qquad \text{for } j = 1, \ldots, n-k, \tag{17}$$

$$\widetilde{\mathsf{Z}}^n(\vec{f}_j) = \theta_z(\vec{f}_j)\mu(\vec{\xi}_j)\mathsf{XZ}(\vec{\xi}_j) = U_c \mathsf{Z}^n(\vec{f}_j) U_c^* \qquad \text{for } j = n-k+1, \ldots, n, \tag{18}$$

for $p = 2$, where $\vec{f}_i$ is a vector such that the ith element is 1 and the other elements are 0. Note that $\vec{\xi}_{n-k+1}, \ldots, \vec{\xi}_n$ are determined by U_c, while $\vec{\xi}_1, \ldots, \vec{\xi}_{n-k}$ are fixed bases of C as we stated in section 2. From definition 5, we have $|\psi\rangle \in Q(\vec{0})$. For $i = 1, \ldots, n-k$, we set $\theta_z(\vec{f}_i)$ so that $\widetilde{\mathsf{Z}}^n(\vec{f}_i)|\psi\rangle = |\psi\rangle$. Specifically, since $Q(\vec{0})$ is an eigenspace that belongs to an eigenvalue

λ_i of $\mathsf{XZ}^n(\vec{\xi}_i)$ for $i = 1, \ldots, n-k$, we set $\theta_z(\vec{f}_i) = \overline{\lambda}_i$ for $p \geqslant 3$ and $\theta_z(\vec{f}_i) = \overline{\lambda}_i \overline{\mu(\vec{\xi}_i)}$ for $p = 2$.

Set $\vec{\eta}_1, \ldots, \vec{\eta}_n$, and $\theta_x(\cdot)$ by

$$\widetilde{\mathsf{X}}^n(\vec{f}_i) = \theta_x(\vec{f}_i)\mathsf{XZ}^n(\vec{\eta}_i) = U_c \mathsf{X}^n(\vec{f}_i) U_c^* \qquad \text{for } i = 1, \ldots, n, \tag{19}$$

for $p \geqslant 3$, and

$$\widetilde{\mathsf{X}}^n(\vec{f}_j) = \theta_x(\vec{f}_j)\mu(\vec{\eta}_j)\mathsf{XZ}(\vec{\eta}_j) = U_c \mathsf{X}^n(\vec{f}_j) U_c^* \qquad \text{for } j = 1, \ldots, n \tag{20}$$

for $p = 2$. Then we have

$$\widetilde{\mathsf{X}}^n(\vec{u}) = \prod_{i=1}^{n} (\widetilde{\mathsf{X}}^n(\vec{f}_i))^{u_i} = U_c \mathsf{X}^n(\vec{u}) U_c^* \quad \text{for } \vec{u} \in \mathbf{Z}_p^n.$$

We also have

$$\begin{aligned} U_c|\vec{u}\rangle &= U_c \mathsf{X}^n(\vec{u})|\vec{0}\rangle \\ &= U_c \mathsf{X}^n(\vec{u}) U_c^* U_c |\vec{0}\rangle \\ &= \widetilde{\mathsf{X}}^n(\vec{u})|\psi\rangle. \end{aligned}$$

Next, we show

$$\widetilde{\mathsf{Z}}^n(\vec{f}_i) = U_c \mathsf{Z}^n(\vec{f}_i) U_c^* \quad \text{for } i = 1, \ldots, n-k. \tag{21}$$

Let $\vec{u} = (e_1, \ldots, e_{n-k}, x_1, \ldots, x_k) \in \mathbf{Z}_p^n$, $\vec{e} = (e_1, \ldots, e_{n-k})$ and $|\varphi(\vec{u})\rangle = U_c|\vec{u}\rangle$. Then, since $|\varphi(\vec{u})\rangle \in Q(\vec{e})$ and $\mathsf{XZ}^n(\vec{\xi}_i)|\varphi(\vec{u})\rangle = \lambda_i \omega^{e_i}|\varphi(\vec{u})\rangle$, we have

$$\begin{aligned} \widetilde{\mathsf{Z}}^n(\vec{f}_i)|\varphi(\vec{u})\rangle &= \theta_z(\vec{f}_i)\mathsf{XZ}^n(\vec{\xi}_i)|\varphi(\vec{u})\rangle \\ &= \omega^{e_i}|\varphi(\vec{u})\rangle \\ &= \omega^{e_i} U_c \mathsf{X}^n(\vec{u}) U_c^* |\psi\rangle \\ &= \omega^{e_i} U_c \mathsf{X}^n(\vec{u}) U_c^* U_c \mathsf{Z}^n(\vec{f}_i)|\vec{0}\rangle \\ &= \omega^{e_i} U_c \mathsf{X}^n(\vec{u}) U_c^* U_c \mathsf{Z}^n(\vec{f}_i) U_c^* |\psi\rangle \\ &= \omega^{e_i} \omega^{-e_i} U_c \mathsf{Z}^n(\vec{f}_i) U_c^* U_c \mathsf{X}^n(\vec{u}) U_c^* |\psi\rangle \\ &= U_c \mathsf{Z}^n(\vec{f}_i) U_c^* |\varphi(\vec{u})\rangle, \end{aligned}$$

for $i = 1, \ldots, n-k$. Since $\{|\varphi(\vec{u})\rangle \mid \vec{u} \in \mathbf{Z}_p^n\}$ form an orthonormal basis of $\mathcal{H}^{\otimes n}$, equation (21) is satisfied.

