Codes for the quantum erasure channel

M. Grassl and Th. Beth
Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, Am Fasanengarten 5, D-76 128 Karlsruhe, Germany

T. Pellizzari
Institut für Theoretische Physik, Universität Innsbruck, Technikerstraβe 25, A-6020 Innsbruck, Austria
(Received 27 September 1996)

The quantum erasure channel (QEC) is considered. Codes for the QEC have to correct for erasures, i.e., arbitrary errors at known positions. We show that four quantum bits are necessary and sufficient to encode one quantum bit and correct one erasure, in contrast to five quantum bits for unknown positions. Moreover, a family of quantum codes for the QEC, the quantum Bose-Chaudhuri-Hocquenghem codes, that can be efficiently decoded is introduced. [S1050-2947(97)01505-9]

PACS number(s): 03.65.Bz

I. INTRODUCTION

The prospect of speeding up certain classes of computations by utilizing the quantum-mechanical superposition principle and the physics of entanglement has received a great deal of attention lately [1]. The potentially useful quantum algorithms so far include factorization of large numbers [2], database search [3], and simulation of quantum-mechanical systems [4]. Recent theoretical and experimental progress in atomic physics and quantum optics has shown that small-scale quantum computing is feasible [5–8].

However, building a quantum computer is an extremely difficult task. The major obstacle is the coupling of the quantum computer to the environment, which destroys quantum-mechanical superpositions very rapidly. This effect is usually referred to as *decoherence* [9]. It is thus of crucial importance to find schemes to actively suppress and *undo* the effects of decoherence.

Schemes to protect static quantum states against decoherence were found independently by Shor [10] and Steane [11,12]. Their proposals gave rise to a large number of subsequent publications (see, for example, [13,14] and references therein). Thus the theory of *quantum error-correcting codes* is increasingly well understood.

In most publications the focus is on finding quantum codes for the most general error model. These quantum codes can correct for arbitrary errors at unknown positions in the code word. However, in many realistic situations additional information on possible errors is available. For example, the physical system may permit dephasing errors only or bit-flip errors only. Of course more efficient codes are possible for restricted error models. For example, the smallest quantum code to correct for errors due to dephasing (or due to bit-flips) has length 3 [15]. On the other hand, Knill and Laflamme have shown that the length of the smallest quantum code for arbitrary errors is five quantum bits (qubits) [13].

In this paper we consider an error model where the position of the erroneous qubits is known. In accordance with classical coding theory we shall call this model the *quantum erasure channel* (QEC). Below, a few physical systems are discussed where this model is applicable. The main results of the present paper are as follows: (i) an explicit example of a code for the quantum erasure channel (QEC code) with four qubits that can correct one erasure is presented; (ii) a proof is presented that four qubits are minimal; (iii) a construction for a family of QEC codes based on classical Bose-Chaudhuri-Hocquenghem (BCH) codes is given. For these codes efficient algorithms for correcting erasures exist.

The paper is organized as follows. In Sec. II we introduce the quantum erasure channel. The error model is discussed and a physical motivation is given. In Sec. III a four-qubit code for the QEC is given and the proof is presented that four qubits are minimal. A construction for quantum BCH codes is given in Sec. IV.

II. THE QUANTUM ERASURE CHANNEL

Whenever the position of an error can be determined by an appropriate measurement the QEC error model applies. In the following we give a few examples for physical scenarios where this is the case.

(i) If errors are accompanied by the emission of quanta they can in principle be detected. For example, if the qubits are represented by atoms an important source of errors is spontaneous emission. Spontaneous photons can be observed by photodetection techniques. There is, however, the difficulty that spontaneous photons from free atoms are emitted in a solid angle of 4π and will very likely elude observation. One may circumvent this problem by modifying the modal structure of the surrounding electromagnetic field by placing the atoms within a cavity and thereby channeling spontaneous decay [16]. Under appropriate conditions photons escape primarily via cavity decay through the cavity mirrors in a well-defined spatial direction. There may also be the possibility to detect the emission of photons by other means, for example via the photon recoil. Similarly, if quantum bits are stored in quantized cavity modes a detected cavity photon indicates an error [17].

