Error-correcting codes for adiabatic quantum computation

Stephen P. Jordan,[1,*] Edward Farhi,[1] and Peter W. Shor[2]

[1]*Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

[2]*Mathematics Department, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Received 20 March 2006; published 14 November 2006)

Recently, there has been growing interest in using adiabatic quantum computation as an architecture for experimentally realizable quantum computers. One of the reasons for this is the idea that the energy gap should provide some inherent resistance to noise. It is now known that universal quantum computation can be achieved adiabatically using two-local Hamiltonians. The energy gap in these Hamiltonians scales as an inverse polynomial in the number of quantum gates being simulated. Here we present stabilizer codes which can be used to produce a constant energy gap against one-local and two-local noise. The corresponding fault-tolerant universal Hamiltonians are four-local and six-local, respectively, which are the optimal result achievable within this framework.

DOI: 10.1103/PhysRevA.74.052322 PACS number(s): 03.67.Pp

Adiabatic quantum computation was originally proposed by Farhi *et al.* as a method for solving combinatorial optimization problems [1]. In this scheme, one starts with a Hamiltonian whose ground state is easy to construct, and gradually varies the Hamiltonian into one whose ground state encodes the solution to a computational problem. By the adiabatic theorem, the system will remain in the instantaneous ground state provided that the Hamiltonian is varied sufficiently slowly. More precisely, any closed system acted on by $H(t/T)$ from $t=0$ to T will remain in the ground state with high probability provided that T is sufficiently large. Different formulations [2–5] of the adiabatic theorem yield different conditions on T, but essentially the minimal T scales polynomially with the inverse eigenvalue gap between the ground state and first excited state.

Recently, there has been growing interest in using adiabatic quantum computation as an architecture for experimentally realizable quantum computers. Aharonov *et al.* [6], building on ideas by Feynman [7] and Kitaev [8], showed that any quantum circuit can be simulated by an adiabatic quantum algorithm. The energy gap for this algorithm scales as an inverse polynomial in G, the number of gates in the original quantum circuit. G is identified as the running time of the original circuit. By the adiabatic theorem, the running time of the adiabatic simulation is polynomial in G. Because the slowdown is only polynomial, adiabatic quantum computation is a form of universal quantum computation.

Most experimentally realizable Hamiltonians involve only few-body interactions. Thus theoretical models of quantum computation are usually restricted to involve interactions between at most some constant number of qubits k. Any Hamiltonian on n qubits can be expressed as a linear combination of terms, each of which is a tensor product of n Pauli matrices, where we include the 2×2 identity as a fourth Pauli matrix. If each of these tensor products contains at most k Pauli matrices not equal to the identity then the Hamiltonian is said to be k-local. The Hamiltonian used in the universality construction of [6] is three-local throughout the time evolution. Kempe *et al.* subsequently improved this to two-local in Ref. [9].

Schrödinger's equation shows that, for any constant g, $gH(gt)$ yields the same time evolution from time 0 to T/g that $H(t)$ yields from 0 to T. Thus, the running time of an adiabatic algorithm would not appear to be well defined. However, in any experimental realization there will be a limit to the magnitude of the fields and couplings. Thus it is reasonable to limit the norm of each term in $H(t)$. Such a restriction enables one to make statements about how the running time of an adiabatic algorithm scales with some measure of the problem size, such as G.

One of the reasons for interest in adiabatic quantum computation as an architecture is the idea that adiabatic quantum computers may have some inherent fault tolerance [10–14]. Because the final state depends only on the final Hamiltonian, adiabatic quantum computation may be resistant to slowly varying control errors, which cause $H(t)$ to vary from its intended path, as long as the final Hamiltonian is correct. An exception to this would occur if the modified path has an energy gap small enough to violate the adiabatic condition. Unfortunately, it is generally quite difficult to evaluate the energy gap of arbitrary local Hamiltonians.

