twogat06.latex–submitted to Phys. Rev. A (AT5101); condmat/9407022

Two-bit gates are universal for quantum computation

David P. DiVincenzo

IBM Research Division

Thomas J. Watson Research Center

P. O. Box 218

Yorktown Heights, NY 10598 USA

(Received June 24, 1994)

Abstract

A proof is given, which relies on the commutator algebra of the unitary Lie groups, that quantum gates operating on just two bits at a time are sufficient to construct a general quantum circuit. The best previous result had shown the universality of three-bit gates, by analogy to the universality of the Toffoli three-bit gate of classical reversible computing. Two-bit quantum gates may be implemented by magnetic resonance operations applied to a pair of electronic or nuclear spins. A "gearbox quantum computer" proposed here, based on the principles of atomic force microscopy, would permit the operation of such two-bit gates in a physical system with very long phase breaking (i.e., quantum phase coherence) times. Simpler versions of the gearbox computer could be used to do experiments on Einstein-Podolsky-Rosen states and related entangled quantum states.

1994 PACS: 03.65.Bz, 89.80.+h, 02.20.Sv, 76.70.Fz

I. INTRODUCTION

Eventually computational devices will stop getting smaller and faster unless new physical principles of operation are discovered. Undoubtedly the physical principles of quantum mechanics will become increasingly important if these devices are ever to operate at the atomic level. The basic idea that a useful computer might be constructed which operates according to the principle of unitary time evolution, the cornerstone of the quantum theory, was first put forward by Benioff [1]. Since then, there has been a steady stream of work on demonstrating how "quantum gates" can be put together into "quantum circuits" which perform any unitary time evolution, and on how such quantum gates could be realized by the electromagnetic pulsing of solid-state spin systems.

While these developments have been of theoretical interest, the importance of these investigations has been heightened by some recent seminal mathematical results concerning the potential power of quantum computing. Deutsch and Josza [2], with some crucial clarifications from Bernstein and Vazirani [3], introduced the subject of quantum complexity theory, and pointed out the possibility that quantum machines may be more efficient in performing certain computations than any classical computer. Very recently Shor [4], following on the work of Simon [5], has proved an extremely exciting result: he has shown that on a quantum computer, prime factoring can be performed in "polynomial" time, that is, $t \propto k^p$, where k is the number of bits in the number to be factored and p is a constant. By contrast, this problem is believed to take $e^{ck^{\frac{1}{3}}}$ time on a classical computer (c is another constant). As the difficulty of prime factoring is of paramount importance in the functioning of certain popular data encryption schemes, the absolute desirability of performing quantum computation, and the interest in understanding how a genuine physical realization might be achieved, has increased sharply.

In this paper, then, I take up some specific problems which will need to be addressed in order to make quantum computing a reality. I begin with some discussion which emphasizes the stringent requirements in quantum computing for the *physical isolation* of the computer from outside influences; this point has been made in much of the previous work, but I wish to emphasize it as probably the most difficult design requirement. Motivated by this, I introduce a computing machine, a "quantum gearbox", which arranges for individual spins to be in very well-isolated environments except during the moment that pairs of spins pass through logic gates. I will point out here that in the "quantum gearbox", and in other physical implementations which have been proposed for quantum circuits as well, it is extremely difficult to imagine a physical implementation of a three-bit quantum gate, that is, a gate in which three bits (i.e., spins) interact simultaneously. It is much easier (although not necessarily easy) to imagine a machine in which spins interact two at a time (this is explicit in the quantum gearbox).

This situation motivates the main results of the paper, on the universality of two-bit computation. It has previously been proved that three-bit gates are sufficient to build any arbitrary quantum network, and no other workers have investigated whether this result can be improved upon. Here, using the techniques of Lie group theory, I prove the desired new result, that two-bit gates suffice to generate any arbitrary quantum network, i.e., any arbitrary unitary transformation. The proof provides an explicit realization of three-bit operations in terms of sequences of two-bit gates, although it remains to be seen whether this may form the basis of a practical, efficient method of designing quantum circuits. Substantial progress has already been made in devising explicit two-bit-gate realizations of some of the key steps in the Shor factoring procedure [6].

II. BUILDING A QUANTUM COMPUTER

A. Why making a quantum computer is very, very difficult

As Shor's work shows, making a quantum computer would have decided technological and economic consequences. Why will neither IBM, nor Dell, nor anyone, be marketing one before the end of the century? The laws of physics give us confidence that the world does indeed evolve by unitary time evolution (i.e., according to an S-matrix–see Sec. III A). The problem is that to make a quantum computer, we insist that a *particular subset* of the world undergo unitary evolution; this is what is very, very hard. A sub-block of a unitary matrix is almost never itself unitary–it would be so only if the matrix were block-diagonal. An S-matrix is only block diagonal if the different subsystems are not interacting; but in the physical world, degrees of freedom are usually interacting with many other degrees of freedom. The understanding of this point is crucial for the explanation of why classical mechanics in the macroscopic world emerges out of the microscopic operation of quantum mechanics.

This discussion makes clear why a transistor, or any conventional computer element, cannot perform quantum computation. The computational state of the system, the "0"'s and "1"'s entering and leaving the gate, is only one degree of freedom out of the countlessly many microscopic degrees of freedom of the device (e.g., the elastic vibrations of the device, the excitations of its conduction electrons). In general, all of these degrees of freedom interact strongly with one another and with the computational state of the device. Even worse, in fact, is that the computational state is often a collective property of this myriad of microscopic states. Such a situation makes even approximate unitary evolution impossible.

