

Decoherence-Free Subspaces for Quantum Computation

D. A. Lidar,¹ I. L. Chuang,² and K. B. Whaley¹

¹*Department of Chemistry, The University of California, Berkeley, California 94720*

²*IBM Almaden Research Center, San Jose, California 94120*

(Received 27 April 1998)

Decoherence in quantum computers is formulated within the semigroup approach. The error generators are identified with the generators of a Lie algebra. This allows for a comprehensive description which includes as a special case the frequently assumed spin-boson model. A generic condition is presented for errorless quantum computation: decoherence-free subspaces are spanned by those states which are annihilated by all the generators. It is shown that these subspaces are stable to perturbations and, moreover, that universal quantum computation is possible within them. [S0031-9007(98)07057-4]

PACS numbers: 03.67.Lx, 03.65.Bz, 03.65.Fd, 89.70.+c

Decoherence remains the most important obstacle to the exploitation of the speedup [1] promised by quantum computers. To this end a remarkable theory of quantum error correction codes (QECC) has recently been constructed [2], in which a logical quantum bit (qubit) is encoded in the larger Hilbert space of several physical qubits. This “active” error *correction* approach builds on the assumption that the most probable errors are those which occur independently to a few qubits during a reasonable time interval. However, correlated errors, which affect many or all qubits, may also be likely in some experimental realizations, particularly when qubits are physically close (for example, nuclear spins in a molecule) [3]. Such situations motivate the present study of an alternative “passive” error *prevention* scheme, in which logical qubits are encoded within subspaces which do not decohere because of reasons of symmetry. The existence of such *decoherence-free* (DF) subspaces has been shown by projection onto the symmetric subspace of multiple copies of a quantum computer [4], and by use of a group-theoretic argument [5]. Construction of these subspaces has been performed explicitly for certain collective error processes in the spin-boson model [6,7]. In this Letter we formulate a general theory for decoherence in quantum computation (QC) within the powerful semigroup approach [8,9], and show that this provides a rigorous and comprehensive criterion for construction of DF subspaces for an arbitrary Hamiltonian.

The semigroup approach.—The dynamics of a quantum system S coupled to a bath B (which together form a closed system) evolves unitarily under the Hamiltonian: $\hat{H}_{SB} = \hat{H} \otimes \hat{I}_B + \hat{I}_S \otimes \hat{H}_B + \hat{H}_I$, where \hat{H} , \hat{H}_B , and \hat{H}_I are the system, bath, and interaction Hamiltonians, respectively. \hat{I} is the identity operator. In the semigroup approach one shows that under the assumptions of (i) Markovian dynamics, (ii) “complete positivity” [9], and (iii) initial decoupling between the system and bath [10], the following master equation provides the most general form for the evolution of the system density

matrix ρ :

$$\frac{\partial \rho}{\partial t} = L[\rho] \equiv -\frac{i}{\hbar} [\mathbf{H}, \rho] + L_D[\rho], \quad (1)$$

$$L_D[\rho] = \frac{1}{2} \sum_{\alpha, \beta=1}^M a_{\alpha\beta} L_{\mathbf{F}_\alpha, \mathbf{F}_\beta}[\rho], \quad (2)$$

$$L_{\mathbf{F}_\alpha, \mathbf{F}_\beta}[\rho] = [\mathbf{F}_\alpha, \rho \mathbf{F}_\beta^\dagger] + [\mathbf{F}_\alpha \rho, \mathbf{F}_\beta^\dagger]. \quad (3)$$

The commutator involving \mathbf{H} is the ordinary, unitary, Heisenberg term. All the nonunitary, decohering dynamics is accounted for by L_D . The time-independent *Hermitian* coefficient matrix $A \equiv \{a_{\alpha\beta}\}$ contains the information about the physical decoherence parameters (lifetimes, longitudinal, or transverse relaxation times, and various equilibrium parameters such as stationary polarization or magnetization) [9].

