View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by University of Queensland eSpace

REVIEWS OF MODERN PHYSICS, VOLUME 79, JANUARY–MARCH 2007

Linear optical quantum computing with photonic qubits

Pieter Kok*

Department of Materials, Oxford University, Oxford OX1 3PH, United Kingdom and Hewlett-Packard Laboratories, Filton Road Stoke Gifford, Bristol BS34 8QZ, United Kingdom

W. J. Munro

Hewlett-Packard Laboratories, Filton Road Stoke Gifford, Bristol BS34 8QZ, United Kingdom

Kae Nemoto

National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

T. C. Ralph

Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Queensland 4072, Australia

Jonathan P. Dowling

Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Louisiana State University, Baton Rouge, Louisiana 70803, USA and Institute for Quantum Studies, Department of Physics, Texas A&M University, College Park, Texas 77843-4242, USA

G. J. Milburn

Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Queensland 4072, Australia

(Published 24 January 2007; corrected 30 May 2007)

Linear optics with photon counting is a prominent candidate for practical quantum computing. The protocol by Knill, Laflamme, and Milburn [2001, Nature (London) **409**, 46] explicitly demonstrates that efficient scalable quantum computing with single photons, linear optical elements, and projective measurements is possible. Subsequently, several improvements on this protocol have started to bridge the gap between theoretical scalability and practical implementation. The original theory and its improvements are reviewed, and a few examples of experimental two-qubit gates are given. The use of realistic components, the errors they induce in the computation, and how these errors can be corrected is discussed.

DOI: 10.1103/RevModPhys.79.135 PACS number(s): 03.67.Lx, 42.50.Dv, 03.65.Ud, 42.79.Ta

CONTENTS

*Electronic address: pieter.kok@materials.ox.ac.uk

 ©2007 The American Physical Society

I. QUANTUM COMPUTING WITH LIGHT

Quantum computing has attracted much attention over the last 10 to 15 years, partly because of its promise of superfast factoring and its potential for the efficient simulation of quantum dynamics. There are many different architectures for quantum computers based on many different physical systems. These include atom- and ion-trap quantum computing, superconducting charge and flux qubits, nuclear magnetic resonance, spin- and charge-based quantum dots, nuclear spin quantum computing, and optical quantum computing [for a recent overview, see Spiller *et al.* (2006)]. All these systems have their own advantages in quantum information processing. However, even though there may now be a few front-runners, such as ion-trap and superconducting quantum computing, no physical implementation seems to have a clear edge over others at this point. This is an indication that the technology is still in its infancy.

Optical quantum systems are prominent candidates for quantum computing, since they provide a natural integration of quantum computation and quantum communication. There are several proposals for building quantum computers that manipulate the state of light, ranging from cat-state logic to encoding a qubit in a harmonic oscillator and optical continuous-variable quantum computing. Cat states are states of the form $|\alpha\rangle \pm |-\alpha\rangle$, where $|\alpha\rangle$ is a weak coherent state. The logical qubits are determined by the sign ($\pm$) of the relative phase (Ralph *et al.*, 2003). Gottesman, Kitaev, and Preskil proposed quantum error correction codes for harmonic oscillators that are used to encode qubit states and showed that fault-tolerant quantum computing is possible using quantum optics (Gottesman *et al.*, 2001). Lloyd and Braunstein showed how the concept of quantum computing can be extended to continuous variables and how electromagnetic fields are a natural physical representation of this formalism (Lloyd and Braunstein, 1999). For a review article on optical quantum information processing with continuous variables, see Braunstein and van Loock (2005).

In this review, we focus on quantum computing with linear quantum optics and single photons. It has the advantage that the smallest unit of quantum information, the photon, is potentially free from decoherence: The quantum information stored in a photon tends to stay there. The downside is that photons do not naturally interact with each other, and in order to apply two-qubit quantum gates such interactions are essential. Therefore, if we are to construct an optical quantum computer, we have to introduce an effective interaction between photons in one way or another. In Sec. I.D, we review the use of so-called large cross-Kerr nonlinearities to induce a single-photon controlled-NOT operation. However, naturally occurring nonlinearities of this sort are many orders of magnitude too small for our purposes. An alternative way to induce an effective interaction between photons is to make projective measurements with photodetectors. The difficulty with this technique is that such optical quantum gates are probabilistic: More often than not, the gate fails and destroys the information in the quantum computation. This can be circumvented by using an exponential number of optical modes, but scalability requires only a polynomial number of modes (see also Sec. I.D). In 2001, Knill, Laflamme, and Milburn (2001) (KLM) constructed a protocol in which probabilistic two-photon gates are teleported into a quantum circuit with high probability. Subsequent error correction in the quantum circuit is used to bring the error rate down to fault-tolerant levels. We describe the KLM protocol in detail in Sec. II.

Initially, the KLM protocol was designed as a proof that linear optics and projective measurements allow for scalable quantum computing in principle. However, it subsequently spurred new experiments in quantum optics, demonstrating the operation of high-fidelity probabilistic two-photon gates. On the theoretical front, several improvements of the protocol were proposed, leading to ever smaller overhead costs on the computation. A number of these improvements is based on cluster-state quantum computing, or the one-way quantum computer. Recently, a circuit-based model was shown to have similar scaling properties as the best-known cluster-state model. In Sec. III, we describe several improvements to linear optical quantum information processing in considerable detail, and in Sec. IV, we describe the issues involved in the use of realistic components such as photon detectors, photon sources, and quantum memories. Given these realistic components, we discuss loss tolerance and general error correction for linear optical quantum computing (LOQC) in Sec. V.

We will restrict our discussion to the theory of single-photon implementations of quantum information processors, and assume some familiarity with the basic concepts of quantum computing. For an introduction to quantum computation and quantum information, see, e.g., Nielsen and Chuang (2000). In Sec. VI we conclude with an outlook on other promising optical quantum information processing techniques, such as photonic band-gap structures, weak cross-Kerr nonlinearities, and hybrid matter-photon systems. We start our review with a short introduction to linear optics, N-port optical interferometers, and circuits, and define the different versions of the optical qubit.

A. Linear quantum optics

The basic building blocks of linear optics are beam splitters, half- and quarter-wave plates, phase shifters, etc. In this section we describe these devices mathematically and establish the convention that is used throughout the rest of the paper.

The quantum-mechanical plane-wave expansion of the electromagnetic vector potential is usually expressed in terms of the annihilation operators $\hat{a}_j(k)$ and their adjoints, the creation operators:

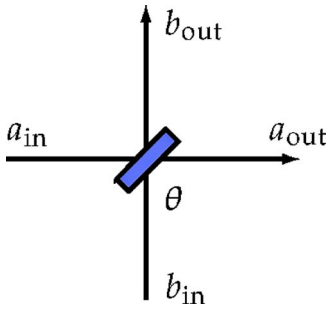

FIG. 1. (Color online) The beam splitter with transmission amplitude cos θ.

$$A^{\mu}(x,t) = \int \frac{d^3k}{\sqrt{(2\pi)^3 2\omega_k}} \sum_{j=1,2} \epsilon_j^{\mu}(k)\hat{a}_j(k)e^{ikx-i\omega_k t} + \text{H.c.},$$

where j denotes the polarization in the Coulomb gauge, ϵ_j^{μ} is the corresponding polarization vector, and μ indicates the components of the four-vector. For the moment we suppress the polarization degree of freedom and consider general properties of the creation and annihilation operators. They bear their names because they act in a specific way on the Fock states $|n\rangle$:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \text{ and } \quad \hat{a}^{\dagger}|n\rangle = \sqrt{n+1}|n+1\rangle, \tag{1}$$

where we suppressed the k dependence. It is straightforward to show that $\hat{n}(k) \equiv \hat{a}^{\dagger}(k)\hat{a}(k)$ is the number operator $\hat{n}|n\rangle = n|n\rangle$ for a given mode with momentum k. The canonical commutation relations between $\hat{a}$ and $\hat{a}^{\dagger}$ are given by

$$[\hat{a}(k),\hat{a}^{\dagger}(k')] = \delta(k-k'),$$
$$[\hat{a}(k),\hat{a}(k')] = [\hat{a}^{\dagger}(k),\hat{a}^{\dagger}(k')] = 0. \tag{2}$$

In the rest of this review, we denote information about the spatial mode k by a subscript, since we will be concerned not with the geometrical details of the interferometers we describe, but only with how the spatial modes are connected. Also to avoid notational clutter we will use operator carets only for nonunitary and non-Hermitian operators, except in cases where omission of the caret would lead to confusion.