The kind of subsystem-isolation which quantum computation requires will probably only be achievable if the computer elements are themselves of atomic or near-atomic dimensions, where the computational state is the quantum state of a single atom. Even in this realm, quantum computation is under substantial constraint: if this computation state is arranged to interact weakly with the rest of the world, then for short times its evolution will be unitary, but eventually even weak interactions will cause significant departures from unitarity. Such systems have a characteristic time for loss of unitarity, which is known in the field of mesoscopic physics as the "dephasing time" t_ϕ [7]. t_ϕ has been measured in various microscopic and mesoscopic physical systems, and it is often extremely short. For example, for the state of an electron traversing a gold wire at temperatures less than 1K, t_ϕ is of order 10^{-13} seconds. (This time is still long enough for interesting "phase coherence" effects to be seen, such as Aharonov-Bohm oscillations [7].) The state of an electron's spin [8] (i.e., the state of the electron's magnetic moment) is more stable, but an upper bound for its dephasing time, recently measured in a salt containing paramagnetic Eu ions [9], is 10^{-3} seconds. Since the program on a quantum computer would have to be finished running in a time less than t_ϕ (probably a great deal less), we see that there are severe limits on the kind of quantum computation which these physical systems can perform. I believe that other microscopic systems which have been discussed for quantum computation, for example the "Notre-Dame logic gate" [10] (operating by the hopping of electrons from one quantum dot to another) or the "atom switch" [11] (operating by the hopping of a single atom from one site on a crystal surface to another) are similarly problematic; although I know of no measurements of t_ϕ in these cases, I expect that it is similarly short. Even these systems will be "too classical" [12].

Although still far from easy, I believe that one of the other microscopic systems which has been discussed in this context has a somewhat greater promise of having the necessary quantum coherence for some kind of quantum computation to be possible: this is the nuclear spin. The spin of the nucleus produces a much smaller magnetic moment than that of the electron (650 times smaller for the proton), so its dipolar magnetic interactions with the rest of the world are much weaker; also, it does not have the same strong exchange interactions arising from the Pauli exclusion principle which electrons do. For this reason, nuclei have t_ϕ's which can, under favorable circumstances, be orders of magnitude longer than for electronic spins, or any other quantum degrees of freedom. The value of this t_ϕ has been estimated, given ideal assumptions about the electromagnetic environment in a Nuclear Magnetic Resonance apparatus, to be 10^{10} seconds (3 years) [13,14]. This number will certainly be much smaller in reality and will depend on many details of the solid-state environment of the spins, which I will discuss in a moment.

B. Gearbox quantum computer

In Fig. 1 I propose the principal working element of a quantum computer. It is meant to be more thought-provoking than real: I don't suggest that experimentalists try immediately to go out to build this device, but I do hope that it provides a springboard for productive thought on what really needs to be done to perform quantum computation. Of course, others before me [15,16] have made proposals for, and explored the feasibility of [17], "potentially realizable quantum computers"; the one I now present exploits somewhat different physical principles than the previous proposals, and hopefully provides ideas for how some of the monstrous obstacles (like the ones discussed in Sec. II A) could be overcome.

In the "gearbox quantum computer" shown, the two meshed gears operate classically, turning in synchrony. The protons, carrying the spins which will evolve quantum mechanically, are firmly attached to the end of the tips of the left-hand gear, and to the base of the grooves of the right-hand gear. By making the gear elements very "quiet" magnetically and electronically, it may be hoped that a very long dephasing time for the spins may be achieved. This quietness may be obtained by using diamagnetic, insulating materials, containing nuclei with mostly no nuclear spins. A gear made from a pure undoped crystal of ^{28}Si (92% natural abundance) could well be optimal.

The teeth of the left-hand gear are shown in the shape of atomic-force microscope (AFM) tips, suggestive of the fact that atomic spatial resolution will be necessary in the meshing of the two gears, in order that the two spins may be brought into atomic contact. The gears are shown with 16 and 15 teeth respectively; by making these numbers relatively prime, it is assured that each pair of spins on either gear may be brought into contact by turning the gearbox. The atomic contact between spins is necessary in order for quantum logic gates, unitary transformations of pairs of bits, to be executed. When the spins are not in contact, the Hamiltonian H_{spin} of the spins is zero, and no time evolution occurs. During the time that the spins are in contact, $H_{spin}(t)$ will be non-zero, inducing, according to the well-known laws of quantum mechanics [18], the unitary transformation

$$U = Te^{-\frac{i}{\hbar}\int H_{spin}(t)dt}, \tag{2.1}$$

where T indicates a time-ordered product. We can write out the Hamiltonian a little further as $H_{spin} = H_{dipole} + H_{ext}$, where H_{dipole} is the magnetic dipole interaction between the two nuclei, and H_{ext} is an external Hamiltonian which may be applied just to the region where the spins are interacting; this may consist of some combination of static and a.c. magnetic fields. It is expected that, as in the work of Lloyd [15], it is possible with suitable external fields to induce any arbitrary two-spin unitary operation in Eq. (2.1), although I have not worked out a detailed protocol for this. In the next section I will discuss the adequacy of these two-bit gates for general quantum computation.

A few more remarks about the "quantum gearbox" are in order. It is obvious that if more bits are needed, for I/O, memory, etc., they can be added simply by adding more gears to the system. Note that since one of the simplest unitary operations is a swap, the state of any spin may be propagated arbitrarily far along an array of gears. Somewhere in the gear system will be located the "output" device, which will require considerable technological ingenuity: This device must sense the state of a single spin and make that information available to the rest of the world. This operation can be done only at the end of the quantum computation, since it involves strong interaction of the quantum computer with other degrees of freedom, destroying the unitary evolution. There is presently no magnetometry of sufficient sensitivity to sense the state of a single proton spin; however, the mechanical detection of magnetic resonance within magnetic force microscopy will, according to Rugar and coworkers [19], be able to perform such detection in the foreseeable future.

