Realization of a collective decoding of code-word states

Masahide Sasaki,[1] Tsuyoshi Sasaki-Usuda,[2] Masayuki Izutsu,[1] and Osamu Hirota[3]
[1]*Communications Research Laboratory, Ministry of Posts and Telecommunications, Koganei, Tokyo 184, Japan*
[2]*Nagoya Institute of Technology, Gokiso-chou, Showa-ku, Nagoya 466, Japan*
[3]*Research Center for Quantum Communications, Tamagawa University, Tamagawa-gakuen, Machida, Tokyo 194, Japan*
(Received 14 October 1997)

A physical model for the optimum collective decoding that attains the minimum average error probability in distinguishing code-word states is presented. This model is based on a cavity QED technique which is available at present. It will open a possibility for a quantum decoder that realizes the superadditivity in classical capacity of quantum channel which was demonstrated in M. Sasaki, preceeding paper, Phys. Rev. A **58**, 146 (1998). [S1050-2947(98)05207-X]

PACS number(s): 03.67.Hk, 89.70.+c, 42.79.Sz, 89.80.+h

I. INTRODUCTION

Distinguishing nonorthogonal quantum states at the minimum error is a fundamental problem in quantum communication. The optimum strategy minimizing the average error probability can be, in principle, derived from a linear optimization in terms of a Bayesian decision problem. Such a strategy is generally represented by a probability operator measure (POM) which is a set of nonnegative Hermitian operators $\hat{\Pi}_i$ satisfying the resolution of the identity [1],

$$\sum_i \hat{\Pi}_i = \hat{I}, \quad \hat{\Pi}_i \geq 0. \tag{1}$$

Except for pure-state signals with a certain symmetry, it is a tedious job to derive explicit expressions for $\{\hat{\Pi}_i\}$ [2]. In addition, even when they can be obtained, corresponding physical processes are not necessarily obvious. Mathematically, the optimum POM can be specified in the Hilbert space of the minimum dimension that a set of signal states spans. However, it can often hardly be interpreted physically. For practical physical implementation, the POM should be constructed in a larger Hilbert space which can fully describe the physical system making the signal states. Such examples have been known only in certain cases of binary signals [3]. In the preceding paper, the problem of decoding M-ary code-word states at the minimum average error probability was discussed. For attaining the minimum error, a *collective decoding* was essential in which each code-word state is detected as a single state vector rather than detected as the individual letter states separately. It was shown that when it is applied to the properly selected code-word states, the *quantum gain* in transmittable information can be obtained.

In this paper we present a physical scheme for the optimum collective decoding of M-ary code-word states, particularly in the case where the letter states are pure and binary. This scheme consists of a quantum circuit and a simple separate measurement on the individual letter states. In the quantum circuit, a certain unitary transformation is carried out on the received code-word state and a superposition of the code-word states is generated. This unitary transformation is designed so that the minimum average error probability is attained when the output from the circuit is detected by the given separate measurement. In the following, the decoding scheme proposed in the preceding paper is briefly reviewed in Sec. II, and then quantum circuit structures are presented in Sec. III. In particular, a concrete model for distinguishing two code-word states of length 2 at the minimum average error will be proposed for an experimental demonstration of the principle of collective decoding. Section IV is for concluding remarks.

II. DECODING SCHEME

Let binary letter states be $\{|+\rangle,|-\rangle\}$ whose state overlap $\kappa=\langle+|-\rangle$ is assumed to be real. They span the two-dimensional Hilbert space $\mathcal{H}_l$. By concatenating them into block sequences of length n, the 2^n possible sequences are made. We then pick up M-ary sequences as code-word states that are denoted as $\{|S_1\rangle, \ldots, |S_M\rangle\}$ ($M \leq 2^n$), and use them with input probabilities $\{\zeta_1, \ldots, \zeta_M\}$. The rest of the sequences are denoted as $\{|S_{M+1}\rangle, \ldots, |S_{2^n}\rangle\}$. Since the code-word states are linearly independent, they span the M-dimensional Hilbert space $\mathcal{H}_s$. Let the nth extended Hilbert space be $\mathcal{H}_l^{\otimes n}$. The optimum collective decoding is described by an orthonormal set $\{|\omega_1\rangle, \ldots, |\omega_M\rangle\}$ on $\mathcal{H}_s \subset \mathcal{H}_l^{\otimes n}$.

This is achieved, in some cases, by the square-root measurement [1,4–6] given by

$$|\mu_i\rangle \equiv \hat{\rho}^{-1/2}|\tilde{S}_i\rangle, \tag{2a}$$

$$\hat{\rho} \equiv \sum_{i=1}^{M} |\tilde{S}_i\rangle\langle\tilde{S}_i|, \tag{2b}$$

$$|\tilde{S}_i\rangle \equiv \sqrt{\zeta_i}|S_i\rangle. \tag{2c}$$

Let us define the Gram matrix $\mathbf{\Gamma} \equiv (\langle\tilde{S}_i|\tilde{S}_j\rangle)$.

