Universal Fault-Tolerant Quantum Computation on Decoherence-Free Subspaces

D. Bacon,[1,2] J. Kempe,[1,3,4] D. A. Lidar,[1,*] and K. B. Whaley[1]

[1]*Department of Chemistry, University of California, Berkeley, California 94720*
[2]*Physics Department, University of California, Berkeley, California 94720*
[3]*Mathematics Department, University of California, Berkeley, California 94720*
[4]*École Nationale Superieure des Télécommunications, Paris, France 75634*

(Received 20 September 1999)

A general scheme to perform universal, fault-tolerant quantum computation within decoherence-free subspaces (DFSs) is presented. At most two-qubit interactions are required, and the system remains within the DFS throughout the entire implementation of a quantum gate. We show explicitly how to perform universal computation on clusters of the four-qubit DFS encoding one logical qubit each under spatially symmetric (collective) decoherence. Our results have immediate relevance to quantum computer implementations in which quantum logic is implemented through exchange interactions, such as the recently proposed spin-spin coupled quantum dot arrays and donor-atom arrays.

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

Decoherence-free subspaces (DFSs) have been recently proposed [1–3] to protect fragile quantum information against the detrimental effects of decoherence. This is especially important for quantum computation, where maintaining the quantum coherence of states forms the cornerstone of the promised speedup compared to classical computers [4]. Under certain assumptions about the symmetry of the noise processes, most notably spatially correlated errors, there exist subspaces of the system's Hilbert space that are not affected by the noise, and are thus decoherence free. Maintaining a system inside a DFS can therefore be thought of as a "passive" error-*prevention* scheme. It was shown recently that DFSs are robust under symmetry-breaking perturbations and are thus ideal codes for quantum *memory* [5]. Prior to the work reported here it was not known whether quantum *computation* on DFSs was possible without catastrophically taking the system outside the DFS [thus exposing it to (collective) errors] under realistic physical constraints. Realistic implementable gates are restricted to one- and two-body interactions and a finite number of measurements. Previous demonstrations of universal quantum computation on DFSs did not satisfy these criteria [3,6].

In this work we develop a formalism that allows us to find Hamiltonians involving only one- and two-qubit interactions, which can be used to implement universal quantum gates *without ever leaving the DFS.* When computation is performed in this manner the system is never exposed to errors, so that this approach is *naturally fault tolerant.* This is in marked contrast to "active" quantum error correction codes (QECCs) [7,8], where errors do take code words out of the code space, and fault tolerance requires a hefty overhead [9]. Moreover, when the symmetric noise process allowing for the existence of the DFS is perturbed, we show that it is possible nevertheless to completely stabilize the computation, fault tolerantly, by using a concatenation scheme with a QECC. This scheme, which we first proposed in [10], has the advantage that it operates with an error threshold that depends only on the *perturbing* error rate, and is thus particularly attractive considering the stringent requirement on the threshold for fault-tolerant quantum computation [9]. The formalism we develop here connects DFSs with the theory of stabilizer QECCs [11]. We apply it to derive gates in the important *collective decoherence* model (the decoherence mechanism expected to dominate in the solid state at very low temperatures), and explicitly construct a universal set of gates operating on clusters of four physical qubits that each encode one logical qubit. In conjuction with the concatenated code of [10], this suffices to implement universal fault-tolerant computation on DFSs *robustly.* Thus we show here that one can employ the full power of DFSs in preserving coherence not merely for quantum memory applications, but also for full-scale quantum computing. We outline an application of our results to a class of potential physical implementations of quantum computers, in which quantum logic is implemented through internal exchange interactions. This class includes the recently proposed spin-spin coupled quantum dot arrays [12] and the silicon-based nuclear quantum computer [13].