From equations (1), (15), (16), (19) and (21), we have

$$\begin{aligned} &\mathsf{XZ}^n(\vec{\xi}_i)\mathsf{XZ}^n(\vec{\xi}_j) = \mathsf{XZ}^n(\vec{\xi}_j)\mathsf{XZ}^n(\vec{\xi}_i) \\ &\mathsf{XZ}^n(\vec{\eta}_i)\mathsf{XZ}^n(\vec{\eta}_j) = \mathsf{XZ}^n(\vec{\eta}_j)\mathsf{XZ}^n(\vec{\eta}_i) \\ &\mathsf{XZ}^n(\vec{\xi}_i)\mathsf{XZ}^n(\vec{\eta}_i) = \omega \mathsf{XZ}^n(\vec{\eta}_i)\mathsf{XZ}^n(\vec{\xi}_i) \\ &\mathsf{XZ}^n(\vec{\xi}_i)\mathsf{XZ}^n(\vec{\eta}_j) = \mathsf{XZ}^n(\vec{\eta}_j)\mathsf{XZ}^n(\vec{\xi}_i), \end{aligned}$$

which mean that $\vec{\xi}_1, \ldots, \vec{\xi}_n$ and $\vec{\eta}_1, \ldots, \vec{\eta}_n$ satisfy equation (4). It is easy to check that $|\psi\rangle$ is an eigenvector of $\mathsf{XZ}^n(\vec{\xi}_1), \ldots, \mathsf{XZ}^n(\vec{\xi}_n)$; thus we can write $|\psi\rangle = |\psi(\vec{0})\rangle \in Q_{\min}(\vec{0})$ for some $Q_{\min}(\vec{0})$.

Consequently, we can construct an encoding operator $U_e \in \mathcal{M}_g(S)$ such that $U_e = U_c$. □

From corollary 1 and lemma 4, we have the following theorem.

Theorem 1. *For a given stabilizer S, $\mathcal{M}_g(S) = \mathcal{M}_{\mathrm{cl}}(S)$.*

3.2. Classification of encoding operators

In this section, we show the correspondence between Bell states and Bell states encoded by encoding operators (lemma 5, corollary 2 and corollary 3). Then we show the output state of our EDPs is always a probabilistic mixture of Bell states if the input state of protocols is a probabilistic mixture of Bell states (theorem 2). Then, we classify encoding operators into equivalence classes such that EDPs constructed from encoding operators in the same equivalence class have the same performance when the input of EDPs are the probabilistic mixture of Bell states (definition 13, and theorems 3, 4).

Lemma 5. *The Bell state* $|\beta^k(\vec{0})\rangle$ *with ancilla qubits* $|\vec{e}\rangle_A \otimes |\vec{e}\rangle_B$*, i.e.,*

$$|\beta^k(\vec{0}), \vec{e}\rangle = \frac{1}{\sqrt{p^k}} \sum_{\vec{v}\in\mathbf{Z}_p^k} |\vec{e}\rangle_A \otimes |\vec{v}\rangle_A \otimes |\vec{e}\rangle_B \otimes |\vec{v}\rangle_B,$$

is mapped by $\overline{U_e} \otimes U_e$ *to*

$$|\phi(\vec{e})\rangle = \frac{1}{\sqrt{p^k}} \sum_{\vec{u}\in\vec{e}\times\mathbf{Z}_p^k} \overline{\widetilde{\mathsf{X}}^n(\vec{u})|\psi(\vec{0})\rangle} \otimes \widetilde{\mathsf{X}}(\vec{u})|\psi(\vec{0})\rangle, \tag{22}$$

where $\overline{\widetilde{\mathsf{X}}^n}(\vec{u})$ *is the complex conjugated matrix of* $\widetilde{\mathsf{X}}(\vec{u})$*, and* $\vec{e} \times \mathbf{Z}_p^k$ *is the subset* $\{(e_1, \ldots, e_{n-k}, x_1, \ldots, x_k) \mid x_i \in \mathbf{Z}_p\}$ *of* $\mathbf{Z}_p^n$*.*

Proof. It is obvious from equation (11) in the definition of the encoding operator U_e. □

Corollary 2. *A Bell state*

$$I_{p^k} \otimes \mathsf{X}^k(\vec{\ell})\mathsf{Z}^k(\vec{m})|\beta^k(\vec{0})\rangle \tag{23}$$

with ancilla qubits $|\vec{e}\rangle_A \otimes |\vec{e}\rangle_B$*, i.e.,*

$$|\beta^k(\vec{\ell}, \vec{m}), \vec{e}\rangle = \frac{1}{\sqrt{p^k}} \sum_{\vec{v}\in\mathbf{Z}_p^k} |\vec{e}\rangle_A \otimes |\vec{v}\rangle_A \otimes |\vec{e}\rangle_B \otimes \mathsf{X}^k(\vec{\ell})\mathsf{Z}^k(\vec{m})|\vec{v}\rangle_B, \tag{24}$$

is mapped by $\overline{U_e} \otimes U_e$ *to*

$$I_{p^n} \otimes \mathsf{XZ}^n(\vec{\ell}G + \vec{m}H)|\phi(\vec{e})\rangle, \tag{25}$$

multiplied by a scalar of unit absolute value, where the matrices G and H are

$$G = \begin{pmatrix} \vec{\eta}_{n-k+1} \\ \vdots \\ \vec{\eta}_n \end{pmatrix}, \qquad H = \begin{pmatrix} \vec{\xi}_{n-k+1} \\ \vdots \\ \vec{\xi}_n \end{pmatrix}.$$

Proof. Let

$$\vec{\ell}' = (0, \ldots, 0, \ell_1, \ldots, \ell_k) \in \mathbf{Z}_p^n \tag{26}$$
$$\vec{m}' = (0, \ldots, 0, m_1, \ldots, m_k) \in \mathbf{Z}_p^n. \tag{27}$$

From equations (12) and (13),

$$U_e\mathsf{X}^n(\vec{\ell}')\mathsf{Z}^n(\vec{m}')U_e^* = \widetilde{\mathsf{X}}^n(\vec{\ell}')\widetilde{\mathsf{Z}}^n(\vec{m}').$$