Theorem

For $0 \leq \kappa < 1$, *the square-root measurement* $\{|\mu_i\rangle\}$ *becomes optimum when all of the diagonal components of* $\mathbf{\Gamma}^{1/2}$ *are equal.*

Unless it is not the case, $\{|\mu_i\rangle\}$ forms, at least, an orthonormal set in $\mathcal{H}_s$. So it is connected with the optimum mea-

surement states $\{|\omega_i\rangle\}$ via a unitary operator $\hat{V}$ in $\mathcal{H}_s$ as $|\omega_i\rangle=\hat{V}|\mu_i\rangle$. A straightforward method to construct such a unitary operator is the Bayes-cost-reduction algorithm proposed by Helstrom [7]. In this algorithm, one chooses a pair of code-word states $\{|S_i\rangle,|S_j\rangle\}$, solves the binary decision problem in the plane spanned by the corresponding pair of measurement basis vectors $\{|\mu_i\rangle,|\mu_j\rangle\}$, and gets the revised basis vectors $\{|\mu_i'\rangle,|\mu_j'\rangle\}$ which can be connected with the previous ones via a U(2) operator $V^{(1)}$ in $\mathcal{H}_s$ as

$$|\mu_i'\rangle=V^{(1)}|\mu_i\rangle, \tag{3a}$$

$$|\mu_j'\rangle=V^{(1)}|\mu_j\rangle. \tag{3b}$$

After revising the basis vectors, the average error probability will decrease or, at worst, remain the same. This kind of step is to be continued till reaching the optimum point. Thus starting from the square-root measurement basis vectors, the optimum ones are derived as

$$|\omega_i\rangle=\cdots V^{(2)}V^{(1)}|\mu_i\rangle \quad \forall\ i. \tag{4}$$

In order to consider a physical scheme, we make an orthonormal set $\{|\omega_1\rangle,\ldots,|\omega_{2^n}\rangle\}$ on the whole space $\mathcal{H}_l^{\otimes n}$ by adding the other basis vectors obtained by using the Schmidt orthogonalization,

$$|\omega_i\rangle=\frac{|S_i\rangle-\sum_{k=1}^{i-1}|\omega_k\rangle\langle\omega_k|S_i\rangle}{\sqrt{1-\sum_{k=1}^{i-1}|\langle\omega_k|S_i\rangle|^2}} \quad (i=M+1,\ldots,2^n). \tag{5}$$

We denote the expansion of all the sequences by the above basis vectors as

$$\begin{pmatrix}|S_1\rangle\\ \vdots\\ |S_{2^n}\rangle\end{pmatrix}=\mathbf{B}\begin{pmatrix}|\omega_1\rangle\\ \vdots\\ |\omega_{2^n}\rangle\end{pmatrix}, \tag{6a}$$

$$\mathbf{B}=(B_{ij})=(\langle\omega_j|S_i\rangle). \tag{6b}$$

Let $\{|a\rangle,|b\rangle\}$ be the measurement basis vectors distinguishing the individual letter states. By concatenating them into the block sequences of length n, the 2^n product basis vectors in $\mathcal{H}_l^{\otimes n}$ are made. We pick up M-ary basis vectors from them, and denote them as $\{|A_1\rangle,\ldots,|A_M\rangle\}$, and the rest of them as $\{|A_{M+1}\rangle,\ldots,|A_{2^n}\rangle\}$. All the sequences can be expanded alternatively by these basis vectors as

$$\begin{pmatrix}|S_1\rangle\\ \vdots\\ |S_{2^n}\rangle\end{pmatrix}=\mathbf{C}\begin{pmatrix}|A_1\rangle\\ \vdots\\ |A_{2^n}\rangle\end{pmatrix}, \tag{7a}$$

$$\mathbf{C}=(C_{ij})=(\langle A_j|S_i\rangle). \tag{7b}$$

The two basis sets are connected via a unitary operator $\hat{U}$ on the whole space $\mathcal{H}_l^{\otimes n}$ as

$$|\omega_i\rangle=\hat{U}^\dagger|A_i\rangle \quad (i=1,\ldots,2^n), \tag{8a}$$

where

$$\hat{U}^\dagger\equiv\sum_{i,j}^{2^n}u_{ji}|A_j\rangle\langle A_i|, \quad u_{ji}\equiv(\mathbf{B}^{-1}\mathbf{C})_{ij}. \tag{8b}$$

