Quantum Computation

Stan Gudder

1. INTRODUCTION. Quantum computers may be the next revolution in the computer industry. Primitive quantum computers have already been constructed using laser, ion trap, or nuclear magnetic resonance technology. Grover's quantum search algorithm is quadratically faster than any possible search algorithm for a classical computer, and Shor's quantum factorization algorithm is exponentially faster than any known classical counterpart. These experimental and theoretical results indicate that quantum computers are feasible and will be incredibly faster than conventional computers. Moreover, since they operate at the atomic or nuclear scale, they will have immensely larger memory. The hardware and software of a quantum computer are based on the principles of quantum mechanics. For this reason, entirely new phenomena such as superpositions of states, entangled states, and quantum uncertainty come into play. As we shall see, these phenomena are important for the great power of quantum computers.

In a nutshell quantum computers gain speed because of the following effect. A conventional computer is limited to a computational space of n-bit strings of zeros and ones. The quantum counterpart is an n-qubit system described by a unit vector in a 2^n-dimensional vector space. Cleverly designed quantum algorithms can exploit this exponential explosion to perform very fast computations. Roughly speaking, a quantum computer operates on a massively parallel scale that can compute 2^n pieces of information simultaneously.

Although the field of quantum computation is only about ten years old, quite a few books and many research articles have been written on the subject. Unfortunately, the existing books either have limited mathematical content (e.g., [**2**], [**3**], [**6**], [**11**], or [**12**]) or they are written at an advanced level (e.g., [**4**], [**5**], [**7**], [**8**], or [**10**]). The first group make interesting and entertaining reading but do not contain enough detail to help one understand the subject in depth. While the books of the second group are well written, they require a level of sophistication that is difficult for newcomers to the field. In this article we try to tread an intermediate path. We do not present any new results but attempt to give an introduction to the subject that is simple and still conveys the essential ideas and principles. We assume only that the reader has some basic knowledge of linear algebra.

To keep this article at a reasonable length and level, there are many important aspects of the subject that are not addressed. For example, we consider only pure states and projective measurements and do not discuss the more general mixed states and measurements. More seriously, we do not consider computational complexity in detail and do not discuss error-correcting codes [**9**] or the physical construction of quantum computers. Our main intent is to illustrate how elementary linear algebra can be applied to the understanding and advancement of an exciting new field with great potential.

2. LINEAR ALGEBRA. This section reviews the elements of linear algebra that are needed in the sequel and introduces Dirac notation. Our main interest is the vector space $V = \mathbb{C}^n$, which is the space of all n-tuples of complex numbers. As usual, addition and scalar multiplication are defined coordinate-wise. When we write

$v = (z_1, \ldots, z_n)$ we do so to economize on printed space, but are actually thinking of v as an $n \times 1$ column vector with entries (or coordinates) $z_1, \ldots, z_n$. The zero vector is denoted by $\theta = (0, \ldots, 0)$. A *subspace* of V is a subset W of V that is also a vector space; that is, W is closed under addition and scalar multiplication.

We define the *inner product* $\langle v \mid w \rangle$ of two vectors $v = (z_1, \ldots, z_n)$ and $w = (y_1, \ldots, y_n)$ by $\langle v \mid w \rangle = \sum z_i^* y_i$, where z_i^* is the complex-conjugate of z_i. Notice that we are using the physicist's definition in which the first argument is conjugated instead of the second. The *norm* $\|v\|$ of a vector v is the nonnegative real number defined by $\|v\| = \sqrt{\langle v \mid v \rangle}$. We say that v is a *unit vector* if $\|v\| = 1$. Two vectors v and w are *orthogonal* (written $v \perp w$) if $\langle v \mid w \rangle = 0$, and a set of vectors v_i, $i = 1, \ldots, m$, is *orthonormal* if they are mutually orthogonal unit vectors. Thus $\{v_1, v_2, \ldots, v_m\}$ is an orthonormal set if $\langle v_i \mid v_j \rangle = \delta_{ij}$, where δ_{ij} is the Kronecker delta. An *orthonormal basis* for V is an orthonormal set containing n elements. In the sequel, whenever we speak of a basis for V we shall mean an orthonormal basis. If $v_1, \ldots, v_n$ is a basis, then any v in V has the unique representation $v = \sum \langle v_i \mid v \rangle v_i$. The *standard basis* for V is $v_1 = (1, 0, \ldots, 0)$, $v_2 = (0, 1, 0, \ldots, 0), \ldots, v_n = (0, \ldots, 0, 1)$. If $v = (z_1, \ldots, z_n)$, the *dual* of v is the row vector $v^\dagger = [z_1^* \cdots z_n^*]$. Notice that in terms of matrix multiplication $\langle v \mid w \rangle = v^\dagger w$.

An *operator* on V is a function $A: V \to V$ that satisfies $A(\sum a_i v_i) = \sum a_i A v_i$ for all complex numbers $a_1, \ldots, a_m$ and vectors $v_1, \ldots, v_m$ in V. If an operator is specified on a basis for V, then it is completely determined by linearity. Two examples of operators on V are the *identity operator* $Iv = v$ and the *zero operator* $0v = \theta$ for all v in V. If A and B are operators on V, their *composition* is the operator $BA: V \to V$ defined by $(BA)v = B(Av)$. If A is an operator on V and $\mathcal{B} = \{v_1, v_2 \ldots, v_n\}$ is a basis for V, then there exist unique complex numbers A_{ij} such that $Av_j = \sum A_{ij} v_i$ for $j = 1, \ldots, n$. The $n \times n$ matrix $[A_{ij}]$ is called the *matrix representation of A relative to the basis* $v_1, \ldots, v_n$ and is denoted by $[A]_{\mathcal{B}}$. Since matrices themselves are operators, this gives a correspondence between matrices and operators. We shall use these two viewpoints interchangeably. It is easy to show that matrix multiplication and operator composition are closely related in the sense that $[BA]_{\mathcal{B}} = [B]_{\mathcal{B}}[A]_{\mathcal{B}}$. Some important matrices in quantum mechanics are the *Pauli matrices*

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1}$$

and the *Hadamard matrix*

$$H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

If A is an operator on V, then there exists a unique operator $A^\dagger$ on V such that $\langle v \mid Aw \rangle = \langle A^\dagger v \mid w \rangle$ for all v and w in V. We call $A^\dagger$ the *adjoint* of A. In terms of matrix representation, we have $(A^\dagger)_{ij} = A_{ji}^*$. An operator U on V is *unitary* if $U^\dagger U = I$ (which implies that $UU^\dagger = I$ as well). The Pauli and Hadamard matrices are unitary. Since

$$\langle Uv \mid Uw \rangle = \langle v \mid U^\dagger U w \rangle = \langle v \mid w \rangle,$$

we see that unitary operators preserve both the inner product and the norm. An *eigenvector* of an operator A on V is a nonzero vector v such that $Av = \lambda v$ where λ is the complex number (the *eigenvalue* of A corresponding to v). It is easy to check that

the eigenvalues of a unitary operator have modulus 1. A *projection operator* P on V satisfies $P = P^\dagger = P^2$. We say that P is the *projection* onto its range, i.e., onto the subspace $W = \{v \in V : Pv = v\}$.

If $W = \mathbb{C}^m$ and $V = \mathbb{C}^n$, there is a natural mapping $T : W \times V \to \mathbb{C}^{mn}$ defined by

$$\begin{aligned} T((x_1, \ldots, x_m), (y_1, \ldots, y_n)) &= (x_1(y_1, \ldots, y_n), \ldots, x_m(y_1, \ldots, y_n)) \\ &= (x_1 y_1, \ldots, x_1 y_n, \ldots, x_m y_1, \ldots, x_m y_n). \end{aligned}$$

We use the notation $w \otimes v$ to symbolize $T(w, v)$ and call $w \otimes v$ the *tensor product* of w and v. The reader should check the following elementary properties of the tensor product:

(1) $a(w \otimes v) = (aw) \otimes v = w \otimes (av)$ for all a in $\mathbb{C}$;

(2) $(w_1 + w_2) \otimes v = w_1 \otimes v + w_2 \otimes v$;

(3) $w \otimes (v_1 + v_2) = w_1 \otimes v_1 + w \otimes v_2$;

(4) $\langle w_1 \otimes v_1 \mid w_2 \otimes v_2 \rangle = \langle w_1 \mid w_2 \rangle \langle v_1 \mid v_2 \rangle$.

