QUBIT DEVICES

HOWARD E. BRANDT

ABSTRACT. This lecture presents brief mathematical descriptions of a variety of potential qubit devices. The qubit devices examined include an interaction-free detector, a quantum key receiver, quantum games, quantum gates, qubit entanglers, Bell state synthesizers, Bell state analyzers, quantum dense coders, entanglement swappers, quantum teleporters, quantum copiers, quantum error correctors, quantum computers, and quantum robots.

1. INTRODUCTION

A *qubit device* [1] is a physical implementation of a set of quantum bits, or qubits, as they are popularly known [2,3]. A *qubit* is a quantum system with a two-dimensional Hilbert space, capable of existing in a superposition of Boolean states, and also capable of being entangled with the states of other qubits [4]. Qubit devices include quantum computers, quantum gates, quantum key receivers, entanglement swappers, quantum teleporters, quantum dense coders, interaction-free detectors, quantum robots, quantum games, quantum copiers, etc.

The exciting new interdisciplinary fields of quantum information processing, quantum computing, quantum communication, and quantum cryptography are rich with a plethora of potentially useful qubit devices [5]. The major obstacle to the successful development of these devices is the phenomenon of quantum decoherence, in which even weak interactions of the qubits with noncomputational environmental degrees of freedom can destroy the off-diagonal components of the reduced density matrix of the qubits, obliterating essential quantum coherence and quantum entanglement. This lecture is an abbreviated version of recent work by the author [5], with some additions; it presents brief mathematical descriptions of a variety of potential qubit devices, and includes expository discussions of the issue of quantum decoherence as it relates to the possible practical development of these devices.

2. INTERACTION-FREE DETECTOR

The interaction-free detector [6–8] provides a simple example of the practical use of path qubits. (The two-dimensional Hilbert space of a path qubit represents two possible quantum-interfering paths of a photon in spacetime [5].) In this photonic device, the presence of an opaque object inside one arm of an interferometer destroys the interference of an incident photon, sometimes signaling the presence of the object, even though the photon could not have taken a path intersecting the object.

A simple example of an interaction-free detector [8] is schematized in Fig. 1. Here, a single photon in polarization state $|u\rangle$ enters a Michelson interferometer consisting of a 50/50 beamsplitter (BS), a 90° phase shifter (ϕ), two mirrors (M_1

1991 *Mathematics Subject Classification.* Primary 81P68, 81V80, 68-01, 68-02, 68Q05, 94-02, 81V45.

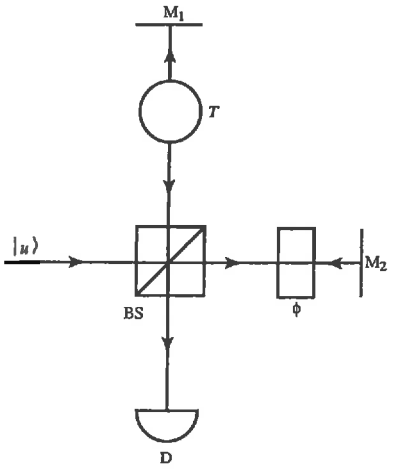

FIGURE 1. Interaction-free detector.

and M_2), and a single-photon photodetector (D). All optical elements are here assumed to be ideal and not to affect the polarization u. An object with transmission coefficient T may or may not lie in the path between the beamsplitter and mirror M_1. If it is not present, its absence is effectively described by $T = 1$. The quantum mechanical probability amplitude [9–12] that the photon reflects at the beamsplitter BS toward mirror M_1 is $2^{-1/2}i$. The factor of $2^{-1/2}$ is due to the 50/50 beamsplitter (with transmission coefficient 1/2), and the factor of i is due to the reflection at the beamsplitter, which produces a phase shift $e^{i\pi/2} = i$ [13–15]. Then the probability amplitude A_1 that the photon also passes through the object with transmission coefficient T, reflects from mirror M_1, returns through the object and the beamsplitter, and goes on to the detector D is given by

$$A_1 = \left(2^{-1/2}\right)\left(T^{1/2}\right)\left(T^{1/2}\right)\left(2^{-1/2}i\right) = 2^{-1}iT. \tag{1}$$

The factor $\left(2^{-1/2}i\right)$ is due to the reflection at the beamsplitter, the two factors of $T^{1/2}$ are due to the two passages through the object characterized by its transmission coefficient T, and the factor $\left(2^{-1/2}\right)$ is due to the passage through the 50/50 beamsplitter with transmission coefficient 1/2. Similarly, the probability amplitude A_2 that the photon initially passes along the other possible path directly through the beamsplitter BS, passes through the 90° phase shifter ϕ to mirror M_2, returns back again to the beamsplitter, and is then reflected to the detector D is given by

$$A_2 = \left(2^{-1/2}i\right)\left(e^{i\pi/2}\right)\left(e^{i\pi/2}\right)\left(2^{-1/2}\right) = -2^{-1}i. \tag{2}$$

Here, reading from right to left, the factor $\left(2^{-1/2}\right)$ is due to the photon passing through the 50/50 beamsplitter with transmission coefficient 1/2, the factors of $e^{i\pi/2}$ are due to the two traversals of the 90° phase shifter, and the factor $\left(2^{-1/2}i\right)$ is due to the reflection at the beamsplitter. It follows that the total quantum mechanical probability amplitude A that the photon triggers the detector D is given by the sum of the amplitudes for both possible paths of the photon through

the interferometer to the detector, namely,

$$A \equiv A_1 + A_2. \tag{3}$$

This is single-particle quantum interference. The beamsplitter effectively converts the state of the photon into a two-state system, corresponding to the two possible paths 1 and 2 of the photon through the interferometer to the detector. This is a *path qubit* [5]. Substituting Eqs. (1) and (2) in Eq. (3), one obtains for the total amplitude

$$A = 2^{-1}i(T-1). \tag{4}$$

The probability that the detector D is triggered is then given by

$$P_D(T) = |A|^2 = \frac{1}{4}(T-1)^2. \tag{5}$$

If the object is not present, then effectively $T = 1$, and according to Eq. (5), the probability that the detector is triggered is vanishing, namely,

$$P_D(1) = 0. \tag{6}$$

Therefore, if the object is not there, the detector D cannot be triggered. If the object is present and opaque, namely $T = 0$, then according to Eq. (5),

$$P_D(0) = \frac{1}{4}. \tag{7}$$

Thus, if the object is there, the detector D will be triggered 25% of the time (probability 1/4 for each single incident photon). The probability that the photon is absorbed if the object is present is clearly 1/2, because that is the probability that the photon entering the interferometer is reflected to the object by the 50/50 beamsplitter. The probability that the photon instead returns to the entrance port is clearly 1/4, and the probabilities add to unity as they must. Thus, with this particular interaction-free detector, one can detect the presence of the object 25% of the time. Clearly, when the object is present and the detector is triggered, the photon cannot have taken the path intersecting the object, because if it did it would be absorbed before reaching the detector. This is the basis for saying that the photon does not "interact" with the object. However, there must be an interaction term in any Hamiltonian describing the system [8].

3. QUANTUM KEY RECEIVER

Another simple example of a photonic qubit device is a quantum key receiver based on a positive operator valued measure (POVM). Specifically, a POVM is a set of nonnegative Hermitian operators A_μ that act in the Hilbert space of a quantum system and sum to the identity operator, namely [16–18],

$$\sum_\mu A_\mu = 1. \tag{8}$$

The index μ labels the various possible outcomes of a measurement implementing the POVM. The probability P_μ of outcome μ, if the system is in a state described by the density matrix ρ, is given by

$$P_\mu = \mathrm{Tr}\,(A_\mu \rho). \tag{9}$$

The advantage of a POVM is that it may have a lower inconclusive rate and may allow the extraction of more information than can the usual von Neumann-type projective measurement [16,20].

Because of the noncommutativity of nonorthogonal photon polarization projective measurement operators, a simple von Neumann-type projective measurement cannot conclusively distinguish the state of a photon having two possible nonorthogonal polarization states. If one wants to be able to distinguish conclusively between two nonorthogonal photon states $|u\rangle$ and $|v\rangle$ at least some of the time, it is useful to consider a POVM used in quantum cryptography [16,19–25]. Quantum cryptography [26–31] provides a number of practical applications for qubit devices.

In quantum cryptography, one is able, in principle, to produce a shared key whose security is guaranteed by the laws of quantum mechanics. The key is a random bit sequence which, when added to the message (encoded in binary), forms the encrypted message, and which, when subtracted from the encrypted message, yields the decrypted message. Qubit devices can be used in transmitting and receiving the key, and also in eavesdropping.

A POVM used in quantum cryptography consists of the following set of three nonnegative Hermitian operators:

$$A_u = (1 + \langle u|v\rangle)^{-1} [1 - |v\rangle \langle v|], \tag{10}$$

$$A_v = (1 + \langle u|v\rangle)^{-1} [1 - |u\rangle \langle u|], \tag{11}$$

$$A_? = 1 - A_u - A_v, \tag{12}$$

in which kets $|u\rangle$ and $|v\rangle$ represent nonorthogonal single-photon states. The POVM operators, Eqs. (10) to (12), clearly satisfy Eq. (8). Specifically in the present work, the states $|u\rangle$ and $|v\rangle$ are taken to be linear-polarization states with the Dirac bracket $\langle u|v\rangle$ given by

$$\langle u|v\rangle = \cos\theta, \tag{13}$$

where θ is the angle between the two polarization states. A general qubit state is given by

$$|\psi\rangle = \alpha |u\rangle + \beta |v,\rangle \tag{14}$$

where α and β are complex numbers. The operators (10) to (12) are clearly Hermitian; however, they are not projection operators, since the product of any one of them with itself does not yield itself. Also, for nonorthogonal states they do not commute.

The probability that an arbitrary qubit $|\psi\rangle$ given by Eq. (14) is measured to be in the u-polarization state can be calculated with Eqs. (9), (10), (13), and (14); the calculation yields

$$P_u = \mathrm{Tr}\ (A_u |\psi\rangle \langle\psi|) = \langle\psi|A_u|\psi\rangle = |\alpha|^2(1 - \cos\theta). \tag{15}$$

The first equality holds, since for a pure state $|\psi\rangle$, the density matrix is $|\psi\rangle \langle\psi|$. A_u is a positive operator, as it must be. This follows since $|\psi\rangle$ can represent any state in the two-dimensional Hilbert space of states, and the right-hand side of Eq. (15) is nonnegative. This must be so, since P_u is a probability. Analogously, one obtains

$$P_v = \langle\psi|A_v|\psi\rangle = |\beta|^2(1 - \cos\theta), \tag{16}$$

and

$$P_? = \langle\psi|A_?|\psi\rangle = |\alpha+\beta|^2\cos\theta, \tag{17}$$

both of which are also clearly nonnegative. In Eq. (16), the qubit is measured to be in the state $|v\rangle$. In Eq. (17), $P_?$ is the probability of an inconclusive measurement, meaning that it is undecided whether the qubit is in state $|u\rangle$ or $|v\rangle$. If the state $|\psi\rangle$, Eq. (14), is normalized to unity, then

$$1 = \langle\psi|\psi\rangle = |\alpha|^2 + (\alpha^*\beta + \alpha\beta^*)\cos\theta + |\beta|^2, \tag{18}$$

and it then follows from Eqs. (15) to (17) that the probabilities sum to unity, as they must:

$$P_u + P_v + P_? = 1. \tag{19}$$

When the incident photon is in the state $|u\rangle$, one has $(\alpha,\beta) = (1,0)$, and Eq. (16) becomes $\langle u|\,A_v\,|u\rangle = 0$. When the incident photon is in the state $|v\rangle$, one has $(\alpha,\beta) = (0,1)$, and Eq. (15) becomes $\langle v|\,A_u\,|v\rangle = 0$. Therefore, when an ideal detector representing the operator A_u responds positively, it follows that a photon with a v-polarization state cannot have been received. Likewise, when an ideal detector representing the operator A_v responds, a photon with a u-polarization state cannot have been received. The operator $A_?$ represents inconclusive responses, since Eq. (17) is nonvanishing for $(\alpha,\beta) = (0,1)$ or $(1,0)$. Thus a u-polarized photon can result in a nonzero expectation value (and the associated response) only for detectors representing the A_u or $A_?$ operators. A v-polarized photon excites only the A_v or $A_?$ detectors. It follows that the POVM of Eqs. (10) to (12) distinguishes conclusively between two nonorthogonal states $|u\rangle$ and $|v\rangle$ at least some of the time.

For the purpose of secure key generation in quantum cryptography, one can employ a train of single photons having two possible equally likely nonorthogonal polarization states $|u\rangle$ and $|v\rangle$, which encode 0 and 1, respectively, to securely communicate a random bit sequence between a sender (Alice) and a receiver (Bob). To detect a photon, Bob can use a *quantum key receiver*. If Bennett's two-state protocol [25] is employed, it can be advantageous for the receiver to be based on a POVM [16,19,20]. In the two-state protocol, a positive response of the receiver (the reception of a photon in a u- or v-polarization state) is publicly communicated by Bob to Alice, without revealing which polarization was detected, and the corresponding bits then constitute the preliminary key shared by Alice and Bob. Bits corresponding to photons that do not excite the u- or v-polarization state detectors in the receiver are excluded from the key. The ideal receiver must be such that if its u-polarization detector is excited, then Bob is certain that the u-polarization state was received. Also, if the v-polarization detector is excited, then a v-polarization state was received. Because of the noncommutativity of nonorthogonal photon polarization-measurement operators representing nonorthogonal photon polarization states [5], and also because arbitrary quantum states cannot be cloned [32,33], any attempt to eavesdrop can, in principle, be detected by Bob and Alice.

A quantum key receiver based on a POVM is shown schematically in Fig. 2. It is an all-optical implementation of the POVM given in Eqs. (10) to (12) [21–23]. The straight lines with arrows represent possible optical pathways for a photon to move through the device. The path labeled $|\psi\rangle$ is the incoming path for a photonic qubit represented by an arbitrary polarization state, given by Eq. (14). Also in Fig. 2, D_u, D_v, and $D_?$ designate photodetectors representing the measurement operators A_u,

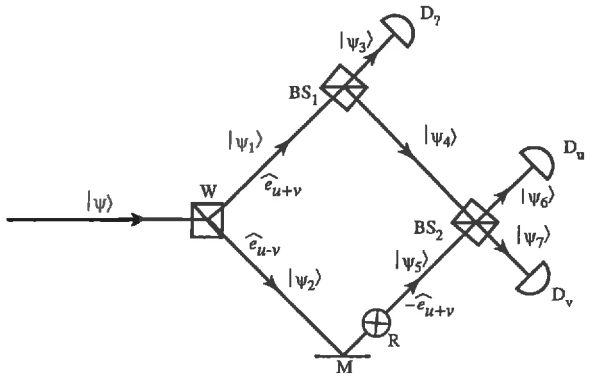

FIGURE 2. Quantum key receiver.

A_v, and $A_?$, respectively. Shown also is a Wollaston prism W [34], which is aligned so that an incident photon with polarization vector $\hat{e}_{u+v}$ takes the path labeled by the state $|\psi_1\rangle$ and $\hat{e}_{u+v}$, and not the path labeled by the polarization vector $\hat{e}_{u-v}$ and the state $|\psi_2\rangle$. Here $\hat{e}_{u+v}$ denotes a unit polarization vector corresponding to polarization state $|u+v\rangle = |u\rangle + |v\rangle$, and is perpendicular to the unit polarization vector $\hat{e}_{u-v}$ corresponding to the polarization state $|u-v\rangle = |u\rangle - |v\rangle$. It follows from Eq. (13) that the states $|u+v\rangle$ and $|u-v\rangle$ are orthogonal, namely,

$$\langle u+v|u-v\rangle = 0. \tag{20}$$

Also, clearly,

$$\hat{e}_{u+v} \cdot \hat{e}_{u-v} = 0, \tag{21}$$

which is consistent with Eqs. (20) and (13). In accordance with the property of a Wollaston prism of separating orthogonal polarization states, an incident photon with polarization vector $\hat{e}_{u-v}$ takes the path labeled by the state $|\psi_2\rangle$.

The device has two beamsplitters [34], designated BS_1 and BS_2 in Fig. 2. Beamsplitter BS_2 is a 50/50 beamsplitter for a photon entering either of its entrance ports. Beamsplitter BS_1 has transmission and reflection coefficients specified in Eqs. (34) and (35) below. The two paths from the Wollaston prism to beamsplitter BS_2 have equal optical path lengths. Also shown in Fig. 2 is a 90° polarization rotator [34], designated R, which transforms a photon with polarization vector $\hat{e}_{u-v}$ into one with polarization vector $-\hat{e}_{u+v}$. There is also a single mirror M, as shown in Fig. 2. All optical elements are here taken to be ideal.

The state of a photon taking the path designated by the state $|\psi_1\rangle$ in Fig. 2 is given by

$$|\psi_1\rangle = |\,\hat{e}_{u+v}\rangle\langle\hat{e}_{u+v}\,|\psi\rangle, \tag{22}$$

where $|\,\hat{e}_{u+v}\rangle$ represents a unit ket corresponding to polarization vector $\hat{e}_{u+v}$. Clearly,

$$|\,\hat{e}_{u+v}\rangle = \frac{|u\rangle + |v\rangle}{[(\langle u| + \langle v|)\,(|u\rangle + |v\rangle)]^{1/2}}. \tag{23}$$

Substituting Eq. (23) in Eq. (22), and using Eqs. (14) and (13), one obtains

$$|\psi_1\rangle = 2^{-1/2}\,(\alpha+\beta)\,(1+\cos\theta)^{1/2}\,|\,\hat{e}_{u+v}\rangle. \tag{24}$$

One also has

$$|\psi_2\rangle = |\,\hat{e}_{u-v}\rangle\langle\hat{e}_{u-v}\,|\psi\rangle, \tag{25}$$

where

$$|\,\hat{e}_{u-v}\rangle = \frac{|u\rangle - |v\rangle}{[(\langle u| - \langle v|)\,(|u\rangle - |v\rangle)]^{1/2}} \tag{26}$$

is a unit ket corresponding to polarization vector $\hat{e}_{u-v}$. Next, using Eqs. (25), (26), (14), and (13), one obtains

$$|\psi_2\rangle = 2^{-1/2}\,(\alpha-\beta)\,(1-\cos\theta)^{1/2}\,|\,\hat{e}_{u-v}\rangle. \tag{27}$$

This device exploits the entanglement of path and polarization qubits. For example, the state $|\psi_{12}\rangle$ of the photon exiting the Wollaston prism is

$$\begin{aligned} |\psi_{12}\rangle \;&=\; |\psi_1\rangle + |\psi_2\rangle = 2^{-1/2}\,(\alpha+\beta)\,(1+\cos\theta)^{1/2}\,|1\rangle\otimes|\,\hat{e}_{u+v}\rangle \\ &\quad + 2^{-1/2}\,(\alpha-\beta)\,(1-\cos\theta)^{1/2}\,|2\rangle\otimes|\,\hat{e}_{u-v}\rangle, \end{aligned} \tag{28}$$

in which the kets $|1\rangle$ and $|2\rangle$ are unit kets corresponding to the upper and lower paths, respectively (to the right of W in Fig. 2). The polarization qubit $\{|u\rangle, |v\rangle\}$ is entangled with the path qubit $\{|1\rangle, |2\rangle\}$.

For ideal photodetectors D_u, D_v, and $\mathrm{D}_?$, it is evident from Fig. 2 and Eq. (9) that one must require

$$P_u = |\psi_6|^2 = \langle\psi_6|\psi_6\rangle = \langle\psi|A_u|\psi\rangle, \tag{29}$$

$$P_v = |\psi_7|^2 = \langle\psi_7|\psi_7\rangle = \langle\psi|A_v|\psi\rangle, \tag{30}$$

and

$$P_? = |\psi_3|^2 = \langle\psi_3|\psi_3\rangle = \langle\psi|A_?|\psi\rangle, \tag{31}$$

respectively, in order that the expectation values of A_u, A_v, and $A_?$, measured by detectors D_u, D_v, and $\mathrm{D}_?$, respectively, equal the probabilities P_u, P_v, and $P_?$ that a photon is incident. From Eqs. (31) and (17), it follows that, up to an irrelevant phase factor, one has

$$|\psi_3\rangle = (\alpha+\beta)\,(\cos\theta)^{1/2}\,|\,\hat{e}_{u+v}\rangle. \tag{32}$$

For a *single* photon incident on beamsplitter BS_1, one can effectively ignore the unused vacuum port of the beamsplitter (see Ref. 23 and also p. 9 of Ref. 35). The transmission coefficient T_1 of beamsplitter BS_1 must then be given by

$$T_1 = \frac{\langle\psi_3|\psi_3\rangle}{\langle\psi_1|\psi_1\rangle}. \tag{33}$$

Therefore, substituting Eqs. (32) and (24) in Eq. (33), one obtains

$$T_1 = 1 - \tan^2(\theta/2). \tag{34}$$

The corresponding reflection coefficient R_1 is

$$R_1 = 1 - T_1 = \tan^2(\theta/2). \tag{35}$$

From Fig. 2, it is also evident that

$$\langle\psi_4|\psi_4\rangle = R_1\langle\psi_1|\psi_1\rangle; \tag{36}$$

substituting Eqs. (24) and (35) in Eq. (36), one obtains

$$\langle\psi_4|\psi_4\rangle = \frac{1}{2}|\alpha+\beta|^2\,(1-\cos\theta)\,. \tag{37}$$

Since the reflection at BS_1 results in a $\pi/2$-phase shift [13–15], resulting in a factor of $\exp(i\pi/2) = i$, it follows from Eq. (37) that

$$|\psi_4\rangle = i2^{-1/2}\,(\alpha+\beta)\,(1-\cos\theta)^{1/2}\,|\,\hat{e}_{u+v}\rangle. \tag{38}$$

Since the polarization rotator R converts polarization in the direction $\hat{e}_{u-v}$ into that in the direction $-\hat{e}_{u+v}$, it follows from Eq. (27) that

$$|\psi_5\rangle = -2^{-1/2}\,(\alpha-\beta)\,(1-\cos\theta)^{1/2}\,|\,\hat{e}_{u+v}\rangle. \tag{39}$$

Since the beamsplitter BS_2 is a 50/50 beamsplitter, its reflection coefficient is

$$R_2 = \frac{1}{2} \tag{40}$$

and its transmission coefficient is

$$T_2 = \frac{1}{2}. \tag{41}$$

It then follows that

$$|\psi_6\rangle = 2^{-1/2}|\psi_5\rangle + i2^{-1/2}|\psi_4\rangle, \tag{42}$$

and

$$|\psi_7\rangle = 2^{-1/2}|\psi_4\rangle + i2^{-1/2}|\psi_5\rangle. \tag{43}$$

Therefore, substituting Eqs. (38) and (39) in Eqs. (42) and (43), one obtains

$$|\psi_6\rangle = -\alpha\,(1-\cos\theta)^{1/2}\,|\,\hat{e}_{u+v}\rangle, \tag{44}$$

and

$$|\psi_7\rangle = i\beta\,(1-\cos\theta)^{1/2}\,|\,\hat{e}_{u+v}\rangle. \tag{45}$$

For an ideal detector, Eq. (29) holds, and by substituting Eq. (44), one gets

$$\langle\psi|A_u|\psi\rangle = |\alpha|^2(1-\cos\theta), \tag{46}$$

consistent with Eq. (15). Similarly, from Eqs. (30) and (45), it follows that

$$\langle\psi|A_v|\psi\rangle = |\beta|^2(1-\cos\theta), \tag{47}$$

consistent with Eq. (16). Thus, the device depicted in Fig. 2 satisfies all the appropriate statistics, Eqs. (29) to (31), and is a faithful all-optical implementation of the POVM given by Eqs. (10) to (12).

Since the quantum key receiver is all-optical, all optical path lengths are only of the order of tens of centimeters, and decohering interactions with the photonic qubits are negligible, it follows that, generally, decoherence is not an issue for this device. However, since it is a very serious issue for many other prospective qubit devices, the following section briefly reviews the physics of quantum decoherence.

4. QUANTUM DECOHERENCE

Consider a two-state system in the absence of environmental interactions. The state vector $|\psi\rangle$ for such a two-state closed system lies in a two-dimensional Hilbert space and is given by

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle , \tag{48}$$

where $|0\rangle$ and $|1\rangle$ are kets representing the two states, here also serving as orthonormal basis vectors, and α_0 and α_1 are complex numbers. Thus, one has

$$\langle 0|0\rangle = \langle 1|1\rangle = 1, \qquad \langle 0|1\rangle = 0. \tag{49}$$

The corresponding density operator is given by [36,16]

$$\rho = |\psi\rangle \langle\psi| . \tag{50}$$

Substituting Eq. (48) in Eq. (50), one obtains for the density operator of this two-state closed system

$$\rho = |\alpha_0|^2 |0\rangle \langle 0| + \alpha_0\alpha_1^* |0\rangle \langle 1| + \alpha_0^*\alpha_1 |1\rangle \langle 0| + |\alpha_1|^2 |1\rangle \langle 1| . \tag{51}$$

The corresponding density matrix is

$$[\rho_{mn}] = [\langle m|\rho|n\rangle] = \begin{bmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* \\ \alpha_0^*\alpha_1 & |\alpha_1|^2 \end{bmatrix} . \tag{52}$$

The diagonal components are the populations, and the off-diagonal components are the coherences [36]. The populations measure the probabilities that the system is in either state, and the coherences measure the amount of interference between the states. The expectation value of any observable represented by an operator A for the two-state system is given by

$$\langle\psi| A |\psi\rangle = \mathrm{Tr}(\rho A) = \sum_{mn} \rho_{mn} A_{nm}, \tag{53}$$

and it is clear that, in general, the coherences are as important as the populations in determining expectation values of observables.

Generally, a system does not exist in absolute isolation, and possible interactions with both the external and internal environments must be taken into account. If the two states of interest are part of an object containing other degrees of freedom, the latter constitute the internal environment, and the external environment is external to the object. For complex systems, the two states of interest might themselves represent two collective observables [37]. Consider now, therefore, a two-state system with state vector $|\psi(t)\rangle$ at time t, including environmental interactions:

$$|\psi(t)\rangle = \alpha_0 |0\rangle \otimes |e_0\rangle + \alpha_1 |1\rangle \otimes |e_1\rangle , \tag{54}$$

in which now the two possible states of the system, $|0\rangle$ and $|1\rangle$, through unitary evolution, have become entangled with the corresponding normalized environmental states $|e_0\rangle$ and $|e_1\rangle$, respectively. The environmental states are, in general, nonorthogonal. Here $\otimes$ denotes the tensor product. The density matrix becomes

$$\begin{aligned} \rho(t) &= |\psi(t)\rangle \langle\psi(t)| \\ &= |\alpha_0|^2 |0\rangle \otimes |e_0\rangle \langle 0| \otimes \langle e_0| + \alpha_0\alpha_1^* |0\rangle \otimes |e_0\rangle \langle 1| \otimes \langle e_1| \\ &\quad + \alpha_0^*\alpha_1 |1\rangle \otimes |e_1\rangle \langle 0| \otimes \langle e_0| + |\alpha_1|^2 |1\rangle \otimes |e_1\rangle \langle 1| \otimes \langle e_1| . \end{aligned} \tag{55}$$

Here and in the following, I use the term "density matrix" interchangeably with "density operator." If we are interested only in what the two-state system is doing,

and not the environment, one need only know the reduced density matrix of the two-state system, with the environmental states traced out [36,37]. For this purpose, choose as environmental basis vectors $|e_0\rangle$ and $|e_0^\perp\rangle$, where

$$\langle e_0^\perp | e_0\rangle = 0, \quad \langle e_0 | e_1\rangle \equiv \cos\,\theta, \quad \langle e_0^\perp | e_1\rangle = \sin\,\theta, \quad \langle e_0 | e_0\rangle = 1, \quad \langle e_1 | e_1\rangle = 1. \tag{56}$$

The reduced density matrix $\rho_s(t)$ of the two-state system is then given by

$$\rho_s(t) = \mathrm{Tr}_e \rho(t) = \langle e_0 | \rho(t) | e_0\rangle + \langle e_0^\perp | \rho(t) | e_0^\perp\rangle\,, \tag{57}$$

where Tr_e denotes the trace over the environmental basis states. Substituting Eq. (55) in Eq. (57), and using Eqs. (56), one obtains

$$\begin{aligned} \rho_s(t) \;=\; & |\alpha_0|^2\,|0\rangle\langle 0| + \alpha_0\alpha_1^*\cos\,\theta\;|0\rangle\langle 1| \\ & + \alpha_0^*\alpha_1\cos\,\theta\;|1\rangle\langle 0| + |\alpha_1|^2\,(\cos^2\theta + \sin^2\theta)\,|1\rangle\langle 1|\,. \end{aligned} \tag{58}$$

If one uses the trigonometric identity $\cos^2\theta + \sin^2\theta = 1$, Eq. (58) becomes

$$\begin{aligned} \rho_s(t) \;=\; & |\alpha_0|^2\,|0\rangle\langle 0| + \alpha_0\alpha_1^*\cos\,\theta\;|0\rangle\langle 1| \\ & + \alpha_0^*\alpha_1\cos\,\theta\;|1\rangle\langle 0| + |\alpha_1|^2\,|1\rangle\langle 1|\,. \end{aligned} \tag{59}$$

Comparing Eq. (59) with Eq. (51), one can see that, as a result of including environmental interactions, the coherences each contain an additional factor of $\cos\,\theta$, the overlap between the environmental states (see Eqs. (56)). The system and its environment evolve, interacting incessantly, and because of decoherence, the overlap between the environmental states $|e_0\rangle$ and $|e_1\rangle$ can become negligible; one then has orthogonalization of the environmental basis states, namely,

$$\cos\,\theta \equiv \langle e_0 | e_1\rangle \longrightarrow 0. \tag{60}$$

In this case, Eq. (59) becomes

$$\rho_s(t) \xrightarrow[\cos\theta\to 0]{} |\alpha_0|^2\,|0\rangle\langle 0| + |\alpha_1|^2\,|1\rangle\langle 1|\,. \tag{61}$$

Decoherence results from interactions with the environment (external and internal). As a result of the decoherence, the reduced density matrix Eq. (61) becomes, effectively, a statistical mixture. The dynamical evolution represented by Eq. (61) is, of course, nonunitary: although the evolution of the total density matrix representing a system and its environment in general evolves unitarily in accordance with the Schrödinger equation, a reduced density matrix does not. Naturally, the details of the evolution (Eq. (61)) depend on the specific structure of the total Hamiltonian of the system together with its environment, including all possible interactions. For macroscopic, mesoscopic, and many microscopic systems, the environment commonly has an enormous (or at least large) Hilbert space and a crowded energy spectrum. Heuristically, in terms of perturbation theory, close energy levels result in high sensitivity to perturbations. Two slightly different perturbations may lead to very different perturbed wave functions, which become orthogonal. Environmental wave functions have many variables, and vanishing wave-function overlap in one variable is sufficient for orthogonality. The Hilbert space of environmental states can become so enormous that two states have a small probability of not being orthogonal [37]. The resulting loss of phase correlations in the high-dimensional environmental configuration space results in orthogonalization of the environmental states that are correlated with the system states. This is the phenomenon of decoherence, resulting in orthogonalization of the off-diagonal components of the reduced density matrix [37–50,1,5]. For a complex macroscopic, or even a mesoscopic, two-state

system, the orthogonalization, Eq. (61), usually occurs very rapidly. The qubits, representing computational degrees of freedom in quantum information processing systems, are two-state systems, and their implementation must be chosen such that interactions with noncomputational internal and external environmental degrees of freedom are small enough that decoherence of the qubits is sufficiently slow. This is, in general, difficult to achieve.