Thus the optimum *collective decoding* $\{|\omega_1\rangle,\ldots,|\omega_M\rangle\}$ can be effected by (i) transforming the code-word states $\{|S_i\rangle\}$ by the unitary transformation $\hat{U}$, and (ii) applying the measurement $\{|A_1\rangle,\ldots,|A_M\rangle\}$ into the transformed code-word states. Note that $\{|A_i\rangle\}$ are the product basis vectors and hence represent the separate measurement on the individual letter states. The unitary transformation $\hat{U}$ plays a role of an *adaptor* to this separate measurement [3]. The minimum error probability is obtained as

$$P_e(\text{opt})=1-\sum_{i=1}^{M}\zeta_i|\langle S_i|\hat{U}^\dagger|A_i\rangle|^2. \tag{9}$$

When the code-word states have a certain symmetry, the construction of $\hat{U}$ will become much easier by choosing the measurement basis vectors $\{|A_1\rangle,\ldots,|A_M\rangle\}$ taking that symmetry into account. See the example later.

Construction of the quantum circuit for $\hat{U}$ can be done (i) by decomposing it into U(2) operators $\hat{T}_{[j,i]}$ by applying the algorithm proposed by Reck and others [8] as

$$\hat{U}=\hat{T}_{[2,1]}\hat{T}_{[3,1]}\cdots\hat{T}_{[2^n,2^n-2]}\hat{T}_{[2^n,2^n-1]}, \tag{10a}$$

where

$$\hat{T}_{[j,i]}=\exp[-\gamma_{ji}(|A_i\rangle\langle A_j|-|A_j\rangle\langle A_i|)], \tag{10b}$$

and (ii) by applying the formula established by Barenco *et al.* for simulating a discrete unitary operator [9]. Here the following point should be noted. Since quantum bits (qubits) in the circuit are the letter states themselves constituting the code-word states, the gates should consist of the single physical species from which the letter states are made. Such gates known so far are Sleator and Weinfurter's gate consisting of two-state atoms [10] and the quantum phase gate acting on two photon-polarization states [11].

III. QUANTUM CIRCUIT STRUCTURES

In this section the structure of the quantum circuit is presented. A model using a physically two-state system such as a two-level atom or a pair of single-mode photon polarizations is considered first, aiming at an experimental demonstration of the collective decoding. Then, an implementation in the case of coherent-state signals is discussed.

A. Physically two-state system

Let $\{|\uparrow\rangle,|\downarrow\rangle\}$ be the upper-level and lower-level states of an atom, or two orthogonal linear polarization states of a single-mode optical field. The measurement basis vectors $\{|a\rangle,|b\rangle\}$ can then be taken naturally as $\{|\uparrow\rangle,|\downarrow\rangle\}$ represent-

ing a level detection or a linear polarizer. Suppose that the letter states are made by rotating the state $|\uparrow\rangle$ by the angle θ or $\pi-\theta$ around the y axis,

$$|+\rangle=\hat{R}_y(\theta)|\uparrow\rangle=\sqrt{1-p}|\uparrow\rangle-\sqrt{p}|\downarrow\rangle, \tag{11a}$$

$$|-\rangle=\hat{R}_y(\pi-\theta)|\uparrow\rangle=\sqrt{p}|\uparrow\rangle-\sqrt{1-p}|\downarrow\rangle, \tag{11b}$$

where

$$\hat{R}_y(\theta)=\begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}=\begin{pmatrix} \sqrt{1-p} & \sqrt{p} \\ -\sqrt{p} & \sqrt{1-p} \end{pmatrix}, \tag{12}$$

and $p=(1-\sqrt{1-\kappa^2})/2$.

Let us consider a simple case of distinguishing two code-word states $\{|++\rangle,|--\rangle\}$, where $|++\rangle$ means $|+\rangle\otimes|+\rangle$, etc. The two measurement basis vectors of the optimum collective decoding are given by

$$|\omega_1\rangle=\sqrt{\frac{1-p_2}{1-\kappa^4}}|++\rangle-\sqrt{\frac{p_2}{1-\kappa^4}}|--\rangle, \tag{13a}$$

$$|\omega_2\rangle=-\sqrt{\frac{p_2}{1-\kappa^4}}|++\rangle+\sqrt{\frac{1-p_2}{1-\kappa^4}}|--\rangle, \tag{13b}$$

where $p_2=(1-\sqrt{1-\kappa^4})/2$ is the minimum bound of the average error probability. The code-word states are expanded as

$$|++\rangle=(1-p)|\uparrow\uparrow\rangle-\sqrt{(1-p)p}(|\uparrow\downarrow\rangle+|\downarrow\uparrow\rangle)+p|\downarrow\downarrow\rangle, \tag{14a}$$

