Fault-Tolerant Quantum Computation via Exchange Interactions

Masoud Mohseni¹ and Daniel A. Lidar²

¹Department of Physics and Center for Quantum Information and Quantum Control, University of Toronto, 60 St. George Street, Toronto, Ontario, Canada M5S 1A7

²Chemical Physical Theory Group, Chemistry Department, and Center for Quantum Information and Quantum Control, University of Toronto, 80 St. George Street, Toronto, Ontario, Canada M5S 3H6 (Received 25 June 2004; published 3 February 2005)

Quantum computation can be performed by encoding logical qubits into the states of two or more physical qubits, and control of effective exchange interactions and possibly a global magnetic field. This "encoded universality" paradigm offers potential simplifications in quantum computer design since it does away with the need to control physical qubits individually. Here we show how encoded universality schemes can be combined with fault-tolerant quantum error correction, thus establishing the scalability of such schemes.

DOI: 10.1103/PhysRevLett.94.040507

In the "standard paradigm" of quantum computing (QC) a universal set of quantum logic gates is enacted via the application of single-qubit gates, along with a nontrivial (entangling) two-qubit gate [1]. It is in this context that the theory of fault-tolerant quantum error correction (QEC) and the well-known associated threshold results (e.g., [2,3]) have been developed. These results are of crucial importance since they establish the in-principle viability of QC, despite the adverse effects of decoherence and inherently inaccurate controls. However, some of the assumptions underpinning the standard paradigm may translate into severe technical difficulties in the laboratory implementation of QC, in particular, in solid-state devices.

Any quantum system comes equipped with a set of "naturally available" interactions, i.e., interactions which are inherent to the system as determined by its symmetries, and are most easily controllable. For example, the symmetries of the Coulomb interaction dictate the special scalar form of the Heisenberg exchange interaction, which appears in a number of promising solid-state QC proposals [4]. The introduction of single-spin operations requires a departure from this symmetry and typically leads to complications, such as highly localized magnetic fields [5], powerful microwave radiation that can cause excessive heating, or g-tensor engineering/modulation [6]. For these reasons the "encoded universality" (EU) alternative to the standard paradigm has been developed, along with other alternatives [7]. In EU, single-qubit interactions with external control fields are replaced by "encoded" singlequbit operations, implemented on logical qubits via control of exchange interactions between their constituent physical qubits. It has been shown that such an exchangeonly approach is also capable of universal OC, on the (decoherence-free) subspace spanned by the encoded qubits [8]. Explicit pulse sequences have been worked out for the implementation of encoded logic gates in the case when only the exchange interaction is available [9,10], which can be simplified by assuming the controllability of a global magnetic field [11].

The issue of the robustness of EU-OC in the presence of decoherence has been addressed before [10], e.g., using a combination of decoherence-free subspaces (DFS's) and dynamical decoupling methods [12]. However, in contrast to the case of the standard paradigm, so far a theory of fault-tolerant QEC has not been developed for EU-QC. The difficulty originates from the fact that EU constructions use only a subspace of the full system Hilbert space and hence are subject to leakage errors to the orthogonal subspace. In particular, standard QEC theory breaks down under the restriction of using only a limited set of interactions, since these interactions are not universal over the orthogonal subspace, and cannot, using preestablished methods, be used to fix the leakage problem. Here we provide a fully constructive method for extending the theory of faulttolerant OEC so as to encompass EU-OC.

PACS numbers: 03.67.Lx, 03.65.Yz, 03.67.Pp

Encoded universality.—We first briefly review EU in the context of a particularly simple encoding of one logical qubit into the states of two neighboring physical qubits: $|0_L\rangle_i = |0_{2i-1}\rangle \otimes |1_{2i}\rangle, |1_L\rangle_i = |1_{2i-1}\rangle \otimes |0_{2i}\rangle,$ where $|0\rangle (|1\rangle)$ is the +1 (-1) eigenstate of σ_z . We refer to this encoding as a "two-qubit universal code" (2QUC), and more generally to EU encodings involving n qubits per logical qubit as "nQUC." In Ref. [11] it was shown how to construct a universal set of encoded quantum logic gates for the 2QUC, generated from the widely applicable class of exchange Hamiltonians of the form $H_{\rm ex} \equiv \sum_{i < i} H_{ij}$, where

$$H_{ij} = J_{ij}(X_i X_j + Y_i Y_j) + J_{ij}^z Z_i Z_j.$$
 (1)