There is another design requirement for a quantum computer whose satisfaction requires some ingenuity in the quantum gearbox. Quantum computations under consideration now [5,4] require that the spins be an initial simple state, e.g., all up. But because of the low energy scales involved, an assemblage of nuclear spins at any reasonable temperature will typically have a random state which is drawn from a Boltzmann distribution. Nevertheless, it would be possible to exploit some of the techniques of magnetic resonance to prepare an initially polarized state. One way of doing this would be to prepare a gear with attached single *electron* spins. Because of their much greater magnetic moment, these can be put in a polarized state at a reasonable temperature. When they are meshed into contact with the nuclear spins, one can use one of the known techniques (the Overhauser effect, coherence transfer [20]), for transferring the electronic spin polarization to the nuclei. This process need not be phase-coherent, because it would precede the start of the quantum computation.

I wish to close this section with a few remarks on the strengths and weaknesses of the quantum gearbox relative to another "potentially realizable quantum computer" discussed recently by Lloyd [15], in which the quantum spins are embedded in a polymer chain or a crystal lattice. One obvious advantage of the polymer computer is that the interaction Hamiltonian between the spins is more controlled, since it depends only on the local environment in the crystal. In the gearbox computer, atomic-scale vibrations and misalignments might be very difficult to control and quite deleterious to the operation. Another advantage of the polymer computer is that the unitary operations can go on in parallel, although the ability to address specific pairs of spins is lost. In the polymer computer, not just two-bit but also three-bit local operations can be executed (but this is not a crucial advantage– see the next section). The polymer computer has the disadvantage that the interaction Hamiltonian between the spins can never be turned off. This does not necessarily lead to insuperable problems, but it makes the control of the phase of the quantum state particularly ungainly. Finally, there is a concern that it may be difficult to make a magnetic polymer or a magnetic crystal sufficiently "quiet", i.e., sufficient immune from interaction with other, non-computational degrees of freedom.

III. DEMONSTRATION OF TWO-ELEMENT GATES FOR UNIVERSAL COMPUTATION

Previous studies, to be reviewed momentarily, have shown how to perform any arbitrary unitary operation by composing a sequence of three-bit operations. This is very inconvenient from the point of view of the gearbox computer; it is exceedingly difficult to imagine a mechanical device which could bring three spins together simultaneously. However, I will prove a new result which resolves this difficulty: even two-bit operations alone suffice to give universal quantum computation.

A. Background: What Deutsch proved

Deutsch [21] has already shown how to obtain a universal quantum computation, defined as an arbitrary unitary transformation on a discrete Hilbert space spanned by the set of all states of a collection of bits. He did this by a simple and elegant generalization of the known specifications for building a reversible *classical* network. There exists a close connection between classical reversible computation and quantum computation, since all unitary quantum operations are necessarily reversible; therefore, reversible computing is a subset of quantum computing. Toffoli [22] showed how the AND and XOR gates necessary for conventional universal computation may be implemented reversibly; conventional AND and XOR gates are not reversible, if for no other reason that a reversible gate must have the same number of output as input bits. He showed that XOR could be implemented reversibly with a two-bit gate in which one output bit returns the conventional XOR $a_1 \oplus a_2$ (a_1 and a_2 are the binary values of the two input bits), while the other output bit returns the original value of a_1 (or a_2). To implement AND reversibly, a three-bit gate is required in which a_1 and a_2 are passed through unchanged, while the third bit is XORed with the AND of the first two, returning $a_1 \cdot a_2 \oplus a_3$. Indeed, since this three-bit gate comprises both the XOR and the AND functions, it can be considered to be *the* universal reversible computation gate, and it has come to be known as the Toffoli gate $\mathbf{T}$.

Given this background, the generalization by Deutsch to the quantum problem is simple and appealing. Following logically from the structure of quantum mechanics, Deutsch generalized the posited operation of a three-bit gate, from one which performs transformations (permutations, actually, in the reversible case) on the $8 = 2^3$ possible states of three bits, to one which performs unitary transformations within the 2^3-dimensional complex vector space (the "Hilbert space") spanned by the states of the three bits. Deutsch proved that all unitary transformations could be obtained from one operating upon three bits, that one being a natural generalization of the Toffoli operation. This result has been used in subsequent studies [23] to understand the complexity of quantum circuits using three-bit gates.

Deutsch's universal gate $\mathbf{Q}$ has the S-matrix [24]

$$(\mathbf{S_Q})^{a_1a_2a_3}_{a_1'a_2'a_3'} = \delta^{a_1}_{a_1'}\delta^{a_2}_{a_2'}[(1-a_1\cdot a_2)\delta^{a_3}_{a_3'} + ia_1\cdot a_2 e^{-\frac{1}{2}i\pi\alpha}(S_N^\alpha)^{a_3}_{a_3'}]. \tag{3.1}$$

"S-matrix" is the quantum mechanical jargon for the unitary transformation executed (in the course of a given length of time, say) upon the Hilbert space. Here the primed variables denote the binary states of the three output bits (as in Fig. 2), α is a fixed arbitrary irrational number, and S_N^α is an elementary one-bit transformation specified by the 2×2 unitary matrix

$$S_N^\alpha = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi\alpha}, & 1-e^{i\pi\alpha} \\ 1-e^{i\pi\alpha}, & 1+e^{i\pi\alpha}\end{pmatrix}, \tag{3.2}$$

to which Deutsch gives the picturesque appellation "the α^{th} power of not". It is noted that when $\alpha = 1$, except for a phase factor Eq. (3.1) is the S-matrix of the classical Toffoli gate:

$$(\mathbf{S_T})^{a_1a_2a_3}_{a_1'a_2'a_3'} = \delta^{a_1}_{a_1'}\delta^{a_2}_{a_2'}[(1-a_1\cdot a_2)\delta^{a_3}_{a_3'} + a_1\cdot a_2(S_N^{\alpha=1})^{a_3}_{a_3'}] = \delta^{a_1}_{a_1'}\delta^{a_2}_{a_2'}\delta^{(a_3\oplus a_1\cdot a_2)}_{a_3'}. \tag{3.3}$$