$$|--\rangle=p|\uparrow\uparrow\rangle-\sqrt{(1-p)p}(|\uparrow\downarrow\rangle+|\downarrow\uparrow\rangle)+(1-p)|\downarrow\downarrow\rangle, \tag{14b}$$

here again $|\uparrow\uparrow\rangle=|\uparrow\rangle\otimes|\uparrow\rangle$, etc. Let us denote $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, and $|\downarrow\downarrow\rangle$ as $|A_1\rangle$, $|A_2\rangle$, $|A_3\rangle$, and $|A_4\rangle$, respectively. It is easy to see the optimum measurement basis vectors can be expressed as

$$|\omega_1\rangle=\hat{U}^\dagger|A_1\rangle, \tag{15a}$$

$$|\omega_2\rangle=\hat{U}^\dagger|A_4\rangle, \tag{15b}$$

where the unitary operator $\hat{U}$ is defined by the following matrix representation in terms of the basis vectors $\{|A_1\rangle,|A_2\rangle,|A_3\rangle,|A_4\rangle\}$:

$$\hat{U}=\frac{1}{2d_0}\begin{pmatrix} 1+d_0 & -\kappa & -\kappa & 1-d_0 \\ \kappa & 1+d_0 & 1-d_0 & \kappa \\ \kappa & 1-d_0 & 1+d_0 & \kappa \\ 1-d_0 & -\kappa & -\kappa & 1+d_0 \end{pmatrix}, \tag{16}$$

with $d_0=\sqrt{1+\kappa^2}$. Thus the optimum collective decoding by $\{|\omega_1\rangle,|\omega_2\rangle\}$ has been decomposed into the unitary transformation by $\hat{U}$ and the separate measurement by $\{|A_1\rangle,|A_4\rangle\}$. As seen in Eq. (14), the code-word states $|++\rangle$ and $|--\rangle$ mainly consist of $|\uparrow\uparrow\rangle$ and $|\downarrow\downarrow\rangle$, respectively, when the letter-state overlap κ is small. In addition, the expansion of Eq. (14) is symmetric in terms of these basis vectors. Therefore choosing $\{|A_1\rangle,|A_4\rangle\}$ as the final measurement seems very natural, and actually simplifies a construction of a quantum circuit for $\hat{U}$.

The transformed code words $\{\hat{U}|++\rangle,\hat{U}|--\rangle\}$ are always within the space spanned by $\{|A_1\rangle,|A_4\rangle\}$. The output is always either $\uparrow\uparrow$ or $\downarrow\downarrow$. The decomposition of the unitary operator $\hat{U}$ into the U(2) operators can be done in the following way:

$$\hat{U}=\hat{T}_{[2,1]}\hat{T}_{[3,1]}\hat{T}_{[3,2]}\hat{T}_{[4,1]}\hat{T}_{[4,1]}\hat{T}_{[4,2]}\hat{T}_{[4,3]}, \tag{17}$$

where the rotation angles γ_{ji} in $\hat{T}_{[j,i]}$ are determined by

$$\cos\frac{\gamma_{43}}{2}=\frac{d_0+1}{d_1}, \quad \sin\frac{\gamma_{43}}{2}=-\frac{\kappa}{d_1}, \tag{18a}$$

$$d_1=\sqrt{(d_0+1)^2+\kappa^2}, \tag{18b}$$

$$\cos\frac{\gamma_{42}}{2}=\frac{d_1}{d_2}, \quad \sin\frac{\gamma_{42}}{2}=-\frac{\kappa}{d_2}, \tag{18c}$$

$$d_2=\sqrt{d_1^2+\kappa^2}, \tag{18d}$$

$$\cos\frac{\gamma_{41}}{2}=\frac{d_2}{d_1}, \quad \sin\frac{\gamma_{41}}{2}=-\frac{d_0-1}{2d_0}, \tag{18e}$$

$$\gamma_{32}=\gamma_{41}, \quad \gamma_{31}=-\gamma_{42}, \quad \gamma_{21}=-\gamma_{43}. \tag{18f}$$

The above U(2) rotations $\hat{T}_{[j,i]}$ can be performed by the quantum circuits shown in Fig. 1. All the notations that are not explained particularly are borrowed from Ref. [9]. In the figure, the time evolves from the left to the right. Denoting a quantum state to be processed as $|\mu\nu\rangle=(|\mu\rangle\otimes|\nu\rangle)$, the upper and lower lines correspond to the evolutions of the first (with the initial state $|\mu\rangle$) and second (with the initial state $|\nu\rangle$) quantum bits (qubits), respectively. The two-bit gates in these circuits, $\wedge_1(\hat{R}_y(\gamma_{ji}))$ can be further decomposed into the circuits of the type shown in Fig. 2. Thus $\hat{T}_{[j,i]}$'s can be carried out by the circuits consisting of the one-bit gates and the controlled-NOT gates.

