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

J. Phys. A: Math. Gen. **36** (2003) 8113–8127 PII: S0305-4470(03)61762-2

Conversion of a general quantum stabilizer code to an entanglement distillation protocol*

Ryutaroh Matsumoto

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

E-mail: ryutaroh@rmatsumoto.org

Received 4 April 2003
Published 8 July 2003
Online at stacks.iop.org/JPhysA/36/8113

Abstract

We show how to convert a quantum stabilizer code to a one- or two-way entanglement distillation protocol. The proposed conversion method is a generalization of those of Shor–Preskill and Nielsen–Chuang. The recurrence protocol and the quantum privacy amplification protocol are equivalent to the protocols converted from [[2, 1]] stabilizer codes. We also give an example of a two-way protocol converted from a stabilizer better than the recurrence protocol and the quantum privacy amplification protocol. The distillable entanglement by the class of one-way protocols converted from stabilizer codes for a certain class of states is equal to or greater than the achievable rate of stabilizer codes over the channel corresponding to the distilled state, and they can distill asymptotically more entanglement from a very noisy Werner state than the hashing protocol.

PACS numbers: 03.67.Pp, 03.67.Mn, 03.67.Hk, 89.70.+c

1. Introduction

In many applications of quantum mechanics to communication, the sender and the receiver have to share a maximally entangled quantum state of two particles. When there is a noiseless quantum communication channel, the sender can send one of two particles in a maximally entangled state to the receiver and sharing of it is easily accomplished. However, the quantum communication channel is usually noisy, that is, the quantum state of the received particle changes probabilistically from the original state of a particle.

Entanglement distillation protocols [2] and quantum error-correcting codes [16, 18] are the schemes for sharing a maximally entangled state over a noisy communication channel.

* A one page abstract of this paper appeared in the Proceedings of 2003 IEEE International Symposium on Information Theory.

A distillation protocol is said to be *two-way* (resp. *one-way*) if it involves two-way (resp. one-way) classical communication. Two-way protocols have larger distillation ability than one-way protocols. However, few two-way protocols have been proposed so far, namely the recurrence protocol [2] and the quantum privacy amplification protocol (QPA protocol) [6]. There may be many two-way protocols better than existing ones, and the discovery of better protocols has been awaited.

Immediately after the proposal of those schemes, Bennett *et al* discovered that one can construct a *one-way* entanglement distillation protocol from a quantum code [3, section V.C], which requires $2n$ additional qubits where n is the number of noisy entangled states to be distilled. Nielsen and Chuang [12, exercise 12.34] observed a construction method of a one-way protocol without extra qubits from a real binary quantum stabilizer code as a generalization of the idea in [17].

By a conversion method from a quantum code to a distillation protocol, we can solve problems of distillation protocols from results in quantum codes. For example, we can construct a good distillation protocol from a good quantum code. Thus such a conversion method deserves further investigation.

It is not known how one can convert a quantum error-correcting code to a *two-way* entanglement distillation protocol. We shall propose a conversion method from an arbitrary quantum stabilizer code to both one- and two-way entanglement distillation protocols as a generalization of Shor and Preskill [17], Nielsen and Chuang [12]. Benefits of the proposed conversion methods are

- We can construct infinitely many two-way protocols. One can easily construct a two-way protocol better than the recurrence protocol and the QPA protocol from a simple stabilizer code (see section 4.2).
- It is known that one-way protocols and quantum error-correcting codes without classical communication have the same ability of sharing maximally entangle states over a noisy quantum channel [3]. The proposed protocols might be used for further clarification of the relation between distillation protocols and quantum error-correcting codes.

This paper is organized as follows: in section 2, basic notation is introduced. In section 3, we present a construction of entanglement distillation protocols from quantum stabilizer codes. In section 4, we give examples of converted protocols equivalent to the recurrence protocol and the QPA protocol, and an example better than them. In section 5, we evaluate the distillable entanglement by the class of one-way protocols converted from stabilizer codes, and show that the converted protocols can distill asymptotically more entanglement from a noisy Werner state than the hashing protocol [3]. In section 6, we derive a lower bound on fidelity with a general initial state of protocols.

2. Notation

In this section, we fix notation and the problem formulation. Let H_A and H_B be p-dimensional complex linear spaces with orthonormal bases $\{|0_A\rangle, \ldots, |(p-1)_A\rangle\}$ and $\{|0_B\rangle, \ldots, |(p-1)_B\rangle\}$, respectively, where p is a prime number. We shall restrict ourselves to p-ary stabilizer codes because an m-ary stabilizer code can be constructed as a tensor product of p_i-ary stabilizer codes [14, p 1831, remarks], where p_i are prime divisors of m, and extension of the proposed conversion method to the m-ary case is straightforward. We define the maximally entangled states in $H_A \otimes H_B$ by

$$|\beta(a,b)\rangle = I \otimes X^a Z^b \frac{1}{\sqrt{p}} \sum_{i=0}^{p-1} |i_A i_B\rangle$$

where $a, b \in \{0, \ldots, p-1\}$, and matrices X and Z are defined by

$$X|i\rangle = |i+1 \bmod p\rangle \qquad Z|i\rangle = \omega^i |i\rangle$$

with a complex primitive pth root ω of 1. The matrices X, Z and their commutation relation were first applied to quantum mechanics by Weyl [20, section 4.15]. Suppose that Charlie prepares n pairs of particles in the state $|\beta(0,0)\rangle$, sends the particles corresponding to H_A to Alice, and sends the other particles corresponding to H_B to Bob. The quantum channels between Alice and Charlie and between Bob and Charlie are noisy in general, and Alice and Bob share a mixed state $\rho \in \mathcal{S}(H_A^{\otimes n} \otimes H_B^{\otimes n})$, where $\mathcal{S}(H_A^{\otimes n} \otimes H_B^{\otimes n})$ is the set of density operators on $H_A^{\otimes n} \otimes H_B^{\otimes n}$. The state ρ can be an arbitrary density operator. The goal of an entanglement distillation protocol is to extract as many pairs of particles with state close to $|\beta(0,0)\rangle$ as possible from n pairs of particles in the state ρ.

3. Protocol

In this section, we shall describe how to make an entanglement distillation protocol from a quantum stabilizer code. In the protocol, we extract a state $\tau \in \mathcal{S}(H_A^{\otimes k} \otimes H_B^{\otimes k})$ from $\rho \in \mathcal{S}(H_A^{\otimes n} \otimes H_B^{\otimes n})$.

The proposed protocol will be constructed from the nonbinary generalization [11, 14] of quantum stabilizer codes [4, 5, 8]. We assume that the reader is familiar with the formalism of the nonbinary stabilizer code. Let us introduce the notation of stabilizer codes. Let $E = \{\omega^i X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} : a_1, b_1, \ldots, a_n, b_n, i \text{ are integers}\}$, and S a commutative subgroup of E. The subgroup S is called a stabilizer.

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

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

Suppose that $\{\mathsf{XZ}(\vec{g}_1), \ldots, \mathsf{XZ}(\vec{g}_{n-k})$ (and possibly some power of ωI) $\}$ is a generating set of the group S, where $\vec{g}_1, \ldots, \vec{g}_{n-k}$ are linearly independent of $\mathbf{Z}_p$.

