Realizable Universal Quantum Logic Gates

Tycho Sleator[1] and Harald Weinfurter[2]
[1]*Department of Physics, New York University, New York, New York 10003*
[2] *Institute for Experimental Physics, University of Innsbruck, A-6020 Innsbruck, Austria*
(Received 31 October 1994)

We identify a 2-bit quantum gate that is sufficient to build any quantum logic network. The existence of such a 2-bit universal gate considerably simplifies the search for physical realizations of quantum computational networks. We propose an explicit construction of this gate, which is based on cavity QED techniques and may be realizable with current technology.

PACS numbers: 89.70.+c, 03.65.Bz, 32.80.–t, 42.50.Dv

The superposition principle and unitary time evolution, key features of quantum mechanics, make the simulation of quantum systems on standard classical computers difficult and in many cases (exponentially) computationally expensive [1]. This fact leads to the question of whether complex problems can be solved more efficiently using a computer based on fundamental quantum mechanical principles than with a classical computer. The formal definition of a quantum Turing machine [2] and the introduction of quantum complexity theory [3] showed the possible realization of quantum computation, and gave first hints of its increased power. Recently, Shor showed that the specific problem of factoring, which for known algorithms takes exponentially increasing time on a classical computer, can be solved in polynomial time using a quantum computer [4].

Although presently existing computers use quantum mechanical effects for their operation, they are not quantum computers in the sense used in this paper. In standard electronic computers, the computational process strictly follows binary algebra and corresponds to a probabilistic Turing machine. The state of a classical computer can be determined at any time during the calculation. This is *not* possible for a quantum computer. Since quantum coherence must be maintained through the whole process, any measurement of an intermediate state would irreversibly influence the calculation.

A quantum computational network can be decomposed into so called quantum logic gates [5], in analogy to the situation for classical computers. In an extension of earlier work on reversible computation [6,7], the *universal* quantum logic gate was defined [5] to be a gate that could be used to simulate *any* quantum logic gate. For classical reversible computation, it has been shown that the simplest universal gate has three input bits (and three output bits). Examples of such reversible universal logic gates are the Fredkin gate [8] or the Toffoli gate [7]. Optical models for these gates have been recently presented [9].

A number of interactions have been proposed for the construction of quantum computers [10], but so far no explicit physical system has been shown to serve as a universal quantum gate. In this Letter we demonstrate that there exists a 2-bit quantum gate that is sufficient to build any quantum logic network [11], a result that considerably simplifies the search for physical realizations. In addition, we identify a realizable physical system, based on the coupling of atoms to the photonic field of microcavities [12,13], that could be used to construct such a universal gate.

In classical computation, the bit a can have the values 0 and 1, whereas the quantum bit is represented by a two state system whose state can be expressed as $|\psi_a\rangle = \lambda_1|1\rangle + \lambda_0|0\rangle$. Similarly, the state of a quantum network consisting of n bits is given by $|\Psi_n\rangle = \sum_{\mathbf{l}} \lambda_{\mathbf{l}}|\mathbf{l}\rangle$ in the 2^n-dimensional computational basis spanned by $|\mathbf{l}\rangle \equiv |l_1, l_2, ..., l_n\rangle, l_i = \{0, 1\}$. Following Deutsch [5] we define an n-bit quantum logic gate by the 2^n-dimensional evolution matrix $\mathbf{S}_q$ acting on $|\Psi_n\rangle_{\text{in}}$,

$$|\Psi_n\rangle_{\text{out}} = \mathbf{S}_q|\Psi_n\rangle_{\text{in}} . \tag{1}$$

Two essential features of any quantum computational process should be noted. First, $|\Psi_n\rangle$ can be a coherent superposition of the basis states, whereas in classical computation operations are defined only for the basis states. Second, the unitarity of the quantum mechanical evolution implies reversibility of the computation.

