DESK COPY

PHYSICAL REVIEW A VOLUME 53, NUMBER 4 APRIL 1996

BRIEF REPORTS

Brief Reports are accounts of completed research which do not warrant regular articles or the priority handling given to Rapid Communications; however, the same standards of scientific quality apply. (Addenda are included in Brief Reports.) A Brief Report may be no longer than four printed pages and must be accompanied by an abstract. The same publication schedule as for regular articles is followed, and page proofs are sent to authors.

Five two-bit quantum gates are sufficient to implement the quantum Fredkin gate

John A. Smolin
Department of Physics, University of California at Los Angeles, Los Angeles, California 90025

David P. DiVincenzo
IBM Research Division, T. J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598

(Received 18 September 1995)

We present an analytic construction of the three-bit quantum conditional swap (Fredkin) gate that uses only five quantum gates, each acting on only two qubits. Our implementation is based on previous work on the three-bit quantum conditional-NOT (Toffoli) gate. Numerical evidence suggests that this is a minimal implementation.

PACS number(s): 03.65.Bz, 89.80.+h

There has been a great deal of interest lately in quantum computation, especially after Shor's discovery of a polynomial-time quantum factoring algorithm [1]. It is now well known that two-bit quantum gates are sufficient to synthesize any unitary operation in any size Hilbert space [2]. We have shown numerically that six two-bit quantum gates are sufficient to generate any three-bit quantum gate [3], but of particular interest are the universal quantum gates and those larger gates that can be simply constructed using them. Several of them are presented in [4].

One gate that has received particular attention is the three-bit conditional swap gate, or Fredkin gate. The Fredkin gate is of interest because it is a universal gate for classical reversible computation [5]. The quantum version has been used by Ekert and Macchiavello [6] to design a circuit for error correcting quantum computations with the symmetric-subspace method of [7].

The quantum Fredkin gate is "quantum" in the sense that in a particular basis (typically one in which each basis vector is a product vector of the two-dimensional Hilbert spaces of individual quantum-bit carriers) it behaves just as a classical Fredkin gate; it also must act on superpositions of the basis vectors unitarily, preserving the superposition rather than collapsing the input state into one of the basis states and then acting upon it.

In [8], Chau and Wilczek give a specific six-gate construction of the three-bit conditional swap gate, or Fredkin gate. They pose the question of whether it can be done in fewer gates. Here we present an analytic five-gate construction which our numerical tests suggest is minimal.

Figure 1 shows seven gates that make a Fredkin gate. The middle five gates make a three-bit conditional-NOT gate, or Toffoli gate. This is a slight modification of a Toffoli gate construction presented in [4]. It is straightforward to verify that a Toffoli gate can be converted to a Fredkin gate with the addition of the two conditional NOT gates around it. The first two gates in the figure are each acting on the same two bits, and therefore can be replaced by a single two-bit gate. The last two gates commute; therefore, the last gate can be moved in front of the preceding gate. There are then two adjacent gates acting on the same two bits. By merging these two gates we arrive at a five-gate design.

We used our numerical minimization routines, described in [3], to search for a shorter implementation and have found none. However, since the numerical search often gets stuck in local minima, even in cases where it eventually finds a solution, the fact that we were unable to find a smaller implementation of the Fredkin gate is not a proof that one does not exist.

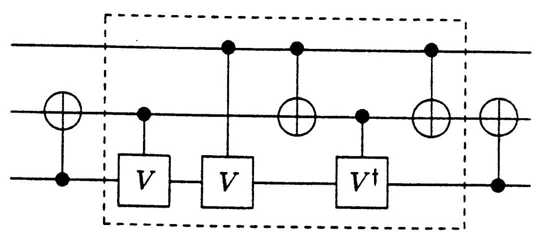

FIG. 1. Seven-gate implementation of a Fredkin gate, which can be converted to a five-gate implementation as discussed in the text. A circle enclosing a cross indicates the state of that bit is conditionally negated if the state of the associated bit marked with a solid dot is 1. A V or $V^{\dagger}$ indicates the state of the bit is multiplied by the 2×2 matrix $V=\begin{pmatrix}0&1\\1&0\end{pmatrix}^{1/2}=(1+i)/2\begin{pmatrix}1&-i\\-i&1\end{pmatrix}$, or its Hermitian conjugate, when the bit indicated by the solid dot is 1.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124.

[2] D. P. DiVincenzo, Phys. Rev. A **50**, 1015 (1995); S. Lloyd, Phys. Rev. Lett **75**, 346 (1995); D. Deutsch, A. Barenco, and A. Ekert, Proc. R. Soc. London Ser. A **449**, 669 (1995).

[3] D. P. DiVincenzo and J. Smolin, in *Proceedings of the Workshop on Physics and Computation, PhysComp '94*, (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 14.

[4] T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995); A. Barenco, C. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

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

[6] A. Ekert and C. Macchiavello (unpublished).

[7] A. Berthiaume, D. Deutsch, and R. Jozsa, in *Proceedings of the Workshop on Physics and Computation, PhysComp '94* (Ref. [3]), p. 60.

[8] H. F. Chau and F. Wilczek, Phys. Rev. Lett. **50**, 748 (1995).