An important optical component is the single-mode phase shift. It changes the phase of the electromagnetic field in a given mode:

$$\hat{a}_{\text{out}}^{\dagger} = e^{i\phi\hat{a}_{\text{in}}^{\dagger}\hat{a}_{\text{in}}}\hat{a}_{\text{in}}^{\dagger}e^{-i\phi\hat{a}_{\text{in}}^{\dagger}\hat{a}_{\text{in}}} = e^{i\phi}\hat{a}_{\text{in}}^{\dagger}, \tag{3}$$

with the interaction Hamiltonian $H_{\varphi} = \phi\hat{a}_{\text{in}}^{\dagger}\hat{a}_{\text{in}}$ (here and throughout this review we use the convention that $\hbar = 1$ and time dependence is absorbed in ϕ). This Hamiltonian is proportional to the number operator, which means that the photon number is conserved. Physically, a phase shifter is a slab of transparent material with an index of refraction that is different from that of free space.

Another important component is the beam splitter (see Fig. 1). Physically, it consists of a semireflective mirror: when light falls on this mirror, part will be reflected and part will be transmitted (Leonhardt, 1997). The theory of the lossless beam splitter is central to LOQC and was developed by Zeilinger (1981) and Fearn and Loudon (1987). Lossy beam splitters were studied by Barnett *et al.* (1989). The transmission and reflection properties of general dielectric media were studied by Dowling (1998). Let the two incoming modes on either side of the beam splitter be denoted by $\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$ and the outgoing modes by $\hat{a}_{\text{out}}$ and $\hat{b}_{\text{out}}$. When we parametrize the probability amplitudes of these possibilities as cos θ and sin θ and the relative phase as φ, then the beam splitter yields an evolution in operator form

$$\hat{a}_{\text{out}}^{\dagger} = \cos\theta\hat{a}_{\text{in}}^{\dagger} + ie^{-i\varphi}\sin\theta\hat{b}_{\text{in}}^{\dagger},$$
$$\hat{b}_{\text{out}}^{\dagger} = ie^{i\varphi}\sin\theta\hat{a}_{\text{in}}^{\dagger} + \cos\theta\hat{b}_{\text{in}}^{\dagger}. \tag{4}$$

The reflection and transmission coefficients R and T of the beam splitter are $R = \sin^2\theta$ and $T = 1-R = \cos^2\theta$. The relative phase shift $ie^{\pm i\varphi}$ ensures that the transformation is unitary. Typically, we choose either $\varphi = 0$ or $\varphi = \pi/2$. Mathematically, the two parameters θ and φ represent the angles of a rotation about two orthogonal axes in the Poincaré sphere. The physical beam splitter can be described by any choice of θ and φ, provided the correct phase shifts are applied to the outgoing modes.

In general the Hamiltonian H_{BS} of the beam-splitter evolution in Eq. (4) is given by

$$H_{\text{BS}} = \theta e^{i\varphi}\hat{a}_{\text{in}}^{\dagger}\hat{b}_{\text{in}} + \theta e^{-i\varphi}\hat{a}_{\text{in}}\hat{b}_{\text{in}}^{\dagger}. \tag{5}$$

Since the operator H_{BS} commutes with the total number operator $[H_{\text{BS}},\hat{n}] = 0$, the photon number is conserved in the lossless beam splitter, as one would expect.

The same mathematical description applies to the evolution due to a polarization rotation, physically implemented by quarter- and half-wave plates. Instead of having two different spatial modes a_{in} and b_{in}, the two incoming modes have different polarizations. We write $\hat{a}_{\text{in}} \to \hat{a}_x$ and $\hat{b}_{\text{in}} \to \hat{a}_y$ for some orthogonal set of coordinates x and y (i.e., $\langle x|y\rangle = 0$). The parameters θ and φ are now angles of rotation:

$$\hat{a}_{x'}^{\dagger} = \cos\theta\hat{a}_x^{\dagger} + ie^{-i\varphi}\sin\theta\hat{a}_y^{\dagger},$$
$$\hat{a}_{y'}^{\dagger} = ie^{i\varphi}\sin\theta\hat{a}_x^{\dagger} + \cos\theta\hat{a}_y^{\dagger}. \tag{6}$$

This evolution has the same Hamiltonian as the beam splitter, and it formalizes the equivalence between the so-called polarization and dual-rail logic. These transformations are sufficient to implement any photonic single-qubit operation (Simon and Mukunda, 1990).

The last linear optical element that we highlight here is the polarizing beam splitter (PBS). In circuit diagrams, it is usually drawn as a box around a regular beam splitter [see Fig. 2(a)]. If the PBS is cut to separate horizontal and vertical polarization, the transformation of the incoming modes (a_{in} and b_{in}) yields the following outgoing modes (a_{out} and b_{out}):

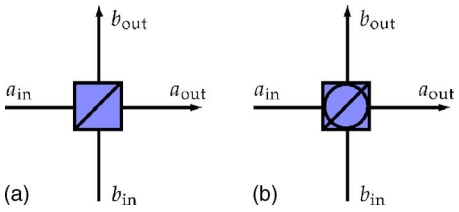

FIG. 2. (Color online) The polarizing beam splitter in different polarization bases. (a) The horizontal-vertical basis. (b) The diagonal basis.

$$\hat{a}_{\text{in},H} \to \hat{a}_{\text{out},H} \quad \text{and} \quad \hat{a}_{\text{in},V} \to \hat{b}_{\text{out},V},$$
$$\hat{b}_{\text{in},H} \to \hat{b}_{\text{out},H} \quad \text{and} \quad \hat{b}_{\text{in},V} \to \hat{a}_{\text{out},V}. \tag{7}$$

Using quarter-wave plates and polarizers, we can also construct a PBS for different polarization directions (e.g., L and R), in which case we make the substitution $H \leftrightarrow L$, $V \leftrightarrow R$. Diagrammatically a PBS with a different polarization typically has a circle drawn inside the box [Fig. 2(b)].

At this point, we should devote a few words to the term "linear optics." Typically this denotes the set of optical elements whose interaction Hamiltonian is bilinear in the creation and annihilation operators:

$$H = \sum_{jk} A_{jk} \hat{a}_j^\dagger \hat{a}_k. \tag{8}$$

An operator of this form commutes with the total number operator and has the property that a simple mode transformation of creation operators into a linear combination of other creation operators affects only the matrix A, but does not introduce terms that are quadratic (or higher) in the creation or annihilation operators. However, from a field-theoretic point of view, the most general linear transformation of creation and annihilation operators is defined by the Bogoliubov transformation

$$\hat{a}_j \to \sum_k u_{jk} \hat{a}_k + v_{jk} \hat{a}_k^\dagger. \tag{9}$$

Clearly, when such a transformation is substituted into Eq. (8) this will give rise to terms such as $\hat{a}_j \hat{a}_k$ and $\hat{a}_j^\dagger \hat{a}_k^\dagger$, i.e., squeezing. The number of photons is not conserved in such a process. For the purpose of this review, we exclude squeezing as a resource other than as a method for generating single photons.