We denote the pair $(C^{mn}, \otimes)$ by $W \otimes V$ and call $W \otimes V$ the *tensor product* of W and V. We can think of $W \otimes V$ as the vector space consisting of all finite formal sums $\sum a_{ij} w_i \otimes v_j$, where w_i and v_j are in W and V, respectively, and the operation $\otimes$ satisfies (1)–(4). It follows from (4) that if w_i, $i = 1, \ldots, m$, and v_j, $j = 1, \ldots, n$, are bases for W and V, respectively, then the set of vectors $w_i \otimes v_j$ forms a basis for $W \otimes V$. If A and B are operators on W and V, respectively, we define the operator $A \otimes B$ on $W \otimes V$ by

$$(A \otimes B)\left(\sum a_{ij} w_i \otimes v_j\right) = \sum a_{ij} A w_i \otimes B v_j.$$

We extend this definition to higher order tensor products $V_1 \otimes \cdots \otimes V_n$ in the natural way. In case $V_1 = \cdots = V_n = V$, we abbreviate $V \otimes \cdots \otimes V$ to $V^{\otimes n}$. We also use the notation $v^{\otimes n} = v \otimes \cdots \otimes v$ and $A^{\otimes n} = A \otimes \cdots \otimes A$.

We now introduce the physics Dirac notation for two reasons. First, this is the notation that is almost always employed in the quantum computation literature, and a reader who wants to study the subject further must be familiar with this notation. Second, Dirac notation provides a convenient and compact way of writing outer products and tensor products. In this notation, we denote a column vector in V by $|v\rangle$. Notice that the entire symbol $|v\rangle$ denotes the vector and that now the letter v serves as a label. Any convenient label is permissible in $|\cdot\rangle$. For example, $|x\rangle$, $|y\rangle$, $|1\rangle$, and $|2\rangle$ denote vectors, where x, y, 1, and 2 are not vectors but are labels for designating vectors. The dual row vector $|v\rangle^\dagger$ is then denoted by $\langle v|$. The relationship between our two notations is specified by $\langle v| \, |w\rangle = \langle v \mid w \rangle$. The left side of the previous equation is the matrix product of the row vector $\langle v|$ with the column vector $|w\rangle$, and the right side is shorthand for the inner product of the two vectors $|v\rangle$ and $|w\rangle$. If A is an operator on V, the Dirac notation for $\langle v \mid Aw \rangle$ is $\langle v|A|w\rangle$. The *outer product* of $|v\rangle$ and $|w\rangle$ is the operator $|v\rangle\langle w|$ on V defined by

$$(|v\rangle\langle w|)\,|v'\rangle = \langle w \mid v' \rangle |v\rangle.$$

More generally, we define the operator $\sum a_i |v_i\rangle\langle w_i|$ on V by

$$\left(\sum a_i |v_i\rangle\langle w_i|\right)|v'\rangle = \sum a_i \langle w_i \mid v' \rangle |v_i\rangle.$$

Let $|i\rangle$, $i = 1, \ldots, n$, be a basis for V. Since $(|i\rangle\langle i|)\,|v\rangle = \langle i \mid v\rangle|i\rangle$, we have that

$$\left(\sum |i\rangle\langle i|\right)|v\rangle = \sum \langle i \mid v\rangle|i\rangle = |v\rangle,$$

and this gives the *completeness equation* $\sum |i\rangle\langle i| = I$. Moreover, if A is an operator on V, then applying the completeness equation twice gives $A = \sum \langle i|A|j\rangle|i\rangle\langle j|$. This shows that any operator has an outer product representation and that the entries of the associated matrix for the basis $|i\rangle$ are $A_{ij} = \langle i|A|j\rangle$. It is not difficult to show that the projection onto a subspace W has the form $P = \sum_{j=1}^{k} |j\rangle\langle j|$, where the vectors $|j\rangle$ furnish a basis for W.

On the tensor product space $V_1 \otimes \cdots \otimes V_n$, instead of writing $|v_1\rangle \otimes \cdots \otimes |v_n\rangle$ we frequently use the notation $|v_1\rangle|v_2\rangle \cdots |v_n\rangle$ or $|v_1, v_2, \ldots, v_n\rangle$ or simply $|v_1 v_2 \cdots v_n\rangle$. Notice that

$$|v_1 v_2 \cdots v_n\rangle^{\dagger} = \langle v_1 v_2 \cdots v_n| = \langle v_1| \otimes \cdots \otimes \langle v_n|.$$

An important case for quantum computation occurs when $V_1 = \cdots = V_n = V = \mathbb{C}^2$, giving rise to the space $V^{\otimes n} = \mathbb{C}^{2^n}$. If $|0\rangle$ $(= (1, 0))$ and $|1\rangle$ $(= (0, 1))$ are Dirac notations for the standard basic vectors for $\mathbb{C}^2$, the *computational basis* for $V^{\otimes n}$ is

$$|0\cdots00\rangle, |0\cdots01\rangle, |0\cdots010\rangle, |0\cdots011\rangle, \ldots, |1\cdots11\rangle,$$

where each vector contains n bits and each bit is 0 or 1. We have written these vectors in binary order. If x is an integer satisfying $0 \le x \le 2^n - 1$ and if x is given in its binary representation, then $|x\rangle$ becomes an element of this basis. We can thus write the computational basis as $|x\rangle$ for $0 \le x \le 2^n - 1$. An important operator on $V^{\otimes n}$ is the *Hadamard transform* $H^{\otimes n}$. The Hadamard operator on $V = \mathbb{C}^2$ has outer product representation

$$H = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right) = \frac{1}{\sqrt{2}}\sum_{x,y}(-1)^{x\cdot y}|x\rangle\langle y|,$$

where x and y belong to $\{0, 1\}$ and $x \cdot y$ signifies ordinary multiplication. (In other words, it is the operator on $\mathbb{C}^2$ corresponding to the Hadamard matrix.) We then have

$$H^{\otimes 2} = \frac{1}{\sqrt{2^2}}\sum_{x,y,x',y'}(-1)^{x\cdot y + x'\cdot y'}\left|xx'\right\rangle\left\langle yy'\right| = \frac{1}{\sqrt{2^2}}\sum_{x'',y''}(-1)^{x''\cdot y''}\left|x''\right\rangle\left\langle y''\right|,$$

where now x'' and y'' lie in the binary set $\{00, 01, 10, 11\}$ and $x'' \cdot y''$ indicates the bitwise inner product modulo 2. For example,

$$\begin{aligned} 01 \cdot 11 &= 0 \cdot 1 + 1 \cdot 1 = 1, \\ 11 \cdot 11 &= 1 \cdot 1 + 1 \cdot 1 = 0 \pmod 2. \end{aligned}$$

Alternatively, we can express $H^{\otimes 2}$ in the manner

$$H^{\otimes 2} = \frac{1}{\sqrt{2^2}}\sum_{x,y}(-1)^{x\cdot y}|x\rangle\langle y|,$$

where $x, y = 0, 1, 2$, or 3, $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$ lists the standard basis of $\mathbb{C}^4$ in the "usual" order, and $x \cdot y$ is the bitwise inner product modulo 2 of the binary expansions of x

and y. Continuing this process we have

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|,$$

where $x, y = 0, 1, 2, \ldots, 2^n - 1$. Although Dirac notation is useful and compact, in certain situations it becomes awkward. In such situations, we revert to standard mathematical notation.

3. QUANTUM MECHANICS. Quantum mechanics is a theory that describes atomic and subatomic particles (quantum particles) and their interactions. Examples of quantum particles are electrons, protons, neutrons, and photons (particles of light). A physical system consisting of one or more quantum particles is called a *quantum system*. To completely describe a quantum particle requires an infinite-dimensional Hilbert space. For quantum computation purposes we shall need only a partial description given by a finite-dimensional inner product space. For example, if the spin of an electron is measured in a specific direction in ordinary three-dimensional space $\mathbb{R}^3$, one obtains just two possible outcomes called "spin up" and "spin down." If we are concerned only with the spin of a single electron, then the state (or condition) of the electron is represented by a unit vector in $\mathbb{C}^2$. For example, if the spin is measured in the z-direction, then the "spin up" state is given by $(1, 0)$ and the "spin down" state is given by $(0, 1)$. In this restricted partial description we say that the electron has a two-dimensional state space. A quantum system is called *finite-dimensional* if we are considering only a partial description in a finite-dimensional state space. The dimension of the state space depends on the quantum system being described. For example, a single electron has a two-dimensional state space and, as we shall see, a pair of electrons has a four-dimensional state space. In the sequel, when we speak of a quantum system we shall always mean a finite-dimensional quantum system. A quantum system is *isolated* if it does not interact with other physical systems.