5. QUANTUM GAMES

The classical theory of games [51–55] is currently being generalized to include quantum games [56–59]. These efforts will inevitably lead to a full-fledged quantum theory of games, as well as a variety of quantum game implementations. In the area of quantum communication, optimal copying of quantum states [59] and quantum eavesdropping [27,60,61] can be treated as strategic games between two or more players with the goal of extracting maximum information [57,62].

In order to gain some insight into quantum games, it is instructive to briefly consider a particular quantum game, involving coin flipping [56]. In this game, there are two players, Alice and Eve, and they must flip a penny. However, a real penny would not suffice to play the game, because the game requires a penny that can be in a superposition state of head up and tail up, and of course even if such a state could be produced, it would decohere so quickly that it would be unobservable. Cavity QED (quantum electrodynamics), ion-trap, or NMR (nuclear magnetic resonance) implementations of the game have been suggested [56]. A simple all-optical implementation might be more practical. In any case, any two quantum states forming a qubit would serve as a quantum "penny," and implementations of appropriate unitary transformations acting on the qubit would be used by Alice and Eve to do the flipping.

The object of the game for Alice is to finish with the qubit tail up; that for Eve is to finish head up. Neither player may observe the qubit in the course of the game. The game begins with Alice putting the qubit in a box in the head-up state $|H\rangle$. Next, if the game is played with classical flipping moves only, Eve either flips the qubit, using a transformation (represented by an operator F), or does not flip it (represented by the identity operator $I = 1$). The state is not observed. Next, Alice either does or does not flip the qubit, without observing it. Next, Eve again flips or does not flip the qubit. Alice and Eve finally observe the qubit, and Eve wins if the qubit ends up in the head-up state $|H\rangle$. Otherwise, Alice wins the game.

As an example, for a particular choice of strategies chosen by Alice and Eve, a possible course of the game might be as follows:

$$FIF\,|H\rangle = FI\,|T\rangle = F\,|T\rangle = |H\rangle\,, \tag{62}$$

where $|T\rangle$ denotes the tail-up state of the qubit. Here Eve's first move is to use the flip operation to flip the qubit, which is initially in the state $|H\rangle$. In the next move, Alice does not flip it, and in the last move Eve does flip it. For this example, the qubit ends up in the state $|H\rangle$, and therefore Eve wins the game. The states $|H\rangle$ and $|T\rangle$ can be represented by

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |T\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{63}$$

respectively. The flipping transformation can be represented by the unitary operator

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{64}$$

and not flipping can be represented by the identity operator

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{65}$$

One notes, in passing, that the operator F in Eq. (64) corresponds to the quantum NOT gate operator, to be discussed in Sect. 6. For the above strategies, one has

$$\begin{aligned} FIF|H\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |H\rangle . \end{aligned} \tag{66}$$

In general, however, the game is conceived as a fully quantum game, in which the nth move corresponds to a general unitary operator U_n, represented by a 2×2 unitary matrix for which F and I represent only special cases [56]. Thus

$$U_n = \begin{pmatrix} U_{n11} & U_{n12} \\ U_{n21} & U_{n22} \end{pmatrix}, \tag{67}$$

where the matrix elements $U_{nij}, i, j = 1,2$ are chosen such that

$$U_n U_n^\dagger = 1. \tag{68}$$

An arbitrary quantum strategy might then be represented by the following sequence of unitary operators [56]:

$$U_3 U_2 U_1 |H\rangle = c_1 |H\rangle + c_2 |T\rangle , \tag{69}$$

in which the first move by Eve is represented by U_1, the next move by Alice is represented by U_2, the last move by Eve is represented by U_3, and c_1 and c_2 are complex numbers. The resulting state of the qubit is some superposition state of head up and tail up, as indicated. Suppose [56]

$$U_3 U_2 U_1 |H\rangle \neq |H\rangle . \tag{70}$$

Then Eve can improve her strategy by replacing U_3 by $U_1^{-1}U_2^{-1}$, which is also unitary, since both U_1 and U_2 are. Thus one has

$$U_3 U_2 U_1 |H\rangle = \left(U_1^{-1}U_2^{-1}\right) U_2 U_1 |H\rangle = (U_2 U_1)^{-1} (U_2 U_1) |H\rangle = |H\rangle , \tag{71}$$

and Eve wins. Or, suppose

$$U_3 U_2 U_1 |H\rangle \neq |T\rangle . \tag{72}$$

Then Alice can improve her strategy by replacing U_2 with $U_3^{-1}FU_1^{-1}$, which is unitary, since U_1,U_3, and F are. Thus

$$U_3 U_2 U_1 |H\rangle = U_3 \left(U_3^{-1}FU_1^{-1}\right) U_1 |H\rangle = \boldsymbol{F} |H\rangle = |T\rangle , \tag{73}$$

and Alice wins. But the qubit state $U_3U_2U_1|H\rangle$, when finally observed, cannot be both $|H\rangle$ and $|T\rangle$, and therefore at least one of the players can improve her strategy if the other player does not change hers. It then follows that the overall strategies represented by $U_3U_2U_1$ cannot be an equilibrium, since their strategies are an equilibrium only if neither player can gain by changing strategy unilaterally [56]. It has, however, also been argued that an equilibrium does exist for mixed

quantum strategies in which various strategies occur with some probabilities [56]. Such a game is a manifestly stochastic quantum game.

In other work, it has been argued that in a quantum game version of the classical two-player binary choice game, *Prisoner's Dilemma* [54], there is no dilemma if quantum strategies are allowed [57]. Also, an interesting two-player protocol was conceived for quantum gambling, and it was demonstrated that neither player can increase his earning beyond some limit [58]. In other recent work, the optimal quantum copying problem is informatively described in the form of a game [59].

Although quantum decoherence is not a major issue for small quantum games such as the coin flipping game (at least if one assumes a sufficiently long-lived qubit is successfully implemented), quantum decoherence is certainly a major issue for quantum eavesdropping games, optimal quantum-state copying games, or large-scale quantum games, just as it is for any large-scale quantum information processor.

6. QUANTUM GATES

In order to develop a multi-component qubit device, it is useful to implement various quantum gates. In the following, I present mathematical descriptions of various photonic implementations. First, consider the *quantum* $\sqrt{\text{NOT}}$ *gate* (square-root-of-not gate). As an example, consider the single-photon optical implementation depicted in Fig. 3, consisting of a single photon incident on a beamsplitter along two possible paths, designated by the corresponding states, $|0\rangle$ and $|1\rangle$, or more generally, in a superposition of those two paths. The exit path states are $|0'\rangle$ and $|1'\rangle$. Using the same methods as in Sect. 2, one has

$$|0'\rangle = 2^{-1/2}\,|0\rangle + 2^{-1/2}i\,|1\rangle\,, \tag{74}$$

$$|1'\rangle = 2^{-1/2}i\,|0\rangle + 2^{-1/2}\,|1\rangle\,, \tag{75}$$

or in matrix form,

$$\begin{pmatrix} |0'\rangle \\ |1'\rangle \end{pmatrix} = 2^{-1/2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}. \tag{76}$$

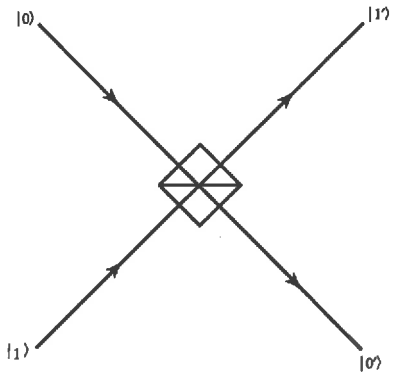

FIGURE 3. Quantum $\sqrt{\text{NOT}}$ gate.

The matrix operator,

$$\sqrt{N} \equiv 2^{-1/2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \tag{77}$$

is known as the "quantum square-root-of-not gate" or quantum $\sqrt{\text{NOT}}$ gate, since

$$\sqrt{N}\sqrt{N} = 2^{-1} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{78}$$

and the matrix operator

$$N \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{79}$$

is the *NOT operator,* which transforms $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$, thus:

$$N \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} |1\rangle \\ |0\rangle \end{pmatrix}. \tag{80}$$

The overall phase factor, $i = e^{i\pi/2}$, in Eq. (78) can be ignored here, and could be physically removed with $-\pi/4$ phase shifters located at both exit ports in Fig. 3. Then, one has, effectively,

$$\sqrt{N}\sqrt{N} = N. \tag{81}$$

This suggests that a *quantum NOT gate* can be constructed from a succession of two quantum $\sqrt{\text{NOT}}$ gates. Note also that the operator N is unitary, since

$$NN^{\dagger} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1. \tag{82}$$

Stacking two beamsplitters successively, as in Fig. 4, produces the succession of two quantum $\sqrt{\text{NOT}}$ gates, as suggested above. The various modes, or paths, are labeled in Fig. 4 by their path states. Using the rules for forming and combining amplitudes (see Sect. 2), one obtains

$$|0''\rangle = 2^{-1/2}\,|0'\rangle + 2^{-1/2}i\,|1'\rangle\,, \tag{83}$$

$$|1''\rangle = 2^{-1/2}i\,|0'\rangle + 2^{-1/2}\,|1'\rangle\,. \tag{84}$$

Next, substituting Eqs. (74) and (75) in Eqs. (83) and (84), one obtains

(85)

$$|0''\rangle = 2^{-1/2}\left(2^{-1/2}\,|0\rangle + 2^{-1/2}i\,|1\rangle\right) + 2^{-1/2}i\left(2^{-1/2}i\,|0\rangle + 2^{-1/2}\,|1\rangle\right) = i\,|1\rangle\,,$$

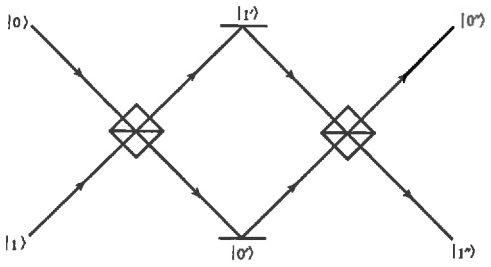

FIGURE 4. Quantum NOT gate.

(86)
$$|1''\rangle = 2^{-1/2}i\left(2^{-1/2}|0\rangle + 2^{-1/2}i|1\rangle\right) + 2^{-1/2}\left(2^{-1/2}i|0\rangle + 2^{-1/2}|1\rangle\right) = i|0\rangle,$$

or, equivalently, in matrix form,

(87)
$$\begin{pmatrix} |0''\rangle \\ |1''\rangle \end{pmatrix} = i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix},$$

which is in agreement with Eq. (78). The common phase factor, $i = e^{i\pi/2}$, can again be ignored, and could be physically removed as indicated previously, or instead by locating $-\pi/2$ phase shifters at both exit ports in Fig. 4. The unitary operator N, Eq. (79), can therefore be faithfully implemented by the device.

Consider next the one-photon device shown in Fig. 5, consisting of one beamsplitter and two $-\pi/2$ phase shifters. The possible paths for a single photon entering from the left are labeled by the corresponding path states. The entering photon may be in path state $|0\rangle$ or $|1\rangle$, or a superposition of the two. From the figure, one can see that the output states $|0'\rangle$ and $|1'\rangle$ are

(88)
$$|0'\rangle = 2^{-1/2}|0\rangle + e^{-i\pi/2}2^{-1/2}i|1\rangle = 2^{-1/2}(|0\rangle + |1\rangle),$$

(89)
$$|1'\rangle = 2^{-1/2}ie^{-i\pi/2}|0\rangle + e^{-i\pi/2}2^{-1/2}e^{-i\pi/2}|1\rangle = 2^{-1/2}(|0\rangle - |1\rangle).$$

Rewriting Eqs. (88) and (89) in matrix form, one has

(90)
$$\begin{pmatrix} |0'\rangle \\ |1'\rangle \end{pmatrix} = 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}.$$

The unitary operator

(91)
$$H = 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

acting on the path qubit, in this example, is called the *Hadamard transform*. The *Hadamard gate*, depicted in Fig. 5, is a one-photon optical implementation of the Hadamard transform acting on a qubit. Two Hadamard gates can be combined to

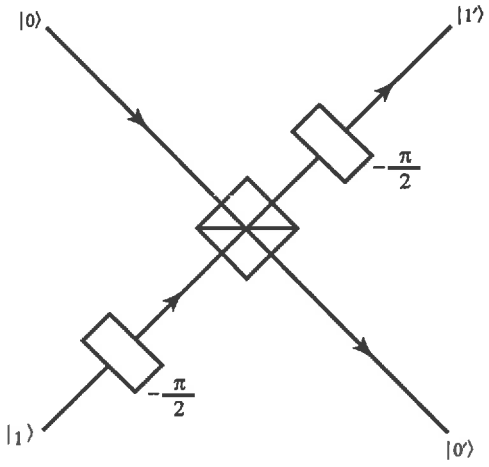

FIGURE 5. Hadamard gate.

form a *single-photon balanced Mach-Zehnder interferometer* [34], as in the following section.

A particularly simple optical example of a single-photon device is depicted in Fig. 6: an optical implementation of the *quantum controlled-NOT gate* (also called the *quantum XOR gate*). It consists of a single polarization rotator that converts horizontal polarization into vertical, and vertical into horizontal, for one of two paths. Here, if a photon with vertical or horizontal polarization enters along path $|0\rangle$, it simply passes to the exit port $|0'\rangle$ unchanged, and if it enters along path $|1\rangle$, its polarization changes from horizontal to vertical, or vertical to horizontal. Thus,

$$|0\rangle\,|{\rightarrow}\rangle \Longrightarrow |0\rangle\,|{\rightarrow}\rangle\,, \tag{92}$$

$$|0\rangle\,|{\uparrow}\rangle \Longrightarrow |0\rangle\,|{\uparrow}\rangle\,, \tag{93}$$

$$|1\rangle\,|{\rightarrow}\rangle \Longrightarrow |1\rangle\,|{\uparrow}\rangle\,, \tag{94}$$

$$|1\rangle\,|{\uparrow}\rangle \Longrightarrow |1\rangle\,|{\rightarrow}\rangle\,, \tag{95}$$

in which tensor products are implicit. Here, the location (path) qubit is the control, and the polarization qubit is the target. Conditional dynamics occurs because the polarization of the photon flips, conditionally on its location. The quantum controlled-NOT gate is a two-qubit gate, the two qubits, in this case, being path and polarization qubits. The transformation Eqs. (92) to (95) can also be characterized as follows in terms of Boolean arithmetic (expressed in binary). If the horizontal and vertical polarization states are chosen to encode Boolean states $|0\rangle$ and $|1\rangle$, respectively, thus

$$|{\rightarrow}\rangle = |0\rangle\,, \quad |{\uparrow}\rangle = |1\rangle\,, \tag{96}$$

and also, the path states $|0\rangle$ and $|1\rangle$ encode the binary Boolean states $|0\rangle$ and $|1\rangle$, respectively, then the transformations (92) to (95) can be written as follows:

$$|0\rangle\,|0\rangle \Longrightarrow |0\rangle\,|0\rangle\,, \tag{97}$$

$$|0\rangle\,|1\rangle \Longrightarrow |0\rangle\,|1\rangle\,, \tag{98}$$

$$|1\rangle\,|0\rangle \Longrightarrow |1\rangle\,|1\rangle\,, \tag{99}$$

$$|1\rangle\,|1\rangle \Longrightarrow |1\rangle\,|0\rangle\,. \tag{100}$$

Here, the first ket refers to a path state, the second ket refers to a polarization state, and the order must be maintained. Equations (97) to (100) can be succinctly represented as follows:

$$|n\rangle\,|m\rangle \Longrightarrow |n\rangle\,|n \oplus m\rangle\,, \tag{101}$$

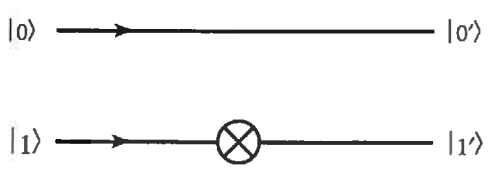

FIGURE 6. Quantum controlled-NOT gate.

with $n \in \{0,1\}$, $m \in \{0,1\}$, and $\oplus$ denoting addition modulo 2. The operation in Eq. (101) is called the *controlled NOT*. In matrix notation, Eqs. (92) to (95), expressing the output states in terms of the possible input states, may be represented as follows:

$$\begin{pmatrix} |0'\rangle_1 \\ |0'\rangle_2 \\ |1'\rangle_1 \\ |1'\rangle_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} |0\rangle\,|\rightarrow\rangle \\ |0\rangle\,|\uparrow\rangle \\ |1\rangle\,|\rightarrow\rangle \\ |1\rangle\,|\uparrow\rangle \end{pmatrix}. \tag{102}$$

The matrix operator appearing in Eq. (102) is known as the quantum controlled-NOT (or XOR) operator,

$$X \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{103}$$

Combinations of the controlled-NOT operation and arbitrary single-qubit rotations can generate any unitary operation [4]. Although decoherence is not an issue for one-time gate operation, in the case of gate implementations for possible use in large-scale quantum computer circuits, the gate error rate must be extremely small for successful computation.

7. SINGLE-PHOTON BALANCED MACH-ZEHNDER INTERFEROMETER

Consider the succession of two Hadamard gates, depicted in Fig. 7. Here a single photon is incident along path $|0\rangle$, path $|1\rangle$, or a superposition of both paths. One has

$$|0''\rangle = e^{-i\pi/2}2^{-1/2}i\,|1'\rangle + 2^{-1/2}\,|0'\rangle = 2^{-1/2}\left(|1'\rangle + |0'\rangle\right), \tag{104}$$

$$|1''\rangle = e^{-i\pi/2}2^{-1/2}e^{-i\pi/2}\,|1'\rangle + 2^{-1/2}ie^{-i\pi/2}\,|0'\rangle = 2^{-1/2}\left(-|1'\rangle + |0'\rangle\right). \tag{105}$$

Next, substituting Eqs. (88) and (89) in Eqs. (104) and (105), one obtains

$$|0''\rangle = 2^{-1/2}\left(2^{-1/2}\left(|0\rangle - |1\rangle\right) + 2^{-1/2}\left(|0\rangle + |1\rangle\right)\right) = |0\rangle, \tag{106}$$

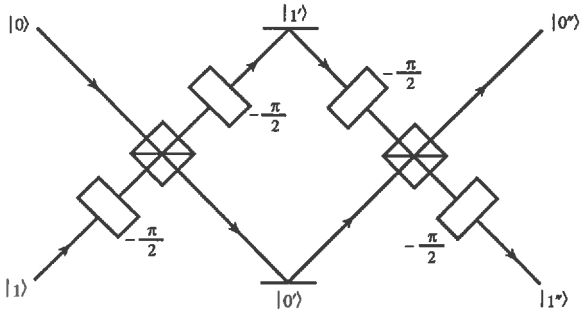

FIGURE 7. Single-photon Mach-Zehnder interferometer.

$$|1''\rangle = 2^{-1/2}\left(-2^{-1/2}(|0\rangle - |1\rangle) + 2^{-1/2}(|0\rangle + |1\rangle)\right) = |1\rangle\,. \tag{107}$$

Thus

$$\begin{pmatrix} |0''\rangle \\ |1''\rangle \end{pmatrix} = \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix}. \tag{108}$$

It is also clear that this must be the case, since, according to Eq. (91), one has

$$HH = 2^{-1}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{109}$$

which is the identity. Thus, the succession of two Hadamard gates produces a balanced single-photon Mach-Zehnder interferometer. If the photon enters along path $|0\rangle$, it also exits in the state $|0''\rangle = |0\rangle$. If it enters in $|1\rangle$, it exits in $|1\rangle$.

8. QUBIT ENTANGLERS

By sandwiching a quantum controlled-NOT gate between two Hadamard gates, one obtains an example of a two-qubit entangler, which entangles a location qubit with a polarization qubit. The two-qubit entangler is shown in Fig. 8. If the input state is $|0\rangle\,|{\rightarrow}\rangle$, one can see from the figure, by taking into account the effect of the first beamsplitter and the phase shifters, that

$$|0'\rangle_1 = 2^{-1/2}\,|{\rightarrow}\rangle\,, \tag{110}$$

$$|1'\rangle_1 = 2^{-1/2}e^{-i\pi/2}i\,|{\rightarrow}\rangle = 2^{-1/2}\,|{\rightarrow}\rangle\,. \tag{111}$$

The index 1 merely distinguishes the particular choice of input state. Therefore, because of the polarization rotator R, one has

$$|0''\rangle_1 = 2^{-1/2}\,|{\rightarrow}\rangle\,, \tag{112}$$

$$|1''\rangle_1 = 2^{-1/2}\,|{\uparrow}\rangle\,. \tag{113}$$

Also, using Eqs. (88) and (89), one has

$$|0'''\rangle_1 = 2^{-1/2}(|0''\rangle_1 + |1''\rangle_1)\,, \tag{114}$$

$$|1'''\rangle_1 = 2^{-1/2}(|0''\rangle_1 - |1''\rangle_1)\,. \tag{115}$$

Next, substituting Eqs. (112) and (113) in (114) and (115), one obtains

$$|0'''\rangle_1 = 2^{-1}(|{\rightarrow}\rangle + |{\uparrow}\rangle)\,, \tag{116}$$

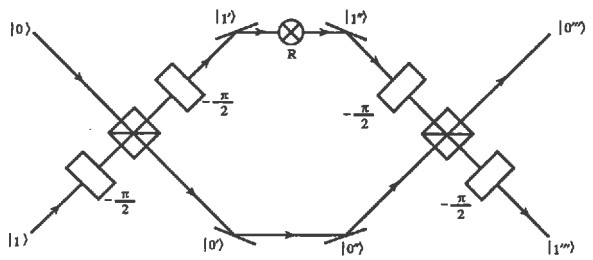

FIGURE 8. Two-qubit entangler.

$$|1'''\rangle_1 = 2^{-1}\left(|{\rightarrow}\rangle - |{\uparrow}\rangle\right). \tag{117}$$

The final state is then given by combining Eqs. (116) and (117), namely,

$$|\psi_1\rangle = |0'''\rangle_1 + |1'''\rangle_1 = 2^{-1}\left(|{\rightarrow}\rangle + |{\uparrow}\rangle\right)|e_{0'''}\rangle + 2^{-1}\left(|{\rightarrow}\rangle - |{\uparrow}\rangle\right)|e_{1'''}\rangle, \tag{118}$$

where $|e_{0'''}\rangle$ and $|e_{1'''}\rangle$ are unit kets corresponding to paths $|0'''\rangle$ and $|1'''\rangle$, respectively. Thus, in the case of the input state $|0\rangle\,|{\rightarrow}\rangle$, one has

$$|0\rangle\,|{\rightarrow}\rangle \Longrightarrow |\psi_1\rangle = 2^{-1}\left(|e_{0'''}\rangle\,|{\rightarrow}\rangle + |e_{0'''}\rangle\,|{\uparrow}\rangle + |e_{1'''}\rangle\,|{\rightarrow}\rangle - |e_{1'''}\rangle\,|{\uparrow}\rangle\right). \tag{119}$$

Thus, the qubit entangler converts the unentangled input state $|0\rangle\,|{\rightarrow}\rangle$ to a state in which the polarization qubit $(|{\rightarrow}\rangle, |{\uparrow}\rangle)$ is entangled with the path qubit $(|e_{0'''}\rangle, |e_{1'''}\rangle)$. Similarly, one obtains

$$|0\rangle\,|{\uparrow}\rangle \Longrightarrow |\psi_2\rangle = 2^{-1}\left(|e_{0'''}\rangle\,|{\rightarrow}\rangle + |e_{0'''}\rangle\,|{\uparrow}\rangle - |e_{1'''}\rangle\,|{\rightarrow}\rangle + |e_{1'''}\rangle\,|{\uparrow}\rangle\right), \tag{120}$$

$$|1\rangle\,|{\rightarrow}\rangle \Longrightarrow |\psi_3\rangle = 2^{-1}\left(|e_{0'''}\rangle\,|{\rightarrow}\rangle - |e_{0'''}\rangle\,|{\uparrow}\rangle + |e_{1'''}\rangle\,|{\rightarrow}\rangle + |e_{1'''}\rangle\,|{\uparrow}\rangle\right), \tag{121}$$

$$|1\rangle\,|{\uparrow}\rangle \Longrightarrow |\psi_4\rangle = 2^{-1}\left(-|e_{0'''}\rangle\,|{\rightarrow}\rangle + |e_{0'''}\rangle\,|{\uparrow}\rangle + |e_{1'''}\rangle\,|{\rightarrow}\rangle + |e_{1'''}\rangle\,|{\uparrow}\rangle\right), \tag{122}$$

for input states $|0\rangle\,|{\uparrow}\rangle$, $|1\rangle\,|{\rightarrow}\rangle$, and $|1\rangle\,|{\uparrow}\rangle$, respectively. The input states have become entangled states of path and polarization qubits.

In each case, Eqs. (119) to (122), the input state is separable (factorizable) into two factors, each corresponding to a state of only one qubit. Each input state is a single product of a path state with a polarization state. The input states are not entangled.

The output states, however, are not factorizable: each is a superposition of product states that is nonseparable into a single product of a path state and a polarization state. The output states are entangled.

The four entangled states $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, and $|\psi_4\rangle$ can be summarized in matrix form as follows:

$$\begin{pmatrix} |\psi_1\rangle \\ |\psi_2\rangle \\ |\psi_3\rangle \\ |\psi_4\rangle \end{pmatrix} = 2^{-1}\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}\begin{pmatrix} |e_{0'''}\rangle\,|{\rightarrow}\rangle \\ |e_{0'''}\rangle\,|{\uparrow}\rangle \\ |e_{1'''}\rangle\,|{\rightarrow}\rangle \\ |e_{1'''}\rangle\,|{\uparrow}\rangle \end{pmatrix}. \tag{123}$$

Next consider, for example, two qubits, each of which can be in two states. Qubit 1 can be in the orthonormal states $|0\rangle_1$ or $|1\rangle_1$, and qubit 2 can be in orthonormal states $|0\rangle_2$ or $|1\rangle_2$, where the subscripts on the kets distinguish the two qubits. The general combined state of the two qubits can be written as

$$|\psi\rangle = \alpha\,|0\rangle_1\,|0\rangle_2 + \beta\,|0\rangle_1\,|1\rangle_2 + \gamma\,|1\rangle_1\,|0\rangle_2 + \delta\,|1\rangle_1\,|1\rangle_2 = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}. \tag{124}$$

(Here, tensor products are implicit, and the notation does not explicitly distinguish between a ket and its representative [12].) Suppose that the initial combined state is given by a simple product of states, namely,

$$|\psi(0)\rangle = |0\rangle_1\,|0\rangle_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{125}$$

This state is not entangled. It is separable into two factors, each corresponding to a state of one qubit. But then, as a result of prescribed controlled interactions between the two particles (which, according to quantum mechanics, can be described by some unitary operator U), the combined state of the two qubits, after a prescribed period of time, will, in general, be

$$|\psi(t)\rangle = U(t)\,|\psi(0)\rangle = \begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ U_{21} & U_{22} & U_{23} & U_{24} \\ U_{31} & U_{32} & U_{33} & U_{34} \\ U_{41} & U_{42} & U_{43} & U_{44} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{126}$$

expressed in terms of the matrix elements of the unitary operator U. Next, if we perform the matrix multiplication, Eq. (126) becomes

$$|\psi(t)\rangle = U_{11}\,|0\rangle_1\,|0\rangle_2 + U_{21}\,|0\rangle_1\,|1\rangle_2 + U_{31}\,|1\rangle_1\,|0\rangle_2 + U_{41}\,|1\rangle_1\,|1\rangle_2\,. \tag{127}$$

The state is no longer separable. It is an entangled state. Any entanglement of the two qubits can, in principle, be achieved by appropriate choice of interaction Hamiltonian between the qubits, thereby determining the appropriate unitary operator U. Thus controlled interactions between two qubits, described by a prescribed unitary operator U, produce a prescribed entangled state. A *qubit entangler* is an implementation of this process.

More generally, it is now well known that controlled qubit entanglement can be produced generically in at least three ways: (1) prescribed and controlled interactions between the qubits, (2) entangled-particle sources, such as Einstein-Podolsky-Rosen (EPR) pair sources, and (3) entanglement swapping. EPR-pair sources are discussed in Sect. 9, and entanglement swapping is discussed in Sect. 13. Concerning method (1), interactions of the qubits with the environment lead, of course, to entanglement with the environment and decoherence, while interactions between the qubits themselves in a controlled way can produce prescribed entanglements. The latter is the basis for networks of quantum gates in a quantum computer.

9. EPR-PAIR SOURCES

Consider the production of entanglement, for example, in a particular *EPR-pair source* [63,64]. This is a source of two Einstein-Podolsky-Rosen (EPR) correlated particles. When an ultraviolet (UV) laser beam is incident on the nonlinear crystal beta-barium borate, one of the photons may be absorbed, with small probability, by interaction with the crystal atoms, and produce a pair of photons of lower frequency (conserving energy). The two photons are emitted into the surface of two cones whose axes (together with the path of the original UV photon) lie in the same plane, and the axes of the two cones make equal and opposite angles with the path of the UV photon (conserving momentum). This is parametric down-conversion. In type II parametric down-conversion, one of the two photons produced has vertical polarization ($\uparrow$), and the other has horizontal polarization ($\rightarrow$). The device can be configured with the two emission cones overlapping, so that the photons carry no individual polarization. Along the two directions where the cones overlap, the state of the two photons is in the entangled state

$$|\psi\rangle = 2^{-1/2}\left(|\rightarrow\rangle_1\,|\uparrow\rangle_2 + e^{i\alpha}\,|\uparrow\rangle_1\,|\rightarrow\rangle_2\right), \tag{128}$$

where the subscripts on the kets distinguish the two particles, and the parameter α is a relative phase resulting from crystal birefringence. This is a general EPR-pair

state. Here, each of the two particles represents a qubit by its two polarization states. Thus, in the state represented by Eq. (128), the two polarization qubits are entangled. Also, the two particles will generally have two separate locations. By controlling the value of the parameter α in Eq. (128), one can produce various EPR-pair entangled states. For EPR sources to be applied to quantum communication in any practical way, the decoherence issue must be addressed: decoherence strongly limits the storage time for EPR correlated states.