As mentioned in the preceding section, the candidates to implement these gates are Sleator and Weinfurter's gate for two-state atoms [10] and the quantum phase gate for binary photon polarizations [11]. For readers' convenience, we give explicit constructions of the gates required in our circuits, supplementing the original paper [10] by practical formula for our particular application. As shown later for the case $n=3$, basic gates for our purpose are the two-bit gate $\wedge_1(\sqrt{\sigma_x})$, the one-bit gates $\wedge_0(\sigma_x)$ and $\wedge_0(\hat{R}_y(\gamma))$. The controlled-NOT gate $\wedge_1(\sigma_x)$ is obviously equivalent to $\wedge_1(\sqrt{\sigma_x})\wedge_1(\sqrt{\sigma_x})$.

Implementations of the one-bit gates are straightforward by using the Ramsey zone (RZ) which is characterized by the Hamiltonian,

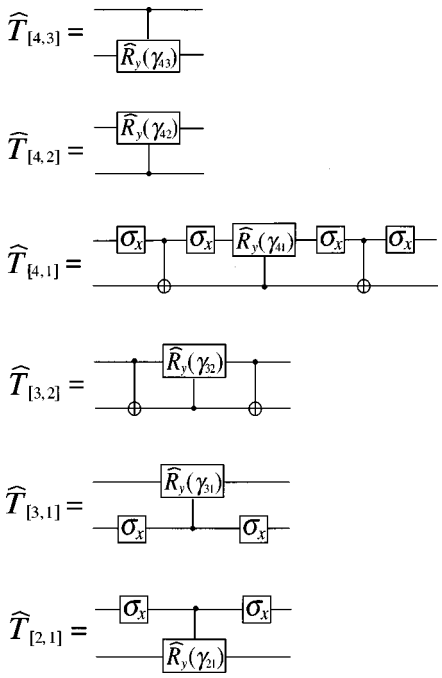

FIG. 1. Diagram representing the quantum circuits for realizing the U(2) rotations in Eq. (17). The time evolves from the left to the right. Denoting a quantum state to be processed as $|\mu\nu\rangle$ $(=|\mu\rangle\otimes|\nu\rangle)$, the upper and lower lines correspond to the evolutions of the first (with the initial state $|\mu\rangle$) and second (with the initial state $|\nu\rangle$) qubit, respectively.

$$\hat{H}_{\mathrm{RZ}}=\frac{1}{2}\hbar\nu(|\uparrow\rangle\langle\uparrow|-|\downarrow\rangle\langle\downarrow|) + i\hbar|\epsilon|(e^{-i\nu t}|\uparrow\rangle\langle\downarrow|-e^{i\nu t}|\downarrow\rangle\langle\uparrow|), \tag{19}$$

whose time evolution is described by the unitary operator,

$$\hat{U}_R(\tau,|\epsilon|)=\begin{pmatrix} e^{-i\nu\tau/2}\cos(|\epsilon|\tau) & e^{-i\nu\tau/2}\sin(|\epsilon|\tau) \\ -e^{i\nu\tau/2}\sin(|\epsilon|\tau) & e^{i\nu\tau/2}\cos(|\epsilon|\tau) \end{pmatrix} \tag{20}$$

in the spinor representation, where $|\epsilon|$ is the pumping field amplitude, the angular frequency ν corresponds to an atomic level separation, and τ is an interaction period. This is capable of implementing the following one-bit operations:

$$\hat{R}_y(\theta)=\begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{21}$$

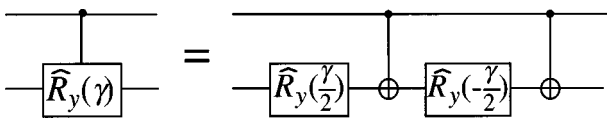

FIG. 2. The diagrammatic representation for a decomposition of the rotation of one qubit around the y axis $\hat{R}_y(\gamma)$ conditioned by the state of the other qubit.

$$\hat{R}_z(\theta)=\begin{pmatrix} \exp(i\theta/2) & 0 \\ 0 & \exp(-i\theta/2) \end{pmatrix}. \tag{22}$$

By using them, $\hat{R}_x(\theta)$ can be realized as,

$$\hat{R}_x(\theta)=\begin{pmatrix} \cos\frac{\theta}{2} & i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}=\hat{R}_z\left(\frac{\pi}{2}\right)\hat{R}_y(\theta)\hat{R}_z\left(-\frac{\pi}{2}\right). \tag{23}$$

$\hat{R}_x(\pi)$ plays a role of $\wedge_0(\sigma_x)$. We also introduce the other rotations for a later purpose,

$$\hat{U}_{R1}=\hat{U}_R(\tau,|\epsilon|) \quad \text{with} \quad |\epsilon|\tau=\frac{\pi}{4}, \tag{24}$$

$$\hat{U}_{R2}=\hat{U}_R(\tau',|\epsilon'|) \quad \text{with} \quad |\epsilon'|\tau'=\frac{\pi}{4}, \tag{25}$$

where $\tau\neq\tau'$ in general.