Here X_i, Y_i, Z_i denote the Pauli matrices σ_x , σ_y , σ_z acting on the ith physical qubit. The Heisenberg interaction is the case $J_{ij} = J^z_{ij}$ (e.g., electron and nuclear spin qubits [4]), while the XXZ and XY models are, respectively, the cases $J_{ij} \neq J^z_{ij} \neq 0$ (e.g., electrons on helium [13]) and $J_{ij} \neq 0$, $J^z_{ij} = 0$ (e.g., quantum dots in cavities [14]). In essentially all pertinent QC proposals one can control the J_{ij} for $|i-j| \leq 2$, though not independently from J^z_{ij} . As usual in the EU discussion we do not assume that the technically

challenging single-qubit operations of the form $\sum f_i^x(t)X_i + f_i^y(t)Y_i$ are available. We do assume that a (global) free Hamiltonian $H_0 = \sum_i \frac{1}{2} \omega_i Z_i$ with nondegenerate ω_i 's can be exploited for QC in the sense that the ω_i are collectively controllable, e.g., via the application of a global magnetic field. Logical operations on and between 2QUC-encoded qubits (denoted by bars) were found in Ref. [11]. For example, single-encoded-qubit gates [encoded su(2)] are generated by $\overline{X}_{2i-1,2i}$ and $\overline{Z}_{2i-1,2i}$, where $\overline{X}_{ij} \equiv \frac{1}{2}(X_iX_j + Y_iY_j)$, $\overline{Z}_{ij} \equiv \frac{1}{2}(Z_i - Z_j)$. Then $|0_L\rangle_i^{\exp(-i\pi\overline{X}_{2i-1,2i})}|1_L\rangle_i$. Importantly, for all cases captured by H_{ij} universal encoded QC is possible via relaxed control assumptions, namely, control of only the parameters $J_{i,i+1}$ and a global magnetic field. These control assumptions (and measurements, discussed below) are the sole ones we make in this work.

Hybrid 2QUC-stabilizer codes.—Our solution for faulttolerant EU involves a concatenation of 20UC and stabilizer codes of QEC theory [1,2]. A stabilizer code is the subspace of the Hilbert space of n qubits that has eigenvalue +1 under the action of a given Abelian subgroup of the *n*-qubit Pauli group. The Pauli group is the group of *n*-fold tensor products of the Pauli matrices, including the identity matrix. We define a hybrid stabilizer-nQUC code (henceforth, "S-nQUC") as the stabilizer code in which each physical qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is replaced by the nQUC qubit state $|\psi_U\rangle = \alpha |0_U\rangle + \beta |1_U\rangle$ (concatenation). With this replacement X_i , Y_i , Z_i must be replaced by their encoded versions \overline{X}_i , \overline{Y}_i , \overline{Z}_i . Thus, physical-level operations on the stabilizer code are replaced by encodedlevel operations on the 2QUC. This replacement rule also applies to give the new stabilizer for the S-nQUC. For example, suppose we concatenate the 2QUC with the three-qubit phase-flip code $|+\rangle^{\otimes 3}$, $|-\rangle^{\otimes 3}$, where $|\pm\rangle$ $(|0\rangle \pm |1\rangle)/\sqrt{2}$. The stabilizer of the latter is generated by X_1X_2 , X_2X_3 . Then the stabilizer for the hybrid S-2QUC $\{|0_U\rangle = \frac{1}{2\sqrt{2}}(|01\rangle + |10\rangle)^{\otimes 3}, |1_U\rangle = \frac{1}{2\sqrt{2}}(|01\rangle - |10\rangle)^{\otimes 3}\} \text{ is }$ just $S = \{\overline{X}_1\overline{X}_2, \overline{X}_2\overline{X}_3\}, \text{ with } \overline{X}_i = X_{2i-1}X_{2i}.$