Conditions for decoherence-free subspaces.—Consider the dynamics of a system S coupled to a bath B which evolves unitarily under the combined system-bath Hamiltonian $\mathbf{H} = \mathbf{H}_S \otimes \mathbf{I}_B + \mathbf{I}_S \otimes \mathbf{H}_B + \sum_{\alpha=1}^{A} \mathbf{S}_\alpha \otimes \mathbf{B}_\alpha$, where $\mathbf{H}_S$ ($\mathbf{H}_B$) is the system (bath) Hamiltonian, $\mathbf{I}_S$ ($\mathbf{I}_B$) is the identity operator on the system (bath), and $\mathbf{S}_\alpha$ ($\mathbf{B}_\alpha$) acts solely on the system (bath). The last term in $\mathbf{H}$ is the interaction Hamiltonian $\mathbf{H}_I$. The evolution in a subspace $\tilde{\mathcal{H}}$ of the system Hilbert space $\mathcal{H}$ is *unitary* for all possible bath states if and only if (i)

$$\mathbf{S}_\alpha|\psi\rangle = c_\alpha|\psi\rangle, \qquad c_\alpha \in \mathbb{C} \tag{1}$$

for all states $|\psi\rangle$ which span $\tilde{\mathcal{H}}$, and for every operator $\mathbf{S}_\alpha$ in $\mathbf{H}_I$, (ii) S and B are initially decoupled, and (iii) $\mathbf{H}_S|\psi\rangle$ has no overlap with states in the subspace orthogonal to $\tilde{\mathcal{H}}$ [1,10]. A subspace of $\mathcal{H}$ which fullfills these requirements is a *decoherence-free subspace.* It is important to notice that if condition (iii) is not fulfilled then states leak out of the DFS, and the usefulness of these subspaces for the storage of quantum information is lost.

General stabilizer formalism.—In order to identify a set of fault-tolerant universal gates for computation on a DFS, and to make a more explicit connection to QECCs, we recast the definition of a DFS [Eq. (1)] into the *stabilizer formalism.* By analogy to QECC [11], we define the *DFS stabilizer* S as a set of operators $\mathbf{D}_\beta$ which act as identity on the DFS states:

$$\mathbf{D}_\beta|\psi\rangle = |\psi\rangle, \quad \forall\, \mathbf{D}_\beta \in S, \quad \text{iff } |\psi\rangle \in \text{DFS}. \tag{2}$$

Here β can be a discrete or continuous index; S can form a finite set or group. Our S is a generalization of the QECC stabilizers which restrict S to an Abelian subgroup of the Pauli group (the group formed by tensor products of Pauli matrices on the qubits) [11]. While some DFSs can also be specified by a stabilizer in the Pauli group [14], many DFSs are specified by non-Abelian groups, and hence are *nonadditive* codes [15]. The stabilizer of a QECC allows identification of the errors the code can correct. In general an error process can be described by the Kraus operator-sum formalism [8]: $\rho \to \sum_\mu \mathbf{A}_\mu \rho \mathbf{A}_\mu^\dagger$. The Kraus operators $\mathbf{A}_\mu$ can be expanded in a basis $\mathbf{E}_i$ of "errors." Two types of errors can be dealt with by stabilizer codes: (i) errors $\mathbf{E}_i^\dagger \mathbf{E}_j$ that anticommute with any $\mathbf{S} \in S$, and (ii) errors that are part of the stabilizer ($\mathbf{E}_i \in S$). The first class is errors that require active correction; the second class is "degenerate" errors that do not affect the code at all. A duality between QECCs and DFSs can be stated as follows: QECCs were designed primarily to deal with type (i) errors, but can also be regarded as DFSs for the errors in their stabilizer [14]. Conversely, DFSs were designed primarily to deal with type (ii) errors, but can in principle be used as a QECC against errors that are type (i) with respect to S.

Consider now the following continuous index stabilizer:

$$\mathbf{D}(v_0, v_1, \ldots, v_A) = \mathbf{D}(\vec{v}) = \exp\left[\sum_{\alpha=1}^{A} (c_\alpha \mathbf{I} - \mathbf{S}_\alpha) v_\alpha\right]. \tag{3}$$