By generalizing the Toffoli gate, Deutsch found a quantum gate (referred to here as the "Deutsch gate") that is universal for all quantum computations. A representation of the Deutsch gate, expressed in terms of the 3-bit computational basis $\{|a, b, c\rangle\} = \{|0, 0, 0\rangle, |0, 0, 1\rangle, ..., |1, 1, 0\rangle, |1, 1, 1\rangle\}$ is given by

$$\mathbf{S}_Q^{(\tau)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & i\cos(\pi\tau/2) & \sin(\pi\tau/2) \\ 0 & 0 & 0 & 0 & 0 & 0 & \sin(\pi\tau/2) & i\cos(\pi\tau/2) \end{pmatrix} . \tag{2}$$

 © 1995 The American Physical Society

This gate changes the state of the quantum bit c ("target bit") only for input basis states in which both "control" bits a and b are equal to 1 ($ab = 1$).

The universal 2-bit quantum gate is a generalization of the reversible "measurement gate" [5]. The two outputs of the measurement gate are defined in terms of its inputs by $a_{\text{out}} = a_{\text{in}}$, and $b_{\text{out}} = a_{\text{in}} \oplus b_{\text{in}}$, where $\oplus$ refers to the logical exclusive-OR (XOR) operation. A simple generalization of the measurement gate to the quantum domain yields the operator (expressed in terms of the 2-bit computational basis $\{|a, b\rangle\} : a, b \in \{0, 1\}$)

$$\mathbf{S}_M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{3}$$

which we refer to as the "quantum measurement gate." A further generalization of the measurement gate yields a 2-bit universal quantum gate, defined by

$$\mathbf{S}_U^{(\tau)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i(\pi/4)} \cos(\pi\tau/2) & e^{-i(\pi/4)} \sin(\pi\tau/2) \\ 0 & 0 & e^{-i(\pi/4)} \sin(\pi\tau/2) & e^{i(\pi/4)} \cos(\pi\tau/2) \end{pmatrix}. \tag{4}$$

We note that, for $\tau = 1, (\mathbf{S}_U^{(\tau)})^2 = \mathbf{S}_M$, so $\mathbf{S}_U^{(1)}$ can be considered a "square root of XOR." To demonstrate the universality of (4), it is sufficient to build a network from $\mathbf{S}_U^{(\tau)}$ that performs the computation of the 3-bit Deutsch gate $\mathbf{S}_Q$. The evolution matrix of a gate operating on only two of three bits is given by the tensor product ($\otimes$) of the 2-dimensional unity matrix with the respective quantum transformation. For example the action of the above defined 2-bit gate on the bits b and c only is given by $\mathbf{S}_{U[a;b,c]}^{(\tau)} \equiv \mathbb{1}_a \otimes \mathbf{S}_{U[b,c]}^{(\tau)}$. We then find that

$$\mathbf{S}_Q^{(\tau)} = \mathbf{S}_{M[c;a,b]} (\mathbf{S}_{U[a;b,c]}^{(\tau/2)})^{-1} \mathbf{S}_{M[c;a,b]} \mathbf{S}_{U[b;a,c]}^{(\tau/2)} \mathbf{S}_{U[a;b,c]}^{(\tau/2)}. \tag{5}$$

For τ irrational, both $(\mathbf{S}_U^{(\tau)})^{-1}$ and $\mathbf{S}_M$ can be obtained by repeated application of $\mathbf{S}_U^{(\tau)}$ [14]. $\mathbf{S}_U^{(\tau)}$ is therefore universal. Figure 1 shows the quantum network expressed by Eq. (5). Insight can be gained into the action of this network by noting first that for classical bits a and b the *logical* AND of a and b can be expressed in terms of *arithmetic* operations on the bit values as $ab = [a + b - (a \oplus b)]/2$. Second, from Fig. 1, we see that bit c undergoes

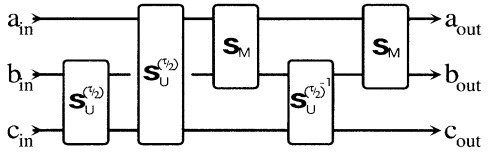

FIG. 1. Decomposition of the universal 3-bit quantum logic gate into a network of 2-bit quantum gates.

three conditional rotations, the first two through an angle $\tau/2$, conditional on a and b, respectively, and the third through an angle $-\tau/2$, conditional on $a \oplus b$. Because of the quantum mechanical superposition principle, these rotations add *arithmetically*. The net result is a rotation about an angle τ, conditional on ab, which is the action of the Deutsch gate.