(ii) It is usually assumed that the system space $\mathcal{H}_{\text{sys}}$ is a tensor product of two-dimensional spaces $\mathcal{H}_2$ (qubits), i.e.,

$$\mathcal{H}_{\text{sys}}=\mathcal{H}_2\otimes\cdots\otimes\mathcal{H}_2 .$$

 © 1997 The American Physical Society

However, this is an approximation. For example, atoms usually have many levels that may be populated due to an unwanted dynamical evolution of the system. Thus the Hilbert space of the system $\mathcal{H}_{\text{sys}}$ is a tensor product of multidimensional spaces with two-dimensional subspaces used for computing:

$$\mathcal{H}_{\text{sys}}=\mathcal{H}_k\otimes\cdots\otimes\mathcal{H}_k,$$

$$\mathcal{H}_{\text{comp}}=\mathcal{H}_2\otimes\cdots\otimes\mathcal{H}_2,$$

where $\mathcal{H}_{\text{comp}}$ is the subspace of allowed computational states. Each two-dimensional space $\mathcal{H}_2$ is a subspace of $\mathcal{H}_k$, but not necessarily a tensor factor of $\mathcal{H}_k$. (For simplicity we assume that the dimensions of all tensor factors are equal.) Therefore, the system space $\mathcal{H}_{\text{sys}}$ can only be decomposed as a direct sum of subspaces

$$\mathcal{H}_{\text{sys}}=\mathcal{H}_{\text{comp}}\oplus\mathcal{H}_{\text{comp}}^{\perp}$$

and generally not as a tensor product. During error-free computations the system remains in $\mathcal{H}_{\text{comp}}$. Any population found in $\mathcal{H}_{\text{comp}}^{\perp}$ is the signature of an error. Besides, we can learn about the position of the error by determining which subsystem has left the allowed Hilbert space $\mathcal{H}_2$. The erroneous subsystem can then be reset by hand to an arbitrary state in $\mathcal{H}_2$, $|0\rangle$ say. As an example we may think of an atom in which unwanted levels are coupled to the ''allowed'' two-level system by nonresonant laser interaction. We can measure the population in these levels, for example, by applying the quantum-jump technique [18].

(iii) QEC codes may be useful in *fault tolerant quantum computing*. This scheme was recently proposed by Shor and permits one to perform quantum computations and error correction with a network of erroneous quantum gates [19]. We may assume that only quantum gates introduce errors and that errors can be detected by appropriate measurements. In this case it is not necessary to use a quantum code for the most general error model because it is known to which qubits the quantum gate was applied when an error is detected. For example, in the cavity QED quantum computer model system proposed by Pellizzari *et al.* [8] the quantum information is safely stored in stable Zeeman ground-state levels while no computations are performed. However, during gate operation a single mode of a quantized cavity is excited, which is much more fragile a quantum system. A photodetector that records photons leaking out of the cavity indicates errors in those atoms that are involved in the current quantum gate.

(iv) It is worthwhile noting that there is a strong connection of codes for the QEC to the error correction scheme for quantum gates recently proposed by Cirac *et al.* [20]. This scheme is designed to correct for a specific but important error in the ion trap quantum computer during quantum gates. In this error model errors are caused by decays in the center-of-mass phonon mode, which is temporarily excited during quantum gate operation. If a residual population in the phonon mode is found an error is detected. As above in (iii) the position of the error is known and thus the QEC error model applies. In this scheme each logical qubit is encoded in two physical qubits. One might expect that a four-qubit code is required for this scheme since the smallest code conforming to the QEC has length 4. However, two qubits are sufficient because specific assumptions about the type of errors are made.

III. CODES FOR THE QEC

A. Conditions on codes for the QEC

For the general case, Knill and Laflamme [13] derived necessary and sufficient conditions on quantum error-correcting codes $\mathcal{QC}$. Given a set of error operators $\{A_i\}$ the conditions on states $|c_k\rangle\in\mathcal{QC}$ are

$$\langle c_k|A_i^{\dagger}A_j|c_k\rangle=\langle c_l|A_i^{\dagger}A_j|c_l\rangle, \tag{1}$$

$$\langle c_k|A_i^{\dagger}A_j|c_l\rangle=0 \quad \text{for } \langle c_k|c_l\rangle=0. \tag{2}$$

For a code of length N that can correct t errors the error operators $\{A_i\}$ are of a special form. They are all *t-error operators*, i.e., operators that differ on at most t of the tensor factors of $\mathcal{H}=\mathcal{H}_2^{\otimes N}$ from identity. In Eqs. (1) and (2) it is sufficient to consider algebra bases for t-error operators. The bases might be tensor products of local bases, e.g., the identity $\mathbb{1}$ and the Pauli spin matrices $\{\sigma_x,\sigma_y,\sigma_z\}$, or the operators $|0\rangle\langle 0|$, $|1\rangle\langle 0|$, $|0\rangle\langle 1|$, and $|1\rangle\langle 1|$. In this paper we consider the one-error operators P_{ij}^k that are the operators $|i\rangle\langle j|$ applied to the kth qubit.