Clearly, the DFS condition [Eq. (1)] implies that $\mathbf{D}(\vec{v})|\psi\rangle = |\psi\rangle$. Conversely, if $\mathbf{D}(\vec{v})\,|\psi\rangle = |\psi\rangle$ for all $\vec{v}$, then, in particular, it must hold that for each α, $\exp[(c_\alpha \mathbf{I} - \mathbf{S}_\alpha)v_\alpha]\,|\psi\rangle = |\psi\rangle$. Recalling that $\phi(\mathbf{A}) = \exp[\mathbf{A}]$ is a one-to-one continuous mapping of a small neighborhood of the zero matrix $\mathbf{0}$ onto a small neighborhood of the identity matrix $\mathbf{I}$, it follows that there must be a sufficiently small v_α such that $(c_\alpha \mathbf{I} - \mathbf{S}_\alpha)\,|\psi\rangle = 0$. Therefore the DFS condition (1) holds if and only if $\mathbf{D}(\vec{v})\,|\psi\rangle = |\psi\rangle$ for all $\vec{v}$.

In order to achieve general-purpose *universal* quantum computation one must demonstrate that one can perform a set of operations (gates) $\mathbf{U}$ which allow for the implementation of nearly every unitary operation on the quantum computer (dense in the set of unitary operations) [16]. In analogy to computation using physical qubits, for universal computation on DFSs two types of gates will be needed: (i) gates performing operations within a DFS; and (ii) gates linking two or more DFS *clusters* (thus performing operations between logical qubits encoded into different clusters). The stabilizer formalism is useful for identifying allowed gates that take code words to code words [11]. The *allowed* operations $\mathbf{U}$ transform the stabilizer into itself. Let $|\psi\rangle \in \tilde{\mathcal{H}}$, i.e., $\mathbf{D}(\vec{v})\,|\psi\rangle = |\psi\rangle$. For $\mathbf{U}$ to be an allowed operation, $\mathbf{U}|\psi\rangle$ must be in $\tilde{\mathcal{H}}$, so $\mathbf{D}(\vec{v}\,')(\mathbf{U}|\psi\rangle) = \mathbf{U}|\psi\rangle$. This means $\mathbf{U}\mathbf{D}(\vec{v})\mathbf{U}^\dagger = \mathbf{D}[\vec{v}\,'(\vec{v})]$ and the $\mathbf{D}[\vec{v}\,'(\vec{v})]$ must cover S. It is sufficient to have $\vec{v}\,'(\vec{v})$ to be a one-to-one mapping. If S is a unitary group then the set of allowed gates is the *normalizer* of S [17]. To derive a similar condition for (ii) which involves gates between two different DFS clusters with stabilizers S_1 and S_2, we note that $S_{12} = S_1 \otimes S_2$ is a stabilizer for the two DFS clusters. The gates $\mathbf{U}$ are unitary transformations performed by switching on Hamiltonians $\mathbf{H}$ for some time t, acting on physical qubits in the DFS. So far we required only that the action of the gate preserve the subspace at the conclusion of the gate operation, but not that the subspace be preserved throughout the entire duration of the gate operation. By posing the stronger requirement that *the state of the system stays inside the DFS during the entire switching time of the gate* we achieve *natural fault tolerance* on the DFS. Rewriting our condition as $\mathbf{U}(t)\mathbf{D}(\vec{v}) = \mathbf{D}[\vec{v}\,'(\vec{v})]\mathbf{U}(t)$, taking the derivative with respect to t and evaluating this at $t = 0$ we obtain:

Theorem: A sufficient condition for the generating Hamiltonian to keep the state at all times entirely within the DFS is $\mathbf{H}\mathbf{D}(\vec{v}) = \mathbf{D}[\vec{v}\,'(\vec{v})]\mathbf{H}$ where $\vec{v}\,'(\vec{v})$ is one to one and time independent.