Let H be a complex linear space with the orthonormal basis $\{|0\rangle, \ldots, |p-1\rangle\}$, and hereafter we shall identify H with H_A and H_B by linear maps $|i\rangle \mapsto |i_A\rangle$ and $|i\rangle \mapsto |i_B\rangle$. Let Q be a stabilizer code defined by S, that is, a joint eigenspace of S in $H^{\otimes n}$. There are many joint eigenspaces of S and we can distinguish an eigenspace by its eigenvalue of $\mathsf{XZ}(\vec{g}_i)$ for $i = 1, \ldots, n-k$. Hereafter, we fix a joint eigenspace Q of S and suppose that Q belongs to the eigenvalue λ_i of $\mathsf{XZ}(\vec{g}_i)$ for $i = 1, \ldots, n-k$.

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

$$\langle \vec{g}_i, \vec{e} \rangle = \sum_{i=1}^{n} b_i c_i - a_i d_i \tag{1}$$

for $\vec{g}_i = (a_1, b_1, \ldots, a_n, b_n)$ and $\vec{e} = (c_1, d_1, \ldots, c_n, d_n)$.

We define $\vec{g}_i^\star = (a_1, -b_1, \ldots, a_n, -b_n)$. Since the complex conjugate of ω is ω^{-1}, we can see that $\mathsf{XZ}(\vec{g}_i^\star)$ is a componentwise complex conjugated matrix of $\mathsf{XZ}(\vec{g}_i)$. Let $S^\star$ be a subgroup of E generated by $\{\mathsf{XZ}(\vec{g}_1^\star), \ldots, \mathsf{XZ}(\vec{g}_{n-k}^\star)\}$. Easy computation shows that $S^\star$ is again commutative. So we can consider joint eigenspaces of $S^\star$. There exists a joint eigenspace $Q^\star$ of $S^\star$ whose eigenvalue of $\mathsf{XZ}(\vec{g}_i^\star)$ is $\bar{\lambda}_i$ (the complex conjugate of λ_i).

With this notation, our protocol is executed as follows:

(1) Alice measures an observable corresponding to $\mathsf{XZ}(\vec{g}_i^\star)$ 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*.
(2) Bob measures an observable corresponding to $\mathsf{XZ}(\vec{g}_i)$ 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*.
(3) Alice sends $(a_1, \ldots, a_{n-k})$ to Bob.
(4) Bob performs the error correction process according to $b_1 - a_1, \ldots, b_{n-k} - a_{n-k}$ as described below.
(5) Alice and Bob apply the inverse of encoding operators of the quantum stabilizer codes.
(6) Alice and Bob discard the last $n - k$ particles.
(7) If the difference of the measurement outcomes $(b_1 - a_1, \ldots, b_{n-k} - a_{n-k})$ indicates that the fidelity between the remaining k particles and $|\beta(0,0)\rangle^{\otimes k}$ is low, Bob discards all of his particles and he tells Alice the disposal of particles.

We shall introduce some notation. For a vector $\vec{u} \in \mathbf{Z}_p^{2n}$ let

$$|\beta(\vec{u})\rangle = (I \otimes \mathsf{XZ}(\vec{u}))|\beta(0,0)\rangle^{\otimes n}.$$

Let $Q(\vec{x})$ [resp $Q^\star(\vec{x})$] $\subset H^{\otimes n} \simeq H_A^{\otimes n} \simeq H_B^{\otimes n}$ be the quantum stabilizer code of S (resp. $S^\star$) belonging to the eigenvalue $\lambda_i\omega^{x_i}$ (resp. $\bar{\lambda}_i\omega^{-x_i}$) of $\mathsf{XZ}(\vec{g}_i)$ (resp. $\mathsf{XZ}(\vec{g}_i^\star)$) for a vector $\vec{x} = (x_1, \ldots, x_{n-k}) \in \mathbf{Z}_p^{n-k}$, and $P(\vec{x})$ (resp. $P^\star(\vec{x})$) be the projection onto $Q(\vec{x})$ (resp. $Q^\star(\vec{x})$).

Lemma 1. *We have*

$$\{P^\star(\vec{x}) \otimes I\}|\beta(\vec{0})\rangle = \{P^\star(\vec{x}) \otimes P(\vec{x})\}|\beta(\vec{0})\rangle \tag{2}$$

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

Proof. Let $\{|0\rangle, \ldots, |p^n - 1\rangle\}$ be an orthonormal basis of $H^{\otimes n}$ consisting of tensor products of $\{|0\rangle, \ldots, |p-1\rangle\} \subset H$, and we have

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

For $\vec{x} \in \mathbf{Z}_p^{n-k}$, let $\{|\vec{x}, 0\rangle, \ldots, |\vec{x}, p^k - 1\rangle\}$ be an orthonormal basis of $Q(\vec{x})$. For a state

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

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 this notation, $\{\overline{|\vec{x}, 0\rangle}, \ldots, \overline{|\vec{x}, p^{n-k} - 1\rangle}\}$ is an orthonormal basis of $Q^\star(\vec{x})$. The set $\{|\vec{x}, i\rangle : \vec{x} \in \mathbf{Z}_p^{n-k}, i = 0, \ldots, p^k - 1\}$ is an orthonormal basis of $H^{\otimes n}$ and there exists a unitary matrix on $H^{\otimes n}$ that transforms the basis $\{|0\rangle, \ldots, |p^n - 1\rangle\}$ to $\{|\vec{x}, i\rangle : \vec{x} \in \mathbf{Z}_p^{n-k}, i = 0, \ldots, p^k - 1\}$. Let $\bar{U}$ be the componentwise complex conjugate of U, that is, $\bar{U}$ transforms $\{|0\rangle, \ldots, |p^n - 1\rangle\}$ to $\{\overline{|\vec{x}, i\rangle} : \vec{x} \in \mathbf{Z}_p^{n-k}, i = 0, \ldots, p^k - 1\}$. We have $\bar{U} \otimes U|\beta(\vec{0})\rangle = |\beta(\vec{0})\rangle$ [10]. Therefore

$$\sqrt{p^n}|\beta(\vec{0})\rangle = \sum_{\vec{x}\in\mathbf{Z}_p^{n-k}} \sum_{i=0}^{p^k-1} \overline{|\vec{x}, i\rangle} \otimes |\vec{x}, i\rangle.$$

Since

$$P^\star(\vec{x}) = \sum_{i=0}^{p^k-1} \overline{|\vec{x}, i\rangle\langle\vec{x}, i|}$$

we have

$$\begin{aligned}\sqrt{p^n}\{P^\star(\vec{x}) \otimes I\}|\beta(\vec{0})\rangle &= \left[\sum_{i=0}^{p^k-1} \overline{|\vec{x}, i\rangle}\,\overline{\langle\vec{x}, i|} \otimes I\right] \sum_{\vec{x}\in\mathbf{Z}_p^{n-k}} \sum_{i=0}^{p^k-1} \overline{|\vec{x}, i\rangle} \otimes |\vec{x}, i\rangle \\ &= \sum_{i=0}^{p^k-1} \overline{|\vec{x}, i\rangle} \otimes |\vec{x}, i\rangle \\ &= \sqrt{p^n}\{P^\star(\vec{x}) \otimes P(\vec{x})\}|\beta(\vec{0})\rangle. \qquad (3)\end{aligned}$$