For the QEC there are similar conditions. Since the positions of the errors are known by definition there is no need to separate the spaces corresponding to errors at different positions. Therefore, in Eqs. (1) and (2) only t-error operators A_i and A_j that differ from identity at the same positions have to be considered. But the product of such t-error operators is also a t-error operator and can be written as linear combination of the A_i since they are an algebra basis. Hence (1) and (2) reduce to

$$\langle c_k|A_i|c_k\rangle=\langle c_l|A_i|c_l\rangle, \tag{3}$$

$$\langle c_k|A_i|c_l\rangle=0 \quad \text{for } \langle c_k|c_l\rangle=0. \tag{4}$$

Equations (1) and (2) for t-error operators A_i imply Eqs. (3) and (4) for $2t$-error operators since the operators $A_i^{\dagger}A_j$ are bases for $2t$-error operators. Hence a quantum error-correcting code correcting t errors is a $2t$ erasure-correcting code.

B. QEC code with four qubits

For the general situation it was shown that the shortest code to encode one qubit and to correct one error has length 5 [13,21]. To encode one qubit and correct one erasure, however, four qubits are sufficient as demonstrated by the code $\mathcal{QC}$ given by

$$|\underline{0}\rangle=|0000\rangle+|1111\rangle,$$

$$|\underline{1}\rangle=|1001\rangle+|0110\rangle.$$

(To simplify the notation, normalization factors are omitted here and in the remainder of the paper.) In [11,12] it is shown that it is sufficient to correct bit flips in two bases that

are Hadamard transforms of each other. The Hadamard transform of the code $\mathcal{QC}$ corresponds to the ''dual'' code $\mathcal{QC}^{\perp}$ given by

$$|\underline{0}^{\perp}\rangle = H|\underline{0}\rangle = |0000\rangle + |0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle,$$

$$|\underline{1}^{\perp}\rangle = H|\underline{1}\rangle = |0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle - |1010\rangle - |1100\rangle + |1111\rangle.$$

By definition of an erasure the position of the error is known, but it is not known what the error is. Since all states of both the code $\mathcal{QC}$ and its dual $\mathcal{QC}^{\perp}$ have even weight, for both bases a single bit-flip error can be detected by computing the overall parity. Odd parity indicates an error. Thus any one-bit error can be corrected since correcting single bit flips in both bases is sufficient.

The code $\mathcal{QC}$ can be extended by the two states $|\underline{2}\rangle$ and $|\underline{3}\rangle$,

$$|\underline{2}\rangle = |1100\rangle + |0011\rangle,$$

$$|\underline{3}\rangle = |1010\rangle + |0101\rangle,$$

with

$$|\underline{2}^{\perp}\rangle = H|\underline{2}\rangle = |0000\rangle + |0011\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle + |1100\rangle + |1111\rangle,$$

$$|\underline{3}^{\perp}\rangle = H|\underline{3}\rangle = |0000\rangle - |0011\rangle + |0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle - |1100\rangle + |1111\rangle.$$

Thus the extended code encodes not only one, but two qubits and corrects for one erasure. Note that this code is equivalent to the code used for error detection in [22]. The existence of a code with these parameters was shown, e.g., in [14].

C. There is no QEC code with fewer than four qubits

In this section we prove that at least four qubits are required for a code that can correct one erasure and encodes one qubit. First we investigate when a quantum code can be shortened.

Theorem 1. Let $\mathcal{QC}$ be a quantum error-correcting code that can correct at least one erasure. If a one-qubit state $|\theta_0\rangle$ is a factor of a state $|\phi_0\rangle \in \mathcal{QC}$ it is a factor of all states $|\phi\rangle \in \mathcal{QC}$.