The $\{\hat{\mathbf{F}}_\alpha\}_{\alpha=0}^M$ ($\hat{\mathbf{F}}_0 = \hat{\mathbf{I}}$) constitute a basis for the vector space of bounded operators acting on \mathcal{H} , the N -dimensional system Hilbert space. This operator space may be restricted—see the classification below. As such, the set $\{\hat{\mathbf{F}}_\alpha\}_{\alpha=1}^M$ forms an M -dimensional Lie algebra \mathcal{L} , with an $N \times N$ (generally $M \leq N^2 - 1$) matrix representation $\{\mathbf{F}_\alpha\}_{\alpha=1}^M$ appearing in Eq. (2) (we omit the hat symbol for matrices). Physically, the $\{\hat{\mathbf{F}}_\alpha\}_{\alpha=1}^M$ describe the various decoherence processes: in the QC context they are the *error generators*. They are often determined implicitly by the interaction Hamiltonian:

$$\hat{H}_I = \sum_{\alpha} \hat{\mathbf{F}}_\alpha \otimes \hat{\mathbf{B}}_\alpha, \quad (4)$$

where $\{\hat{\mathbf{B}}_\alpha\}$ are bath operators (see Ref. [11] for examples).

Decoherence of a quantum register.—Consider a quantum computer made of K qubits. States in the corresponding $N = 2^K$ -dimensional register Hilbert space \mathcal{H} are tensor products of single qubit states $|\varepsilon_\kappa\rangle$, $\varepsilon_\kappa = 0, 1$. It is convenient to adopt the following classification of decoherence models of interest, in terms of the above

Lie-algebraic scheme: (i) “Total decoherence”: This provides the maximum possible complexity of error generation, in which combined errors from any number of qubits are generated. As is well known, *single*-qubit errors can be fully described by the three Pauli matrices [i.e., the defining representation of the Lie algebra $\text{su}(2)$]. Thus when $|\varepsilon_\kappa\rangle$ are the eigenstates of the σ_κ^z Pauli matrix, a single qubit can either undergo a phase-flip (σ_κ^z), a bit-flip (σ_κ^x), or both (σ_κ^y). Taking into account also the possibility of no single-qubit error, there are four possibilities per qubit, so that the maximal total number of combined errors on K qubits is $M = 4^K - 1$, if we disregard the case of zero overall errors. The Lie algebra $\text{su}(N)$ has $N^2 - 1$ generators, so the corresponding M tensor products of Pauli matrices $\{\hat{\mathbf{F}}_\alpha\}$ form the defining representation of $\mathcal{L} = \text{su}(2^K)$. (ii) “Independent qubit decoherence”: In this, the ideal starting point for QECC, we have the much simpler case of merely one independent error per qubit, with all other qubits unaffected. There clearly are $3K$ such errors, each formed by taking the tensor product of a single Pauli matrix on one qubit with the identity on all the rest. Since errors on different qubits commute, this leads to a representation of the Lie algebra $\mathcal{L} = \bigoplus_{\kappa=1}^K \text{su}_\kappa(2)$. (iii) “Collective decoherence”: One could also consider the extreme case of all qubits undergoing the same decoherence process simultaneously [7], i.e., assuming full permutation invariance of the qubits. There are then just three possible errors and $\mathcal{L} = \text{su}(2)$. (iv) “Cluster decoherence”: Situations intermediate between the above three cases follow when the register can be partitioned into clusters k of K' qubits, with collective decoherence taking place within each cluster, but the clusters decohering independently. This leads to $\mathcal{L} = \bigoplus_{k=1}^{K/K'} \text{su}_k(2)$. Lastly, a very interesting case (dealt with in detail below) arises when a symmetry (e.g., permutation invariance) is broken *perturbatively*.

Conditions for decoherence-free dynamics.—Within the extremes delineated by the above categorization, a particularly interesting question is the following: what are necessary and sufficient conditions for the existence of a generic DF subspace? By generic (as opposed to general), we mean that one should (a) *avoid fine tuning of the noise parameters characterizing the decoherence processes*, and (b) *avoid a dependence on initial conditions*. Suppose that $\{|i\rangle\}_{i=1}^{N_0}$ is a basis for an N_0 -dimensional *invariant* DF subspace $\mathcal{H} \subseteq \mathcal{H}$. In this basis, we may express states as the density matrix

$$\tilde{\rho} = \sum_{i,j=1}^{N_0} \tilde{\rho}_{ij} |i\rangle\langle j|. \quad (5)$$