Collective decoherence.—We now focus on a particularly important system-bath interaction model, in which clusters of several qubits couple to the same bath mode: the *collective decoherence* model. Specifically, the interaction Hamiltonian is of the form $\mathbf{H}_I = \sum_{\alpha=x,y,z} \mathbf{S}_\alpha \otimes \mathbf{B}_\alpha$, where $\mathbf{S}_\alpha \equiv \sum_{j=1}^{K} \sigma_\alpha^j$ and σ_α^j are the Pauli matrices applied to the jth qubit. The $\mathbf{S}_\alpha$ form the (semisimple) Lie algebra $su(2)$ and the DFS condition (1) becomes $\mathbf{S}_\alpha|\psi\rangle = 0$ [3]. The stabilizer for the collective decoherence DFS [Eq. (3)] is given by

$$\mathbf{D}(\vec{v}) = e^{i\vec{v}\cdot\vec{\mathbf{S}}} \bigotimes_{J=1}^{K} [\mathbf{I}^j \cos \|\vec{v}\| \\ + \vec{\sigma}^j \cdot \vec{v}/\,\|\vec{v}\| \sin \|\vec{v}\|]$$

where $\vec{\mathbf{S}} = (\mathbf{S}_x, \mathbf{S}_y, \mathbf{S}_z)$ and $\|\vec{v}\| \equiv (\sum_\alpha v_\alpha^2)^{1/2}$ may be complex. $\mathbf{D}(\vec{v})$ consists of all collective qubit rotations + contractions, i.e., an operation of the form $\mathbf{G}^{\otimes K}$ where $\mathbf{G}(\vec{v})$ is any element in $SL(2)$. The smallest number of physical qubits yielding a full "encoded DFS qubit" is four [1], given by the two states with 0 total angular momentum:

$$|0_L\rangle = |s\rangle \otimes |s\rangle,$$
$$|1_L\rangle = \frac{1}{\sqrt{3}}[|t_+\rangle \otimes |t_-\rangle - |t_0\rangle \otimes |t_0\rangle + |t_-\rangle \otimes |t_+\rangle], \tag{4}$$

where $|s\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ is the singlet state of two qubits, and $|t_{-,0,+}\rangle = \{|00\rangle, (|01\rangle + |10\rangle)/\sqrt{2}, |11\rangle\}$ are the corresponding triplet states. Let $\tilde{\mathcal{H}}_4 = \{|0_L\rangle, |1_L\rangle\}$; $\tilde{\mathcal{H}}_4$ is immune to all errors which can be written as sums of collective operations of the form $\mathbf{G}^{\otimes 4}$. In addition it is easy to check that $\tilde{\mathcal{H}}_4$ is a distance-2 QECC [8,18], meaning that it can *detect* arbitrary single qubit errors.

Universal gates for a logical qubit.—We now apply the general formalism developed above to derive a set of universal gates on clusters of four-qubit DFSs under collective decoherence. While it is certainly desirable to consider computation using DFSs over arbitrary block size [18], it is important to realize that the encoding into $L = K/4$ blocks of four is entirely sufficient to implement universal "encoded quantum computation" over $\tilde{\mathcal{H}}_4^{\otimes L}$. The four-qubit DFS is also of special interest in the concatenation scheme proposed in [10]. There the DFS qubit of Eq. (4) becomes the building block for a QECC that protects against perturbing single physical qubit errors. By using DFS qubits instead of physical qubits, the resulting concatenated code offers an error threshold for fault-tolerant computation that depends only on the *perturbing* single qubit error rate. However, the threshold for QECC relies heavily on the ability to perform error correction (i.e., "computation") which does not catastrophically create more errors than it fixes (fault tolerance). Concatenated DFS-QEC codes will be efficient only if (i) a realistic (no more than two-body interactions) set of universal quantum gates keeping states entirely *within* the DFS is used, and (ii) preparation and decoding of DFS states are performed fault tolerantly. Here we provide such a set of universal quantum gates, and detail the preparation and decoding of DFS states.