10. BELL-STATE SYNTHESIZER

The EPR-pair source also serves as an example of a *Bell-state synthesizer.* Using a birefringent phase shifter, one can set the value of the relative phase parameter α in the EPR-pair state of Eq. (128) to the values 0 and π [63]. Also, a half-wave plate in one path can change horizontal to vertical polarization and vice versa. In this way, the following four EPR *Bell states* can be produced:

$$|\psi^{\pm}\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle_1\,|{\uparrow}\rangle_2 \pm |{\uparrow}\rangle_1\,|{\rightarrow}\rangle_2\right), \tag{129}$$

$$|\phi^{\pm}\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle_1\,|{\rightarrow}\rangle_2 \pm |{\uparrow}\rangle_1\,|{\uparrow}\rangle_2\right). \tag{130}$$

The four states given by Eqs. (129) and (130) are widely known as Bell states. The Bell states form a maximally entangled orthonormal basis for the Hilbert space of the two qubits. *Maximal entanglement* means that all information is carried by both particles jointly, and no information is stored in an individual particle. The parametric down-conversion EPR-pair source is thereby made into a *Bell-state source.*

11. QUANTUM DENSE CODER

Classically, with two pennies, each having two possible states, head up or tail up, one can encode two bits of information, represented by (H, H), (H, T), (T, H), and (H, H). Here the state of one of the pennies is the first entry, and the state of the other penny is the second entry. This allows four encodings, or $\log_2 4 = 2$ bits. In *quantum dense coding* [65], two entangled two-state systems are used to encode information. It has been demonstrated experimentally [66] that, with quantum dense coding, it is presently feasible to transmit one of three messages by manipulating only one of two entangled qubits shared between a transmitter Bob and a receiver Alice. In other words, by manipulating only one of two entangled qubits, Bob can transmit $\log_2 3 = 1.58$ bits, namely a *trit,* to Alice.

In principle, however, one of four messages (two bits) could be transmitted by manipulating only one of the qubits. With two photonic qubits, each having two polarization states (vertical polarization represented by the ket $|{\uparrow}\rangle$, and horizontal polarization represented by the ket $|{\rightarrow}\rangle$), the two bits can be encoded in entangled superposition states, such as

$$|\psi^{+}\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle\,|{\uparrow}\rangle + |{\uparrow}\rangle\,|{\rightarrow}\rangle\right). \tag{131}$$

Here on the right-hand side, tensor products are implicit, and kets are taken to be ordered with the first and second kets in each term representing the first and second particles, respectively. An analogous entangled state would never be seen with two pennies, because of quantum decoherence. The state $|\psi^{+}\rangle$, along with three other

states, forms a maximally entangled basis for two independent particles, the *Bell basis*. The other three states are

$$|\psi^-\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle\,|{\uparrow}\rangle - |{\uparrow}\rangle\,|{\rightarrow}\rangle\right), \tag{132}$$

$$|\phi^+\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle\,|{\rightarrow}\rangle + |{\uparrow}\rangle\,|{\uparrow}\rangle\right), \tag{133}$$

$$|\phi^-\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle\,|{\rightarrow}\rangle - |{\uparrow}\rangle\,|{\uparrow}\rangle\right). \tag{134}$$

Equations (131) to (134) are the four Bell states, Eqs. (129) and (130) with suppressed indices, and with ket order distinguishing the two qubits. Maximal entanglement between the two photons means that all information is carried by the photons jointly, and no information is stored in any individual photon. Note that for each of the four states, Eqs. (131) to (134), each photon is unpolarized by itself, since it is equally likely to have horizontal or vertical polarization. Also, the states are orthonormal; for example,

$$\langle\psi^+|\phi^-\rangle = 2^{-1}\left(\langle{\rightarrow}|\,\langle{\uparrow}| + \langle{\uparrow}|\,\langle{\rightarrow}|\right)\left(|{\rightarrow}\rangle\,|{\rightarrow}\rangle - |{\uparrow}\rangle\,|{\uparrow}\rangle\right) = 0. \tag{135}$$

The symmetries of the entanglement are made more evident when we summarize the four Bell basis states, Eqs. (131) to (134), as follows (as in Eqs. (129) and (130)):

$$|\psi^\pm\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle\,|{\uparrow}\rangle \pm |{\uparrow}\rangle\,|{\rightarrow}\rangle\right), \tag{136}$$

$$|\phi^\pm\rangle = 2^{-1/2}\left(|{\rightarrow}\rangle\,|{\rightarrow}\rangle \pm |{\uparrow}\rangle\,|{\uparrow}\rangle\right). \tag{137}$$

With these four states, two bits of information can still be encoded. However, in the encoding with entangled states, none of the qubits carries well-defined information. For example, if the states $|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle$, and $|\phi^-\rangle$ are chosen to encode messages 1, 2, 3, and 4, respectively, then one can see directly from Eqs. (136) and (137) that performing a local measurement of the polarization state of one of the two qubits (which may be spatially separated) is not sufficient to determine the message. The information is stored in the entanglement. It is encoded globally into relations between the two qubits, since the two particles are generally spatially separated. To obtain the information, one needs to know about the states of both qubits.

Although the four Bell states $|\psi^\pm\rangle$ and $|\phi^\pm\rangle$ can still encode only two bits of information, the encoding can be accomplished by manipulation of only one of the particles. Suppose Bob and Alice each share one of two EPR particles produced in the state $|\psi^+\rangle$, for example, by a Bell state source, as in the previous section. Bob, who wishes to transmit a message to Alice, performs one out of four possible unitary transformations on his particle alone, represented by the first ket in each term in the state $|\psi^+\rangle$. The four operators are

(1) the identity operator, for which

$$|\psi^+\rangle \longrightarrow |\psi^+\rangle, \tag{138}$$

(2) the polarization interchange ($|{\uparrow}\rangle \Longleftrightarrow |{\rightarrow}\rangle$), for which

$$|\psi^+\rangle \longrightarrow 2^{-1/2}\left(|{\uparrow}\rangle\,|{\uparrow}\rangle + |{\rightarrow}\rangle\,|{\rightarrow}\rangle\right) = |\phi^+\rangle, \tag{139}$$

(3) the polarization-dependent phase shift ($e^{i\alpha}$ for $|{\uparrow}\rangle$ and $e^{i(\alpha+\pi)}$ for $|{\rightarrow}\rangle$, where α is some phase), for which

$$|\psi^+\rangle \longrightarrow 2^{-1/2}\left(-e^{i\alpha}\,|{\rightarrow}\rangle\,|{\uparrow}\rangle + e^{i\alpha}\,|{\uparrow}\rangle\,|{\rightarrow}\rangle\right) = -e^{i\alpha}\,|\psi^-\rangle \tag{140}$$

(the factor of $-e^{i\alpha}$ is an unimportant overall phase factor), and, finally,

(4) the polarization-dependent phase shift ($e^{i\alpha}$ for $|\uparrow\rangle$ and $e^{i(\alpha+\pi)}$ for $|\rightarrow\rangle$) and polarization interchange, for which

$$|\psi^+\rangle \longrightarrow 2^{-1/2}\left(-e^{i\alpha}|\uparrow\rangle|\uparrow\rangle + e^{i\alpha}|\rightarrow\rangle|\rightarrow\rangle\right) = e^{i\alpha}|\phi^-\rangle \tag{141}$$

(again, there is an irrelevant overall phase factor).

The above four unitary operations are commonly referred to as (1) the identity operator, (2) the bit flip, (3) the phase shift, and (4) the combined phase shift/bit flip, respectively. These four manipulations by Bob of his particle result in the four orthogonal Bell states, which can represent four distinguishable messages: two bits of information. The information capacity of the transmission channel is therefore two bits, compared to the classical maximum of one bit. Alice must, of course, measure the Bell state to complete the information transfer. To do this, she uses a *Bell state analyzer*, as discussed in the following section.

A schematic diagram of a *quantum dense coder* is shown in Fig. 9. In the figure, BSS designates the Bell-state source of two entangled photons to be shared by Bob and Alice. BSE designates the Bell-state encoder with which Bob performs one of the four operations on his photon, thereby projecting the pair into a particular Bell state. He next sends the photon to Alice, who measures the state of the pair using the Bell-state analyzer BSA. Bob can thus, in principle, send two bits of information to Alice by manipulating only one of the two shared EPR photons.

Thus, dense quantum coding can, in principle, double the transmission channel information capacity. However, to date, existing Bell state analyzers can measure only three of the four Bell states, and therefore Alice can read only three different messages (1 trit). Measurement of all four Bell states awaits the development of a gate-enabling robust nonlinear interaction between two qubits [67].

Nonlinear response can be very effective for strong fields consisting of many photons [68,69]; however, at the few-photon level, the fields are far too weak for nonlinear response to be exploited. For example, combining two photons conditionally in a nonlinear crystal has an efficiency that is far too low. Several possible approaches to developing the required gate are being pursued, including cooperative two-photon interactions with pairs of atoms in a medium [70–72] and cavity-QED techniques [73–75]. The development of a robust two-qubit gate is also needed for the development of quantum computers.

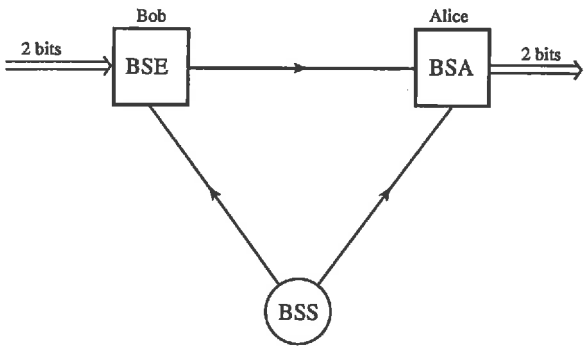

FIGURE 9. Quantum dense coder.

Quantum decoherence is an impediment to the useful implementation of dense coding, because it limits transmission range and state storage time. However, quantum error correction methods may be implemented to change this (see Sect. 21).

12. BELL-STATE ANALYZER

The *Bell-state analyzer* addressed here exploits the quantum statistics of two qubits interacting with a beamsplitter [67,76]. Note first that the state $|\psi^-\rangle$, Eq. (132), is antisymmetric in the interchange of the two particles:

$$|\psi^-\rangle = 2^{-1/2}\,(|{\rightarrow}\rangle\,|{\uparrow}\rangle - |{\uparrow}\rangle\,|{\rightarrow}\rangle) \longrightarrow 2^{-1/2}\,(|{\uparrow}\rangle\,|{\rightarrow}\rangle - |{\rightarrow}\rangle\,|{\uparrow}\rangle) = -\,|\psi^-\rangle\,. \tag{142}$$

The other three Bell states, Eqs. (131), (133), and (134), are symmetric under particle interchange:

$$|\psi^+\rangle = 2^{-1/2}\,(|{\rightarrow}\rangle\,|{\uparrow}\rangle + |{\uparrow}\rangle\,|{\rightarrow}\rangle) \longrightarrow 2^{-1/2}(|{\uparrow}\rangle\,|{\rightarrow}\rangle + |{\rightarrow}\rangle\,|{\uparrow}\rangle) = |\psi^+\rangle\,; \tag{143}$$

and clearly,

$$|\phi^\pm\rangle = 2^{-1/2}\,(|{\rightarrow}\rangle\,|{\rightarrow}\rangle \pm |{\uparrow}\rangle\,|{\uparrow}\rangle) \longrightarrow |\phi^\pm\rangle\,. \tag{144}$$

The connection between spin and statistics [77,78] is that (1) half-integer spin particles are fermions and obey Fermi-Dirac statistics: that is, their total wave function is completely antisymmetric under interchange of particles; and (2) integer spin particles are bosons and obey Bose-Einstein statistics: that is, their total wave function is completely symmetric under interchange of the particles. Photons have spin-one, namely integer spin, and are therefore bosons and obey Bose-Einstein statistics. Therefore, the two-photon wave function must be totally symmetric. The total wave function has a spatial part and a spin part (polarization corresponds to spin [5]). It follows that for the two photons in the polarization Bell state $|\psi^-\rangle$, which, according to Eq. (142), is antisymmetric, the spatial part of the wave function must also be antisymmetric, so that the total wave function is completely symmetric. To see this, note that under particle interchange, one has, letting $|\Psi_A\rangle$ denote the antisymmetric spatial part of the wave function,

$$|\Psi_A\rangle\,|\psi^-\rangle \longrightarrow (-\,|\Psi_A\rangle)(-\,|\psi^-\rangle) = |\Psi_A\rangle\,|\psi^-\rangle\,. \tag{145}$$

Similarly, for the two photons in the symmetric polarization states $|\psi^+\rangle$ or $|\phi^\pm\rangle$, the spatial part of the wave function must also be symmetric, for under the interchange, one has, letting $|\Psi_S\rangle$ denote the symmetric spatial part of the wave function,

$$|\Psi_S\rangle\,|\psi^+\rangle \longrightarrow (+\,|\Psi_S\rangle)\,(+\,|\psi^+\rangle) = |\Psi_S\rangle\,|\psi^+\rangle\,, \tag{146}$$

$$|\Psi_S\rangle\,|\phi^\pm\rangle \longrightarrow (+\,|\Psi_S\rangle)\,(+\,|\phi^\pm\rangle) = |\Psi_S\rangle\,|\phi^\pm\rangle\,. \tag{147}$$

Next, consider two photons (see Fig. 10) incident from the left on a 50/50 beamsplitter, serving as a partial Bell-state analyzer. The mode $|1\rangle$ represents the upper path, and the mode $|0\rangle$ represents the lower path. Coincidence detection (designated by C in the figure) is performed at the two output ports of the beamsplitter. If one could ignore statistics, then the mode state $|1\rangle\,|0\rangle$ for the two particles, with one particle in each spatial mode, could be expressed as

$$|1\rangle\,|0\rangle = 2^{-1}\,[|1\rangle\,|0\rangle + |0\rangle\,|1\rangle] + 2^{-1}\,[|1\rangle\,|0\rangle - |0\rangle\,|1\rangle]\,. \tag{148}$$

I have used a trivial algebraic identity to rewrite the function in terms of a symmetric part and an antisymmetric part, corresponding to the first and second bracketed

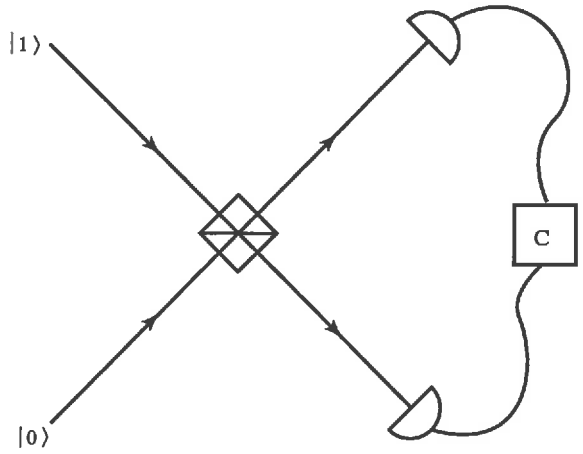

FIGURE 10. Bell-state analyzer.

terms in Eq. (148). However, depending on the symmetry of the polarization state of the two photons, only the symmetric or the antisymmetric part of the two-photon spatial-mode state can be nonvanishing. Thus, the possible normalized spatial-mode states for the two photons incident from the left are either the normalized symmetric state,

$$|\Psi_S\rangle = 2^{-1/2}(|1\rangle\,|0\rangle + |0\rangle\,|1\rangle), \tag{149}$$

or the normalized antisymmetric state,

$$|\Psi_A\rangle = 2^{-1/2}(|1\rangle\,|0\rangle - |0\rangle\,|1\rangle). \tag{150}$$

Since the two-photon total wave function must be completely symmetric, the total state, including both spatial and polarization parts, must be one of the following four states:

$$|\psi^+\rangle\,|\Psi_S\rangle\,,\ |\psi^-\rangle\,|\Psi_A\rangle\,,\ |\phi^+\rangle\,|\Psi_S\rangle\,,\ |\phi^-\rangle\,|\Psi_S\rangle\,. \tag{151}$$

Only the second state, $|\psi^-\rangle\,|\Psi_A\rangle$, is antisymmetric in both its polarization and spatial parts.

The beamsplitter does not affect the photon polarization state. Also, it can be shown that for all three of the states involving the polarization-symmetric part $|\Psi_S\rangle$, both photons emerge together in only one of the exit ports of the beamsplitter [67,79]; therefore, the coincidence detectors will not respond to those three states. It is also true that the antisymmetric state $|\Psi_A\rangle$ is an eigenstate of the beamsplitter [67,80], which I demonstrate explicitly below. It follows that the beamsplitter can discriminate the state $|\psi^-\rangle\,|\Psi_A\rangle$ from all the other states, since only that state will register coincidences [67,80]. Furthermore, for $|\psi^+\rangle$, the two photons have different polarizations, while for both $|\phi^+\rangle$ and $|\phi^-\rangle$, both photons have the same polarization state. Therefore, by performing polarization measurements, one can decide whether the photons are in the state $|\psi^+\rangle$ or one of the remaining states $|\phi^+\rangle$ or $|\phi^-\rangle$. To complete the Bell-state analysis, a robust optical element involving nonlinear interactions is needed (see the previous section) [70–72,73].

It is appropriate to independently demonstrate that the spatially antisymmetric state $|\Psi_A\rangle$ is, in fact, an eigenstate of the beamsplitter. The beamsplitter does not

change this state, except for an irrelevant overall phase factor. To see this, one can use the following vector representation of $|\Psi_A\rangle$, Eq. (150), in terms of vectors $\binom{1}{0}$ and $\binom{0}{1}$, representing spatial modes $|1\rangle$ and $|0\rangle$, respectively; thus

$$|\Psi_A\rangle = 2^{-1/2}\left[\binom{1}{0}\binom{0}{1} - \binom{0}{1}\binom{1}{0}\right]. \tag{152}$$

Tensor products are again implicit here. A general state

$$\binom{a}{b} = a\binom{1}{0} + b\binom{0}{1}, \tag{153}$$

incident on the beamsplitter, can be depicted as in Fig. 11. Since the probability amplitude [9–12] that a photon enters the beamsplitter on the upper left is a, and that it enters on the lower left is b, then the amplitude that it exits on the upper right is $2^{-1/2}ia + 2^{-1/2}b$ (the factor of $2^{-1/2}$ is due to the 50/50 beamsplitter, and the factor of i is due to the reflection [13–15]). Analogously, the amplitude that the photon exits on the lower right is $2^{-1/2}a + 2^{-1/2}ib$. The exit state can therefore be represented by

$$2^{-1/2}\binom{ia+b}{a+ib} = 2^{-1/2}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}. \tag{154}$$

Thus, the effect of the beamsplitter is represented by the operator

$$M = 2^{-1/2}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}. \tag{155}$$

The operator M is unitary:

$$MM^\dagger = 2^{-1}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}\begin{pmatrix} -i & 1 \\ 1 & -i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1. \tag{156}$$

It then follows that the effect of the beamsplitter on the spatially antisymmetric state of two photons, Eq. (152), is faithfully represented by

$$|\Psi'_A\rangle = MM\,|\Psi_A\rangle\,, \tag{157}$$

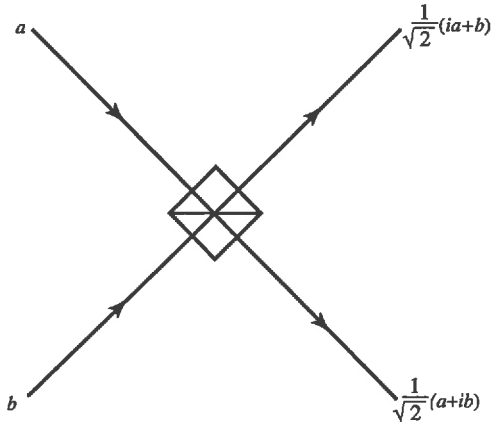

FIGURE 11. Beamsplitter input-output modes.

in which $|\Psi'_A\rangle$ is the output state, the first operator M represents the beamsplitter acting on the first photon appearing in the expression for the Bell state, and the second operator M represents the same beamsplitter acting on the second photon (tensor products are again implicit). Thus, using Eqs. (155), (152), and (157), one has

$$\begin{aligned}
|\Psi'_A\rangle &= 2^{-1/2}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} 2^{-1/2}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} 2^{-1/2}\left[\binom{1}{0}\binom{0}{1} - \binom{0}{1}\binom{1}{0}\right] \\
&= 2^{-3/2}\left[\binom{i}{1}\binom{1}{i} - \binom{1}{i}\binom{i}{1}\right] \\
&= 2^{-3/2}\left\{\left[i\binom{1}{0} + \binom{0}{1}\right]\left[\binom{1}{0} + i\binom{0}{1}\right]\right. \\
&\quad \left. - \left[\binom{1}{0} + i\binom{0}{1}\right]\left[i\binom{1}{0} + \binom{0}{1}\right]\right\} \\
&= -2^{-1/2}\left[\binom{1}{0}\binom{0}{1} - \binom{0}{1}\binom{1}{0}\right] \\
&= -|\Psi_A\rangle . \qquad (158)
\end{aligned}$$

One concludes that, in fact, the spatially antisymmetric state $|\Psi_A\rangle$ is an eigenstate of the beamsplitter, as already stated. Bell state analyzers can be particularly useful in *entanglement swappers.*

13. ENTANGLEMENT SWAPPERS

With an entanglement swapper, two well-separated particles that have never interacted can become entangled. This *entanglement swapping* [81–85,67], has been accomplished experimentally [86]. Two separate EPR-pair down-conversion sources were used to produce two separate pairs of entangled photons, and a Bell-state measurement was then performed on two of the photons, one from each of the separate entangled pairs. The Bell-state measurement results in projecting the remaining two photons (one from each pair), which have never interacted, into an entangled state. The device is depicted schematically in Fig. 12. EPR_1 and EPR_2 designate the two separate EPR-pair down-conversion sources that produce two separate EPR pairs of photons, (1, 2) and (3, 4). BSM designates the Bell-state measurement performed on photons 2 and 3. The Bell-state measurement of photons 2 and 3 results in the entanglement of photons 1 and 4, which have never interacted. Thus, entanglement can occur by entanglement swapping, and not only by a common source, or by interaction in the past.

Proceeding then to examine entanglement in more detail, assume the two EPR-pair sources EPR_1 and EPR_2 each produce a pair of particles in the antisymmetric polarization state given by the Bell state $|\psi^-\rangle$, Eq. (132):

$$|\psi^-\rangle_{12} = 2^{-1/2}\left(|{\rightarrow}\rangle_1 |{\uparrow}\rangle_2 - |{\uparrow}\rangle_1 |{\rightarrow}\rangle_2\right), \qquad (159)$$

$$|\psi^-\rangle_{34} = 2^{-1/2}\left(|{\rightarrow}\rangle_3 |{\uparrow}\rangle_4 - |{\uparrow}\rangle_3 |{\rightarrow}\rangle_4\right). \qquad (160)$$

Here the states are labeled explicitly with subscripts explicitly designating the particles, so that one can ignore the order of the kets, for ease of algebraic analysis. The total combined state of all four photons is then given by [86]

$$|\psi\rangle_{1234} = |\psi^-\rangle_{12} |\psi^-\rangle_{34} . \qquad (161)$$

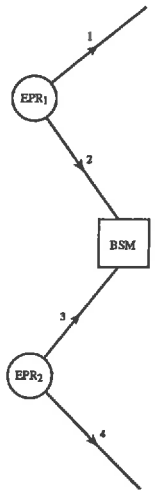

FIGURE 12. Entanglement swapper.

Although each separate pair is separately entangled, neither pair is entangled with the other pair. However, Eq. (161) can also be rewritten as follows:

(162)
$$|\psi\rangle_{1234} = 2^{-1}\left(|\psi^+\rangle_{14}\,|\psi^+\rangle_{23} - |\psi^-\rangle_{14}\,|\psi^-\rangle_{23} - |\phi^+\rangle_{14}\,|\phi^+\rangle_{23} + |\phi^-\rangle_{14}\,|\phi^-\rangle_{23}\right)$$

in terms of the Bell states $|\psi^\pm\rangle_{14}$, $|\psi^\pm\rangle_{23}$, $|\phi^\pm\rangle_{14}$, and $|\phi^\pm\rangle_{23}$ (see Eqs. (131) to (134)), where

(163)
$$|\psi^\pm\rangle_{14} = 2^{-1/2}\left(|{\rightarrow}\rangle_1\,|{\uparrow}\rangle_4 \pm |{\uparrow}\rangle_1\,|{\rightarrow}\rangle_4\right),$$

(164)
$$|\psi^\pm\rangle_{23} = 2^{-1/2}\left(|{\rightarrow}\rangle_2\,|{\uparrow}\rangle_3 \pm |{\uparrow}\rangle_2\,|{\rightarrow}\rangle_3\right),$$

(165)
$$|\phi^\pm\rangle_{14} = 2^{-1/2}\left(|{\rightarrow}\rangle_1\,|{\rightarrow}\rangle_4 \pm |{\uparrow}\rangle_1\,|{\uparrow}\rangle_4\right),$$

(166)
$$|\phi^\pm\rangle_{23} = 2^{-1/2}\left(|{\rightarrow}\rangle_2\,|{\rightarrow}\rangle_3 \pm |{\uparrow}\rangle_2\,|{\uparrow}\rangle_3\right).$$

(Equation (162) corrects the sign errors in Eq. (3) in Ref. 86.) To see that Eq. (162) is equivalent to Eq. (161) above, first note, using Eqs. (163) to (166), that

(167)
$$\begin{aligned}|\psi^\pm\rangle_{14}\,|\psi^\pm\rangle_{23} \;=\; & 2^{-1}\left(|{\rightarrow}\rangle_1\,|{\uparrow}\rangle_4\,|{\rightarrow}\rangle_2\,|{\uparrow}\rangle_3 \pm |{\rightarrow}\rangle_1\,|{\uparrow}\rangle_4\,|{\uparrow}\rangle_2\,|{\rightarrow}\rangle_3\right.\\ & \left. \pm |{\uparrow}\rangle_1\,|{\rightarrow}\rangle_4\,|{\rightarrow}\rangle_2\,|{\uparrow}\rangle_3 + |{\uparrow}\rangle_1\,|{\rightarrow}\rangle_4\,|{\uparrow}\rangle_2\,|{\rightarrow}\rangle_3\right)\end{aligned}$$

and

(168)
$$\begin{aligned}|\phi^\pm\rangle_{14}\,|\phi^\pm\rangle_{23} \;=\; & 2^{-1}\left(|{\rightarrow}\rangle_1\,|{\rightarrow}\rangle_4\,|{\rightarrow}\rangle_2\,|{\rightarrow}\rangle_3 \pm |{\rightarrow}\rangle_1\,|{\rightarrow}\rangle_4\,|{\uparrow}\rangle_2\,|{\uparrow}\rangle_3\right.\\ & \left. \pm |{\uparrow}\rangle_1\,|{\uparrow}\rangle_4\,|{\rightarrow}\rangle_2\,|{\rightarrow}\rangle_3 + |{\uparrow}\rangle_1\,|{\uparrow}\rangle_4\,|{\uparrow}\rangle_2\,|{\uparrow}\rangle_3\right).\end{aligned}$$

Next, substituting Eqs. (167) and (168) in Eq. (162), one obtains

(169)
$$\begin{aligned}|\psi\rangle_{1234} \;=\; & 2^{-1}\left(|{\rightarrow}\rangle_1\,|{\uparrow}\rangle_4\,|{\uparrow}\rangle_2\,|{\rightarrow}\rangle_3 + |{\uparrow}\rangle_1\,|{\rightarrow}\rangle_4\,|{\rightarrow}\rangle_2\,|{\uparrow}\rangle_3\right.\\ & \left. - |{\rightarrow}\rangle_1\,|{\rightarrow}\rangle_4\,|{\uparrow}\rangle_2\,|{\uparrow}\rangle_3 - |{\uparrow}\rangle_1\,|{\uparrow}\rangle_4\,|{\rightarrow}\rangle_2\,|{\rightarrow}\rangle_3\right).\end{aligned}$$

By reordering terms and factors within each term, Eq. (169) becomes

$$|\psi\rangle_{1234} = 2^{-1}\left(|{\rightarrow}\rangle_1|{\uparrow}\rangle_2|{\rightarrow}\rangle_3|{\uparrow}\rangle_4 - |{\rightarrow}\rangle_1|{\uparrow}\rangle_2|{\uparrow}\rangle_3|{\rightarrow}\rangle_4 - |{\uparrow}\rangle_1|{\rightarrow}\rangle_2|{\rightarrow}\rangle_3|{\uparrow}\rangle_4 + |{\uparrow}\rangle_1|{\rightarrow}\rangle_2|{\uparrow}\rangle_3|{\rightarrow}\rangle_4\right). \tag{170}$$

However, Eq. (170) factors directly into the following form:

$$|\psi\rangle_{1234} = 2^{-1}\left(|{\rightarrow}\rangle_1|{\uparrow}\rangle_2 - |{\uparrow}\rangle_1|{\rightarrow}\rangle_2\right)\left(|{\rightarrow}\rangle_3|{\uparrow}\rangle_4 - |{\uparrow}\rangle_3|{\rightarrow}\rangle_4\right). \tag{171}$$

Finally, substituting Eqs. (159) and (160) in Eq. (171), one obtains Eq. (161). Thus, in fact, Eq. (162) is true.