Proof. Assume without loss of generality that the first qubit is a factor, i.e., $|\phi_0\rangle = |\theta_0\rangle|\psi_0\rangle$. Inserting the local operator $P_{|\theta_0\rangle} = |\theta_0\rangle\langle\theta_0| \otimes \mathbb{1}$ in Eq. (3) yields, for any state $|\phi\rangle \in \mathcal{QC}$,

$$\langle\phi|P_{|\theta_0\rangle}|\phi\rangle = \langle\phi_0|P_{|\theta_0\rangle}|\phi_0\rangle = 1.$$

Hence $|\theta_0\rangle$ is a factor of every code state.

Thus we have the following corollary.

Corollary 1. If a quantum code $\mathcal{QC}$ of length N has a one-qubit factor deleting this position yields a quantum code $\mathcal{QC}'$ of length $N-1$ and equal dimension with same error-correcting capabilities.

Next we show that every two-dimensional subspace of $\mathcal{H}_2 \otimes \mathcal{H}_2$ contains at least one product state.

Lemma 1. For every two-dimensional subspace of $\mathcal{H}_2 \otimes \mathcal{H}_2$ there is a basis that contains at least one product state, i.e., a state $|\pi\rangle = |\pi_1\rangle|\pi_2\rangle$.

Proof. Let the subspace be generated by $\{|b_1\rangle, |b_2\rangle\}$. A product state $|\pi\rangle \in \mathcal{H}_2 \otimes \mathcal{H}_2$ is characterized by

$$\langle 00|\pi\rangle\langle 11|\pi\rangle = \langle 01|\pi\rangle\langle 10|\pi\rangle. \tag{5}$$

Inserting $|\pi\rangle = \eta_1|b_1\rangle + \eta_2|b_2\rangle$ in Eq. (5) yields a quadratic equation for the complex coefficients η_1 and η_2:

$$0 = c_1\eta_1^2 + c_{12}\eta_1\eta_2 + c_2\eta_2^2, \tag{6}$$

with

$$c_1 = \langle 00|b_1\rangle\langle 11|b_1\rangle - \langle 01|b_1\rangle\langle 10|b_1\rangle,$$

$$c_{12} = \langle 00|b_1\rangle\langle 11|b_2\rangle + \langle 11|b_1\rangle\langle 00|b_2\rangle - \langle 01|b_1\rangle\langle 10|b_2\rangle - \langle 10|b_1\rangle\langle 01|b_2\rangle,$$

$$c_2 = \langle 00|b_2\rangle\langle 11|b_2\rangle - \langle 01|b_2\rangle\langle 10|b_2\rangle.$$

If c_1 vanishes $|b_1\rangle$ is a product state and the lemma holds. Similarly, $|b_2\rangle$ is a product state if $c_2 = 0$. Now consider the case $c_1 \neq 0$ and $c_2 \neq 0$. The solutions of Eq. (6) are given by

$$\eta_1 = \frac{-c_{12} \pm \sqrt{c_{12}^2 - 4c_1c_2}}{2c_1}\,\eta_2.$$

For $c_1 \neq 0$ and $c_2 \neq 0$ there is at least one nontrivial solution with $\eta_1 \neq 0$ and $\eta_2 \neq 0$ and thus a product state exists.

Using Lemma 1 we are able to prove the following theorem.

Theorem 2. There is no quantum error-correcting code of length 2 that can correct one erasure and encodes one qubit.

Proof. Assume that such a code exists. The states $|\underline{0}\rangle$ and $|\underline{1}\rangle$ span a two-dimensional subspace $\mathcal{QC}$ of $\mathcal{H}_2 \otimes \mathcal{H}_2$. According to Lemma 1, $\mathcal{QC}$ contains a product state $|\pi_1\rangle|\pi_2\rangle$. From Theorem 1 it follows that both $|\pi_1\rangle$ and $|\pi_2\rangle$ are factors of all code states and thus the code cannot be two-dimensional.

Theorem 3. There is no quantum error-correcting code of length 3 that can correct one erasure and encodes one qubit.