Consider the action of the error generators on the basis states: $\hat{\mathbf{F}}_\alpha |i\rangle = \sum_{j=1}^{N_0} c_{ij}^\alpha |j\rangle$. The DF dynamics condition is $L_D[\tilde{\rho}] = 0$, so that by Eq. (1) the dynamics is purely unitary in the subspace \mathcal{H} . Consider then Eq. (2): condition (a) above implies that each of the terms $L_{\mathbf{F}_\alpha, \mathbf{F}_\beta}[\tilde{\rho}]$

should vanish separately $\forall \alpha, \beta$. A straightforward calculation yields

$$L_{\mathbf{F}_\alpha, \mathbf{F}_\beta}[\tilde{\rho}] = \sum_{ij, mn=1}^{N_0} \tilde{\rho}_{ij} (2c_{jm}^{\beta*} c_{in}^\alpha |n\rangle\langle m| - c_{mn}^{\beta*} c_{in}^\alpha |m\rangle\langle j| - c_{jm}^{\beta*} c_{nm}^\alpha |i\rangle\langle n|). \quad (6)$$

To satisfy condition (b) above, each of the terms in parentheses must vanish separately. This can be achieved only if there is just one projection operator $|n\rangle\langle m|$ in each term. The least restrictive choice leading to this is $c_{in}^\alpha = c_i^\alpha \delta_{in}$. Equation (6) then becomes

$$L_{\mathbf{F}_\alpha, \mathbf{F}_\beta}[\tilde{\rho}] = \sum_{ij=1}^{N_0} \tilde{\rho}_{ij} |i\rangle\langle j| (2c_j^{\beta*} c_i^\alpha - c_i^{\beta*} c_i^\alpha - c_j^{\beta*} c_j^\alpha). \quad (7)$$

Assuming $c_i^\alpha \neq 0$ then yields $\frac{c_{aj}}{c_{ai}} + \frac{c_{bi}^*}{c_{bj}} = 2$. This has to hold in particular for $\alpha = \beta$. With $z = c_{aj}/c_{ai}$, we then obtain $z + 1/z^* = 2$, which has the unique solution $z = 1$. This implies that c_{ai} must be independent of i and therefore that $\hat{\mathbf{F}}_\alpha |i\rangle = c_\alpha |i\rangle$, $\forall \alpha$. As a result, we conclude that $[\hat{\mathbf{F}}_\alpha, \hat{\mathbf{F}}_\beta] |i\rangle = 0$. If \mathcal{L} is *semisimple* (has no Abelian invariant subalgebra) [12] then the commutator can be expressed in terms of nonvanishing structure constants $f_{\alpha, \beta}^\gamma$ of the Lie algebra: $[\hat{\mathbf{F}}_\alpha, \hat{\mathbf{F}}_\beta] = \sum_{\gamma=1}^M f_{\alpha, \beta}^\gamma \hat{\mathbf{F}}_\gamma$. We then arrive at the condition on the structure constants

$$\sum_{\gamma=1}^M f_{\alpha, \beta}^\gamma c_\gamma = 0 \quad \forall \alpha, \beta. \quad (8)$$

Now, it is known that the structure constants themselves define the M -dimensional “adjoint” matrix representation of \mathcal{L} [12]: $[\text{ad}(\hat{\mathbf{F}}_\alpha)]_{\gamma, \beta} = f_{\alpha, \beta}^\gamma$. Since the generators of the Lie algebra are linearly independent, so must be the matrices of the adjoint representation. One can readily show that this is inconsistent with Eq. (8) unless all $c_\gamma = 0$. We have thus proved [13]:

Theorem 1.—A necessary and sufficient condition for generic decoherence-free dynamics ($L_D[\tilde{\rho}] = 0$) in a subspace $\mathcal{H} = \text{Span}[\{|i\rangle\}_{i=1}^{N_0}]$ of the register Hilbert space, is that all basis states $|i\rangle$ are degenerate eigenstates of all the error generators $\{\hat{\mathbf{F}}_\alpha\}$: $\hat{\mathbf{F}}_\alpha |i\rangle = c_\alpha |i\rangle$, $\forall \alpha$; or, if \mathcal{L} is semisimple, that all $|i\rangle$ are annihilated by all $\{\hat{\mathbf{F}}_\alpha\}$:

$$\hat{\mathbf{F}}_\alpha |i\rangle = 0 \quad \forall \alpha, i. \quad (9)$$

Equivalently, the DF subspace is spanned by those states transforming according to the one-dimensional irreducible representations (irreps) of the Lie group with algebra \mathcal{L} . Those states are *singlets*. The size of the DF code provided by this subspace is its dimension N_0 , which can be used to further encode $\log_2(N_0)$ logical qubits.