□

Suppose that we perform the protocol above to the state $|\beta(\vec{u})\rangle = \{I \otimes \mathsf{XZ}(\vec{u})\}|\beta(\vec{0})\rangle$. After we get $\vec{a} = (a_1, \ldots, a_{n-k}) \in \mathbf{Z}_p^{n-k}$ as a measurement outcome in step 1, the state is

$$\begin{aligned}\{P^\star(\vec{a}) \otimes I\}\{I \otimes \mathsf{XZ}(\vec{u})\}|\beta(\vec{0})\rangle &= \{I \otimes \mathsf{XZ}(\vec{u})\}\{P^\star(\vec{a}) \otimes I\}|\beta(\vec{0})\rangle \\ &= \{I \otimes \mathsf{XZ}(\vec{u})\}\{P^\star(\vec{a}) \otimes P(\vec{a})\}|\beta(\vec{0})\rangle \qquad \text{(by equation (2))}.\end{aligned}$$

Observe that the vector $\{I \otimes \mathsf{XZ}(\vec{u})\}\{P^\star(\vec{a}) \otimes P(\vec{a})\}|\beta(\vec{0})\rangle$ belongs to $Q^\star(\vec{a}) \otimes Q(\vec{b})$, where

$$\vec{b} = \vec{a} + (\langle\vec{g}_1, \vec{u}\rangle, \ldots, \langle\vec{g}_{n-k}, \vec{u}\rangle).$$

Thus the measurement outcome in step 2 must be $\vec{b}$.

For simplicity of presentation, we assume that the state $\rho \in \mathcal{S}\left(H_A^{\otimes n} \otimes H_B^{\otimes n}\right)$ can be written as

$$\rho = \sum_{\vec{u}\in\mathbf{Z}_p^{2n}} \alpha(\vec{u})|\beta(\vec{u})\rangle\langle\beta(\vec{u})| \qquad (4)$$

where $\left\{\alpha(\vec{u}) : \vec{u} \in \mathbf{Z}_p^{2n}\right\}$ is a probability distribution. A general case will be treated in section 6.

After performing step 1 in the proposed protocol to state (4) and getting $\vec{a} \in \mathbf{Z}_p^{n-k}$ as a measurement outcome, the state is

$$\sum_{\vec{u}\in\mathbf{Z}_p^{2n}} \alpha(\vec{u})\{I \otimes \mathsf{XZ}(\vec{u})\}P(\vec{a}, \vec{a})\rho(\vec{0})P(\vec{a}, \vec{a})\{I \otimes \mathsf{XZ}(\vec{u})^*\}$$

where $P(\vec{a}, \vec{a}) = P^\star(\vec{a}) \otimes P(\vec{a})$ and $\rho(\vec{0}) = |\beta(\vec{0})\rangle\langle\beta(\vec{0})|$. Suppose that we get $\vec{b}$ as a measurement outcome in step 2, and denote $(b_1 - a_1, \ldots, b_{n-k} - a_{n-k})$ by $\vec{s}$. The state $\{I \otimes \mathsf{XZ}(\vec{u})\}P(\vec{a}, \vec{a})|\beta(\vec{0})\rangle$ belongs to $Q^\star(\vec{a}) \otimes Q[\vec{a} + (\langle\vec{g}_1, \vec{u}\rangle, \ldots, \langle\vec{g}_{n-k}, \vec{u}\rangle)]$. Thus the state after step 2 is

$$
\begin{aligned}
&\sum_{\vec{u}\in\mathbf{Z}_p^{2n}} \alpha(\vec{u})P(\vec{a},\vec{b})\{I\otimes \mathsf{XZ}(\vec{u})\}P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})\{I\otimes \mathsf{XZ}(\vec{u})^*\}P(\vec{a},\vec{b})\\
&\qquad = \sum_{\vec{u}\in D(\vec{s})} \alpha(\vec{u})P(\vec{a},\vec{b})\{I\otimes \mathsf{XZ}(\vec{u})\}P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})\{I\otimes \mathsf{XZ}(\vec{u})^*\}P(\vec{a},\vec{b})\\
&\qquad = \sum_{\vec{u}\in D(\vec{s})} \alpha(\vec{u})\{I\otimes \mathsf{XZ}(\vec{u})\}P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})\{I\otimes \mathsf{XZ}(\vec{u})\}
\end{aligned}
$$

where

$$D(\vec{s}) = \left\{\vec{u}\in\mathbf{Z}_p^{2n} : \langle\vec{g}_i,\vec{u}\rangle = b_i - a_i,\ \text{for each } i\right\}.$$

Let C be the linear subspace of $\mathbf{Z}_p^{2n}$ spanned by $\vec{g}_1,\ldots,\vec{g}_{n-k}$, and $C^\perp$ be the orthogonal space of C with respect to the symplectic inner product (1). For vectors $\vec{u},\vec{v}$ such that $\vec{u}-\vec{v}\in C$, $\mathsf{XZ}(\vec{u})$ and $\mathsf{XZ}(\vec{v})$ have the same effect on states in $Q(\vec{a})$ for any $\vec{a}$, and we can identify errors $\mathsf{XZ}(\vec{u})$ and $\mathsf{XZ}(\vec{v})$ if $\vec{u}-\vec{v}\in C$, which is equivalent to $\vec{v}\in\vec{u}+C$. Thus, among errors $\mathsf{XZ}(\vec{u})$ corresponding to $D(\vec{s})$, the most likely error vector $\vec{u}$ is one having maximum

$$\sum_{\vec{v}\in\vec{u}+C} \alpha(\vec{v})$$

in the set $D(\vec{s})$. Let $\vec{e}$ be the most likely error vector in $D(\vec{s})$. The set $D(\vec{s})$ is equal to

$$\vec{e}+C^\perp = \{\vec{e}+\vec{u} : \vec{u}\in C^\perp\}.$$

Bob applies $\mathsf{XZ}(\vec{e})^{-1}$ to his particles. This is step 4. After applying $\mathsf{XZ}(\vec{e})^{-1}$ to Bob's particles, the joint state of particles of Alice and Bob is

$$\sum_{\vec{u}\in\vec{e}+C^\perp} \alpha(\vec{u})\{I\otimes \mathsf{XZ}(\vec{u}-\vec{e})\}P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})\{I\otimes \mathsf{XZ}(\vec{u}-\vec{e})^*\}. \tag{5}$$

Recall that $\mathsf{XZ}(\vec{u}-\vec{e})$ does not change a state in $Q(\vec{a})$ if $\vec{u}-\vec{e}\in C$. Therefore, the state (5) is equal to

$$
\begin{aligned}
&\sum_{\vec{u}\in\vec{e}+C} \alpha(\vec{u})P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})\\
&\qquad + \sum_{\vec{u}\in\vec{e}+(C^\perp\setminus C)} \alpha(\vec{u})[I\otimes \mathsf{XZ}(\vec{u}-\vec{e})]P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})[I\otimes \mathsf{XZ}(\vec{u}-\vec{e})^*].
\end{aligned}
\tag{6}
$$