Another reason to expect that adiabatic quantum computations may be inherently fault tolerant is that the energy gap should provide some inherent resistance to noise caused by stray couplings to the environment. Intuitively, the system will be unlikely to get excited out of its ground state if k_bT is less than the energy gap. Unfortunately, in most proposed applications of adiabatic quantum computation, the energy gap scales as an inverse polynomial in the problem size. Such a gap only affords protection if the temperature scales the same way. However, a temperature which shrinks polynomially with the problem size may be hard to achieve experimentally.

To address this problem, we propose taking advantage of the possibility that the decoherence will act independently on the qubits. The rate of decoherence should thus depend on the energy gap against local noise. We construct a class of stabilizer codes such that encoded Hamiltonians are guaranteed to have a constant energy gap against single-qubit exci-

[*] Electronic address: sjordan@mit.edu

tations. These stabilizer codes are designed so that adiabatic quantum computation with four-local Hamiltonians is universal for the encoded states. We illustrate the usefulness of these codes for reducing decoherence using a noise model, proposed in Ref. [10], in which each qubit independently couples to a photon bath.

To protect against decoherence we wish to create an energy gap against single-qubit disturbances. To do this we use a quantum error-correcting code such that applying a single Pauli operator to any qubit in a codeword will send this state outside of the code space. Then we add an extra term to the Hamiltonian which gives an energy penalty to all states outside the codespace. Since we are only interested in creating an energy penalty for states outside the code space, only the fact that an error has occurred needs to be detectable. Since we are not actively correcting errors, it is not necessary for distinct errors to be distinguishable. In this sense, our code is not truly an error-correcting code but rather an error-detecting code. Such passive error correction is similar in spirit to ideas suggested for the circuit model in Ref. [15].

It is straightforward to verify that the four-qubit code

$$|0_L\rangle = \frac{1}{2}(|0000\rangle + i|0011\rangle + i|1100\rangle + |1111\rangle), \tag{1}$$

$$|1_L\rangle = \frac{1}{2}(-|0101\rangle + i|0110\rangle + i|1001\rangle - |1010\rangle) \tag{2}$$

satisfies the error-detection requirements, namely,

$$\langle 0_L|\sigma|0_L\rangle = \langle 1_L|\sigma|1_L\rangle = \langle 0_L|\sigma|1_L\rangle = 0, \tag{3}$$

where σ is any of the three Pauli operators acting on one qubit. Furthermore, the following two-local operations act as encoded Pauli X, Y, and Z operators:

$$X_L = Y \otimes I \otimes Y \otimes I,$$

$$Y_L = -I \otimes X \otimes X \otimes I,$$

$$Z_L = Z \otimes Z \otimes I \otimes I. \tag{4}$$

That is,

$$X_L|0_L\rangle = |1_L\rangle, \qquad X_L|1_L\rangle = |0_L\rangle,$$

$$Y_L|0_L\rangle = i|1_L\rangle, \qquad Y_L|1_L\rangle = -i|0_L\rangle,$$

$$Z_L|0_L\rangle = |0_L\rangle, \qquad Z_L|1_L\rangle = -|1_L\rangle.$$

An arbitrary state of a single qubit $\alpha|0\rangle+\beta|1\rangle$ is encoded as $\alpha|0_L\rangle+\beta|1_L\rangle$.

Starting with an arbitrary two-local Hamiltonian H on N bits, we obtain a new fault tolerant Hamiltonian on $4N$ bits by the following procedure. An arbitrary two-local Hamiltonian can be written as a sum of tensor products of pairs of Pauli matrices acting on different qubits. After writing out H in this way, make the following replacements:

$$I \to I^{\otimes 4}, \qquad X \to X_L, \qquad Y \to Y_L, \qquad Z \to Z_L$$

to obtain a new four-local Hamiltonian H_{SL} acting on $4N$ qubits. The total fault tolerant Hamiltonian H_S is

$$H_S = H_{SL} + H_{SP}, \tag{5}$$

where H_{SP} is a sum of penalty terms, one acting on each encoded qubit, providing an energy penalty of at least E_p for going outside the code space. We use the subscript S to indicate that the Hamiltonian acts on the system, as opposed to the environment, which we introduce later. Note that H_{SL} and H_{SP} commute, and thus they share a set of simultaneous eigenstates.

