Almost Any Quantum Logic Gate is Universal

Seth Lloyd

Information Sciences, Mechanical Engineering, Massachusetts Institute of Technology 3-339, Cambridge, Massachusetts 02139
(Received 14 November 1994)

It is shown that if one can apply some Hamiltonian repeatedly to a few variables at a time one can in general effect any desired unitary time evolution on an arbitrarily large number of variables. As a result, almost any quantum logic gate with two or more inputs is computationally universal in that copies of the gate can be "wired together" to effect any desired logic circuit, and to perform any desired unitary transformation on a set of quantum variables.

PACS numbers: 89.70.+c

Suppose that an experimenter can act on two or more quantum variables by "turning on" a given Hamiltonian for a controlled period of time. What can she do with this capability? In this paper, it is shown that by acting with the Hamiltonian first on some variables and then on others the experimenter can in general effect any desired unitary transformation on an arbitrarily large number of variables. This result implies in turn that almost any quantum logic gate is universal: Quantum devices that perform some unitary operation on their input variables can be "wired together" to effect any desired unitary transformation on an arbitrary set of inputs. In particular, almost any quantum logic gate can be used to construct a quantum-mechanical computer.

Quantum information processing.—The discrete nature of quantum-mechanical variables makes them natural quantities for registering information. A bit of information can be registered by a spin-1/2 particle, with spin up corresponding to 1 and spin down to 0, or by the polarization of a photon, with clockwise polarization corresponding to 1 and counterclockwise to 0, or by an electron in a hydrogen atom, with the first excited state corresponding to 1 and the ground state to 0. One can not only register information on such a quantum bit, but also process it: For example, one can "flip" the bit registered by an electron's spin by putting the electron in a magnetic field and rotating the spin by π using magnetic resonance techniques.

A quantum computer is a device that stores and processes information on quantum variables. Quantum computers differ from classical computers in that they can maintain quantum-mechanical coherence: an electron can be in a coherent superposition of spin up and spin down, and a quantum bit can be in a coherent superposition of 0 and 1, but a capacitor in an integrated circuit cannot be in a coherent superposition of charged and uncharged. The idea of quantum computation was first introduced by Benioff [1], and further developed by Feynman [2]; computers that exploit quantum coherence were introduced by Deutsch [3], who also introduced the notion of a quantum logic gate [4]; error generation and correction were discussed by Peres [5] and Zurek [6]; and quantum cellular automata computers were discussed by Margolus [7]. These contributions considered quantum computers in the abstract. During the same period, Landauer [8] produced an extensive critique of the difficulties involved in actually realizing quantum computers. In recent years, Deutsch and Jozsa [9] showed that there exist problems that can be solved more rapidly on quantum than on classical computers, and Shor [10] showed that large numbers could be factored in polynomial time on a quantum computer. In parallel, progress has been made towards realistic designs for quantum computers [11], and difficulties in maintaining quantum coherence have been explored [12]. The properties of quantum computers considered in the abstract continue to be developed [13–19].

Whether full-blown quantum computation can be realized or not, quantum information-processing techniques could prove useful to physicists who wish to realize and test the properties of complicated quantum states. Even if one cannot maintain hundreds or thousands of quantum bits in a coherent superposition, the ability to store, manipulate, and read two or three, or four or five bits would allow one to explore a variety of quantum phenomena [20], such as Einstein-Podolsky-Rosen states [21], Greenberger-Horne-Zeilinger states [22], and quantum teleportation [23]. In this paper, it is shown that almost any interaction between quantum-mechanical variables can in principle be exploited to effect any desired unitary evolution for the variables. In particular, almost any interaction between quantum-mechanical variables can be used to create a universal quantum logic gate. A practical example of such a universal interaction is the nonlinear interaction between light and matter in small-cavity quantum electrodynamics [24–27].