We shall explain how to use an encoding operator in step 5 to extract $|\beta(0,0)\rangle^{\otimes k}$ from the above state. Let $|\mathrm{a}\rangle\in H^{\otimes n-k}$ be an ancillary state. Consider an encoding operator U_e on $H^{\otimes n}$ sending $|i\rangle\otimes|\mathrm{a}\rangle\in H^{\otimes n}$ to $|\vec{a},i\rangle$ for $i=0,\ldots,p^k-1$, where $\{|\vec{a},0\rangle,\ldots,|\vec{a},p^k-1\rangle\}$ is an orthonormal basis of $Q(\vec{a})$ defined above. Observe that $\overline{U_\mathrm{e}}$ is an encoding operator for $Q^\star(\vec{a})$ sending $|i\rangle\otimes|\mathrm{a}\rangle\in H^{\otimes n}$ to $\overline{|\vec{a},i\rangle}$ for $i=0,\ldots,p^k-1$. Applying $\overline{U_\mathrm{e}}^{-1}\otimes U_\mathrm{e}^{-1}$ to state (5) yields

$$
\begin{aligned}
&\sum_{\vec{u}\in\vec{e}+C^\perp} \alpha(\vec{u})\big(\overline{U_\mathrm{e}}^{-1}\otimes U_\mathrm{e}^{-1}\big)[I\otimes \mathsf{XZ}(\vec{u}-\vec{e})]P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})[I\otimes \mathsf{XZ}(\vec{u}-\vec{e})^*](\overline{U_\mathrm{e}}\otimes U_\mathrm{e})\\
&\qquad = \sum_{\vec{u}\in\vec{e}+C} \alpha(\vec{u})\big(\overline{U_\mathrm{e}}^{-1}\otimes U_\mathrm{e}^{-1}\big)P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})(\overline{U_\mathrm{e}}\otimes U_\mathrm{e}) \quad \text{(by equation (6))}\\
&\qquad\quad + \sum_{\vec{u}\in\vec{e}+(C^\perp\setminus C)} \alpha(\vec{u})\big(\overline{U_\mathrm{e}}^{-1}\otimes U_\mathrm{e}^{-1}\big)[I\otimes \mathsf{XZ}(\vec{u}-\vec{e})]P(\vec{a},\vec{a})\rho(\vec{0})\\
&\qquad\quad \times P(\vec{a},\vec{a})[I\otimes \mathsf{XZ}(\vec{u}-\vec{e})^*](\overline{U_\mathrm{e}}\otimes U_\mathrm{e})
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{\vec{u}\in\vec{e}+C} \alpha(\vec{u})\left(\overline{U_{\mathrm{e}}}^{-1} \otimes U_{\mathrm{e}}^{-1}\right) \left[\frac{1}{p^n}\left\{\sum_{i=0}^{p^k-1} \overline{|\vec{a}, i\rangle} \otimes |\vec{a}, i\rangle\right\}\right.\\
&\quad \times \left.\left\{\sum_{i=0}^{p^k-1} \overline{\langle\vec{a}, i|} \otimes \langle\vec{a}, i|\right\}\right] (\overline{U_{\mathrm{e}}} \otimes U_{\mathrm{e}}) \qquad \text{(by equation (3))}\\
&\quad + \sum_{\vec{u}\in\vec{e}+(C^{\perp}\setminus C)} \alpha(\vec{u})\left(\overline{U_{\mathrm{e}}}^{-1} \otimes U_{\mathrm{e}}^{-1}\right)[I \otimes \mathsf{XZ}(\vec{u}-\vec{e})]P(\vec{a},\vec{a})\rho(\vec{0})\\
&\quad \times P(\vec{a},\vec{a})[I \otimes \mathsf{XZ}(\vec{u}-\vec{e})^{*}](\overline{U_{\mathrm{e}}} \otimes U_{\mathrm{e}})\\
&= \frac{1}{p^n}\sum_{\vec{u}\in\vec{e}+C} \alpha(\vec{u})\{|\beta(0,0)\rangle^{\otimes k} \otimes |\mathrm{a}\rangle^{\otimes 2}\}\{\langle\beta(0,0)|^{\otimes k}\\
&\quad \otimes \langle\mathrm{a}|^{\otimes 2}\} \qquad \text{(by definition of } U_{\mathrm{e}})\\
&\quad + \sum_{\vec{u}\in\vec{e}+(C^{\perp}\setminus C)} \alpha(\vec{u})\left(\overline{U_{\mathrm{e}}}^{-1} \otimes U_{\mathrm{e}}^{-1}\right)[I \otimes \mathsf{XZ}(\vec{u}-\vec{e})]P(\vec{a},\vec{a})\rho(\vec{0})\\
&\quad \times P(\vec{a},\vec{a})[I \otimes \mathsf{XZ}(\vec{u}-\vec{e})^{*}](\overline{U_{\mathrm{e}}} \otimes U_{\mathrm{e}}).
\end{aligned} \tag{7}
$$

Taking partial trace of the first term over the last $n-k$ qubits yields $|\beta(0,0)\rangle^{\otimes k}$, which is step 6.

Let τ_5 be the final state of step 5, that is, state (7), and τ_6 be the state after step 6. In step 7, Bob computes the fidelity between the state $|\beta(0,0)\rangle^{\otimes k}$ and τ_6 by using knowledge of $\vec{s}$ and $\{\alpha(\vec{u}) : \vec{u} \in \mathbf{Z}_p^{2n}\}$. $\mathrm{Tr}[\tau_5]$ is not 1 because τ_5 is a state after projection. We have

$$
\begin{aligned}
\mathrm{Tr}[\tau_6] = \mathrm{Tr}[\tau_5] &= \mathrm{Tr}[P(\vec{a},\vec{a})\rho(\vec{0})P(\vec{a},\vec{a})] \sum_{\vec{u}\in\vec{e}+C^{\perp}} \alpha(\vec{u})\\
&= \langle\beta(\vec{0})|P^{\star}(\vec{a}) \otimes I|\beta(\vec{0})\rangle \sum_{\vec{u}\in\vec{e}+C^{\perp}} \alpha(\vec{u}) \qquad \text{(by equation (2))}\\
&= \frac{1}{p^{n-k}} \sum_{\vec{u}\in\vec{e}+C^{\perp}} \alpha(\vec{u}) \qquad \text{(by equation (3))}.
\end{aligned}
$$

If the initial state is $|\beta(\vec{u})\rangle$ such that $\vec{u} \in \vec{e}+C$, we can get $(1/p^{n-k})|\beta(0,0)\rangle^{\otimes k}\langle\beta(0,0)|^{\otimes k}$ as τ_6. Therefore, we have

$$
\langle\beta(0,0)|^{\otimes k}\tau_6|\beta(0,0)\rangle^{\otimes k} \geqslant \frac{1}{p^{n-k}} \sum_{\vec{u}\in\vec{e}+C} \alpha(\vec{u}).
$$

Thus Bob estimates that the fidelity between $|\beta(0,0)\rangle^{\otimes k}$ and the normalized state of τ_6 is at least

$$
\frac{\sum_{\vec{u}\in\vec{e}+C} \alpha(\vec{u})}{\sum_{\vec{u}\in\vec{e}+C^{\perp}} \alpha(\vec{u})}. \tag{8}
$$

The value (8) varies according to $\vec{s} = (b_1 - a_1, \ldots, b_{n-k} - a_{n-k})$. If obtained difference $\vec{s}$ implies low fidelity, Bob discards all the particles and tell Alice of the disposal.

Note that if we include step 7 then the whole protocol needs two-way classical communication, but if we exclude step 7 then it needs only one-way classical communication.

When Alice and Bib do not execute step 7, the average of fidelity (8) should be considered instead of respective values of equation (8) for each difference $\vec{s}$ of measurement outcomes. The average of equation (8) is at least

$$\sum_{\vec{s}\in\mathbf{Z}_p^{n-k}} \sum_{\vec{u}\in\vec{e}(\vec{s})+C} \alpha(\vec{u}) \tag{9}$$

where $\vec{e}(\vec{s})$ is the guessed-error vector for a given difference $\vec{s}$ of measurement outcomes. This average fidelity (9) will be studied in sections 4 and 6.