Proof. Assume that such a code exists. Since there is no code of length 2 the states in the code cannot be factored. With reference to the first qubit the encoding can be written as

$$|\underline{0}\rangle = |0\rangle|\Phi_0\rangle + |1\rangle|\Phi_1\rangle,$$

$$|\underline{1}\rangle = |0\rangle|\Theta_0\rangle + |1\rangle|\Theta_1\rangle,$$

where $|\Phi_i\rangle, |\Theta_j\rangle$ are, in general, unnormalized and nonorthogonal states. The states $|\Phi_0\rangle$ and $|\Phi_1\rangle$ have to be linearly independent since otherwise $|\underline{0}\rangle$ is a product state and a code of length one exists (cf. Corollary 1). Similarly, $|\Theta_0\rangle$ and $|\Theta_1\rangle$ have to be linearly independent.

For the projections $P_{ij}^{(1)} = |i\rangle\langle j| \otimes \mathbb{1} \otimes \mathbb{1}$, $i,j \in \{0,1\}$ Eq. (4) implies

$$\langle \underline{1}|P_{00}^{(1)}|\underline{0}\rangle = \langle \Theta_0|\Phi_0\rangle = 0,$$

$$\langle \underline{1}|P_{10}^{(1)}|\underline{0}\rangle = \langle \Theta_1|\Phi_0\rangle = 0,$$

$$\langle \underline{1}|P_{01}^{(1)}|\underline{0}\rangle = \langle \Theta_0|\Phi_1\rangle = 0,$$

$$\langle \underline{1}|P_{11}^{(1)}|\underline{0}\rangle = \langle \Theta_1|\Phi_1\rangle = 0.$$

Thus the subspaces $\mathcal{H}_{|\underline{0}\rangle}$ spanned by $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ and $\mathcal{H}_{|\underline{1}\rangle}$ spanned by $\{|\Theta_0\rangle,|\Theta_1\rangle\}$ are two dimensional and orthogonal. This yields a decomposition of the joint Hilbert space of the second and third qubits:

$$\mathcal{H}_2 \otimes \mathcal{H}_2 = \mathcal{H}_{|\underline{0}\rangle} \oplus \mathcal{H}_{|\underline{1}\rangle}.$$

We now choose an orthonormal basis $B=\{|b_1\rangle, |b_2\rangle,|b_3\rangle,|b_4\rangle\}$ for the Hilbert space of the second and third qubits such that $\{|b_1\rangle,|b_2\rangle\}$ and $\{|b_3\rangle,|b_4\rangle\}$ span $\mathcal{H}_{|\underline{0}\rangle}$ and $\mathcal{H}_{|\underline{1}\rangle}$, respectively. In the orthonormal basis B, the code-words can be written as

$$|\underline{0}\rangle = |\alpha\rangle|b_1\rangle + |\beta\rangle|b_2\rangle$$

$$|\underline{1}\rangle = |\gamma\rangle|b_3\rangle + |\delta\rangle|b_4\rangle,$$

where $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$, and $|\delta\rangle$ are, in general, unnormalized and nonorthogonal states in the Hilbert space of the first qubit.

According to Lemma 1, without loss of generality $|b_1\rangle$ and $|b_3\rangle$ can be assumed to be product states. Since a local unitary transformation of a $\mathcal{QC}$ yields another $\mathcal{QC}$ with same parameters, without loss of generality $|b_1\rangle=|00\rangle$ can be chosen. At least one factor of the product state $|b_3\rangle$, say the first one, has to be $|1\rangle$ since $\langle b_1|b_3\rangle=0$.

Therefore, the orthonormal basis B has the form

$$|b_1\rangle = |00\rangle,$$

$$|b_2\rangle = k_1|01\rangle - k_2 b_{31}^*|10\rangle + k_2 b_{30}^*|11\rangle,$$

$$|b_3\rangle = b_{30}|10\rangle + b_{31}|11\rangle,$$

$$|b_4\rangle = -k_2^*|01\rangle - k_1^* b_{31}^*|10\rangle + k_1^* b_{30}^*|11\rangle,$$

with $|k_1|^2+|k_2|^2=1$ and $|b_{30}|^2+|b_{31}|^2=1$. The code words are of the form

$$|\underline{0}\rangle = |\alpha\rangle|00\rangle + k_1|\beta\rangle|01\rangle - k_2 b_{31}^*|\beta\rangle|10\rangle + k_2 b_{30}^*|\beta\rangle|11\rangle$$

$$|\underline{1}\rangle = -k_2^*|\delta\rangle|01\rangle + b_{30}|\gamma\rangle|10\rangle - k_1^* b_{31}^*|\delta\rangle|10\rangle + b_{31}|\gamma\rangle|11\rangle + k_1^* b_{30}^*|\delta\rangle|11\rangle. \quad (7)$$

If $k_2=0$ the state $|\underline{0}\rangle$ would have the factor $|0\rangle$ at the second position and a code of length 2 would exist. Therefore, we have $k_2\neq 0$.