B. Proof that Q can be realized by two-bit gates

In this subsection I will show explicitly how one of Deutsch's three-bit gates may be realized by a set of one- and two-bit gates; the result is summarized graphically in Fig. 2. Here I will work only with one version of the Deutsch gate, "$\mathbf{U}_\lambda$", leaving the proof for the general Deutsch gate to the next sub-section. $\mathbf{U}_\lambda$ denotes the S-matrix

$$\mathbf{U}_\lambda = \begin{pmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && 1 &&&&& \\ &&& 1 &&&& \\ &&&& 1 &&& \\ &&&&& 1 && \\ &&&&&& \cos\lambda & i\sin\lambda \\ &&&&&& i\sin\lambda & \cos\lambda \end{pmatrix}, \tag{3.4}$$

where now we have exhibited the S-matrix as an 8×8 unitary matrix; we take the basis to be the "computational basis" labelled 0 through 7, identified with the three-bit states $0 = |0,0,0>$, $1 = |0,0,1>$, ..., $7 = |1,1,1>$. The labeling of the three bits is indicated in Fig. 2. The action of $\mathbf{U}_\lambda$ may be expressed in words as follows: "Perform a rotation of the quantum state by angle λ in the plane in Hilbert space defined by the state vectors $|1,1,0>$ and $|1,1,1>$ (states 6 and 7). Leave all other components of the state, those for which either the first of the second bit is a zero, unchanged." $\mathbf{U}_\lambda$ is obtained by four applications of $\mathbf{S_Q}$ in Eq. (3.1), with the identification $\lambda = -2\pi\alpha$.

In Fig. 2 I introduce new gates $\mathbf{X}$ and $\mathbf{V}$, which operate only on pairs of bits at a time. In a two-bit basis they have the S-matrices

$$\mathbf{X}^{(2)} = \begin{pmatrix} e^{i\phi} &&& \\ & 1 && \\ && 1 & \\ &&& 1 \end{pmatrix}, \mathbf{V}^{(2)} = \begin{pmatrix} 1 &&& \\ & 1 && \\ && \cos\phi & \sin\phi \\ && -\sin\phi & \cos\phi \end{pmatrix}. \tag{3.5}$$

The S-matrices of these gates operating in the basis of all three bits is a direct product, e.g., $\mathbf{V}^{(2)} \otimes \mathbb{1}$, and so is a block-diagonal 8×8 matrix, although with an ordering of rows and columns which is determined by which pair of bits $\mathbf{V}$ operates upon. For example, when $\mathbf{V}$ operates on bits 1 and 3 as in Fig. 2, the full S-matrix is

$$\mathbf{V_{13}} = \begin{pmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && 1 &&&&& \\ &&& 1 &&&& \\ &&&& \cos\phi & \sin\phi && \\ &&&& -\sin\phi & \cos\phi && \\ &&&&&& \cos\phi & \sin\phi \\ &&&&&& -\sin\phi & \cos\phi \end{pmatrix}, \tag{3.6}$$

and similarly for $\mathbf{X_{23}}$. The operator $\mathbf{N}$ is simply the classical "NOT", i.e., Eq.(3.2) with $\alpha = 1$. Now, it is a straightforward algebraic exercise, involving the multiplication of a succession of 8×8 matrices, to show that the equation of Fig. 2 is true, (or, in mathematical symbols,

$$\mathbf{U}_\lambda(\lambda = \delta) \simeq \mathbf{N_2 V_{13}}(\phi = \sqrt{\delta})\mathbf{X_{23}}(\phi = -\sqrt{\delta})\mathbf{V_{13}}(\phi = -\sqrt{\delta})\mathbf{X_{23}}(\phi = \sqrt{\delta})\mathbf{N_2}\ ), \tag{3.7}$$

to first order in the small parameter δ. To obtain $\mathbf{U}_\lambda$ for any λ to a desired degree of accuracy, it is only necessary to concatenate a set of small rotations, by writing $\mathbf{U}_\lambda = (\mathbf{U}_{\lambda/N})^N$; the error made by using the set of two-bit operations in Eq. (3.7) can be shown to be of order $1/\sqrt{N}$.

C. Completion of the proof: generating the entire Lie algebra

The foregoing does not quite complete the proof of the universality of two-bit gates, because I have only shown that one particular three-bit gate ($\mathbf{U}_\lambda$) is obtainable; Deutsch uses three others (which he called $\mathbf{V}_\lambda$, $\mathbf{W}_\lambda$ and $\mathbf{X}_\lambda$) to generate an arbitrary quantum network. Rather than continue on in the same pedestrian fashion for these other three cases (which gets a bit more involved), I will show that the above results, and the other ones which are required, may be obtained very compactly within the language of Lie groups [25].

Expressed in group-theoretic language, all the computational gates discussed above are elements of the Lie group $U(2^3)$, and the question of universality is the same as the question of whether the set of transformations I have defined suffice to *generate* $U(2^3)$. Deutsch has already demonstrated that the set of $U(2^3)$ elements $\mathbf{U}_\lambda$—$\mathbf{X}_\lambda$ in turn suffice to generate the group $U(2^k)$ for an arbitrary number of bits k.