If the ground space of H is spanned by $|\psi^{(1)}\rangle \cdots |\psi^{(m)}\rangle$ then the ground space of H_S is spanned by the encoded states $|\psi_L^{(1)}\rangle \cdots |\psi_L^{(m)}\rangle$. Furthermore, the penalty terms provide an energy gap against one-local noise which does not shrink as the size of the computation grows.

The code described by Eqs. (1) and (2) can be obtained using the stabilizer formalism [16,17]. In this formalism, a quantum code is not described by explicitly specifying a set of basis states for the code space. Rather, one specifies the generators of the stabilizer group for the code space. Let G_n be the Pauli group on n qubits (i.e., the set of all tensor products of n Pauli operators with coefficients of ± 1 or $\pm i$). The stabilizer group of a code space C is the subgroup S of G_n such that $x|\psi\rangle = |\psi\rangle$ for any $x \in S$ and any $|\psi\rangle \in C$.

A 2^k-dimensional code space over n bits can be specified by choosing n-k independent commuting generators for the stabilizer group S. By independent we mean that no generator can be expressed as a product of others. In our case we are encoding a single qubit using four qubits, thus $k=1$ and $n=4$, and we need three independent commuting generators for S.

To satisfy the orthogonality conditions, listed in Eq. (3), which are necessary for error detection, it suffices for each Pauli operator on a given qubit to anticommute with at least one of the generators of the stabilizer group. The generators

$$g_1 = X \otimes X \otimes X \otimes X,$$

$$g_2 = Z \otimes Z \otimes Z \otimes Z,$$

$$g_3 = X \otimes Y \otimes Z \otimes I \tag{6}$$

satisfy these conditions, and generate the stabilizer group for the code given in Eqs. (1) and (2).

Adding one term of the form

$$H_p = -E_p(g_1 + g_2 + g_3) \tag{7}$$

to the encoded Hamiltonian for each encoded qubit yields an energy penalty of at least E_p for any state outside the code space.

Two-local encoded operations are optimal. None of the encoded operations can be made one-local, because they would then have the same form as the errors we are trying to detect and penalize. Such an operation would not commute with all of the generators.

Intuitively, one expects that providing an energy gap against a Pauli operator applied to any qubit protects against one-local noise. We illustrate this using a model of decoherence proposed in Ref. [10]. In this model, the quantum computer is a set of spin-1/2 particles weakly coupled to a large photon bath. The Hamiltonian for the combined system is

$$H = H_S + H_E + \lambda V,$$

where $H_S(t)$ is the adiabatic Hamiltonian that implements the algorithm by acting only on the spins, H_E is the Hamiltonian which acts only on the photon bath, and λV is a weak coupling between the spins and the photon bath. Specifically, V is assumed to take the form

$$V = \sum_i \int_0^\infty \mathrm{d}\omega [g(\omega) a_\omega \sigma_+^{(i)} + g^*(\omega) a_\omega^\dagger \sigma_-^{(i)}],$$

where $\sigma_\pm^{(i)}$ are raising and lowering operators for the ith spin, a_ω is the annihilation operator for the photon mode with frequency ω, and $g(\omega)$ is the spectral density.

From this premise Childs *et al.* obtain the following master equation:

$$\frac{d\rho}{dt} = - i[H_S,\rho] - \sum_{a,b} M_{ab}\mathcal{E}_{ab}(\rho), \tag{8}$$

where

$$M_{ab} = \sum_i [N_{ba}|g_{ba}|^2\langle a|\sigma_-^{(i)}|b\rangle\langle b|\sigma_+^{(i)}|a\rangle + (N_{ab}+1)|g_{ab}|^2\langle b|\sigma_-^{(i)}|a\rangle\langle a|\sigma_+^{(i)}|b\rangle]$$