Thus, a state in equation (24) is mapped by $\overline{U_e} \otimes U_e$ to

$$\begin{aligned}(\overline{U_e} \otimes U_e)|\beta^k(\vec{\ell},\vec{m}),\vec{e}\rangle &= (\overline{U_e} \otimes U_e)(I_{p^n} \otimes \mathsf{X}^n(\vec{\ell}')\mathsf{Z}^n(\vec{m}'))|\beta^k(\vec{0}),\vec{e}\rangle \\ &= (\overline{U_e} \otimes U_e)(I_{p^n} \otimes \mathsf{X}^n(\vec{\ell}')\mathsf{Z}^n(\vec{m}'))(\overline{U_e}^* \otimes U_e^*)(\overline{U_e} \otimes U_e)|\beta^k(\vec{0}),\vec{e}\rangle \\ &= I_{p^n} \otimes \widetilde{\mathsf{X}}^n(\vec{\ell}')\widetilde{\mathsf{Z}}^n(\vec{m}')|\phi(\vec{e})\rangle \\ &\overset{(a)}{\simeq} I_{p^n} \otimes \mathsf{XZ}^n(\vec{\ell}G)\mathsf{XZ}^n(\vec{m}H)|\phi(\vec{e})\rangle \\ &\simeq I_{p^n} \otimes \mathsf{XZ}^n(\vec{\ell}G + \vec{m}H)|\phi(\vec{e})\rangle,\end{aligned}$$

where $\simeq$ denotes that one vector is equal to another vector multiplied by a scalar of unit absolute value. Note that (a) follows from equations (1), (9) and (10). □

Corollary 3. *The state*

$$I_{p^n} \otimes \mathsf{XZ}^n(\vec{\ell}G + \vec{m}H)|\phi(\vec{e})\rangle$$

is mapped by $\overline{U_e}^* \otimes U_e^*$ *to*

$$|\beta^k(\vec{\ell},\vec{m}),\vec{e}\rangle = \frac{1}{\sqrt{p^k}} \sum_{\vec{v}\in\mathbf{Z}_p^k} |\vec{e}\rangle_A \otimes |\vec{v}\rangle_A \otimes |\vec{e}\rangle_B \otimes \mathsf{X}^k(\vec{\ell})\mathsf{Z}^k(\vec{m})|\vec{v}\rangle_B$$

multiplied by a scalar of unit absolute value, i.e., $|\beta^k(\vec{w})\rangle$ *with ancilla qudits* $|\vec{e}\rangle_A \otimes |\vec{e}\rangle_B$, *where* $\vec{w} = (\ell_1,\ldots,\ell_k \mid m_1,\ldots,m_k)$.

Definition 12. *For a vector* $\vec{s} = (s_1,\ldots,s_{n-k})$, *we define the set* $D(\vec{s})$ *by*

$$D(\vec{s}) = \left\{\vec{t} \in \mathbf{Z}_p^{2n} \;\middle|\; \langle\vec{\xi}_i,\vec{t}\rangle = s_i\right\}.$$

Lemma 6. *When we apply steps (i)–(v) of our distillation protocol to the state* $|\beta^n(\vec{t})\rangle$ *and Alice and Bob do not abort the protocol in step (ii), the resulting quantum state is*

$$I_{p^k} \otimes \mathsf{XZ}^n(f(\vec{t}))|\phi(\vec{a})\rangle,$$

where $f(\cdot)$ *is the mapping from* $\mathbf{Z}_p^{2n}$ *to* $C^\perp$ *and depends on the error correction process in step (v). Specifically,* $f(\cdot)$ *is defined as follows. Let* $\vec{t}'$ *be the most likely error in* $D(\vec{b}-\vec{a})$. *The mapping* $f(\cdot)$ *is defined as*

$$f : D(\vec{b}-\vec{a}) \ni \vec{x} \mapsto \vec{x} - \vec{t}' \in C^\perp \tag{28}$$

for each $D(\vec{b}-\vec{a})$. *Note that* $\cup_{\vec{s}\in\mathbf{Z}_p^{n-k}} D(\vec{s}) = \mathbf{Z}_p^{2n}$.

Proof. After steps (i) and (ii), the state becomes

$$\mathsf{P}^\star(\vec{a}) \otimes \mathsf{P}(\vec{b})|\beta^n(\vec{t})\rangle = I_{p^k} \otimes \mathsf{XZ}^n(\vec{t})|\phi(\vec{a})\rangle \in Q^\star(\vec{a}) \otimes Q(\vec{b}),$$

where $\mathsf{P}^\star(\vec{a})$ and $\mathsf{P}(\vec{b})$ represent the projection on to $Q^\star(\vec{a})$ and $Q(\vec{b})$, respectively. In step (v), Bob decides the most likely error $\vec{t}' \in D(\vec{b}-\vec{a})$ and applies $M = \mathsf{XZ}^n(-\vec{t}')$. Then the state becomes

$$I_{p^k} \otimes \mathsf{XZ}^n(\vec{t}-\vec{t}')|\phi(\vec{a})\rangle = I_{p^k} \otimes \mathsf{XZ}^n(f(\vec{t}))|\phi(\vec{a})\rangle \in Q^\star(\vec{a}) \otimes Q(\vec{a}).$$

The condition $MQ(\vec{b}) = Q(\vec{a})$ implies $\vec{t}-\vec{t}' \in C^\perp$. □

Remark 3. The mapping $f(\cdot)$ does not depend on the choice of a basis $\{\vec{\xi}_1,\ldots,\vec{\xi}_{n-k}\}$ of C or the joint eigenspace $Q(\vec{0})$. Since there exists one-to-one correspondence between $D(\vec{s})$ and

a coset of $\mathbf{Z}_p^{2n}/C^{\perp}$, the mapping $f(\cdot)$ is defined only by a representative $\vec{t}'$ of each coset of $\mathbf{Z}_p^{2n}/C^{\perp}$ in equation (28).