Next, from Eq. (162), it is evident that a Bell-state projective measurement of photons 2 and 3 also projects photons 1 and 4 onto a Bell state. Thus, for example, if the Bell-state projective measurement operator $|\psi^+\rangle_{23\,23}\langle\psi^+|$ for the Bell state $|\psi^+\rangle_{23}$ acts on $|\psi\rangle_{1234}$ in Eq. (162), one obtains

$$\left(|\psi^+\rangle_{23\,23}\langle\psi^+|\right)|\psi\rangle_{1234} = 2^{-1}|\psi^+\rangle_{14}|\psi^+\rangle_{23}, \tag{172}$$

because of the orthonormality of the Bell states (see Eq. (135), for example). Analogously, one obtains

$$\left(|\psi^-\rangle_{23\,23}\langle\psi^-|\right)|\psi\rangle_{1234} = -2^{-1}|\psi^-\rangle_{14}|\psi^-\rangle_{23}, \tag{173}$$

$$\left(|\phi^\pm\rangle_{23\,23}\langle\phi^\pm|\right)|\psi\rangle_{1234} = \mp 2^{-1}|\phi^\pm\rangle_{14}|\phi^\pm\rangle_{23}. \tag{174}$$

Note that in each case both projected Bell states are the same as the measured Bell state. That is, if the result of the Bell state measurement of particles 2 and 3 is $|\psi^\pm\rangle_{23}$ or $|\phi^\pm\rangle_{23}$, then the state of particles 1 and 4 is projected onto the entangled states $|\psi^\pm\rangle_{14}$ or $|\phi^\pm\rangle_{14}$, respectively. Also, in every case photons 1 and 4 become entangled, even though they never interacted.

In the experimental demonstration [86], an ultraviolet pulse first passed through a nonlinear crystal to produce the two separate entangled pairs of photons (1, 2) and (3, 4). A beamsplitter, phase plates, and coincidence detectors were used to perform the Bell-state measurement of photons 2 and 3. The Bell-state analyzer, for analysis of photons 1 and 4, consisted of a polarizing beamsplitter, phase plates, polarizer, narrow bandwidth filters, and coincidence detectors.

Entanglement swapping has also been generalized to manipulate entangled multiparticle systems [84,85]. Entangled states of many particles can, in principle, be generated in a controlled way. Potential applications include cryptographic conferencing, multiparticle generalizations of superdense coders, message reading from more than one source by making only one measurement, the construction of a quantum telephone exchange, the speeding up of the distribution of entangled particles, and series purification [84,85]. Decoherence amelioration will also be essential to further practical development of entanglement swappers.

14. QUANTUM TELEPORTER

Another exciting application of entanglement is the quantum teleporter. In *quantum teleportation* [82,83], an unknown quantum state can be disassembled by a sender (Alice) into ordinary classical information, which can then be used together with an EPR pair of particles, shared by both Alice and a receiver (Bob), to enable Bob to reconstruct the initial unknown state. To accomplish this, Alice must make a joint measurement on her EPR particle, together with the unknown quantum system, which of course destroys the unknown quantum state. She next sends Bob

the result of her measurement over a classical communication channel. With this information, Bob can then convert the state of his EPR particle into an exact replica of the initial unknown state.

A quantum teleporter is depicted schematically in Fig. 13. EPR designates a down-conversion source producing an EPR pair of photons, 2 and 3, shared by Alice and Bob, respectively. Alice first performs a Bell-state measurement, designated by BSM, on particle 1, whose state $|\chi\rangle_1$ is unknown, together with her EPR photon 2. The measurement randomly projects the two-particle state onto any one of four Bell states. She gains no information about any of the particles, but she does obtain one of four possible joint states. She next transmits the corresponding two classical bits of information to Bob, informing him which of four unitary operations (designated U in the figure) Bob must perform to transform the state of his EPR particle 3 into the original unknown state $|\chi\rangle_3$. Bob thereby has a teleported reappearance of the original state $|\chi\rangle_1$. Quantum teleportation has been experimentally demonstrated by several groups [87–90].

Let us examine quantum teleportation in more detail. Assume the EPR pair of photons 2 and 3 is in the antisymmetric two-particle Bell state $|\psi^-\rangle_{23}$, Eq. (164), namely,

$$|\psi^-\rangle_{23} = 2^{-1/2}\,(|{\rightarrow}\rangle_2\,|{\uparrow}\rangle_3 - |{\uparrow}\rangle_2\,|{\rightarrow}\rangle_3)\,. \tag{175}$$

(The states are labeled here explicitly with subscripts, designating the particles.) Denote the unknown state of Alice's particle 1 (also a photon) by

$$|\chi\rangle_1 = a\,|{\rightarrow}\rangle_1 + b\,|{\uparrow}\rangle_1\,, \tag{176}$$

with unknown complex coefficients a and b. The combined state of Alice's unknown state and the EPR pair is then given by

$$|\psi\rangle_{123} = |\psi^-\rangle_{23}\,|\chi\rangle_1 = 2^{-1/2}\,(|{\rightarrow}\rangle_2\,|{\uparrow}\rangle_3 - |{\uparrow}\rangle_2\,|{\rightarrow}\rangle_3)\,(a\,|{\rightarrow}\rangle_1 + b\,|{\uparrow}\rangle_1)\,. \tag{177}$$

Next, expanding the state $|\psi\rangle_{123}$ in terms of the Bell-state basis for particles 1 and 2, namely, $|\psi^\pm\rangle_{12}$ and $|\phi^\pm\rangle_{12}$ (see Eqs. (129) and (130)), one obtains

$$\begin{aligned} |\psi\rangle_{123} \;=\; & |\psi^-\rangle_{12}\,{}_{12}\langle\psi^-|\psi\rangle_{123} + |\psi^+\rangle_{12}\,{}_{12}\langle\psi^+|\psi\rangle_{123} \\ & + |\phi^-\rangle_{12}\,{}_{12}\langle\phi^-|\psi\rangle_{123} + |\phi^+\rangle_{12}\,{}_{12}\langle\phi^+|\psi\rangle_{123}\,. \end{aligned} \tag{178}$$

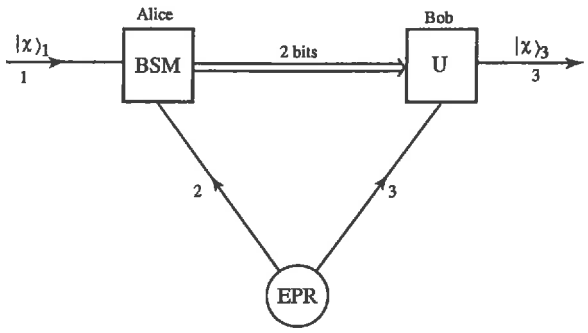

FIGURE 13. Quantum teleporter.

Next, using Eqs. (129), (130), and (177), one obtains

$$
\begin{aligned}
{}_{12}\langle\psi^-|\psi\rangle_{123} &= 2^{-1}\,({}_1\langle\rightarrow|\,{}_2\langle\uparrow| - {}_1\langle\uparrow|\,{}_2\langle\rightarrow|) \\
&\quad \times (|\rightarrow\rangle_2\,|\uparrow\rangle_3 - |\uparrow\rangle_2\,|\rightarrow\rangle_3)\,(a\,|\rightarrow\rangle_1 + b\,|\uparrow\rangle_1) \\
&= 2^{-1}\,(-a\,|\rightarrow\rangle_3 - b\,|\uparrow\rangle_3)\,, \qquad (179)
\end{aligned}
$$

$$
\begin{aligned}
{}_{12}\langle\psi^+|\psi\rangle_{123} &= 2^{-1}\,({}_1\langle\rightarrow|\,{}_2\langle\uparrow| + {}_1\langle\uparrow|\,{}_2\langle\rightarrow|) \\
&\quad \times (|\rightarrow\rangle_2\,|\uparrow\rangle_3 - |\uparrow\rangle_2\,|\rightarrow\rangle_3)\,(a\,|\rightarrow\rangle_1 + b\,|\uparrow\rangle_1) \\
&= 2^{-1}\,(-a\,|\rightarrow\rangle_3 + b\,|\uparrow\rangle_3)\,, \qquad (180)
\end{aligned}
$$

$$
\begin{aligned}
{}_{12}\langle\phi^-|\psi\rangle_{123} &= 2^{-1}\,({}_1\langle\rightarrow|\,{}_2\langle\rightarrow| - {}_1\langle\uparrow|\,{}_2\langle\uparrow|) \\
&\quad \times (|\rightarrow\rangle_2\,|\uparrow\rangle_3 - |\uparrow\rangle_2\,|\rightarrow\rangle_3)\,(a\,|\rightarrow\rangle_1 + b\,|\uparrow\rangle_1) \\
&= 2^{-1}\,(a\,|\uparrow\rangle_3 + b\,|\rightarrow\rangle_3)\,, \qquad (181)
\end{aligned}
$$

$$
\begin{aligned}
{}_{12}\langle\phi^+|\psi\rangle_{123} &= 2^{-1}\,({}_1\langle\rightarrow|\,{}_2\langle\rightarrow| + {}_1\langle\uparrow|\,{}_2\langle\uparrow|) \\
&\quad \times (|\rightarrow\rangle_2\,|\uparrow\rangle_3 - |\uparrow\rangle_2\,|\rightarrow\rangle_3)\,(a\,|\rightarrow\rangle_1 + b\,|\uparrow\rangle_1) \\
&= 2^{-1}\,(a\,|\uparrow\rangle_3 - b\,|\rightarrow\rangle_3)\,. \qquad (182)
\end{aligned}
$$

Then, substituting Eqs. (179) to (182) in Eq. (178), one obtains

$$
\begin{aligned}
|\psi\rangle_{123} &= 2^{-1}\,\big[|\psi^-\rangle_{12}\,(-a\,|\rightarrow\rangle_3 - b\,|\uparrow\rangle_3) + |\psi^+\rangle_{12}\,(-a\,|\rightarrow\rangle_3 + b\,|\uparrow\rangle_3) \\
&\quad + |\phi^-\rangle_{12}\,(b\,|\rightarrow\rangle_3 + a\,|\uparrow\rangle_3) + |\phi^+\rangle_{12}\,(-b\,|\rightarrow\rangle_3 + a\,|\uparrow\rangle_3)\big]\,. \qquad (183)
\end{aligned}
$$

The four Bell-state measurement outcomes are equally likely. This follows, since the probabilities of Bell states $|\psi^\pm\rangle_{12}$ are

$$
4^{-1}\,|-a\,|\rightarrow\rangle_3 \pm b\,|\uparrow\rangle_3|^2 = 4^{-1}\left(|a|^2 + |b|^2\right) = 1/4, \qquad (184)
$$

assuming that state $|\chi\rangle_1$, Eq. (176), is normalized to unity. Similarly, the probabilities of Bell states $|\phi^\pm\rangle_{12}$ are

$$
4^{-1}\,|\mp b\,|\rightarrow\rangle_3 + a\,|\uparrow\rangle_3|^2 = 4^{-1}\left(|b|^2 + |a|^2\right) = 1/4. \qquad (185)
$$

Each has a probability of 1/4. After Alice's measurement, Bob's EPR particle 3 will have been projected into one of the four pure-state superpositions in Eq. (183), according to the Bell-state measurement outcome. Each of the possible resulting states of Bob's EPR particle 3 is simply related to the initial state $|\chi\rangle_1$. The state $|\chi\rangle_1$, given by Eq. (176), can be represented by the vector

$$
|\chi\rangle_1 = \begin{pmatrix} a \\ b \end{pmatrix} \qquad (186)
$$

in a basis in which vertical and horizontal polarizations are represented by the basis vectors

$$
|\uparrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad |\rightarrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad (187)
$$

respectively. If Bob's measurement outcome is $|\psi^-\rangle_{12}$, then the state of Bob's EPR particle 3, according to Eq. (183), is given by

$$
|1\rangle_3 = -a\,|\rightarrow\rangle_3 - b\,|\uparrow\rangle_3 = -\begin{pmatrix} a \\ b \end{pmatrix}, \qquad (188)
$$

which is the same as Alice's initial state $|\chi\rangle_1$, except for an irrelevant phase factor ($e^{i\pi} = -1$). If Bob's measurement outcome is $|\psi^+\rangle_{12}$, then the state of Bob's EPR particle 3, according to Eq. (183), is

$$|2\rangle_3 = -a\,|{\rightarrow}\rangle_3 + b\,|{\uparrow}\rangle_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}. \tag{189}$$

We can convert this state to a replica of Alice's initial state $|\chi\rangle_1$ by applying the unitary operator

$$U_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{190}$$

since $U_2\,|2\rangle_3 = \binom{a}{b}$. I note in passing that the operator Eq. (190) is proportional to the operator HNH, since, according to Eqs. (79), (91), and (190), one has

(191)

$$HNH = 2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} 2^{-1/2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -U_2.$$

If Bob's measurement outcome is $|\phi^-\rangle_{12}$, then the state of Bob's EPR particle 3, according to Eq. (183), is given by

$$|3\rangle_3 = b\,|{\rightarrow}\rangle_3 + a\,|{\uparrow}\rangle_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}. \tag{192}$$

This state can be converted to a replica of Alice's initial state $|\chi\rangle_1$ by the application of the unitary operator

$$U_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{193}$$

since $U_3\,|3\rangle_3 = \binom{a}{b}$. Note that the operator (193) is the NOT operator, Eq. (79). Finally, if Bob's measurement outcome is $|\phi^+\rangle_{12}$, then the state of Bob's EPR particle 3, according to Eq. (183), is given by

$$|4\rangle_3 = -b\,|{\rightarrow}\rangle_3 + a\,|{\uparrow}\rangle_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}, \tag{194}$$

which Bob can convert to a replica of Alice's initial state $|\chi\rangle_1$ by applying the unitary operator

$$U_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{195}$$

since $U_4\,|4\rangle_3 = \binom{a}{b}$. Bob can use a suitable combination of half-wave plates to perform the unitary operations U_2, U_3, and U_4. In each case an accurate teleportation is obtained if Alice communicates (classically) to Bob the classical outcome of her measurement, after which Bob applies the required operation with his wave plates to transform the state of his EPR photon into a replica of Alice's original state $|\chi\rangle_1$. The state of qubit $|\chi\rangle_1$, Eq. (176), has been transferred to the state $|\chi\rangle_3 = a\,|{\rightarrow}\rangle_3 + b\,|{\uparrow}\rangle_3$. Alice is left with particles 1 and 2 in one Bell state $|\psi^\pm\rangle_{12}$ or $|\phi^\pm\rangle_{12}$, and she acquires no information on the original state $|\chi\rangle_1$. Although a perfect copy of the original qubit can be created in quantum teleportation, the original qubit is completely destroyed. This is compatible with the fact that arbitrary quantum states cannot be cloned [32,33]. In recent teleportation experiments, the

entire quadrature phase amplitude of a light beam was teleported [89], instead of just discrete polarization states.

Quantum teleportation is in principle possible even if Alice and Bob lose track of each other's location after sharing their EPR pair, provided Alice can broadcast the requisite classical information, and provided the EPR particle states are sufficiently long lived. However, decoherence severely limits the storage time of any qubits. Thus, decoherence is a critical issue for the development of practical quantum teleporters. It is presently not possible to store separated EPR particles for a sufficiently long period of time, because of decoherence. For example, the effects of attenuation and noise on a single photon, sent through an optical fiber, lead to coherence lengths ~10 km and decoherence times of order (10 km)/(3 $\times 10^8$ m/s) $\sim 10^{-5}$ s. The implementation of error-correction methods (see Sect. 21) may, however, lead to significant improvements.

15. QUANTUM COPIERS

According to the no-cloning theorem, arbitrary quantum states cannot be cloned because of the linearity of quantum mechanics [32,33]. The implication is that one cannot produce an exact copy of an arbitrary qubit. This does not mean, however, that an approximate copy cannot be made. The function of one type of *quantum copier* is to produce an approximate copy of a qubit that is as close to being an exact copy as possible, and with the original qubit changed as little as possible in the process. A number of types of quantum copiers have been considered in the literature [91–104,59].

A universal copier is one that produces two identical copies whose quality is independent of the input state [91,92]. The universal quantum copier must copy an arbitrary pure state, which can be written in a chosen basis, $\{|0\rangle_{a_0}, |1\rangle_{a_0}\}$ as [96]

$$|\psi\rangle_{a_0} = \alpha\,|0\rangle_{a_0} + \beta\,|1\rangle_{a_0}\,, \tag{196}$$

for which a general parameterization of the coefficients is

$$\alpha = \sin\theta\; e^{i\phi}, \qquad \beta = \cos\theta. \tag{197}$$

A universal quantum copier satisfies three basic requirements [92]:

(1) If the state of the original qubit at the output of the quantum copier is denoted by the density operator $\rho_{a_0}^{(\mathrm{out})}$, and that of the quantum copy is $\rho_{a_1}^{(\mathrm{out})}$, one requires that

$$\rho_{a_0}^{(\mathrm{out})} = \rho_{a_1}^{(\mathrm{out})}. \tag{198}$$

(2) If the measure of distance $d(\rho_1, \rho_2)$ between two states with density operators ρ_1 and ρ_2 is taken to be the square of the Hilbert-Schmidt norm, that is,

$$d(\rho_1, \rho_2) \equiv \mathrm{Tr}\,\left[(\rho_1 - \rho_2)^2\right], \tag{199}$$

then the requirement that pure states should be copied equally well can be expressed by

$$d(\rho_{a_i}^{(\mathrm{out})}, \rho_{a_i}^{(\mathrm{id})}) = C, \qquad i = 0, 1, \tag{200}$$

where $\rho_{a_i}^{(\mathrm{id})}$ is the ideal density operator describing the input state, and C is a constant, independent of the input state.

(3) Equation (200) should be minimized with respect to all unitary transformations within the Hilbert space of the two qubits and the quantum copier.

It can be shown that the unitary transformation that implements the universal quantum copier by satisfying requirements (1) to (3) is given by [92,96]

$$|0\rangle_{a_0}|Q\rangle_x \Rightarrow (3/2)^{-1/2}|0\rangle_{a_0}|0\rangle_{a_1}|\uparrow\rangle_x + 3^{-1/2}|+\rangle_{a_0a_1}|\downarrow\rangle_x , \tag{201}$$

and

$$|1\rangle_{a_0}|Q\rangle_x \Rightarrow (3/2)^{-1/2}|1\rangle_{a_0}|1\rangle_{a_1}|\downarrow\rangle_x + 3^{-1/2}|+\rangle_{a_0a_1}|\uparrow\rangle_x , \tag{202}$$

where

$$|+\rangle_{a_0a_1} = 2^{-1/2}\left(|1\rangle_{a_0}|0\rangle_{a1} + |0\rangle_{a_0}|1\rangle_{a1}\right). \tag{203}$$

Here, indices a_0, a_1, and x designate the original qubit, the copy, and the copier, respectively. The copier has a two-dimensional state space with basis vectors $|\uparrow\rangle_x$ and $|\downarrow\rangle_x$, and $|Q\rangle_x$ denotes the initial state of the copier. The implication of Eqs. (201) and (202) is that the copy contains 5/6 of the desired state and 1/6 undesired.

The universal quantum copier can be implemented with a network of simple quantum logic gates [92,96]. Also, a quantum copier has been designed that produces multiple identical copies from one or more original qubits [96–99,59].

In other work, it has been shown that, owing to residual correlations between the copy and the quantum copier, quantum copying degrades entanglement [100]. A quantum copier can also involve quantum teleportation schemes [101,102]. Quantum copiers implementing a quality measure based on state distinguishability have also been investigated [103,104]. Decoherence is an obstacle to useful implementations of quantum copying, because it limits the state storage time.

16. ALL-OPTICAL QUANTUM INFORMATION PROCESSORS

It is next appropriate to begin to address various possible qubit devices for quantum computation. Consider first *all-optical quantum information processors.* All-optical quantum computers are of two general types, depending on whether nonlinear optical elements are employed. In a quantum computer based on linear optics, the basic qubit consists of two path states of a single photon [105,106]. A photon leaving an optical element, such as a beamsplitter with two exit ports, has a propensity to exit along either path, so the photon becomes a two-path-state system. The linear optical elements composing the device include beamsplitters, mirrors, polarizers, wave plates, etc. The initial state of the device need only consist of a single photon entering the device at a beamsplitter. All the necessary quantum gates can be implemented (see Sect. 6). Even two-qubit gates such as the controlled-NOT gate can be implemented. By cascading the number of beamsplitters, locating one at each alternative path in a network of optical elements, we make the device a multiple-qubit system. However, because of the resulting exponential proliferation of optical elements needed to form a large number of path qubits, such a linear-optical quantum computer is limited to a relatively small number of qubits. The device is therefore limited to implementing small-scale quantum networks for performing small quantum algorithms, such as those involved in simple quantum error correction and quantum teleportation [105].

The second type of all-optical quantum computer is a multi-photon device employing nonlinear optical elements [107–109]. Nonlinear optical elements are needed so that the state of one photonic qubit can control the state of another at certain nodes in the network. The use of many photons circumvents the exponential cascading required by large linear optical quantum computers. The problem with the

use of traditional nonlinear optical elements for implementing conditional dynamics, in which the state of one photon conditionally modulates the state of another, is the huge nonlinear susceptibility required to produce the necessary phase shifts at the two-photon level of intensity (see Sect. 11). Practical nonlinear photon gates operating at the two-photon level of intensity are not presently available; however, innovative approaches are currently under investigation. These involve mutual interactions between two gate photons and atoms in a medium [70–72,110,111] or in a QED cavity [73].

Although decoherence is not an obstacle to the development of a reasonably small, special-purpose, all-optical quantum information processor, it would become an issue in any attempt to scale up the device to include large numbers of optical elements. Before considering other physical quantum computer implementations, it is well to review the concept of a *universal quantum computer.*

17. UNIVERSAL QUANTUM COMPUTER

A universal quantum computer [112–116] ideally consists of a set of n qubits on which the following operations can be performed: (1) each qubit can be initialized in some state $|0\rangle$; (2) a universal quantum gate, or set of gates, can be applied to any subset of qubits; (3) each qubit can be measured in the basis $\{|0\rangle, |1\rangle\}$; and (4) the qubits evolve only as a result of these transformations.

In the network model [115], logic gates are applied sequentially. The logic gates are typically implemented by interactions that can be turned on or off at appropriate times.

A universal quantum gate is one that, when applied to different combinations of qubits, can produce the same result as any other gate. Since all quantum systems evolve according to the Schrödinger equation, and quantum evolution is unitary, the set of all possible quantum gates must be such that all possible unitary transformations on the n qubits of the computer can be generated. The controlled-NOT gate and single-qubit rotations are universal, since any $n \times n$ unitary matrix can be formed by combining two-qubit controlled-NOT operators and single-qubit rotations. The controlled-NOT gate and rotation can be combined into a single universal quantum gate, which is a conditional rotation [4,117–120]. The universal quantum computer can, in principle, simulate, by finite means, and arbitrarily closely, any finitely realizable physical system. This is the quantum extension of the Church-Turing principle [114–116]. The extended principle holds, since (1) the state of any finite quantum system can be represented by a vector in Hilbert space, and can therefore be precisely represented by a finite number of qubits; and (2) the evolution of the state of any finite quantum system can be represented by a unitary transformation, and can therefore be simulated on a quantum computer capable of generating any unitary transformation with arbitrary precision.

It must be assumed that the tasks performed by the quantum computer are such that the number of steps is predictable, or that the quantum computer can indicate completion of a computation by means of a dedicated qubit not otherwise involved in the computation. Otherwise, there are fundamental unavoidable obstacles to the construction of a halt qubit to control task completion [121–123]. Also, possible contradictions have recently been suggested between the Church-Turing principle and the inclusion of unrestricted classes of quantum observables and unitary operators [124].

It must be emphasized that, as described above, the universal quantum computer is an ideal theoretical construct that does not take into account imprecise gate operations, quantum decoherence, imprecise measurements, and quantum error correction. Only with qualifications to the stated requirements might the prescription for a universal quantum computer be implementable.

A quantum computer is not a closed system, and therefore the computational degrees of freedom cannot evolve unitarily. Interactions between the computational degrees of freedom and noncomputational degrees of freedom, both outside and inside the computer, will result in qubit decoherence, and consequent deterioration of the qubit entanglements necessary for successful computer operation. Inexact tuning of quantum gates and structural inaccuracies will also result in erroneous evolution of quantum states. Quantum error correction must therefore be implemented (see Sect. 21).

18. QUANTUM SIMULATORS

A quantum computer can be used to simulate other quantum systems [125–138]. Such a quantum computer is a *quantum simulator.* A quantum computer needs at least n qubits to simulate a state vector in a 2^n-dimensional Hilbert space. It must implement unitary transformations in the 2^n-dimensional Hilbert space, and this will typically require an exponential number of elementary quantum logic gates. The implication is that a quantum computer cannot efficiently simulate every physical system. However, many physical systems can be simulated with a quantum computer that could not, in practice, be simulated with a classical computer because of intractability [125–134]. A computation is only tractable if its complexity is such that the resources required to perform it do not increase exponentially with the number of digits in the input. The time evolution of the wave function of a quantum many-body system could be faithfully simulated on a quantum computer [131–137]. Quantum chaos may also be efficiently calculated on a quantum computer [138]. Ultimately, the simulation of quantum field theory may also be possible on a large quantum computer [134]. However, presently, no quantum simulator exists of sufficient scale to perform any interesting simulations of quantum systems.

19. QUANTUM FACTORIZER

A strong incentive for attempts to develop practical quantum computers arises from their possible use in speedily factoring very large numbers for cryptographic applications. A quantum computer could be used to factor large L-digit numbers in $\sim L^3$ time compared to $\sim e^{(\ln L)^{2/3} L^{1/3}}$ time for a classical computer [139–141]. This would exploit the coherence of the quantum wave function of a quantum register implementing an array of qubits. To factor a number N, choose a number x at random that is coprime with N. Use the quantum computer to calculate the order r of x mod N; that is, to find r such that

$$x^r = 1 \bmod N. \tag{204}$$

If r is even, then the greatest common divisor of $\left(x^{r/2} \pm 1\right)$ and N is a factor of N, and can be determined with Euclid's algorithm. For example, if $N = 1295$ and $x = 6$, one has

$$6^r = 1 \bmod 1295 \Rightarrow r = 4, \tag{205}$$

$$6^{4/2} \pm 1 = 36 \pm 1 = \{35, 37\}, \tag{206}$$

$$1295 = 5 \cdot 7 \cdot 37. \tag{207}$$

A *quantum factorizer* would implement Shor's quantum factoring algorithm to calculate the order r [139–141] A number q having small prime factors is first chosen, such that

$$N^2 < q < 2N^2. \tag{208}$$

By means of appropriate quantum gates, the qubits constituting the quantum register (see Sect. 20) can be manipulated to produce the state

$$|\psi_1\rangle = q^{-1/2} \sum_{a=0}^{q-1} |a, 0\rangle\,, \tag{209}$$

where $|a, 0\rangle$ denotes the tensor-product state $|a\rangle\,|0\rangle$. Next, an additional set of quantum gates must be used to implement a unitary transformation of the state $|\psi_1\rangle$ to produce the state

$$|\psi_2\rangle = q^{-1/2} \sum_{a=0}^{q-1} |a, x^a \bmod N\rangle\,. \tag{210}$$

Here $|a, x^a \bmod N\rangle$ denotes $|a\rangle\,|x^a \bmod N\rangle$. Next, the state $|\psi_2\rangle$ must be Fourier transformed with the quantum computer to produce the state

$$|\psi_3\rangle = q^{-1/2} \sum_{m=0}^{q-1} \sum_{a=0}^{q-1} e^{i2\pi am/q}\, |m, x^a \bmod N\rangle\,. \tag{211}$$

Both arguments of the superposition must be measured, resulting in $\{c, x^k\}$ for

$$m = c, \quad x^a = x^k, \quad 0 < k < r. \tag{212}$$

Then, the probability of the result $\{c, x^k\}$ is

$$P(c, x^k) = \left| q^{-1/2} \sum_{a=0, x^a = x^k \bmod N}^{q-1} e^{i2\pi ac/q} \right|^2. \tag{213}$$

The probability is periodic in c with period q/r and is sharply peaked at $c = pq/r$ for integer p. Therefore, the period yields r after a few trial runs.

Note that the state $|\psi_2\rangle$ in Eq. (210) is a superposition of product states, and cannot be expressed as a single-product state. It is entangled. Entanglement, in addition to superposition, is an essential feature of quantum computation. The performance of the operations leading from $|\psi_1\rangle$ in Eq. (209) to $|\psi_2\rangle$ in Eq. (210), for example, would exploit the massive quantum parallelism characteristic of a quantum computer. Because the input $|\psi_1\rangle$ for large N is set up in a large superposition of states, the quantum computer would carry out all the computations for each value of a simultaneously. Although there are $q > N^2$ input qubits in Eq. (209), there is only one output qubit, corresponding to the measured values of Eq. (212). The computation must be repeated enough times to determine the peaks of the probability distribution in c, Eq. (213).

It is necessary that the rate of decoherence be sufficiently low for the computation to be completed [140,142,143]. Although a quantum factorizer capable of factoring a 250-digit number does not presently exist, if and when one does, the

widespread cryptosystems relying on the difficulty of factoring large numbers will be rendered insecure and obsolete. However, to date, not even a 5-digit number has been factored with a quantum computer.

20. QUANTUM REGISTER

One of the main ingredients of any sizable quantum computer would be the *quantum register*. A quantum register may be thought of as a row of N qubits. A binary number,

$$n = \sum_{k=0}^{N-1} n_k 2^k, \qquad n_k = 0 \text{ or } 1 \tag{214}$$

can be stored in the quantum register, and is represented by a product state of the N qubits, namely,

$$|n\rangle = |n_{N-1}\rangle\,|n_{N-2}\rangle \cdots |n_1\rangle\,|n_0\rangle\,. \tag{215}$$

Here, tensor products are implicit, and the order of the kets corresponds to the order of the qubits in the register. Each ket in the product corresponds to a single qubit. A general state $|\psi\rangle$ of the free quantum register is given by the N-qubit entangled state,

$$|\psi\rangle = \sum_{n=0}^{2^N-1} \alpha_n\,|n\rangle\,, \tag{216}$$

where the α_n are complex numbers, and the sum is over all 2^N possible product Boolean states, Eq. (215), thereby forming a 2^N-dimensional Hilbert space.

For example, a three-bit classical register can store only one of eight different numbers, {000,001,010,011,100,101,110,111}, using a binary representation of numbers between 0 and 7. But a quantum register consisting of three qubits can store up to eight numbers at the same time in a quantum superposition. The state of the three-qubit quantum register is, in general, given by

$$\begin{aligned} |\psi\rangle \;=\; & \alpha_{000}\,|0\rangle\,|0\rangle\,|0\rangle + \alpha_{001}\,|0\rangle\,|0\rangle\,|1\rangle + \alpha_{010}\,|0\rangle\,|1\rangle\,|0\rangle + \alpha_{011}\,|0\rangle\,|1\rangle\,|1\rangle \\ & + \alpha_{100}\,|1\rangle\,|0\rangle\,|0\rangle + \alpha_{101}\,|1\rangle\,|0\rangle\,|1\rangle + \alpha_{110}\,|1\rangle\,|1\rangle\,|0\rangle + \alpha_{111}\,|1\rangle\,|1\rangle\,|1\rangle\,. \end{aligned} \tag{217}$$

This is a coherent superposition of the numbers from 0 to 7.

