Programmable Quantum Gate Arrays

M. A. Nielsen[1,*] and Isaac L. Chuang[2,†]

[1]*Center for Advanced Studies, Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156*

[2]*Theoretical Astrophysics T-6, Los Alamos National Laboratory, Los Alamos, New Mexico 87545*

(Received 18 March 1997)

We show how to construct quantum gate arrays that can be programmed to perform different unitary operations on a *data register*, depending on the input to some *program register*. It is shown that a *universal quantum gate array*—a gate array which can be programmed to perform *any* unitary operation—exists only if one allows the gate array to operate in a probabilistic fashion. Thus it is not possible to build a fixed, general purpose quantum computer which can be programmed to perform an arbitrary quantum computation. [S0031-9007(97)03547-3]

PACS numbers: 89.70.+c, 03.65.–w

Quantum computers [1–3] can perform arbitrary unitary operations on a set of two-level systems known as *qubits*. These unitary operations are usually decomposed as *quantum gate arrays* which implement the desired unitary operation using a finite amount of resources. Depending on what unitary operation is desired, different gate arrays are used [4].

By contrast, a classical computer can be implemented as a fixed classical gate array, into which is input a *program*, and *data*. The program specifies the operation to be performed on the data. A universal gate array can be programmed to perform any possible function on the input data.

This paper addresses the question of whether it is possible to build analogous *programmable* quantum gate arrays—fixed circuits, which take as input a quantum state specifying a *quantum program*, and a *data register*, to which the unitary operator corresponding to the quantum program is applied.

These gate arrays are modeled in the following manner: the initial state of the system is assumed to be of the form

$$|d\rangle \otimes |\mathcal{P}\rangle, \tag{1}$$

where $|d\rangle$ is a state of the m-qubit data register, and $|\mathcal{P}\rangle$ is a state of the n-qubit program register. Note that the two registers are not entangled. The total dynamics of the programmable gate array is given by a unitary operator, G,

$$|d\rangle \otimes |\mathcal{P}\rangle \rightarrow G[|d\rangle \otimes |\mathcal{P}\rangle]. \tag{2}$$

This operation is implemented by some fixed quantum gate array. A unitary operator, U, acting on m qubits, is said to be *implemented* by this gate array if there exists a state $|\mathcal{P}_U\rangle$ of the program register such that

$$G[|d\rangle \otimes |\mathcal{P}_U\rangle] = (U|d\rangle) \otimes |\mathcal{P}'_U\rangle, \tag{3}$$

for all states $|d\rangle$ of the data register, and some state $|\mathcal{P}'_U\rangle$ of the program register. *A priori*, it is possible that $|\mathcal{P}'_U\rangle$ depends on $|d\rangle$. To see that this is not the case, suppose

$$G[|d_1\rangle \otimes |\mathcal{P}\rangle] = (U|d_1\rangle) \otimes |\mathcal{P}'_1\rangle, \tag{4}$$

$$G[|d_2\rangle \otimes |\mathcal{P}\rangle] = (U|d_2\rangle) \otimes |\mathcal{P}'_2\rangle. \tag{5}$$

Taking the inner product of these equations we see that $\langle \mathcal{P}'_1 | \mathcal{P}'_2 \rangle = 1$ provided $\langle d_1 | d_2 \rangle \neq 0$ (the case $\langle d_1 | d_2 \rangle = 0$ follows by similar reasoning), and thus $|\mathcal{P}'_1\rangle = |\mathcal{P}'_2\rangle$, and therefore there is no $|d\rangle$ dependence of $|\mathcal{P}'_U\rangle$. A schematic of this setup is shown in Fig. 1.

The set of unitary operators on m qubits can be parametrized by 2^{2m} independent real numbers, which is fewer than the $2^{2m+1} - 1$ real numbers needed to parametrize a set of $2m$ qubits. Therefore, it seems that it might be possible to implement a *universal* quantum gate array—one which can be programmed to implement *any* unitary operation. Universal gate arrays are certainly possible for classical computers, since by counting the number of possible functions we see that an arbitrary function on m bits can be specified using $m2^m$ bits, and it is straightforward to design a classical circuit which will take as input $m2^m$ program bits and implement the corresponding function on m data bits.