4. Examples

In this section, we show how one can construct the well-known recurrence protocol and the QPA protocol from stabilizer codes, and give a two-way protocol constructed from a stabilizer better than the recurrence protocol and the QPA protocol.

4.1. The recurrence protocol and the QPA protocol

The recurrence protocol without twirling [2, step (A2)] has the same effect on any density operator on $H_A^{\otimes 2} \otimes H_B^{\otimes 2}$ as the proposed protocol with $p = 2, n = 2, k = 1$, the stabilizer S generated by $Z \otimes Z$, encoding operators $U_{\mathrm{e}}(+1) : (\alpha_0|0\rangle + \alpha_1|1\rangle)|\mathrm{a}\rangle \mapsto \alpha_0|00\rangle + \alpha_1|11\rangle$ for the code belonging to eigenvalue +1 of $Z \otimes Z$, $U_{\mathrm{e}}(-1) : (\alpha_0|0\rangle + \alpha_1|1\rangle)|\mathrm{a}\rangle \mapsto \alpha_0|01\rangle + \alpha_1|10\rangle$ for the code belonging to eigenvalue -1 of $Z \otimes Z$, and discarding particles in step 7 if $\vec{s} = (1) \in \mathbf{Z}_2^1$. This can be seen by a tedious but straightforward computation.

The QPA protocol [6] has the same effect as the protocol converted from the stabilizer S generated by $XZ \otimes XZ$, encoding operators $U_{\mathrm{e}}(+1) : (\alpha_0|0\rangle + \alpha_1|1\rangle)|\mathrm{a}\rangle \mapsto \alpha_0(|0\rangle - i|1\rangle)(|0\rangle + i|1\rangle) + \alpha_1(|0\rangle + i|1\rangle)(|0\rangle - i|1\rangle)$ for the code belonging to eigenvalue +1 of $XZ \otimes XZ$, $U_{\mathrm{e}}(-1) : (\alpha_0|0\rangle + \alpha_1|1\rangle)|\mathrm{a}\rangle \mapsto \alpha_0(|0\rangle - i|1\rangle)(|0\rangle - i|1\rangle) + \alpha_1(|0\rangle + i|1\rangle)(|0\rangle + i|1\rangle)$ for the code belonging to eigenvalue -1 of $XZ \otimes XZ$, and discarding particles in step 7 if $\vec{s} = (1) \in \mathbf{Z}_2^1$.

4.2. A better protocol

We shall compare the protocol constructed from the stabilizer generated by $\{X \otimes X \otimes X \otimes X, Z \otimes Z \otimes Z \otimes Z\}$ ($p = 2$) with the recurrence protocol and the QPA protocol in a similar way to [3, figure 8]. We discard particles in the protocol unless the measurement outcomes completely agree, i.e., $\vec{s} = (0, 0)$.

Encoding operators for the stabilizer codes belonging to the eigenvalue $(-1)^{s_1}$ of $X \otimes X \otimes X \otimes X$ and $(-1)^{s_2}$ of $Z \otimes Z \otimes Z \otimes Z$ are described in table 1.

Suppose that we have many copies of noisy entangled state

$$F|\beta(0,0)\rangle\langle\beta(0,0)| + \frac{1-F}{3}(|\beta(0,1)\rangle\langle\beta(0,1)| + |\beta(1,0)\rangle\langle\beta(1,0)| + |\beta(1,1)\rangle\langle\beta(1,1)|)$$

and we want to distill the Bell state $|\beta(0,0)\rangle\langle\beta(0,0)|$ as often as possible by using the hashing protocol and a two-way protocol chosen from the recurrence protocol *without twirling*, the QPA protocol, and the protocol constructed from $\{X \otimes X \otimes X \otimes X, Z \otimes Z \otimes Z \otimes Z\}$. We use the hashing protocol to distill the perfect Bell state $|\beta(0,0)\rangle\langle\beta(0,0)|$ after a suitable number of iterations of a two-way protocol as described in [3, section III.B.1].

The number of perfect Bell states distillable by the three two-way protocols are compared in figure 1. Observe that an example of the proposed protocol has larger distillable entanglement for the range of F between 0.75 and 0.87.

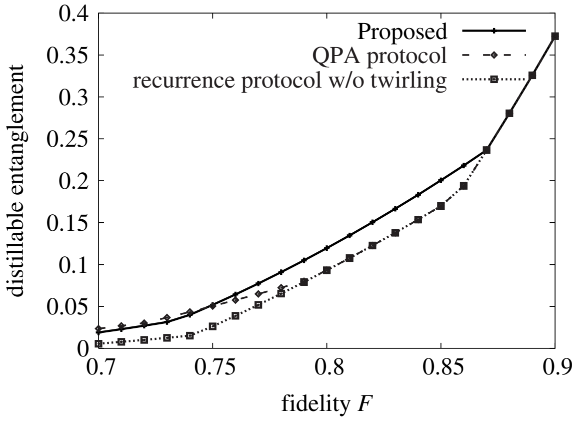

Figure 1. Comparison of two-way protocols.

Table 1. Encoding maps.

Eigenvalues	Encoding map
$(s_1, s_2) = (0, 0)$	$\|00\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0000\rangle + \|1111\rangle)$
	$\|01\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0011\rangle + \|1100\rangle)$
	$\|10\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0101\rangle + \|1010\rangle)$
	$\|11\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0110\rangle + \|1001\rangle)$
$(s_1, s_2) = (0, 1)$	$\|00\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0001\rangle + \|1110\rangle)$
	$\|01\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0010\rangle + \|1101\rangle)$
	$\|10\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0100\rangle + \|1011\rangle)$
	$\|11\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|1000\rangle + \|0111\rangle)$
$(s_1, s_2) = (1, 0)$	$\|00\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0000\rangle + \|1111\rangle)$
	$\|01\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0011\rangle + \|1100\rangle)$
	$\|10\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0101\rangle + \|1010\rangle)$
	$\|11\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0110\rangle + \|1001\rangle)$
$(s_1, s_2) = (1, 1)$	$\|00\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0001\rangle + \|1110\rangle)$
	$\|01\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0010\rangle + \|1101\rangle)$
	$\|10\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|0100\rangle + \|1011\rangle)$
	$\|11\rangle\|a\rangle \mapsto \frac{1}{\sqrt{2}}(\|1000\rangle + \|0111\rangle)$

5. Distillable entanglement by the converted protocols

In this section, we evaluate the distillable entanglement by one-way protocols constructed from stabilizers. Distillable entanglement is the most important measure of the performance of a class of protocols.

We mean by an $[[n, k]]$ entanglement distillation protocol a protocol always leaving k pairs of particles out of given n pairs of particles. Let $\mathcal{D}$ be a class of $[[n, k]]$ entanglement distillation protocol for $n = 1, 2, \ldots,$ and $k = 1, \ldots, n$. Let ρ_n be a density operator on $H^{\otimes 2n}$. The distillable entanglement by the protocol $\mathcal{D}$ for the sequence of states $\{\rho_n\}$ is the maximum of a real number R such that for any $R' < R$ and any $\epsilon > 0$ there exists an $[[n, k]]$ $(k \geqslant nR')$ protocol in $\mathcal{D}$ such that the protocol extracts a state $\tau \in H^{\otimes 2k}$ from ρ_n such that the fidelity between τ and a maximally entangled state in $H^{\otimes k}$ is at least $1-\epsilon$. Roughly speaking, the distillable entanglement by $\mathcal{D}$ is the largest number of maximally entangled pairs in $H^{\otimes 2}$ distillable from one pair of particles. Our definition imposes on protocols the restriction that a protocol always produces the same number of pairs of particles. A general definition without this restriction was given by Rains [15].