For the N-qubit quantum register, although measuring the register's contents will yield only one number, a quantum computation can effectively manipulate all 2^N numbers at once. For example, if each qubit consists of two states of an atom, tuned laser pulses can switch the electronic states so that an initial superposition of 2^N numbers will evolve into a different superposition. This evolution results in massive parallelism, since each number in the superposition is affected.

To prepare a specific number in a quantum register, N elementary operations must be performed. Each of the N qubits must be put in one of two states. N elementary operations, which can be represented by unitary transformations on each qubit, can prepare the register in a coherent superposition of 2^N numbers, to be stored in the register. This process can be seen as follows. One can represent the Boolean states $|0\rangle$ and $|1\rangle$ by the vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{218}$$

If, for example, the first qubit of a three-qubit register is in the state $|0\rangle$, then applying the Hadamard operator H, Eq. (91), causes the state of the qubit to become

$$H|0\rangle = 2^{-1/2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 2^{-1/2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 2^{-1/2}(|0\rangle + |1\rangle), \tag{219}$$

which is an equally weighted superposition of Boolean states $|0\rangle$ and $|1\rangle$. The Hadamard transform applied to each qubit of a three-qubit quantum register, each initially in state $|0\rangle$, yields the state,

$$\begin{aligned} |\psi\rangle &= \prod_{i=1}^{3}(H|0\rangle) = H|0\rangle H|0\rangle H|0\rangle = 2^{-3/2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= 2^{-3/2}(|0\rangle + |1\rangle)(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \\ &= 2^{-3/2}(|0\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|1\rangle \\ &\quad + |1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle), \end{aligned} \tag{220}$$

in which the order of the kets is preserved and corresponds to the order of the qubits in the register. Next, using a notation for states representing numbers to the base 10, that is,

$$\begin{aligned} &|0\rangle \equiv |0\rangle|0\rangle|0\rangle, \quad |1\rangle \equiv |0\rangle|0\rangle|1\rangle, \quad |2\rangle \equiv |0\rangle|1\rangle|0\rangle, \quad |3\rangle \equiv |0\rangle|1\rangle|1\rangle, \\ &|4\rangle \equiv |1\rangle|0\rangle|0\rangle, \quad |5\rangle \equiv |1\rangle|0\rangle|1\rangle, \quad |6\rangle \equiv |1\rangle|1\rangle|0\rangle, \quad |7\rangle \equiv |1\rangle|1\rangle|1\rangle, \end{aligned} \tag{221}$$

one can rewrite Eq. (220) as

$$|\psi\rangle = 2^{-3/2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle) = 2^{-3/2}\sum_{n=0}^{2^3-1}|n\rangle. \tag{222}$$

Thus, more generally, if an N-qubit register is initially in the state $|0\rangle|0\rangle|0\rangle\ldots|0\rangle$, one can apply the Hadamard operator H, Eq. (219), to each qubit, and the resulting state of the register is an equally weighted superposition of all 2^N numbers, namely,

$$|\psi\rangle = \prod_{i=1}^{N}(H|0\rangle) = H|0\rangle H|0\rangle \ldots H|0\rangle = 2^{-N/2}\sum_{n=0}^{2^N-1}|n\rangle. \tag{223}$$

The N elementary operations generate a state containing all 2^N possible numerical values of the register. This provides a method for generating the state, Eq. (209), in Shor's quantum factoring algorithm. If the quantum register is prepared in such a coherent superposition of numbers, and all subsequent computational transformations are unitary (preserving the superposition of states), then in each step the computation is performed on each of the numbers in the superposition simultaneously.

21. QUANTUM ERROR CORRECTORS

Quantum error-correction methods may provide the means to successfully combat decoherence in quantum computers and other qubit devices [144–176,83,116]. *Quantum error correctors* are implementations of these methods that involve quantum circuits consisting of networks of quantum gates. The interaction of a qubit in a general state,

$$|\phi\rangle = a|0\rangle + b|1\rangle, \tag{224}$$

with its environment in state $|e\rangle$, results, in general, in the following entanglement between the qubit and its environment [116,170]:

$$\begin{aligned} |e\rangle\,|\phi\rangle &= |e\rangle\,(a\,|0\rangle + b\,|1\rangle) \Rightarrow a\,(c_{00}\,|e_{00}\rangle\,|0\rangle + c_{01}\,|e_{00}\rangle\,|1\rangle) \\ &\quad + b\,(c_{10}\,|e_{10}\rangle\,|1\rangle + c_{11}\,|e_{11}\rangle\,|0\rangle)\,, \end{aligned} \tag{225}$$

where $|e_{ij}\rangle$ denote states of the environment, and c_{ij} are complex coefficients that depend on the environmental interactions with the qubit. Equivalently, Eq. (225) can be rewritten as follows [116]:

$$|e\rangle\,|\phi\rangle \Rightarrow (|e_I\rangle\,I + |e_X\rangle\,X + |e_Y\rangle\,Y + |e_Z\rangle\,Z)\,|\phi\rangle\,, \tag{226}$$

where the operators $\{I, X, Y, Z\}$ are defined by

$$I \equiv |0\rangle\,\langle 0| + |1\rangle\,\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{227}$$

$$X \equiv |0\rangle\,\langle 1| + |1\rangle\,\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{228}$$

$$Z \equiv |0\rangle\,\langle 0| - |1\rangle\,\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{229}$$

$$Y \equiv XZ = |1\rangle\,\langle 0| - |0\rangle\,\langle 1| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{230}$$

The corresponding matrix representatives are also given in Eqs. (227) to (230) (these matrices can also be simply related to the Pauli spin matrices [36]). Note that by completeness, I, in Eq. (227), is the identity operator, which corresponds to the unit matrix. Also, the operator X is the NOT operator, Eq. (79), since in matrix form one has

$$X = [\langle m|X|n\rangle] = [\langle m|\,(|0\rangle\,\langle 1| + |1\rangle\,\langle 0|)\,|n\rangle] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = N. \tag{231}$$

Analogously, one obtains the matrix representatives shown for Z and Y in Eqs. (229) and (230), respectively. Also, in Eq. (226), the states $|e_I\rangle$, $|e_X\rangle$, $|e_Y\rangle$, and $|e_Z\rangle$ are given by

$$|e_I\rangle = 2^{-1}\,(c_{00}\,|e_{00}\rangle + c_{10}\,|e_{10}\rangle)\,, \tag{232}$$

$$|e_X\rangle = 2^{-1}\,(c_{01}\,|e_{01}\rangle + c_{11}\,|e_{11}\rangle)\,, \tag{233}$$

$$|e_Y\rangle = 2^{-1}\,(c_{01}\,|e_{01}\rangle - c_{11}\,|e_{11}\rangle)\,, \tag{234}$$

$$|e_Z\rangle = 2^{-1}\,(c_{00}\,|e_{00}\rangle - c_{10}\,|e_{10}\rangle)\,. \tag{235}$$

Equation (226) represents three types of errors, corresponding to the operators X, Y, and Z. The operator X represents a bit flip, since it interchanges the basis states, thus

$$X \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} |1\rangle \\ |0\rangle \end{pmatrix}. \tag{236}$$

The operator Z represents a phase error, since it introduces a relative phase $e^{i\pi} = -1$:

$$Z \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} |0\rangle \\ -|1\rangle \end{pmatrix}. \tag{237}$$

The operator $Y = XZ$ represents a phase change together with a bit flip, since

$$Y \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} -|1\rangle \\ |0\rangle \end{pmatrix}. \tag{238}$$

To see that Eq. (226) is equivalent to Eq. (225), note that if we use Eqs. (227) to (230), (232) to (235), and Eq. (224),

$$\begin{aligned} |e\rangle\,|\phi\rangle \;\Rightarrow\; & (|e_I\rangle\, I + |e_X\rangle\, X + |e_Y\rangle\, Y + |e_Z\rangle\, Z)\,|\phi\rangle \\ = \;& 2^{-1}\,(c_{00}\,|e_{00}\rangle + c_{10}\,|e_{10}\rangle)\,(|0\rangle\langle 0| + |1\rangle\langle 1|)\,(a\,|0\rangle + b\,|1\rangle) \\ & + 2^{-1}\,(c_{01}\,|e_{01}\rangle + c_{11}\,|e_{11}\rangle)\,(|0\rangle\langle 1| + |1\rangle\langle 0|)\,(a\,|0\rangle + b\,|1\rangle) \\ & + 2^{-1}\,(c_{01}\,|e_{01}\rangle - c_{11}\,|e_{11}\rangle)\,(|1\rangle\langle 0| - |0\rangle\langle 1|)\,(a\,|0\rangle + b\,|1\rangle) \\ & + 2^{-1}\,(c_{00}\,|e_{00}\rangle - c_{10}\,|e_{10}\rangle)\,(|0\rangle\langle 0| - |1\rangle\langle 1|)\,(a\,|0\rangle + b\,|1\rangle) \\ = \;& 2^{-1}\,(c_{00}\,|e_{00}\rangle + c_{10}\,|e_{10}\rangle)\,(a\,|0\rangle + b\,|1\rangle) \\ & + 2^{-1}\,(c_{01}\,|e_{01}\rangle + c_{11}\,|e_{11}\rangle)\,(b\,|0\rangle + a\,|1\rangle) \\ & + 2^{-1}\,(c_{01}\,|e_{01}\rangle - c_{11}\,|e_{11}\rangle)\,(-b\,|0\rangle + a\,|1\rangle) \\ & + 2^{-1}\,(c_{00}\,|e_{00}\rangle - c_{10}\,|e_{10}\rangle)\,(a\,|0\rangle - b\,|1\rangle) \\ = \;& a\,(c_{00}\,|e_{00}\rangle\,|0\rangle + c_{01}\,|e_{01}\rangle\,|1\rangle) + b\,(c_{10}\,|e_{10}\rangle\,|1\rangle + c_{11}\,|e_{11}\rangle\,|0\rangle)\,. \end{aligned} \tag{239}$$

Thus Eq. (226) is equivalent to Eq. (225).

Suppose that a quantum computer manipulates k qubits in the general state $|\phi_k\rangle$. Then add $n-k$ qubits in the state $|0\rangle$ to the computer, so that there are n qubits. Next, perform the encoding operation

$$E\,(|\phi_k\rangle\,|0\rangle) = |\phi_E\rangle\,, \tag{240}$$

which produces, in general, some entangled state $|\phi_E\rangle$ of all n qubits. Then let noise affect all n qubits. The noise can be represented as a sum of error operators M, where each M is a tensor product of n operators I,X,Y,Z, one acting on each qubit. For example, if I operates on qubit 1, X on 2, Z on 3, X on 4, Y on 5, X on 6, Y on 7, and I on 8, this can be represented by the operator

$$M = I_1 X_2 Z_3 X_4 Y_5 X_6 Y_7 I_8\,. \tag{241}$$

Then, general interactions between the n qubits and the environment produce the general noisy state

$$|\psi\rangle_N = \sum_s |e_s\rangle\, M_s\, |\phi_E\rangle\,, \tag{242}$$

where each M_s is an operator involving products of the four operators I,X,Y,Z, such that each of the n qubits is acted on by one of them. Next, add another $n-k$ ancilla qubits, prepared in the state $|0\rangle_a$. For any encoding E, there is some

operator A, called the syndrome extraction operator, which identifies the type of corrected error, namely [116],

$$A\left(M_s\left|\phi_E\right\rangle\left|0\right\rangle_a\right) = \left(M_s\left|\phi_E\right\rangle\right)\left|s\right\rangle_a \ \forall M_s \in S, \tag{243}$$

where S is the set of correctable errors and depends on the encoding. Here, the symbol s in $\left|s\right\rangle_a$ is a binary number that identifies the error operator M_s considered, and the states $\left|s\right\rangle_a$ are mutually orthogonal. For the simple case that the general noise state $\left|\psi\right\rangle_N$, Eq. (242), contains only $M_s \in S$, the joint state of the n nonancilla qubits, environment, and ancilla (following the syndrome extraction) is given by

$$\left|\psi\right\rangle_{Na} = A\left|\psi\right\rangle_N\left|0\right\rangle_a = A\left[\left(\sum_s \left|e_s\right\rangle M_s\left|\phi_E\right\rangle\right)\left|0\right\rangle_a\right] = \sum_s \left|e_s\right\rangle\left(M_s\left|\phi_E\right\rangle\right)\left|s\right\rangle_a . \tag{244}$$

If the ancilla state is measured with the measurement operator $\left|s\right\rangle_{a\,a}\!\left\langle s\right|$, then

$$\begin{aligned}\left(\left|s\right\rangle_{a\,a}\!\left\langle s\right|\right)\left|\psi\right\rangle_{Na} &= \left|s\right\rangle_{a\,a}\!\left\langle s\right|\sum_{s'}\left|e_{s'}\right\rangle\left(M_{s'}\left|\phi_E\right\rangle\right)\left|s'\right\rangle_a \\ &= \left|s\right\rangle_a\sum_{s'}\left|e_{s'}\right\rangle\left(M_{s'}\left|\phi_E\right\rangle\right)\delta_{ss'} \\ &= \left|e_s\right\rangle\left(M_s\left|\phi_E\right\rangle\right)\left|s\right\rangle_a ; \end{aligned} \tag{245}$$

that is, the entire state collapses into $\left|e_s\right\rangle\left(M_s\left|\phi_E\right\rangle\right)\left|s\right\rangle_a$ for a particular s. Thus, the measurement reveals the value s, thereby determining the error operator M_s (s is the error syndrome).

Next, if the operator M_s^{-1} is applied to the measured state by means of various quantum gates X,Y, or Z, there results

$$M_s^{-1}\left(\left|s\right\rangle_{a\,a}\!\left\langle s\right|\left|\psi\right\rangle_{Na}\right) = M_s^{-1}\left[\left|e_s\right\rangle\left(M_s\left|\phi_E\right\rangle\right)\left|s\right\rangle_a\right] = \left|e_s\right\rangle\left|\phi_E\right\rangle\left|s\right\rangle_a , \tag{246}$$

resulting in the noise-free state $\left|\phi_E\right\rangle$. The state $\left|e_s\right\rangle$ of the environment, appearing here, is of no interest, and the ancilla state $\left|s\right\rangle_a$ can be put back in state $\left|0\right\rangle_a$ and used again. If the noise in $\left|\psi\right\rangle_N$, Eq. (242), contains errors M_s that are not in the correctable set S, then the probability must be large that when the syndrome is extracted, the state collapses onto a correctable state.

The error-correction procedure must be such that the encoding operation E and the extraction operation A are such that the set S of correctable errors includes all likely errors. If uncorrelated stochastic noise is assumed, for which the effect on a qubit at different times is uncorrelated (and the effect on different qubits is uncorrelated also), then all possible error operators can be categorized in terms of their likelihood. Those affecting fewer qubits are more likely. If a quantum error-correcting code is such that all errors affecting up to t qubits are correctable, then the code is a t-error correcting code [147,148,151,154,83].

Errors can also occur in the ancilla, quantum gates, and measurements. Methods have been discovered by which the error correction suppresses more noise than it produces [156,158,168,170,175]. Error-correcting codes may require an extremely large overhead in terms of the numbers of qubits (required for sufficient redundancy to recover from errors) and gates (required to process the redundantly encoded data and to diagnose and reverse errors). The error probability per qubit per gate must be very small (below the *accuracy threshold)* if the error correction is to succeed for arbitrarily long computations [161–163,165]. The requirements are formidable for reliable quantum computing using such fault-tolerant quantum error-correcting

codes [160,171]. Furthermore, quantum error-correcting codes usually assume that errors in distant qubits are, at most, weakly correlated, and the codes are inadequate to deal with strongly correlated errors involving many qubits [171].

Note that much simpler quantum error-correction methods can be used if enough is known about the sources of noise [177,172,173]. Several passive error-prevention schemes have been proposed, in which the encoding occurs within subspaces that do not decohere because of symmetry properties [178–181]. It has been argued [181], on the basis of a semigroup description of quantum decoherence [182,183], that error-free quantum computation is possible in decoherence-free subspaces. The evolution of the computational degrees of freedom, which form a subspace of the total Hilbert space describing the quantum dynamics of the qubit device and its environment, is nonunitary, and is described by a semigroup. The decoherence-free subspaces are spaces spanned by states annihilated by all error generators (the operators X, Y, and Z in Eq. (226) are error generators). Also, various methods of decoherence control are currently under investigation. These include the application of feedback [184,185] and of external controllable interactions [186–189]. It is argued that the effects of qubit-environment interactions can be removed by suitable decoupling perturbations acting on the qubit device over time scales comparable to the correlation time of the environment [187–189].

22. QUANTUM COMPUTERS

I proceed to discuss possible quantum computer implementations that are currently under development [114–116,142,190–195]. In the ion-trap quantum computer [196], a one-dimensional lattice of identical ions is stored and laser cooled in a linear Paul trap (radio-frequency (rf) quadrupole trap) [197–200,75]. The linear array of ions acts as a quantum register (see previous section). The rf trap potential strongly confines the ions radially about the trap axis, and an electrostatic potential causes the ions to oscillate along the trap axis in an effective harmonic potential. Laser cooling results in localization of the ions along the trap axis, with spacing determined by Coulomb repulsion and the confining axial potential. The lowest frequency mode of collective oscillation of the ions is the axial center-of-mass mode, in which all the ions oscillate with the same phase together. Each of the trapped ions acts as a qubit, in which the two pertinent states are the electronic ground state and a long-lived excited state. By means of coherent interaction of a precisely controlled laser pulse with any one of the ions in a standing-wave configuration, one can manipulate the ion's electronic state and the quantum state of the collective center of mass mode of the oscillator. The center of mass mode can then be used as a bus, quantum dynamically connecting the qubits, to implement the necessary quantum logic gates. The general state of the line of ions that the quantum register comprises is an entangled linear superposition of their states. A completed computation can be read out by a quantum jump measurement technique [196]. Experimental demonstration of the ion-trap approach began with state preparation, quantum gates, and measurement for a single trapped ion [201]. Since then, a number of experimental and theoretical issues regarding the ion-trap approach to quantum computation have been explored [202–229,116,85]. Presently, the main experimental difficulty in implementing this approach is cooling the ions to the ground state in the trap. The primary source of decoherence is apparently the heating due to coupling between the ions and noise voltages in the

trap electrodes [204,205]. In the near term, it is contemplated that 100 quantum gate operations could be applied to a few ions [116]. It is, however, very questionable that sufficient storage capacity and coherence will ever be achieved to enable factorization of hundred-digit numbers by the trapped-ion approach [85,227–229]. Also, the speed of an ion-trap quantum computer would apparently be limited by the frequencies of vibrational modes in the trap.

Another popular approach to the development of a quantum computer is provided by cavity quantum electrodynamics (QED). In the cavity QED [230–233] approach, a number of neutral atoms are trapped inside a high-finesse optical cavity [234]. Electronic states of the atom act as qubits to store information. The atoms in the cavity interact with a quantized mode of the cavity. The separations between the atoms are much greater than the wavelength of the cavity mode, and the atoms can interact individually with laser pulses. This permits sequences of operations between two qubits and the implementation, in principle, of an entire quantum network. The qubits consist of ground-state levels of the trapped atoms. Quantum gates can be implemented by the atoms being coupled to individual laser pulses and entangled by exchange of a cavity photon. Pulsed lasers can be used to drive transitions in one atom conditionally on the internal states of another atom. Also, the polarization states of a photon can serve as a qubit. An atom trapped in the cavity can serve as an effective nonlinear medium to mediate interactions between two photons, and thereby implement a two-photon quantum gate, in which the polarization state of one photon alters the phase of the other photon [73,235]. Letting $|l\rangle_i$ and $|r\rangle_i$ denote left and right circular polarization states of photon i ($i = 1,2$), one has, effectively,

$$|l\rangle_1 |l\rangle_2 \Longrightarrow |l\rangle_1 |l\rangle_2 , \tag{247}$$

$$|l\rangle_1 |r\rangle_2 \Longrightarrow e^{i\phi_2} |l\rangle_1 |r\rangle_2 , \tag{248}$$

$$|r\rangle_1 |l\rangle_2 \Longrightarrow e^{i\phi_1} |r\rangle_1 |l\rangle_2 , \tag{249}$$

$$|r\rangle_1 |r\rangle_2 \Longrightarrow e^{i(\phi_1+\phi_2+\Delta)} |r\rangle_1 |r\rangle_2 , \tag{250}$$

where ϕ_1 and ϕ_2 are differential phases between the two polarization states, and Δ is the conditional phase shift. The transformations, Eqs. (247) to (250), are accomplished first by one photon being stored in the cavity, in which the right circular polarization state couples strongly to the atom, but the left circular polarization state does not. Next, another photon traverses the cavity, also interacting preferentially in one polarization state with the atom, and acquiring the conditional phase shift only if the photons are in the right circular polarization state. Thus, the phase shift is conditional on the polarization state of both photons; the result is a two-qubit quantum logic gate. The gate exploits the extremely large optical nonlinearities that are achievable in cavity QED. The cavity operates in a pioneering parameter regime, in which [73]

$$\kappa > (g^2/\kappa) > \gamma, \tag{251}$$

where κ is the cavity-field damping rate, g is the dipole coupling rate of the atom to the cavity, and γ is the transverse atomic decay rate to noncavity modes. Under these conditions, the coherent coupling of the atom to the cavity mode (at rate g^2/κ) dominates incoherent emission into free space (at rate γ). This enables strong coupling of a single atom to the cavity mode, allowing efficient transfer

of electromagnetic fields from input to output channels (at rate κ). Conditional dynamics at the single quantum level has also been achieved with single atoms interacting with very weak microwave fields in superconducting cavities [74]. Atomic wave function phase shifts were produced by microwave fields with, on average, much less than one photon in the cavity. In related work, a quantum memory was implemented, in which the quantum information carried by a two-level atom was transferred to a cavity and subsequently to another atom [236]. Within the same framework, a methodology was developed for the construction of arbitrary quantum computational networks with all the necessary quantum gates to perform all quantum logic operations [237,238]. In cavity QED, sources of decoherence include spontaneous emission from excited states of atoms and cavity decay during gate operation. Maintaining coherence between multiple cavities is problematic. Also, the trapping and localization of atoms inside cavities present formidable difficulties. Possible scaling up of the cavity-QED approaches to more than several qubits remains to be accomplished and poses serious problems that may limit the practical utility of *cavity-QED quantum computers* to special-purpose, small-scale quantum computations (for use in quantum communication, for example).

Cavity QED is also being implemented in the development of possible *quantum computer communication networks.* In the cavity-QED approach to quantum information processing, both the states of atoms confined in cavities and the states of photons interacting with the atoms may serve as qubits to store and transfer quantum information. Although the difficulties in the successful trapping and localization of atoms inside high-finesse optical cavities are considerable (possibly making the development of large-scale universal quantum computers based on the cavity-QED concept an unattainable goal), the development of small-scale, special-purpose quantum information processors involving limited numbers of trapped atoms will likely be possible. For example, the cavity-QED paradigm may provide a practical approach to the development of controlled single-photon sources [239], the synthesis of entangled states [240], and quantum teleportation between cavities [241]. Both photonic and atomic qubits may be exploited with the cavity-QED paradigm, in the form of quantum information networks that enable the implementation of quantum communication protocols and distributed quantum computation [242–246]. Multiple atom-cavity systems located at distant network nodes may be interconnected with optical fibers, or perhaps even use free-space transmission. Analysis has been performed of basic network operations, including local quantum information processing, quantum-state transmission between network nodes, and quantum entanglement distribution [242–248]. Ideal transmission may be permitted after a finite number of trials, without disturbing the quantum information. Possible sources of error include absorption of photons in the optical fibers and cavity mirrors, cavity and laser design errors, and spontaneous emission from excited states.

A recent proof of principle of quantum computation has been accomplished by another approach, which makes innovative use of established nuclear magnetic resonance (NMR) technology. NMR [249,250] can be used as the basis for quantum computation when certain liquids are used along with available NMR instrumentation [251–256]. The qubits are the spins of atomic nuclei in the molecules constituting the liquid. These qubits are extremely well isolated from their environment. The nuclear spin orientations in a single molecule form a quantum data register. The liquid contains about 10^{23} molecules at room temperature and undergoes strong

random thermal fluctuations. The liquid is located in a large magnetic field, and each spin can be oriented either in the direction of the magnetic field ($|\uparrow\rangle = |0\rangle$) or opposite ($|\downarrow\rangle = |1\rangle$). An *NMR quantum computer* operating on N qubits uses molecules having N atoms with distinguishable spins in the frequency domain. The input to the computer is an ensemble of nuclear spins initially in thermal equilibrium. Each spin can be manipulated with resonant rf pulses, and the coupling between neighboring nuclear spins can be exploited to produce quantum logic gates. The spins have dipole-dipole interactions, and a driving pulse in resonance can tip a spin conditional on the state of another spin, thus providing a quantum bus channel. A sequence of rf pulses and delays produces a series of quantum logic gates connecting the initial state to a desired final state. By suitable timing of each pulse, a desired unitary transformation can be resonantly performed on a single spin of a molecule, even though all the spins in the molecule are exposed, since they all have slightly different resonant frequencies. The decoherence times of the spins are long enough that the qubits can be stored for a sufficiently long time. The average magnetic moment of all the nuclei together is big enough to produce a detectable magnetic field for measurement purposes. The liquid consists effectively of a statistical ensemble of single-molecule quantum computers, which can be described by a density matrix. The method exploits the structure present in thermal equilibrium to produce a perturbation in the system's large density matrix that is effectively equivalent to a pure state of much smaller dimension, a pseudo-pure state. The system of molecules, each having N nuclear spins, can be described by a density matrix [251–253],

$$\rho = 2^{-N} I + \rho_\Delta, \tag{252}$$

in which the first term describes an equilibrium part that is proportional to the identity I, and the second term ρ_Δ is a traceless matrix representing the deviation from equilibrium. For an appropriate pulsed field sequence, the deviation transforms as a density matrix, the *deviation density matrix*, and represents the statistical ensemble of single-molecule quantum computers in the form of a bulk effective quantum computer. An effective pure state can be distilled out of ρ_Δ by means of a data compression pulse sequence. An appropriate computational procedure yields a deterministic result in which measuring the ensemble yields a nonvanishing average. Readout is performed by measurement of the magnetization of the bulk sample. This is bulk quantum computation employing large ensembles of quantum systems instead of single systems. Such a bulk quantum computer acts as an ensemble of many small quantum computers carrying out computations independently in parallel. The initial state of each is random, and only ensemble averages of each computer register can be measured. The ensemble can effectively behave like a pure state, since even if, for example, only a small fraction of the systems are in their ground states, the ones that are not can be arranged so that their signals cancel each other, and only the fraction in the ground state produces a nonvanishing signal, making the ensemble appear to be pure. Generally, if a chosen fraction of the states can be labeled, and the rest caused to average away, then an effective pure state can be produced [251–253]. Experimental implementations to date include (1) synthesis of high-resolution samples of several two- and three-qubit molecules [257], (2) implementation of Grover's fast quantum search algorithm for a system with only four states [257–259], (3) a proof of principle for three-qubit quantum computation [260,261], (4) proof-of-principle quantum error

correction [262], (5) implementation of a quantum algorithm determining whether an unknown function is constant, or has value 0 for half its arguments and 1 for the rest [263,264], and (6) implementation of a quantum algorithm for estimating the number of matching items in a search operation [265,266]. The NMR quantum computers have poor scaling with the number of qubits. The measured signal scales as 2^{-N}. This feature will likely limit NMR quantum computers to applications requiring only 10 to 20 qubits [267]. Other concepts involving the manipulation of spin states have also been proposed that use (1) electron spins [268], (2) atomic-force microscopy to manipulate nuclear spins [269,120], and (3) electron-nuclear spin interactions in the Hall regime [270].

NMR can be combined with semiconductor technology in a hybrid quantum computer implementation, the *silicon-based nuclear spin quantum computer*. Since it is unlikely that NMR quantum computers can be scaled up to produce large-scale quantum computations involving very large numbers of qubits, a hybrid concept has been proposed that uses semiconductor physics to deterministically manipulate nuclear spins [271]. The silicon-based nuclear spin quantum computer would consist of an equally spaced linear or planar array of dopant phosphorus nuclear spins implanted in a silicon semiconductor crystal, separated by an insulator layer from overlaying voltage-controlled metal gate electrodes; the gate electrodes would implement quantum logic operations by affecting the shape of the electron wavefunction surrounding each phosphorus nucleus. The qubits are the nuclear spins of the phosphorus nuclei embedded periodically in the silicon crystal, each located directly beneath a gate referred to as an "A gate." A phosphorus atom in a silicon host is an electron donor, and at room temperature one of its outer electrons can move freely in the crystal; however, at the very low temperature of operation of the device, the electron is weakly bound by the phosphorus ion, and the electron spin can interact with the nuclear spin. Thus, the weakly bound electron spin can affect the state of a qubit, since electron and nuclear spins are coupled by the hyperfine interaction [249]. Also, the electrons can mediate nuclear spin interactions and facilitate the measurement of nuclear spins. A voltage applied to an A gate can cause the wave function of the electron bound to the phosphorus nucleus beneath it to become altered, thereby changing its overlap with the nucleus. This electron-nucleus interaction affects the relative energies of the nuclear qubit, and therefore also the resonant rf frequency needed to cause a nuclear spin flip. This makes it possible for a resonant rf pulse to selectively change the state of only that nucleus. Between any two neighboring A gates is a "J gate," for affecting the overlap between two electron orbitals bound to neighboring phosphorus nuclei in the lattice. This J gate results in an indirect coupling between the two neighboring phosphorus qubits, and makes it possible to implement the quantum gates necessary for quantum computation. Since it is prohibitively difficult to directly measure the spin state of an individual nucleus, an indirect approach is implemented, involving a chain of interactions among the nuclear spin, its bound electron and a neighboring electron, the external magnetic field, and the J gate overlaying the two electron orbitals; these interactions affect the capacity between neighboring A gate electrodes, which can be measured. Normally, all electron spins are pointed in the direction of the external magnetic field, but if the overlap between two neighboring electron orbitals is sufficiently increased by an applied J-gate voltage, it may become energetically favorable for the pair of electrons to change their state so that their spins are opposite. Whether this happens depends on the direction of whichever

phosphorus spin is coupled most strongly to its bound electron, and that depends on the A-gate voltage. The Pauli exclusion principle does not allow both electrons to hop into the same atom, unless their spins are opposite, and a hop changes the capacitance between the neighboring A electrodes. This same mechanism also enables qubit states to be initialized, since each can be measured individually, and the measured state can be reversed with an NMR pulse if necessary. Before such a device can be successfully implemented, many formidable technological problems must be overcome, including (1) emplacement of individual phosphorus atoms in a prescribed regular array in a perfect Silicon crystal, (2) development of defect-free semiconductor and overlaying layers, (3) limitation of the decoherence rate of the phosphorus qubits in the presence of electrode fluctuations, gate biasing, rf-induced eddy currents, charge fluctuations, spin impurities, and crystal defects, (4) sufficient limitation of the probability of error in each operation, and (5) nanoscale fabrication [271–273].