With the linear optical elements introduced in this section we can build large optical networks. In particular, we can make computational circuits by using known states as the input and measuring the output states. Next we will study these optical circuits in more detail.

B. *N*-port interferometers and optical circuits

An optical circuit can be thought of as a black box with incoming and outgoing modes of the electromagnetic field. The black box transforms a state of the incoming modes into a different state of outgoing modes. The modes might be mixed by beam splitters, or they might pick up a relative phase shift or polarization rotation. These operations all belong to a class of optical components that preserve the photon number, as described in the previous section. In addition, the box may include measurement devices, the outcomes of which may modify optical components on the remaining modes. This is called feedforward detection, and it is an important technique that can increase the efficiency of a device (Clausen *et al.*, 2003; Lapaire *et al.*, 2003).

Optical circuits can also be thought of as a general unitary transformation on N modes, followed by the detection of a subset of these modes (followed by unitary transformation on the remaining modes, detection, and so on). The interferometric part of this circuit is also called an N-port interferometer. N-ports yield a unitary transformation U of the spatial field modes a_k, with $j,k \in \{1,\ldots,N\}$:

$$\hat{b}_k \to \sum_{j=1}^{N} U_{jk} \hat{a}_j \quad \text{and} \quad \hat{b}_k^\dagger \to \sum_{j=1}^{N} U_{jk}^* \hat{a}_j^\dagger, \tag{10}$$

where the incoming modes of the N-port are denoted by a_j and the outgoing modes by b_j. The explicit form of U is given by the repeated application of transformations like those given by Eqs. (3), (4), and (6).

The two-mode operators $\hat{L}_+ = \hat{a}^\dagger \hat{b}$, $\hat{L}_- = \hat{a}\hat{b}^\dagger$, and $\hat{L}_0 = (\hat{a}^\dagger \hat{a} - \hat{b}^\dagger \hat{b})/2$ form an su(2) Lie algebra:

$$[\hat{L}_0, \hat{L}_\pm] = \pm \hat{L}_\pm \quad \text{and} \quad [\hat{L}_+, \hat{L}_-] = 2\hat{L}_0. \tag{11}$$

This means that any two-mode interferometer exhibits U(2) symmetry.[1] In general, an N-port interferometer can be described by a transformation from the group U(N). Reck *et al.* (1994) demonstrated that the converse is also true, i.e., that any unitary transformation of N optical modes can be implemented efficiently with an N-port interferometer. They showed how a general U(N) element can be broken down into SU(2) elements, for which we have a complete physical representation in terms of beam splitters and phase shifters (see Fig. 3). The primitive element is a matrix T_{pq} defined on the modes p and q, which corresponds to a beam splitter and phase shifts. Implicit in this notation is the identity operator on the rest of the optical modes, such that $T_{pq} \equiv T_{pq} \otimes \mathbb{1}_{\text{rest}}$. We then have

$$\text{U}(N) \times T_{N,N-1} \times \cdots \times T_{N,1} = \text{U}(N-1) \oplus e^{i\phi}, \tag{12}$$

where ϕ is a single-mode phase. Concatenating this procedure leads to a full decomposition of U(N) into T elements, which in turn are part of SU(2). The maximum

[1]Two remarks: Lie algebras are typically denoted in lower case, while the group itself is denoted in upper case. Second, single-mode phase shifts break the special symmetry (det $U = 1$), which is why an interferometer is described by U(N), rather than SU(N).

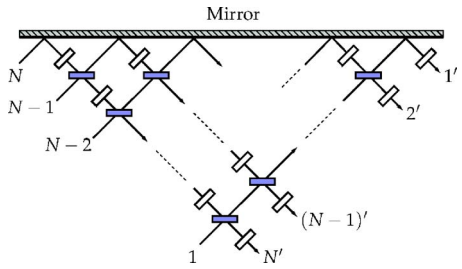

FIG. 3. (Color online) Decomposing an N-port unitary U(N) into SU(2) group elements, i.e., beam splitters and phase shifters. Moreover, this is an efficient process: the maximum number of beam splitters needed is $N(N-1)/2$.

number of beam-splitter elements T that are needed is $N(N-1)/2$. This procedure is thus manifestly scalable.

Subsequently, Jex *et al.* (1995) and Törmä *et al.* (1995, 1996) showed how to construct multimode Hamiltonians that generate these unitary mode transformations, and a three-path Mach-Zehnder interferometer was demonstrated experimentally by Weihs *et al.* (1996). A good introduction to linear optical networks has been given by Leonhardt (2003), and a determination of effective Hamiltonians has been given by Leonhardt and Neumaier (2004). For a treatment of optical networks in terms of their permanents, see Scheel (2004). Optical circuits in a (general) relativistic setting have been described by Kok and Braunstein (2006).

C. Qubits in linear optics

Formally, a qubit is a quantum system that is described by the fundamental representation of the SU(2) symmetry group. We saw above that two optical modes form a natural implementation of this symmetry. In general, two modes with fixed total photon number n furnish natural irreducible representations of this group with the dimension of the representation given by $n+1$ (Biedenharn and Louck, 1981). It is at this point not specified whether we should use spatial or polarization modes. In linear optical quantum computing, the qubit of choice is usually taken to be a single photon that has the choice of two different modes $|0\rangle_L=|1\rangle\otimes|0\rangle\equiv|1,0\rangle$ and $|1\rangle_L=|0\rangle\otimes|1\rangle\equiv|0,1\rangle$. This is called a dual-rail qubit. When the two modes represent the internal polarization degree of freedom of the photon ($|0\rangle_L=|H\rangle$ and $|1\rangle_L=|V\rangle$), we speak of a polarization qubit. In this review we will reserve the term "dual rail" for a qubit with two spatial modes. As we showed earlier, these two representations are mathematically equivalent and we can physically switch between them using polarization beam splitters. In addition, some practical applications (typically involving a dephasing channel such as a fiber) may call for so-called time-bin qubits, in which the two computational qubit values are "early" and "late" arrival times in a detector. However, this degree of freedom does not exhibit a natural internal SU(2) symmetry: Arbitrary single-qubit operations are very difficult to implement. In this review we will be concerned mainly with polarization and dual-rail qubits.

In order to build a quantum computer, we need both single-qubit and two-qubit operations. Single-qubit operations are generated by the Pauli operators σ_x, σ_y, and σ_z, in the sense that the operator $\exp(i\theta\sigma_j)$ is a rotation about the j axis in the Bloch sphere with angle θ. As we have seen, these operations can be implemented with phase shifters, beam splitters, and polarization rotations on polarization and dual-rail qubits. In this review, we will use the convention that σ_x, σ_y, and σ_z denote physical processes, while we use X, Y, and Z for the corresponding logical operations on the qubit. These two representations become inequivalent when we deal with logical qubits that are encoded in multiple physical qubits.