Let $\left\{\alpha(i, j) : (i, j) \in \mathbf{Z}_p^2\right\}$ be a probability distribution, and consider the density operator

$$\rho = \sum_{(i,j)\in\mathbf{Z}_p^2} \alpha(i, j)|\beta(i, j)\rangle\langle\beta(i, j)|$$

on $H_A \otimes H_B$. We shall estimate the distillable entanglement by the proposed protocol for the sequence of states $\{\rho_n = \rho^{\otimes n} : n = 1, \ldots\}$, and show the distillable entanglement is at least as large as the achievable rate of quantum stabilizer codes over the quantum channel Γ on H with an error $X^i Z^j$ occuring with probability $\alpha(i, j)$.

The achievable rate by quantum stabilizer codes over Γ is the maximum of a real number R such that for any $R' < R$ and any $\epsilon > 0$ there exists an $[[n, k]]$ $(k \geqslant nR')$ stabilizer code Q such that any state $|\varphi\rangle \in Q$ can be transmitted over Γ with fidelity at least $1 - \epsilon$.

Proposition 2. *We assume that the decoding of a quantum stabilizer code is implemented as follows: first measure an observable whose eigenspaces are the same as the stabilizer of the code, determine the most likely error of the form* $X^{i_1}Z^{j_1} \otimes \cdots \otimes X^{i_n}Z^{j_n}$*, and apply the inverse of the guessed error to the codeword. Under this assumption, the distillable entanglement by the proposed protocol without step 7 for* $\{\rho_n = \rho^{\otimes n} : n = 1, \ldots\}$ *is at least as large as the achievable rate by quantum stabilizer codes over* Γ.

Proof. Let R be the achievable rate by quantum stabilizer codes over Γ. Then for any $R' < R$ and $\epsilon' > 0$ there exists an $[[n, k]]$ $(k \geqslant nR')$ quantum stabilizer code Q with stabilizer S such that for any state $|\varphi\rangle \in Q$ can be transmitted over Γ with fidelity at least $1 - \epsilon'$. Let S be generated by $\{\mathsf{XZ}(\vec{g}_1), \ldots, \mathsf{XZ}(\vec{g}_{n-k})$ (and possibly some power of ωI)$\}$, and Q belongs to the eigenvalue λ_i of $\mathsf{XZ}(\vec{g}_i)$. Suppose that the decoder guesses the error as $\mathsf{XZ}(\vec{e}(\vec{s}))$ when the measurement outcomes indicate that the received state belongs to eigenvalue $\lambda_i\omega^{s_i}$ of $\mathsf{XZ}(\vec{g}_i)$ for $i = 1, \ldots, n-k$, where $\vec{s} = (s_1, \ldots, s_{n-k})$. Then the decoder can correct any error $\mathsf{XZ}(\vec{u})$ if

$$\vec{u} \in \left\{\vec{e}(\vec{s}) + C : \vec{s} \in \mathbf{Z}_p^{n-k}\right\} \tag{10}$$

where C is a linear subspace of $\mathbf{Z}_p^{2n}$ spanned by $\vec{g}_1, \ldots, \vec{g}_{n-k}$.

By lemma 3 (see the appendix), there exists a codeword $|\varphi\rangle \in Q$ such that if $|\varphi\rangle$ is transmitted and $\mathsf{XZ}(\vec{u})|\varphi\rangle$ is received with $\vec{u}$ not in the set (10) then the fidelity between $|\varphi\rangle$ and the decoded state is at most $9/16$, because the set (10) is equal to the set of correctable errors by Q in lemma 3. Since $|\varphi\rangle$ can be transmitted through Γ with fidelity at least $1 - \epsilon'$, the probability of the correctable error (10) over $\Gamma^{\otimes n}$ is at least $1 - 16\epsilon'/9$.

Suppose that we apply the proposed protocol to $\rho^{\otimes n}$ such that if the difference $\vec{s}$ of measurement outcomes is observed then $\mathsf{XZ}(\vec{e}(\vec{s}))^{-1}$ is applied in step 4. Then the average (9) of the fidelity is at least $1 - 16\epsilon'/9$, because the errors in the set (10) are also correctable by the proposed protocol (see equation (6)). For given $\epsilon > 0$ set $\epsilon' = 9\epsilon/16$ in the above argument, and we can see that the distillable entanglement is at least as large as the achievable rate of quantum stabilizer codes over Γ. □

The best known lower bound on the achievable rate by quantum stabilizer codes over Γ is given by Hamada [9], and his lower bound gives the true value for the depolarizing channels. Let us compare the distillable entanglement by the converted protocols and that by the hashing protocol [3] for the Werner state of fidelity F, which is given by $\alpha(1,1) = F, \alpha(0,1) = \alpha(1,0) = \alpha(0,0) = (1-F)/3$ and $p = 2$. The Werner state is converted to

$$F|\beta(0,0)\rangle\langle\beta(0,0)| + \frac{1-F}{3}(|\beta(0,1)\rangle\langle\beta(0,1)| + |\beta(1,0)\rangle\langle\beta(1,0)| + |\beta(1,1)\rangle\langle\beta(1,1)|) \tag{11}$$

by applying XZ on Bob's particle. The distillable entanglement of state (11) by the hashing protocol is estimated as

$$1 - H_2(F, (1-F)/3, (1-F)/3, (1-F)/3) \tag{12}$$

where H_b is the Shannon entropy with base b. The distillable entanglement of state (11) by the converted protocols is strictly larger than equation (12) for certain range of F, because the achievable rate of the Shor–Smolin concatenated codes is strictly larger than equation (12) over the depolarizing channel of fidelity F [7] and they can be written as stabilizer codes [9].

Let us consider the case of $p = 3, \alpha(0,0) = F$, and $\alpha(i,j) = (1-F)/8$ for $(i,j) \neq (0,0)$. The distillable entanglement by the nonbinary generalization [19] of the hashing protocol is estimated as

$$1 - H_3(\{\alpha(i,j)\}). \tag{13}$$

The achievable rate by the quantum stabilizer codes is strictly greater than equation (13) for $0.2552 \leqslant F \leqslant 0.2557$ [9, section VI.C], and so is the distillable entanglement by the converted protocols.

6. Fidelity calculation in the general case

In the preceding argument we assumed that the initial state shared by Alice and Bob was in the form of equation (4). In this section, we remove this restriction. Let ρ be an arbitrary density operator in $H_A^{\otimes n} \otimes H_B^{\otimes n}$. We shall consider applying the proposed protocol without step 7 to ρ and calculate the fidelity between the distilled state and $|\beta(0,0)\rangle^{\otimes k}$. Precisely speaking, we shall calculate the fidelity between $|\beta(0,0)\rangle^{\otimes k} \otimes |\mathrm{a}\rangle^{\otimes 2}$ and the state after step 5, which is equal to that between $|\beta(0,0)\rangle^{\otimes k}$ and the state after step 6.