Another popular solid-state approach to quantum computer development is the *quantum-dot quantum computer*. Various approaches have been considered to the potential development of quantum dot quantum computers [274–286]. In one of the most interesting approaches [277–281], a qubit would be the two spin states of an electron in a single-electron quantum dot, and a quantum register would consist of an array of coupled single-electron quantum dots. Each semiconductor quantum dot would consist of one excess electron with spin 1/2 in a potential well that confines the electron in all three dimensions. Quantum gate operations would be performed by gating of the tunneling barrier between neighboring dots, to produce controlled entanglements of the qubits. The tunnel barrier between dots could be raised or lowered by the application of a higher or lower gate voltage [277,279]. If the barrier is sufficiently reduced, virtual tunneling can occur, resulting in transient spin-spin coupling. Hopping to a neighboring auxiliary ferromagnetic dot can be used to implement single-qubit operations. Also, readout can be implemented through tunneling to a neighboring auxiliary paramagnetic dot, which can nucleate a ferromagnetic domain that could then be measured [277]. Alternatively, spin-dependent tunneling into another neighboring auxiliary dot can enable spin measurement by means of an electrometer [280]. Reversing this procedure might accomplish general-state preparation. Ground-state preparation can be accomplished by cryogenic cooling in a uniform applied magnetic field. In other approaches, the qubit does not consist of electron spin states, but instead of pseudo-spin states, corresponding to charged orbital degrees of freedom [282–285]. Real spin has the advantage of (1) permanent well-defined qubits with no extra dimensions for qubit state leakage, and (2) much longer dephasing times [277]. Although spin degrees of freedom are not significantly affected by fluctuations in electric potential, they are subject to decoherence arising from magnetic coupling to the environment. In other approaches, gate operation may be performed by spectroscopic manipulation. Coherent optical control of quantum-dot states is an important area of research. Picosecond optical excitation can be used to coherently control quantum-dot states on a time scale that is small compared to the decoherence time [286]. Generally, it is expected that solid-state systems, because of their complex internal field and many-particle environment, will subject qubit states to numerous possible mechanisms of quantum decoherence, presenting formidable obstacles to the development of a practical large-scale quantum computer based on the quantum-dot approach.

Another possible condensed-matter approach to quantum computer development involves macroscopic superconducting quantum states. One of these is the *Josephson junction quantum computer.* Efforts are also under way to develop a Josephson junction quantum computer [287–293]. In one relatively simple exploratory approach, a nanoelectronic device would consist of an array of low-capacitance Josephson junctions [287–291]. The device would exploit coherent tunneling in the superconducting state, with the possibility of controlling individual charges by means of Coulomb blockade effects. The Josephson junction qubit is implemented in a small superconducting island connected by a tunnel junction to a superconducting electrode. The qubit consists of two charge states of the superconducting island adjacent to the junction. The logical states differ by one Cooper-pair charge. The island is connected to an ideal voltage source with a gate capacitor between them. An array of such Josephson junction qubits, each with its own voltage source, are connected in parallel with each other and also with a mutual inductor. The array would serve as a quantum register. One- and two-qubit gates can be implemented by application of appropriate sequences of voltages across the junctions, and by the tuning of selected qubits to resonance. Readout can be accomplished by capacitively coupling a dissipative normal-metal single-electron transistor to a qubit [288]. It is encouraging that coherent tunneling of Cooper pairs, and related characteristics of quantum superposition of charge states, have already been theoretically investigated and experimentally demonstrated [294–298]. This simple design presents various challenges: it requires high-precision timing control, and it involves residual two-qubit interactions that will produce errors. An improved design is being considered, in which the Josephson junctions are replaced by SQUIDs (superconducting quantum interference devices) that can be controlled by magnetic fluxes [289]. This design would enable exact on-off switching of the two-qubit coupling, relaxation of the timing control and system parameter requirements, and complete control of two-qubit couplings. Parallel operations on different qubits may be achieved, in principle, by more advanced designs, including additional tunable SQUIDs to decouple different parts of the circuit. Scaling to large numbers of qubits with massively parallel operation will necessitate much more elaborate designs, significant progress in nanotechnology, reduction in working temperature, near-perfect control of time-dependent gate voltages, and much longer decoherence times. It is well also to mention another possible approach to quantum computation using Josephson junctions [293], which would exploit the quantized states of position of superconducting vortices [299–301]. The two basis states of a qubit might be a vortex positioned in one of two neighboring superconducting loops with a Josephson junction between them. A vortex would have to be capable of being in a quantum superposition of positions. In other work, high-temperature-superconductor Josephson junctions are being considered for possible use in the construction of a quantum computer [292].

Another approach to quantum computer development involves a *SQUID quantum computer*, which would exploit the physics of superconducting quantum interference. The quantized flux in a SQUID might also be used as the basic qubit, instead of the charge of a Josephson junction island. This would provide the basis for a potential SQUID quantum computer [302–304]. It is encouraging that experimental demonstrations have been made of quantum jumps in SQUID rings [305] and resonant tunneling of the flux between quantized energy levels in different flux states of a SQUID [306,307]. Although SQUIDs are macroscopic objects, and macroscopic

objects generally suffer decoherence in the extreme, many of the dissipative mechanisms that normally operate in macroscopic systems can be eliminated in SQUID systems [37,308–312]. The Hamiltonian of an rf SQUID can be represented as a two-state system [310]. The SQUID consists of a single tunnel junction with critical current I_c shunted by an inductor L. If a magnetic flux of half the fundamental flux quantum,

$$\phi_0 = \pi\hbar/e, \tag{253}$$

is applied to the loop (e is the magnitude of the charge of the electron), and if

$$1 < 2\pi L I_c/\phi_0 < 5\pi/2, \tag{254}$$

then a two-state system can be created, in which the two states correspond to the loop containing either one flux quantum or none at all [302]. A supercurrent then circulates the SQUID ring in either direction. In principle, a superposition state can also be created, but this has not yet been accomplished, despite concerted attempts [313,314]. One must also be able to entangle multiple qubits with each other. No quantum logic gate has yet been experimentally demonstrated in the SQUID approach. Important issues in the SQUID approach to quantum computer development include the required operating temperature, required junction quality, suppression of competing modes, magnetic coupling of flux qubits to magnetic impurities, unidentified decoherence mechanisms, sufficiently small junction capacitances, and required fabrication technology.

Another innovative approach to quantum computer development involves trapped atoms in optical lattices. Lasers can be used to confine ultracold atoms in periodic lattices [315–325]. The atoms are held together with light (instead of chemical bonds, as in a solid). Laser cooling and trapping techniques, used in producing Bose-Einstein condensation, are also used to form optical lattices. In an optical lattice, ultracold atoms can be arranged in a crystal-like array in an optical potential in which the intensity or polarization of light varies periodically. Near-zero-temperature webs of interfering laser beams can be used to cool a collection of atoms, and the atoms become suspended in well-defined positions in the interfering beams. The separations of the atoms in an optical lattice are hundreds of times that in an ordinary solid. Currently, only about one in ten lattice sites is filled. The potential well depth is $\sim 10^{-9}$ that in a solid, and the dynamical oscillations of the atoms (1 to 100 kHz) are $\sim 10^6$ to 10^9 lower in frequency than in a solid. Defects and impurities are absent in the optical lattice. Through changes in the polarization and the direction of propagation of the laser beams, many different crystalline structures can be created in one, two, or three dimensions. The optical potential seen by an atom in an optical lattice depends on the magnetic quantum number of the atom. Dissipation and decoherence in optical lattices occurs due to spontaneous emission [326]. Evaporative cooling may be able to produce lattices in which every site is filled. Atoms can be trapped in a two-dimensional lattice and cooled to the zero point of motion by resolved-sideband cooling [327]. These characteristics are important for initial state preparation and the manipulation of quantum states. An optical lattice may serve as the arena for *neutral atom quantum computers*, as discussed below. Also, it will likely be possible to create Bose-Einstein condensates trapped in optical lattices [321]. This would provide the arena for *Bose condensate quantum computers.*

It may become possible to implement quantum logic with neutral atoms trapped in an optical lattice, very far off resonance [328]. A qubit would consist of two states of an atom. If the lasers are detuned very far off resonance, photon scattering is made negligible, and high laser intensities will maintain substantial potential wells. By means of laser cooling, the atoms can be prepared in the ground state of the potential well. The lattice geometry can be varied dynamically: changing the angle between different laser polarizations can control the distance between wells. Two atoms trapped in neighboring wells can be forced into the same well by varying the polarization of the trapping lasers. An auxiliary laser can then induce a near-resonant electric dipole, and the electric dipole-dipole potential will provide the predominant interaction between the atoms. Following this, the atoms can be separated by adiabatic rotation of the laser polarization. Quantum gates would be implemented through the induced coherent dipole interactions. Single-qubit operations would be performed with polarized resonant Raman pulses. Two-qubit operations would require conditioning the state of one atom on that of the other. A controlled-NOT gate could be achieved by conditioning the target atomic resonance on a resolvable level shift induced by the control atom. The resonant dipoles would be conditionally turned on only during conditional logic operations, and environmental decoherence would thereby be suppressed. Large numbers of atoms could be entangled by a sequence of two-qubit interactions. If the atoms are lightly confined to separations small relative to the wavelength, then a coherent dipole-dipole interaction can be induced with negligible photon scattering. The coherent level shift can thereby be substantially enhanced, while the cooperative emission rate is substantially suppressed. The atoms couple very weakly to the environment and would interact only during two-qubit logical operations, and all manipulations would be performed rapidly relative to the photon scattering rate, thus impeding spontaneous emission, which is the main source of decoherence. Before an operational neutral atom quantum computer can be successfully developed to perform even elementary quantum computations, many issues must be explored, including (1) increasing the filling fraction of atoms in the lattice, (2) developing methods for addressing and reading out individual qubits, (3) investigating the effect of atomic collisions, and (4) implementing quantum error-correction methods.

Bose condensates in optical lattices provide another innovative approach to quantum computer development. Bose condensates can be confined in an optical dipole trap [329]. They can also be created in an optical lattice [330]; the theory of condensates in optical potentials has been investigated [331]. A very innovative scheme has been proposed [332] to fill an optical lattice with a Bose condensate, and exploit ideas related to Mott transitions in optical lattices [333]. A far-detuned optical lattice acts as a conservative potential and could be loaded with a Bose condensed atomic vapor, resulting in tens of atoms per lattice site. It has been argued [333] that the dynamics of bosonic atoms corresponds to that of a Bose-Hubbard model [334], which describes the hopping of bosonic atoms between the lowest vibrational states of lattice sites. The important system parameters can be controlled by appropriate laser parameters and configurations. The model predicts a phase transition from a superfluid phase to a Mott insulator phase at low temperature. This results in the formation of an optical crystal with long-range order and period controlled by the laser light. A finite gap is produced in the excitation spectrum. An optical crystal could be created with uniform lattice occupation, or tailored atomic patterns could be produced. This would occur at sufficiently

low temperature that cold laser-controlled coherent interactions could implement conditional dynamics in moving trap potentials. Methods were investigated for producing two-qubit quantum gates and highly entangled states, and may provide the basis for a possible *Bose condensate quantum computer.*

23. QUANTUM ROBOTS

Since computer technology has often been closely linked with automata or robot technology, it is a natural progression to consider the possibility of a *quantum robot.* A quantum robot would be a mobile quantum system containing a quantum computer and other ancillary systems [335–338]. It would perform tasks such as measuring the environment and changing the state of the environment. The robot's quantum computer can be modeled as a cyclic network of quantum gates. Computations performed by the quantum robot would include determining its next action, and recording information about the environment. Actions of the robot would include moving itself and recording information on the environment.

For analytical and numerical convenience, models of quantum robots have been developed based on discretized space and time. Environments can be open or closed, and are modeled to include arbitrary numbers and types of systems moving in one-, two-, and three-dimensional spatial lattices. The systems are characterized by some internal quantum numbers, and can interact with each other or be free.

Quantum robot dynamics is described in terms of performing tasks. Tasks are described by their goals, such as producing changes in the state of the environment, and making measurements by transfer of information from the environment to the robot.

An example of a task might be to move each system, located in a spatial region R of a one-dimensional lattice, two sites to the right if the destination site is unoccupied. The path taken by the robot and the criteria for determining when it is inside or outside the region R must be specified, and the robot must be able to make the required movements. If there are, for example, three systems in region R at locations x_1, x_2, and x_3, then the initial state of the environment in that region is

$$|x\rangle \equiv |x_1\rangle\,|x_2\rangle\,|x_3\rangle\,, \tag{255}$$

and the final state is

$$|x+2\rangle \equiv |x_1+2\rangle\,|x_2+2\rangle\,|x_3+2\rangle\,. \tag{256}$$

If the initial state of R is a linear superposition,

$$|\psi\rangle = \sum_x c_x\,|x\rangle\,, \tag{257}$$

of three position states $|x\rangle$ in R, then the final state is

$$|\psi'\rangle = \sum_x c_x\,|x+2\rangle\,. \tag{258}$$

This equation illustrates the fact that quantum robots can complete the same task simultaneously on many environments.

Another task might be to perform measurements or experiments on the environment: for example, to determine the distance between a particle and the quantum robot.

The dynamics of each task can be described as a sequence of alternating computation and action phases. The purpose of each computation phase is to determine the action of the robot in the subsequent action phase, and to record local environment information. The computational input to the robot's computer includes the local state of the environment and other useful information, such as the output of the previous computation phase. During each action phase, the state of the environment can be changed. What happens during an action phase depends on the state of the output system and the state of the local environment. (A simple example of an environment is a one-dimensional lattice of qubits, or a one-dimensional lattice containing a particle located at some site.)

A unitary step operator T is associated with each task and describes the task dynamics during one time step. The system dynamics for n future directed time steps is represented by T^n, and for n past directed time steps by $(T^\dagger)^n$. The step operator T has two components,

$$T = T_c + T_a, \tag{259}$$

where T_c and T_a represent the computation and action phases, respectively, of the quantum robot.

The robot's quantum computer includes a finite-state output system o. In the computation phase represented by the operator T_c, the action to be carried out is determined. The states of o and the nearby environment are computational inputs. The multistep computation determines a new state of o as output. The action phase represented by T_a is carried out based on the state of o, and includes motion of the quantum robot and local changes in the state of the environment. The computer also has a control qubit c to regulate whether T_c or T_a is active. If c is in state $|0\rangle$, then T_c is active. If c is in state $|1\rangle$, then T_a is active. The last step of T_c or T_a includes the changes $|0\rangle \Rightarrow |1\rangle$ or $|1\rangle \Rightarrow |0\rangle$, respectively. The operators T_c and T_a must satisfy certain requirements.

The requirement that T_c not change the robot location or the state of the environment is expressed as follows [336]:

$$T_c = \sum_{xE} P^{\mathrm{e}}_{xE} T_c P^{\mathrm{e}}_{xE} P^{\mathrm{c}}_{o}, \tag{260}$$

where

$$P^{\mathrm{e}}_{xE} = |xE\rangle \langle xE| \tag{261}$$

is a projection operator for the quantum robot when it is located at site x in state $|x\rangle$ and the environment is in state $|E\rangle$, and

$$|xE\rangle = |x\rangle |E\rangle , \tag{262}$$

where the tensor product is implicit. Equation (260) ensures that iteration of T_c does not change the location of the robot or the state of the environment. Also in Eq. (260),

$$P^{\mathrm{c}}_{0} = |0\rangle \langle 0| \tag{263}$$

is the projection operator for the control qubit in state $|0\rangle$, and it ensures that T_c is inactive if the control qubit is in state $|1\rangle$. Another condition on T_c follows from the requirement that it depend on the environment only in the neighborhood of the quantum robot [336].

The action phase operator T_a depends on the states of o, but does not change them. This results in an algebraic condition on T_a similar to Eq. (260), namely [336],

$$T_a = \sum_{xx'l_1} P^{\mathrm{qr}}_{x'} P^{\mathrm{o}}_{l_1} T_a P^{\mathrm{o}}_{l_1} P^{\mathrm{qr}}_{x} P^{\mathrm{c}}_{1} , \tag{264}$$

where $P^{\mathrm{o}}_{l_1}$ is the projection operator for o in state $|l_1\rangle$, P^{qr}_{x} is the projection operator for the quantum robot at site x, P^{c}_{1} is the projection operator for c in state $|1\rangle$, and the sum restricts any movement during a time step to a neighboring site only. Also, T_a is independent of the states of the computer and the states of distant environmental systems, and this results in another algebraic condition on T_a [336].

The time development of a task can be expressed in terms of a sum over paths [339]. The overall state $|\psi(n)\rangle$ of the system after n time steps is

$$|\psi(n)\rangle = T^n |\psi(0)\rangle , \tag{265}$$

where $|\psi(0)\rangle$ is the initial overall state of the system. If $|b\rangle$, $|l\rangle$, and $|i\rangle$ denote basis states for the computer, output, and control qubit, respectively, then a basis state for the overall system is

$$|blixE\rangle = |b\rangle\,|l\rangle\,|i\rangle\,|x\rangle\,|E\rangle , \tag{266}$$

and by completeness of the set of states, one has

$$\sum_{blixE} |blixE\rangle\,\langle blixE| = 1. \tag{267}$$

Substituting Eq. (267) in Eq. (265), one has

$$\begin{aligned} |\psi(n)\rangle &= T^n \left(\sum_{blixE} |blixE\rangle\,\langle blixE| \right) |\psi(0)\rangle \\ &= \sum_{b_1 l_1 i_1 x_1 E_1} T^n |b_1 l_1 i_1 x_1 E_1\rangle\,\langle b_1 l_1 i_1 x_1 E_1|\psi(0)\rangle , \end{aligned} \tag{268}$$

in which dummy summation variables b, l, i, x, and E are replaced by b_1, l_1, i_1, x_1, and E_1, respectively. Therefore, the amplitude for ending in the state $|blixE\rangle$ is

$$\langle blixE|\psi(n)\rangle = \sum_{b_1 l_1 i_1 x_1 E_1} \langle blixE| T^n |b_1 l_1 i_1 x_1 E_1\rangle\,\langle b_1 l_1 i_1 x_1 E_1|\psi(0)\rangle . \tag{269}$$

The notation is simplified if we define

$$|wi\rangle \equiv |blixE\rangle . \tag{270}$$

Then Eq. (269) can be written as

$$\langle wi|\psi(n)\rangle = \sum_{w_1 i_1} \langle wi| T^n |w_1 i_1\rangle\,\langle w_1 i_1|\psi(0)\rangle . \tag{271}$$

The matrix element $\langle wi| T^n |w_1 i_1\rangle$ appearing in Eq. (271) gives the amplitude for evolving from the state $|w_1 i_1\rangle$ to the state $|wi\rangle$ in n steps.

It is true that

$$T^n = T\,1T\,1 \ldots 1T . \tag{272}$$

Therefore, substituting Eq. (272) and the completeness relation, Eq. (267), in the matrix element $\langle wi|\, T^n\, |w_1 i_1\rangle$, one obtains the following expression [336]:

(273)
$$\langle wi|\, T^n\, |w_1 i_1\rangle = \sum_{w_2 i_2 \ldots w_n i_n} \langle wi|\, T\, |w_n i_n\rangle \langle w_n i_n|\, T\, |w_{n-1} i_{n-1}\rangle \ldots \langle w_2 i_2|\, T\, |w_1 i_1\rangle .$$

As in the path integral approach [339], Eq. (273) can also be written in terms of a sum over paths of states $\{|wi\rangle\}$ of length $n+1$, where the initial element is $|w_1 i_1\rangle$, and the final element is $|wi\rangle$, namely,

$$\begin{aligned}
&\langle wi|\, T^n\, |w_1 i_1\rangle \\
&\quad = \sum_{\substack{\text{paths } p \text{ of} \\ \text{length } n+1}} \langle wi|p_{n+1}\rangle \langle p_{n+1}|\, T\, |p_n\rangle \langle p_n|\, T\, |p_{n-1}\rangle \ldots \langle p_2|\, T\, |p_1\rangle \langle p_1|w_1 i_1\rangle \\
&\quad = \sum_{\substack{\text{paths } p \text{ of} \\ \text{length } n+1}} \langle p_{n+1}|\, T\, |p_n\rangle \langle p_n|\, T\, |p_{n-1}\rangle \ldots \langle p_2|\, T\, |p_1\rangle \langle p_{n+1}|wi\rangle^* \langle p_1|w_1 i_1\rangle .
\end{aligned}$$

(274)

The control qubit projection operators are given by Eq. (263), together with

(275)
$$P_1^c = |1\rangle \langle 1| .$$

Also, by completeness, one has

(276)
$$P_0^c + P_1^c = 1 ,$$

and one can therefore write

(277)
$$T^n = (P_0^c + P_1^c)\, T\, (P_0^c + P_1^c)\, T\, (P_0^c + P_1^c) \ldots (P_0^c + P_1^c)\, T\, (P_0^c + P_1^c) .$$

From Eqs. (259), (260), and (264), one has

(278)
$$T\, P_1^c = (T_c + T_a)\, P_1^c = T_a P_1^c = T_a ,$$

since

(279)
$$P_1^c P_0^c = 0, \qquad P_1^c P_1^c = P_1^c, \qquad P_0^c P_0^c = P_0^c .$$

Similarly,

(280)
$$T\, P_0^c = T_c .$$

Using Eqs. (278) and (280) in Eq. (277), one obtains [336]

(281)
$$T^n = \sum_{v_1 = a,c} \sum_{t=1}^{n} \sum_{h_1, h_2, \ldots h_t = 1}^{\delta(\Sigma, n)} (P_0^c + P_1^c)\, (T_{v_t})^{h_t} \left(T_{v_{t-1}}\right)^{h_{t-1}} \ldots (T_{v_2})^{h_2}\, (T_{v_1})^{h_1} ,$$

where $v_{j+1} = a$ if $v_j = c$, and $v_{j+1} = c$ if $v_j = a$. The summation upper limit $\delta(\Sigma, n)$ means that the sum must satisfy $h_1 + h_2 + \ldots + h_t = n$. Equation (281) expresses T^n as a sum of alternating computation and action phase operators. The operators T_a and T_c do not commute, and the operators for each phase are time

ordered, with $\left(T_{v_{j+1}}\right)^{h_{j+1}}$ occurring after $\left(T_{v_j}\right)^{h_j}$. With Eq. (281), it can be shown that [336]

$$\begin{aligned}\langle wi|\, T^n\, |w_1 0\rangle &= \sum_{t=1}^{n} \sum_{w_2 \ldots w_t} \sum_{h_1, h_2, \ldots h_t = 1}^{\delta(\Sigma, n)} \langle wi|\, \left(T_{v_t}\right)^{h_t}\, |w_t\rangle \ldots \\ &\times \langle w_3|\, \left(T_a\right)^{h_2}\, |w_2\rangle\, \langle w_2|\, \left(T_c\right)^{h_1}\, |w_1\rangle\,, \end{aligned} \tag{282}$$

where

$$|w\rangle \equiv |b\rangle\, |l\rangle\, |x\rangle\, |E\rangle\,. \tag{283}$$

In terms of paths, the same matrix element becomes [336]

$$\begin{aligned}\langle wi|\, T^n\, |w_1 0\rangle &= \sum_{t=1}^{n} \sum_{\text{paths } p \text{ of length } t+1} \sum_{h_1, h_2, \ldots h_t = 1}^{\delta(\Sigma, n)} \langle p_{t+1} i|\, \left(T_{v_t}\right)^{h_t}\, |p_t\rangle \ldots \\ &\times \langle p_3|\, \left(T_a\right)^{h_2}\, |p_2\rangle\, \langle p_2|\, \left(T_c\right)^{h_1}\, |p_1\rangle\, \langle w|p_{t+1}\rangle\, \langle p_1|w_1\rangle\,, \end{aligned} \tag{284}$$

where

$$|p_j\rangle \equiv |w_j\rangle \equiv |b_j\rangle\, |l_j\rangle\, |x_j\rangle\, |E_j\rangle \tag{285}$$

denotes the jth state in path p.

The formalism given above was used in a simple example in which the environment consists of one particle on a one-dimensional spatial lattice, and the robot is to determine its distance from the particle [336]. To complete the task, the robot moves to the right on the lattice, and counts the number of lattice sites as it moves. When the particle is located, the number of steps is registered as the distance. The robot then returns to its initial position, and the task is complete. More complex tasks that result in entanglement can also be addressed: tasks involving decision trees of sequences of measurements of noncommuting observables, or even tasks of factoring numbers [139] or searching a database [340], could also be treated as tasks for the quantum robot.

The possibility of a qubit device quantum dynamically affecting and reacting to both itself and its quantum environment is interesting. However, the same decoherence issues facing quantum computer development will also apply to quantum robots. Notwithstanding these difficulties, heroic efforts have been successfully made in recent years to develop quantum error-correction methods to overcome quantum decoherence problems (see Sect. 21).

24. CONCLUSIONS

Revolutionary new advances have been made recently in the areas of quantum communication, quantum information processing, quantum computing, and quantum cryptography. These advances have led to a wide variety of potentially useful qubit devices. Several of these devices (such as interaction-free detectors, quantum key receivers, quantum games, all-optical quantum information processors, and various quantum gates) offer near-term opportunities for practical development. Other qubit devices must first overcome the obstacle of quantum decoherence. It is therefore important that the physics of quantum decoherence be much more extensively and thoroughly investigated, both experimentally and theoretically, if these qubit devices are to become a useful reality. Although heroic efforts have been made to develop both theory and methods of quantum error correction and decoherence

control, many practical issues remain, and it is important that these theoretical methods be physically implemented and tested.

Qubits have been successfully implemented with photons, atoms, and nuclear spins, including the production of superposition states and qubit entanglements. However, the qubits that would form the basis for quantum computers based on quantum dots, Josephson junctions, SQUIDs, and Bose condensates remain to be experimentally demonstrated. It is important to stress that a viable qubit must not only be a two-state system, it must also be capable of existing in a superposition of Boolean states and being entangled with other qubits.

To test the validity of the various approaches to useful quantum information processing, it is important to implement a variety of qubit entanglers that can construct multiple-qubit entanglements using photons, atoms, nuclear spins, quantum dots, Josephson junctions, SQUIDs, and Bose condensates. For the full power of quantum technology to be exploited, large-scale controlled entanglements must be producible.

The quantum key receiver is ready for practical development, and should be useful both in quantum cryptography and in fundamental studies of the generalized measurement of photonic qubits, based on a POVM. Deterministic single-photon sources need development.

Although quantum game theory has only begun to develop, it is possible that interesting quantum games could be constructed with NMR or all-optical quantum information processors. Also, all the various quantum gates should be implemented with all the various types of qubits, and their engineering design should be optimized to meet the severe fidelity requirements for large-scale quantum computation.

A variety of EPR-pair sources should be developed, along with innovative methods for efficiently storing EPR correlated states. Also, Bell-state synthesizers, using various types of qubits, need much further development for use in quantum dense coding and quantum teleportation. Bell-state analyzers must be developed that can measure all four Bell states; for that purpose, it is important that gates be developed that enable robust nonlinear interaction between two qubits.

Robust Bell-state analyzers are essential for the useful implementation of entanglement swapping. Theoretical generalizations of entanglement swapping to manipulate entangled multiparticle systems remain to be experimentally demonstrated. Possible applications of entanglement swapping include cryptographic conferencing and quantum telephone exchanges. Decoherence is a critical issue also for the development of practical entanglement swappers and quantum teleporters. It is presently not possible to store separated EPR particles for periods of time that are sufficiently long for many applications. Still awaiting exploration is the possible implementation of quantum-error correction methods, which are needed for reliable quantum teleportation and for long-distance quantum key distribution.

Although quantum states cannot be cloned, it is important to thoroughly investigate methods for making approximate copies of arbitrary quantum states for possible information processing and quantum cryptographic applications. All-optical quantum information processors are ready for practical development and should be exploited for proof-of-principle demonstrations of quantum computation, and as small special-purpose quantum information processors.

The construction of practical universal quantum computers is presently not feasible, and must await further new revolutionary discoveries and advances. The successful development of quantum simulators could enable simulations of physical

systems that are intractable on classical computers. Although a quantum factorizer does not presently exist that can factor even a 5-digit number, if one were successfully developed to factor numbers of more than 250 digits, many cryptosystems would be rendered insecure and obsolete.

Although ion-trap quantum computers are unlikely candidates for performing large-scale quantum computations involving more than 100 qubits, the ion-trap technology affords continuing opportunities for experimental investigations of many issues of quantum decoherence and quantum information processing, and may also lead to the development of special-purpose, small-scale quantum computers.

The cavity QED approach to quantum computing needs much more extensive experimental verification. Cavity QED continues to serves as a near-term arena for experimental investigations of the fundamental physics of quantum information processing and quantum decoherence, and may also be useful for small-scale quantum computation; however, it is unlikely that it will lead to a practical large-scale quantum computer. Cavity QED does offer interesting possibilities for the development of quantum communication networks.

The NMR quantum computer is the first small-scale proof-of-principle quantum computer, and it continues to furnish useful insights into practical quantum information processing; because of its poor scaling, however, it will likely be limited to computations requiring only 10 to 20 qubits. Nevertheless, the possibility of combining NMR with semiconductor technology is currently receiving considerable attention. It is hoped that the silicon-based, nuclear spin quantum computer can be scaled up to perform large-scale quantum computations involving large numbers of qubits. The quantum-dot quantum computer is another attempt to implement semiconductor technology in quantum computation. However, severe problems posed by quantum decoherence face any quantum computer based on the solid state.

Josephson junction and SQUID quantum computers would be based on the superconducting state, and for both types, robust viable qubits (which can exist in superpositions and be entangled with each other) remain to be demonstrated. Neutral atoms or Bose condensates trapped in optical lattices provide still another possible innovative approach to quantum computer development.

Quantum robots offer the exciting possibility of a qubit device that can quantum dynamically affect and react to both its environment and itself. The successful implementation of quantum robots, quantum computers, and most qubit devices will depend on incorporating effective quantum error-correction methods, together with effective decoherence avoidance and control.

The future of quantum information science and technology appears bright, as do the prospects for successful implementations of a broad spectrum of innovative qubit devices.