Note also that by Eq. (4): $\hat{\mathbf{H}}_I |i\rangle \otimes |b\rangle = 0$, where $|b\rangle$ is any bath state. Theorem 1 thus not only reduces the identification of DF subspaces to a standard problem in

representation theory of Lie algebras, but also has the expected physical interpretation, namely that the DF states are those that are annihilated by the interaction Hamiltonian. (Note that this is only a *necessary* condition.)

Effect of the system Hamiltonian.— While $\tilde{\rho}$, by construction, is unaffected by the error generators, the absence of decoherence may still be spoiled by the system Hamiltonian itself. To see this explicitly, consider the *mixed-state fidelity*:

$$F(t) = \text{Tr}[\rho(0)\rho(t)] = \text{Tr}\{\rho(0)\exp(Lt)[\rho(0)]\}, \quad (10)$$

which is a natural measure of the decay of quantum coherence due to coupling of the system with the environment. In ideal quantum computation, one would like to have $F(t) = 1$, corresponding to perfect, noiseless memory. In reality $F(t) = 1 - \epsilon$, $\epsilon > 0$. A formal power expansion yields

$$F(t) = \sum_{n=0}^{\infty} \frac{t^n}{n!} \text{Tr}\{\rho(0)[L]^n[\rho(0)]\} \equiv \sum_{n=0}^{\infty} \frac{1}{n!} \left(\frac{t}{\tau_n}\right)^n, \quad (11)$$

where the “decoherence times” are

$$\tau_n = \{\text{Tr}[\rho(0)(L)^n[\rho(0)]]\}^{-1/n}.$$

In particular, the first order decoherence rate is

$$\frac{1}{\tau_1} = \text{Tr}\{\rho(0)L[\rho(0)]\}. \quad (12)$$

Since $\text{Tr}\{\rho[\hat{\mathbf{H}}, \rho]\} = 0$ (by cyclic permutation), it thus follows from Eq. (1) that $1/\tau_1 = 0$ for $\tilde{\rho}$. However, as is easily checked, generally $1/\tau_2 \neq 0$ because $\hat{\mathbf{H}}$ may cause transitions outside of \mathcal{H} . Therefore, the *full dynamics* in \mathcal{H} , including the effect of the system Hamiltonian, is DF to *first order*.

Effect of symmetry breaking perturbations.— Suppose we have identified the DF subspace for the Lie algebra \mathcal{L} underlying L_D . Let us consider the effect of adding new error generators $\{\hat{\mathbf{G}}_p\}_{p=1}^P$ which perturbatively break the symmetry, i.e., which do not belong to \mathcal{L} . We assume that the $\{\hat{\mathbf{G}}_p\}$ are due to an additional interaction Hamiltonian $\hat{\mathbf{H}}'_I$ which can be identified as appearing with a small parameter ϵ in the full system-bath Hamiltonian: $\hat{\mathbf{H}}_{SB} = \hat{\mathbf{H}} + \hat{\mathbf{H}}_B + \hat{\mathbf{H}}_I + \epsilon\hat{\mathbf{H}}'_I$. Then the *new* terms added to L_D are

$$\begin{aligned} L'_D[\tilde{\rho}] = & \sum_{\alpha=1}^M \sum_{p=1}^P (a_{\alpha p} L_{\mathbf{F}_{\alpha}, \epsilon \mathbf{G}_p}[\tilde{\rho}] + a_{\alpha p}^* L_{\epsilon \mathbf{G}_p, \mathbf{F}_{\alpha}}[\tilde{\rho}]) \\ & + \sum_{p,q=1}^P a_{pq} L_{\epsilon \mathbf{G}_p, \epsilon \mathbf{G}_q}[\tilde{\rho}]. \end{aligned} \quad (13)$$

Under the assumption $\epsilon \ll 1$ we may neglect the last term since it is $O(\epsilon^2)$. As for the terms in the double sum, $\mathbf{F}_{\alpha}\tilde{\rho} = \tilde{\rho}\mathbf{F}_{\alpha}^{\dagger} = 0$ by Eqs. (5) and (9). Expanding out the

remaining terms leaves

$$L'_D[\tilde{\rho}] \approx \epsilon \sum_{\alpha=1}^M \sum_{p=1}^P a_{\alpha p} \tilde{\rho} \mathbf{G}_p^{\dagger} \mathbf{F}_{\alpha} + \text{H.c.} \quad (14)$$