The identification of a 2-bit universal quantum gate considerably simplifies the search for implementations of quantum computational networks. The equivalence of the quantum measurement gate (3) to an ideal quantum nondemolition (QND) measurement points to already existing QND schemes as candidates. QND measurements are currently investigated for a number of different systems. In most cases, however, either the coupling is too small for single particle resolution [15], or there is a lack of experimental expertise for otherwise very promising systems [10]. Cavity quantum electrodynamics [13,16] is to our knowledge the only candidate capable of realizing quantum logic gates in the near future [17]. Recent results [13] have shown that QND measurements can achieve single particle (photon) resolution, a condition necessary for construction of a universal quantum gate.

We now outline specific implementations based on cavity QED of the 2-bit universal quantum gate. Our proposed implementations consist of microwave cavities, Ramsey zones, and a set of two-level atoms. There is never more than one photon in a cavity, so the state of the cavity field can be described in terms of the basis states $|0\rangle$ and $|1\rangle$, corresponding to the vacuum and one photon states, respectively. The atoms are the carriers of the bits (between gates), and are described by the basis states $|g\rangle$ and $|e\rangle$, which correspond in the computational basis to $|0\rangle$ and $|1\rangle$, respectively.

Two different kinds of atom-cavity interactions are used in our schemes. In the "on-resonant" atom-cavity interaction, the cavity is tuned *exactly* to the atomic transition, and the interaction Hamiltonian is given by

$$H_{\text{on}} = i\hbar\Omega_1(\sigma_- a^\dagger - \sigma_+ a), \tag{6}$$

where $\sigma_+ = |e\rangle\langle g|$ and $\sigma_- = |g\rangle\langle e|$, and Ω_1 is the one photon Rabi frequency. In the "off-resonant" interaction, the cavity frequency is sufficiently detuned from the $|g\rangle$ to $|e\rangle$ transition frequency that there are no transitions between these two levels during the interaction. Here, the Hamiltonian can be modeled by [18]

$$H_{\text{off}} = \hbar(\Omega_2/2)a^\dagger a(|e\rangle\langle e| - |g\rangle\langle g|), \tag{7}$$

where Ω_2 is the change in atomic level spacing per photon in the cavity. In our schemes, the on-resonant interaction is used to transfer quantum states between atom and cavity, while the off-resonant interaction is used to produce conditional phase shifts in the atomic states, controlled by the photon number of the cavity field. These two types of interactions can be produced from a single

atomic species by appropriate Stark shifting of the atomic levels.

The Ramsey zone consists of a classical rf field, which can produce an arbitrary rotation of the atomic two-level systems when appropriate values of the frequency and amplitude of the field are used. In the following discussion, we assume the Ramsey zone produces a $\pi/2$ rotation about the y axis in spin space and is described by the operator where $\sigma_y = i(|e\rangle\langle g| - |g\rangle\langle e|)$.