From Eqs. (4) and (7) we obtain the conditions

$$0 = \langle \underline{1}|P_{00}^{(2)}|\underline{0}\rangle = -k_1 k_2 \langle \delta|\beta\rangle, \quad (8)$$

$$0 = \langle \underline{1}|P_{01}^{(3)}|\underline{0}\rangle = k_2 (b_{30}^*)^2 \langle \gamma|\beta\rangle - k_1 k_2 b_{30}^* b_{31} \langle \delta|\beta\rangle, \quad (9)$$

$$0 = \langle \underline{1}|P_{10}^{(3)}|\underline{0}\rangle = -k_2 \langle \delta|\alpha\rangle - k_2 (b_{31}^*)^2 \langle \gamma|\beta\rangle - k_1 k_2 b_{30} b_{31}^* \langle \delta|\beta\rangle, \quad (10)$$

$$0 = \langle \underline{1}|P_{10}^{(2)}|\underline{0}\rangle = b_{30}^* \langle \gamma|\alpha\rangle - k_1 b_{31} \langle \delta|\alpha\rangle + k_1 b_{31}^* \langle \gamma|\beta\rangle + k_1^2 b_{30} \langle \delta|\beta\rangle, \quad (11)$$

$$0 = \langle \underline{1}|P_{01}^{(2)}|\underline{0}\rangle = -k_2^2 b_{30}^* \langle \delta|\beta\rangle. \quad (12)$$

In the following we distinguish whether or not k_1 and b_{30} vanish.

(i) $k_1\neq 0$, $b_{30}\neq 0$: From Eq. (8) follows $\langle \delta|\beta\rangle=0$ and thus Eq. (9) reduces to $\langle \gamma|\beta\rangle=0$.

(ii) $k_1\neq 0$, $b_{30}=0$: From Eq. (8) follows $\langle \delta|\beta\rangle=0$. Equations (10) and (11) reduce to

$$-k_2 \langle \delta|\alpha\rangle - k_2 (b_{31}^*)^2 \langle \gamma|\beta\rangle = 0,$$

$$-k_1 b_{31} \langle \delta|\alpha\rangle + k_1 b_{31}^* \langle \gamma|\beta\rangle = 0.$$

This implies $\langle \delta|\alpha\rangle=0$ and $\langle \gamma|\beta\rangle=0$.

(iii) $k_1=0$, $b_{30}\neq 0$: From Eqs. (12) and (9) follows $\langle \delta|\beta\rangle=0$ and $\langle \gamma|\beta\rangle=0$.

(iv) $k_1=0$, $b_{30}=0$: The basis states $|b_3\rangle$ and $|b_4\rangle$ are $|11\rangle$ and $|01\rangle$, i.e., $|\underline{1}\rangle$ has the factor $|1\rangle$ in the third position.

For the first three cases $\langle \delta|\beta\rangle=0$ and $\langle \gamma|\beta\rangle=0$ implies that $|\gamma\rangle$ and $|\delta\rangle$ are linearly dependent or $|\beta\rangle=0$. Both results in a factorization of the code. Thus, for all cases the code can be factored and thus reduced to a code of length 2 which contradicts Theorem 2.

IV. QUANTUM BCH CODES

In principle, every quantum error-correcting code applies for the quantum erasure channel since a t error-correcting code is a $2t$ erasure-correcting code. But even for classical codes, error correction is a hard task [23]. The same is true for the correction of erasures.

But for some codes there are efficient algorithms to correct erasures and errors. Using the algorithm of Berlekamp and Massey [24] for decoding binary BCH codes with designed distance d_{BCH}, ν erasures and t errors can be corrected provided that $\nu+2t<d_{\mathrm{BCH}}$.