On the other hand, the implementation of the two-bit gate employs a microcavity and the Ramsey zones. The atom-cavity field interaction is described by the Jaynes-Cummings Hamiltonian,

$$\hat{H}=\hbar\omega\hat{a}^\dagger\hat{a}+\frac{1}{2}\hbar\nu(|\uparrow\rangle\langle\uparrow|-|\downarrow\rangle\langle\downarrow|) + \hbar g(\hat{a}^\dagger|\downarrow\rangle\langle\uparrow|+\hat{a}|\uparrow\rangle\langle\downarrow|), \tag{26}$$

where $\hat{a}$ $(\hat{a}^\dagger)$ is an annihilation (creation) operator for the cavity field with the angular frequency ω, and g is the coupling constant between the cavity field and the atom. It is assumed that ν is originally detuned from the cavity resonant frequency ω so that the atom undergoes an off-resonant interaction whose time evolution is given as

$$\hat{U}_{\mathrm{off}}(t)=\sum_{n=0}^{\infty}|n\rangle\langle n|\otimes\begin{pmatrix} e^{-i(\nu/2+g_{\mathrm{eff}})t-ing_{\mathrm{eff}}t} & 0 \\ 0 & e^{i\nu t/2+ing_{\mathrm{eff}}t} \end{pmatrix}, \tag{27}$$

where $g_{\mathrm{eff}}=g^2/\delta$, $\delta=\nu-\omega$, and $|n\rangle$ is the n-photon state. Phase factors involving ω have been omitted since it will give no physical effect. If ν is tuned to ω by an appropriate Stark shifting, an on-resonant interaction can be carried out as

$$\hat{U}_{\mathrm{on}}=\begin{pmatrix} 0 & -i|0\rangle\langle 1| \\ -i|1\rangle\langle 0| & |0\rangle\langle 0| \end{pmatrix}, \tag{28}$$

where the interaction period t_0 is chosen as $gt_0=\pi/2$ and the fact is taken into account that the cavity field is either $|0\rangle$ or $|1\rangle$ throughout the gate operation. Denoting the control-, target-bit atoms and the cavity as a, b, and c, respectively, $\wedge_1(\sqrt{\sigma_x})$ can be realized by applying a unitary process,

$$\hat{R}_z^{(a)}(-\tfrac{5}{4}\pi)\hat{R}_x^{(a)}(\pi)\hat{U}_{\mathrm{on}}^{(a,c)}\hat{U}_R^{(b)}(\tau',|\epsilon'|)\hat{U}_{\mathrm{off}}^{(b,c)}(t) \times\hat{U}_R^{(b)}(\tau,|\epsilon|)\hat{U}_{\mathrm{on}}^{(a,c)}\hat{R}_x^{(a)}(\pi), \tag{29}$$

where the superscript indicates on what system(s) the operator acts. Here $|\epsilon|\tau=|\epsilon'|\tau'=\pi/4$ and

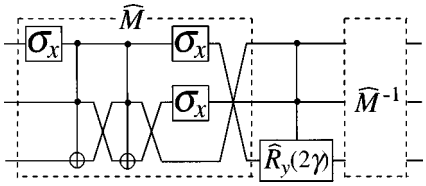

FIG. 3. The quantum circuit effecting the rotation $\hat{T}_{6,3}=\exp[-\gamma(|\uparrow\downarrow\uparrow\rangle\langle\downarrow\uparrow\downarrow|-|\downarrow\uparrow\downarrow\rangle\langle\uparrow\downarrow\uparrow|)]$ which is used for constructing the decoder of the code-word states of length 3.

$$i\frac{\nu(\tau-\tau')}{2}-i\frac{\nu t}{2}-i\frac{g_{\rm eff}t}{2}=2\pi n \quad (n=\text{integer})$$

should be satisfied.

In the decoder based on the above cavity QED system, either of the code-word states $|++\rangle$ or $|--\rangle$ passes through the sequence of the Ramsey zones and the cavities that are mounted according to the circuit for Eq. (17), and then detected by a level detector.

In the case of binary photon polarizations which is a more practical system for communication, the decoder structure is quite parallel to the two-state atomic case by replacing the Ramsey zone and the two-bit gate with a polarizer and the quantum phase gate, respectively.