Postulate 1. *Associated with an isolated quantum system is an inner product space $V = \mathbb{C}^n$ called the "state space" of the system. The system at any given time is described by a "state," which is a unit vector in V.*

The simplest quantum system has state space $V = \mathbb{C}^2$ and is called a *qubit*. If $|0\rangle$ and $|1\rangle$ form a basis for V, then an arbitrary qubit state has the form $|x\rangle = a|0\rangle + b|1\rangle$, where a and b in $\mathbb{C}$ have $|a|^2 + |b|^2 = 1$. Notice that we do not write $x = a|0\rangle + b|1\rangle$ because this would be inconsistent with Dirac notation. The states $|0\rangle$ and $|1\rangle$ are analogous to the bits 0 and 1. A qubit state differs from a bit because "superpositions" $|x\rangle = a|0\rangle + b|1\rangle$ are possible, and we cannot say that the system is definitely in the state $|0\rangle$ or definitely in the state $|1\rangle$. As we shall later show, all we can say is that the system is in state $|0\rangle$ with probability $|a|^2$ and in state $|1\rangle$ with probability $|b|^2$. In general, if $|\psi_i\rangle$ are given states, which need not be mutually orthogonal, we call a state of the form $\sum a_i|\psi_i\rangle$ a *superposition* of the states $|\psi_i\rangle$ with corresponding *amplitudes* a_i. For example, the qubit state $(|0\rangle - |1\rangle)/\sqrt{2}$ is a superposition of $|0\rangle$ and $|1\rangle$ with amplitudes $1/\sqrt{2}$ and $-1/\sqrt{2}$, respectively.

Postulate 2. *The evolution of an isolated quantum system is described by a unitary operator on its state space. That is, the state $|\psi(t_1)\rangle$ at time t_1 is related to the state $|\psi(t_2)\rangle$ at time t_2 by a unitary operator U_{t_1,t_2}, i.e., $|\psi(t_2)\rangle = U_{t_1,t_2}|\psi(t_1)\rangle$.*

The main reason that unitary operators are employed is that they preserve the norm and hence map states into states. Moreover, the superposition principle, which says that evolutions preserve superpositions, requires that U be linear. Of course, no physical system is really isolated except the universe as a whole. However, isolation can be achieved to good approximation. We may want to observe or make a measurement on a system to find out what is happening inside it. In this case the measurement apparatus interacts with the system, so the system is no longer isolated. We shall only consider measurements that have a finite number of possible outcomes, which we usually label by $m = 1, 2, \ldots, n$. One of the basic tenants of quantum mechanics states that the outcome of a measurement can only be predicted probabilistically.

Postulate 3. *Quantum measurements are described by a finite set $\{P_m\}$ of projections acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur. The projections satisfy the completeness equation $\sum P_m = I$. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by $p(m) = \langle\psi|P_m|\psi\rangle$; if the result m occurs, then the state of the system immediately after the measurement is*

$$\frac{P_m|\psi\rangle}{\langle\psi|P_m|\psi\rangle^{1/2}} = \frac{P_m|\psi\rangle}{\sqrt{p(m)}}.$$

The completeness equation ensures that probabilities sum to one:

$$\sum_m p(m) = \sum_m \langle\psi|P_m|\psi\rangle = \langle\psi|\sum P_m|\psi\rangle = \langle\psi \mid \psi\rangle = 1.$$

As an example, consider a qubit with basis states $|0\rangle$ and $|1\rangle$. Let $\{P_0, P_1\}$ be the measurement in which $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$. Suppose the state being measured is $|\psi\rangle = a|0\rangle + b|1\rangle$. Then the probability of obtaining outcome 0 (or the probability of state $|0\rangle$) is

$$p(0) = \langle\psi|P_0|\psi\rangle = |\langle 0 \mid \psi\rangle|^2 = |a|^2$$

and similarly $p(1) = |b|^2$. The states after measurement in the two cases become $|a|^{-1} P_0|\psi\rangle = a\,|a|^{-1}|0\rangle$ and $|b|^{-1} P_1|\psi\rangle = b\,|b|^{-1}|1\rangle$, respectively. As we shall see, multipliers like $a/|a|$ that have modulus 1 can effectively be ignored, so the two post-measurement states are $|0\rangle$ and $|1\rangle$. We call $\{P_0, P_1\}$ a *measurement in the computational basis*.

If ϕ is a real number, we say that state $e^{i\phi}|\psi\rangle$ is equal to state $|\psi\rangle$ up to a *phase factor* $e^{i\phi}$. Two such states give the same measurement statistics, so we consider them to be physically identical. Indeed, if $\{P_m\}$ is a measurement, then the probability that outcome m occurs is

$$\left\langle e^{i\phi}\psi \middle| P_m \middle| e^{i\phi}\psi \right\rangle = e^{-i\phi}e^{i\phi}\langle\psi|P_m|\psi\rangle = \langle\psi|P_m|\psi\rangle.$$

If we combine several quantum systems, the total system is called a *composite* quantum system and the individual quantum systems that are combined are called *components*.

Postulate 4. *The state space of a composite quantum system is the tensor product of the state spaces of its components. If systems numbered 1 through n are prepared in states $|\psi_i\rangle$, $i = 1, \ldots, n$, then the joint state of the composite total system is $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.*

Suppose a composite system consists of n qubits, each with computational basis $|0\rangle$ and $|1\rangle$. The composite system is called an *n-qubit* and has computational basis $|i_1 \cdots i_n\rangle$ with i_j in $\{0, 1\}$, or written another way, $|x\rangle$ for $x = 0, 1, \ldots, 2^n - 1$. When we speak of making a measurement in the computational basis for an n-qubit, we mean the measurement given by the set of projections $\{P_x : x = 0, 1, \ldots, 2^n - 1\}$, where $P_x = |x\rangle\langle x|$.

A state $|\psi\rangle$ in the state space $V^{\otimes n}$ is called a *product state* if it has the form $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$. If a state cannot be written as a product state, it is said to be *entangled*. For example, the 2-qubit state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is entangled. Indeed, suppose $|00\rangle + |11\rangle = |a\rangle \otimes |b\rangle$ for some $|a\rangle$ and $|b\rangle$. Taking inner products with $|00\rangle$, $|11\rangle$, and $|01\rangle$ and applying property (4) of tensor products gives $\langle 0 \mid a\rangle\langle 0 \mid b\rangle = 1$, $\langle 1 \mid a\rangle\langle 1 \mid b\rangle = 1$, and $\langle 0 \mid a\rangle\langle 1 \mid b\rangle = 0$, respectively. Since neither $\langle 0 \mid a\rangle$ nor $\langle 1 \mid b\rangle$ is 0, this gives a contradiction.

Suppose that a 2-qubit is in the state

$$|\psi\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle,$$

where $\sum |a_i|^2 = 1$. What does it mean to measure the first qubit in the computational basis? Remember that a qubit is a 2-dimensional quantum system (say a photon) and a 2-qubit is a composite of two qubits (say two photons). When we measure the first qubit in the composite system, the measuring apparatus interacts with the first qubit and leaves the second qubit undisturbed. Thus, we apply the measurement $\{P_0, P_1\}$, in which $P_0 = |0\rangle\langle 0| \otimes I$ and $P_1 = |1\rangle\langle 1| \otimes I$. We obtain the result 0 with probability

$$p_1(0) = \langle\psi|P_0|\psi\rangle = \langle\psi|a_0|00\rangle + \langle\psi|a_1|01\rangle = |a_0|^2 + |a_1|^2,$$

leading to the post-measurement state

$$\left|\psi_1^0\right\rangle = \frac{P_0|\psi\rangle}{\sqrt{p_1(0)}} = \frac{a_0|00\rangle + a_1|01\rangle}{\sqrt{|a_0|^2 + |a_1|^2}}.$$

Similarly, we obtain the result 1 with probability

$$p_1(1) = \langle\psi|P_1|\psi\rangle = |a_2|^2 + |a_3|^2,$$

resulting in the post-measurement state

$$\left|\psi_1^1\right\rangle = \frac{P_1|\psi\rangle}{\sqrt{p_1(1)}} = \frac{a_2|10\rangle + a_3|11\rangle}{\sqrt{|a_2|^2 + |a_3|^2}}.$$

In the same way, if we measure the second qubit we obtain

$$p_2(0) = |a_0|^2 + |a_2|^2, \qquad \left|\psi_2^0\right\rangle = \frac{a_0|00\rangle + a_2|10\rangle}{\sqrt{|a_0|^2 + |a_2|^2}},$$

$$p_2(1) = |a_1|^2 + |a_3|^2, \qquad \left|\psi_2^1\right\rangle = \frac{a_1|01\rangle + a_3|11\rangle}{\sqrt{|a_1|^2 + |a_3|^2}}.$$

In particular, if the 2-qubit is in the entangled state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, then

$$p_1(0) = p_1(1) = p_2(0) = p_2(1) = \frac{1}{2}$$

and

$$\left|\psi_1^0\right\rangle = \left|\psi_2^0\right\rangle = |00\rangle, \quad \left|\psi_1^1\right\rangle = \left|\psi_2^1\right\rangle = |11\rangle.$$

Thus, a measurement of the second qubit always gives the same result as a measurement of the first qubit even if the two qubits are far apart and cannot communicate in the time between the two measurements. We then say that the two measurements are *perfectly correlated*.