Whereas single-qubit operations are straightforward in the polarization and dual-rail representations, the two-qubit gates are more problematic. Consider, for example, the transformation from a state in the computational basis to a maximally entangled Bell state:

$$|H,H\rangle_{ab}\rightarrow\frac{1}{\sqrt{2}}(|H,V\rangle_{cd}+|V,H\rangle_{cd}). \tag{13}$$

This is the type of transformation that requires a two-qubit gate. In terms of the creation operators (and ignoring normalization), the linear optical circuit that is supposed to create Bell states out of computational basis states is described by a Bogoliubov transformation of both creation operators

$$\begin{aligned}\hat{a}_H^\dagger\hat{b}_H^\dagger&\rightarrow\left(\sum_{k=H,V}\alpha_k\hat{c}_k^\dagger+\beta_k\hat{d}_k^\dagger\right)\left(\sum_{k=H,V}\gamma_k\hat{c}_k^\dagger+\delta_k\hat{d}_k^\dagger\right)\\&\neq\hat{c}_H^\dagger\hat{d}_V^\dagger+\hat{c}_V^\dagger\hat{d}_H^\dagger.\end{aligned} \tag{14}$$

It is immediately clear that the right-hand sides in both lines cannot be made the same for any choice of α_k, β_k, γ_k, and δ_k: The top line is a separable expression in the creation operators, while the bottom line is an entangled expression in the creation operators. Therefore, linear optics alone cannot create maximal polarization entanglement from single polarized photons in a deterministic manner (Kok and Braunstein, 2000a). Entanglement that is generated by changing the definition of our subsystems in terms of the global field modes is inequivalent to the entanglement that is generated by applying true two-qubit gates to single-photon polarization or dual-rail qubits.

Note also that if we choose our representation of the qubit differently, we can implement a two-qubit transformation. Consider the single-rail qubit encoding $|0\rangle_L=|0\rangle$ and $|1\rangle_L=|1\rangle$. That is, the qubit is given by the vacuum and single-photon state. We can then implement the following (unnormalized) transformation deterministically:

$$|1,0\rangle\rightarrow|1,0\rangle+|0,1\rangle. \tag{15}$$

This is a 50:50 beam-splitter transformation. However, in this representation the single-qubit operations cannot be

implemented deterministically with linear optical elements, since these transformations do not preserve the photon number (Paris, 2000). This implies that we cannot implement single-qubit and two-qubit gates deterministically for the same physical representation. For linear optical quantum computing, we typically need the ability to (dis)entangle field modes. We therefore have to add a nonlinear component to our scheme. Two possible approaches are the use of Kerr nonlinearities, which we briefly review in the next section, and the use of projective measurements. In the rest of this review, we concentrate mainly on linear optical quantum computing with projective measurements, based on the work by Knill, Laflamme, and Milburn.

Finally, in order to make a quantum computer with light that can outperform any classical computer, we need to understand more about the criteria that make quantum computers "quantum." For example, some simple schemes in quantum communication require only superpositions of quantum states to distinguish them from their corresponding classical ones. However, we know that this is not sufficient for general computational tasks.

First, we give two definitions. The Pauli group P is the set of Pauli operators with coefficients $\{\pm 1, \pm i\}$. For instance, the Pauli group for one qubit is $\{\mathbb{1}, \pm X, \pm Y, \pm Z, \pm i\mathbb{1} \pm iX, \pm iY, \pm iZ,\}$, where $\mathbb{1}$ is the identity matrix. The Pauli group for n qubits consists of elements that are products of n Pauli operators, including the identity. In addition, we define the Clifford group C of transformations that leave the Pauli group invariant. In other words, for any element of the Clifford group c and any element of the Pauli group p, we have

$$cpc^{\dagger} = p' \quad \text{with } p' \in P. \tag{16}$$

Prominent members of the Clifford group are the Hadamard, phase, and controlled-NOT (CNOT) transformations.[2] Note that the Pauli group is a subgroup of the Clifford group.

The Gottesman-Knill theorem (1999) states that any quantum algorithm that is initiated in the computational basis and employs only transformations (gates) from the Clifford group, along with projective measurements in the computational basis, can be efficiently simulated on a classical computer. This means that there is no computational advantage in restricting the quantum computer to such circuits. A classical machine could simulate them efficiently.

In discrete-variable quantum information processing, the Gottesman-Knill theorem provides a valuable tool for assessing the classical complexity of a given process. [For a precise formulation and proof of this theorem, see Nielsen and Chuang (2000), p. 464.] Although the set of gates in the Pauli and Clifford groups does not satisfy the universality requirements, the addition of a single-qubit $\pi/8$ gate $U_{\pi/8} \equiv \mathrm{diag}\{1, e^{i\pi/4}\}$ will render the set universal. In single-photon quantum information processing we have easy access to such single-qubit operations.

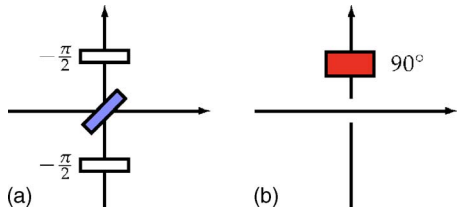

FIG. 4. (Color online) Linear optical quantum computing simulation according to Cerf, Adami, and Kwiat. (a) Hadamard gate. (b) CNOT gate. The four two-qubit degrees of freedom are carried by which-path and polarization information. The dashed line indicates that there is no interaction between the crossing modes.

D. Early optical quantum computers and nonlinearities

Before the work of Knill, Laflamme, and Milburn, quantum information processing with linear optics was among the topics studied in nonscalable architectures by Cerf, Adami, and Kwiat (1998). Their linear optical protocol can be considered a simulation of a quantum computer: n qubits are represented by a single photon in 2^n different paths. In such an encoding, both single- and two-qubit gates are easily implemented using (polarization) beam splitters and phase shifters. For example, let a single qubit be given by a single photon in two optical modes: $|0\rangle_L = |1,0\rangle$ and $|1\rangle_L = |0,1\rangle$. The Hadamard gate acting on this qubit can then be implemented with a 50:50 beam splitter given by Eq. (4), with $\varphi = 0$, and two $-\pi/2$ phase shifters [see Fig. 4(a)]:

$$|1,0\rangle \rightarrow |1,0\rangle + i|0,1\rangle \rightarrow |1,0\rangle + |0,1\rangle,$$

$$|0,1\rangle \rightarrow -i(i|1,0\rangle + |0,1\rangle) \rightarrow |1,0\rangle - |0,1\rangle_{\mathrm{out}},$$

where we suppressed the normalization.

The CNOT gate in the Cerf-Adami-Kwiat protocol is even simpler: suppose that the two optical modes in Fig. 4(b) carry polarization. The spatial degree of freedom carries the control qubit, and the polarization carries the target. If the photon is in the vertical spatial mode, it will undergo a polarization rotation, thus implementing a CNOT operation. The control and target qubits can be interchanged trivially using a polarization beam splitter.

Since this protocol requires an exponential number of optical modes, this is a simulation rather than a fully scalable quantum computer. Other proposals in the same spirit include work by Clauser and Dowling (1996), Summhammer (1997), Ekert (1998), and Spreeuw (1998). Using this simulation, a classical version of Grover's search algorithm can be implemented (Kwiat *et al.*, 2000). General quantum logic using polarized photons was studied by Stenholm (1996), Törmä and Stenholm (1996), and Franson and Pittman (1999).

Prior to the work of KLM, it was widely believed that scalable all-optical quantum computing needed a nonlin-

[2]See Eq. (25b) for a definition of the CNOT operation.

ear component, such as a Kerr medium. These media are typically characterized by a refractive index n_{Kerr}, which has a nonlinear component:

$$n_{\mathrm{Kerr}} = n_0 + \chi^{(3)} E^2. \tag{17}$$

Here n_0 is the ordinary refractive index and E^2 is the optical intensity of a probe beam with proportionality constant $\chi^{(3)}$. A beam traversing a Kerr medium will then experience a phase shift that is proportional to its intensity.