The standard concept from Lie-group theory of *infinitesimal generators* fits hand-in-glove with the construction of unitary logical gates. The infinitesimal generators $\mathbf{H}$ of the Lie group are defined by

$$\delta\mathbf{U} = \mathbb{1} + i\epsilon\mathbf{H}. \tag{3.8}$$

In our problem $\delta\mathbf{U}$ are 8×8 unitary matrices differing infinitesimally from the identity, ϵ is an arbitrarily small number, and $\mathbf{H}$, the generators, are 8×8 Hermitian matrices. There are 64 distinct 8×8 Hermitian matrices; for later reference I write out here a convenient set of them $\mathbf{H}_{\alpha\alpha}$, $\mathbf{H}^r_{\alpha\beta}$ and $\mathbf{H}^i_{\alpha\beta}$ $(0\leq\alpha<\beta\leq 7)$; their matrix elements are

$$(\mathbf{H}_{\alpha\alpha})_{ij}=\delta_{i\alpha}\delta_{j\alpha}, \tag{3.9a}$$

$$(\mathbf{H}^r_{\alpha\beta})_{ij}=\delta_{i\alpha}\delta_{j\beta}+\delta_{i\beta}\delta_{j\alpha}, \tag{3.9b}$$

$$(\mathbf{H}^i_{\alpha\beta})_{ij}=-i\delta_{i\alpha}\delta_{j\beta}+i\delta_{i\beta}\delta_{j\alpha}. \tag{3.9c}$$

A key theorem of Lie-group theory is that, if $\mathbf{H}_1$ and $\mathbf{H}_2$ are generators of the group, then other generators may be obtained by *commutation*, producing the *Lie algebra*:

$$\mathbf{H}_3=i[\mathbf{H}_1,\mathbf{H}_2]. \tag{3.10}$$

Moreover, one can write down an explicit expression for how the unitary operation $\exp(i\epsilon\mathbf{H}_3)$ is obtained from $\exp(i\epsilon\mathbf{H}_1)$ and $\exp(i\epsilon\mathbf{H}_2)$:

$$e^{i\delta(i[\mathbf{H}_1,\mathbf{H}_2])}\simeq e^{i\sqrt{\delta}\mathbf{H}_2}e^{-i\sqrt{\delta}\mathbf{H}_1}e^{-i\sqrt{\delta}\mathbf{H}_2}e^{i\sqrt{\delta}\mathbf{H}_1}, \tag{3.11}$$

this valid for small parameter δ. Thus we see that the sequence of gates illustrated in Fig. 2 and in Eq. (3.7) is nothing more than the execution of a commutator of the Lie algebra.

With this machinery, the question of whether two-bit gates suffice to produce all possible three-bit unitary operations boils down to the question of whether the successive commutation of the Hermitian generators of our set of two-bit gates fills out the entire 64-dimensional Lie algebra spanned by Eqs. (3.9). Actually the exercise is simpler than this, because as Deutsch showed, obtaining the generators corresponding to just four unitary operators $\mathbf{U}_\lambda$, $\mathbf{V}_\lambda$, $\mathbf{W}_\lambda$ and $\mathbf{X}_\lambda$ suffices to produce all of $U(8)$. The four corresponding Hermitian generators are $\mathbf{H}_{66}$, $\mathbf{H}_{77}$, $\mathbf{H}^r_{67}$ and $\mathbf{H}^i_{67}$. So, I forthwith show the explicit commutator expressions for these four generators, keeping in mind that I am also allowed to introduce the one-bit "NOT" operation, in addition to the two-bit operations:

$$\mathbf{H}^r_{67} = \mathbf{N}_2(i[\mathbf{H}_{\mathbf{X_{23}}}, \mathbf{H}_{\mathbf{V_{13}}}])\mathbf{N}_2, \tag{3.12a}$$

$$\mathbf{H}^i_{67} = \mathbf{N}_2(i[\mathbf{H}_{\mathbf{X_{23}}}, \mathbf{H}_{\mathbf{U_{13}}}])\mathbf{N}_2, \tag{3.12b}$$

$$\mathbf{H}_{66} = \mathbf{N}_2(-\frac{i}{4}[[\mathbf{H}_{\mathbf{X_{23}}}, \mathbf{H}_{\mathbf{V_{13}}}], [\mathbf{H}_{\mathbf{X_{23}}}, \mathbf{H}_{\mathbf{U_{13}}}]] + \frac{1}{2}\mathbf{N}_1\mathbf{H}_{\mathbf{X_{12}}}\mathbf{N}_1)\mathbf{N}_2, \tag{3.12c}$$

$$\mathbf{H}_{77} = \mathbf{N}_2(\frac{i}{4}[[\mathbf{H}_{\mathbf{X_{23}}}, \mathbf{H}_{\mathbf{V_{13}}}], [\mathbf{H}_{\mathbf{X_{23}}}, \mathbf{H}_{\mathbf{U_{13}}}]] + \frac{1}{2}\mathbf{N}_1\mathbf{H}_{\mathbf{X_{12}}}\mathbf{N}_1)\mathbf{N}_2. \tag{3.12d}$$

Here $\mathbf{U_{13}}$ is a two-bit gate not previously introduced; it is similar to $\mathbf{V_{13}}$, having the two-bit S-matrix (cf. Eq. (3.5)):

$$\mathbf{U}^{(2)} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \cos\phi & i\sin\phi \\ & & i\sin\phi & \cos\phi \end{pmatrix}. \tag{3.13}$$

The Hermitian matrices $\mathbf{H}_{\mathbf{V_{13}}}$, etc. are the generators corresponding to the designated two-bit operations, which may be obtained from a Taylor-series expansion of the corresponding 8×8 S-matrices (e.g., Eq. (3.6)).

Eqs. (3.12) complete the proof that all necessary three-bit operations can be executed using two-bit gates; the explicit sequence of gates can be read off the equations. This is not to say that they provide a very practical implementation of quantum logic. For one thing, Eqs. (3.12) only provide a way of getting unitary operations with small rotation angles. Secondly, these equations specify a rather lengthy sequence of two-bit gates, especially Eqs. (3.12c) and (3.12d), for which the analog of Fig. 2 would contain a sequence of 21 gates! Clearly it would be worthwhile to seek for more efficient techniques for implementing some quantum computations of interest, such as the Fourier transform of Shor.