4. QUANTUM CIRCUITS. Classical computer circuits consist of wires and logic gates. The wires are used to carry information in the form of current around the circuit, while the logic gates convert the information from one form into another. The computer has an internal clock that marks time at equal time steps. At each time step, the state (or internal configuration) of the computer is transformed by a logic gate into another state according to a program prescription. The operation of a classical computer can be described by a set of logic gates that act sequentially on the state, together with input and output data. At the end of the program, the output data is observed and the computation is completed.

A quantum computer acts in a similar way, except now the wires represent the state evolution of a quantum system and the logic gates are replaced by quantum gates that, in accordance with Postulate 2, are described by unitary operators on the state space. A finite sequence of unitary operators called *quantum gates* acting on the state space of an n-qubit is said to be a *quantum circuit*. In order to observe output data we also allow a quantum circuit to contain measurements that are usually placed at the end of the sequence. We define a *quantum computer* to be a quantum circuit that can be used to perform a computation. Quantum gates for single qubits are easily constructed in the laboratory, and more complex quantum gates are usually implemented by tensor products of these simple gates. All the quantum gates that we shall present can be efficiently constructed. The efficient construction of more complex quantum gates has been studied (for example, in [**1**]) but will not be considered here.

Can a quantum computer perform any computation that a classical computer can perform? It can be shown that the answer is yes. The main problem in answering this question is that a logic gate may be irreversible (not one-to-one), whereas quantum gates are reversible because they are given by unitary operators. For example, the classical AND-gate transforms the 2-bits 00, 01, 10, and 11 to the 1-bits 0, 0, 0, and 1, respectively. Denoting the Cartesian product $\{0, 1\} \times \{0, 1\}$ by $\{0, 1\}^2$, the AND-gate is described by the function $f: \{0, 1\}^2 \to \{0, 1\}$ given by $f(x, y) = xy$, which is not one-to-one. The reason the AND-gate is described by the function f is that the truth table for the AND-gate is identical to the table of values for f.

x	y	x AND y	$f(x, y)$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

However, there are universal logic gates such as the Toffoli gate that are reversible. That is, any logic gate can be simulated by a finite number of Toffoli gates. The *Toffoli gate* is described by the function $g: \{0, 1\}^3 \to \{0, 1\}^3$ given by $g(x, y, z) = (x, y, z \oplus xy)$, where $\oplus$ signifies addition modulo 2. Notice that $g \circ g$ is the identity mapping. Hence, g is its own inverse, so g is one-to-one. It turns out that there is a quantum

gate that simulates a classical Toffoli gate, thus ensuring that quantum computers are at least as powerful as classical computers.

As an indication that quantum computers are actually more powerful than classical computers, we point out that no classical computer can generate bits that are truly random. For a quantum computer, on the other hand, just start by preparing a qubit in the state $|0\rangle$, send it through a Hadamard gate H to produce $(|0\rangle + |1\rangle)/\sqrt{2}$, and then measure the state in the computational basis. The result will be $|0\rangle$ or $|1\rangle$, each with probability exactly $1/2$. As another indication, there is only one nontrivial logic gate for a 1-bit system. This is the NOT-gate that transforms 0 to 1 and 1 to 0, which is called a *bit flip*. By contrast, there are infinitely many unitary operators and hence infinitely many quantum gates for a 1-qubit system.

We now briefly discuss some quantum gates. Since the Pauli matrix X satisfies $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$, we call X the *quantum* NOT-*gate*. An important 2-qubit gate is the *controlled*-NOT or CNOT-*gate*. This gate has two input qubits, known as the *control qubit* and the *target qubit*. If the control qubit is $|0\rangle$, the target qubit is left alone. If the control qubit is $|1\rangle$, the target qubit is flipped. This can be summarized as $|x\rangle|y\rangle \to |x\rangle|x \oplus y\rangle$, where x and y belong to $\{0, 1\}$. The unitary matrix for the CNOT-gate is

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

When a quantum gate has multiple wires entering it (and leaving it), each wire represents a qubit state and the combined wires represent the tensor product of the individual wires. The CNOT-gate is illustrated in Figure 1.

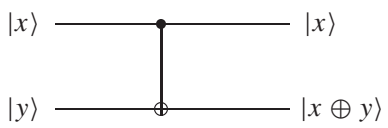

Figure 1. CNOT-gate.

If U is a unitary operator acting on an n-qubit state space, the *controlled-U-gate* acts on an $(n + 1)$-qubit state space and is a natural extension of a CNOT-gate. Such a gate has a single control qubit and n target qubits. If the control qubit state is $|0\rangle$, then nothing happens to the target qubits. If the control qubit state is $|1\rangle$, then U is applied to the target qubit states. If we let $U = X$, then the controlled-U-gate is just a CNOT-gate. The controlled-U-gate is illustrated in Figure 2, where $\not{\;}^{n}$ indicates that there are n wires.

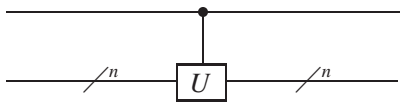

Figure 2. Controlled-U-gate.

Besides quantum gates, the other important component of a quantum circuit is a measurement device represented by M, as in Figure 3. This device performs the operation of converting a qubit state $|\psi\rangle = a|0\rangle + b|1\rangle$ into a probabilistic classical bit x (written as a double-line wire) that is 0 with probability $|a|^2$ and 1 with probability $|b|^2$. In general, a measurement with n possible outcomes has n wires leaving it.

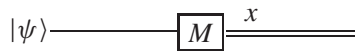

Figure 3. Measurement.

Figure 4 depicts a useful quantum circuit. This circuit diagram tells us that $H \otimes I$ is applied to $|x\rangle|y\rangle$ and then the CNOT-gate is applied to the result. Letting x and y belong to $\{0, 1\}$, we have

$$|00\rangle \to \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \to \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle,$$
$$|01\rangle \to \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \to \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\beta_{01}\rangle,$$
$$|10\rangle \to \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \to \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\beta_{10}\rangle,$$
$$|11\rangle \to \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \to \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\beta_{11}\rangle.$$

The entangled states $|\beta_{xy}\rangle$ are called *Bell states*. We can write

$$|\beta_{xy}\rangle = \frac{|0y\rangle + (-1)^x|1\overline{y}\rangle}{\sqrt{2}},$$

where $\overline{y}$ is the negation $1 - y$ of y. This simple quantum circuit shows that Bell states can easily be prepared in the laboratory.

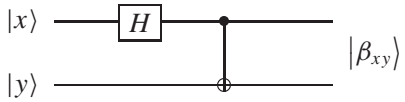

Figure 4. Bell state generator.

The unitary matrix for the quantum circuit in Figure 4 is given by:

$$U_{CN}(H \otimes I) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$
$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}.$$

We now illustrate the difficulty in copying an unknown quantum state. To be precise, given an unknown quantum state $|\psi\rangle$ we would like to reproduce $|\psi\rangle$ together with an exact copy of $|\psi\rangle$. A classical CNOT-logic-gate, which is the same as in Figure 1 with the vector brackets deleted, can be used to copy an unknown bit x. Just let x be the control bit, and let 0 be the target bit to obtain $x0 \to xx$. That is, the input to the gate is the pair of bits $x, 0$ and the output is the pair of bits x, x. We have thus reproduced x and a copy of x. Let us try to copy a qubit in the unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ in the same way using a quantum CNOT-gate. The input state is

$$(a|0\rangle + b|1\rangle)\,|0\rangle = a|00\rangle + b|10\rangle,$$

and the output state becomes $a|00\rangle + b|11\rangle$. If we had copied $|\psi\rangle$, we would have the output state $|\psi\rangle|\psi\rangle$. But

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle.$$

These two output states are not the same unless $ab = 0$. Thus, we can copy an unknown state by this method only if it is $|0\rangle$ or $|1\rangle$. We now show that no method will work, a state of affairs described as the "no-cloning theorem."

Suppose we have a quantum copying machine (quantum circuit) that copies unknown states $|\psi\rangle$ and starts out in some standard state $|s\rangle$. The initial state is $|\psi\rangle|s\rangle$ and some unitary evolution implements the copy procedure: $U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$. Suppose this machine works for two particular states $|\psi\rangle$ and $|\phi\rangle$. Then $U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$ and $U(|\phi\rangle|s\rangle) = |\phi\rangle|\phi\rangle$. Taking inner products of both sides gives $\langle\psi \mid \phi\rangle = \langle\psi \mid \phi\rangle^2$. Hence $\langle\psi \mid \phi\rangle = 0$ or 1, so either $|\psi\rangle = |\phi\rangle$ or $|\psi\rangle \perp |\phi\rangle$. Thus, if the machine copies $|\psi\rangle$, then it cannot copy a state that is not orthogonal to $|\psi\rangle$. We conclude that it is highly unlikely that the machine will copy an arbitrary unknown state $|\phi\rangle$.

