PHYSICAL REVIEW A, VOLUME 64, 022314

Fidelity of a *t*-error-correcting quantum code with more than *t* errors

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

(Received 13 November 2000; revised manuscript received 12 January 2001; published 16 July 2001)

It is important to study the behavior of a *t*-error-correcting quantum code when the number of errors is greater than *t* because it is likely that there are also small errors besides *t* large correctable errors. We estimate the fidelity of a *t*-error-correcting stabilizer code over a general memoryless channel, allowing more than *t* errors. We also show that the fidelity can be made arbitrary close to 1 by increasing the code length.

DOI: 10.1103/PhysRevA.64.022314 PACS number(s): 03.67.Hk, 89.70.+c

I. INTRODUCTION

In the study of the quantum error-correcting codes, it is usually assumed that only a small number of qubits are affected and the rest of the qubits are left unchanged. However, it is important to study the behavior of a *t*-error-correcting quantum code when the number of errors is greater than *t* because it is likely that there are also *small* errors besides *t* large correctable errors. The goal of this paper is to provide a lower bound for the fidelity of the quantum error correction under the general noise model without any approximation. The fact that quantum error-correcting codes work under the general noise model seems a folklore result, and the original contributions of this paper are a rigorous proof and a quantitative relation between the fidelity and the noisiness of the channel.

The following research has been done prior to this paper. It has been informally argued in Ref. [1] Sec. VI, that those small errors do not result in a large error in the recovered quantum state. The first rigorous analysis was done in Ref. [2] Sec. 5.4, in which the authors assumed that the channel was memoryless, that is, each qubit interacts with different environment, and there was a scalar multiple of the identity operator in an operator sum representation of the channel superoperator. In Ref. [3], Sec. 7.4.2, quantitative relations between the fidelity and the noisiness were given for two specific classes of memoryless channels. Aharonov and Ben-Or [4] Sec. 8, analyzed the fault-tolerant quantum computation under the general noise model that is equivalent to a memoryless channel, and showed that if the channel is not too noisy then the error-free computation is possible. However, they did not provide a quantitative condition of general channels allowing the error-free computation. (They provided that of restricted channels.)

In this paper we assume that a unitary representation of the channel superoperator has large identity component (Assumption 3), and we give a lower bound [Eq. (7)] for the average of the fidelity between the original state and the recovered state without using any approximation, where the average is taken over the measurement outcome in the error correction process. As a consequence we show that the average of the fidelity can be made arbitrary close to 1 over a general memoryless channel by increasing the code length. This fact has been proved only over specific classes of quantum channels [2,3]. Our estimation is restricted to the stabilizer quantum codes introduced in Refs. [5–7], which include almost all good quantum codes discovered so far. It should be noted that the essential idea in our analysis already appeared in Ref. [3], Sec. 7.4.

This paper is organized as follows. In Sec. II we introduce notations used in this paper, and review the stabilizer quantum codes and their error-correction process. In Sec. III we give a lower bound for the fidelity. In Sec. IV several consequences and generalizations are discussed.

II. PRELIMINARIES

A. Notations

Let $\mathcal{H}$ be a Hilbert space. We denote by $\mathcal{S}(\mathcal{H})$ the set of density operators on $\mathcal{H}$. For a density operator ρ on $\mathcal{H}$ and a state vector $|\psi\rangle \in \mathcal{H}$, the fidelity [8,9] between them is defined by

$$F(|\psi\rangle,\rho)=\langle\psi|\rho|\psi\rangle.$$

It measures how close $|\psi\rangle$ and ρ are.