So far, distinguishing code-word states at the minimum average error probability has never been done even for the simplest case $\{|++\rangle,|--\rangle\}$. Possible methods for it are not necessarily the above kind of scheme. As shown by Brody and Meister [12], the separate measurement together with the suitable feedback arrangement is capable of distinguishing the *two* code-word states at the minimum average error probability. For code-word states made of spin particles, the generalized Stern-Gerlach measurement may effect the optimum collective decoding [13]. As yet, however, it is strongly desired to demonstrate the scheme based on quantum circuits plus a simple standard measurement proposed in this paper because it seems the most natural and systematic method for designing a practical decoder.

Recently, an experiment designed to distinguish binary photon polarizations $\{|+\rangle,|-\rangle\}$ at the minimum average error probability p was done by Barnett and Riis [14]. It has a significant meaning for optical communication. The next step might be to demonstrate the discrimination of $\{|++\rangle,|--\rangle\}$ at the error rate p_2. It will be possible if the Barnett-Riis experiment is assisted with the circuits involving the quantum phase gate. Once a breakthrough is made in this direction, an extension to the optimum collective decoding for M-ary code-word states of optical polarizations might be straightforward.

From an information theoretic point of view, the optimum collective decoding of the four code-word states of length $n=3$ is of significant importance, because the superadditivity of classical capacity can appear as shown in the preceding paper. The circuits for $\hat{T}_{[ji]}$'s become more complicated. It might be worth giving one of such circuits. The principle of the formula can easily be understood by showing an example, say, a rotation $\hat{T}_{6,3}=\exp[-\gamma(|\uparrow\downarrow\uparrow\rangle\langle\downarrow\uparrow\downarrow|-|\downarrow\uparrow\downarrow\rangle\langle\uparrow\downarrow\uparrow|)]$. It can be executed by the circuit shown in Fig. 3. The block denoted as $\hat{M}$ is for mapping $\{|\uparrow\downarrow\uparrow\rangle,|\downarrow\uparrow\downarrow\rangle\}$ into $\{|\downarrow\downarrow\uparrow\rangle,|\downarrow\downarrow\downarrow\rangle\}$. In the mapped plane, the desired rotation is carried out as the three-bit gate operation $\wedge_2(\hat{R}_y(2\gamma))$. The two three-bit gates in Fig. 3 can be further decomposed into circuits of the two-bit gates as illustrated in Fig. 4. Thus it is easy to see that the basic gates for our circuits are the one-bit gates $\wedge_0(\hat{R}_y(\pm\gamma))$ and $\wedge_0(\sigma_x)$, and the two-bit gate $\wedge_1(\sqrt{\sigma_x})$.

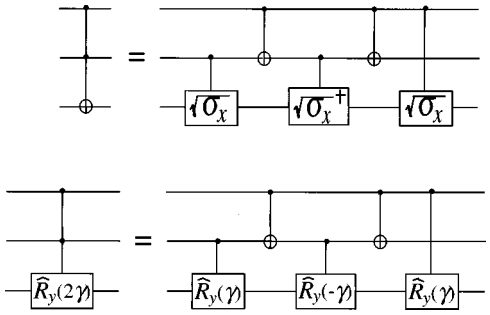

FIG. 4. The diagrammatic representation for decompositions of the 3-bit gates $\wedge_2(\sigma_x)$ and $\wedge_2(\hat{R}_y(2\gamma))$ into the 2-bit gates.

B. Binary phase-shift-keyed signals

We would like to mention the case of binary phase-shift-keyed (BPSK) signals of optical coherent states $\{|\alpha\rangle, |-\alpha\rangle\}$. This signal system is the most basic keying in long distance and ultrafast coherent light communications. If the collective decoding for this case could be realized, it will have a great impact on communication technology. Although the letter states are binary, the signal system is *not* a physically *two-state* system in this case. Therefore in order to apply the above decoding scheme, a new class of gates must be invented. Their specifications depend directly on what kind of measurement basis vectors are chosen as $\{|a\rangle,|b\rangle\}$.

Let us consider the following example. We first transform the received code-word state by combining each field of the letter state, $|\alpha\rangle$ or $|-\alpha\rangle$, sequentially with a local oscillating field with very large intensity via a beam splitter having almost perfect transmittance. Each process is represented by a unitary operator $\hat{D}(\alpha)=\exp(\alpha\hat{a}^{\dagger}-\alpha^{*}\hat{a})$. The transformed code-word states consist of the new letter states $\{|0\rangle, |-2\alpha\rangle\}$. The optimum collective decoding is then performed for the transformed code-word states. In that decoding they undergo further the certain unitary transformation $\hat{U}$ and are detected by the separate measurement that distinguishes each letter state $|0\rangle$ or $|-2\alpha\rangle$ according to the measurement basis vectors $|a\rangle$ or $|b\rangle$ such as

$$|a\rangle=|0\rangle, \tag{30a}$$

$$|b\rangle=\frac{|-2\alpha\rangle-|0\rangle\langle 0|-2\alpha\rangle}{\sqrt{1-|\langle 0|-2\alpha\rangle|^2}}. \tag{30b}$$

The state $|b\rangle$ only includes the Fock states with finite photons. Therefore this final measurement $\{|a\rangle\langle a|,|b\rangle\langle b|\}$

is equivalently accomplished by the photon counting $\{|0\rangle\langle 0|, \Sigma_{n=1}^{\infty}|n\rangle\langle n|\}$.