A variation on this is the cross-Kerr medium, in which the phase shift of a signal beam is proportional to the intensity of a second probe beam. In the language of quantum optics, we describe the cross-Kerr medium by the Hamiltonian

$$H_{\mathrm{Kerr}} = \kappa \hat{n}_s \hat{n}_p, \tag{18}$$

where $\hat{n}_s$ and $\hat{n}_p$ are the number operators for the signal and probe modes, respectively. Compare H_{Kerr} with the argument of the exponential in Eq. (3): Transforming the probe (signal) mode using this Hamiltonian induces a phase shift that depends on the number of photons in the signal (probe) mode. Indeed, the mode transformations of the signal and probe beams are

$$\hat{a}_s \to \hat{a}_s e^{-i\tau \hat{m}_p} \quad \text{and} \quad \hat{a}_p \to \hat{a}_p e^{-i\tau \hat{m}_s}, \tag{19}$$

with $\tau \equiv \kappa t$. When the cross-Kerr medium is placed in one arm of a balanced Mach-Zehnder interferometer, a sufficiently strong phase shift τ can switch the field from one output mode to another [see Fig. 5(a)]. For example, if the probe beam is a (weak) optical field and the signal mode may or may not be populated with a single photon, then the detection of the output ports of the Mach-Zehnder interferometer reveals whether there was a photon in the signal beam. Moreover, we obtain this information without destroying the signal photon. This is called a quantum nondemolition measurement (Imoto *et al.*, 1985).

It is not hard to see that we can use this mechanism to create an all-optical controlled-phase (CZ) gate for photonic qubits [for the definition of a CZ gate, see Eq. (25a)]. Such a gate would give us the capability to build an all-optical quantum computer. Let us assume that our qubit states are single photons with horizontal or vertical polarization. In Fig. 5(b), we show how the cross-Kerr medium should be placed. The mode transformations are[3]

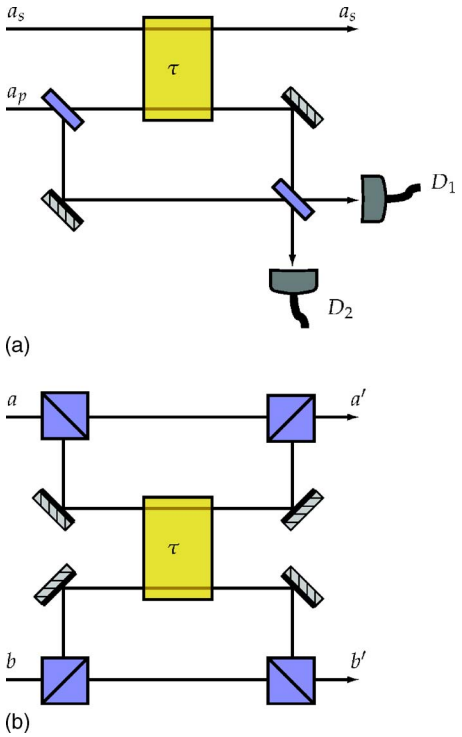

FIG. 5. (Color online) Using cross-Kerr nonlinearities (τ) in optical information processing. (a) Single-photon quantum nondemolition measurement. The Mach-Zehnder interferometer is balanced such that the presence of a photon in the signal mode directs the probe field to the dark output port. (b) Single-photon CZ gate. When both photons in modes a and b are vertically polarized, the two-photon state acquires a relative phase. This results in an entangling gate that, together with single-photon rotations, is sufficient for universal quantum computing.

$$\begin{aligned} &\hat{a}_H \hat{b}_H \to \hat{a}'_H \hat{b}'_H, \quad \hat{a}_V \hat{b}_H \to \hat{a}'_V \hat{b}'_H, \\ &\hat{a}_H \hat{b}_V \to \hat{a}'_H \hat{b}'_V, \quad \hat{a}_V \hat{b}_V \to \hat{a}'_V \hat{b}'_V e^{i\tau}, \end{aligned} \tag{20}$$

which means that the strength of the Kerr nonlinearity should be $\tau = \pi$ in order to implement a CZ gate. It is trivial to transform this gate into a CNOT gate. A Kerr-based Fredkin gate was developed by Yamamoto *et al.* (1988) and Milburn (1989). Architectures based on these or similar nonlinear optical gates were studied by Chuang and Yamamoto (1995), d'Ariano *et al.* (2000), and Howell and Yeazell (2000b, 2000c). Nonlinear interferometers are treated by Sanders and Rice (2000), while state transformation using Kerr media is the subject of Clausen *et al.* (2002). Recently, Hutchinson and Milburn (2004) proposed cross-Kerr nonlinearities to create cluster-states for quantum computing. We will discuss cluster state quantum computing in some detail in Sec. III.A.

Unfortunately, even the largest natural cross-Kerr nonlinearities are extremely weak ($\chi^{(3)} \approx 10^{-22}$ m^2 V^{-2}). Operating in the optical single-photon regime with a mode volume of approximately 0.1 cm^3, the Kerr phase shift is only $\tau \approx 10^{-18}$ (Kok *et al.*, 2002). This makes Kerr-

[3]Note that the phase factors in these operator transformations are evaluated for the vacuum state of modes a and b.

based optical quantum computing extremely challenging, if not impossible: If such a material is used to create long fibers for enhanced nonlinearities, photon losses in the Kerr medium will prevent the gate from operating properly. Furthermore, Kerr nonlinearities are typically very noisy, since the effective interaction Hamiltonian includes not only the term $\hat{a}^\dagger\hat{a}\hat{b}^\dagger\hat{b}$, but also all other four-mode terms consisting of two creation and two annihilation operators such as $\hat{a}^\dagger\hat{b}\hat{c}^\dagger\hat{d}$ and $\hat{a}^{\dagger 2}\hat{a}^2$. Much larger cross-Kerr nonlinearities of $\tau\approx 10^{-5}$ can be obtained with electromagnetically induced transparent materials (Schmidt and Imamoğlu, 1996). However, this value of τ is still much too small to implement the gates we discussed above. Toward the end of this review we will indicate how such small but not tiny cross-Kerr nonlinearities may be used for quantum computing.

Turchette *et al.* (1995) proposed a different method of inducing a phase shift, when a signal mode s and probe mode p of different frequency are both populated by a single polarized photon. By sending both modes through a cavity containing cesium atoms, they obtain a phase shift that is dependent on the polarizations of the input modes:

$$\begin{aligned}
|L,L\rangle_{sp} &\rightarrow |L,L\rangle_{sp},\\
|R,L\rangle_{sp} &\rightarrow e^{i\phi_s}|R,L\rangle_{sp},\\
|L,R\rangle_{sp} &\rightarrow e^{i\phi_p}|L,R\rangle_{sp},\\
|R,R\rangle_{sp} &\rightarrow e^{i(\phi_s+\phi_p+\delta)}|R,R\rangle_{sp},
\end{aligned} \tag{21}$$

where $|L\rangle=|H\rangle+i|V\rangle$ and $|R\rangle=|H\rangle-i|V\rangle$. Using weak coherent pulses, Turchette *et al.* found $\phi_s=17.5°\pm1°$, $\phi_p=12.5°\pm1°$, and $\delta=16°\pm3°$. An improvement of this system was proposed by Hofmann *et al.* (2003). These authors showed how a phase shift of π can be achieved with a single two-level atom in a one-sided cavity. The cavity effectively enhances the tiny nonlinearity of the atom. The losses in this system are negligible.

In Sec. VI we will return to systems in which (small) phase shifts can be generated using nonlinear optical interactions, but the principal subject of this review is how projective measurements can induce enough of a nonlinearity to make possible linear optical quantum computing.