When an atom passes sequentially through a Ramsey zone R, a cavity (with off-resonant interaction of duration T), and another Ramsey zone R^{-1}, the resulting transformation is

$$\mathbf{U}(\phi) = R^{-1}\exp(i\phi a^\dagger a|e\rangle\langle e|)R = (1 - a^\dagger a)\mathbb{1} + a^\dagger a R_{\hat{x}}(\phi), \quad (8)$$

where $\phi = \Omega_2 T$, and $R_{\hat{x}}(\phi) \equiv [\mathbb{1}\cos(\phi/2) - i\sigma_x \sin(\phi/2)]$ represents a rotation of the atomic state by an angle ϕ about the x axis. The transformation (8) results in a rotation of the atomic state when the state of the cavity field is $|1\rangle$, but leaves the atomic state alone when the cavity state is $|0\rangle$. When both input bits (a and b) are carried by atoms, the gate $\mathbf{U}(\phi)$ can be realized in the following way. Before the off-resonant interaction (8) is carried out, the state of the control bit (a) is transferred to the cavity (originally in the vacuum state $|0\rangle$) by the on-resonant interaction [Eq. (6)] with strength $\Omega_1 T = \pi$. The atom always leaves the cavity in the ground state and can be discarded [19]. Atom b then passes through the Ramsey zones and cavity (with the off-resonant interaction), and the system undergoes the interaction described by Eq. (8). Afterwards the state of the cavity can be transferred again to that of an atom, thereby accomplishing the operation of $\mathbf{U}(\phi)$ [20].

To realize the more general operation of the universal 2-bit gate $\mathbf{S}_U^{(\tau)}$, the operation $\mathbf{U}(\phi)$ with $\phi = \pi\tau$ is first performed (see Fig. 2). In addition, a conditional phase shift of $\theta = \pi/4$ needs to be carried out on the "target" bit b, which can be achieved [21] simply by rotating the control bit a an angle θ about the z axis $[R_z(\theta) = e^{i\theta/2}|e\rangle\langle e| + e^{-i\theta/2}|g\rangle\langle g|]$. This rotation also produces a global phase shift of $-\theta/2$, which has no physical consequences. In our proposed implementation, this rotation is achieved by passing the atom carrying bit a through a Ramsey zone after it leaves the cavity. Here we emphasize that the appropriate choice of the Ramsey zone transformation and phase shifts ϕ and θ would allow one to produce an *arbitrary* unitary transformation of bit b, conditional on the state of the control bit a. In particular, choosing $\phi = \pi$ in Eq. (8) and $\theta = \pi/2$ yields the measurement gate $\mathbf{S}_M$.

The construction of the Deutsch gate, according to the decomposition of Eq. (5), would require five cavities. Only three cavities are required, however, if the bits a, b, and the result of $a \oplus b$ are stored in these three cavities (labeled C_1, C_2, and C_3), respectively. The following

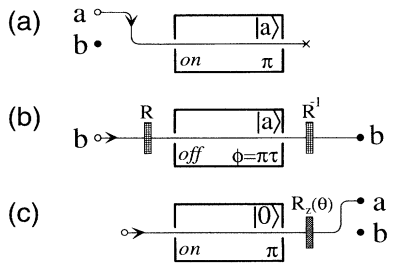

FIG. 2. Implementation of the 2-bit universal quantum logic gate by cavity QED techniques: The rectangles represent the cavities, with the type and strength of the atom-cavity interaction indicated. The state of the cavity after the passage of the atom is shown in the upper right corner, assuming basis states ($\{|a,b\rangle : a,b \in \{0,1\}\}$) are used for inputs. The trajectory of the atom is indicated by the solid line. The shaded regions represent Ramsey zones. (a) The state of the control bit a is transferred to the cavity. (b) Atom b is sent through the Ramsey zones and cavity and undergoes a conditional rotation. (c) The state of the control bit is transferred back to an atom, which is then rotated about the z axis by a Ramsey zone.