While this will generally take the singlet states outside of the DF subspace, this effect is also readily seen to be only of second order, because the first-order decoherence time [Eq. (12)] is now given by

$$\begin{aligned} \frac{1}{\tau_1} = & \epsilon \sum_{p=1}^P \{a_{\alpha p} \text{Tr}[\tilde{\rho}(0)\tilde{\rho}(0)\mathbf{G}_p^{\dagger}\mathbf{F}_{\alpha}] \\ & + a_{\alpha p}^* \text{Tr}[\tilde{\rho}(0)\mathbf{F}_{\alpha}^{\dagger}\mathbf{G}_p\tilde{\rho}(0)]\} = 0, \end{aligned} \quad (15)$$

by cyclic permutation under the first trace. The higher order decoherence times, τ_n , clearly involve ϵ^n and can thus be made negligible. Therefore we have proved that the DF subspace is *stable* to first order under a symmetry breaking perturbation.

This property is very promising from a quantum computational perspective, since one should be able to apply standard QECC techniques to correct errors which then occur within the DF subspace. Of particular concern are errors which take states out of the DF subspace; these are analogs of amplitude damping errors, which abstractly model, for example, scattering and spontaneous emission processes. Such errors can be corrected by simple codes [14], for example, by taking the DF singlet states as the computational basis states, and combining them into QEC codewords. Provided that $\hat{\mathbf{H}}'_I$ causes independent errors on different singlet states, we can conclude from the threshold theorem [15,16] that as long as ϵ is sufficiently small, the QECC encoding will render quantum computation within \mathcal{H} robust against these errors. Typical estimates of the threshold error probability range from 10^{-6} to 10^{-3} [16] and are extremely difficult to achieve in practice. The error probability is usually proportional to ϵ^2 . However, within \mathcal{H} , the error probability is reduced to ϵ^4 . Thus, QC within a DF subspace has potentially significant advantages.

The dimension of DF subspaces: the size of codes.— As shown in Ref. [7] for the spin-boson model, in the limit of collective decoherence [i.e., when $\mathcal{L} = \text{su}(2)$] the size of the DF subspace is

$$N_0 \xrightarrow{K \gg 1} K - \frac{3}{2} \log_2 K. \quad (16)$$

The encoding efficiency N_0/K is thus asymptotically unity. However, in the opposite limit of independent qubit decoherence, $\mathcal{L} = \bigoplus_{k=1}^K \text{su}_k(2)$, which is addressed by QECC, there does *not* exist a DF subspace [17]. The size of the code obtained in the intermediate cases of cluster decoherence can be estimated from Eq. (16) by replacing K by K' (the number of qubits per cluster), as long as $K' \leq K$. However, the most interesting situation arises in the perturbative scenario. Imagine a case of collective decoherence symmetry which is

perturbatively broken by small independent couplings between individual qubits and the bath. As long as the symmetry-breaking inhomogeneities are not too strong, we can conclude that, to first order, the exponentially large DF subspace is still available.

Universal quantum computation.—Our discussion so far has centered on the preservation of quantum *memory*. To complete it we still need to show that universal quantum computation can actually be performed in the DF subspace. As is well known, the controlled-NOT operation, together with arbitrary single qubit rotations, can generate any unitary operation [18]. The corresponding unitary operations are implemented by a driving Hamiltonian \hat{H}_d , which contains experimentally manipulable, time varying parameters, together with the system Hamiltonian \hat{H} .

We now give an example of universal 1- and 2-qubit operators acting on a four-dimensional singlet subspace. Let $|i\rangle$, $0 \leq i \leq 3$ be singlet states. These four states span 2 encoded qubits $|q_1\rangle, |q_2\rangle$ where q_1q_2 (with $q_j = 0, 1$) is the binary representation of i . A controlled-NOT gate can be constructed from a Hamiltonian represented in the encoded basis by the following combination of projection operators: $\hat{H}_{12}^{\text{not}} = c(t)[|11\rangle\langle 10| + |10\rangle\langle 11|]$. Here $c(t)$ is a time-dependent classical control parameter. Upon exponentiation this yields the familiar conditional unitary operator form. Single encoded-qubit rotations can be constructed from, e.g., $\hat{H}_2^{\text{rot}} = n_0(t) \times [|01\rangle\langle 00| + |00\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|]$. The generalization to larger singlet space systems is straightforward: one constructs the appropriate projection operators on the *singlet* states. By construction the resulting gates will leave the dynamics DF. Thus, in principle, universal DF-QC is possible within the singlet subspace. The main experimental challenge will involve implementation of the corresponding operations on the *physical* qubits. In addition, one should expect the actual implementation to involve some of the amplitude damping errors discussed above, i.e., some \hat{H}_d operations will take the singlets out of the DF subspace. However, as long as QECC is invoked, our previous arguments show that DF-QC is still possible.