We assume that it is possible to make measurements directly in the 2QUC basis. This involves, e.g., distinguishing a singlet $(|01\rangle - |10\rangle)/\sqrt{2}$ from a triplet state $(|01\rangle + |10\rangle)/\sqrt{2}$, or performing a nondemolition measurement of the first qubit in each 2QUC logical qubit; these tasks are currently under active investigation, e.g., [15]. In conjunction with the encoded universal gate set, it is then evidently possible to perform the entire repertoire of quantum operations needed to compute fault tolerantly on the 2QUC, using standard stabilizer-QEC methods [1,2]. However, because our stabilizer code is built from 2QUC qubits, it is, a priori, not designed to fix errors on the physical qubits. Thus, our next task is to consider these physical-level errors

Physical phase flips.—Consider a physical phase-flip error afflicting an S-2QUC state $|\psi_U\rangle$, e.g., on the first

physical qubit. Its action in the case of the example above is $|0_U\rangle \mapsto \frac{1}{2\sqrt{2}}(|01\rangle - |10\rangle)(|01\rangle + |10\rangle)^{\otimes 2} \equiv |0_U'\rangle, |1_U\rangle \mapsto \frac{1}{2\sqrt{2}}(|01\rangle + |10\rangle)(|01\rangle - |10\rangle)^{\otimes 2} \equiv |1_U'\rangle.$ Since $|0_U'\rangle$ and $|1_U'\rangle$ are orthogonal, there exists a measurement that distinguishes between them. From the general theory of stabilizer codes we know that this is a measurement of one of the generators of the S-2QUC stabilizer. Indeed, it is simple to verify that measurement of either $\overline{X}_1\overline{X}_2$ or $\overline{X}_2 \dot{\overline{X}}_3$ (at least one of which anticommutes with Z_i , $1 \le 1$ $i \le 6$) will reveal the location of any single-physical-qubit phase flip, without collapsing the ("erred") state $\alpha |0_{IJ}'\rangle$ + $\beta|1_{II}'\rangle$. Moreover, one readily verifies that arbitrary products of phase-flip error operators anticommute with at least one of the stabilizer generators $\overline{X}_1\overline{X}_2$, $\overline{X}_2\overline{X}_3$ or have a trivial effect on $\alpha |0_U\rangle + \beta |1_U\rangle$. Therefore, the correctibility condition of errors on stabilizer codes [1,2] is satisfied, and hence a phase-flip error on any physical qubit in a hybrid S-2QUC is always correctible.

Physical bit flip.—In contrast to physical-level phase flips, bit flips, $\{X_{2i-1}, Y_{2i-1}, X_{2i}, Y_{2i}\}$, cause leakage from the 2QUC subspace via transitions to the orthogonal, "leakage" subspace spanned by $\{|0_{2i-1}0_{2i}\rangle, |1_{2i-1}1_{2i}\rangle\}$. Any gate of the form $\exp(-i\theta \overline{X}_{2i-1,2i})$, $\exp(-i\theta \overline{Z}_{2i-1,2i})$ acts as identity on this subspace and hence will fail to produce the desired effect if used to implement standard QEC operations.

Two-physical-qubit errors.—Finally we need to consider the case of two-physical-level errors affecting two qubits of the same 2QUC block. Listing all possible such errors we find that (i) $\{XX = \overline{X}, XY = -\overline{Y}, YX = \overline{Y}, YY = \overline{X}, ZZ = -\overline{I}\}$ act as single-encoded-qubit errors and thus are correctible by the stabilizer QEC and (ii) $\{XZ, YZ, ZX, ZY\}$ all act as leakage errors. We conclude that our task is to find a way to solve the leakage problem by using only the available interactions. We do this in two steps: first we construct a unitary "leakage correction unit" (LCU) assuming perfect pulses; then we consider fault tolerance in the presence of imperfections in the LCU and computational operations.