Lemma 7. *When we apply step (i)–(vii) of our distillation protocol to the state* $|\beta^n(\vec{t})\rangle$ *and Alice and Bob do not abort the protocol in step (ii), the resulting quantum state is*

$$|\beta^k(\vec{w})\rangle = |\beta^k(g \circ f(\vec{t}))\rangle,$$

where the mapping g *is the mapping from* $C^{\perp}$ *to* $\mathbf{Z}_p^{2k}$*, more precisely*

$$g : C^{\perp} \ni \vec{\ell}G + \vec{m}H + \vec{v} \mapsto \vec{w} = (\ell_1, \ldots, \ell_k \mid m_1, \ldots, m_k) \in \mathbf{Z}_p^{2k} \quad \forall \vec{v} \in C. \tag{29}$$

Proof. From lemma 6, after steps (i)–(v) the resulting quantum state is

$$I_{p^k} \otimes \mathsf{XZ}^n(f(\vec{t}))|\phi(\vec{a})\rangle,$$

with $f(\vec{t}) \in C^{\perp}$. Since $\vec{\xi}_1, \ldots, \vec{\xi}_n, \vec{\eta}_{n-k+1}, \ldots, \vec{\eta}_n$ form a basis of $C^{\perp}$ and $\vec{\xi}_1, \ldots, \vec{\xi}_{n-k}$ form a basis of C, $f(\vec{t})$ can be written as a linear combination

$$f(\vec{t}) = \sum_{i=1}^{k} \ell_i \vec{\eta}_{n-k+i} + m_i \vec{\xi}_{n-k+i} + \vec{v}, \tag{30}$$

where $\vec{v} \in C$. Since $|\phi(\vec{a})\rangle$ is a joint eigenvector of S,

$$\begin{aligned} I_{p^k} \otimes \mathsf{XZ}^n(f(\vec{t}))|\phi(\vec{a})\rangle &= I_{p^n} \otimes \mathsf{XZ}^n(\vec{\ell}G + \vec{m}H + \vec{v})|\phi(\vec{a})\rangle \\ &\simeq I_{p^n} \otimes \mathsf{XZ}^n(\vec{\ell}G + \vec{m}H)|\phi(\vec{a})\rangle. \end{aligned}$$

By corollary 3, after step (vi) and (vii) the quantum state becomes $|\beta^k(\vec{w})\rangle = |\beta^k(g \circ f(\vec{t}))\rangle$, where $\vec{w} = (\ell_1, \ldots, \ell_k \mid m_1, \ldots, m_k)$. □

Theorem 2. *When the input to our distillation protocol is a probabilistic mixture of Bell states* $|\beta^n(\vec{t})\rangle$ *for* $\vec{t} \in \mathbf{Z}_p^{2n}$*, i.e.,*

$$\rho_{\text{in}} = \sum_{\vec{t} \in \mathbf{Z}_p^{2n}} P_{\text{in}}(\vec{t})|\beta^n(\vec{t})\rangle\langle\beta^n(\vec{t})| \tag{31}$$

and the difference of Alice and Bobs' measurement result is $\vec{b} - \vec{a} \in T$*, then the output from our distillation protocol is also a probabilistic mixture of Bell states* $|\beta^k(\vec{w})\rangle$ *for* $\vec{w} \in \mathbf{Z}_p^{2k}$*, i.e.,*

$$\rho_{\text{out}} = \sum_{\vec{w} \in \mathbf{Z}_p^{2k}} P_{\text{out}}(\vec{w})|\beta^k(\vec{w})\rangle\langle\beta^k(\vec{w})|,$$

where $P_{\text{out}}(\vec{w})$ *is given by*

$$P_{\text{out}}(\vec{w}) = \sum_{\vec{t} \in D(\vec{b}-\vec{a}) : g \circ f(\vec{t}) = \vec{w}} P'_{\text{in}}(\vec{t}), \tag{32}$$

and $P'_{\text{in}}(\vec{t})$ *is normalized as*

$$P'_{\text{in}}(\vec{t}) = \frac{P_{\text{in}}(\vec{t})}{\sum_{\vec{t} \in D(\vec{b}-\vec{a})} P_{\text{in}}(\vec{t})}.$$

Proof. After steps (1)–(4) of our distillation protocol, from the linearity of the measurement and the error correction, the input state ρ_{in} becomes

$$\rho' = \sum_{\vec{t} \in D(\vec{b}-\vec{a})} P'_{\text{in}}(\vec{t})(I_{p^k} \otimes \mathsf{XZ}^n(f(\vec{t}))|\phi(\vec{a})\rangle\langle\phi(\vec{a})|I_{p^k} \otimes \mathsf{XZ}^n(f(\vec{t}))^*).$$

After applying the inverse of the encoding operator, the state ρ' becomes

$$\rho_{\text{out}} = \sum_{\vec{t}\in D(\vec{b}-\vec{a})} P'_{\text{in}}(\vec{t})|\beta^k(g\circ f(\vec{t}))\rangle\langle\beta^k(g\circ f(\vec{t}))| \tag{33}$$

$$= \sum_{\vec{w}\in\mathbf{Z}_p^{2k}} P_{\text{out}}(\vec{w})|\beta^k(\vec{w})\rangle\langle\beta^k(\vec{w})|, \tag{34}$$

where $P_{\text{out}}(\vec{w})$ is given by

$$P_{\text{out}}(\vec{w}) = \sum_{\vec{t}\in D(\vec{b}-\vec{a}):g\circ f(\vec{t})=\vec{w}} P'_{\text{in}}(\vec{t}).$$

□

When the input of EDPs are the probabilistic mixture of Bell states, the performance of the distillation protocol only depends on the coefficients $P_{\text{out}}(\vec{w})$ of the output of the protocol. Hereafter, we fix the stabilizer S and the error correction process $f(\cdot)$.