The quantum circuit realizing the required unitary transformation $\hat{U}$ should act on the qubits consisting of $\{|0\rangle, |b\rangle\}$. In particular, the basic two-bit gate $\wedge_1(\sqrt{\sigma_x})$ is specified as

$$|0\rangle_a|0\rangle_b|\psi\rangle_c \rightarrow |0\rangle_a|0\rangle_b|\psi\rangle_c ,$$

$$|0\rangle_a|b\rangle_b|\psi\rangle_c \rightarrow |0\rangle_a|b\rangle_a|\psi\rangle_c ,$$

$$|b\rangle_a|0\rangle_b|\psi\rangle_c \rightarrow |b\rangle_a \frac{1}{\sqrt{2}}(e^{i\pi/4}|0\rangle_b + e^{-i\pi/4}|b\rangle_b)|\psi\rangle_c ,$$

$$|b\rangle_a|b\rangle_b|\psi\rangle_c \rightarrow |b\rangle_a \frac{1}{\sqrt{2}}(e^{-i\pi/4}|0\rangle_b + e^{i\pi/4}|b\rangle_b)|\psi\rangle_c ,$$

where $|\psi\rangle_c$ represents a certain ancillary system. That is, depending on whether the control bit is the vacuum state or consists only of the finite-photon Fock states, the target bit should remain unchanged or should be transformed into the superposition between $|0\rangle$ and $|b\rangle$, respectively. It is an open question to find physical models accomplishing this function.

IV. CONCLUDING REMARKS

As shown in the preceding paper, the collective decoding plays an essential role in realizing true benefits of quantum communication. A systematic design of such a decoder becomes possible when techniques established in quantum computation are applied. The concrete scheme for the simplest collective decoding of $\{|++\rangle, |--\rangle\}$ at the minimum error rate was presented. It is implementable by use of the current cavity QED technique. Experimental demonstration is strongly desired. Further it is a challenging task to demonstrate experimentally the information theoretic quantum gain $I_n/n - C_1 > 0$ which must be seen for the code-word states $\{|+++\rangle, |+--\rangle, |--+\rangle, |-+-\rangle\}$. The amount of gain is quantitatively small but it will become measurable by increasing numbers of trials of transmission. From a practical viewpoint of coherent light communication, the problem was addressed on an implementation of a new class of gates that can act on the binary coherent states.

ACKNOWLEDGMENTS

The authors would like to thank Dr. H. Mabuchi of California Institute of Technology, Dr. M. Ban of Hitachi Advanced Research Laboratory, and Dr. K. Yamazaki and Dr. M. Osaki of Tamagawa University, Tokyo, for their helpful discussions.

[1] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[2] M. Osaki and O. Hirota, in *Quantum Communication and Measurement*, edited by V. P. Belavkin, O. Hirota, and R. L. Hudson (Plenum Publishing, New York, 1995), pp. 401–409; M. Osaki, M. Ban, and O. Hirota, Phys. Rev. A **54**, 1691 (1996).
[3] M. Sasaki and O. Hirota, Phys. Lett. A **210**, 21 (1996); **224**, 213 (1997); M. Sasaki, T. S. Usuda, O. Hirota, and A. S. Holevo, Phys. Rev. A **53**, 1273 (1996); M. Sasaki and O. Hirota, *ibid.* **54**, 2728 (1996).
[4] A. S. Holevo, Theor. Probab. Appl. **23**, 411 (1978).
[5] P. Hausladen and W. K. Wootters, J. Mod. Opt. **41**, 2385 (1994).
[6] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996).
[7] C. W. Helstrom, IEEE Trans. Inf. Theory **IT-28**, 359 (1982).
[8] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[9] A. Barenco, C. H. Bennet, R. Cleve, D. P. M. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[10] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).
[11] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).
[12] D. Brody and B. Meister, Phys. Rev. Lett. **76**, 1 (1996).
[13] A. R. Swift and R. Wright, J. Math. Phys. **21**, 77 (1980).
[14] S. M. Barnett and E. Riis, J. Mod. Opt. **44**, 1061 (1997).