In this section we present a construction of quantum error-correcting codes based on certain binary BCH codes that can be decoded efficiently using the algorithm of Berlekamp and Massey. In a recent paper [14] the term *quantum BCH code* is used for codes derived from BCH codes over $GF(4)$. This definition is more general than ours since every cyclic code over $GF(2)$ is a subcode of a cyclic code over $GF(4)$. But a BCH code over $GF(4)$ need not be a binary BCH code and thus correction of erasures for the codes defined in [14] is not straightforward.

The construction of quantum codes from classical codes is based on the following theorem [12].

Theorem 4. Given two classical binary error-correcting codes $\mathcal{C}_1=[N,K_1,d_1]$ and $\mathcal{C}_2=[N,K_2,d_2]$ such that $\mathcal{C}_1$ contains the dual of $\mathcal{C}_2$, i.e., $\mathcal{C}_2^{\perp}\leq\mathcal{C}_1$, a quantum error-correcting

code $\mathcal{QC}=[[N,K_1-(N-K_2),\min(d_1,d_2)]]$ exists.

Here $\mathcal{C}=[N,K,d]$ denotes a classical binary linear error-correcting code of length N, dimension K, and minimum distance d; $\mathcal{QC}=[[N,K,d]]$ denotes a quantum error-correcting code with N qubits that encodes K qubits and allows correction of arbitrary errors of at least $t<d/2$ qubits. Decoding of $\mathcal{QC}$ is based on (classical) decoding algorithms for $\mathcal{C}_1$ and $\mathcal{C}_2$.

We consider the special case where $\mathcal{C}_1=\mathcal{C}_2=\mathcal{C}$. Then $\mathcal{C}^\perp\leqslant\mathcal{C}$ is required, i. e., $\mathcal{C}^\perp$ has to be a weakly self-dual code and an efficient decoding algorithm for $\mathcal{C}$ is needed. For the construction of quantum BCH codes, $\mathcal{C}$ is chosen to be a binary BCH code with $\mathcal{C}^\perp$ weakly self-dual.

Definition 1 (quantum BCH codes). Let $\mathcal{C}$ be a binary BCH code with $\mathcal{C}^\perp$ weakly self-dual. The states of the quantum BCH (QBCH) code code are given (up to normalization) by

$$|\psi_{\boldsymbol{v}}\rangle=\sum_{\boldsymbol{c}\in\mathcal{C}^\perp}|\boldsymbol{c}+\boldsymbol{v}\rangle \quad \text{for } \boldsymbol{v}\in\mathcal{C}/\mathcal{C}^\perp.$$

In the remainder of this section we show how to construct the BCH codes needed for QBCH codes. First we recall some properties of BCH codes (for proofs and details see, for example, [25]).

A cyclic code of length N is defined by the set of roots of its generator polynomial. The roots are distinct powers of a primitive Nth root α. Equivalently, the code corresponds to the set of exponents of the roots of its generator polynomial, the *defining set* $\mathcal{I}_\mathcal{C}$. For binary cyclic codes the defining set is a union of cyclotomic cosets $C_i:=\{i\ 2^k \bmod N: k=0,1,2,\dots\}$. For the construction of a binary BCH code with designed distance d_{BCH}, $\mathcal{I}_\mathcal{C}$ is chosen as $\mathcal{I}_\mathcal{C}=C_b\cup C_{b+1}\cup\cdots\cup C_{b+d_{\mathrm{BCH}}-2}$, i.e., the union of cyclotomic cosets of $d_{\mathrm{BCH}}-1$ consecutive numbers.

The defining set $\mathcal{I}_{\mathcal{C}^\perp}$ of the dual code $\mathcal{C}^\perp$ can be computed from that of the code in the following manner:

$$\mathcal{I}_{\mathcal{C}^\perp}=\bigcup_{i\in\bar{\mathcal{I}}_\mathcal{C}}C_{-i},$$

where $\bar{\mathcal{I}}_\mathcal{C}=\{0,\dots,N-1\}\setminus\mathcal{I}_\mathcal{C}$. A cyclic code $\mathcal{C}$ is weakly self-dual if and only if the defining set $\mathcal{I}_\mathcal{C}$ contains that of its dual, i.e., $\mathcal{I}_{\mathcal{C}^\perp}\subseteq\mathcal{I}_\mathcal{C}$ or, equivalently, $\mathcal{I}_{\mathcal{C}^\perp}\cap\bar{\mathcal{I}}_\mathcal{C}=\varnothing$.