In this paper we consider *t*-error-correcting $[[n,k]]$ binary quantum codes unless otherwise stated. Let H_2 be the Hilbert space of dimension 2. Let Γ be a superoperator on H_2, that is, a trace-preserving completely positive linear map from $\mathcal{S}(H_2)$ to $\mathcal{S}(H_2)$. We assume that the channel is represented by Γ, which means that when we send a density operator $\rho \in \mathcal{S}(H_2)$ through the channel we get $\Gamma(\rho) \in \mathcal{S}(H_2)$ at the receiving end. The channel considered in this paper is assumed to be memoryless. So when we send a state $\rho \in \mathcal{S}(H_2^{\otimes n})$ we get $\Gamma^{\otimes n}(\rho)$.

We shall review the unitary representation of a superoperator [10]. A simplified proof can be found in Ref. [11], in the Appendix. Let Γ be a superoperator on a Hilbert space $\mathcal{H}$. Then there exists a Hilbert space $\mathcal{H}_E$, a state vector $|0_E\rangle \in \mathcal{H}_E$, and a unitary operator U on $\mathcal{H}\otimes\mathcal{H}_E$ such that

$$\Gamma(\rho)=\mathrm{Tr}_E(U(\rho\otimes|0_E\rangle\langle 0_E|)U^*), \tag{1}$$

for all $\rho \in \mathcal{S}(\mathcal{H})$, where Tr_E is the partial trace over $\mathcal{H}_E$. That is called a unitary representation of Γ.

B. Stabilizer quantum codes

In this section we review the method of quantum error correction proposed in Refs. [5–7]. Let

*Electronic address: ryutaroh@rmatsumoto.org

$$\sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \quad \sigma_z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

and $E=\{\pm w_1\otimes\cdots\otimes w_n\}$, where w_i is either I, σ_x, σ_z or $\sigma_x\sigma_z$. The set E is a noncommutative group with matrix multiplication as its group operation. Let S be a commutative subgroup of E. A quantum error-correcting code $Q\subset H_2^{\otimes n}$ is defined as an eigenspace of S.

For $M\in E$ we define $MQ=\{M|\varphi\rangle:|\varphi\rangle\in Q\}$. The set MQ is also an eigenspace of S for any $M\in E$. Moreover, $\{MQ:M\in E\}$ is equal to the set of eigenspaces of S. It follows that every eigenspace of S has the same dimension. Let $\dim Q=2^k$. Then there are 2^{n-k} eigenspaces of S. Let $S'=\{N\in E:MN=NM \text{ for all } M\in S\}$. It is known that

$$S'=\{M\in E:MQ=Q\}. \tag{2}$$

We shall describe the error correction procedure. Let H_{env} be the Hilbert space representing the environment around the channel. Suppose that we send a pure state $|\varphi\rangle\in Q$, and the environment is initially in a pure state $|0_{\text{env}}\rangle\in H_{\text{env}}$. Suppose also that we receive an entangled state $|\psi\rangle\in H_2^{\otimes n}\otimes H_{\text{env}}$. We measure an observable of $H_2^{\otimes n}$ whose eigenspaces are the same as those of S. Then the state $|\psi\rangle$ is projected to $|\psi'\rangle\in Q'\otimes H_{\text{env}}$, where Q' is some eigenspace of S.

We will define the weight of an operator $M\in E$ for error correction. Let $M=\pm w_1\otimes\cdots\otimes w_n$, where w_i is either I, σ_x, σ_z, or $\sigma_x\sigma_z$. The weight of M is defined to be $|\{i:w_i\neq I\}|$, and denoted by $w(M)$. We define the numbers d and d' by

$$d=\min\{w(M):M\in S' \text{ and } \pm M\notin S\},$$

$$d'=\min\{w(M):M\in S' \text{ and } \pm M\neq I\}.$$

The number d is called the minimum distance of Q. The code Q is said to be pure if $d=d'$ and impure if $d>d'$. We define $t=\lfloor(d-1)/2\rfloor$, where $\lfloor x\rfloor$ denotes the largest integer $\leqslant x$.