25. ACKNOWLEDGEMENT

This work was sponsored by the U.S. Army Research Laboratory. The hospitality is gratefully acknowledged of the University of Cambridge Isaac Newton Institute for Mathematical Sciences, where some of this work was completed. The author thanks Prof. Samuel Lomonaco for the invitation to present this lecture as part of the short course, *Quantum Computation: The Grand Mathematical Challenge for the Twenty-first Century and the Millennium*, at the American Mathematical Society Annual Meeting, 17–18 January 2000, in Washington DC.

REFERENCES

[1] H. E. Brandt, "Quantum Decoherence in Qubit Devices," Opt. Eng. **37**, 600–709 (1998).

[2] B. Schumacher, "Quantum Coding," Phys. Rev. A **51**, 2738–2747 (1995).

[3] B. Schumacher and M. D. Westmoreland, "Sending Classical Information via Noisy Quantum Channels," Phys. Rev. A **56**, 131–138 (1997).

[4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary Gates for Quantum Computation," Phys. Rev. A **52**, 3457–3467 (1995).

[5] H. E. Brandt, Qubit Devices and the Issue of Quantum Decoherence, Progr. Quantum Electron. **22**, 257–370 (1998).

[6] A. C. Elitzur and L. Vaidman, "Quantum Mechanical Interaction-Free Measurements," Found. Phys. **23**, 987–997 (1993).

[7] L. Vaidman, "On the Realization of Interaction-Free Measurements," Quant. Opt. **6**, 119–124 (1994).

[8] P. G. Kwait, "Experimental and Theoretical Progress in Interaction-Free Measurements," Physica Scripta **T76**, 115–121 (1998).

[9] P.A.M. Dirac, *The Principles of Quantum Mechanics,* Revised Fourth Edition, Oxford University Press (1967).

[10] R. P. Feynman, *The Theory of Fundamental Processes,* Addison-Wesley Publishing Company, Redwood City, California (1961).

[11] R. P. Feynman, R. B. Leighton, and M. L. Sands, *The Feynman Lectures on Physics, Volume III, Quantum Mechanics,* Addison-Wesley Publishing Company, Redwood City, California (1989).

[12] G. Baym, *Lectures on Quantum Mechanics, Addison-Wesley Publishing Company,* Reading, Massachusetts (1969).

[13] V. Degiorgio, "Phase Shift Between the Transmitted and the Reflected Optical Fields of a Semireflecting Lossless Mirror is $\pi/2$," Am. J. Phys. **48**, 81–82 (1980).

[14] A. Zeilinger, "General Properties of Lossless Beamsplitters in Interferometry," Am. J. Phys. **49**, 882–883 (1981).

[15] Z. Y. Ou and L. Mandel, "Derivation of Reciprocity Relations for a Beamsplitter from Energy Balance," Am J. Phys. **57**, 66–67 (1989).

[16] A. Peres, *Quantum Theory: Concepts and Methods,* Kluwer, Dordrecht (1993).

[17] E. B. Davies, *Quantum Theory of Open Systems,* Academic, New York (1976).

[18] C. W. Helstrom, *Quantum Detection and Estimation Theory,* Academic Press, New York (1976).

[19] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, "Eavesdropping on Quantum-Cryptographical Systems," Phys. Rev. A **50**, 1047–1056 (1994).

[20] H. E. Brandt, "Inconclusive Rate with a Positive Operator Valued Measure," preprint NI99015-CCP, University of Cambridge Isaac Newton Institute for Mathematical Sciences (1999).

[21] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., "Aspects of Entangled Translucent Eavesdropping in Quantum Cryptography," Phys. Rev. A **56**, 4456–4465 (1997); **58**, 2617 (1998).

[22] H. E. Brandt and J. M. Myers, Invention Disclosure: POVM Receiver for Quantum Cryptography (U.S. Army Research Laboratory, Adelphi, MD, 1996).

[23] J. M. Myers and H. E. Brandt, "Converting a Positive Operator-Valued Measure to a Design for a Measuring Instrument on the Laboratory Bench," Meas. Sci. Technol. **8**, 1222–1227 (1997).

[24] H. E. Brandt, "Eavesdropping Optimization for Quantum Cryptography using a Positive Operator Valued Measure," Phys. Rev. A **59**, 2665–2669 (1999).

[25] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," Phys. Rev. Lett. **68**, 3121–3124 (1992).

[26] C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum Cryptography," Sci. Am., 50–57 (October 1992).

[27] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," J. Cryptology **5**, 3–28 (1992).

[28] J. D. Franson and H. Ilves, "Quantum Cryptography Using Optical Fibers," Appl. Opt. **33**, 2949–2954 (1994).

[29] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, "Quantum Cryptography," Contemp. Phys. **36**, 149–163 (1995).
[30] S.J.D. Phoenix and P. D. Townsend, "Quantum Cryptography: How to Beat the Code Breakers Using Quantum Mechanics," Contemp. Phys. **36**, 165–195 (1995).
[31] A. E. Ekert, "From Quantum Code-Making to Quantum Code-Breaking," in *The Geometric Universe: Science, Geometry and the Work of Roger Penrose*, A. A. Huggett et al, editors, 195–214, Oxford University Press (1998).
[32] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be Cloned," Nature (London) **299**, 802–803 (1982).
[33] D. Dieks, "Communication by EPR Devices," Phys. Lett. **92A**, 271–272 (1982).
[34] B.E.A. Saleh and M. C. Teich, *Fundamentals of Photonics*, John Wiley and Sons, Inc., New York (1991).
[35] P. Busch, M. Grabowski, and P. J. Lahti, *Operational Quantum Physics*, Springer, Berlin (1995).
[36] C. Cohen-Tannoudji, B. Diu, and F. Laloe, *Quantum Mechanics,* Volumes 1 and 2, Wiley, New York (1977).
[37] R. Omnes, *The Interpretation of Quantum Mechanics*, Princeton University Press, Princeton, NJ (1994).
[38] R. Omnes, *Understanding Quantum Mechanics*, Princeton University Press, Princeton, NJ (1999).
[39] D. Giulini, E. Joos, C. Kiefer, J. Kupsch, I. O. Stamatescu, and H. D. Zeh, *Decoherence and the Appearance of a Classical World in Quantum Theory,* Springer, Berlin (1996).
[40] W. H. Zurek, "Pointer Basis of Quantum Apparatus: Into What Mixture Does the Wave Packet Collapse?," Phys. Rev. D **24**, 1516–1525 (1981).
[41] W. H. Zurek, "Environment-Induced Superselection Rules," Phys. Rev. D **26**, 1862–1880 (1982).
[42] W. H. Zurek, "Decoherence and the Transition from Quantum to Classical," Phys. Today, 36–44 (October 1991).
[43] J. R. Anglin, J. P. Paz, and W. H. Zurek, "Deconstructing Decoherence," Phys. Rev. A **55**, 4041–4053 (1997).
[44] W. H. Zurek, "Decoherence, Einselection and the Existential Interpretation (The Rough Guide)," Phil. Trans. R. Soc. Lond. A **356**, 1793–1821 (1998).
[45] W. H. Zurek, "Decoherence, Chaos, Quantum-Classical Correspondence, and the Algorithmic Arrow of Time," Physica Scripta **T76**, 186–198 (1998).
[46] J. P. Paz and W. H. Zurek, "Quantum Limit of Decoherence: Environment Induced Superselection of Energy Eigenstates," quant-ph/9811026 (1998).
[47] K. Hepp and E. H. Lieb, "Phase Transitions in Reservoir-Driven Open Systems with Applications to Lasers and Superconductors," Helv. Phys. Acta **46**, 573–603 (1973).
[48] R. Omnès, "General Theory of the Decoherence Effect in Quantum Mechanics," Phys. Rev. A **56**, 3383–3394 (1997).
[49] R. Omnès, "Theory of the Decoherence Effect," Fortschr. Phys. **46**, 771–777 (1998).
[50] C. Kiefer and E. Joos, "Decoherence: Concepts and Examples," quant-ph/9803052 (1998).
[51] J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior,* John Wiley and Sons, Inc., New York (1967).
[52] D. Blackwell and M. A. Girshick, *Theory of Games and Statistical Decisions,* Dover Publications, Inc., New York (1979).
[53] R. D. Luce and H. Raiffa, *Games and Decisions: Introduction and Critical Survey,* Dover Publications, Inc., New York (1989).
[54] M. D. Davis, *Game Theory: A Nontechnical Introduction,* Dover Publications, Inc., Mineola, New York (1997).
[55] A. P. Maitra and W. D. Sudderth, *Discrete Gambling and Stochastic Games,* Springer-Verlag, New York (1996).
[56] D. A. Meyer, "Quantum Strategies," Phys. Rev. Lett. **82**, 1052–1055 (1999).
[57] J. Eisert and M. Wilkens, "Quantum Games and Quantum Strategies," lanl e-print quant-ph/9806088 (1998).
[58] L. Goldenberg. L Vaidman, and S. Wiesner, "Quantum Gambling," lanl e-print quant-ph/9808001 (1998).
[59] R. F. Werner, "Optimal Cloning of Pure States," Phys. Rev. A **58**, 1827–1832 (1998).

[60] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
[61] N. Gisin and B. Huttner, "Quantum Cloning, Eavesdropping and Bell's Inequality," Phys. Lett. A **228**, 13–21 (1997).
[62] R. Derka, V. Buzek, and A. K. Ekert, "Universal Algorithm for Optimal Estimation of Quantum States for Finite Ensembles via Realizable Generalized Measurement," Phys. Rev. Lett. **80**, 1571–1575 (1998).
[63] P. G. Kwait, K. Mattle, H. Winfurter, and A. Zeilinger, "New High-Intensity Source of Polarization-Entangled Photon Pairs," Phys. Rev. Lett. **75**, 4337–4341 (1995).
[64] P. G. Kwait, E. Waks, A. G. White, I. Appelbaum and P. H. Eberhard, "Ultra-Bright Source of Polarization Entangled Photons," quant-ph/9810003 (1998), to appear in Phys. Rev. A (1999).
[65] C. H. Bennett, S. J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," Phys. Rev. Lett. **69**, 2881–2884 (1992).
[66] K. Mattle, H. Weinfurter, P. G. Kwait, and A. Zeilinger, "Dense Coding in Experimental and Quantum Communication," Phys. Rev. Lett. **76**, 4656–4659 (1996).
[67] A. Zeilinger, "Quantum Entanglement: A Fundamental Concept Finding its Applications," Physica Scripta **T-76**, 203–209 (1998).
[68] N. Bloembergen, *Nonlinear Optics*, World Scientific, Singapore (1996).
[69] *Selected Papers on Nonlinear Optics*, H. E. Brandt, editor, SPIE Optical Engineering Press, Bellingham, WA (1991).
[70] J. D. Franson, "Cooperative Enhancement of Optical Quantum Gates," Phys. Rev. Lett. **78**, 3852–3855 (1997).
[71] J. D. Franson and T. B. Pittman, "Quantum Logic Operations Based on Photon Exchange Interactions," Phys. Rev. A **60**, 917–936 (1999).
[72] J. D. Franson and T. B. Pittman, "Nonlocality in Quantum Computing," Fortschr. Phys. **46**, 6–8 (1998).
[73] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of Conditional Phase Shifts for Quantum Logic," Phys. Rev. Lett. **75**, 4710–4713 (1995).
[74] M. Brune, P. Nussenzveig, F. Schmidt-Kaler, F. Bernardot, A. Maali, J. M. Raimond, and S. Haroche, "From Lamb Shift to Light Shifts: Vacuum and Subphoton Cavity Fields Measured by Atomic Phase Sensitive Detection," Phys. Rev. Lett. **72**, 3339–3342 (1994).
[75] *Atomic, Molecular, and Optical Physics Handbook*, G.W.F. Drake, editor, American Institute of Physics, Woodbury, New York (1996).
[76] A. Zeilinger, H. J. Bernstein, and M. A. Horne, "Information Transfer with Two-State Two-Particle Quantum Systems," J. Mod. Opt. **41**, 2375–2384 (1994).
[77] W. Pauli, "The Connection Between Spin and Statistics," Phys. Rev. **58**, 716–722 (1940).
[78] R. F. Streater and A. S. Wightman, *PCT, Spin and Statistics, and All That*, Addison-Wesley Publishing Company, Inc., Redwood City, CA (1989).
[79] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of Subpicosecond Time Intervals Between Two Photons by Interference," Phys. Rev. Lett. **59**, 2044–2046 (1987).
[80] M. Oberparleiter, "Bosonic and Fermionic Statistics in Two-Photon Interference," Diploma thesis, University of Innsbruck (1997).
[81] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "'Event-Ready-Detectors,' Bell Experiment via Entanglement Swapping," Phys. Rev. Lett. **71**, 4287–4290 (1993).
[82] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," Phys. Rev. Lett. **70**, 1895–1899 (1993).
[83] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-State Entanglement and Quantum Error Correction," Phys. Rev. A **54**, 3824–3851 (1996).
[84] S. W. Bose, V. Vedral, and P. L. Knight, "Multiparticle Generalization of Entanglement Swapping," Phys. Rev. A **57**, 822–829 (1998).
[85] S. Bose, P. L. Knight, M. Murao, M. B. Plenio, and V. Vedral, "Implementations of Quantum Logic: Fundamental and Experimental Limits," Phil. Trans. R. Soc. Lond. A **356**, 1823–1839 (1998).
[86] J. W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental Entanglement Swapping: Entangling Photons that Never Interacted," Phys. Rev. Lett. **80**, 3891–3894 (1998).

[87] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, "Experimental Quantum Teleportation," Nature **390**, 575–579 (1997).
[88] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental Realization of Teleportating an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels," Phys. Rev. Lett. **80**, 1121–1125 (1998).
[89] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional Quantum Teleportation," Science **282**, 706–709 (1998).
[90] M. A. Nielsen, E. Knill, and R. Laflamme, "Complete Quantum Teleportation Using Nuclear Magnetic Resonance," Nature **396**, 52–55 (1998).
[91] 180. V. Buzek and M. Hillery, "Quantum Copying: Beyond the No-Cloning Theorem," Phys. Rev. A **54**, 1844–1852 (1996).
[92] V. Buzek, S. L. Braunstein, M. Hillery, and D. Bruss, "Quantum Copying: A Network," Phys. Rev. A **56**, 3446–3452 (1997).
[93] M. Hillery and V. Buzek, "Quantum Copying: Fundamental Inequalities," Phys. Rev. A **56**, 1212–1216 (1997).
[94] V. Buzek, V. Vedral, M. Plenio, P. L. Knight, and M. Hillery, "Broadcasting of Entanglement via local Copying," Phys. Rev. A **55**, 3327–3332 (1997).
[95] V. Buzek and M. Hillery, "Universal Optimal Cloning of Arbitrary Quantum States: From Qubits to Quantum Registers," Phys. Rev. Lett. **81**, 5003–5006 (1998).
[96] V. Buzek, M. Hillery, and P. L. Knight, "Flocks of Quantum Clones: Multiple Copying of Qubits," Fortschr. Phys. **46**, 521–533 (1998).
[97] N. Gisin and S. Massar, "Optimal Quantum Cloning Machines," Phys. Rev. Lett **79**, 2153–2156 (1997).
[98] D. Bruss, A. Ekert, and C. Macchiavello, "Optimal Universal Quantum Cloning and State Estimation," Phys. Rev. Lett. **81**, 2598–2601 (1998).
[99] M. Keyl and R. F. Werner, "Optimal Cloning of Pure States, Judging Single Clones," quant-ph/9807010 (1998).
[100] P. Masiek and P. L. Knight, "Copying of Entangled States and the Degradation of Correlations," quant-ph/9808043 (1998).
[101] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, "Optimal Universal and State-Dependent Quantum Cloning," Phys. Rev. A **57**, 2368–2378 (1998).
[102] M. Murao, D, Jonathen, M. B. Plenio, and V. Vedral, "Quantum Telecloning and Multiparticle Entanglement," quant-ph/9806082 (1998).
[103] C. S. Niu and R. B. Griffiths, "Optimal Copying of One Quantum Bit," Phys. Rev. A **58**, 4377–4393 (1998).
[104] C. S. Niu and R. B. Griffiths, "Two Qubit Copy Machine for Economical Quantum Eavesdropping," quant-ph/9810008 (1998).
[105] C. Adami and N. J. Cerf, "Quantum Computation with Linear Optics," quant-ph/9806048 (1998).
[106] N. J. Cerf, C. Adami, and P. G. Kwait, "Optical Simulation of Quantum Logic," Phys. Rev. A **57**, R1477–1480 (1998).
[107] A. Ekert, "Quantum Interferometers as Quantum Computers," Physica Scripta **T76**, 218–222 (1998).
[108] I. L. Chuang and Y. Yamamoto, "Simple Quantum Computer," Phys. Rev. A **52**, 3489–3496 (1995).
[109] I. L. Chuang and Y. Yamamoto, "Quantum Bit Regeneration," Phys. Rev. Lett. **76**, 4281–4284 (1996).
[110] G. J. Milburn, "Quantum Optical Fredkin Gate," Phys. Rev. Lett. **62**, 2124–2127 (1989).
[111] P. Törmä and S. Stenholm, "Quantum Logic Using Polarized Photons," Phys. Rev. A **54**, 4701–4706 (1996).
[112] S. Lloyd, "Necessary and Sufficient Conditions for Quantum Computation," J. Mod. Optics **41**, 2503–2520 (1994).
[113] E. Bernstein and U. Vazirani, "Quantum Complexity Theory," SIAM J. Comput. **26**, 1411–1473 (1997).
[114] Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," Proc. R. Soc. Lond. A **400**, 97–117 (1985).
[115] Deutsch, "Quantum Computational Networks," Proc. R. Soc. Lond. A **425**, 73–90 (1989).

[116] A. Steane, "Quantum Computing," Rep. Prog. Phys. **61**, 117–173 (1998).
[117] D. Deutsch, A. Barenco, and A. Ekert, "Universality in Quantum Computation," Proc. R. Soc. Lond. A **449**, 669–677 (1995).
[118] S. Lloyd, "Almost Any Quantum Logic Gate is Universal," Phys. Rev. Lett. **75**, 346–349 (1995).
[119] A. Barenco, "A Universal Two-Bit Gate for Quantum Computation," Proc. R. Soc. A **449**, 679–683 (1995).
[120] D. P. DiVincenzo, "Two-Bit Gates are Universal for Quantum Computation," Phys. Rev. A **51**, 1015–1022 (1995).
[121] J. M. Myers, "Can a Universal Quantum Computer be Fully Quantum?," Phys. Rev. Lett. **78**, 1823–1824 (1997).
[122] N. Linden and S. Popescu, "The Halting Problem for Quantum Computers," quant-ph/9806054 v2 (1998).
[123] T. D. Kieu and M. Danos, "The Halting Problem for Universal Quantum Computers," quant-ph/9811001 (1998).
[124] M. A. Nielsen, "Computable Functions, Quantum Measurements, and Quantum Dynamics," Phys. Rev. Lett. **79**, 2915–2918 (1997).
[125] R. P. Feynman, "Simulating Physics with Computers," Int. J. Theoret. Phys. **21**, 467–488 (1982).
[126] R. P. Feynman, "Quantum Mechanical Computers," Found. Phys. **16**, 507–531 (1986).
[127] S. Lloyd, "Universal Quantum Simulators," Science **273**, 1073–1078 (1996).
[128] C. Zalka, "Efficient Simulation of Quantum Systems by Quantum Computers," Fortschr. Phys. **46**, 877–879 (1998).
[129] S. Wiesner, "Simulations of Many-Body Quantum Systems by a Quantum Computer," quant-ph/9603028 (1996).
[130] D. A. Meyer, " Quantum Mechanics of Lattice Gas Automata: One-Particle Plane Waves and Potentials," Phys. Rev. E **55**, 5261–5269 (1997).
[131] D. A. Lidar and O. Biham, "Simulating Ising Spin Glasses on a Quantum Computer," Phys. Rev. E **56**, 3661–3681 (1997).
[132] D. S. Abrams and S. Lloyd, "Simulation of Many-Body Fermi Systems on a Universal Quantum Computer," Phys. Rev. Lett. **79**, 2586–2589 (1997).
[133] B. M. Boghosian and W. Taylor, "Simulating Quantum Mechanics on a Quantum Computer," Physica D **120**, 30–42 (1998).
[134] C. Zalka, "Simulating Quantum Systems on a Quantum Computer," Proc. R. Soc. Lond. A **454**, 313–322 (1998).
[135] B. Boghosian and W. Taylor, "A Quantum Lattice-Gas Model for the Many-Body Schrödinger Equation in d Dimensions," quant-ph/9604035 (1996).
[136] D. A. Meyer, "From Quantum Cellular Automata to Quantum Lattice Gases," J. Stat. Phys. **85**, 551–574 (1996).
[137] B. M. Terhal and D. P. DiVincenzo, "On the Problem of Equilibration and the Computation of Correlation Functions on a Quantum Computer," quant-ph/9810063 (1998).
[138] R. Schack, "Using a Quantum Computer to Investigate Quantum Chaos," Phys. Rev. A **57**, 1634–1635 (1998).
[139] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," Proc. 35th Annual Symp. on Foundations of Computer Science (Sante Fe, NM: IEEE Computer Society Press, Los Alamitos, CA, 1994), 124–134; SIAM J. Comput. **26**, 1484–1509 (1997).
[140] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, "Quantum Computers, Factoring and Decoherence," Science **270**, 1633–1635 (1995).
[141] A. Ekert and R. Jozsa, "Quantum Computation and Shor's Factoring Algorithm," Rev. Mod. Phys. **68**, 733–753 (1996).
[142] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, "Efficient Networks for Quantum Factoring," Phys. Rev. **54**, 1034–1063 (1996).
[143] C. Miquel, J. P. Paz, and R. Perazzo, "Factoring in a Dissipative Quantum Computer," Phys. Rev. A **54**, 2605–2613 (1996).
[144] P. W. Shor, "Scheme for Reducing Decoherence in Quantum Computer Memory," Phys. Rev. A **52**, R2493–2496 (1995).

[145] M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum, "Information-Theoretic Approach to Quantum Error Correction and Reversible Measurement," Proc. R. Soc. Lond. A **454**, 277–304 (1998).
[146] A. M. Steane, "Error Correcting Codes in Quantum Theory," Phys. Rev. Lett. **77**, 793–797 (1996).
[147] M. Steane, "Multiple Particle Interference and Quantum Error Correction," Proc. R. Soc. A **452**, 2551–2577 (1996).
[148] A. R. Calderbank and P. W. Shor, "Good Quantum Error-Correcting Codes Exist," Phys. Rev. A **54**, 1098–1105 (1996).
[149] E. Knill and R. Laflamme, "Theory of Quantum Error-Correcting Codes," Phys. Rev. A **55**, 900–911 (1997).
[150] A. Ekert and C. Macchiavello, "Quantum Error Correction for Communication," Phys. Rev. Lett. **77**, 2585–2588 (1996).
[151] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect Quantum Error Correcting Code," Phys. Rev. Lett. **77**, 198–201 (1996).
[152] E. M. Rains, R. H. Hardin, P. W. Shor, and N.J.A. Sloane, "Nonadditive Quantum Code," Phys. Rev. Lett **79**, 953–954 (1997).
[153] D. Gottesman, "Class of Quantum Error-Correcting Codes Saturating the Quantum Hamming Bound," Phys. Rev. A **54**, 1862–1868 (1996).
[154] A. R. Calderbank, E. M. Rains. P. W. Shor, and N.J.A. Sloane, "Quantum Error Correction and Orthogonal Geometry," Phys. Rev. Lett. **78**, 405–408 (1997).
[155] P. W. Shor and R. Laflamme, "Quantum Analog of the Mac Williams Identities for Classical Coding Theory," Phys. Rev. Lett. **78**, 1600–1602 (1997).
[156] P. W. Shor, "Fault Tolerant Quantum Computation," *Proc. 37th Annual Symp. on Foundations of Computer Science* (Los Alamitos, CA: IEEE Computer Society Press) 56–65 (1996).
[157] T. Pellizzari, "Quantum Computers, Error-Correction and Networking: Quantum Optical Approaches," in *Introduction to Quantum Computation and Information*, H. K. Lo et al, editors, 270–310, World Scientific, Singapore (1998).
[158] D. P. DiVincenzo and P. W. Shor, "Fault-Tolerant Error Correction with Efficient Quantum Codes," Phys. Rev. Lett. **77**, 3260–3263 (1996).
[159] A. M. Steane, "Active Stabilization, Quantum Computation, and Quantum State Synthesis," Phys. Rev. Lett. **78**, 2252–2255 (1997).
[160] A. M. Steane, "Space, Time, Parallelism and Noise Requirements for Reliable Quantum Computing," Fortschr. Phys. **46**, 443–457 (1998).
[161] E. Knill and R. Laflamme, "Concatenated Quantum Codes," quant-ph/9608012 (1996).
[162] E. Knill, R. Laflamme, and W. H. Zurek, "Threshold Accuracy for Quantum Computation," quant-ph/9610011 (1996).
[163] D. Aharonov and M. Ben-Or, "Fault-Tolerant Quantum Computation with Constant Error," quant-ph/9611025 (1996).
[164] A. M. Steane, "Simple Quantum Error-Correcting Codes," Phys. Rev. A **54**, 4741–4751 (1996).
[165] E. Knill, R. Laflamme, and W. H. Zurek, "Resilient Quantum Computation: Error Models and Thresholds," Proc. R. Soc. Lond. A **454**, 365–384 (1998).
[166] E. Knill, R. Laflamme, and W. H. Zurek, "Resilient Quantum Computation," Science **279**, 342–345 (1998).
[167] D. Gottesman, "Theory of Fault-Tolerant Quantum Computation," Phys. Rev. A **57**, 127–137 (1998).
[168] A. Kitaev, "Fault-Tolerant Quantum Computation by Anyons," quant-ph/9707021 (1997).
[169] A. Barenco, T. A. Brun, R. Schack, and T. P. Spiller, "Effects of Noise on Quantum Error Correction Algorithms," Phys. Rev. A **56**, 1177–1188 (1997).
[170] A. M. Steane, "Introduction to Quantum Error Correction," Phil. Trans. R. Soc. Lond. A **356**, 1739–1758 (1998).
[171] J. Preskill, "Reliable Quantum Computers," Proc. R. Soc. Lond. A **454**, 385–410 (1998).
[172] J. I. Cirac, T. Pellizari, and P. Zoller, "Enforcing Coherent Evolution in Dissipative Quantum Dynamics," Science **273**, 1207–1210 (1996).
[173] I. L. Chuang and Y. Yamamoto, "Creation of a Persistent Qubit Using Error Correction," Phys. Rev. A **55**, 114–127 (1997).

[174] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," Ph.D. thesis, California Institute of Technology, quant-ph/9705052 (1997).
[175] J. Preskill, "Fault Tolerant Quantum Computation," in *Introduction to Quantum Computation and Information,* H. K. Lo et al, editors, 213–269, World Scientific, Singapore (1998).
[176] A. M. Steane, "Quantum Error Correction," in *Introduction to Quantum Computation and Information,* H. K. Lo et al, editors, 184–212, World Scientific, Singapore (1998).
[177] G. M. Palma, K. Suominen, and A. K. Ekert, "Quantum Computers and Dissipation," Proc. R. Soc. Lond. A **452**, 567–584 (1996).
[178] P. Zanardi and M. Rasetti, "Error Avoiding Quantum Codes," Mod. Phys. Lett. B **11**, 1085–1093 (1997).
[179] P. Zanardi and M. Rasetti, "Noiseless Quantum Codes," Phys. Rev. Lett. **79**, 3306–3309 (1997).
[180] P. Zanardi, "Dissipation and Decoherence in a Quantum Register," Phys. Rev. A **57**, 3276–3284 (1998).
[181] D. A. Lidar, I. L. Chuang, and K. B. Whaley, "Decoherence-Free Subspaces for Quantum Computation," Phys. Rev. Lett. **81**, 2594–2597 (1998).
[182] G. Lindblad, "On the Generators of Quantum Dynamical Semigroups," Commun. Math. Phys. **48**, 119–130 (1976).
[183] R. Alicki and K. Lendi, *Quantum Dynamical Semigroups and Applications*, in Lecture Notes in Physics, No. 286, Springer-Verlag, Berlin (1987).
[184] D. Vitali, P. Tombesi, and G. J. Milburn, "Controlling the Decoherence of a 'Meter' via Stroboscopic Feedback," Phys. Rev. Lett. **79**, 2442–2445 (1997).
[185] D. Vitali and P. Tombesi, "Decoherence Control for Optical Qubits," quant-ph/9802033 (1998).
[186] S. Lloyd, "Quantum Controllers for Quantum Systems," quant-ph/9703042 (1997).
[187] L. Viola and S. Lloyd, "Dynamical Suppression of Decoherence in Two-State Quantum Systems," Phys. Rev. A **58**, 2733–2744 (1998).
[188] L. Viola and S. Lloyd, "Decoherence Control in Quantum Information Processing: Simple Models," quant-ph/9809058 (1998), to appear in *Proc. of 4th International Conference on Quantum Measurement, Communication, and Computing*, P. Kumar, editor, Northwestern.
[189] L. Viola, E. Knill, and S. Lloyd, "Dynamical Decoupling of Open Quantum Systems," Phys. Rev. Lett **82**, 2417–2421 (1999), quant-ph/9809071 (1998).
[190] Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation,* http://www.theory.caltech.edu/people/preskill/ph229/#lecture (1998).
[191] A. Barenco, "Quantum Physics and Computers," Contemp. Phys. **37**, 375–389 (1996).
[192] S. Lloyd, "Quantum-Mechanical Computers," Sci. Am., 140–145 (October 1995).
[193] C. P. Williams and S. H. Clearwater, *Explorations in Quantum Computing,"* Springer-Verlag, New York (1998).
[194] *Introduction to Quantum Computation and Information,* H. K. Lo, S. Popescu, and T. Spiller, editors, World Scientific, Singapore (1998).
[195] J. Gruska, *Quantum Computing*, McGraw-Hill, London (1999).
[196] J. I. Cirac and P. Zoller, "Quantum Computation with Cold Trapped Ions," Phys. Rev. Lett. **74**, 4091–4094 (1995).
[197] W. Paul and H. Steinwedel, "Ein neues Massenspektrometer ohne Magnetfeld," Z. Naturforsch. A **8**, 448–450 (1953).
[198] W. Paul, "Electromagnetic Trap for Charged and Neutral Particles," Rev. Mod. Phys. **62**, 531–540 (1990).
[199] M. G. Raizen, J. M. Gillligan, J. C. Bergquist, W. M. Itano, and D. J. Wineland, "Ionic Crystals in a Linear Paul Trap," Phys. Rev. A **45**, 6493–6501 (1992).
[200] P. K. Ghosh, *Ion Traps*, Clarendon Press, Oxford (1995).
[201] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a Fundamental Quantum Logic Gate," Phys. Rev. Lett. **75**, 4714–4717 (1995).
[202] C. Monroe, D. M. Meekhof, B. E. King, and D. J. Wineland, "A 'Schrödinger Cat' Superposition State of an Atom," Science **272**, 1131–1136 (1996).
[203] Q. A. Turchette, C. S. Wood, B. E. King, C. J. Myatt, D. Leibfried, W. M. Itano, C. Monroe, and D. J. Wineland, "Deterministic Entanglement of Two Trapped Ions," Phys. Rev. Lett. **81**, 3631–3634 (1998).