Quantum logic gates.—A quantum logic gate is an input-output device whose inputs and outputs are discrete quantum variables such as spins. The action of such a gate on its inputs is described by a unitary operator U that takes the input variables from a state $|\psi\rangle$ to a state $|\psi'\rangle = U|\psi\rangle$ (the question of dissipative, nonunitary quantum gates will not be addressed here). In analogy with classical logic gates, quantum gates can be wired together to form a quantum circuit, where a "wire" is a device that takes an output variable from one gate and

 0031-9007/95/75(2)/346(4)$06.00

moves it to the input of another gate. (A quantum wire is itself a nontrivial device that may be difficult to realize [11].) A quantum gate is said to be universal if copies of it can be wired together to make circuits to evaluate any desired classical logic function (that is, a quantum universal gate is also a classical universal gate), and to enact any desired unitary transformation on a set of quantum variables.

The concept of the quantum logic gate was first introduced by Deutsch [4], who showed that a "controlled-controlled rotation" gate was universal: This gate has three two-state or Q-bit inputs (e.g., spin-$\frac{1}{2}$ particles) and three Q-bit outputs; the first two inputs go through unchanged, while the third bit is rotated by an angle that is irrationally related to π if and only if the first two inputs are 1. Repeated application of this gate allows one to come as close as one wants to a controlled-controlled NOT gate that flips the third input if and only if the first two inputs are 1. Controlled-controlled NOT is a classical universal gate, capable of performing NOT, AND, and COPY operations (copies of any gate that can perform these operations can be wired together to realize any desired logical function). Deutsch also showed that copies of this gate can be wired together to give a circuit that comes as close as desired to evaluating any desired unitary transformation on a set of Q-bit variables. More recently, DiVincenzo [14] showed that a set of two Q-bit logic gates is adequate for universal computation, and Barenco [18] and Sleator and Weinfurter [19] independently showed that a "controlled rotation" gate is in and of itself a quantum universal gate: This gate leaves its first input unchanged, and rotates the second input by an angle and multiplies it by a phase if and only if the first input is 1 (Fig. 1).

In the same paper in which Deutsch proposed quantum logic gates as a way of performing quantum computation, he conjectured that most quantum logic gates with three or more binary inputs are universal. Here, a stronger result is proved.

Theorem. Almost any quantum logic gate with two or more inputs (not necessarily binary) is universal.

The proof of this theorem follows from a more general fact; a more detailed proof will be given elsewhere. Let a set of quantum variables evolve according to a Hamiltonian A on an n-dimensional Hilbert space. Suppose that an experimental physicist can "turn on" and "turn off" a different Hamiltonian B over a time t that she is able to control. All the physicist can do is let the variables evolve according to A for a time t_1, then apply B for a time t_2, then let them evolve according to A for time t_3, then apply B for a time t_4, etc., a process that corresponds to unitary operators of the form

$$U = \cdots e^{iBt_4} e^{iAt_3} e^{iBt_2} e^{iAt_1} . \tag{1}$$

Which U can be created by such an experiment?

Answer: any $U = e^{iLt}$, where L is a member of the algebra $\mathcal{L}$ generated from A and B through commutation.

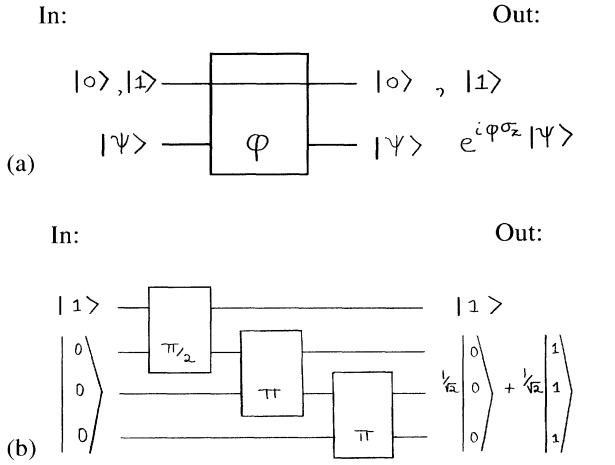

FIG. 1. (a) A quantum-mechanical controlled rotation gate. If the first input is 1, the second input is rotated by ϕ about the z axis and multiplied by a phase. When ϕ/π is irrational, this gate is a quantum universal logic gate. (b) Construction of a Greenberger-Horne-Zeilinger state using controlled rotation gates. Controlled rotation gates can be wired together to create any desired quantum state, and to perform any desired unitary transformation. Controlled rotation gates suffice to construct a quantum computer.