5. SUPERDENSE CODING AND TELEPORTATION. We begin with the problem of distinguishing quantum states. Like many ideas in this subject, distinguishability is most easily understood using the metaphor of a game involving two parties, say Alice and Bob. Alice chooses a state $|\psi_j\rangle$ from some fixed set of states $|\psi_i\rangle$, $1 \le i \le n$, known to both parties. She gives $|\psi_j\rangle$ to Bob, whose task is to identify the index j. If the states are mutually orthogonal, Bob can distinguish the states with the measurement $\{P_i : i = 0, 1, \ldots, n\}$, where $P_i = |\psi_i\rangle\langle\psi_i|$ for $i = 1, \ldots, n$, and $P_0 = I - \sum_{i=1}^{n} P_i$. In this case, $p(j) = \langle\psi_j|P_j|\psi_j\rangle = 1$ and $p(i) = \langle\psi_j|P_i|\psi_j\rangle = 0$ for $i \ne j$, so the outcome j occurs with certainty and he identifies the state as $|\psi_j\rangle$ reliably. Bob is thus able to distinguish the orthogonal states $|\psi_i\rangle$. The next result shows that this cannot be done for nonorthogonal states. Thus if you have one of the two nonorthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, then no measurement will allow you to tell with certainty which state you have.

Theorem 1. *No measurement can reliably distinguish two nonorthogonal states* $|\psi_1\rangle$ *and* $|\psi_2\rangle$.

Proof. Suppose that a measurement $\{P_i : i = 1, 2, \ldots, n\}$ can reliably distinguish $|\psi_1\rangle$ and $|\psi_2\rangle$. If the measurement has outcome j, then it must be possible to decide whether the state is $|\psi_1\rangle$ or $|\psi_2\rangle$. Thus, there exists a function $f : \{1, \ldots, n\} \to \{1, 2\}$ such that $f(j) = 1$ if the state is $|\psi_1\rangle$ and $f(j) = 2$ if the state is $|\psi_2\rangle$. Define $Q_i = \sum \{P_j : f(j) = i\}$ for $i = 1, 2$. Because of reliability, we have $\langle\psi_1|Q_1|\psi_1\rangle = \langle\psi_2|Q_2|\psi_2\rangle = 1$. Since $Q_1 + Q_2 = I$, we also have

$$\langle\psi_1|Q_1|\psi_1\rangle + \langle\psi_1|Q_2|\psi_1\rangle = \langle\psi_1|I|\psi_1\rangle = \langle\psi_1 \mid \psi_1\rangle = 1.$$

Hence $\langle Q_2\psi_1 \mid Q_2\psi_1\rangle = \langle\psi_1|Q_2|\psi_1\rangle = 0$, implying that $Q_2|\psi_1\rangle = \theta$. Now we can write $|\psi_2\rangle = a|\psi_1\rangle + b|\phi\rangle$, where $\|\phi\| = 1$, $|\phi\rangle \perp |\psi_1\rangle$, $|a|^2 + |b|^2 = 1$, and (because $|\psi_1\rangle \not\perp |\psi_2\rangle$) $|b| < 1$. Then $Q_2|\psi_2\rangle = bQ_2|\phi\rangle$. Since

$$\langle\phi|Q_2|\phi\rangle \le \langle\phi|Q_1|\phi\rangle + \langle\phi|Q_2|\phi\rangle = \langle\phi \mid \phi\rangle = 1,$$

we find that

$$\langle\psi_2|Q_2|\psi_2\rangle = \langle Q_2\psi_2 \mid Q_2\psi_2\rangle = |b|^2\,\langle\phi|Q_2|\phi\rangle \le |b|^2 < 1.$$

This is a contradiction. ∎

In *superdense coding*, Alice and Bob are a long way from one another, and Alice wants to transmit some classical information in the form of a 2-bit to Bob. We shall show that this can be achieved with Alice sending a single qubit to Bob. (This can be generalized to sending a 2^n-bit using an n-qubit.) Superdense coding provides a means for communicating classical information in terms of a "smaller amount" of quantum information.

Alice and Bob initially share a 2-qubit in the entangled state

$$|\psi\rangle = \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}.$$

(Remember that a 2-qubit is just a pair of quantum particles.) Alice keeps the first qubit (particle), while Bob keeps the second qubit (particle) and then moves far away. Note that $|\psi\rangle$ is a fixed state and it is not necessary for Alice to send any qubits to Bob to prepare this state. For example, a third party may prepare the entangled state ahead of time, sending one of the qubits to Alice and the other to Bob. In either case this state $|\psi\rangle = |\beta_{00}\rangle$ can be prepared by employing the Bell state generator of Figure 4.

If Alice wishes to send the 2-bit 00 to Bob, she just transmits her qubit. If she wishes to send 01, she applies the quantum gate X (recall the Pauli matrices (1) in section 2) to her qubit and transmits it to Bob. If she wants to send 10, she applies the Pauli matrix Z to her qubit and transmits it. Finally, if she wants to send 11, she applies iY to her qubit and transmits it. The four resulting states are:

$$\begin{aligned}
&00\text{: } (I \otimes I)|\psi\rangle = |\psi\rangle = |\beta_{00}\rangle,\\
&01\text{: } (X \otimes I)|\psi\rangle = |\beta_{01}\rangle,\\
&10\text{: } (Z \otimes I)|\psi\rangle = |\beta_{10}\rangle,\\
&11\text{: } (iY \otimes I)|\psi\rangle = |\beta_{11}\rangle.
\end{aligned}$$

These entangled states are the Bell states considered earlier. They constitute a basis for $\mathbb{C}^4$, hence they can be distinguished by an appropriate measurement. Since Bob is in possession of both qubits, he can perform a measurement on this Bell basis and reliably determine which of the four possible 2-bits Alice sent. Classically, this task would be impossible to perform if Alice transmitted a single bit. (N.B. Superdense coding has been performed in the laboratory.)

In science fiction shows like Star Trek, people are teleported (transported) from one location to another. We now know that this is theoretically possible. Although single qubits have been teleported in practice, it would be prohibitively expensive to teleport the immense n-qubit describing a person, at least with present technology. We have seen that an unknown qubit state $|\psi\rangle$ cannot be copied. However, as we shall

see, $|\psi\rangle$ can be teleported through a classical channel, destroying the original state in the process. Alice wants to transmit $|\psi\rangle$ to Bob by sending him classical information (bits). This looks impossible: even if she knew $|\psi\rangle$, describing it precisely would take an infinite amount of classical information because $|\psi\rangle$ takes values in the continuous space $\mathbb{C}^2$.

The teleportation procedure begins as in superdense coding. Beforehand, Alice and Bob generate a 2-qubit Bell state $|\beta_{00}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Alice takes the first qubit (particle), and Bob moves with the other to a different location. At a later time, when Alice wants to teleport $|\psi\rangle$ to Bob, she combines the qubit in the state $|\psi\rangle$ with her qubit and measures the resulting 2-qubit in her possession, thereby obtaining one of the four classical results 00, 01, 10, or 11. She sends this information to Bob. Depending on Alice's classical information, Bob performs one of four operations on his qubit and amazingly can recover the original state $|\psi\rangle$.

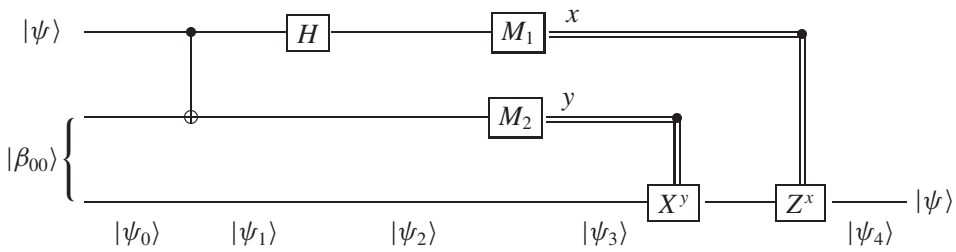

Figure 5. Teleportation circuit.