Leakage correction unit.—Let physical qubits 1, 2 (3, 4) encode a data (ancilla) 2QUC qubit. We assume that we can reliably prepare the ancilla in the state $|0_L\rangle$. We now define an LCU as the unitary operator L whose action, up to a global phase, on a data (first) and ancilla (second) 2QUC qubit is [10]

$$L|0_L\rangle|0_L\rangle = |0_L\rangle|0_L\rangle, \qquad L|2_L\rangle|0_L\rangle = |0_L\rangle|2_L\rangle, L|1_L\rangle|0_L\rangle = |1_L\rangle|0_L\rangle, \qquad L|3_L\rangle|0_L\rangle = |0_L\rangle|3_L\rangle,$$
(2)

where $|2_L\rangle \equiv |00\rangle$, $|3_L\rangle \equiv |11\rangle$. The action of L on the remaining 12 basis states is completely arbitrary. The LCU thus *conditionally* swaps a leaked data qubit with the ancilla, resetting the data qubit to $|0_L\rangle$; this corresponds to a logical error on the data qubit, which can be fixed by the stabilizer code. Note that L entangles the data and

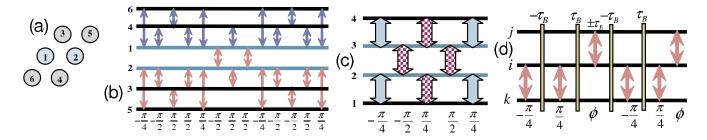


FIG. 1 (color online). Analytically derived circuits for the $\sqrt{\text{sWAP}^j}$ operation. Time flows from left to right. Data-physical qubits are numbered 1, 2, while 3–6 are ancilla-physical qubits. Ancilla qubits 5 and 6 are added to allow parallel operations within each LCU, which reduces the time overhead by a factor of 2. (a) The circles represent a possible arrangement of qubits so that all are nearest neighbors throughout the <u>pulse</u> sequence. (b) $\sqrt{\text{sWAP}^j}$ in the XY model: an angle ϕ under an arrow connecting qubits i,j represents the pulse $\exp(-i\phi \overline{X}_{ij})$. (c) $\sqrt{\text{sWAP}^j}$ in the Heisenberg or XXZ model: an angle ϕ under a solid (checkered) arrow connecting qubits i,j represents the pulse $\exp(-i\phi Z_i Z_j)$ [$\exp(-i\phi \overline{X}_{ij})$]. These pulses are, in turn, realized with the pulse sequence in (d), where the angle 2ϕ in (d) corresponds to the angles $\pm \pi/4$, $\pm \pi/2$ used in circuit (c). (d) Refocusing the Ising terms: each arrow represents a Heisenberg or XXZ exchange interaction between corresponding qubits. The choice $+\tau_E$ [$-\tau_E$] for the central pulse selects $\exp(-i2\phi Z_i Z_j)$, with $\phi = \frac{1}{\hbar} \int_{-i}^{\tau_E} J_{ij}^z(t) dt$ [$\exp(-i2\phi \overline{X}_{ij})$, with $\phi = \frac{2}{\hbar} \int_{-i}^{\tau_E} J_{ij}(t) dt$] used in circuit (c). Qubit indices are i,j=1,2,3,4 and i=1,2,3,4 and i=1,2,3,4 and i=1,2,3,4 and i=1,3,4 and i=

ancilla qubits, which means that we can determine with certainty if a leakage correction has occurred or not by measuring the state of ancilla. The generalization of Eq. (2) to an arbitrary nQUC is clear: L must conditionally swap any "leakage state" with $|0_L\rangle$ [10]. Constraints for the construction of L in the case of the 3QUC and Heisenberg-only computation were given in Ref. [10]. We next show, for the first time, how to construct the transformation L explicitly from the available interactions. Our construction is limited to the 2QUC case, but note that the 2QUC encompasses essentially all exchange interactions of interest [11], so that this is not a severe restriction. Finding explicit constructions for nQUCs with $n \geq 3$ is an open problem and will involve much higher overhead than the n = 2 case.

We decompose L in general as follows: $L = \sqrt{\text{SWAP}} \times \sqrt{\text{SWAP}'}$, where

$$\sqrt{\text{SWAP}} = \exp\left[-i\frac{\pi}{4}(\overline{X}_{13} + \overline{X}_{24})\right],\tag{3}$$

$$\sqrt{\text{SWAP}'} = \exp\left[-i\frac{\pi}{4}(\overline{X}_{13}Z_2Z_4 + \overline{X}_{24}Z_1Z_3)\right], \quad (4)$$

and $\exp[-i\frac{\pi}{4}\overline{X}_{ij}]$ is just the square root of the swap gate between physical qubits i and j. The gate $\sqrt{\text{SWAP}}$ applies this operation on qubits 1, 3 and 2, 4 in parallel. Depending on whether the eigenvalues of Z_2Z_4 and Z_1Z_3 are +1 or -1 on the four basis states of Eq. (2), the gates $\sqrt{\text{SWAP}}$ and $\sqrt{\text{SWAP}'}$ multiply constructively (destructively) to generate a full swap (identity). Equation (4) involves four-body spin interactions. Figure 1 shows how to construct these from available two-body interactions.