This algebra is the set of Hermitian matrices, regarded as vectors, spanned by $A, B, i[A,B]$, $[A,[A,B]]$, ... If the repertoire of interactions available to the experimentalist includes more than one Hamiltonian, $B, C, \ldots$, then any $U = e^{iLt}$ can be created, where L belongs to the algebra generated by $\{A, B, C, \ldots,\}$.

This result can be demonstrated in a number of ways. First, one can build up transformations infinitesimally, using the fact that

$$\lim_{n\to\infty}\left(e^{-iB\sqrt{t/n}} e^{-iA\sqrt{t/n}} e^{iB\sqrt{t/n}} e^{iA\sqrt{t/n}}\right)^n = e^{[A,B]t} . \tag{2}$$

Any $U = e^{iLt}$ can be built up in this fashion, but the number of transformations, and the time required to enact them, can be arbitrarily large. The second way of constructing transformations is noninfinitesimal: As each additional transformation is added to Eq. (1), the dimension of the submanifold of transformations that can be reached by varying $t_1, t_2 \ldots$, goes up by 1, until it reaches the dimension of $\mathcal{L}$, at which point additional transformations no longer increase the dimension of the space of reachable transformations. The submanifold of transformations reachable in $\dim\mathcal{L}$ steps is a nonzero measure subspace of the space of transformations of the form $U = e^{iLt}$. If $\mathcal{L}$ has finite dimension, this space is compact: As a result, at most, a number of transformations proportional to the number of generators of $\mathcal{L}$ is required to reach any desired transformation in the space.

Suppose that the experimenter is presented with two $n \times n$ Hamiltonians A and B: What does $\mathcal{L}$ look like? The only way that $\mathcal{L}$ can fail to be the entire space of $n \times n$ Hermitian matrices is for both e^{iAt} and e^{iBt} to lie in an n-dimensional unitary representation of some Lie group other than $\mathrm{U}(n)$. Which Lie groups have such representations depends on n, but for any n there are a finite number of inequivalent representations for such groups, each one of whose algebras have fewer than n^2 generators [28–30]. Assume that A is not proportional to the identity matrix, and work in a basis in which A is diagonal; for A and B to fall in a representation of a Lie group other than $\mathrm{U}(n)$, B must lie on some submanifold of Hermitian matrices of dimension equal to the number of generators for the group. This submanifold has dimension less than n^2 [for $\mathrm{SU}(n)$, for example, the submanifold has dimension $n^2 - 1$], and is of measure zero in the n^2-dimensional manifold of all $n \times n$ Hermitian matrices.

That is, for all $n \times n$ matrices A and B, except a set of measure zero, the algebra generated by A and B is the entire space of $n \times n$ Hermitian matrices. (The analogous statement for the rotation group is that any rotation can be generated by repeated application of rotations about two randomly selected axes.) The number of terms in the product in Eq. (1) needed to generate an arbitrary U is on the order of the number of generators for the algebra, in this case n^2. By turning on and turning off a single Hamiltonian, the experimenter can in general effect any desired unitary transformation.

This proof is an "existence" proof, but the "construction" problem is only that of constructing a controlled-rotation gate, since Refs. [4,14,18,19] show how such a gate can be used to construct a quantum computer. Once such a gate has been realized, the "wiring diagram" by which copies of the gate are combined to realize quantum computation is independent of the form of the interactions used to realize the gate.

Now suppose that the experimenter can only apply each different Hamiltonian A, B for a predetermined time interval t_A, t_B. That is, the experimenter can generate unitary operators of the form

$$U = \cdots U_B^{m_4} U_A^{m_3} U_B^{m_2} U_A^{m_1}, \tag{3}$$

where $U_A = e^{iAt_A}$, $U_B = e^{iBt_B}$, for fixed t_A, t_B, and m_i are integers. Which U can be realized now? In fact, by applying sequences of Hamiltonians for predetermined time intervals, one can get arbitrarily close to any of the U that one could create before using continuous times. The reason is simple: As long as the eigenvalues of U_A have phases that are irrationally related to π, then for all t there exist some m such that $||U_A^m - e^{iAt}|| < \epsilon$, where the norm is the trace norm. Here m is of the order of ϵ^{-n}. Similarly for U_B. That is, each of the terms in the product in Eq. (1) can be approximated to accuracy ϵ by iterating one of the operations a number of times on the order of ϵ^{-n}. Since the iterations can be chosen so that the errors tend to cancel in the product of Eq. (3), the total number of iterations in Eq. (3) required to enact an arbitrary U to accuracy ϵ is on the order of $n^2\epsilon^{-n}$.