For the QBCH codes, a binary BCH code $\mathcal{C}$ with $\mathcal{C}^\perp$ weakly self-dual is needed. Therefore, the condition for $\mathcal{C}$ is

$$\bigcup_{i\in\mathcal{I}_\mathcal{C}}C_i=\mathcal{I}_\mathcal{C}\subseteq\mathcal{I}_{\mathcal{C}^\perp}=\bigcup_{j\in\bar{\mathcal{I}}_\mathcal{C}}C_{-j}=\bigcup_{j\notin\mathcal{I}_\mathcal{C}}C_{-j}.$$

Thus $\mathcal{I}_\mathcal{C}$ must not contain both C_i and C_{-i}. In particular, $\mathcal{I}_\mathcal{C}$ must not contain cyclotomic cosets with $C_i=C_{-i}$.

The following lemma summarizes the preceding.

Lemma 2 (BCH codes for QBCH codes). Let $\mathcal{C}$ be a binary BCH code of length N and defining set $\mathcal{I}_\mathcal{C}$ such that

$$\forall i:[i\in\mathcal{I}_\mathcal{C}\Rightarrow(-i \bmod N)\notin\mathcal{I}_\mathcal{C}].$$

Then the dual code $\mathcal{C}^\perp$ is weakly self-dual and a QBCH code can be constructed.

V. CONCLUSION

We conclude by noting that finding efficient codes for restricted error models is relevant for proof-of-principle demonstrations of quantum error correction in the near future. The first prototype quantum computers will presumably have only a few qubits and will not be powerful enough to implement the most general error correction schemes. For example, a simplified demonstration of quantum error correction could consist in deliberately inducing an error in a known qubit. In this case the QEC error model applies.

ACKNOWLEDGMENTS

The authors acknowledge fruitful discussions with Peter Zoller and helpful comments from David DiVincenzo. T.P. is supported by the Austrian Science Foundation under Grant No. S06514PHY. This research was supported in part by the National Science Foundation under Grant No. PHY94-07194.

[1] For an overview see, e.g., A. Ekert, in *Atomic Physics 14: Proceedings of the 14th International Conference on Atomic Physics*, edited by J. Wineland *et al.*, AIP Conf. Proc. No. 323 (AIP, New York, 1955), p. 450; D. P. DiVincenzo, Science **270**, 255 (1995).

[2] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 1994), p. 124. An excellent review of the Shor algorithm is A. Ekert and R. Josza, Rev. Mod. Phys. **68**, 733 (1996).

[3] L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (ACM, New York, 1996), p. 212.

[4] S. Lloyd, Science **273**, 1073 (1996).

[5] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).

[6] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).

[7] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[8] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **75**, 3788 (1995).

[9] R. Landauer, Philos. Trans. R. Soc. London Ser. A **353**, 367 (1995); W. G. Unruh, Phys. Rev. A **51**, 992 (1995); G. M. Palma, K.-A. Suominen, and A. Ekert, Proc. R. Soc. London Ser. A **452**, 567 (1996).

[10] P. W. Shor, Phys. Rev. A **52**, 2493 (1995).

[11] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[12] A. M. Steane, Proc. R. Soc. London Ser. A **452**, 2551 (1996).

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

[14] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane (unpublished).

[15] S. L. Braunstein (unpublished).
[16] R. Blatt (private communication).
[17] H. Mabuchi and P. Zoller, Phys. Rev. Lett. **76**, 3108 (1996).
[18] W. Nagourney *et al.*, Phys. Rev. Lett. **56**, 2797 (1986); Th. Sauter *et al.*, *ibid.* **57**, 1696 (1986); J. C. Bergquist *et al.*, *ibid.* **57**, 1699 (1986).
[19] P. W. Shor, in *Proceedings of the 37th Symposium on Foundations of Computer Science* (IEEE, Los Alamitos, 1996), p. 56.
[20] J. I. Cirac, T. Pellizzari, and P. Zoller, Science **273**, 5279 (1996).
[21] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[22] L. Vaidman, L. Goldenberg, and S. Wiesner, Phys. Rev. A **54**, R1745 (1996).
[23] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, IEEE Trans. Inf. Theory **24**, 384 (1978).
[24] J. L. Massey, IEEE Trans. Inf. Theory **15**, 122 (1969).
[25] N. J. A. Sloane and F. J. MacWilliams, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1977).