The idea of the following argument is borrowed from section 7.4 of [13]. Since there is no selection of particles in steps 1–6 by a measurement, the whole process of steps 1–6 can be written as a completely positive trace-preserving map Λ on the density operators on $H_A^{\otimes n} \otimes H_B^{\otimes n}$.

Let $|\psi\rangle \in H_A^{\otimes n} \otimes H_B^{\otimes n} \otimes H_{\mathrm{env}}$ is a purification of ρ. Since $\left\{|\beta(\vec{x})\rangle : \vec{x} \in \mathbf{Z}_p^{2n}\right\}$ is an orthonormal basis of $H_A^{\otimes n} \otimes H_B^{\otimes n}$, we can write $|\psi\rangle$ as

$$|\psi\rangle = \sum_{\vec{x} \in \mathbf{Z}_p^{2n}} |\beta(\vec{x})\rangle \otimes |\mathrm{env}(\vec{x})\rangle \tag{14}$$

where $|\mathrm{env}(\vec{x})\rangle$ is a vector in H_{env}.

In step 4, the inverse error operator $\mathsf{XZ}(\vec{e})^{-1}$ is determined from the difference $\vec{s}$ of measurement outcomes and knowledge of $\left\{\alpha(\vec{u}) : \vec{u} \in \mathbf{Z}_p^{2n}\right\}$. When we deal with an arbitrary but known density operator ρ, determine $\vec{e}$ from $\vec{s}$ so that the lower bound (16) below on fidelity becomes large. Once we fix a determination rule of $\vec{e}$ from $\vec{s}$, we can define $\mathsf{Good} = \{\vec{u} \in \mathbf{Z}_p^{2n}$: the protocol can perfectly distill $|\beta(0,0)\rangle^{\otimes k}$ from $|\beta(\vec{u})\rangle\}$. Equation (14) can be written as

$$\sum_{\vec{x}\in\mathsf{Good}} |\beta(\vec{x})\rangle \otimes |\mathrm{env}(\vec{x})\rangle + \sum_{\vec{x}\in\mathbf{Z}_p^{2n}\setminus\mathsf{Good}} |\beta(\vec{x})\rangle \otimes |\mathrm{env}(\vec{x})\rangle. \tag{15}$$

Almost the same argument as section 7.4 of [13] shows that the fidelity between $|\beta(0,0)\rangle^{\otimes k}$ and the state after step 6 is at least

$$1 - \left\| \sum_{\vec{x}\in\mathbf{Z}_p^{2n}\setminus\mathsf{Good}} |\beta(\vec{x})\rangle \otimes |\mathrm{env}(\vec{x})\rangle \right\|^2. \tag{16}$$

Acknowledgments

The author would like to thank Professor Tomohiko Uyematsu and Mr Toshiyuki Morita for helpful discussions. This research was supported by the Japan Society for the Promotion of Science under contract no 14750278.

Appendix. Bad codeword lemma

We consider a quantum channel over which an error of the form $\mathsf{XZ}(\vec{e})$ occurs with the probability $\alpha(\vec{e})$ for $\vec{e} \in \mathbf{Z}_p^{2n}$, and we also consider the following decoding method: measure the observable of $H^{\otimes n}$ whose eigenspaces are the same as those of S, and apply an operator $\mathsf{XZ}(\vec{r}_e)$ $\left(\vec{r}_e \in \mathbf{Z}_p^{2n}\right)$ determined by the measurement outcome and some deterministic criterion. With this decoding method, we can correct at most p^{2n-2k} errors among all the p^{2n} errors for an $[[n,k]]$ quantum stabilizer code.

Lemma 3. *Let Q be an $[[n,k]]$ quantum stabilizer code. Suppose that we have a fixed decoding method as described above. There exists a codeword $|\varphi\rangle \in Q$ such that*

$$|\langle\varphi|\mathsf{XZ}(\vec{r}_e)\mathsf{XZ}(\vec{e})|\varphi\rangle| \leqslant \tfrac{3}{4}$$

for all uncorrectable error $\mathsf{XZ}(\vec{e})$, where an error $\mathsf{XZ}(\vec{e})$ is said to be correctable *if a received state $\mathsf{XZ}(\vec{e})|\varphi\rangle$ is decoded to $|\varphi\rangle$ for all $|\varphi\rangle \in Q$ and* uncorrectable *otherwise.*

Proof. Consider the following map

$$f : \begin{cases} E & \longrightarrow \qquad \mathbf{Z}_p^{2n} \\ \omega^i X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_n} Z^{b_n} & \longmapsto \quad (a_1, b_1, \ldots, a_n, b_n) \end{cases}.$$

Let $C = f(S) \subset \mathbf{Z}_p^{2n}$. Since S is commutative, we have $C \subseteq C^\perp$. Let $C_{\max}$ be a subspace of $\mathbf{Z}_p^{2n}$ such that

$$C_{\max} = C_{\max}^\perp$$
$$C \subseteq C_{\max} \subseteq C^\perp.$$

Such a space $C_{\max}$ always exists by the Witt theorem (see section 20 of [1]). Since $C_{\max} = C_{\max}^\perp$, we have $\dim C_{\max} = n$. The set $f^{-1}(C_{\max})$ is a commutative subgroup of E, so we can consider a quantum stabilizer code $Q_{\min} \subset Q$ defined by $f^{-1}(C_{\max})$. We have $\dim Q_{\min} = p^{n-\dim C_{\max}} = 1$. Let $|\psi_1\rangle \in Q_{\min}$ be a normalized state vector. We shall construct the desired codeword $|\varphi\rangle$ in lemma 3 from $|\psi_1\rangle$.

By the property of stabilizer codes, if $\vec{x} + C_{\max} \neq \vec{y} + C_{\max}$ then

$$\langle \psi_1 | \mathsf{XZ}(\vec{x})^* \mathsf{XZ}(\vec{y}) | \psi_1 \rangle = 0. \tag{17}$$

Let $R \subset C^\perp$ be a set of coset representatives of $C_{\max}$ in $C^\perp$, that is, R has the same number of elements as $C^\perp / C_{\max}$, and if $\vec{x}, \vec{y} \in R$ and $\vec{x} \neq \vec{y}$ then $\vec{x} + C_{\max} \neq \vec{y} + C_{\max}$. We assume $\vec{0} \in R$. Define

$$|\psi_2\rangle = \frac{1}{\sqrt{p^k}} \sum_{\vec{x} \in R} \mathsf{XZ}(\vec{x}) |\psi_1\rangle$$

which is a normalized state vector in Q by equation (17).

We want to take $|\varphi\rangle$ in lemma 3 as a multiple of $|\psi_1 + \psi_2\rangle$, so let us compute

$$\begin{aligned} \langle \psi_1 | \psi_2 \rangle &= \frac{1}{\sqrt{p^k}} \sum_{\vec{x} \in R} \langle \psi_1 | \mathsf{XZ}(\vec{x}) | \psi_1 \rangle \\ &= \frac{1}{\sqrt{p^k}} \langle \psi_1 | \psi_1 \rangle \qquad \text{by equation (17) and } \vec{0} \in R. \end{aligned}$$

By equation (17) we also have $\langle \psi_2 | \psi_2 \rangle = \langle \psi_1 | \psi_1 \rangle$. Therefore, $\langle \psi_1 + \psi_2 | \psi_1 + \psi_2 \rangle = (2 + 2/\sqrt{p^k}) \langle \psi_1 | \psi_1 \rangle$. Define $|\varphi\rangle$ by

$$\frac{1}{\sqrt{2 + 2/\sqrt{p^k}}} |\psi_1 + \psi_2\rangle$$

which is a normalized state vector in Q. We shall show that $|\varphi\rangle$ has the desired property.