II. A NEW PARADIGM FOR OPTICAL QUANTUM COMPUTING

In 2000, Knill, Laflamme, and Milburn proved that it is indeed possible to create universal quantum computers with linear optics, single photons, and photon detection (Knill *et al.*, 2001). They constructed an explicit protocol, involving off-line resources, quantum teleportation, and error correction. In this section, we will describe this new paradigm, which has become known as the KLM scheme, starting from the description of linear optics that we developed in the previous section. In Secs. II.A–II.C, we introduce some elementary probabilistic gates and their experimental realizations, followed by a characterization of gates in Sec. II.D and a general discussion on nonlinear unitary gates with projective measurements in Sec. II.E. We then describe how to teleport these gates into an optical computational circuit in Secs. II.F and II.G, and the necessary error correction is outlined in Sec. II.H. Recently, Myers and Laflamme (2005) published a tutorial on the original KLM theory.

A. Elementary gates

Physically, we cannot construct deterministic two-qubit gates in the polarization and dual-rail representations because photons do not interact with each other. The only way that photons can directly influence each other is via the bosonic symmetry relation. Indeed, linear optical quantum computing exploits exactly this property, i.e., the bosonic commutation relation $[\hat{a},\hat{a}^\dagger]=1$. To see what we mean by this statement, consider two photons in separate spatial modes interacting on a 50:50 beam splitter. The transformation will be

$$\begin{aligned}
|1,1\rangle_{ab} &= \hat{a}^\dagger\hat{b}^\dagger|0\rangle\\
&\rightarrow \frac{1}{2}(\hat{c}^\dagger+\hat{d}^\dagger)(\hat{c}^\dagger-\hat{d}^\dagger)|0\rangle_{cd}\\
&= \frac{1}{2}(\hat{c}^{\dagger 2}-\hat{d}^{\dagger 2})|0\rangle_{cd}\\
&= \frac{1}{\sqrt{2}}(|2,0\rangle_{cd}-|0,2\rangle_{cd}).
\end{aligned} \tag{22}$$

It is clear (from the second and third lines) that the bosonic nature of the electromagnetic field gives rise to photon bunching: the incoming photons pair off together. This is a strictly quantum-mechanical effect, since classically the two photons could equally well end up in different output modes. In terms of quantum interference, there are two paths leading from the input state $|1,1\rangle_{\text{in}}$ to the output state $|1,1\rangle_{\text{out}}$: Either both photons are transmitted or both photons are reflected. The relative phases of these paths are determined by the beam-splitter equation (4):

$$\begin{aligned}
|1,1\rangle_{\text{in}} &\rightarrow_{\text{trans}} \cos^2\theta|1,1\rangle_{\text{out}},\\
|1,1\rangle_{\text{in}} &\rightarrow_{\text{refl}} -\sin^2\theta e^{i\varphi}e^{-i\varphi}|1,1\rangle_{\text{out}}.
\end{aligned} \tag{23}$$

For a 50:50 beam splitter, we have $\cos^2\theta=\sin^2\theta=1/2$ and the two paths cancel exactly, irrespective of the value of φ.

The absence of the $|1,1\rangle_{cd}$ term is called the Hong-Ou-Mandel effect (Hong *et al.*, 1987), and it lies at the heart of linear optical quantum computing. However, as we have argued in Sec. I.C, this is not enough to make deterministic linear optical quantum computing possible, and we have to turn our attention instead to probabilistic gates.

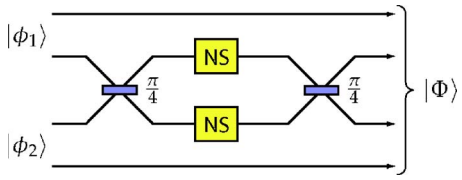

FIG. 6. (Color online) The conditional phase gate (CZ). This gate uses two NS gates to change the relative phase of the two qubits: when both qubits are in the $|1\rangle$ state, the two photons interfere on the 50:50 beam splitter $[\cos^2(\pi/4)=1/2]$. The Hong-Ou-Mandel effect then ensures that both photons exit the same output mode and the NS gates induce a relative phase π. Upon recombination on the second beam splitter, this phase shows up only in the states where both qubits were in the $|1\rangle$ state.

As was shown by Lloyd (1995), almost any two-qubit gate is universal for quantum computing (in addition to single-qubit gates), but in linear optics we usually consider the controlled-phase gate (CZ, also sometimes known as CPHASE or CSIGN) and the controlled-NOT gate (CNOT). In terms of a truth table, they induce the following transformations:

Control	Target	CZ	CNOT
$\|0\rangle$	$\|0\rangle$	$\|0,0\rangle$	$\|0,0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0,1\rangle$	$\|0,1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1,0\rangle$	$\|1,1\rangle$
$\|1\rangle$	$\|1\rangle$	$-\|1,1\rangle$	$\|1,0\rangle$

(24)

which is identical to

$$|q_1,q_2\rangle \xrightarrow[\text{CZ}]{} (-1)^{q_1 q_2}|q_1,q_2\rangle, \tag{25a}$$

$$|q_1,q_2\rangle \xrightarrow[\text{CNOT}]{} |q_1,q_2 \oplus q_1\rangle. \tag{25b}$$

Here q_k takes the qubit values 0 and 1, while $q_2 \oplus q_1$ is taken modulo 2.

A CZ gate can be constructed in linear optics using two nonlinear sign (NS) gates. The NS gate acts on the three lowest Fock states in the following manner:

$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \rightarrow \alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle. \tag{26}$$

Its action on higher-number states is irrelevant, as long as it does not change the amplitude of $|0\rangle$, $|1\rangle$, or $|2\rangle$. Consider the optical circuit drawn in Fig. 6, and suppose the (separable) input state is given by $|\phi_1\rangle \otimes |\phi_2\rangle = (\alpha|0,1\rangle + \beta|1,0\rangle)(\gamma|0,1\rangle + \delta|1,0\rangle)$. Subsequently, we apply the beam-splitter transformation to the first and third modes and find the Hong-Ou-Mandel effect only when both modes are populated by one photon. The NS gates will then induce a phase shift of π. Applying a second beam-splitter operation yields

$$|\Phi\rangle = \alpha\gamma|0,1,0,1\rangle + \alpha\delta|0,1,1,0\rangle + \beta\gamma|1,0,0,1\rangle - \beta\delta|1,0,1,0\rangle. \tag{27}$$

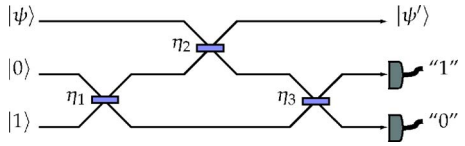

FIG. 7. (Color online) The nonlinear sign (NS) gate according to Knill, Laflamme, and Milburn. The beam-splitter transmission amplitudes are $\eta_1=\eta_3=1/(4-2\sqrt{2})$ and $\eta_2=3-2\sqrt{2}$.

This is no longer separable in general. In fact, when we choose $\alpha=\beta=\gamma=\delta=1/\sqrt{2}$, the output state is a maximally entangled state. The overall probability of this CZ gate $p_{\text{CZ}}=p_{\text{NS}}^2$.

It is immediately clear that we cannot make the NS gate with a regular phase shifter, because only the state $|2\rangle$ picks up a phase. A linear optical phase shifter would also induce a factor i (or $-i$) in the state $|1\rangle$. However, it is possible to perform the NS gate probabilistically using projective measurements. The fact that two NS gates can be used to create a CZ gate was first realized by Knill, Laflamme, and Milburn (2001). Their probabilistic NS gate is a three-port device, including two ancillary modes the output of which is measured with perfect photon-number discriminating detectors (see Fig. 7). The input states for the ancillae are the vacuum and a single photon, and the gate succeeds when the detectors D_1 and D_2 measure zero and one photons, respectively. For an arbitrary input state $\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle$, this occurs with probability $p_{\text{NS}}=1/4$. The general upper bound for such gates was found to be $1/2$ (Knill, 2003). Without any feedforward mechanism, the success probability of the NS gate cannot exceed $1/4$. It was shown numerically by Scheel and Lütkenhaus (2004) and proved analytically by Eisert (2005) that, in general, the NS_N gate defined by

$$\sum_{k=0}^{N} c_k|k\rangle \rightarrow_{\text{NS}_N} \sum_{k=0}^{N-1} c_k|k\rangle - c_N|N\rangle \tag{28}$$

can be implemented with probability $1/N^2$ [see also Scheel and Audenaert (2005)].