[204] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof, "Experimental Issues in Coherent Quantum-State Manipulation of Trapped Atomic Ions," J. Res. Natl. Inst. Stand. Technol. **103**, 259–328 (1998).

[205] A. M. Steane, "The Ion Trap Quantum Information Processor," Appl. Phys. B **64**, 623–642 (1997).

[206] D. J. Wineland, C. Monroe, W. M. Itano, B. E. King, D. Leibfried, D. M. Meekhof, C. Myatt, and C. Wood, "Experimental Primer on the Trapped Ion Quantum Computer," Fortschr. Phys. **46**, 363–390 (1998).

[207] D. J. Wineland, C. Monroe, W. M. Itano, B. E. King, D. Leibfried, C. Myatt, and C. Wood, "Trapped-Ion Quantum Simulator," Phys. Scripta **T76**, 147–151 (1998).

[208] D. M. Meekhof, C. Monroe, B. E. King, W. M. Itano, and D. J. Wineland, "Generation of Nonclassical Motional States of a Trapped Atom," Phys. Rev. Lett. **76**, 1796–1799 (1996).

[209] D. J. Wineland, C. Monroe, D. M. Meekhof, B. E. King, D. Leibfried, W. M. Itano, J. C. Bergquist, D. Berkeland, J. J. Bollinger, and J. Miller, "Quantum State Manipulation of Trapped Atomic Ions," Proc. R. Soc. Lond. A **454**, 411–429 (1998).

[210] C. Monroe, D. Leibfried, B. E. King, D. M. Meekhof, W. M. Itano, and D. J. Wineland, "Simplified Quantum Logic with Trapped Ions," Phys. Rev. A **55**, R2489–2491 (1997).

[211] B. E. King, C. S. Wood, C. J. Myatt, Q. A. Turchette, D. Leibfried, W. M. Itano, C. Monroe, and D. J. Wineland, "Cooling the Collective Motion of Trapped Ions to Initialize a Quantum Register," Phys. Rev. Lett. **81**, 1525–1528 (1998).

[212] R. J. Hughes, "Cryptography, Quantum Computation and Trapped Ions," Phil. Trans. R. Soc. Lond. A **356**, 1853–1868 (1998).

[213] R. J. Hughes and D.F.V. James, "Prospects for Quantum Computation with Trapped Ions," Fortschr. Phys. **46**, 759–769 (1998).

[214] R. J. Hughes, D.F.V. James, J. J. Gomez, M. S. Gulley, M. H. Holzscheiter, P. G. Kwait, S. K. Lamoreaux, C. G. Peterson, V. D. Sandberg, M. M. Schauer, C. M. Simmons, C. E. Thorburn, D. Tupa, P. Z. Wang, and A. G. White, "The Los Alamos Trapped Ion Quantum Computer Experiment," Fortschr. Phys. **46**, 329–361 (1998).

[215] D.F.V. James, M. S. Gulley, M. H. Holzscheiter, R. J. Hughes, P. G. Kwait, S. K. Lamoreaux, C. G. Peterson, V. D. Sanberg, M. M. Schauer, C. M. Simmons, D. Tupa, P. Z. Wang, and A. G. White, "Trapped Ion Quantum Computer Research at Los Alamos," quant-ph/9807071 (1998).

[216] R. J. Hughes, D.F.V. James, E. H. Knill, R. Laflamme, and A. G. Petschek, "Decoherence Bounds on Quantum Computation with Trapped Ions," Phys. Rev. Lett. **77**, 3240–3243 (1996).

[217] D.F.V. James, "Theory of Heating of the Ground State of Trapped Ions," Phys. Rev. Lett. **81**, 317–320 (1998).

[218] D. Stevens, J. Brochard, and A. M. Steane, "Simple Experimental Methods for Trapped-Ion Quantum Processors," Phys. Rev. A **58**, 2750–2759 (1998).

[219] J. Steinbach, J. Twamley, and P. L. Knight, "Engineering Two-Mode Interaction in Ion Trap," Phys. Rev. A **56**, 4815–4825 (1997).

[220] S. Schneider, H. M. Wiseman, W. J. Munro, and G. J. Milburn, "Measurement and State Preparation via Ion Trap Quantum Computing," Fortschr. Phys. **46**, 391–399 (1998).

[221] S. Schneider and G. J. Milburn, "Decoherence in Ion Traps Due to Laser Intensity and Phase Fluctuations," Phys. Rev. A **57**, 3748–3752 (1998).

[222] S. Schneider and G. J. Milburn, "Decoherence and Fidelity in Ion Traps with Fluctuating Trap Parameters," quant-ph/9812044 (1998).

[223] R. Onofrio and L. Viola, "Lindblad Approach to Nonlinear Jaynes-Cummings Dynamics of a Trapped Ion," Phys. Rev. A **56**, 39–43 (1997).

[224] J. F. Poyatos, J. I. Cirac, and P. Zoller, "Quantum Gates with 'Hot Trapped Ions'," Phys. Rev. Lett. **81** 1322–1325 (1998).

[225] S. Schneider, D.F.V. James, and G. J. Milburn, "Method of Quantum Computation with 'Hot' Trapped Ions," quant-ph/9808012 (1998).

[226] K. M. Obenland and A. M. Despain, "Simulating the Effect of Decoherence and Inaccuracies on a Quantum Computer," quant-ph/9804038 (1998).

[227] M. B. Plenio and P. L. Knight, "Decoherence Limits to Quantum Computation Using Trapped Ions," Proc. R. Soc. Lond. A **453**, 2017–2041 (1997).

[228] M. B. Plenio and P. L. Knight, "Realistic Lower Bounds for the Factorization Time of Large Numbers on a Quantum Computer," Phys. Rev. A **53**, 2986–2990 (1996).
[229] M. Murao and P. L. Knight, "Decoherence in Nonclassical Motional States of a Trapped Ion," Phys. Rev. A **58**, 663–669 (1998).
[230] P. R. Berman, editor, *Cavity Quantum Electrodynamics*, Academic Press, Boston (1994).
[231] H. J. Kimble, "Strong Interaction of Single Atoms and Photons in Cavity QED," Physica Scripta **T76**, 127–137 (1998).
[232] M. Brune and S. Haroche, "Cavity Quantum Electrodynamics," in *Quantum Dynamics of Simple Systems*, G.-L. Oppo, S. M. Barnett, E. Riis, and M. Wilkinson, editors, Inst. of Physics Publishers, Bristol, 49–70 (1996).
[233] S. Haroche, "Mesoscopic Coherences in Cavity QED," Il Nuovo Cimento **110B**, 545–556 (1995).
[234] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, "Decoherence, Continuous Observation, and Quantum Computing: A Cavity QED Model," Phys. Rev. Lett. **75**, 3788–3791 (1995).
[235] H. J. Kimble, Q. A. Turchette, N. Ph. Georgiades, C. J. Hood, W. Lange, H. Mabuchi, E. S. Polzik, and D. W. Vernooy, "Cavity Quantum Electrodynamics with a Capital Q," in *Coherence and Quantum Optics VII*, J. H. Eberly, L. Mandel, and E. Wolf, editors, 203–310, Plenum Press, New York (1996).
[236] X. Maître, E. Hagley, G. Nogues, C. Wunderlich, P. Goy, M. Brune, J. M. Raimond, and S. Haroche, "Quantum Memory with a Single Photon in a Cavity," Phys. Rev. Lett. **79**, 769–772 (1997).
[237] T. Sleator and H. Weinfurter, "Realizable Universal Quantum Logic Gates," Phys. Rev. Lett. **74**, 4087–4090 (1995).
[238] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche, "Simple Cavity-QED Two-Bit Quantum Logic Gate: The Principle and Expected Performances," Phys. Rev. A. **52**, 3554–3559 (1995).
[239] C. K. Law and H. J. Kimble, "Deterministic Generation of a Bit-Stream of Single-Photon Pulses," J. Mod. Opt. **44**, 2067–2074 (1997).
[240] K. M. Gheri, C. Saavedra, P. Törmä, J. I. Cirac, and P. Zoller, "Entanglement Engineering of One-Photon Wave Packets Using a Single-Atom Source," Phys. Rev. A **58**, R2627–2630 (1998).
[241] L. Davidovich, N. Zagury, M. Brune, J. M. Raimond, and S. Haroche, "Teleportation of an Atomic State Between Two Cavities Using Nonlocal Microwave Fields," Phys. Rev. A **50**, R895–898 (1994).
[242] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, "Quantum State Transfer and Entanglement Distribution Among Distant Nodes in a Quantum Network," Phys. Rev. Lett. **78**, 3221–3224 (1997).
[243] H. J. Kimble, "Strong Interactions of Single Atoms and Photons in Cavity QED," Physica Scripta **T76**, 127–137 (1998).
[244] H.-J. Briegel, W. Dür, S. J. Van Enk, J. I. Cirac, and P. Zoller, "Quantum Communication and the Creation of Maximally Entangled Pairs of Atoms over a Noisy Channel," Phil Trans. R. Soc. Lond. A **356**, 1841–1851 (1998).
[245] J. I. Cirac, S. J. Van Enk, P. Zoller, H. J. Kimble, and H. Mabuchi, "Quantum Communication in a Quantum Network," Physica Scripta **T76**, 223–232 (1998).
[246] S. J. Van Enk, J. I. Cirac, and P. Zoller, "Photonic Channels for Quantum Communication," Science **279**, 205–208 (1998).
[247] S. J. Van Enk, J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, "Quantum State Transfer in a Quantum Network: a Quantum Optical Implementation," J. Mod. Opt. **44**, 1727–1736 (1997).
[248] S. J. van Enk, J. I. Cirac, and P. Zoller, "Ideal Quantum Communication over Noisy Channels: A Quantum Optical Implementation," Phys. Rev. Lett. **78**, 4293–4296 (1997).
[249] C. P. Slichter, *Principles of Magnetic Resonance*, 3rd Edition, Springer, New York (1996).
[250] M. Goldman, *Quantum Description of High-Resolution NMR in Liquids*, Oxford Scientific Publications, London (1988).
[251] N. A. Gershenfeld and I. L. Chuang, "Bulk Spin-Resonance Quantum Computation," Science **275**, 350–356 (1997).

[252] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung, "Bulk Quantum Computation with Nuclear Magnetic Resonance: Theory and Experiment," Proc. R. Soc. Lond. A **454**, 447–467 (1998).
[253] I. L. Chuang, "Quantum Computation with Nuclear Magnetic Resonance," in *Introduction to Quantum Computation and Information*, H. K. Lo et al, editors, 311–339, World Scientific, Singapore (1998).
[254] D. G. Cory, A. F. Fahmy, and T. F. Havel, "Ensemble Quantum Computing by NMR Spectroscopy," Proc. Natl. Acad. Sci. USA **94**, 1634–1639 (1997).
[255] S. S. Somaroo, D. G. Cory, and T. F. Havel, "Expressing the Operations of Quantum Computing in Multiparticle Geometric Algebra," Phys. Lett. A **240**, 1–7 (1998).
[256] T. F. Havel, S. S. Somaroo, C.-H. Tseng, and D. G. Cory, "Principles and Demonstrations of Quantum Information Processing by NMR Spectroscopy," quant-ph/9812086 (1998).
[257] I. L. Chuang, N. Gershenfeld, and M. Kubinic, "Experimental Implementation of Fast Quantum Searching," Phys. Rev. Lett. **80**, 3408–3411 (1998).
[258] J. A. Jones, M. Mosca, and R. H. Hansen, "Implementation of a Quantum Search Algorithm on a Quantum Computer," Nature **393**, 344–346 (1998).
[259] J. A. Jones, "Fast Searches with Nuclear Magnetic Resonance Computers," Science **280**, 229 (1998).
[260] D. G. Cory, M. D. Price, T. F. Havel, "Nuclear Magnetic Resonance Spectroscopy: An Experimentally Accessible Paradigm for Quantum Computing," Physica D **120**, 82–101 (1998).
[261] R. Laflamme, E. Knill, W. H. Zurek, P. Catasti, and S.V.S. Mariappan, "NMR Greenberger-Horne-Zeiliger States," Phil. Trans. R. Soc. Lond. A **356**, 1941–1948 (1998).
[262] D. G. Cory, M. D. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo, "Experimental Quantum Error Correction," Phys. Rev. Lett. **81**, 2152–2155 (1998).
[263] I. L. Chuang. L.M.K. Vandersypen, Y. Zhou, D. W. Leung, and S. Lloyd, "Experimental Realization of a Quantum Algorithm," Nature **393**, 143–146 (1998).
[264] J. A. Jones, "Implementation of a Quantum Algorithm on a Nuclear Magnetic Resonance Quantum Computer," J. Chem. Phys. **109**, 1648–1653 (1998).
[265] N. Linden, H. Barjat, and R. Freeman, "An Implementation of the Deutsch-Jozsa Algorithm on a Three-Qubit NMR Quantum Computer," quant-ph/9808039 (1998).
[266] J. A. Jones and M. Mosca, "Approximate Quantum Counting on an NMR Ensemble Quantum Computer," quant-ph 19808056 (1998).
[267] W. S. Warren, "The Usefulness of NMR Quantum Computing," Science **277**, 1688–1689 (1997).
[268] J. R. Friedman, M. P. Sarachik, J. Tejada, and R. Ziolo, "Macroscopic Measurement of Resonant Magnetization Tunneling in High-Spin Molecules," Phys. Rev. Lett. **76**, 3830–3833 (1996).
[269] D. P. DiVincenzo, "Quantum Computation," Science **270**, 255–261 (1995).
[270] V. Privman, I. D. Vagner, and G. Kventsel, "Quantum Computation in Quantum-Hall Systems," Phys. Lett. A **239**, 141–146 (1998).
[271] B. E. Kane, "A Silicon-Based Nuclear Spin Quantum Computer," Nature **393**, 133–137 (1998).
[272] J. W. Lyding, "UHV/STM Nanofabrication: Progress, Technology, Spin-offs, and Challenges," Proc. IEEE **85**, 589–600 (1997).
[273] D. P. DiVincenzo, "Real and Realistic Quantum Computers," Nature **393**, 113–114 (1998).
[274] S. Bandyopadhyay and V. Roychowdhury, "Computational Paradigms in Nanoelectronics: Quantum Coupled Electron Logic and Neuromorphic Networks," Jpn. J. Appl. Phys. **35**, 3350–3362 (1996).
[275] S. N. Molotkov, "Quantum Controlled-NOT Gate Based on a Single Quantum Dot," JETP Lett. **64**, 237–243 (1996).
[276] S. Bandyopadhyay, A. Balandin, V. P. Roychowdhury, and F. Vatan, "Nanoelectronic Implementation of Reversible and Quantum Logic," Superlat. and Microstr. **23**, 445–464 (1998).
[277] D. Loss and D. P. DiVincenzo, "Quantum Computation with Quantum Dots," Phys. Rev. A **57**, 120–126 (1998).
[278] D. P. DiVincenzo and D. Loss, "Quantum Information is Physical," Superlat. and Microstr. **23**, 419–432 (1998).

[279] G. Burkard, D. Loss, and D. P. DiVincenzo, "Coupled Quantum Dots as Quantum Gates," cond-mat/9808026 v2 (1998).
[280] D. P. DiVincenzo, "Quantum Computing and Single-Qubit Measurement Using the Spin Filter Effect," cond-mat/9810295 (1998), to appear in J. Appl. Phys. (1999).
[281] D. P. DiVincenzo and D. Loss, "Quantum Computers and Quantum Coherence," cond-mat/9901137 (1998), to appear in J. Magn. Matl. (1999).
[282] A. Barenco, D. Deutsch, A. Ekert, and R. Josza, "Conditioned Quantum Dynamics and Logic Gates," Phys. Rev. Lett. **74**, 4083–4086 (1995).
[283] J. A. Brum and P. Hawrylak, "Coupled Quantum Dots as Quantum Exclusive-OR Gate," Superlat. and Microstr. **22**, 431–436 (1997).
[284] P. Zanardi and F. Rossi, "Quantum Information in Semiconductors: Noiseless Encoding in a Quantum Dot Array," Phys. Rev. Lett. **81**, 4752–4755 (1998).
[285] P. Zanardi and F. Rossi, "Subdecoherent Information Encoding in a Quantum-Dot Array," Phys. Rev. B **59**, 8170 (1999), quant-ph/9808036 (1998).
[286] N. H. Bonadeo, J. England, D. Gammon, D. Park, D. S. Katzer, and D. G. Steel, "Coherent Optical Control of the Quantum State of a Single Quantum Dot," Science **282**, 1473–1476 (1998).
[287] A. Shnirman, G. Schön, and Z. Hermon, "Quantum Manipulations of Small Josephson Junctions," Phys. Rev. Lett. **79**, 2371–2374 (1997).
[288] A. Shnirman and G. Schön, "Quantum Measurements Performed with a Single-Electron Transistor," Phys. Rev. B **57**, 15 400–15 407 (1998).
[289] Y. Makhlin, G. Schön, and A. Shnirman, "Josephson-Junction Qubits with Controlled Coupling," Nature **398**, 305–307 (1999), cond-mat/9808067 (1998).
[290] G. Schön, A. Shnirman, and Y. Makhlin, "Josephson-Junction Qubits and the Readout Process by Single-Electron Transistors," cond-mat/9811029 (1998).
[291] D. V. Averin, "Adiabatic Quantum Computation with Cooper Pairs," Solid State Commun. **105**, 65 (1998).
[292] L. B. Ioffe, V. B. Geshkenbein, M. V. Feigel'man, A. L. Fauchère, and G. Blatter, "Quiet SDS Josephson Junctions for Quantum Computing," cond-mat/9809116 (1998).
[293] D. P. DiVincenzo, "Topics in Quantum Computers," in *Mesoscopic Electron Transport*, L. Sohn, L. Kouwenhoven, and G. Shoen, editors, 657–677, Kluwer (1997), cond-mat/9612126 v.2 (1996).
[294] V. Bouchiat, D. Vion, P.Joyez, D. Esteve, and M. H. Devoret, "Quantum Coherence with a Single Cooper Pair," Physica Scripta **T76**, 165–170 (1998).
[295] A. M. van den Brink, G. Schön, and L. J. Geerligs, "Combined Single-Electron and Coherent-Cooper-Pair Tunneling in Voltage-Biased Josephson Junctions," Phys. Rev. Lett. **67**, 3030–3033 (1991).
[296] M. T. Tuominen, J. M. Hergenrother, T. S. Tighe, and M. Tinkham, "Experimental Evidence for Parity-Based 2e Periodicity in a Superconducting Single-Electron Tunneling Transistor," Phys. Rev. Lett. **69**, 1997–2000 (1992).
[297] J. Siewert and G. Schön, "Charge Transport in Voltage-Biased Superconducting Single-Electron Transistors," Phys. Rev. B **54**, 7421–7424 (1996).
[298] Y. Nakamura, C. D. Chen, and J. S. Tsai, "Spectroscopy of Energy-Level Splitting Between Two Macroscopic Quantum States of Charge Coherently Superposed by Josephson Coupling," Phys. Rev. Lett. **79**, 2328–2331 (1997).
[299] A. Van Oudenaarden and J. E. Mooij, "One Dimensional Mott Insulator Formed by Quantum Vortices in Josephson Junction Arrays," Phys. Rev. Lett. **76**, 4947–4950 (1996).
[300] W. J. Elion, J. J. Wachters, L. L. Sohn, and J. E. Mooij, "Observation of the Aharonov-Casher Effect for Vortices in Josephson-Junction Arrays," Phys. Rev. Lett. **71**, 2311–2314 (1993).
[301] W. J. Elion, J. J. Wachters, L. L. Sohn, and J. E. Mooij, "The Aharonov-Casher Effect for Vortices in Josephson-Junction Arrays," Physica B **203**, 497–503 (1994).
[302] M. F. Bocko, A. M. Herr, and M. J. Feldman, "Prospect for Quantum Coherent Computation Using Superconducting Electrons," IEEE Trans. Appl. Superconductivity **7**, 3638–3641 (1997).
[303] B. Rosen, "Superconducting Circuit Implementation of Qubits and Quantum Computer Logic," preprint (1997).
[304] X. Xue and H. Wei, "Superconducting State Quantum Logic," quant-ph/9702041 v2 (1997).

[305] R. J. Prance, R. Whiteman, T. D. Clark, J. Diggins, H. Prance, J. F. Ralph, G. Buckling, G. Colyer, C. Vittoria, A. Widom, and Y. Srivastava, "Observation of Quantum Jumps in SQUID Rings," in *Quantum Communications and Measurement,* V. P. Belavkin et al, editors, Plenum Press, New York, 299–306 (1995).

[306] R. Rouse, S. Y. Han, and J. E. Lukens, "Observation of Resonant Tunneling Between Macroscopically Distinct Quantum Levels," Phys. Rev. Lett. **75**, 1614–1617 (1995).

[307] R. Rouse, S. Han, and J. E. Lukens, "Photon Assisted Resonant Tunneling Between Macroscopically Distinct States of a SQUID," in *Quantum Coherence and Decoherence,* K. Fujikawa and Y. A. Ono, editors, Elsevier, Amsterdam, 179–182 (1996).

[308] L. Viola, R. Onofrio, and T. Calarco, "Macroscopic Quantum Damping in SQUID Rings," Phys. Lett. A **229**, 23–31 (1997).

[309] T. D. Clark, J. Diggins, J. F. Ralph, M. Everitt, R. J. Prance, H. Prance, R. Whiteman, A. Widom, and Y. N. Srivastava, "Coherent Evolution and Quantum Transitions in a Two Level Model of a SQUID Ring," Annals of Phys. **268**, 1–30 (1998).

[310] A. J. Leggett, S. Chakravarty, A. T. Dorsey, M.P.A. Fisher, A. Garg, and W. Zwerger, "Dynamics of the Dissipative Two-State System," Rev. Mod. Phys. **59**, 1–85 (1987).

[311] A. O. Caldiera and A. J. Leggett, "Quantum Tunneling in a Dissippative System," Ann. Phys. **149**, 374–456 (1983).

[312] U. Weiss, H. Grabert, and S. Linkwitz, "Influence of Temperature and Friction on Macroscopic Quantum Coherence in SQUID-Rings," Jap. J. Appl. Phys. **26**, Suppl 26-3, 1391 (1987).

[313] C. D. Tesche, "Schrödinger's Cat: A Realization in Superconducting Devices," in *New Techniques and Ideas in Quantum Measurement Theory,* D. M. Greenberger, editor, Annals New York Acad. Sci. **480**, 36–50 (1986).

[314] C. D. Tesche, "Can a Noninvasive Measurement of Magnetic Flux be Performed with Superconducting Circuits?," Phys. Rev. Lett. **64**, 2358–2361 (1990).

[315] P. Verkerk, B. Luonis, C. Salomon, C. Cohen-Tannoudji, J.-Y. Courtois, and G. Grynberg, "Dynamics and Spatial Order of Cold Cesium Atoms in a Periodic Optical Potential," Phys. Rev. Lett. **68**, 3861–3864 (1992).

[316] P. S. Jessen, C. Gerz, P. Lett, W. D. Phillips, S. L. Rolston, R.J.C. Spreeuw, and C. I. Westbrook, "Observation of Quantized Motion of Rb Atoms in an Optical Field," Phys. Rev. Lett. **69**, 49–52 (1992).

[317] I. H. Deutsch and P. S. Jessen, "Quantum-State Control in Optical Lattices," Phys. Rev. A **57** 1972–1986 (1998).

[318] A. Hemmerich and T. W. Hänsch, "Two-Dimensional Atomic Crystal Bound by Light," Phys. Rev. Lett. **70**, 410–413 (1993).

[319] G. Grynberg, B. Luonis, P. Verkerk, J.-Y. Courtois, and C. Salomon, "Quantized Motion of Cold Cesium Atoms in Two- and Three-Dimensional Optical Potentials," Phys. Rev. Lett. **70**, 2249–2252 (1993).

[320] A. Görlitz, M. Weidenmüller, T. W. Hänsch, and A. Hemmerich, "Observing the Position Spread of Atomic Wave Packets," Phys. Rev. Lett. **78**, 2096–2099 (1997).

[321] S. Rolston, "Optical Lattices," Physics World, 27–32 (October 1998).

[322] D. R. Meacher, "Optical Lattices—Crystalline Structures Bound by Light," Contemp. Phys. **39**, 329–350 (1998).

[323] C. S. Adams and E. Riis, "Laser Cooling and Trapping of Neutral Atoms," Prog. Quant. Electr. **21**, 1–79 (1997).

[324] D. L. Haycock, S. E. Hamann, G. Klose, and P. S. Jessen, "Atomic Trapping in Deeply Bound States of a Far-Off Resonance Optical Lattice," Phys. Rev. A **55**, R3991–3994 (1997).

[325] P. S. Jessen and I. H. Deutsch, "'Optical Lattices," in *Advances in Atomic, Molecular, and Optical Physics* **37**, B. Bederson and H. Walther, editors, 95, Cambridge (1996).

[326] G. Raithel, W. D. Phillips, and S. L. Rolston, "Collapse and Revivals of Wave Packets in Optical Lattices," Phys. Rev. Lett. **81**, 3615–3618 (1998).

[327] S. E. Hamann, D. L. Haycock, G. Klose, P. H. Pax, I. H. Deutsch, and P. S. Jessen, "Resolved-Sideband Raman Cooling to the Ground State of an Optical Lattice," Phys. Rev. Lett. **80**, 4149–4152 (1998).

[328] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch, "Quantum Logic Gates in Optical Lattices," Phys. Rev. Lett. **82**, 1060–1063 (1999).

[329] D. M. Stamper-Kurn, M. R. Andrews, A. P. Chikkatur, S. Inouye, H.-J. Miesner, J. Stenger, and W. Ketterle, "Optical Confinement of a Bose-Einstein Condensate," Phys. Rev. Lett. **80**, 2027–2030 (1998).

[330] B. P. Anderson and M. A. Kasevich, "Macroscopic Quantum Interference from Atomic Tunnel Arrays," Science **282**, 1686–1689 (1998).

[331] K. Marzlin and W. Zhang, "Photonic Band Gap and Defect States Induced by Excitations of Bose-Einstein Condensates in Optical Lattices," preprint cond-mat/9810085 (1998).

[332] D. Jaksch, H.-J. Briegel, J. I. Cirac, C. W. Gardiner, and P. Zoller, "Entanglement of Atoms via Cold Controlled Collisions," Phys. Rev. Lett. **82**, 1975–1978 (1999), quant-ph/9810087 (1998).

[333] D. Jaksch, C. Bruder, J. I. Cirac, C. W. Gardiner, and P. Zoller, "Cold Bosonic Atoms in Optical Lattices," Phys. Rev. Lett. **81**, 3108–3111 (1998).

[334] M.P.A. Fisher, P. B. Weichman, G. Grinstein, and D. S. Fisher, "Boson Localization and the Superfluid-Insulator Transition," Phys. Rev. B **40**, 546–570 (1989).

[335] P. Benioff, "Quantum Robots," in *Feynman and Computation: Exploring the Limits,* A.J.G. Hey, editors, Perseus Books, Reading, Massachusetts, 155–175 (1999).

[336] P. Benioff, "Quantum Robots and Environments," Phys. Rev. A **58**, 893–904 (1998).

[337] P. Benioff, "Some Foundational Aspects of Quantum Computers and Quantum Robots," Superlatt. and Microstr. **23**, 407–417 (1998).

[338] P. Benioff, "Quantum Robots Plus Environments," quant-ph/9807032 (1998), to appear in *Proc. of 4th International Conference on Quantum Measurement, Communication and Computing,* P. Kumar, editor, Northwestern.

[339] R. P. Feynman and A. R. Hibbs, *Quantum Mechanics and Path Integrals*, McGraw-Hill, New York (1965).

[340] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," Phys. Rev. Lett. **79**, 325–328 (1997).

U.S. Army Research Laboratory, Adelphi, MD 20783 and University of Cambridge Isaac Newton Institute for Mathematical Sciences, Cambridge, UK

Recent Newton Institute Preprints

NI99001-DAD **C Terquem, J Eislöffel, JCB Papaloizou et al**
Precession of collimated outflows from young stellar objects

NI99002-APF **KJ Falconer and RD Mauldin**
Fubini-type theorems for general measure constructions

NI99003-DAD **JCB Papaloizou and C Terquem**
Critical protoplanetary core masses in protoplanetary disks and the formation of short-period giant planets

NI99004-TRB **CR Doering and JD Gibbon**
Anomalous scaling and regularity of the Navier-Stokes equations

NI99005-TRB **WD McComb and C Johnston**
Elimination of turbulent modes using a conditional average with asymptotic freedom

NI99006-APF **KJ Falconer, M Järvenpää and P Mattila**
Examples illustrating the instability of packing dimensions of sections

NI99007-APF **J Kigami**
Markov property of Kusuoka-Zhou's Dirichlet forms on self-similar sets

NI99008-APF **RM Solovay**
A version of Ω for which ZFC can not predict a single bit

NI99009-TRB **BJ Geurts and A Leonard**
Is LES ready for complex flows?

NI99010-TRB **A Tsinober**
Vortex stretching versus production of strain/dissipation

NI99011-TRB **A Tsinober**
On statistics and structure(s) in turbulence

NI99012-TRB **AJ Young and WD McComb**
An ad hoc operational method to compensate for absent turbulence modes in an insuffiently resolved numerical simulation

NI99013-TRB **ND Sandham**
A review of progress on direct and large-eddy simulation of turbulence

NI99014-NSP **R Baraniuk**
Optimal tree approximation with wavelets

NI99015-CCP **HE Brandt**
Inconclusive rate with a positive operator valued measure

NI99016-DAD **U Torkelsson, GI Ogilvie, A Brandenburg et al**
The response of a turbulent accretion disc to an imposed epicyclic shearing motion

NI99017-TRB **M Kholmyansky and A Tsinober**
On the origins of intermittency in real turbulent flows

NI99018-SFU **T Shiromizu, K-i Maeda and M Sasaki**
The Einstein equations on the 3-brane world

NI99019-CCP **V Coffman, J Kundu and WK Wootters**
Distributed entabglement

NI99020-CCP **H Brandt**
Qubit devices

Information about Newton Institute Preprints is also available at
`http://www.newton.cam.ac.uk/preprints.html`