There are many operators $M\in E$ such that $MQ=Q'$. Let M be an operator whose weight is minimum among them. Note that if the weight of M is greater than $\lfloor(d'-1)/2\rfloor$ then there may be another operator M' such that $w(M')=w(M)$, $M'Q=Q'$, and $M\neq\pm M'$. We guess that the original pure state is $(M^{-1}\otimes I_{\text{env}})|\psi'\rangle$, where I_{env} is the identity operator on H_{env}.

If the number of errors $\leqslant t$, then $|\psi'\rangle$ is the tensor product of $|\varphi'\rangle\in Q'$ and some pure state in H_{env}, and $M^{-1}|\varphi'\rangle=|\varphi\rangle$. However, we do not make such an assumption, and we shall analyze the closeness (fidelity) between $|\varphi\rangle$ and $M^{-1}\,\mathrm{Tr}_{H_{\text{env}}}(|\psi'\rangle\langle\psi'|)(M^{-1})^*$.

We shall use the following fact later.

Proposition 1. Let $M'\in E$ be an operator such that $M'Q=MQ$. If $\pm M'\notin MS$ then $w(M')>t$, where $MS=\{MN:N\in S\}$.

Proof. If $w(M)>t$ then $w(M')>t$ by the definition of M. Suppose that $w(M)\leqslant t$ and $w(M')\leqslant t$. Then $w(M^{-1}M')\leqslant 2t<d$, $M^{-1}M'\in S'$ by Eq. (2), and $M^{-1}M'\notin S$. This contradicts to the definition of d. ∎

III. LOWER BOUND FOR THE FIDELITY

In this section we consider the fidelity between the original state and recovered state. Let Γ be the channel superoperator of H_2 as in Sec. II A. Since I, σ_x, σ_z, and $\sigma_x\sigma_z$ form a basis of linear operators on H_2, in a unitary representation of Γ we can write U in Eq. (1) as

$$I\otimes L_{0,0}+\sigma_x\otimes L_{1,0}+\sigma_z\otimes L_{0,1}+\sigma_x\sigma_z L_{1,1},$$

where $L_{i,j}$ is a linear operator on a Hilbert space H_E. Let $|0_E\rangle$ be the initial state of H_E.

Lemma 2. We retain notations as above. $\|L_{0,0}0_E\|\leqslant 1$, where $\|\cdot\|$ denotes the norm of a vector $\cdot$.

Proof. Let $\{|0\rangle,|1\rangle\}$ be the orthonormal basis such that $\sigma_x|0\rangle=|1\rangle$, $\sigma_x|1\rangle=|0\rangle$, $\sigma_z|0\rangle=|0\rangle$, and $\sigma_z|1\rangle=-|1\rangle$. Then we have

$$\begin{aligned}U(|0\rangle\otimes|0_E\rangle)=&|0\rangle\otimes(L_{0,0}|0_E\rangle+L_{0,1}|0_E\rangle)\\&+|1\rangle\otimes(L_{1,0}|0_E\rangle+L_{1,1}|0_E\rangle,\\ U(|1\rangle\otimes|0_E\rangle)=&|1\rangle\otimes(L_{0,0}|0_E\rangle-L_{0,1}|0_E\rangle)\\&+|0\rangle\otimes(L_{1,0}|0_E\rangle-L_{1,1}|0_E\rangle.\end{aligned}$$

Since both vectors are of unit norm, it follows that

$$\|L_{0,0}|0_E\rangle+L_{0,1}|0_E\rangle\|\leqslant 1,$$

$$\|L_{0,0}|0_E\rangle-L_{0,1}|0_E\rangle\|\leqslant 1.$$

We conclude $\|L_{0,0}0_E\|\leqslant 1$. ∎

Assumption 3. Assume that

$$\|L_{0,1}0_E\|^2+\|L_{1,0}0_E\|^2+\|L_{1,1}0_E\|^2=p.$$

Hereafter we denote $H_E^{\otimes n}$ by H_{env} and $|0_E\rangle\otimes\cdots\otimes|0_E\rangle$ by $|0_{\text{env}}\rangle$. Suppose that we send $|\varphi\rangle\in Q$ and the recovered state is $M^{-1}\,\mathrm{Tr}_{H_{\text{env}}}(|\psi'\rangle\langle\psi'|)(M^{-1})^*$ as in Sec. II B.