Quantum teleportation employs the quantum circuit in Figure 5. The top two wires represent Alice's system, the bottom wire Bob's. The state to be teleported is $|\psi\rangle = a|0\rangle + b|1\rangle$, where a and b are unknown complex amplitudes. The input state to the circuit is the 3-qubit state

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[a|0\rangle\left(|00\rangle + |11\rangle\right) + b|1\rangle\left(|00\rangle + |11\rangle\right)\right],$$

in which the first two qubits (particles) belong to Alice and the third qubit (particle) to Bob. Alice applies a CNOT-gate, given by Figure 1, to her two qubits to obtain

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[a|0\rangle\left(|00\rangle + |11\rangle\right) + b|1\rangle\left(|10\rangle + |01\rangle\right)\right].$$

She then applies a Hadamard gate to the first qubit, resulting in

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{\sqrt{2}}\left[a\left(|0\rangle + |1\rangle\right)\left(|00\rangle + |11\rangle\right) + b\left(|0\rangle - |1\rangle\right)\left(|10\rangle + |01\rangle\right)\right] \\ &= \frac{1}{\sqrt{2}}\left[|00\rangle\left(a|0\rangle + b|1\rangle\right) + |01\rangle\left(a|1\rangle + b|0\rangle\right) + |10\rangle\left(a|0\rangle - b|1\rangle\right)\right. \\ &\quad \left. + |11\rangle\left(a|1\rangle - b|0\rangle\right)\right].\end{aligned}$$

In each of these four terms the 2-qubit state on the left is Alice's and the qubit state on the right is Bob's. Notice that information about $|\psi\rangle$ that was originally the first qubit state has miraculously moved to Bob's third qubit state, which is represented by the third (bottom) wire of Figure 5. Alice now measures her 2-qubit in the computational

basis to get 00, 01, 10, or 11. In each case there is only one possibility for Bob's qubit state $|\psi_3\rangle$:

$$00 \Rightarrow |\psi_3\rangle = a|0\rangle + b|1\rangle, \qquad 01 \Rightarrow |\psi_3\rangle = a|1\rangle + b|0\rangle,$$
$$10 \Rightarrow |\psi_3\rangle = a|0\rangle - b|1\rangle, \qquad 11 \Rightarrow |\psi_3\rangle = a|1\rangle - b|0\rangle.$$

That is, if Alice's measurement results in the outcome 00, then Bob's qubit state $|\psi_3\rangle$ must be $a|0\rangle + b|1\rangle$, etc. Alice sends her classical 2-bit result to Bob. Once Bob has learned the result he can fix up his state $|\psi_3\rangle$ to recover $|\psi\rangle$ by applying the appropriate quantum gate as follows:

$$00\text{: } Z^0X^0|\psi_3\rangle = I|\psi_3\rangle = |\psi\rangle,$$
$$01\text{: } Z^0X^1|\psi_3\rangle = X|\psi_3\rangle = aX|1\rangle + bX|0\rangle = a|0\rangle + b|1\rangle = |\psi\rangle,$$
$$10\text{: } Z^1X^0|\psi_3\rangle = Z|\psi_3\rangle = aZ|0\rangle - bZ|1\rangle = a|0\rangle + b|1\rangle = |\psi\rangle,$$
$$11\text{: } Z^1X^1|\psi_3\rangle = Z\,(aX|1\rangle - bX|0\rangle) = aZ|0\rangle - bZ|1\rangle = a|0\rangle + b|1\rangle = |\psi\rangle.$$

It might appear that quantum teleportation allows the transfer of information faster than the speed of light, which would contradict relativity theory. It is true that the CNOT and Hadamard gates change the state of Bob's qubit instantaneously. However, Alice must transmit her measurement result over a classical communications channel, which limits the speed to that of light. In fact, it can be shown that without this classical communication, teleportation conveys no information whatsoever [**7**].

6. DEUTSCH-JOZSA AND GROVER ALGORITHMS. Quantum parallelism is a feature of quantum mechanics that allows quantum computers to evaluate a function $f(x)$ for many values of x simultaneously. Let $f\colon \{0,1\}^n \to \{0,1\}$ be a function that takes an n-bit into a bit. Letting $V = \mathbb{C}^2$, we define the transformation $U_f\colon V^{\otimes n} \otimes V \to V^{\otimes n} \otimes V$ by $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$ for x in $\{0,1\}^n$ and y in $\{0,1\}$, and extend by linearity. Since $U_f|x,0\rangle = |x, f(x)\rangle$ and $U_f|x,1\rangle = |x, \overline{f(x)}\rangle$, we see that U_f is unitary and is thus a quantum gate. A quantum parallelism circuit is depicted in Figure 6, in which the second gate is a U_f-gate. If $|0\rangle^{\otimes n}$ is input into the upper multiple wire and $|0\rangle$ into the lower single wire of Figure 6, then we produce the state

$$U_f(H^{\otimes n} \otimes I)|0\rangle = \frac{1}{\sqrt{2^n}} U_f \sum_x |x,0\rangle = \frac{1}{\sqrt{2^n}} \sum_x U_f|x,0\rangle$$
$$= \frac{1}{\sqrt{2^n}} \sum_x |x, f(x)\rangle.$$

The final state on the right contains information about all the values of $f(x)$ simultaneously.

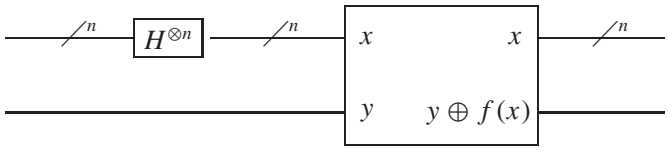

Figure 6. Quantum parallelism circuit.

The Deutsch-Jozsa algorithm shows that a quantum computer is definitely more powerful (faster) than a classical computer. We call a function $f:\{0,1\}^n \to \{0,1\}$ *balanced* if $f(x) = 1$ for exactly half of all possible x and $f(x) = 0$ for the other half. Suppose that Bob has a function $f:\{0,1\}^n \to \{0,1\}$ that is either constant or balanced, and Alice wants to find out which it is with certainty. Alice selects an integer x from 0 to $2^n - 1$ and sends x to Bob. Bob calculates $f(x)$ and replies with the result, which is either 0 or 1. What is the fewest number of queries that Alice can make to determine whether or not f is constant?

In the classical case, Alice can send Bob one value of the n-bit x in each query. If Alice ever gets two different replies, she knows that f is balanced and can stop. At worst, she will need to query Bob $2^{n-1} + 1$ times, because she may first receive 2^{n-1} zeros and will need one more query to decide. We say that this problem has exponential time complexity classically. On the other hand, if Alice and Bob were able to exchange qubits instead of just classical bits, then Alice could achieve her goal in just one query using the Deutsch-Jozsa algorithm, which we now discuss.

Alice has an n-qubit register in which to store her query and a 1-qubit register that she gives Bob in which to store the answer. She begins by preparing both her query and answer registers in a superposition state, as explained in detail later. Bob evaluates $f(x)$ using a quantum parallelism circuit and leaves the result in the answer register. Alice then applies a Hadamard transformation $H^{\otimes n}$ to the query register and finishes by a suitable measurement to determine whether f is constant or balanced. The quantum circuit is depicted in Figure 7.

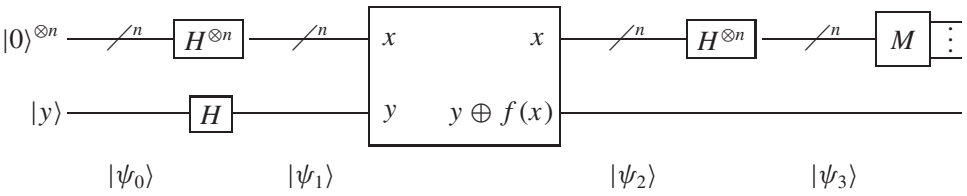

Figure 7. Deutsch-Jozsa algorithm.

The input state for the circuit in Figure 7 is $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$. The state $|\psi_1\rangle$ becomes

$$|\psi_1\rangle = H^{\otimes(n+1)}|\psi_0\rangle = H^{\otimes n}|0\rangle^{\otimes n}H|1\rangle = \sum_x \frac{|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right),$$

where x belongs to $\{0,1\}^n$. To obtain the state $|\psi_2\rangle$ we compute

$$\begin{aligned}|\psi_2\rangle = U_f|\psi_1\rangle &= \sum_x \frac{|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \oplus |f(x)\rangle\right) \\ &= \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).\end{aligned}$$

Hence,

$$|\psi_3\rangle = (H^{\otimes n} \otimes I)|\psi_2\rangle = \sum_{x,y} \frac{(-1)^{x\cdot y + f(x)}|y\rangle}{2^n}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Alice now makes a measurement on the query register. Note that the amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$. If f is constant, this amplitude is ± 1. Since $\||\psi_3\rangle\| = 1$, all the other amplitudes must be 0. Thus, the measurement outcome is 0 with certainty. If f is balanced, then the amplitude for the state $|0\rangle^{\otimes n}$ is 0. Hence, the measurement outcome must be different from 0. We have two possibilities: Alice obtains the outcome zero or the outcome nonzero. In the first case, f is certainly constant and in the second case f must be balanced.