steps outline the operation of the Deutsch gate. (i) Atoms a and b are transferred (by the on-resonant interaction) to C_1 and C_2, respectively. (ii) A third atom x (prepared in state $|g\rangle$) is sent through a Ramsey zone R, off resonantly through C_1 and C_2 (with $\Omega_2\tau_2 = \pi$), through a second Ramsey zone R^{-1}, and then resonantly through C_3. After passing through the two Ramsey zones and two cavities, the atom x carries the computation $a \oplus b$. The resonant interaction of x with C_3 transfers the state of x to C_3. (iii) Atom c passes through a Ramsey zone R, all three cavities, and another Ramsey zone R^{-1}. The atom-cavity interactions are all off resonant, and satisfy the conditions $\Omega_2\tau_2 = \phi/2$ for both C_1 and C_2, and $\Omega_2\tau_2 = -\phi/2$ for C_3. Under these conditions, the total rotation experienced by atom c after interacting with the three cavities is 0 unless both a *and* b are initially in the excited state, in which case the rotation of atom c is $R_{\hat{x}}(\phi)$. (iv) The information in C_3 is removed by passing an atom x', initially in $|g\rangle$, *backwards* through C_3, and then through cavities C_2 and C_1. The interactions are the same as for step (ii) above, and the action of x' undoes the action of x. (v) Finally, the states of cavities C_1 and C_2 are transferred back to atoms (with the on-resonant interaction) for the readout of bits a and b. To produce the controlled phase shift on the target bit c, appropriate rotations R_z must be performed on the control bits a and b, as well as on the bit carrying $a \oplus b$.

We have shown in this Letter that cavity QED techniques can, in principle, be used to construct an arbitrary quantum computational network. The number and different kinds of experimental steps necessary to realize even the 3-bit Deutsch gate, however, indicate that extended networks would be exceedingly difficult to build. It appears that the principal difficulty with the cavity QED technique is the required coherence between all cavities involved and the control of the individual atoms at the

cavities. Furthermore, in current cavity QED experiments a thermal source of atoms is used, giving rise to a random distribution of atomic arrival times. A first demonstration of a quantum gate could be made with a weak atomic source, while disregarding those cases in which the wrong number of atoms has traversed the cavity. For a practical implementation, however, a controlled source of single particles is necessary. Such a source can be constructed for photons (which would carry the bits) by using parametric down conversion. While the interaction (7) is applicable to pairs of photons in a Kerr medium [15], the strength of the interaction is currently orders of magnitude too small to be of practical value.

In this Letter we have demonstrated the possibility of performing all quantum logic operations with networks consisting of 2-bit universal quantum gates. This universal quantum gate can, in principle, be realized with cavity QED techniques. External noise and quickly decaying coherence may limit the performance of such a device, but continuing improvements in cavity lifetime and control of the atom-field coupling will likely allow demonstration of the first universal quantum logic gates in the near future. The generic interactions [particularly Eq. (7)] described in this paper can also be applied to other systems, e.g., spin-spin coupling of nuclear spins, quantum dots [10], interactions between trapped ions [17], or photon-photon coupling in an all-optical realization. It is unknown in which of these or any other systems the numerous problems of generating single particle states, weak coupling, and noise and decoherence [22] can be solved, so that extended quantum networks can be built.

We thank C. H. Bennett and D. P. DiVincenzo for helpful discussions, and A. Ekert and M. Cords for comments on a draft of this work. H. W. was supported by the Austrian Fonds zur Förderung der Wissenschaftler Forschung. T. S. received support from the David and Lucile Packard Foundation.

[1] R. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[2] P. Benioff, J. Stat. Phys. **29**, 515 (1982); D. Deutsch, Proc. R. Soc. London A **400**, 96 (1985).

[3] D. Deutsch and R. Jozsa, Proc. R. Soc. London A **439**, 553 (1992); A. Berthiaume and G. Brassard, J. Mod. Opt. **41**, 2521 (1994); A. Berthiaume and G. Brassard, in *Proceedings of the Workshop on Physics of Computation* (IEEE, New York, 1992), p. 195; E. Bernstein and U. Vazirani, in *Proceedings of the 25th ACM Symposium on Theory of Computing* (ACM Press, New York, 1993), p. 11.

[4] P. W. Shor, in *Proceedings of the 35th Annual Symposium on FOCS*, edited by S. Goldwasser (IEEE Comput. Soc. Press, Los Alamitos, 1994), p. 124. The difficulty of factoring large numbers is one of the cornerstones of some important cryptographic schemes.