We shall consider the average of $F(|\varphi\rangle, M^{-1}\,\mathrm{Tr}_{H_{\text{env}}}(|\psi'\rangle\langle\psi'|)(M^{-1})^*)$ for an arbitrary fixed state $|\varphi\rangle\in Q$ under the assumption that the channel is memoryless. The superoperator of the channel is $\Gamma^{\otimes n}$. Let $\mathbf{Z}_2=\{0,1\}$ with the addition and the multiplication taken modulo 2. For $\vec{a}=(a_1,\ldots,a_n)\in\mathbf{Z}_2^n$, we define

$$X(\vec{a})=\sigma_x^{a_1}\otimes\cdots\otimes\sigma_x^{a_n},$$

$$Z(\vec{a})=\sigma_z^{a_1}\otimes\cdots\otimes\sigma_z^{a_n}.$$

Then a unitary representation of $\Gamma^{\otimes n}$ can be written as

$$\sum_{\vec{a},\vec{b}\in\mathbf{Z}_2^n}X(\vec{a})Z(\vec{b})\otimes L_{\vec{a}\vec{b}},$$

where

$$L_{\vec{a}\vec{b}}=L_{a_1,b_1}\otimes\cdots\otimes L_{a_n,b_n}.$$

Let $|\psi\rangle$ be as in Sec. II B. By notations defined so far, $|\psi\rangle$ can be written as

$$|\psi\rangle = \sum_{\vec{a},\vec{b}\in \mathbf{Z}_2^n} X(\vec{a})Z(\vec{b})|\varphi\rangle \otimes L_{\vec{a}\vec{b}}|0_{\mathrm{env}}\rangle .$$

Let Q' be an eigenspace of S. We shall consider the probability $P_{Q'}$ of $|\psi\rangle$ being projected to $Q'\otimes H_{\mathrm{env}}$ after the measurement. Let $(\vec{a}_{Q'},\vec{b}_{Q'})$ be a pair of vectors such that $X(\vec{a}_{Q'})Z(\vec{b}_{Q'})Q = Q'$ and that if $M'Q = Q'$ then $w(M') \geqslant w(X(\vec{a}_{Q'})Z(\vec{b}_{Q'}))$. Observe that if $w(X(\vec{a}_{Q'})Z(\vec{b}_{Q'})) > \lfloor (d'-1)/2 \rfloor$ then there may be another operator M' such that $M'Q = Q'$, $w(M') = w(X(\vec{a}_{Q'})Z(\vec{b}_{Q'}))$, and $M' \neq \pm X(\vec{a}_{Q'})Z(\vec{b}_{Q'})$. This implies that $(\vec{a}_{Q'},\vec{b}_{Q'})$ is not uniquely determined by Q'. One may choose whichever $(\vec{a}_{Q'},\vec{b}_{Q'})$ provided that $X(\vec{a}_{Q'})Z(\vec{b}_{Q'})$ has the minimum weight (see also Sec. IV D). Let $T_{Q'} = \{(\vec{c},\vec{d}) \in \mathbf{Z}_2^n \times \mathbf{Z}_2^n : X(\vec{c})Z(\vec{d})Q = Q'$ and $\pm X(\vec{c})Z(\vec{d}) \notin X(\vec{a}_{Q'})Z(\vec{b}_{Q'})S\}$. We define

$$|\sigma_{Q'}\rangle = \sum_{\substack{\vec{c},\vec{d}\in \mathbf{Z}_2^n \\ \pm X(\vec{c})Z(\vec{d}) \in X(\vec{a}_{Q'})Z(\vec{b}_{Q'})S}} X(\vec{c})Z(\vec{d})|\varphi\rangle \otimes L_{\vec{c}\vec{d}}|0_{\mathrm{env}}\rangle ,$$

$$|\sigma'_{Q'}\rangle = \sum_{(\vec{c}_{Q'},\vec{d}_{Q'})\in T_{Q'}} X(\vec{c}_{Q'})Z(\vec{d}_{Q'})|\varphi\rangle \otimes L_{\vec{c}_{Q'}\vec{d}_{Q'}}|0_{\mathrm{env}}\rangle .$$