The following result shows that no universal quantum gate array (of finite extent) can be realized. More specifically, we show that every implementable unitary operation requires an extra Hilbert space dimension in the program register. Since the number of possible unitary operations on m qubits is infinite, it follows that a universal gate array would require an infinite number of qubits in the program register, and thus no such array exists. Note also that a program register with d dimensions can be used to implement d unitary operations

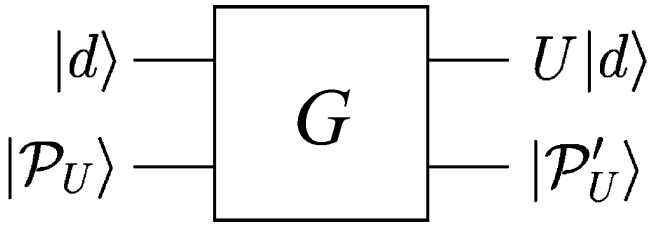

FIG. 1. Conceptual schematic of a programmable quantum gate array which implements the unitary operation U, determined by the quantum program $|\mathcal{P}_U\rangle$.

which are distinct up to a global phase by performing an appropriate sequence of controlled unitary operations [4].

Result: Suppose distinct (up to a global phase) unitary operators $U_1, \ldots, U_N$ are implemented by some programmable quantum gate array. Then the program register is at least N dimensional, that is, contains at least $\log_2 N$ qubits. Moreover, the corresponding programs $|\mathcal{P}_1\rangle, \ldots, |\mathcal{P}_N\rangle$ are mutually orthogonal.

The proof is to suppose that $|\mathcal{P}\rangle$ and $|\mathcal{Q}\rangle$ are programs which implement unitary operators U_p and U_q which are distinct up to global phase changes. Then for arbitrary data $|d\rangle$ we have

$$G(|d\rangle \otimes |\mathcal{P}\rangle) = (U_p|d\rangle) \otimes |\mathcal{P}'\rangle, \tag{6}$$

$$G(|d\rangle \otimes |\mathcal{Q}\rangle) = (U_q|d\rangle) \otimes |\mathcal{Q}'\rangle, \tag{7}$$

where $|\mathcal{P}'\rangle$ and $|\mathcal{Q}'\rangle$ are states of the program register. Taking the inner product of the previous two equations gives

$$\langle \mathcal{Q} \,|\, \mathcal{P}\rangle = \langle \mathcal{Q}' \,|\, \mathcal{P}'\rangle \langle d|U_q^\dagger U_p|d\rangle. \tag{8}$$

Suppose $\langle \mathcal{Q}' \,|\, \mathcal{P}'\rangle \neq 0$. Then dividing through both sides of the equation gives

$$\frac{\langle \mathcal{Q} \,|\, \mathcal{P}\rangle}{\langle \mathcal{Q}' \,|\, \mathcal{P}'\rangle} = \langle d|U_q^\dagger U_p|d\rangle. \tag{9}$$

The left hand side of this equation has no $|d\rangle$ dependence, and thus $U_q^\dagger U_p = \gamma I$ for some c-number γ. It follows that the only way we can have $\langle \mathcal{Q}' \,|\, \mathcal{P}'\rangle \neq 0$ is if U_p and U_q are the same up to a global phase. But we have assumed that this is not so and thus $\langle \mathcal{Q}' \,|\, \mathcal{P}'\rangle = 0$. Equation (8) now tells us that

$$\langle \mathcal{Q} \,|\, \mathcal{P}\rangle = 0. \tag{10}$$

That is, the programs are orthogonal. The result follows.

This result demonstrates that no *deterministic* universal quantum gate array exists. We will now see that it is possible to implement a universal quantum gate array in a *probabilistic* fashion.