Definition 13. *For two stabilizer-based EDPs constructed from encoding operators U_e and V_e, respectively, let the mapping g_U be determined by U_e in equation (29) and g_V be determined by V_e in equation (29). If $g_U(\cdot) = g_V(\cdot)$, then we define two encoding operators U_e and V_e are similar and denote it by $U_e \sim V_e$.*

Theorem 3. *For two stabilizer-based EDPs constructed from encoding operators U_e and V_e respectively, let*

$$\rho_{\text{out},U_e} = \sum_{\vec{w}\in\mathbf{Z}_p^{2k}} P_{\text{out},U_e}(\vec{w})|\beta^k(\vec{w})\rangle\langle\beta^k(\vec{w})|$$

and

$$\rho_{\text{out},V_e} = \sum_{\vec{w}\in\mathbf{Z}_p^{2k}} P_{\text{out},V_e}(\vec{w})|\beta^k(\vec{w})\rangle\langle\beta^k(\vec{w})|$$

be output states of each protocols when inputs of each protocol are equation (31). If $U_e \sim V_e$, then we have

$$P_{\text{out},U_e}(\vec{w}) = P_{\text{out},V_e}(\vec{w}) \quad \forall\vec{w}\in\mathbf{Z}_p^{2k}, \tag{35}$$

i.e., performances of two protocols are the same.

Proof. From equation (32) and the fact that $g_U(\cdot) = g_V(\cdot)$, for any $\vec{w}\in\mathbf{Z}_p^{2k}$

$$P_{\text{out},U_e}(\vec{w}) = \sum_{\vec{t}\in D(\vec{b}-\vec{a}):g_U\circ f(\vec{t})=\vec{w}} P'_{\text{in}}(\vec{t})$$

$$= \sum_{\vec{t}\in D(\vec{b}-\vec{a}):g_V\circ f(\vec{t})=\vec{w}} P'_{\text{in}}(\vec{t}) = P_{\text{out},V_e}(\vec{w}).$$

□

Theorem 4. *If equation (35) holds for any input state of the form in equation (31), then $U_e \sim V_e$.*

Proof. We prove the contraposition of this statement, i.e., if $U_e \not\sim V_e$, then equation (35) does not hold for some input states. Since $g_U(\cdot) \neq g_V(\cdot)$, there exists $\vec{u}\in C^\perp$ such that $g_U(\vec{u}) \neq g_V(\vec{u})$. Consider the following input state. Let

$$P_{\text{in}}(\vec{t}) = \begin{cases} \dfrac{1}{\left|\left\{\vec{s}\in\mathbf{Z}_p^{2n} \;\middle|\; f(\vec{s})=\vec{u}\right\}\right|} & \text{if } f(\vec{t})=\vec{u} \\ 0 & \text{if } f(\vec{t})\neq\vec{u} \end{cases}$$

Then we have

$$P_{\mathrm{out},U_e}(\vec{w}) = \begin{cases} 1 & \text{if } \vec{w} = g_U(\vec{u}) \\ 0 & \text{if } \vec{w} \neq g_U(\vec{u}), \end{cases} \qquad P_{\mathrm{out},V_e}(\vec{w}) = \begin{cases} 1 & \text{if } \vec{w} = g_V(\vec{u}) \\ 0 & \text{if } \vec{w} \neq g_V(\vec{u}), \end{cases}$$

and equation (35) does not hold. □

3.3. Enumeration of equivalence classes of encoding operators

Classify $\mathcal{M}_g(S)$ into equivalence classes by $\sim$, and denote the representative set of the equivalence classes by $\widehat{\mathcal{M}}_g(S)$. In this section, we show how to enumerate all elements of $\widehat{\mathcal{M}}_g(S)$ in theorem 5.

Lemma 8. *Let two encoding operators U_e and V_e be constructed from $\{\vec{\xi}_{n-k+1}, \ldots, \vec{\xi}_n, \vec{\eta}_{n-k+1}, \ldots, \vec{\eta}_n\}$ and $\{\vec{\xi}'_{n-k+1}, \ldots, \vec{\xi}'_n, \vec{\eta}'_{n-k+1}, \ldots, \vec{\eta}'_n\}$ respectively and the other parameters (a) $\theta_x(\cdot)$, (b) $\vec{\eta}_1, \ldots, \vec{\eta}_{n-k}$ and (c) $Q_{\min}(\vec{0})$ be the same. Further assume that $\vec{\xi}_i \equiv \vec{\xi}'_i \pmod{C}$ for all $n-k+1 \leqslant i \leqslant n$ and $\vec{\eta}_i \equiv \vec{\eta}'_i \pmod{C}$ for all $n-k+1 \leqslant i \leqslant n$. Then $U_e \sim V_e$.*

Proof. Let g_U, G_U, and H_U be determined by U_e in equation (29), and g_V, G_V and H_V be determined by V_e in equation (29). For any vector $\vec{u} \in C^{\perp}$, we have

$$\vec{u} = \vec{\ell} G_U + \vec{m} H_U + \vec{v} = \vec{\ell} G_V + \vec{m} H_V + \vec{v}' \quad \exists \vec{v}, \vec{v}' \in C.$$

Thus, we have

$$g_U(\vec{u}) = g_V(\vec{u}) \quad \forall \vec{u} \in C^{\perp}.$$

and $U_e \sim V_e$. □

Lemma 9. *Let two encoding operators U_e and V_e be constructed from $\{\vec{\xi}_{n-k+1}, \ldots, \vec{\xi}_n, \vec{\eta}_{n-k+1}, \ldots, \vec{\eta}_n\}$ and $\{\vec{\xi}'_{n-k+1}, \ldots, \vec{\xi}'_n, \vec{\eta}'_{n-k+1}, \ldots, \vec{\eta}'_n\}$ respectively and the other parameters (a). $\theta_x(\cdot)$, (b). $\vec{\eta}_1, \ldots, \vec{\eta}_{n-k}$ and (c). $Q_{\min}(\vec{0})$ are the same. If $g_U(\cdot) = g_V(\cdot)$, i.e., $U_e \sim V_e$, then $\vec{\xi}_i \equiv \vec{\xi}'_i \pmod{C}$ for all $n-k+1 \leqslant i \leqslant n$ and $\vec{\eta}_i \equiv \vec{\eta}'_i \pmod{C}$ for all $n-k+1 \leqslant i \leqslant n$.*