Observe that

$$|\psi\rangle = \sum_{Q' \text{ is an eigenspace of } S} |\sigma_{Q'} + \sigma'_{Q'}\rangle , \tag{3}$$

and the projection of $|\psi\rangle$ to $Q'\otimes H_{\mathrm{env}}$ is $|\sigma_{Q'} + \sigma'_{Q'}\rangle$. Thus $P_{Q'}$ is given by $\| \sigma_{Q'} + \sigma'_{Q'} \|^2$.

Let $|\psi'\rangle = |\sigma_{Q'} + \sigma'_{Q'}\rangle / \| \sigma_{Q'} + \sigma'_{Q'} \|$ and $M = X(\vec{a}_{Q'})Z(\vec{b}_{Q'})$. Next we shall calculate a lower bound for the fidelity between $|\varphi\rangle$ and the recovered state $M^{-1}\,\mathrm{Tr}_{H_{\mathrm{env}}}(|\psi'\rangle\langle\psi'|)(M^{-1})^*$ when $|\psi\rangle$ is projected to $|\sigma_{Q'} + \sigma'_{Q'}\rangle \in Q'\otimes H_{\mathrm{env}}$ after the measurement. Observe that taking partial trace over H_{env} and applying M^{-1} to $|\sigma_{Q'}\rangle$ and $|\sigma_{Q'} + \sigma'_{Q'}\rangle$ yields the original state $|\varphi\rangle$ and the recovered state $M^{-1}\,\mathrm{Tr}_{H_{\mathrm{env}}}(|\psi'\rangle\langle\psi'|)(M^{-1})^*$, respectively. The fidelity between $|\varphi\rangle$ and $M^{-1}\,\mathrm{Tr}_{H_{\mathrm{env}}}(|\psi'\rangle\langle\psi'|)(M^{-1})^*$ is not less than that between $|\sigma_{Q'}\rangle$ and $|\sigma_{Q'} + \sigma'_{Q'}\rangle$, because the fidelity does not decrease by unitary operations and taking partial trace [12]. We shall calculate a lower bound for the fidelity $F_{Q'}$ between $|\sigma_{Q'}\rangle$ and $|\sigma_{Q'} + \sigma'_{Q'}\rangle$,

$$\begin{aligned}
1 - F_{Q'} &= 1 - \frac{\langle \sigma_{Q'} | \sigma_{Q'} + \sigma'_{Q'}\rangle \langle \sigma_{Q'} + \sigma'_{Q'} | \sigma_{Q'}\rangle}{\langle \sigma_{Q'} | \sigma_{Q'}\rangle \langle \sigma_{Q'} + \sigma'_{Q'} | \sigma_{Q'} + \sigma'_{Q'}\rangle} \\
&= \frac{\langle \sigma_{Q'} | \sigma_{Q'}\rangle \langle \sigma'_{Q'} | \sigma'_{Q'}\rangle - \langle \sigma'_{Q'} | \sigma_{Q'}\rangle \langle \sigma_{Q'} | \sigma'_{Q'}\rangle}{\langle \sigma_{Q'} | \sigma_{Q'}\rangle \langle \sigma_{Q'} + \sigma'_{Q'} | \sigma_{Q'} + \sigma'_{Q'}\rangle} \\
&\leqslant \frac{\langle \sigma_{Q'} | \sigma_{Q'}\rangle \langle \sigma'_{Q'} | \sigma'_{Q'}\rangle}{\langle \sigma_{Q'} | \sigma_{Q'}\rangle \langle \sigma_{Q'} + \sigma'_{Q'} | \sigma_{Q'} + \sigma'_{Q'}\rangle} \\
&= \frac{\langle \sigma'_{Q'} | \sigma'_{Q'}\rangle}{\langle \sigma_{Q'} + \sigma'_{Q'} | \sigma_{Q'} + \sigma'_{Q'}\rangle} .
\end{aligned}$$