Overhead.—To assess the physical qubit and time resources associated with our method, we consider the typical switching times of global magnetic fields and exchange interactions. Using estimates from [7], a π rotation on an electron spin requires a current pulse of duration $\tau_{B} \approx$ 60 ns. For electron-spin qubits in quantum dots and in donor atoms (Heisenberg models) [4], and also for quantum dots in cavities (XY model) [14], in the adiabatic switching mode of $J_{ij}(t)$, the duration τ_E of a swap gate is 10-100 ps, while for exciton-coupled quantum dots (XY) model) $\tau_E \lesssim 1$ ps. For simplicity we now assume uniform values $\tau_B=10$ ns and $\tau_E=100$ ps. Thus, global magnetic field switching dominates the time overhead. We compute the time to implement the LCU, $\tau_{\rm LCU}$, using the circuits in Fig. 1. The number of exchange pulses for an LCU in the XY model is 14, and no global magnetic field is needed, yielding $\tau_{\rm LCU} \approx 1.4$ ns. The time $\tau_{\overline{\rm CNOT}}$ for a single-encoded controlled-NOT (CNOT) gate, which can be implemented using 15 exchange pulses and 6 global magnetic field pulses, is $\tau_{\overline{\text{CNOT}}} \approx 60 \text{ ns} \gg \tau_{\text{LCU}}$. For the XXZ and Heisenberg models an LCU requires 20 global magnetic field pulses and 31 exchange pulses, compared to 8 global and 14 exchange pulses for a CNOT. In this case $\tau_{\rm LCU} \approx 2.5 \tau_{\overline{\rm cnot}}$. These 10–100 ns time scales should be compared, e.g., to recent estimates of dephasing times $T_2 \sim 50 \ \mu s$ for electron spins in GaAs quantum dots [16].

Fault-tolerant computation on the S-2QUC.—So far we have assumed perfect gates. We now relax this assumption. Fault-tolerant computation is defined as a procedure in which if any component of a circuit fails, the number of errors that appears in each encoded block does not exceed the maximum number of errors that the code is designed to handle [1–3]. Transversal quantum operations, such as the

normalizer elements CNOT, phase, and Hadamard, are those which can be implemented in pairwise fashion over physical gubits. This ensures that an error from an encoded block of qubits cannot spread into more than one physical qubit in another encoded block of qubit [1–3]. Transversal operations become automatically fault tolerant. In order to construct a universal fault tolerant set of gates we should in addition be able to implement, e.g., a fault-tolerant encoded $\pi/8$ gate; although this gate is not transversal it can be realized by performing fault-tolerant measurements [1]. By inspection of Ref. [1], pp. 482-493, it is easy to see that all transversal operations and all operations needed to construct the $\pi/8$ gate, in particular, fault-tolerant measurements and cat-state preparation, can be done in the 2QUC basis using the EU-QC methods of Ref. [11], without any modification, as long as one can measure directly in the 2QUC basis (as discussed above). Hence, with respect to logical errors on the 2QUC qubits, the hybrid S-nQUC preserves all the required fault-tolerance properties.

This leaves the physical-level phase and bit flip errors during *encoded logic gates*. We already showed that phaseflip errors act as logical errors that the stabilizer-QEC can correct. Bit flip errors are more problematic: a single leakage error invalidates the stabilizer code block in which it occurs, since the QEC procedures are ineffective in the leakage subspace. Hence if such errors were to propagate during a logic operation such as encoded CNOT, they would—if left uncorrected—overwhelm the stabilizer level and result in catastrophic failure. The solution is to invoke the LCU after each logic operation, and before the QEC circuitry. The LCU turns a leakage error into a logical error, after which multilevel concatenated OEC [1–3] can correct these errors to arbitrary accuracy. However, uncontrolled leakage error propagation during QEC syndrome measurements must be avoided by applying LCU's to each 2QUC qubit after the cat-state preparation and before the verification step.