IV. CONCLUSIONS

It appears that very rapid progress is now being made on the fundamentals of quantum computing. It is well to keep in mind, though, that many basic issues of the realization of quantum computers remain unsolved or very difficult. The physical difficulties go well beyond the necessity for long phase-coherence times emphasized in Sec. II A. As Landauer has discussed [26], quantum computers suffer from instabilities in their time evolution which are inherent to any Hamiltonian system; in addition quantum computers cannot be error-corrected in any traditional sense, since error correction is intrinsically dissipative. Considerable ingenuity will be needed if these obstacles are to be overcome; the quantum factoring algorithm of Shor shows that there is considerable value in overcoming these obstacles.

Another cautionary note, though, has been sounded by the computer scientists. There is evidence that quantum computers, while undoubtedly more powerful than classical computers, may not be able to solve efficiently all the famous hard problems known to computational theorists. For example, there is evidence that quantum computers cannot solve the NP class of problems [27] any more rapidly than classical computers, although the method of proof used, employing a so called "random oracle", is known not to be definitive. Indeed, quantum mechanics has clearly created a whole new challenging and interesting area of investigation for computational complexity theorists. The main definite result for the time being is Shor's factoring algorithm, which gives the hope that closely related problems such as graph isomorphisms [28] might also have a rapid solution.

The present work shows that all quantum logic can in principle be designed with two-bit gates; however, it does not offer any practical design principles for quantum logic, and this remains an important open issue for the future. For the specific case of the Shor algorithm, Coppersmith [6] has very cleverly shown how both the essentially quantum-mechanical parts of his algorithm, and the "conventional" reversible part, may be very efficiently designed in two-bit gates.

I wish to close by pointing out the path for new physics experiments which is suggested by the gearbox quantum computer. The present proposal envisions a very ambitious program in which perhaps thousands of quantum-mechanical operations are carried out to execute a quantum algorithm; but even the execution of a few of the unitary operations of Eq. (2.1) would constitute new and interesting physics. For example, with just one such operation a so-called "Einstein-Podolsky-Rosen" pair [29] can be formed. By spatially separating this pair and performing single-spin measurements on the two, one would observe the space-like non-locality unique to quantum mechanics, and learn crucial information about dephasing times for pairs of spins. Other unique quantum phenomena like "teleportation" [30] could also be investigated. Such investigations could well be as exciting as the creation of the quantum computer itself, and they certainly lie along the path to it.

ACKNOWLEDGMENTS

I am grateful to my colleagues N. Amer, C. H. Bennett, D. Coppersmith, N. Gershenfeld, A. D. Kent, R. Landauer and S. Lloyd for many helpful discussions about this work. Thanks particularly to D. Coppersmith for supplying a crucial piece of help in establishing the sufficiency of two-bit gates, and for some useful references.

REFERENCES

[1] See, e.g., P. Benioff, "Quantum mechanical Hamiltonian models of Turing machines", J. Stat. Phys. **29**, 515 (1982). Ref. [26] has a complete set of references.

[2] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation", Proc. Roy. Soc. Lond. A **439**, 554 (1992).

[3] E. Bernstein and U. Vazirani, "Quantum complexity theory", Proceedings of the 25th Annual ACM Symposium on the Theory of Computing, 1993, p. 11.

[4] P. W. Shor, "Algorithms for quantum computation: discrete log and factoring", Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, 1994 (to be published).

[5] D. R. Simon, "On the power of quantum computation", Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, 1994 (to be published).

[6] D. Coppersmith, "An approximate Fourier transform useful in quantum factoring", preprint (1994); and unpublished.

[7] See, e.g., S. Washburn and R. A. Webb, "Aharonov-Bohm effect in normal metal quantum coherence and transport", Adv. Phys. **35**, 375 (1986).

[8] Using the electron spin as a computational degree of freedom has been discussed by S. Bandyopadhyay, B. Das, and A. E. Miller, "Supercomputing with spin-polarized single electrons in a quantum coupled architecture", submitted to Nanotechnology (1994). There are other, largely unexplored, possibilities of using natural Ising-spin systems for computation; see, e.g., W. P. Wolf, "Anisotropic interactions between magnetic ions", J. Phys. **32**, C1-26 (1970).

[9] R. W. Equall, Y. Sun, R. L. Cone, and R. M. Macfarlane, "Ultraslow optical dephasing in $Eu^{3+} : Y_2SiO_5$", Phys. Rev. Lett. **72**, 2179 (1994).

[10] C. S. Lent, P. D. Tougaw, W. Porod, and G. H. Bernstein, "Quantum cellular automata", Nanotechnology **4**, 49 (1993).

[11] D. M. Eigler, C. P. Lutz, and W. E. Rudge, "An atomic switch realized with the scanning tunneling microscope", Nature **352**, 600 (1991).

[12] This discussion indicated that hopefully, an ongoing goal of solid state and low temperature physics should be to find new quantum subsystems with long t_ϕ's.

[13] A. Abragham, *The Principles of Nuclear Magnetism*, (Oxford University Press, 1961), p. 265.

[14] See also discussion in S. Lloyd, "Programming pulse driven quantum computers", preprint (1994).

[15] S. Lloyd, "A potentially realizable quantum computer", Science, **261**, 1569 (1993); "Envisioning a quantum supercomputer", Science, **263**, 695 (1994).

[16] K. Obermayer, W. G. Teich and G. Mahler, "Structural basis of multistationary quantum systems. I. Effective single-particle dynamics", Phys. Rev. B **37**, 8096 (1988); W. G. Teich, K. Obermayer and G. Mahler, "Structural basis of multistationary quantum systems. II. Effective few-particle dynamics", Phys. Rev. B **37**, 8111 (1988).

[17] G. P. Berman, G. D. Doolen, D. D. Holm, and V. I. Tsifrinovich, "Quantum computer on a class of one-dimensional Ising systems", LANL preprint LA-UR-94-1404 (1994).

[18] J. W. Negele and H. Orland, *Quantum Many-Particle Systems*, (Addison-Wesley, 1988), Eq. (2.11).