Several simplifications of the NS gate were reported shortly after the original KLM proposal. First, a three-port NS gate with only marginally lower success probability $p'_{\text{NS}}=(3-\sqrt{2})/7$ was proposed by Ralph, White, *et al.* (2002). This gate uses only two beam splitters (see Fig. 8). Second, similar schemes using two ancillary photons have been proposed (Zou *et al.*, 2002; Scheel *et al.*, 2004). These protocols have success probabilities of 20% and 25%, respectively.

Finally, a scheme equivalent to the one by Ralph, White, *et al.* was proposed by Rudolph and Pan (2001), in which the variable beam splitters are replaced with polarization rotations. These might be more convenient to implement experimentally, since the irrational transmission and reflection coefficients of the beam splitters are translated into polarization rotation angles (see Fig. 9). For pedagogical purposes, we treat this gate in a little more detail. Assume that the input mode is horizontally

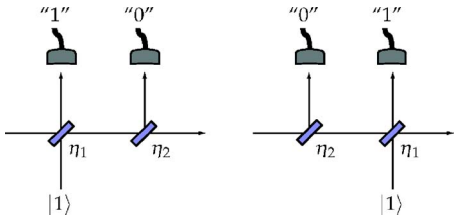

FIG. 8. (Color online) The two equivalent versions of the NS gate by Ralph, White, *et al.* (2002). Only two beam splitters are used, while the other resources are identical to the NS gate by Knill, Laflamme, and Milburn. The success probability of this gate is $(3-\sqrt{2})/7$.

polarized. The polarization rotation then gives $\hat{a}_H \rightarrow \cos\sigma\hat{a}_H + \sin\sigma\hat{a}_V$, and the input state transforms according to

$$\left(\alpha + \beta\hat{a}_H^\dagger + \frac{\gamma}{\sqrt{2}}\hat{a}_H^{\dagger 2}\right)\hat{b}_V^\dagger|0\rangle$$
$$\rightarrow \left[\alpha + \beta\cos\sigma\hat{a}_H + \beta\sin\sigma\hat{a}_V + \frac{\gamma}{\sqrt{2}}(\cos^2\sigma\hat{a}_H^{\dagger 2} + \sin 2\sigma\hat{a}_H^\dagger\hat{a}_V^\dagger + \sin^2\sigma\hat{a}_V^{\dagger 2})\right]\hat{b}_V^\dagger|0\rangle.$$

Detecting no photons in the first output port yields

$$\left(\alpha + \beta\cos\sigma\hat{a}_H^\dagger + \frac{\gamma}{\sqrt{2}}\cos^2\sigma\hat{a}_H^{\dagger 2}\right)\hat{b}_V^\dagger|0\rangle,$$

after which we apply the second polarization rotation: $\hat{a}_H \rightarrow \cos\theta\hat{a}_H + \sin\theta\hat{a}_V$ and $\hat{a}_V \rightarrow -\sin\theta\hat{a}_H + \cos\theta\hat{a}_V$. This gives the output state

$$\left[\alpha + \beta\cos\sigma(\cos\theta\hat{a}_H^\dagger + \sin\theta\hat{a}_V^\dagger) + \frac{\gamma}{\sqrt{2}}\cos^2\sigma(\cos\theta\hat{a}_H^\dagger + \sin\theta\hat{a}_V^\dagger)^2\right]$$
$$\times(-\sin\theta\hat{a}_H^\dagger + \cos\theta\hat{a}_V^\dagger)|0\rangle.$$

After detecting a single vertically polarized photon in the second output port, we have

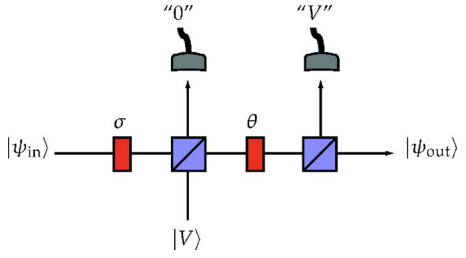

FIG. 9. (Color online) The NS gate by Rudolph and Pan. Based on a vacuum detection of the first output port and a single vertically polarized photon on the second output port, the interferometer applies a NS gate to the input state. The success probability is also $(3-\sqrt{2})/7$, which is close to the optimal value of 1/4.

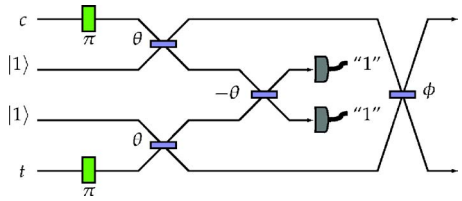

FIG. 10. (Color online) The Knill CZ gate based on two ancilla photons and two detected photons. The beam-splitter angles are $\theta=54.74°$ and $\phi=17.63°$, such that the transmission amplitudes are given by $\cos\theta$ and $\cos\phi$, respectively.

$$|\psi_{\text{out}}\rangle = \alpha\cos\theta|0\rangle + \beta\cos\sigma\cos 2\theta|1\rangle + \gamma\cos^2\sigma\cos\theta(1-\sin^2 3\theta)|2\rangle.$$

When we choose $\sigma\simeq 150.5°$ and $\theta\simeq 61.5°$, this yields the NS gate with the same probability $\cos^2\theta=(3-\sqrt{2})/7$. Finally, in Fig. 10, the circuit of the CZ gate by Knill (2002) is shown. The success probability is 2/27. This is the most efficient CZ gate known to date.

Sometimes it might be sufficient to apply destructive two-photon gates. For example, a Bell measurement in teleportation does not need to be nondestructive in order to successfully teleport a photon. In this case, we can increase the probability of success of the gate considerably. A CNOT gate that needs post-selection to make sure there is one polarized photon in each output mode was proposed by Ralph, Langford, *et al.* (2002). It makes use only of beam splitters with reflection coefficient of 1/3 and polarizing beam splitters. The success probability is 1/9. An identical gate was proposed independently by Hofmann and Takeuchi (2002). It was also shown that the success probability of an array of n CZ gates of this type can be made to operate with a probability of $p=(1/3)^{n+1}$, rather than $p=(1/9)^n$ (Ralph, 2004).