Now, let U_A correspond to the action of some arbitrary gate on ℓ inputs, and let W be the unitary operator corresponding to switching two of the gate's inputs. The set of such $U_A, U_B = U_A W$ that do not obey the criteria of the previous paragraph is of measure zero, and U_A and W can be iterated to enact a universal gate such as a controlled-rotation gate on two of the inputs. But a gate that can enact a universal gate is itself universal. This proves the theorem. By doing only two things, but by doing them cleverly, the experimenter can effect any desired unitary transformation on the input variables.

This universality can be proved directly (though nonconstructively). Almost any ℓ-input quantum logic gate can be "wired together" with copies of itself to effect any desired unitary transformation on N input variables, where N can be arbitrarily large. Let U_A give the action of the gate on ℓ of the N inputs, and let W_π give the action of the permutation π (a "rewiring") on the input variables. In general, the algebra generated by $\{\log U_A, \log U_A W_\pi\}$ over all permutations π is the entire set of Hermitian matrices on the Hilbert space $\mathcal{H}_N$ of the input variables, and so by the same proof as above, U_A and W_π may be iterated to get arbitrarily close to any desired unitary operation on $\mathcal{H}_N$. That is, the experimenter can perform any desired unitary operation not only on ℓ inputs, but on an arbitrary number of inputs. The total number of iterations required to get within ϵ of the desired unitary transformation is on the order of $[\mathrm{Dim}(\mathcal{H}_\mathcal{N})]^2\epsilon^{-n}$, where n is the dimension of the input space of the gate. QED.

Example [31].—Suppose that the experimenter can arrange an interaction between two spins or photon polarizations that takes the state $|00\rangle \to |00\rangle, |01\rangle \to e^{i\chi t}|01\rangle, |10\rangle \to e^{i\xi t}|10\rangle$, and $|11\rangle \to e^{i\omega t}|11\rangle$ over time t, for some spin or polarization basis $|0\rangle, |1\rangle$ for each particle. If, in addition, the experimenter can perform phase shifts and rotations on each individual spin or photon polarization, then the theorem implies that this interaction suffices to effect universal quantum computation *if and only if* $\chi + \xi \neq \omega \pmod{2\pi}$; that is, *any* nonlinear phase shift suffices to allow computation. In fact, it can be shown that a single application of this interaction, together with phase shifts and rotations, allows the construction of a universal controlled-rotation gate. Small cavity quantum electrodynamics afford strongly nonlinear light-matter interactions of this form, and might be used to effect quantum logic and to create novel multiparticle quantum states [24–27].

Conclusion.—An experimenter who performs a single operation accurately and repeatedly on a few variables at a time can in principle accomplish any desired unitary transformation on an arbitrary number of variables. The demonstration is straightforward: If one can repeatedly apply a Hamiltonian to a system, then as long as the

algebra generated by the applied Hamiltonian and the system's unperturbed Hamiltonian via commutation only closes on the entire space of Hamiltonians for the system, one can effect any desired unitary transformation on the system. As a result, almost any quantum logic gate is universal. A variety of experimentally realizable systems are reasonable candidates for universal quantum logic gates: Essentially, any nontrivial interaction between quantum variables will do. If realized, quantum logic gates could be used to create previously unobserved multiparticle states, and to effect quantum computation.

The author would like to thank Jeff Kimble, Jon Preskill, and David DiVincenzo for helpful discussions, and Michael Arbib and the Center for Neural, Informational, and Behavioral Sciences at USC for their hospitality during the composition of this paper.

Note added.—After the submission of this paper, a similar result, independently derived, was submitted by D. Deutsch, A. Barenco, and A. Ekert to the Proceedings of the Royal Society, under the title *Universality in Quantum Computation.*

[1] P. Benioff, J. Stat. Phys. **22**, 563 (1980); Phys. Rev. Lett. **48**, 1581 (1982); J. Stat. Phys. **29**, 515 (1982); Ann. N.Y. Acad. Sci. **480**, 475 (1986).