It was shown how decoherence in QC can be described very generally in terms of the semigroup approach. The usual QC “error generators” were identified with the generators of a Lie algebra, whose identity depends on the pertinent decoherence process. Without reference to a specific system-bath interaction model, we derived *the generic condition for DF subspaces*: these are spanned by those states which are annihilated by all the error generators. We showed further that the DF subspaces are stable to first order under symmetry breaking perturbations, which allowed us to extend their utility by application of QECC. Finally, we showed that the DF subspaces support universal quantum computation.

This work was supported by NSF CHE-9616615 (K.B.W.) and by DARPA DAAG55-97-1-0341 (I.L.C.).

We would like to acknowledge helpful conversations with Dr. Paulo Zanardi, Dr. Robert N. Cahn, and Dr. Umesh Vazirani.

-
- [1] (a) P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124; (b) L.K. Grover, Phys. Rev. Lett. **79**, 4709 (1997).
 - [2] (a) P.W. Shor, Phys. Rev. A **52**, 2493 (1995); (b) A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996); (c) A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
 - [3] N. Gershenfeld and I.L. Chuang, Science **275**, 350 (1997).
 - [4] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello, SIAM J. Comp. **26**, 1541 (1997).
 - [5] P. Zanardi and M. Rasetti, Mod. Phys. Lett. B **11**, 1085 (1997).
 - [6] (a) G.M. Palma, K.-A. Suominen, and A.K. Ekert, Proc. R. Soc. London Sect. A **452**, 567 (1996); (b) L.-M Duan and G.-C. Guo, Phys. Rev. Lett. **79**, 1953 (1997); (c) L.-M Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998); (d) P. Zanardi, Phys. Rev. A **56**, 4445 (1997).
 - [7] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
 - [8] G. Lindblad, Commun. Math. Phys. **48**, 119 (1976).
 - [9] R. Alicki and K. Lendi, *Quantum Dynamical Semigroups and Applications*, in Lecture Notes in Physics (Springer-Verlag, Berlin, 1987), No. 286.
 - [10] (a) P. Pechukas, Phys. Rev. Lett. **73**, 1060 (1994); (b) R. Alicki, Phys. Rev. Lett. **75**, 3020 (1995); (c) P. Pechukas, *ibid.*, **75**, 3021 (1995).
 - [11] R. Kosloff, M.A. Ratner, and W.B. Davis, J. Chem. Phys. **106**, 7036 (1997).
 - [12] J.F. Cornwell, *Group Theory in Physics*, Techniques of Physics: 7 Vol. II (Academic Press, London, 1984).
 - [13] A related result was derived independently by P. Zanardi, Phys. Rev. A **57**, 3276 (1998).
 - [14] (a) I.L. Chuang, D.W. Leung, and Y. Yamamoto, Phys. Rev. A **56**, 1114 (1997); (b) I.L. Chuang and Y. Yamamoto, Phys. Rev. Lett. **27**, 4281 (1997); (c) D.W. Leung, M.A. Nielsen, I.L. Chuang, and Y. Yamamoto, Phys. Rev. A **56**, 2567 (1997).
 - [15] (a) D. Aharonov and M. Ben-Or, LANL Report No. quant-ph/9611025; E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).
 - [16] J. Preskill, Proc. R. Soc. London Sect. A **454**, 385 (1998).
 - [17] Since the irreps of a direct sum algebra are given by the direct product of the irreps of the constituent algebras [12], the representation realized for the $\{\hat{F}_\alpha\}$ is therefore in this case already irreducible and (since it is a tensor product of $K \times 2 \times 2$ matrices) 2^K dimensional. Thus it cannot contain any 1D irreps.
 - [18] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995), and references therein.