Proof. For $\vec{u} \in C^{\perp}$ such that

$$g_U(\vec{u}) = g_V(\vec{u}) = (\vec{f}_i | \vec{0}) \in \mathbf{Z}_p^{2k},$$

from equation (29), we have

$$\vec{u} = \vec{\xi}_i + \vec{v} = \vec{\xi}'_i + \vec{v}' \quad \exists \vec{v}, \vec{v}' \in C.$$

Thus, we have

$$\vec{\xi}_i - \vec{\xi}'_i = \vec{v} - \vec{v}' \in C,$$

which means $\vec{\xi}_i \equiv \vec{\xi}'_i \pmod{C}$ for $n-k+1 \leqslant i \leqslant n$. Similarly, for $\vec{u} \in C^{\perp}$ such that

$$g_U(\vec{u}) = g_V(\vec{u}) = (\vec{0} | \vec{f}_i) \in \mathbf{Z}_p^{2k},$$

from equation (29), we have

$$\vec{u} = \vec{\eta}_i + \vec{v} = \vec{\eta}'_i + \vec{v}' \quad \exists \vec{v}, \vec{v}' \in C.$$

Thus, we have

$$\vec{\eta}_i - \vec{\eta}'_i = \vec{v} - \vec{v}' \in C,$$

which means $\vec{\eta}_i \equiv \vec{\eta}'_i \pmod{C}$ for $n-k+1 \leqslant i \leqslant n$. □

Definition 14. *Let $\vec{x}+C$ and $\vec{y}+C$ be elements of the coset $C^{\perp}/C$. Define a symplectic inner product of $\vec{x}+C$ and $\vec{y}+C$ as*

$$\langle \vec{x}+C, \vec{y}+C\rangle = \langle \vec{x}, \vec{y}\rangle. \tag{36}$$

Note that this inner product does not depend on choices of a representative $\vec{x}$ of $\vec{x}+C$ or $\vec{y}$ of $\vec{y}+C$.

Lemma 10. *The linear space $C^{\perp}/C$ is a $2k$-dimensional symplectic space with respect to the symplectic inner product in equation (36), and $\{\vec{\xi}_{n-k+1}+C, \ldots, \vec{\xi}_n+C, \vec{\eta}_{n-k+1}+C, \ldots, \vec{\eta}_n+C\}$ form a hyperbolic basis of $C^{\perp}/C$.*

Proof. It is easy to check that $\{\vec{\xi}_{n-k+1}+C, \ldots, \vec{\xi}_n+C, \vec{\eta}_{n-k+1}+C, \ldots, \vec{\eta}_n+C\}$ form a basis of $C^{\perp}/C$. From equations (4), we have

$$\langle \vec{\xi}_i+C, \vec{\eta}_j+C\rangle = \delta_{ij}, \qquad \langle \vec{\xi}_i+C, \vec{\xi}_j+C\rangle = 0, \qquad \langle \vec{\eta}_i+C, \vec{\eta}_j+C\rangle = 0$$

for $i, j \in \{n-k+1, \ldots, n\}$. □

As a consequence of lemmas 8 and 9, we have the following theorem.

Theorem 5. *There is one-to-one correspondence between elements of $\widehat{\mathcal{M}}_g(S)$ and choices of hyperbolic bases of $C^{\perp}/C$ with respect to the inner product in equation (36). Specifically, if two encoding operators U_e and V_e are different only by (a) $\theta_x(\cdot)$, (b) $\vec{\eta}_1, \ldots, \vec{\eta}_{n-k}$, or (c) $Q_{\min}(\vec{0})$, then $U_e \sim V_e$. Two encoding operators U_e and V_e are $U_e \sim V_e$ if and only if $\vec{\xi}_i \equiv \vec{\xi}_i' \pmod{C}$ for all $n-k+1 \leqslant i \leqslant n$ and $\vec{\eta}_i \equiv \vec{\eta}_i' \pmod{C}$ for all $n-k+1 \leqslant i \leqslant n$, i.e., two hyperbolic bases $\{\vec{\xi}_{n-k+1}+C, \ldots, \vec{\xi}_n+C\ \vec{\eta}_{n-k+1}+C, \ldots, \vec{\eta}_n+C\}$ and $\{\vec{\xi}_{n-k+1}'+C, \ldots, \vec{\xi}_n'+C\ \vec{\eta}_{n-k+1}'+C, \ldots, \vec{\eta}_n'+C\}$ of $C^{\perp}/C$ are equal (lemmas 8 and 9).*

Remark 4. When the input of the protocol is a probabilistic mixture of Bell states, we can find the best stabilizer-based EDP as follows. For a given parameter n and k, find appropriate values for the following parameters.

(i) a stabilizer S: a self-orthogonal subspace $C \subset \mathbf{Z}_p^{2n}$.
(ii) decision rule whether or not to abort the protocol in step (iv): a set $T \subset \mathbf{Z}_p^{n-k}$.
(iii) error correction process: mapping $f(\cdot)$ from $\mathbf{Z}_p^{2n}$ to $C^{\perp}$.
(iv) an equivalence class of encoding operator: a hyperbolic basis of $C^{\perp}/C$.