[2] R. P. Feynman, Opt. News **11**, 11 (1985); Found. Phys. **16**, 507 (1986); Int. J. Theor. Phys. **21**, 467 (1982).

[3] D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).

[4] D. Deutsch, Proc. R. Soc. London A **425**, 73 (1989).

[5] A. Peres, Phys. Rev. A **32**, 3266 (1985).

[6] W. H. Zurek, Phys. Rev. Lett. **53**, 391 (1984).

[7] N. Margolus, Ann. N.Y. Acad. Sci. **480**, 487 (1986); in *Complexity, Entropy, and the Physics of Information,* edited by W. H. Zurek, Santa Fe Institute Series, Vol. 8 (Addison Wesley, Redwood City, CA, 1991), pp. 273–288.

[8] R. Landauer, Int. J. Theor. Phys. **21**, 283 (1982); Found. Phys. **16**, 551 (1986); Nature (London) **335**, 779 (1988); *Nanostructure Physics and Fabrication,* edited by M. A. Reed and W. P. Kirk (Academic, Boston, 1989), pp. 17–29; Phys. Today **42**, No. 10, 119 (1989); in *Proceedings of the 3rd International Symposium on Foundations of Quantum Mechanics, Tokyo, 1989,* edited by S. Kobayashi *et al.* (Physical Society of Japan, Tokyo, 1990), p. 407; Physica (Amsterdam) **168A**, 75 (1990); Phys. Today **44**, No. 5, 23 (1991); in *Proceedings of the Workshop on Physics of Computation II,* edited by D. Matzke (IEEE, New York, 1992), p. 1; Philos. Trans. R. Soc. London A (to be published); in *Proceedings of the Drexel Symposium on Quantum Nonintegrability—Quantum Classical Correspondence,* edited by D. H. Feng and B. L. Hu (Gordon and Breach Science Publishers, Langhorne, PA, 1993).

[9] D. Deutsch and R. Jozsa, Proc. R. Soc. London A **439**, 553 (1992).

[10] P. Shor (to be published).

[11] S. Lloyd, Science **261**, 1569 (1993); **263**, 695 (1994).

[12] W. Unruh (to be published).

[13] A. Ekert (to be published).

[14] D. DiVincenzo (to be published).

[15] S. Lloyd, Phys. Rev. Lett. **71**, 943 (1993); (to be published).

[16] E. Bernstein and U. Vazirani, in Proceedings of the 25th Annual ACM Symposium on the Theory of Computing, 1993 (to be published), pp. 11–20.

[17] A. Berthiaume and G. Brassard, in *Proceedings of the Workshop on Physics and Computation—Physcomp '92,* edited by D. Matzke (IEEE, New York, 1992), pp. 195–199.

[18] A. Barenco, Oxford University report, 1994 (to be published).

[19] T. Sleator and H. Weinfurter (to be published).

[20] J. P. Paz and G. Mahler, Phys. Rev. Lett. **71**, 3235 (1993).

[21] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[22] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Phys. Today **46**, No. 9, 22 (1993).

[23] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[24] H. Mabuchi and H. J. Kimble, Opt. Lett. **19**, 749 (1993).

[25] A. B. Matsko, S. P. Vyatchanin, H. Mabuchi, and H. J. Kimble, Phys. Lett. A **192**, 175 (1994).

[26] H. J. Kimble, O. Carnal, N. Georgiades, H. Mabuchi, E. S. Polzik, R. J. Thompson, and Q. A. Turchette, in Proceedings of the International Conference on Atomic Physics (to be published).

[27] M. Brune, P. Nussenzveig, F. Schmidt-Kaler, F. Bernardot, A. Maali, J. M. Raimond, and S. Haroche, Phys. Rev. Lett. **72**, 3339 (1994).

[28] N. Jacobson, *Lie Algebras* (Wiley Interscience, New York, 1962).

[29] G. Hochschild, *The Structure of Lie Groups* (Holden-Day, San Francisco, 1965).

[30] D. B. Lichtenberg, *Unitary Symmetry and Elementary Particles* (Academic, New York, 1978), 2nd ed.

[31] This example was worked out in collaboration with H. J. Kimble and the Caltech Quantum Computation group.