It is sufficient to be able to apply (i) all single qubit rotations $[SU(2)]$ together with (ii) the two-qubit controlled phase gate ($\mathbf{C}_P$ defined below) on any two logical qubits, in order to perform any unitary transformation [19]. We now show how to construct this universal set of gates. The stabilizer for the four-qubit DFS $\tilde{\mathcal{H}}_4$ is of the form $\mathbf{D}(\vec{v}) = \mathbf{G}^{\otimes 4}$, which is manifestly invariant under permutations of the qubits. The Hermitian exchange (transposition) operation that switches only qubits i and j, $\mathbf{E}_{ij}|x\rangle_i|y\rangle_j = |y\rangle_i|x\rangle_j$ ($x, y = 0$ or 1), leaves the stabilizer element-wise invariant and so trivially fulfills the conditions of the Theorem (with $\vec{v}\,' = \vec{v}$). Thus $\exp[-i\theta\mathbf{E}_{ij}]$ preserves the DFS, and is a valid unitary operation by a two physical qubit Hamiltonian (see also [20]). Consider the action of $\mathbf{E}_{ij}$ on the basis states of Eq. (4): $\mathbf{E}_{12} = \mathbf{E}_{34}$ acting on these states takes $|0_L\rangle \to -|0_L\rangle$ and $|1_L\rangle \to |1_L\rangle$. $-\mathbf{E}_{12}$ thus acts as the encoded σ_z ($\bar{Z}$—a bar indicates operations on the encoded DFS qubits). Furthermore, $\mathbf{E}_{13} = \mathbf{E}_{24}$ applied to the basis states in Eq. (4) acts as

$$\mathbf{E}_{13} = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}. \tag{5}$$

Thus $\mathbf{H}_x = -(2/\sqrt{3})(\mathbf{E}_{13} + \frac{1}{2}\mathbf{E}_{12})$ acts as an encoded σ_x ($\bar{X}$) on the DFS qubit. $\mathbf{H}_x$ can be implemented either by turning on the two-qubit Hamiltonians at the same time, or approximated by using a finite number of terms in the Lie sum formula: $e^{i(\alpha A + \beta B)} = \lim_{n\to\infty}(e^{i\alpha A/n}e^{i\beta B/n})^n = e^{i\alpha A/n}e^{i\beta B/n} + O(1/n^2)$. The ability to implement $\bar{Z}$ and $\bar{X}$ is sufficient to complete the Lie algebra $\overline{su(2)}$, and thus to implement any gate in $SU(2)$ on the encoded qubits. This can be done using an Euler angle construction for the desired gate as is done routinely in NMR [21], or, following the standard arguments for universality [19], through an approximation to the Lie product formula $e^{[A,B]} = \lim_{n\to\infty} Q^n = Q + O(1/n^{3/2})$, where $Q = e^{iA/\sqrt{n}}e^{iB/\sqrt{n}}e^{-iA/\sqrt{n}}e^{-iB/\sqrt{n}}$. We note that the Euler angle construction is in general simpler to implement in practical implementations because it does not require extremely fast switching, but we defer the construction of optimal gate sequences to future work. To conclude, *we can generate any $SU(2)$ operation on the encoded qubits by simply turning on and off the appropriate two-qubit exchange Hamiltonian.*

To complete the universal set of gates we explicitly construct an encoded controlled phase gate $\bar{\mathbf{C}}_P$ between two DFS qubits (i.e., two separate four-qubit DFS clusters). In doing so we assume that the qubits are physically close during the gate switching time, so that they form an eight-qubit, 14-dimensional collective decoherence DFS $\tilde{\mathcal{H}}_8$ (see [20] for a derivation of a general dimension formula). Four of these 14 dimensions are spanned by the two four-qubit DFSs ($\tilde{\mathcal{H}}_4 \otimes \tilde{\mathcal{H}}_4$). Given two clusters of K physical qubits each, the exchange interaction between any two qubits preserves $\tilde{\mathcal{H}}_{2K}$, since the stabilizer is just $\mathbf{G}^{\otimes 2K}$. Thus a sequence of gates constructed purely out of exchange operations will *never* take the system out of $\tilde{\mathcal{H}}_{2K}$. Remarkably, exchange interactions alone can be shown to generate the full (special) unitary group on any collective DFS $\tilde{\mathcal{H}}_{2K}$ (in particular, $K = 4$) [18]. Therefore generating $\bar{\mathbf{C}}_P$ is a matter of finding an appropriate explicit construction, which we now present. Defining $\mathbf{h}_1 = [\mathbf{E}_{26}, \mathbf{E}_{12} + \mathbf{E}_{25}] + [\mathbf{E}_{15}, \mathbf{E}_{12} + \mathbf{E}_{16}]$, $\mathbf{h}_2 = \sum_{j=5}^{8}(\mathbf{E}_{1j} + \mathbf{E}_{2j})$, and $\mathbf{c} = \frac{1}{32}[\mathbf{h}_1, (\mathbf{h}_2, \mathbf{h}_1)]$, a calculation shows that $\mathbf{c}$ acts on the two four-qubit DFSs as $|0_L0_L\rangle \to 0$, $|0_L1_L\rangle \to |0_L1_L\rangle$, $|1_L0_L\rangle \to 0$, and $|1_L1_L\rangle \to 0$. The Hamiltonian $\mathbf{c}$ then yields a controlled phase gate by exponentiation: $\bar{\mathbf{C}}_P(\theta) = \exp[i\mathbf{c}\theta]$. The action of $\mathbf{c}$ can be understood as follows: (i) $\mathbf{h}_1$ takes states from $\tilde{\mathcal{H}}_4 \otimes \tilde{\mathcal{H}}_4$ into $\tilde{\mathcal{H}}_8$; (ii) $\mathbf{h}_2$ then applies a phase to a single one of the states in $\tilde{\mathcal{H}}_8$; (iii) $\mathbf{h}_1$ returns the states from $\tilde{\mathcal{H}}_8$ into $\tilde{\mathcal{H}}_4 \otimes \tilde{\mathcal{H}}_4$. *We have thus explicitly constructed a naturally fault-tolerant universal set of gates, which utilizes only two-body exchange interactions.*