Remark 3 and theorem 5 significantly reduce the number of candidates of good EDPs. Indeed, for a given parameter n and k, we enumerate $(n-k)$-dimensional self-orthogonal subspaces C (enumerating stabilizers S) and all hyperbolic bases of $C^{\perp}/C$ for each C (enumerating the equivalence classes of encoding operators), instead of all hyperbolic bases of $\mathbf{Z}_p^{2n}$ (enumerating stabilizers S and all encoding operators). The number of all hyperbolic bases of $\mathbf{Z}_p^{2n}$ is equal to the cardinality of the set of symplectic mappings on $\mathbf{Z}_p^{2n}$, i.e., $|\mathrm{Sp}_{2n}(\mathbf{Z}_p)| = p^{n^2}\prod_{i=1}^{n}(p^{2i}-1)$ [22, theorem 3.1.2]. While, the number of $(n-k)$-dimensional self-orthogonal subspace of $\mathbf{Z}_p^{2n}$ is $\prod_{i=0}^{n-k-1}(p^{2n-i}-p^i)/(p^{n-k}-p^i)$ (see remark 5), and the number of all hyperbolic bases of $C^{\perp}/C$ is equal to $|\mathrm{Sp}_{2k}(\mathbf{Z}_p)| = p^{k^2}\prod_{i=1}^{k}(p^{2i}-1)$. Thus the number of candidates of EDPs is reduced by $1/\{p^{n^2-k^2}\prod_{i=1}^{n-k}(p^i-1)\}$. For example, the number of candidates of EDPs is reduced by $1/12288$ when $n=4, k=2$ and $p=2$. Note that the number of permutation-based EDPs [7] for a given parameter n, k and p is also same as the number of all hyperbolic bases of $\mathbf{Z}_p^{2n}$.

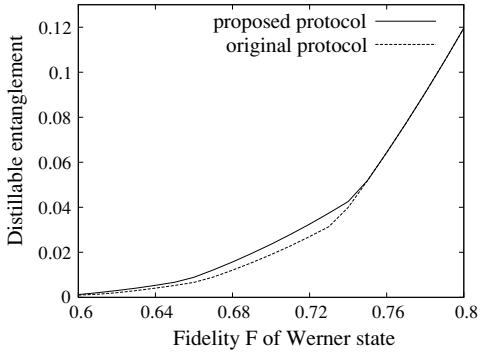

Figure 1. Comparison of the performance between the proposed protocol and the protocol originally proposed in [20].

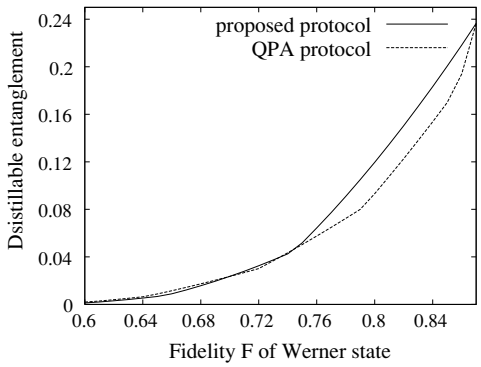

Figure 2. Comparison of the performance between the proposed protocol and the QPA protocol.

Remark 5. The number of $(n-k)$-dimensional self-orthogonal subspace of $\mathbf{Z}_p^{2n}$ is the number of $n-k$ mutually orthonormal vectors $\prod_{i=0}^{n-k-1}(p^{2n-i}-p^i)$ divided by the number of bases of the $(n-k)$-dimensional self-orthogonal subspace $\prod_{i=0}^{n-k-1}(p^{n-k}-p^i)$.

4. EDP with good performance

We can improve the performance of the protocol proposed in [20] by choosing an optimal encoding operator. The improved protocol has the best performance over the range of fidelity greater than 0.6 for a parameter $n=4, k=2, p=2$ and $T=\{\vec{0}\}$. Note that there is no choice of error correction process when $T=\{\vec{0}\}$. We calculated the performance by using the protocol appropriate times iteratively followed by the hashing protocol. The performance is plotted in figure 1 and is compared to the performance of the protocol in [20]. The proposed protocol is also compared to the performance of the QPA protocol in figure 2, and has a better performance than the QPA protocol over the wide range of fidelity. We remark that the QPA protocol has the best performance among EDPs constructed from [[2, 1]] stabilizer codes.

The proposed protocol is constructed from a stabilizer code with a stabilizer

$$S=\{X\otimes X\otimes X\otimes X, Z\otimes Z\otimes Z\otimes Z\}.$$

The encoding operator is constructed as follows. The vector representation of the stabilizer is

$$\vec{\xi}_1 = (1111|0000), \qquad \vec{\xi}_2 = (0000|1111).$$

Then we choose $\vec{\xi}_3, \vec{\xi}_4$ and $\vec{\eta}_1, \ldots, \vec{\eta}_4$ to be

$$\begin{aligned} \vec{\xi}_3 &= (1100|0000), & \vec{\xi}_4 &= (1010|0000), \\ \vec{\eta}_1 &= (0000|1110), & \vec{\eta}_2 &= (1110|0000), \\ \vec{\eta}_3 &= (0000|1010), & \vec{\eta}_4 &= (1010|1100). \end{aligned}$$

We choose

$$\begin{aligned} \widetilde{\mathsf{X}}^4(\vec{f}_1) &= Z \otimes Z \otimes Z \otimes I_2 & \widetilde{\mathsf{X}}^4(\vec{f}_2) &= X \otimes X \otimes X \otimes I_2 \\ \widetilde{\mathsf{X}}^4(\vec{f}_3) &= Z \otimes I_2 \otimes Z \otimes I_2 & \widetilde{\mathsf{X}}^4(\vec{f}_4) &= \mathbf{i}XZ \otimes Z \otimes X \otimes I_2 \end{aligned}$$

and

$$\begin{aligned} \widetilde{\mathsf{Z}}^4(\vec{f}_1) &= X \otimes X \otimes X \otimes X & \widetilde{\mathsf{Z}}^4(\vec{f}_2) &= Z \otimes Z \otimes Z \otimes Z \\ \widetilde{\mathsf{Z}}^4(\vec{f}_3) &= X \otimes X \otimes I_2 \otimes I_2 & \widetilde{\mathsf{Z}}^4(\vec{f}_4) &= X \otimes I_2 \otimes X \otimes I_2. \end{aligned}$$