The procedure is illustrated in Fig. 2 for the case of $m = 1$. In the general case the $2m$ qubit program for the m qubit unitary operation U is found as follows:

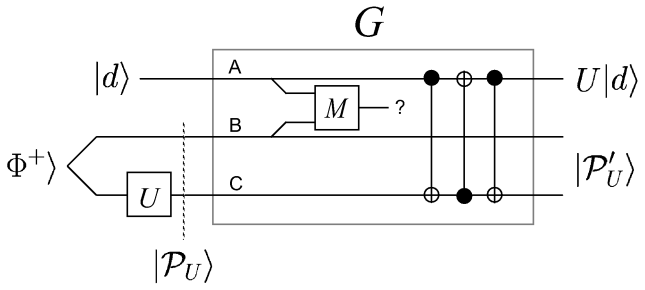

FIG. 2. A probabilistic universal quantum gate array.

$$|\mathcal{P}_U\rangle = (I_m \otimes U) \bigotimes_{i=1}^{m} |\Phi^+_{i,m+i}\rangle, \tag{11}$$

where I_m is the identity operator on the first m qubits of the program register, and the state $|\Phi^+_{x,y}\rangle$ is a Bell state $|\Phi^+\rangle \equiv (|00\rangle + |11\rangle)/\sqrt{2}$ shared between qubits x and y of the program register. Joint measurements are made on the data qubits and the first m program qubits as follows. The Bell basis is defined to consist of the states

$$|\Phi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{12}$$

$$|\Psi^\pm\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{13}$$

Suppose a joint measurement M in the Bell basis is made on the first data qubit and the first program qubit. A joint measurement in the Bell basis is then made on the second data qubit and the second program qubit, and so on for all m data qubits.

Specifically, for $m = 1$, we have the program

$$|\mathcal{P}\rangle = (I \otimes U)\,|\Phi^+\rangle = \frac{|0\rangle U|0\rangle + |1\rangle U|1\rangle}{\sqrt{2}}. \tag{14}$$

For an input data register $|d\rangle = a|0\rangle + b|1\rangle$, the input $|d\rangle\,|\mathcal{P}\rangle$ to the gate array may be rewritten as

$$[a|0\rangle + b|1\rangle]\,\frac{|0\rangle U|0\rangle + |1\rangle U|1\rangle}{\sqrt{2}} = \frac{1}{2}[a(|\Phi^+\rangle + |\Phi^-\rangle)U|0\rangle + a(|\Psi^+\rangle + |\Psi^-\rangle)U|1\rangle$$

$$+ b(|\Psi^+\rangle - |\Psi^-\rangle)U|0\rangle + b(|\Phi^+\rangle - |\Phi^-\rangle)U|1\rangle] \tag{15}$$

$$= \frac{1}{2}[|\Phi^+\rangle(aU|0\rangle + bU|1\rangle) + |\Phi^-\rangle(aU|0\rangle - bU|1\rangle)$$

$$+ |\Psi^+\rangle(aU|1\rangle + bU|0\rangle) + |\Psi^-\rangle(aU|1\rangle - bU|0\rangle)] \tag{16}$$

$$= \frac{1}{2}[|\Phi^+\rangle(U|d\rangle) + |\Phi^-\rangle(U\sigma_z|d\rangle) + |\Psi^+\rangle(U\sigma_x|d\rangle)$$

$$+ i|\Psi^-\rangle(U\sigma_y|d\rangle)]. \tag{17}$$

Now, when the measurement result from M gives an eigenvalue corresponding to $|\Phi^+\rangle$, then the postmeasurement state of the second qubit of the program register will be $U|d\rangle$, which is the desired transform. Three controlled-NOT gates then swap the state $U|d\rangle$ of the second qubit of the program register back into the data register, completing a successful operation of the programmable gate array. However, for the other three possible outcomes, the result will be different. Thus, in the $m = 1$ case, the gate array is *nondeterministic*, and succeeds with probability $1/4$. Note that the result of the measurement tells us with certainty whether the gate array has succeeded.

This reasoning is easily generalized to larger m, in which case if the result of all the measurements corresponds to the Bell state $|\Phi^+\rangle$, then the state of the final m qubits of the program register is $U|d\rangle$. This event has probability 2^{-2m}, independent of the initial state $|d\rangle$ or U. To complete the operation of the universal gate array the state of the final m qubits of the program register is swapped back into the data register, to give the desired output $U|d\rangle$. This is easily accomplished using cascaded controlled-NOT gates [5]. Alternatively, the location of the data register output can be redefined appropriately.