[19] D. Rugar, C. S. Yannoni and J. A. Sidles, "Mechanical detection of magnetic resonance", Nature **360**, 563 (1992); O. Züger and D. Rugar, "First images from a magnetic resonance force microscope", Appl. Phys. Lett. **63**, 2496 (1993).

[20] C. P. Slichter, *Principles of Magnetic Resonance* (Third Edition, Springer-Verlag, 1992).

[21] D. Deutsch, "Quantum computational networks", Proc. Roy. Soc. Lond. A **425**, 73 (1989).

[22] T. Toffoli "Reversible Computing", in *Automata, Languages and Programming*, eds. J. W. de Bakker and J. van Leeuwen (Springer, New York, 1980), p. 632; Technical Memo MIT/LCS/TM-151, MIT Lab. for Comp. Sci. (unpublished).

[23] A. C.-C. Yao, "Quantum Circuit Complexity", Proceedings of the 34th IEEE Symposium on the Foundations of Computer Science, 1993, p. 352.

[24] In his calculation, Deutsch wishes the parameter α in Eq. (3.1) to take an irrational value, in order that all neighborhoods in the parameter space of rotations may eventually be visited by successive applications of $\mathbf{Q}$. I take a slightly different approach, which is to assume that α is an infinitesimal number. This permits me to connect my discussion more closely with the well-known and powerful results of Lie-algebra theory, which is directly applicable to my demonstration that two-bit gates are universal for quantum computation.

[25] See, e.g., J. Mathews and R. L. Walker, *Mathematical Methods of Physics*, (Benjamin, Second Edition, 1970), Chap. 16, and J. D. Talman, *Special Functions, A Group Theoretic Approach*, (Benjamin, 1968), Chaps. 3, 4.

[26] R. Landauer, "Is quantum mechanics useful?", Proc. Roy. Soc. Lond., (to be published).

[27] C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani, "Strengths and weaknesses of quantum computing", Proceedings of the 26th Annual ACM Symposium on the Theory of Computing, 1994 (to be published).

[28] P. Shor, private communication.

[29] See, e.g., A. Peres, *Quantum Theory: Concepts and Methods*, (Kluwer, 1993), Chap. 6.

[30] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Perez, and W. Wooters, "Teleport-

ing an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", Phys. Rev. Lett. **70**, 1895 (1993).

FIGURES

FIG. 1. The gearbox quantum computer. The two meshed gears operate classically, turning in synchrony. A single quantum spin-1/2 degree of freedom, discussed as a proton nuclear spin in the text, is firmly attached to the end of the tips of the left-hand gear, and to the base of the grooves of the right-hand gear. Other gears may be added for I/O, memory, etc. The teeth of the left-hand gear are shown in the shape of atomic-force microscope (AFM) tips, suggestive of the fact that atomic spatial resolution will be necessary in the meshing of the two gears, in order that the two spins may be brought into atomic contact. The gears are shown with 16 and 15 teeth respectively; by making these numbers relatively prime, it is assured that each pair of spins from the two separate gears may be brought into contact by turning the gearbox.

FIG. 2. Explicit demonstration of the equivalence of one of Deutsch's three-bit gates with a sequence of two-bit gates, for infinitesimal values of the rotation parameter δ. The S-matrices of gates $\mathbf{U}_\lambda$, $\mathbf{X}$ and $\mathbf{V}$ are described in Eqs. (3.4,3.5,3.6). The labeling of the three bits discussed in the text is indicated, including the primed notation for their output states. The sequence of two-bit gates shown amounts to the execution of a commutator of the generators of the $U(8)$ Lie algebra, as discussed in Sec. III C.