We shall calculate an upper bound for the average of $1 - F_{Q'}$, where the average is taken over the measurement outcome. The following fact will be used. For a pair of vectors $(\vec{a},\vec{b})$, $w(\vec{a},\vec{b})$ denotes $w(X(\vec{a})Z(\vec{b}))$.

Proposition 4. We have

$$\cup_{Q' \text{ is an eigenspace of } S} T_{Q'} \subset \{(\vec{a},\vec{b}) \in \mathbf{Z}_2^n \times \mathbf{Z}_2^n : w(\vec{a},\vec{b}) > t\}.$$

Proof. The assertion follows from Proposition 1. ■

In the following calculation Q' runs through the set of eigenspaces of S,

$$\begin{aligned}
\sum_{Q'} P_{Q'}(1 - F_{Q'}) &\leqslant \sum_{Q'} \langle \sigma'_{Q'} | \sigma'_{Q'}\rangle \\
&= \sum_{Q'} \left\| \sum_{(\vec{c}_{Q'},\vec{d}_{Q'})\in T_{Q'}} X(\vec{c}_{Q'})Z(\vec{d}_{Q'})|\varphi\rangle \otimes L_{\vec{c}_{Q'}\vec{d}_{Q'}}|0_{\mathrm{env}}\rangle \right\|^2 \\
&\leqslant \sum_{Q'} \sum_{(\vec{c}_{Q'},\vec{d}_{Q'})\in T_{Q'}} \| X(\vec{c}_{Q'})Z(\vec{d}_{Q'})|\varphi\rangle \otimes L_{\vec{c}_{Q'}\vec{d}_{Q'}}|0_{\mathrm{env}}\rangle \|^2 \\
&\leqslant \sum_{\substack{\vec{c},\vec{d}\in \mathbf{Z}_2^n \\ w(\vec{c},\vec{d}) > t}} \| X(\vec{c})Z(\vec{d})|\varphi\rangle \otimes L_{\vec{c}\vec{d}}|0_{\mathrm{env}}\rangle \|^2 \quad \text{(by Proposition 4)} \\
&= \sum_{\substack{\vec{c},\vec{d}\in \mathbf{Z}_2^n \\ w(\vec{c},\vec{d}) > t}} \| L_{\vec{c}\vec{d}} 0_{\mathrm{env}} \|^2 .
\end{aligned} \tag{4}$$

For a vector $\vec{a}=(a_1,\ldots,a_n)\in\mathbf{Z}_2^n$, let

$$\ell(0)=\|L_{0,0}0_E\|^2,$$

$$\ell(1)=\|L_{0,1}0_E\|^2+\|L_{1,0}0_E\|^2+\|L_{1,1}0_E\|^2,$$

$$\Delta(\vec{a})=\prod_{i=1}^{n}\ell(a_i),$$

$$h(\vec{a})=|\{i:a_i\neq 0\}|.$$

Observe that $\Delta(\vec{a})\leqslant p^{h(\vec{a})}$ by Assumption 3 and Lemma 2. For vectors $\vec{a}$, $\vec{b}\in\mathbf{Z}_2^n$, let $\mathrm{or}(\vec{a},\vec{b})$ be the bitwise logical or of them. By these notations, for a vector $\vec{a}\in\mathbf{Z}_2^n$ we can see