Suppose you find a telephone number on a scrap of paper but have forgotten whose number it is. In your little black book you have listed your friends with their telephone numbers. If there are N people in your list, you might have to check about N numbers (technically, the number of steps involved is denoted by $O(N)$). This is the best that can be done for a classical search algorithm on an unstructured data base. We shall see that Grover's quantum search algorithm requires only $O(\sqrt{N})$ searches. This again shows that a quantum computer is more powerful than a classical computer. Moreover, unlike the Deutsch-Jozsa algorithm, Grover's algorithm solves a practical problem with many applications. Of course, for structured data bases (for example, alphabetical or numerical order) there are much faster algorithms.

When we search through a set of N elements we can assume that the elements are indexed from 0 to $N-1$ and look for the index of the element we want to find. We assume that $N = 2^n$, so the index can be stored in n bits, and for simplicity we shall assume that there is exactly one solution y. At the end we shall discuss what to do when there are M solutions. Let $f\colon \{0, 1, \ldots, 2^n - 1\} \to \{0, 1\}$ be defined by $f(x) = \delta_{xy}$. An *oracle* is a black box that can recognize the solution to the search problem. The oracle does not know the solution beforehand, it can just verify the solution if it sees it. We define the oracle as the unitary operator $\mathcal{O}$ on $\mathbb{C}^N = (\mathbb{C}^2)^{\otimes n}$ given by $\mathcal{O}|x\rangle = (-1)^{f(x)}|x\rangle$ for each member $|x\rangle$ of the computational basis. We say that the oracle *marks* the solution by shifting its phase.

The crucial quantum gate in the algorithm is the *Grover operator* defined by performing the following operations in sequence:

(1) apply the oracle $\mathcal{O}$;
(2) apply the Hadamard transformation $H^{\otimes n}$;
(3) perform the conditional phase shift $F_c|0\rangle = |0\rangle$ and $F_c|x\rangle = -|x\rangle$ for $x > 0$;
(4) apply $H^{\otimes n}$ again.

Notice that

$$F_c|x\rangle = -(-1)^{\delta_{x0}}|x\rangle = (2|0\rangle\langle 0| - I)\,|x\rangle,$$

so $F_c = 2|0\rangle\langle 0| - I$. Thus the Grover operator G is the product of four unitary operators

$$G = H^{\otimes n} F_c H^{\otimes n} \mathcal{O} = H^{\otimes n}\,(2|0\rangle\langle 0| - I)\,H^{\otimes n}\mathcal{O}.$$

To simplify the expression for G, let

$$|\psi\rangle = H^{\otimes n}|0\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle.$$

Since $H^2 = I$, we have

$$H^{\otimes n}\,(2|0\rangle\langle 0| - I)\,H^{\otimes n} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I = 2|\psi\rangle\langle\psi| - I.$$

Hence, $G = (2|\psi\rangle\langle\psi| - I)\,\mathcal{O}$. The reason we did not just define G in this simple way is that we wanted to show how G can be efficiently implemented using standard quantum gates that can be constructed in practice.

We can visualize G geometrically as a two-dimensional rotation. Recalling that y is the unique solution to our search problem, we let $|\alpha\rangle$ be the unit vector given by

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq y} |x\rangle.$$

The uniform superposition $|\psi\rangle$ can then be written as follows:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle + \frac{1}{\sqrt{N}} |y\rangle = \sqrt{1 - \frac{1}{N}}\, |\alpha\rangle + \sqrt{\frac{1}{N}}\, |y\rangle.$$

The oracle $\mathcal{O}$ performs a reflection across $|\alpha\rangle$ in the plane $\mathcal{P}$ spanned by $|\alpha\rangle$ and $|y\rangle$. That is,

$$\mathcal{O}\,(a|\alpha\rangle + b|y\rangle) = a|\alpha\rangle - b|y\rangle.$$

Similarly, $2|\psi\rangle\langle\psi| - I$ performs a reflection in $\mathcal{P}$ across $|\psi\rangle$. Indeed, if $|\psi'\rangle$ is a unit vector orthogonal to $|\psi\rangle$ in $\mathcal{P}$, then

$$(2|\psi\rangle\langle\psi| - I)\left(a|\psi\rangle + b\big|\psi'\big\rangle\right) = a|\psi\rangle - b\big|\psi'\big\rangle.$$

But the product of two reflections is a rotation. This tells us that $G^k|\psi\rangle$ remains in $\mathcal{P}$ for all k. We can obtain the rotation angle as follows. Let $\cos(\theta/2) = \sqrt{1 - 1/N}$, so that

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |\alpha\rangle + \sin\left(\frac{\theta}{2}\right) |y\rangle.$$

Figure 8 then shows that $G|\psi\rangle = \cos(3\theta/2)|\psi\rangle + \sin(3\theta/2)|y\rangle$, making the rotation angle θ.

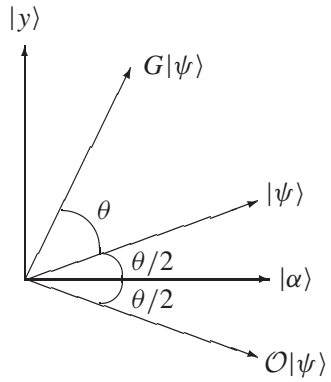

Figure 8. Rotation angle.

A repeated application of G takes $|\psi\rangle$ to

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\,\theta\right) |\alpha\rangle + \sin\left(\frac{2k+1}{2}\,\theta\right) |y\rangle$$

and can rotate $|\psi\rangle$ close to $|y\rangle$. When this occurs, a measurement in the computational basis gives outcome y with high probability and thus solves the search problem.

How many times must G be repeated to rotate $|\psi\rangle$ close to $|y\rangle$? To get an exact rotation to $|y\rangle$ would require k' applications of G, with k' satisfying

$$0 = \cos\left(\frac{2k'+1}{2}\,\theta\right) = \cos\left(k'\theta + \frac{\theta}{2}\right) = \cos(k'\theta)\cos\left(\frac{\theta}{2}\right) - \sin(k'\theta)\sin\left(\frac{\theta}{2}\right)$$

$$= \sqrt{1-\frac{1}{N}}\,\cos(k'\theta) - \sqrt{\frac{1}{N}}\,\sin(k'\theta).$$

Hence $\tan(k'\theta) = \sqrt{N-1}$, which gives $\cos(k'\theta) = \sqrt{1/N}$ and

$$k' = \frac{\cos^{-1}\left(\sqrt{1/N}\right)}{\theta}.$$

Of course, k is an integer, so we take $k = \lceil k' \rceil$, where $\lceil\ \rceil$ denotes the ceiling function (i.e., $\lceil x \rceil$ is the smallest integer that is greater than or equal to x). Therefore, we must repeat the Grover operator

$$R = \left\lceil \frac{\cos^{-1}\left(\sqrt{1/N}\right)}{\theta} \right\rceil \leq \left\lceil \frac{\pi}{2\theta} \right\rceil$$

times. Because

$$\sqrt{\frac{1}{N}} = \sin\left(\frac{\theta}{2}\right) \leq \frac{\theta}{2},$$

we have $4\sqrt{1/N} \leq 2\theta$, whence $R \leq \lceil \pi\sqrt{N}/4 \rceil$. Thus, fewer than $\sqrt{N}$ oracle calls must be performed to solve the search problem with high probability. To estimate this probability, we see from Figure 8 that G^R rotates $|\psi\rangle$ to within $\theta/2$ of $|y\rangle$. Since N is fairly large in practice, we have

$$\frac{\theta}{2} \approx \sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{1}{N}},$$

which yields a probability of at most $1/N$ that an error occurs.

If there is a known number $1 \leq M \leq N$ of solutions to the search problem, then a slightly more delicate argument gives the same results with N replaced by N/M. In this case, $R \leq \lceil \pi\sqrt{N/M}/4 \rceil$, which is reasonable because fewer searches should be required to find a solution. If the number of solutions M is unknown, then the situation gets more complicated. In that event, a separate algorithm based on the phase estimation algorithm discussed in the next section can be applied to approximate M to any degree of accuracy (this also works if $M = 0$). Moreover, this separate algorithm still requires $O\left(\sqrt{N/M}\right)$ operations. Once M is determined, we can proceed as before.

7. QUANTUM FOURIER TRANSFORM. Probably the most impressive quantum algorithm to date is Shor's factorization algorithm. This algorithm enables a quantum computer to factor integers exponentially faster than any known algorithm for a classical computer. It turns out that Shor's algorithm can be reduced to the phase estimation

algorithm discussed in this section, and both of these algorithms rely on the quantum Fourier transform. The reduction requires a considerable knowledge of number theory and will not be considered here.