The final possibility we must contend with is leakage errors taking place during the operation of the LCU itself. Such a faulty LCU could incorrectly change the state of the ancilla qubit in Eq. (2). Therefore finding the ancilla in either $|00\rangle$ or $|11\rangle$ is an inconclusive result. Let p(s) be the probability of a success event in one trail LCU operation (this depends on accurate gating of the interaction Hamiltonian, etc.). Let $p(\omega) = \text{Tr}(\rho_f | 0_L) \langle 0_L |)$ be the probability of finding the ancilla qubit in the final state $|0_I\rangle$, where ρ_f represents the final entangled state of data qubit and ancilla $[p(\omega)]$ critically depends on the error model]. The probability, p(c), of achieving *conclusive* and correct information about the state of the data qubit (being in the logical subspace) is p(c) = $p(\omega \text{ and } s)/p(\omega)$. This is the conditional probability of LCU success when we already know that the ancilla is in state $|0_L\rangle$. Then 1-p(c) is the probability of achieving a *conclusive* but *wrong* result. We can arbitrarily boost the success probability of the LCU + measurement, $1-[1-p(c)]^n$, to be higher than some constant c_0 , by repeating this procedure until we obtain $n \ge \log_{1-p(c)}(1-c_0)$ consecutive no-leakage events.

Outlook.—By constructing error correction operations from a Hamiltonian formulation, as done here, rather than from gates as the elementary building blocks, an accurate calculation of the fault-tolerance threshold is possible. Previous threshold results cannot be directly used in the case of EU quantum computing, since leakage errors were considered to be negligible. However, in the EU case these errors are dominant and the extra resources needed for the implementation of the LCU's should be accounted for in a new threshold calculation.

Support from OGSST and NSERC (to M.M.), the DARPA-QuIST program (managed by AFOSR under Agreement No. F49620-01-1-0468), and the Sloan foundation (to D. A. L.) is gratefully acknowledged. We thank K. Khodjasteh and A. Shabani for useful discussions.

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation* and *Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).
- [2] D. Gottesman, quant-ph/9705052; J. Preskill, in Introduction to Quantum Computation and Information, edited by H. K. Lo, S. Popescu, and T. P. Spiller (World Scientific, Singapore, 1999).
- [3] E. Knill, R. Laflamme, and W. Zurek, Science 279, 342 (1998); A. M. Steane, Phys. Rev. A 68, 042322 (2003).
- [4] D. Loss and D.P. DiVincenzo, Phys. Rev. A 57, 120 (1998); B.E. Kane, Nature (London) 393, 133 (1998);
 R. Vrijen et al., Phys. Rev. A 62, 012306 (2000).
- [5] D. A. Lidar and J. H. Thywissen, J. Appl. Phys. 96, 754 (2004).
- [6] E. Yablonovitch et al., Proc. IEEE 91, 761 (2003).
- [7] L.-A. Wu, D. A. Lidar, and M. Friesen, Phys. Rev. Lett. 93, 030501 (2004).
- [8] D. Bacon et al., Phys. Rev. Lett. 85, 1758 (2000); J. Kempe et al., Phys. Rev. A 63, 042307 (2001).
- [9] D. P. DiVincenzo et al., Nature (London) 408, 339 (2000).
- [10] J. Kempe et al., Quantum Inf. Comput. 1, 33 (2001).
- [11] D. A. Lidar and L.-A. Wu, Phys. Rev. Lett. 88, 017905 (2002).
- [12] L.-A. Wu, M. S. Byrd, and D. A. Lidar, Phys. Rev. Lett. 89, 127901 (2002); L. Viola, Phys. Rev. A 66, 012307 (2002);
 Y. Zhang et al., Phys. Rev. A 69, 042315 (2004).
- [13] P. M. Platzman and M. I. Dykman, Science 284, 1967 (1999).
- [14] A. Imamoğlu et al., Phys. Rev. Lett. 83, 4204 (1999).
- [15] M. Friesen et al., Phys. Rev. Lett. 92, 037901 (2004).
- [16] R. de Sousa and S. Das Sarma, Phys. Rev. B 67, 033301 (2003).