$$\sum_{\substack{\vec{c},\vec{d}\in\mathbf{Z}_2^n\\ \mathrm{or}(\vec{c},\vec{d})=\vec{a}}}\|L_{\vec{c}\vec{d}}0_{\mathrm{env}}\|^2=\Delta(\vec{a})\leqslant p^{h(\vec{a})},$$

and $w(\vec{c},\vec{d})=h(\mathrm{or}(\vec{c},\vec{d}))$. By these observations we can rewrite Eq. (4) as

$$\sum_{\substack{\vec{c},\vec{d}\in\mathbf{Z}_2^n\\ w(\vec{c},\vec{d})>t}}\|L_{\vec{c}\vec{d}}0_{\mathrm{env}}\|^2=\sum_{\substack{\vec{a}\in\mathbf{Z}_2^n\\ h(\vec{a})>t}}\Delta(\vec{a}) \tag{5}$$

$$\leqslant\sum_{\substack{\vec{a}\in\mathbf{Z}_2^n\\ h(\vec{a})>t}}p^{h(\vec{a})}$$

$$=\sum_{i=t+1}^{n}\binom{n}{i}p^i. \tag{6}$$

Thus

$$1-\sum_{i=t+1}^{n}\binom{n}{i}p^i \tag{7}$$

is a lower bound for the average of the fidelity between the original state and the state recovered by a t-error-correcting quantum code of length n.

Example 5. By Table III of Ref. [6], it is known that there exists a $[[25,5,7]]$ code. We take it as an example. Then we have $t=3$. At $p=0.01$, the value of Eq. (7) is $1-0.000\,132$, and at $p=0.001$ the value of Eq. (7) is $1-0.127\times10^{-7}$.

IV. CONSEQUENCES AND GENERALIZATIONS

A. Error-free communication is asymptotically possible

In classical information transmission we can make the error probability arbitrary small by increasing the code length. The same result also holds in the quantum case. Let α be a real number such that $2p^{\alpha}<1$. Suppose that there exists a sequence of t_i-error-correcting quantum codes of length n_i such that $t_i/n_i\rightarrow\alpha$ and $n_i\rightarrow\infty$ as $i\rightarrow\infty$. The existence of such a sequence is guaranteed by the quantum Varshamov-Gilbert bound [5], Theorem 2, in a certain range of α.

We shall consider the asymptotic behavior of Eq. (7),

$$\sum_{i=t+1}^{n}\binom{n}{i}p^i\leqslant p^{t+1}\sum_{i=t+1}^{n}\binom{n}{i}\leqslant p^{t+1}\sum_{i=1}^{n}\binom{n}{i}=p^{t+1}2^n.$$

If $t/n\geqslant\alpha$ then $p^{t+1}2^n\leqslant p(2p^{\alpha})^n$, which converges to 0 as $n\rightarrow\infty$. Thus if we use the sequence of quantum codes described above, we can make the average of fidelity arbitrary close to 1 by increasing the code length. Note that our estimate differs by a factor of 2^n from an intuition $1-O(p^{t+1})$ of the fidelity of quantum error correction.

B. General channel

The memoryless assumption is used only in Eq. (6). We can calculate a lower bound for the average of the fidelity over an arbitrary channel as Eq. (5) by rewriting the unitary operator in a unitary representation as

$$\sum_{\vec{a},\vec{b}\in\mathbf{Z}_2^n}X(\vec{a})Z(\vec{b})\otimes L_{\vec{a}\vec{b}}.$$

C. Nonbinary codes

We can generalize the result to nonbinary stabilizer codes as follows. We consider q-ary stabilizer codes. Let H_q be the q-dimensional Hilbert space and $|0\rangle,\ldots,|q-1\rangle$ an orthonormal basis of H_q. Let λ be a primitive qth root of 1, for example, $\exp(2\pi i/q)$. We define a linear map C_q sending $|i\rangle$ to $|i+1 \bmod q\rangle$ and D_λ sending $|i\rangle$ to $\lambda^i|i\rangle$ [13]. Observe that $C_2=\sigma_x$ and $D_{-1}=\sigma_z$ when $q=2$.