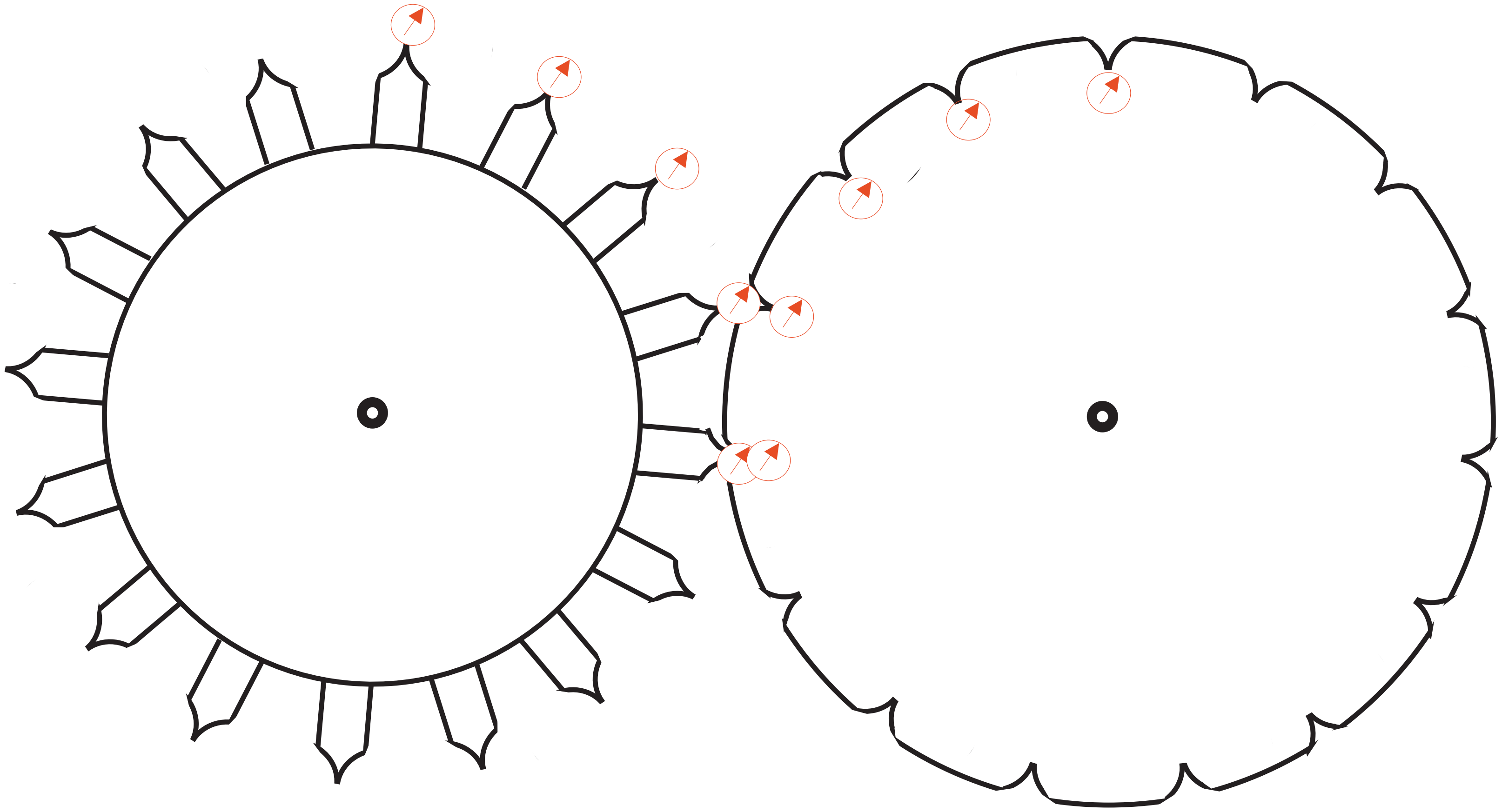

Fig. 1

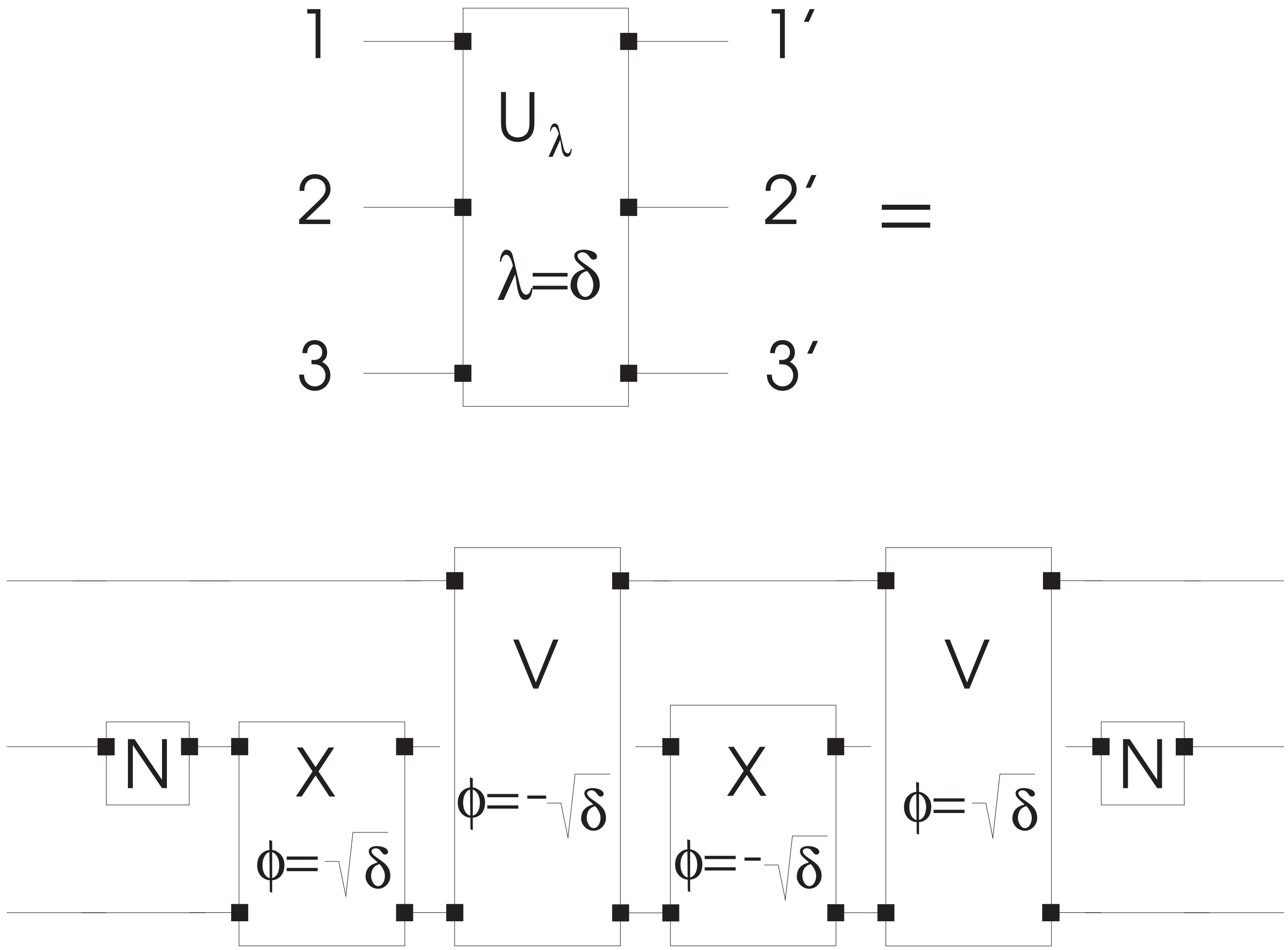
1
2
3
U_λ
$\lambda=\delta$
1′
2′
3′
=
N
X
$\phi=\sqrt{\delta}$
V
$\phi=-\sqrt{\delta}$
X
$\phi=-\sqrt{\delta}$
V
$\phi=\sqrt{\delta}$
N

Fig. 2