is a scalar,

$$\mathcal{E}_{ab}(\rho) = |a\rangle\langle a|\rho + \rho|a\rangle\langle a| - 2|b\rangle\langle a|\rho|a\rangle\langle b|$$

is an operator, $|a\rangle$ is the instantaneous eigenstate of H_S with energy ω_a,

$$N_{ba} = \frac{1}{\exp[\beta(\omega_b - \omega_a)] - 1}$$

is the Bose-Einstein distribution at temperature $1/\beta$, and

$$g_{ba} = \begin{cases} \lambda g(\omega_b - \omega_a), & \omega_b > \omega_a, \\ 0, & \omega_b \leqslant \omega_a. \end{cases} \tag{9}$$

Suppose that we encode the original N-qubit Hamiltonian as a $4N$-qubit Hamiltonian as described above. As stated in Eq. (5), the total spin Hamiltonian H_S on $4N$ spins consists of the encoded version H_{SL} of the original Hamiltonian H_S plus the penalty terms H_{SP}.

Most adiabatic quantum computations use an initial Hamiltonian with an eigenvalue gap of order unity, independent of problem size. In such cases, a nearly pure initial state can be achieved at constant temperature. Therefore, we will make the approximation that the spins start in the pure ground state of the initial Hamiltonian, which we will denote $|0\rangle$. Then we can use Eq. (8) to examine $d\rho/dt$ at $t=0$. Since the initial state is $\rho=|0\rangle\langle 0|$, $\mathcal{E}_{ab}(\rho)$ is zero unless $|a\rangle=|0\rangle$. The master equation at $t=0$ is therefore

$$\left.\frac{d\rho}{dt}\right|_{t=0} = - i[H_S,\rho] - \sum_b M_{0b}\mathcal{E}_{0b}(\rho). \tag{10}$$

H_{SP} is given by a sum of terms of the form (7), and it commutes with H_{SL}. Thus, H_S and H_{SP} share a complete set of simultaneous eigenstates. The eigenstates of H_S can thus be separated into those which are in the code space C (i.e., the ground space of H_{SP}) and those which are in the orthogonal space $C^\perp$. The ground state $|0\rangle$ is in the code space. M_{0b} will be zero unless $|b\rangle \in C^\perp$, because $\sigma_\pm=(X\pm iY)/2$, and any Pauli operator applied to a single bit takes us from C to $C^\perp$. Equation (10) therefore becomes

$$\left.\frac{d\rho}{dt}\right|_{t=0} = - i[H_S,\rho] + \sum_{b\in C^\perp} M_{0b}\mathcal{E}_{0b}(\rho). \tag{11}$$

Since $|0\rangle$ is the ground state, $\omega_b \geqslant \omega_0$, thus Eq. (9) shows that the terms in M_{0b} proportional to $|g_{0b}|^2$ will vanish, leaving only

$$M_{0b} = \sum_i N_{b0}|g_{b0}|^2\langle 0|\sigma_-^{(i)}|b\rangle\langle b|\sigma_+^{(i)}|0\rangle.$$

Now let us examine N_{b0}.

$$\omega_b - \omega_0 = \langle b|(H_{SL}+H_{SP})|b\rangle - \langle 0|(H_{SL}+H_{SP})|0\rangle.$$

$|0\rangle$ is in the ground space of H_{SL}, thus

$$\langle b|H_{SL}|b\rangle - \langle 0|H_{SL}|0\rangle \geqslant 0,$$

and so

$$\omega_b - \omega_0 \geqslant \langle b|H_{SP}|b\rangle - \langle 0|H_{SP}|0\rangle.$$

Since $|b\rangle \in C^\perp$ and $|0\rangle \in C$,

$$\langle b|H_{SP}|b\rangle - \langle 0|H_{SP}|0\rangle = E_p,$$

thus $\omega_b - \omega_0 \geqslant E_p$.