Let Γ be the channel superoperator on H_q, and suppose that a unitary representation of Γ is

$$\Gamma(\rho)=\mathrm{Tr}_{H_E}(U(\rho\otimes|0_E\rangle\langle0_E|)U^*).$$

We can write U as

$$U=\sum_{(i,j)\in\mathbf{Z}_q^2}C_q^iD_\lambda^j\otimes L_{i,j},$$

where $\mathbf{Z}_q=\{0,\ldots,q-1\}$ and $L_{i,j}$ is a linear operator on H_E.

Replace the definition of p in Assumption 3 with

$$p=\sum_{(0,0)\neq(i,j)\in\mathbf{Z}_q^2}\|L_{i,j}0_E\|^2.$$

Then the lower bound Eq. (7) also holds for q-ary stabilizer codes.

D. Bounded distance decoding

In the error correction process described in Sec. II B we have to find an operator $M\in E$ such that $w(M)$ is minimum among operators $N \in E$ such that $NQ = Q'$. The task of finding such M from the measurement outcome becomes computationally difficult when both the code length and the minimum distance are large [15,16]. In practice, we may give up finding such M if there is no operator N of weight $\leqslant t'$ such that $NQ = Q'$, where t' is an integer $\leqslant t$. This is a quantum analog of the classical bounded distance decoding [14]. We shall slightly modify this bounded distance decoding and give a lower bound for the average of fidelity.

Let Q, Q', $|\psi'\rangle$ and I_{env} be as in Sec. II B. If there is an operator $N \in E$ such that $NQ = Q'$ and $w(N) \leqslant t'$, then let $M = N$. Otherwise choose an operator $M \in E$ such that $MQ = Q'$. Let the recovered state be $(M^{-1} \otimes I_{\mathrm{env}})|\psi'\rangle$. With this error-correction process the average of the fidelity is bounded from below by

$$1 - \sum_{i=t'+1}^{n} \binom{n}{i} p^i.$$

The proof is almost the same as that of Eq. (7).

E. Nonstabilizer codes

It seems difficult to generalize the result in this paper to nonstabilizer codes. Because in the error correction of nonstabilizer codes we cannot write $|\psi\rangle$ as sum of eigenvectors of the measured observable as in Eq. (3).

F. Entanglement fidelity

The entanglement fidelity introduced in Refs. [2,11] should also be considered in some applications, and we can estimate the entanglement fidelity from the fidelity by their relation [2], Theorem V.3.

ACKNOWLEDGMENTS

The author would like to thank Professor Tomohiko Uyematsu for discussion about the inequality in Sec. IV A, Dr. Keiji Matsumoto for pointing out the critical error in the initial version of this paper, and Dr. Mitsuru Hamada for telling us that a similar idea was already used in Ref. [3], Sec. 7.4. The author was supported by the JSPS during this research.

[1] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[2] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[3] J. Preskill, Lecture Notes for Physics 229: Quantum Information and Computation, URL: http://theory.caltech.edu/people/preskill/ph229, Chap. 7.

[4] D. Aharonov and M. Ben-Or, e-print quant-ph/9906129.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, IEEE Trans. Inf. Theory **44**, 1369 (1998).

[7] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).

[8] R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994).

[9] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[10] K. Kraus, *States, Effects, and Operations*, Lecture Notes in Physics Vol. 190 (Springer-Verlag, Berlin, 1983).

[11] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

[12] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[13] E. Knill, e-print quant-ph/9608048.

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (Elsevier, Amsterdam, 1977).

[15] R. Matsumoto and T. Uyematsu, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E83-A**, 1878 (2000).

[16] When a stabilizer code is constructed from a $GF(4)$-linear code with a classical decoding algorithm, we can use the classical decoding algorithm to determine M from the measurement outcome. This fact seems a folklore result. Its nonbinary extension can be found in Ref. [15], Sec. 3.2.