Suppose that an error $\mathsf{XZ}(\vec{e}\,')$ occurred and we applied $\mathsf{XZ}(\vec{r}_e\,')$ as the recovery operator. If $\vec{e} = \vec{e}\,' - \vec{r}_{e'} \in C$, then the error $\vec{e}\,'$ is correctable, otherwise $\vec{e}\,'$ is uncorrectable. If $\vec{e} \notin C^\perp$, the decoded state is orthogonal to any transmitted state, so we may assume $\vec{e} \in C^\perp \setminus C$ hereafter.

For $\vec{e} \in C_{\max} \backslash C$,

$$\begin{aligned} & p^k \langle \psi_2 | \mathsf{XZ}(\vec{e}) | \psi_2 \rangle \\ &\quad = \sum_{\vec{x}, \vec{y} \in R} \langle \psi_1 | \mathsf{XZ}(\vec{x})^* \mathsf{XZ}(\vec{e}) \mathsf{XZ}(\vec{y}) | \psi_1 \rangle \\ &\quad = \sum_{\substack{\vec{x}, \vec{y} \in R \\ \vec{x} + C_{\max} = \vec{e} + \vec{y} + C_{\max}}} \langle \psi_1 | \mathsf{XZ}(\vec{x})^* \mathsf{XZ}(\vec{e}) \mathsf{XZ}(\vec{y}) | \psi_1 \rangle \qquad \text{(by equation (17))} \\ &\quad = \sum_{\vec{x} \in R} \langle \psi_1 | \mathsf{XZ}(\vec{x})^* \mathsf{XZ}(\vec{e}) \mathsf{XZ}(\vec{x}) | \psi_1 \rangle \\ &\quad = \sum_{\vec{x} \in R} \omega^{\langle \vec{e}, \vec{x} \rangle} \langle \psi_1 | \mathsf{XZ}(\vec{x})^* \mathsf{XZ}(\vec{x}) \mathsf{XZ}(\vec{e}) | \psi_1 \rangle \\ &\quad = \langle \psi_1 | \mathsf{XZ}(\vec{e}) | \psi_1 \rangle \sum_{\vec{x} \in R} \omega^{\langle \vec{e}, \vec{x} \rangle}. \end{aligned}$$

Consider the linear map $L_{\vec{e}}$ from $C^\perp$ to $\mathbf{Z}_p$ defined by

$$L_{\vec{e}}(\vec{x}) = \langle \vec{e}, \vec{x} \rangle.$$

Then the kernel of $L_{\vec{e}}$ contains $C_{\max}$ because $\vec{e} \in C_{\max}$, and $\vec{e} \notin C$ implies that $L_{\vec{e}}$ is not a zero linear map. Hence we can partition R into cosets of $\ker(L_{\vec{e}})$ in $C^\perp$. Each coset of $\ker(L_{\vec{e}})$ in $C^\perp$ contains exactly p^{k-1} elements of R, and each element in a coset has the same value under $L_{\vec{e}}$. Therefore

$$\begin{aligned}\sum_{\vec{x}\in R}\omega^{\langle\vec{e},\vec{x}\rangle} &= \sum_{\vec{x}\in R}\omega^{L_{\vec{e}}(\vec{x})}\\ &= p^{k-1}\sum_{i=0}^{p-1}\omega^{i}\\ &= 0.\end{aligned}$$

Summarizing these results we have

$$\begin{aligned}\vec{e}\in C^{\perp}\backslash C_{\max} &\implies \langle\psi_1|\mathsf{XZ}(\vec{e})|\psi_1\rangle = 0 \qquad \text{(by equation (17))}\\ \vec{e}\in C_{\max}\backslash C &\implies \langle\psi_2|\mathsf{XZ}(\vec{e})|\psi_2\rangle = 0\end{aligned}$$

and by equation (17) we have for $\vec{e}\in C^{\perp}$

$$|\langle\psi_1|\mathsf{XZ}(\vec{e})|\psi_2\rangle| = \frac{1}{\sqrt{p^k}}.$$

Thus we have for $\vec{e}\in C^{\perp}\setminus C$

$$\begin{aligned}&|\langle\psi_1+\psi_2|\mathsf{XZ}(\vec{e})|\psi_1+\psi_2\rangle|\\ &\quad\leqslant \frac{1}{2+2/\sqrt{p^k}}(\underbrace{|\langle\psi_1|\mathsf{XZ}(\vec{e})|\psi_1\rangle| + |\langle\psi_2|\mathsf{XZ}(\vec{e})|\psi_2\rangle|}_{\leqslant 1} + \underbrace{2|\langle\psi_1|\mathsf{XZ}(\vec{e})|\psi_2\rangle|}_{=2/\sqrt{p^k}})\\ &\quad\leqslant \frac{1+2/\sqrt{p^k}}{2+2/\sqrt{p^k}}\\ &\quad\leqslant 3/4\end{aligned}$$

which completes the proof of lemma 3. □

References

[1] Aschbacher M 2000 *Finite Group Theory* 2nd edn *(Cambridge Studies in Advanced Mathematics vol 10)* (Cambridge: Cambridge University Press)

[2] 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)

[3] 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)

[4] 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)

[5] 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. Inf. Theory* **44** 1369–87 (*Preprint* quant-ph/9608006)

[6] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 Quantum privacy amplification and the security of quantum cryptography over noisy channels *Phys. Rev. Lett.* **77** 2818–21 (*Preprint* quant-ph/9604039)

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 (erratum)

[7] DiVincenzo D P, Shor P W and Smolin J A 1998 Quantum-channel capacity of very noisy channels *Phys. Rev.* A **57** 830–39 (*Preprint* quant-ph/9706061)

DiVincenzo D P, Shor P W and Smolin J A 1999 Quantum-channel capacity of very noisy channels *Phys. Rev.* A **59** 1717 (erratum)

[8] Gottesman D 1996 Class of quantum error-correcting codes saturating the quantum Hamming bound *Phys. Rev.* A **54** 1862–8 (*Preprint* quant-ph/9604038)

[9] Hamada M 2002 Information rates achievable with algebraic codes on quantum discrete memoryless channels version 1 *Preprint* quant-ph/0207113v1

[10] Horodecki M and Horodecki P 1999 Reduction criterion of separability and limits for a class of distillation protocols *Phys. Rev.* A **59** 4206–16 (*Preprint* quant-ph/9708015)

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

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

[13] Preskill J 1998 Lecture notes for physics 229: quantum information and computation; webpage http://www. theory. caltech. edu/people/preskill/ph229

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

[15] Rains E M 1999 Rigorous treatment of distillable entanglement *Phys. Rev.* A **60** 173–8 (*Preprint* quant-ph/9809078)

[16] Shor P W 1995 Scheme for reducing decoherence in quantum computer memory *Phys. Rev.* A **52** 2493–6

[17] 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)

[18] Steane A M 1996 Error correcting codes in quantum theory *Phys. Rev. Lett.* **77** 793–7

[19] Vollbrecht K G H and Wolf M M 2003 Efficient distillation beyond qubits *Phys. Rev.* A **67** 012303 (*Preprint* quant-ph/0208152)

[20] Weyl H 1931 *The Theory of Groups and Quantum Mechanics* 2nd edn (London: Methuen)