A sufficiently large βE_p will make N_{ba} small enough that the term $\Sigma_{b\in C^\perp} M_{0b}\mathcal{E}(\rho)$ can be neglected from the master equation, leaving

$$\left.\frac{d\rho}{dt}\right|_{t=0} \approx - i[H_S,\rho],$$

which is just Schrödinger's equation with a Hamiltonian equal to H_S and no decoherence. Note that the preceding derivation did not depend on the fact that $\sigma_\pm^{(i)}$ are raising and lowering operators, but only on the fact that they act on a single qubit and can therefore be expressed as a linear combination of Pauli operators.

N_{b0} is small but nonzero. Thus, after a sufficiently long time, the matrix elements of ρ involving states other than $|0\rangle$ will become non-negligible and the preceding picture will break down. How long the computation can be run before this happens depends on the magnitude of $\Sigma_{b\in C^\perp} M_{ob}\mathcal{E}(\rho)$, which shrinks exponentially with E_p/T and grows only polynomially with the number of qubits N. Thus it should be sufficient for $1/T$ to grow logarithmically with the problem size. In contrast, one expects that if the Hamiltonian had only an inverse polynomial gap against one-local noise, the temperature would need to shrink polynomially rather than logarithmically.

Now that we know how to obtain a constant gap against one-local noise, we may ask whether the same is possible for two-local noise. To accomplish this we need to find a stabilizer group such that any pair of Pauli operators on two bits anticommutes with at least one of the generators. This is exactly the property satisfied by the standard [17] five-qubit stabilizer code, whose stabilizer group is generated by

$$
\begin{aligned}
g_1 &= X \otimes Z \otimes Z \otimes X \otimes I,\\
g_2 &= I \otimes X \otimes Z \otimes Z \otimes X,\\
g_3 &= X \otimes I \otimes X \otimes Z \otimes Z,\\
g_4 &= Z \otimes X \otimes I \otimes X \otimes Z.
\end{aligned}
\qquad (12)
$$

The codewords for this code are

$$
\begin{aligned}
|0_L\rangle = \frac{1}{4}[&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle\\
&- |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle\\
&- |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle\\
&+ |00101\rangle],
\end{aligned}
$$

$$
\begin{aligned}
|1_L\rangle = \frac{1}{4}[&|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle\\
&- |00100\rangle - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle\\
&- |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle\\
&+ |11010\rangle].
\end{aligned}
$$

The encoded Pauli operations for this code are conventionally expressed as

$$
\begin{aligned}
X_L &= X \otimes X \otimes X \otimes X \otimes X,\\
Y_L &= Y \otimes Y \otimes Y \otimes Y \otimes Y,\\
Z_L &= Z \otimes Z \otimes Z \otimes Z \otimes Z.
\end{aligned}
$$

However, multiplying these encoded operations by members of the stabilizer group does not affect their action on the code space. Thus we obtain the following equivalent set of encoded operations:

$$
\begin{aligned}
X_L &= -X \otimes I \otimes Y \otimes Y \otimes I,\\
Y_L &= -Z \otimes Z \otimes I \otimes Y \otimes I,\\
Z_L &= -Y \otimes Z \otimes Y \otimes I \otimes I.
\end{aligned}
\qquad (13)
$$

These operators are all three-local. This is the best that can be hoped for, because the code protects against two-local operations and therefore any two-local operation must anticommute with at least one of the generators.

In addition to increasing the locality of the encoded operations, one can seek to decrease the number of qubits used to construct the codewords. The quantum singleton bound [17] shows that the five-qubit code is already optimal and cannot be improved in this respect.

The distance d of a quantum code is the minimum number of qubits of a codeword which need to be modified before obtaining a nonzero inner product with a different codeword. For example, applying X_L, which is three-local, to $|0_L\rangle$ of the five-qubit code converts it into $|1_L\rangle$, but applying any two-local operator to any of the codewords yields something outside the code space. Thus the distance of the five-qubit code is 3. Similarly the distance of our four-qubit code is 2. To detect t errors a code needs a distance of $t+1$, and to correct t errors, it needs a distance of $2t+1$.