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

[6] C. H. Bennett, IBM J. Res. Dev. **6**, 525 (1973).

[7] T. Toffoli, Math. Systems Theory **14**, 13 (1981).

[8] E. Fredkin and T. Toffoli, Int. J. Theor. Phys. **21**, 219 (1982).

[9] J. Shamir, H. J. Caulfield, W. Miceli, and R. J. Seymour, Proc. SPIE Int. Soc. Opt. Eng. **625**, 2 (1986); G. J. Milburn, Phys. Rev. Lett. **62**, 2124 (1989).

[10] W. G. Teich, K. Obermayer, and G. Mahler, Phys. Rev. B **37**, 8111 (1988); D. M. Eigler, C. P. Lutz, and W. E. Rudge, Nature (London) **352**, 600 (1991); C. S. Lent, P. D. Tougaw, W. Porod, and G. H. Berstein, Nanotechnology **4**, 49 (1993); S. Lloyd, Science **261**, 1569 (1993); S. Lloyd, Science **263**, 695 (1994).

[11] An algebraic approach to decompose the Deutsch gate into an infinite series of 2-bit quantum gates is given by D. P. DiVincenzo [Phys. Rev. A **51**, 1015 (1995)]. A construction of the Deutsch gate similar to the one presented here is used by A. Barenco, "A Universal Two-Bit Gate for Quantum Computation" (unpublished).

[12] T. Sleator and H. Weinfurter, in Proceedings of Fundamental Problems in Quantum Theory, Baltimore, 1994, edited by D. Greenberger (to be published).

[13] M. Brune *et al.*, Phys. Rev. Lett. **65**, 976 (1990); Phys. Rev. A **45**, 5193 (1992); Phys. Rev. Lett. **72**, 3339 (1994). This last paper demonstrates a sensitivity, in phase shift per photon, of $\phi = 0.2\pi$ [see Eq. (8)].

[14] T. Sleator and H. Weinfurter (unpublished).

[15] J. Ph. Poizat and P. Grangier, Phys. Rev. Lett. **70**, 271 (1993); S. F. Pereira, Z. Y. Ou, and H. J. Kimble, *ibid.* **72**, 214 (1994).

[16] O. Benson, G. Raithel, and H. Walther, Phys. Rev. Lett. **72**, 3506 (1994); for an overview, see *Cavity Quantum Electrodynamics*, edited by P. R. Berman (Academic Press, New York, 1994).

[17] A recently proposed scheme for quantum computation that uses trapped ions may be experimentally feasible: J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[18] Strictly speaking, the Hamiltonian equation (7) should include an additional term $\hbar(\Omega_2/2)|e\rangle\langle e|$. The only physical consequence of this term is to produce a field *independent* rotation of the atomic state. This rotation can easily be compensated for by appropriate modification of the Ramsey fields [see discussion following Eq. (8)].

[19] The transfer of quantum states between atom and cavity has been discussed in Ref. [12]; T. Sleator and H. Weinfurter, in *IQEC Technical Digest Series 1994* (Optical Society of America, Washington, DC, 1994), Vol. 9, p. 140; M. A. Davidovich *et al.*, Phys. Rev. A **50**, R895 (1994).

[20] The operations described here are similar to those used in cavity QED schemes for teleportation. See Refs. [12,19] and J. I. Cirac and A. S. Parkins, Phys. Rev. A **50**, R4441 (1994).

[21] D. P. DiVincenzo *et al.*, "Elementary Gates for Quantum Computation" (unpublished).

[22] Discussions of the difficulties associated with quantum computation are given by R. Landauer, in Proceedings of the Drexel-4 Symposium on Quantum Nonintegrability–Quantum Classical Correspondence, edited by D. H. Feng and B-L. Hu (International Press, to be published); W. G. Unruh, Phys. Rev. A **51**, 992 (1995).