It remains to be shown that it is possible to prepare and decode states in the DFS fault tolerantly. We first note that the $|0_L\rangle$ state of Eq. (4) can be constructed by simply preparing two pairs of qubits in the singlet state (in general for $K \geq 4$ qubits the state $|0_L\rangle$ can always be chosen to be a product of singlets). All the other DFS states (like $|1_L\rangle$) can be obtained by applying the appropriate encoded operation to $|0_L\rangle$ (like $\bar{X}$). To verify correct state preparation and to decode we need *fault-tolerant* measurements in the encoded computational basis $\{|0_L\rangle, |1_L\rangle\}$ (eigenstates of $\bar{Z}$). It is easily checked that measuring $\{\sigma_z^1, \sigma_z^2, \sigma_x^3, \sigma_x^4\}$ on the four qubits allows one to distinguish $|0_L\rangle$ and $|1_L\rangle$ but destroys the DFS state. To perform a fault-tolerant and nondestructive measurement of $\bar{Z}$ we require ancilla states prepared in the DFS state $|0_L\rangle$ and an encoded controlled-not ($\bar{\mathbf{C}}_X$) gate, which we have at our disposal from the construction of universal gates above [$\bar{\mathbf{C}}_X$ acts as $|x_L, y_L\rangle \rightarrow |x_L, (x_L + y_L)\text{mod}2\rangle$, where $x, y = 0$ or 1]. By applying a $\bar{\mathbf{C}}_X$ gate between the DFS state to be measured and the ancilla, and performing a destructive measurement on the ancilla, we obtain a nondestructive measurement of $\bar{Z}$, which is tolerant of collective errors on the two DFSs. To prevent possible uncontrolled error propagation caused by an incorrectly prepared ancilla, we prepare multiple $|0_L\rangle$ ancillas and apply $\bar{\mathbf{C}}_X$'s between the DFS state to be measured and each ancilla. Together with majority voting this provides a fault-tolerant method for measuring $\bar{Z}$ [11]. This procedure can also be used to verify the preparation of $|0_L\rangle$, and thus assures fault-tolerant DFS-state preparation.