The quantum singleton bound states that the distance of any quantum code which uses n qubits to encode k qubits will satisfy

$$
n - k \geqslant 2(d-1). \qquad (14)
$$

To detect two errors, a code must have distance 3. A code which encodes a single qubit with distance 3 must use at least five qubits, by Eq. (14). Thus the five-qubit code is optimal. To detect 1 error, a code must have distance 2. A code which encodes a single qubit with distance 2 must have at least three qubits, by Eq. (14). Thus it appears possible that our four-qubit code is not optimal. However, no three-qubit stabilizer code can detect all single-qubit errors, which we show as follows.

The stabilizer group for a three-qubit code would have two independent generators, each being a tensor product of three Pauli operators:

$$
\begin{aligned}
g_1 &= \sigma_{11} \otimes \sigma_{12} \otimes \sigma_{13},\\
g_2 &= \sigma_{21} \otimes \sigma_{22} \otimes \sigma_{23}.
\end{aligned}
$$

These must satisfy the following two conditions: (1) they commute and (2) an X, Y, or Z on any of the three qubits anticommutes with at least one of the generators. This is impossible, because condition (2) requires $\sigma_{1i} \neq \sigma_{2i} \neq I$ for each $i=1,2,3$. In this case g_1 and g_2 anticommute.

The stabilizer formalism describes most but not all currently known quantum error-correcting codes. We do not know whether a three-qubit code which detects all single-qubit errors while still maintaining two-local encoded operations can be found by going outside the stabilizer formalism. It may also be interesting to investigate whether there exist computationally universal three-local or two-local adiabatic Hamiltonians with a constant energy gap against local noise.

We thank Ed Platt, Jay Gill, Shay Mozes, Daniel Lidar, and Mark Rudner for useful discussions. We especially thank David DiVincenzo for encouraging us to work on this topic, and Andrew Childs for helping to clarify an important point. E.F. gratefully acknowledges support from the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) Contract No. W911NF-04-1-0216. S.J. gratefully acknowledges support from ARO/ARDA's QuaCGR program. P.S. gratefully acknowledges support from the NSF under Grant No. CCF-0431787.

[1] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, quant-ph/0001106 (unpublished).

[2] A. Messiah, *Quantum Mechanics* (Dover, New York, 1958).

[3] S. Jansen, M. B. Ruskai, and R. Seiler, quant-ph/0603175 (unpublished).

[4] G. Schaller, S. Mostame, and R. Schützhold, Phys. Rev. A **73**, 062307 (2006).

[5] A. Joye, math-ph/0608059 (unpublished).

[6] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, in *Proceedings of the 45th Annual Symposium on the Foundations of Computer Science (FOCS'04)* (IEEE Computer Society Press, Los Alamitos, CA, 2004), p. 42.

[7] R. Feynman, Found. Phys. **16**, 507 (1986).

[8] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, Vol. 47 of Graduate Studies in Mathematics (American Mathematical Society, Providence, RI, 2002).

[9] J. Kempe, A. Kitaev, and O. Regev, SIAM J. Comput. **35**, 1070 (2006).

[10] A. Childs, E. Farhi, and J. Preskill, Phys. Rev. A **65**, 012322 (2001).

[11] M. S. Sarandy and D. A. Lidar, Phys. Rev. Lett. **95**, 250503 (2005).

[12] J. Åberg, D. Kult, and E. Sjöqvist, Phys. Rev. A **72**, 042317 (2005).

[13] J. Roland and N. J. Cerf, Phys. Rev. A **71**, 032330 (2005).

[14] W. M. Kaminsky and S. Lloyd, in *Quantum Computing and Quantum Bits in Mesoscopic Systems* (Kluwer Academic, Dordrecht, 2003).

[15] D. Bacon, K. R. Brown, and K. B. Whaley, Phys. Rev. Lett. **87**, 247902 (2001).

[16] D. Gottesman, Ph.D. thesis, Caltech, Pasadena, 1997.

[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).