Readers familiar with quantum teleportation [6] can understand why the scheme works in the following way. Divide the total system up into three systems: A, the data register, B, the first m lines of the program register, and C, the final m lines of the program register. The scheme as described is equivalent to applying U to system C, where B and C are initially bit-pairwise maximally entangled. The usual measurement procedure for teleportation is then applied to systems A and B. Since this procedure involves only systems A and B it commutes with the application of U to system C, and we can suppose for the purposes of analysis that the measurement was actually performed *before* the unitary U. By our knowledge of teleportation we know that for one (and only one) of the measurement outcomes that may occur, the effect is simply to transfer the state of system A to system C, without the need to unitarily "fix up" the state of system C. Provided this measurement outcome, which has probability 2^{-2m}, occurs, the total operation is equivalent to teleporting the data register to system C and then applying U to that system. The procedure is completed by swapping system C back to system A. As has been pointed out previously, this entire procedure can be accomplished by a quantum circuit [7].

It is clear from this explanation in terms of teleportation that the universal gate array works for nonunitary as well as unitary quantum operations [8,9]. Unitary quantum operations have programs which are pure states, while nonunitary operations have programs which are mixed states.

This universal quantum gate array is particularly remarkable because the number of gate operations is polynomial (indeed, linear) in the number of data qubits. This is a great contrast to classical (deterministic) universal gate arrays, which must be exponential in the number of data bits. To see this, consider that there are at least $m2^m$ program bits in the classical universal gate array, and each one of these bits must pass through at least one gate if it is to have any effect on the data as a "program" bit. If the maximum number of bits used as input to any gate in the array is k, then it follows that a classical universal gate array must have at least $m2^m/k$ gates. The quantum universal gate array we have demonstrated trades off an exponentially smaller number of gates than the classical universal gate array at the expense of an exponentially small probability of success. On *average* the number of gate operations required for *successful operation* of the universal quantum gate array goes like $m2^{2m}$. Where the universal quantum gate array wins out over the classical universal gate array is the much larger variety of transformations it is able to effect.

We have demonstrated that no deterministic universal quantum gate array exists. More generally, a deterministic programmable gate array must have as many Hilbert space dimensions in the program register as the number of programs implemented. Thus, it is not possible to build a fixed, general purpose quantum computer, of finite extent, which can be programmed to perform an arbitrary quantum computation. This is an essential difference between classical and quantum computing. In the context of laboratory experiments on quantum computation, this means that a large number of classically distinguishable states must be available in order to build useful quantum computing devices. Fortunately, there is no shortage of such states in the laboratory. Note that our results limit but do not exclude the possibility of building a programmable gate array which can be programmed to perform an interesting subclass of unitary operations. In this spirit, we have exhibited a probabilistic universal quantum gate array that requires only a linear number of gates, but which has an exponentially small probability of success. It would be extremely interesting to know if this is the best that can be done, or if it is possible to build a universal quantum gate array which is more efficient. It may also be possible to develop a theory of program complexity based on the universal gate array we have proposed, perhaps based on measures of entanglement for quantum programs.

We thank Carlton M. Caves and Richard Cleve for useful discussions about this work. This work was supported by the Office of Naval Research (Grant No. N00014-93-1-0116) and the Australian-American Educational Foundation (Fulbright Commission).

*Electronic address: mnielsen@tangelo.phys.unm.edu
†Electronic address: ike@lanl.gov

[1] D. P. DiVincenzo, Science **270**, 255 (1995).
[2] C. H. Bennett, Phys. Today **48**, No. 10, 24 (1995).
[3] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 1 (1996).
[4] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995).
[5] A. Barenco, D. Deutsch, and A. Ekert, Phys. Rev. Lett. **74**, 4083 (1995).
[6] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[7] G. Brassard, S. Braunstein, and R. Cleve (to be published).
[8] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).
[9] B. W. Schumacher, Phys. Rev. A **54**, 2614 (1996).