Application to solid-state quantum computer implementations.—Two of the most promising proposals for quantum computer implementations, the spin-spin coupled quantum dots [12] and the Si:^{31}P nuclear spin array [13], rely on controllable exchange interactions for the implementation of quantum logic. The pertinent part of the internal Hamiltonian is of the Heisenberg type: $\mathbf{H}_{\text{Heis}} = \frac{1}{2}\sum_{i\neq j} J_{ij}\mathbf{S}_i \cdot \mathbf{S}_j$. Here $\mathbf{S}_i = (\sigma_x^i, \sigma_y^i, \sigma_z^i)$ is the Pauli matrix vector of spin i and J_{ij} are exchange coefficients, tunable by variation of external parameters such as local electric and magnetic fields. It is easily checked that $\mathbf{E}_{ij} \equiv \frac{1}{2}(\mathbf{I}_S + \mathbf{S}_i \cdot \mathbf{S}_j)$ is an exchange operator of physical qubits i and j [22]. Details of the tuning of the J_{ij} were worked out in [12,13], and show high sensitivity to externally applied electric and magnetic fields. A range of about 0–1 meV is attainable in quantum dots [12] by tuning the magnetic field through 0–2 T. *Thus* $\mathbf{H}_{\text{Heis}}$ *is a sum over exchange terms with tunable coefficients, and can be used to implement quantum computation over a DFS as detailed above.* A magnetic field ≥2 T and a temperature ≤100 mK are required in the Si:^{31}P proposal in order that the electrons occupy only the lowest energy bound state at the ^{31}P donor [13]. At these extremely low temperatures we expect that collective decoherence conditions are attained (also in coupled quantum dots), since only the longest wavelength phonon modes are occupied [23], to which the qubits are then coupled collectively [1,20]. Our results therefore imply that quantum computation on DFSs in nuclear spin arrays and quantum dots should be possible with carefully controlled exchange interactions.

In summary, we have derived general conditions for fault-tolerant quantum computation on a DFS, and shown how to implement a universal set of gates for the important case of collective decoherence by turning on/off only two-qubit exchange Hamiltonians. In our construction the system *never* leaves the DFS during the entire execution of a gate, so that fault tolerance is natural and, in stark contrast to the usual situation in quantum error correction, necessitates no extra resources during the computation. Our results are directly applicable to any quantum computer architecture in which quantum logic is implemented using exchange interactions, in particular, to some of the recent promising solid-state proposals for quantum computation.

This material is based upon work supported by the U.S. Army Research Office under Contract/Grant No. DAAG55-98-1-0371. We thank Kenneth Brown for useful discussions.

*Permanent address: Department of Chemistry, 80 St. George Street, University of Toronto, Toronto, Ontario, Canada M5S 3H6.

[1] P. Zanardi and M. Rasetti, Mod. Phys. Lett. B **11**, 1085 (1997); Phys. Rev. Lett. **79**, 3306 (1997).
[2] L.-M. Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998).
[3] D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[4] J. Preskill, Proc. R. Soc. London A **454**, 469 (1998).
[5] D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **60**, 1944 (1999).
[6] P. Zanardi, Phys. Rev. A **60**, R729 (1999).
[7] A. R. Calderbank and P. Shor, Phys. Rev. A **54**, 1098 (1996); A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[8] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[9] D. Aharonov and M. Ben-Or, quant-ph/9906129; E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998).
[10] D. A. Lidar, D. Bacon, and K. B. Whaley, Phys. Rev. Lett. **82**, 4556 (1999).
[11] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[12] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998); G. Burkard, D. Loss, and D. P. DiVincenzo, Phys. Rev. B **59**, 2070 (1999); X. Hu and S. Das Sarma, Phys. Rev. A **61**, 062301 (2000).
[13] B. E. Kane, Nature (London) **393**, 133 (1998).
[14] D. A. Lidar *et al.,* quant-ph/9908064; quant-ph/0007013.
[15] E. M. Rains *et al.,* Phys. Rev. Lett. **79**, 953 (1997).
[16] S. Lloyd, Phys. Rev. Lett. **75**, 346 (1995).
[17] D. Gottesman, Phys. Rev. A **57**, 127 (1997).
[18] J. Kempe *et al.,* quant-ph/0004064.
[19] D. P. DiVincenzo, Phys. Rev. A **51**, 1015 (1995).
[20] D. A. Lidar *et al.,* Phys. Rev. A **61**, 052307 (2000).
[21] C. P. Slichter, *Principles of Magnetic Resonance* (Springer, Berlin, 1996).
[22] M. B. Ruskai, Phys. Rev. Lett. **95**, 194 (2000).
[23] See, e.g., T. Takagahara, J. of Lumin. **70**, 129 (1996) for a case study in semiconductor nanocrystals.