Let $V = \mathbb{C}^N$ with computational basis $|0\rangle, \ldots, |N-1\rangle$. The *quantum Fourier transform* on V is the operator $F: V \to V$ defined by

$$F|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle,$$

where in this context $i = \sqrt{-1}$. We first show that F is unitary.

$$\langle j' | F^\dagger F | j \rangle = \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi ik(j-j')/N}.$$

If $j = j'$, the sum is 1; if $j \neq j'$, the sum is

$$\frac{1}{N} \sum_{k=0}^{N-1} \left[e^{2\pi i(j-j')/N} \right]^k = \frac{1}{N} \left[\frac{1 - e^{2\pi i(j-j')}}{1 - e^{2\pi i(j-j')/N}} \right] = 0.$$

Hence $\langle j' | F^\dagger F | j \rangle = \delta_{jj'} = \langle j' \mid j \rangle$ for $j', j = 0, 1, \ldots, N-1$. It follows that $F^\dagger F = I$, confirming that F is unitary.

In the sequel we take $N = 2^n$, so the basis $|0\rangle, \ldots, |2^n - 1\rangle$ is the computational basis for an n-qubit. As earlier, we frequently write $|j\rangle$ in terms of its binary representation $j = j_1 \cdots j_n$, i.e.,

$$|j\rangle = |j_1 \cdots j_n\rangle = |j_1\rangle \cdots |j_n\rangle.$$

We also use the notation $0.j_\ell j_{\ell+1} \ldots j_m$ to represent the *binary fraction*

$$j_\ell/2 + j_{\ell+1}/2^2 + \cdots + j_m/2^{m-\ell+1}.$$

The product representation in the next lemma makes it easy to derive an efficient quantum circuit for F using simple 1-qubit quantum gates.

Lemma 2. *For $|j\rangle = |j_1 \cdots j_n\rangle$ it is the case that*

$$F|j\rangle = \frac{1}{2^{n/2}} \left[\left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle \right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n} |1\rangle \right) \right].$$

Proof. This follows from the calculation

$$\begin{aligned}
F|j\rangle &= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left(2\pi ij \sum_{\ell=1}^{n} k_\ell 2^{-\ell} \right) |k_1 \cdots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \otimes_{\ell=1}^{n} e^{2\pi ijk_\ell 2^{-\ell}} |k_\ell\rangle = \frac{1}{2^{n/2}} \otimes_{\ell=1}^{n} \sum_{k_\ell=0}^{1} e^{2\pi ijk_\ell 2^{-\ell}} |k_\ell\rangle \\
&= \frac{1}{2^{n/2}} \otimes_{\ell=1}^{n} \left(|0\rangle + e^{2\pi ij2^{-\ell}} |1\rangle \right).
\end{aligned}$$

This last term gives the required expression. ∎

Suppose that a unitary operator U has a known eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\phi}$, where ϕ is unknown. The *phase estimation algorithm* is employed to estimate ϕ. This algorithm uses two registers. The first register contains t qubits initially in the state $|0\rangle$. The choice of t depends on the number of digits of accuracy we wish for our estimate of ϕ and the probability with which we want the estimation to be successful. The second register begins in the state $|u\rangle$ and contains as many qubits as is necessary to store $|u\rangle$ to a desired accuracy. Phase estimation has three stages, the first of which is depicted in Figure 9.

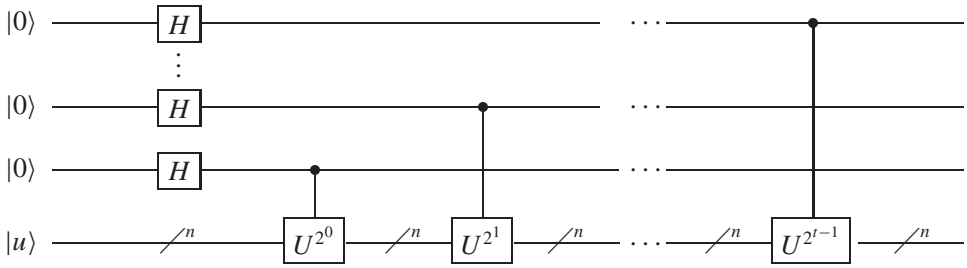

Figure 9. First stage of the phase estimation algorithm.

Recall that the controlled-U^j-gate with matrix A satisfies

$$\begin{aligned} A\left[\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)\right]|u\rangle &= \frac{1}{\sqrt{2}}A|0\rangle|u\rangle+\frac{1}{\sqrt{2}}A|1\rangle|u\rangle \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle+|1\rangle U^j|u\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle+|1\rangle e^{2\pi ij\phi}|u\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle+e^{2\pi ij\phi}|1\rangle\right)|u\rangle. \end{aligned}$$

By Lemma 2, the final state of the first register becomes

$$\frac{1}{2^{t/2}}\left(|0\rangle+e^{2\pi i2^{t-1}\phi}|1\rangle\right)\left(|0\rangle+e^{2\pi i2^{t-2}\phi}|1\rangle\right)\cdots\left(|0\rangle+e^{2\pi i2^{0}\phi}|1\rangle\right)=\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi ik\phi}|k\rangle.$$

We omit the second register from the rest of the description because it stays in the state $|u\rangle$ throughout the computation. The second stage of phase estimation is to apply the inverse quantum Fourier transform

$$F^\dagger|j\rangle=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{-2\pi ijk/N}|k\rangle$$

to the first register. The third and final stage is to read out the state of the first register by applying a measurement in the computational basis. This provides a good estimate of ϕ.

To get an idea as to why phase estimation works, suppose ϕ can be exactly expressed by t bits as $\phi = 0.\phi_1 \dots \phi_t$. Then by Lemma 2, the state resulting from the first stage is

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 0.\phi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\phi_{t-1}\phi_t}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.\phi_1 \dots \phi_t}|1\rangle\right) = F|\phi_1\phi_2\dots\phi_t\rangle.$$

Taking the inverse quantum Fourier transform $F^\dagger$ in the second stage leads to $|\phi_1\phi_2\dots\phi_t\rangle$. A measurement in the computational basis then gives ϕ exactly with probability 1.

Thus, we can solve the problem exactly whenever ϕ is rational. If ϕ is irrational, this algorithm (with t sufficiently large) provides an estimate for ϕ to any desired degree of accuracy with probability arbitrarily close to 1. To demonstrate this requires a fairly long analysis [**7**], [**8**] that we shall omit. The end result is the following: to obtain ϕ accurate to n bits with probability of success at least $1 - \varepsilon$, choose $t = n + \lceil \log_2\left(2 + \frac{1}{2\varepsilon}\right)\rceil$.

REFERENCES

1. A. Barenco, C. H. Bennett, R. Cleve, D. DiVincenzo, N. Margolous, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* **52** (1995), 3457–3467.
2. M. Brooks, *Quantum Computing and Communications*, Springer-Verlag, London, 1999.
3. R. Feynman, *Feynman Lectures on Computation*, Perseus Publishing, Cambridge, MA, 1999.
4. J. Gruska, *Quantum Computing*, McGraw-Hill, London, 1999.
5. H.-K. Lo, T. Spiller, and S. Popescu, *Quantum Information and Computation*, World Scientific, Singapore, 1998.
6. G. Milburn, *The Feynman Processor*, Perseus Books, Reading, MA, 1998.
7. M. Nielsen and I. Chuang, *Quantum Computations and Quantum Information*, Cambridge University Press, Cambridge, 2000.
8. A. Pittenger, *An Introduction to Quantum Computing Algorithms*, Birkhäuser, Boston, 1999.
9. H. Pollatsek, Quantum error correction: classic group theory meets a quantum challenge, *Amer. Math. Monthly* **108** (2001) 932–962.
10. J. Preskill, *Quantum Computation and Information*, California Institute of Technology, Pasadena, CA, 1998.
11. C. Williams and S. Clearwater, *Ultimate Zero and One*, Springer-Verlag, New York, 2000.
12. C. Williams and S. Clearwater, *Explorations in Quantum Computing*, Springer-Verlag, New York, 1998.

STAN GUDDER may be found either teaching or conducting research at the University of Denver, skiing or hiking in the mountains, or playing with his grandchildren. He has written over two hundred articles on functional analysis, ordered algebraic structures, foundations of quantum mechanics, and quantum computation. He has authored two editions of an undergraduate text *A Mathematical Journey* (McGraw-Hill, 1994) and two research monographs: *Stochastic Methods in Quantum Mechanics* (North Holland, 1979) and *Quantum Probability* (Academic Press, 1988).

Department of Mathematics, University of Denver, Denver Colorado 80208
sgudder@math.du.edu