We choose one of joint eigenspaces $Q(\vec{0})$ spanned by

$$\{|0000\rangle + |1111\rangle, |0011\rangle + |1100\rangle, |1001\rangle + |0110\rangle, |0101\rangle + |1010\rangle\},$$

and choose $Q_{\min}(\vec{0})$ as

$$Q_{\min}(\vec{0}) = \{|0000\rangle + |1111\rangle + |0011\rangle + |1100\rangle + |1001\rangle + |0110\rangle + |0101\rangle + |1010\rangle\}.$$

5. Conclusion

In this paper, we showed a method for enumerating all encoding operators in the Clifford group for a given stabilizer code systematically. We further classified those encoding operators into equivalence classes such that EDPs constructed from encoding operators in the same equivalence class have the same performance when the input of EDPs is a probabilistic mixture of Bell states. By this classification, we can search EDPs with good performances efficiently. As a result, we found the best EDP among EDPs constructed from [[4, 2]] stabilizer codes. Although in this paper we employed $T = \{\vec{0}\}$, i.e., we abort the protocol if Alice and Bobs' measurement outcomes disagree, performances of stabilizer EDPs may be improved by employing $T \neq \{\vec{0}\}$, i.e., we decide whether to abort or perform the error correction according to the difference of Alice and Bobs' measurement outcome. Exploring the potential of $T \neq \{\vec{0}\}$ is a future research agenda.

For a general two-way EDP, the distillable entanglement is upper bounded by the relative entropy of entanglement [24, 26]. We do not know what rate is achievable by using an optimal stabilizer code and an optimal encoding operator. It is also not clear how much performance is improved by using an optimal encoding operator for a fixed stabilizer. Evaluating the performance analytically is also a future research agenda.

Acknowledgments

This research is in part supported by International Communication Foundation, Japan. The authors deeply acknowledge the financial support.

References

[1] Ambainis A and Gottesman D 2006 The minimum distance problem for two-way entanglement purification *IEEE Trans. Inform. Theor.* **52** 748–53 (*Preprint* quant-ph/0310097v2)

[2] Artin E 1957 *Geometric Algebra* (New York: Interscience)

[3] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 Purification of noisy entanglement and faithful teleportation via noisy channels *Phys. Rev. Lett.* **76** 722–5 (*Preprint* quant-ph/9511027)

[4] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction *Phys. Rev.* A **54** 3824–51 (*Preprint* quant-ph/9604024)

[5] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1997 Quantum error correction and orthogonal geometry *Phys. Rev. Lett.* **78** 405–8 (*Preprint* quant-ph/9605005)

[6] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1998 Quantum error correction via codes over GF(4) *IEEE Trans. Inform. Theor.* **44** 1369–87 (*Preprint* quant-ph/9608006)

[7] Dehaene J, Nest M V D and Moor B D 2003 Local permutations of products of Bell states and entanglement distillation *Phys. Rev.* A **67** 022310 (*Preprint* quant-ph/0207154)

[8] Dehaene J and Moor B D 2003 Clifford group, stabilizer states, and linear quadratic operations over $GF(2)$ *Phys. Rev.* A **68** 042318 (*Preprint* quant-ph/0304125)

[9] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1998 Quantum privacy amplification and the security of quantum cryptography over noisy channels *Phys. Rev. Lett.* **80** 2022 (*Preprint* quant-ph/9604039)

[10] Gottesman D 1996 Class of quantum error-correcting codes saturating the quantum Hamming bound *Phys. Rev.* A **54** 1862–68 (*Preprint* quant-ph/9604038)

[11] Gottesman D 1998 Theory of fault-tolerant quantum computation *Phys. Rev.* A **57** 127–37 (*Preprint* quant-ph/9702029)

[12] Gottesman D 1998 Fault-tolerant quantum computation with higher-dimensional systems *Preprint* quant-ph/9802007v2

[13] Gottesman D 1998 The Heisenberg representation of quantum computers *Preprint* quant-ph/9807006

[14] Gottesman D 1997 Stabilizer codes and quantum error correction *Caltech PhD Thesis* (*Preprint* quant-ph/9705052)

[15] Gottesman D and Lo H K 2003 Proof of security of quantum key distribution with two-way classical communications *IEEE Trans. Inform. Theor.* **49** 457–75 (*Preprint* quant-ph/0105121)

[16] Hamada M 2003 Notes on the fidelity of symplectic quantum error-correcting codes *Int. J. Quantum Infor.* **1** pp 443–63 (*Preprint* quant-ph/0311003)

[17] Hostens E, Dehaene J and Moor B D 2005 Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic *Phys. Rev.* A **71** 042315 (*Preprint* quant-ph/0408190)

[18] Hostens E, Dehaene J and Moor B D 2004 The equivalence of two approaches to the design of entanglement distillation protocol *Preprint* quant–ph/0406017

[19] Knill E 1996 Non-binary unitary error bases and quantum codes *Preprint* quant-ph/9608048

[20] Matsumoto R 2003 Conversion of a general quantum stabilizer code to an entanglement distillation protocol *J. Phys. A: Math. Gen.* **36** 8113–27 (*Preprint* quant-ph/0209091)

[21] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[22] O'Meara O T 1978 Symplectic groups *Mathematical Surveys* vol 16 (Providence, RI: American Mathematical Society)

[23] Rains E M 1999 Nonbinary quantum codes *IEEE Trans. Inform. Theor.* **45** 1827–32 (*Preprint* quant-ph/9703048)

[24] Rains E M 2001 A semidefinite program for distillable entanglement *IEEE Trans. Inform. Theor.* **47** 2921–33 (*Preprint* quant-ph/0008047)

[25] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4 (*Preprint* quant-ph/0003004)

[26] Vedral V and Plenio M B 1998 Entanglement measures and purification procedures *Phys. Rev.* A **57** 1619–33 (*Preprint* quant-ph/9707035)