B. Parity gates and entangled ancillae

A special optical gate that will become important in Sec. III is the so-called parity check. It consists of a single polarizing beam splitter, followed by photon detection in the complementary basis of one output mode. If the input modes are denoted by a and b and the output modes are c and d, then the Bogoliubov transformation is given by Eq. (7). For two input qubits in the computational basis $\{|H\rangle,|V\rangle\}$ this gate induces the following transformation:

$$\begin{aligned} |H,H\rangle_{ab} &\rightarrow |H,H\rangle_{cd}, \\ |H,V\rangle_{ab} &\rightarrow |HV,0\rangle_{cd}, \\ |V,H\rangle_{ab} &\rightarrow |0,HV\rangle_{cd}, \\ |V,V\rangle_{ab} &\rightarrow |V,V\rangle_{cd}, \end{aligned} \tag{29}$$

where $|HV,0\rangle_{cd}$ denotes a vertically and horizontally polarized photon in mode c and nothing in mode d. Making a projective measurement in mode c onto the

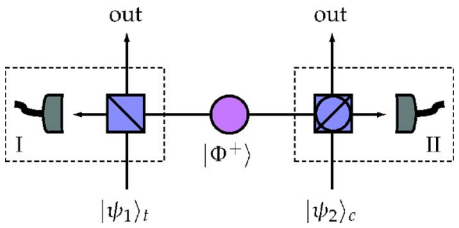

FIG. 11. (Color online) The CNOT gate by Pittman *et al.* (2001). The two boxes I and II are parity gates in two complementary bases, where the detector measures in a complementary basis with respect to the polarizing beam splitter. The gate makes use of a maximally entangled ancillary state $|\Phi^+\rangle$, which boosts the success probability up to one-quarter. The target $|\psi_1\rangle_t$ and control $|\psi_2\rangle_c$ input states will evolve into an entangled output state conditioned on the required detector signature.

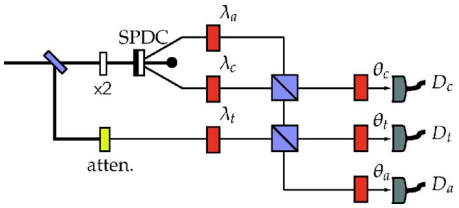

FIG. 12. (Color online) Schematic diagram of the experimental setup of the three-photon CNOT gate of Pittman *et al.* (2003). The gate starts by preparing the qubits with polarization rotations λ_i, followed by mixing the ancilla and control qubits on a polarizing beam splitter. The ancilla qubit is then mixing with the target qubit on the second polarizing beam splitter. The gate is implemented upon a threefold detector coincidence in the control, target, and ancilla modes. The polarization rotations θ_i are used to select different polarization bases.

complementary basis $(|H\rangle \pm |V\rangle)/\sqrt{2}$ then yields a parity check: If we detect a single photon in mode c, we know that the input qubits had the same logical value. This value is transmitted into the output qubit in mode d (up to a σ_z transformation depending on the measurement result). On the other hand, if we detect zero or two photons in mode c, the input qubits were not identical. In this case, the state of the output mode is no longer in the single-qubit subspace.

This gate was used by Cerf, Adami, and Kwiat to construct small optical quantum circuits (1998). As we have seen in Sec. I.D, however, their approach is not scalable since n-qubit circuits involve 2^n distinct paths. When two parity gates in complementary bases are combined with a maximally entangled ancilla state $|\Phi^+\rangle = (|H,H\rangle + |V,V\rangle)/\sqrt{2}$, a CNOT gate with success probability 1/4 is obtained (Koashi *et al.*, 2001; Pittmann *et al.*, 2001). The setup is shown in Fig. 11.

For a detailed analysis of several probabilistic gates, see Lund and Ralph (2002), Gilchrist *et al.* (2003), and Lund *et al.* (2003). General two-qubit gates based on Mach-Zehnder interferometry were proposed by Englert *et al.* (2001). For a general discussion of entanglement in quantum information processing see Paris *et al.* (2003).

All the gates that we have discussed so far are probabilistic, and indeed all two-qubit gates based on projective measurements must be probabilistic. However, one might think that feedforward protocols can increase this probability to unity. As mentioned before, Knill (2003) demonstrated that the highest possible success probability for the NS gate (possibly using feedforward) is one-half. He did not show that this bound is saturated. Indeed, numerical evidence strongly suggests an upper bound of one-third for infinite feedforward without entangled ancillae (Scheel *et al.*, 2006). This indicates that the benefit of feedforward might not outweigh its cost.

C. Experimental demonstrations of gates

A number of experimental groups have already demonstrated all-optical probabilistic quantum gates. Early experiments involved a parity check of two polarization qubits on a polarizing beam splitter (Pittman *et al.*, 2002b) and a two-photon conditional phase switch (Resch *et al.*, 2002). A destructive CNOT gate was demonstrated by Franson *et al.* (2003) and O'Brien *et al.* (2003). In this section we will describe the experimental demonstration of three CNOT gates.

First, we consider the three-photon CNOT gate performed by Pittman *et al.* (2003). The gate is shown in Fig. 12 and consists of three polarization-encoded single-photon qubits and two polarizing beam splitters. Two of the polarization qubits represent the control and target qubits and are initially in an arbitrary two-qubit state $|\psi\rangle_{\text{in}} = \alpha_1|HH\rangle_{ct} + \alpha_2|HV\rangle_{ct} + \alpha_3|VH\rangle_{ct} + \alpha_4|VV\rangle_{ct}$. The third photon is used as an ancilla qubit and is initially prepared in the state $(|H\rangle + |V\rangle)/\sqrt{2}$. In the experiment of Pittman *et al.* the control and ancillary qubits are created using pulsed parametric down-conversion. The target qubit is generated by an attenuated laser pulse where the pulse is branched off the pump laser. The pulse is converted by a frequency doubler to generate entangled photon pairs at the same frequency as the photon constituting the target qubit. The CNOT gate is then implemented as follows: The action of the polarizing beam splitters on the control, target, and ancilla qubits transforms them according to

$$|\psi\rangle_{\text{out}} \propto |H\rangle_a U_{\text{C}}|\psi\rangle_{\text{in}} + |V\rangle_a \tilde{U}_{\text{C}}|\psi\rangle_{\text{in}} + \sqrt{6}|\xi\rangle_{act}, \tag{30}$$

where U_{C} is the CNOT operator between the control and target modes c and t and $\tilde{U}_{\text{C}} = (\mathbb{1}\otimes\sigma_x)U_{\text{C}}(\mathbb{1}\otimes\sigma_x)$. The state $|\xi\rangle_{act}$ represents terms with zero, two, or three photons present in the modes a, c, and t. Depending on the polarization of the measured ancillary photon in mode a (and one photon in the control and target modes) a CNOT gate up to a local transformation is applied to the control and target qubits. For a horizontally measured $|H\rangle_a$ photon the CNOT gate is exactly implemented, while for a vertically measured $|V\rangle_a$ photon the control and target qubits undergo a CNOT gate up to a bit flip on the target qubit. In Fig. 13 the truth table is shown as a function of the output qubit analyzers for all four computational basis states HH, HV, VH, and VV in the in-

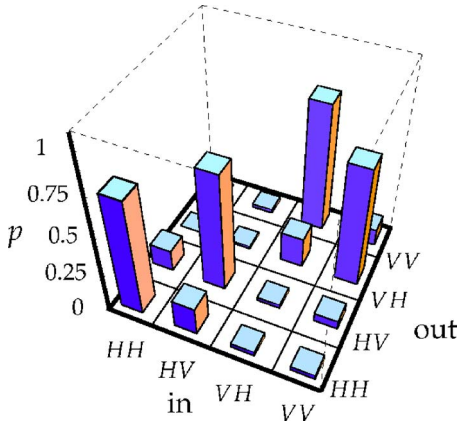

FIG. 13. (Color online) Experimental demonstration of the CNOT gate by Pittman *et al.* (2003). The probability of threefold coincidences as a function of the output qubit analyzers for all four computational basis states *HH*, *HV*, *VH*, and *VV* in the input registers is shown. The experimental error in the gate is approximately 21%.

put. The success probability for this gate is $p=1/4$ with an experimental error of approximately 21%.

The second experiment we consider is the CNOT gate of O'Brien *et al.*, depicted in Fig. 14 (O'Brien *et al.*, 2003), which is an implementation of the gate proposed by Ralph, Langford, *et al.* (2002). This is a postselected two-photon gate where two polarized qubits are created in a parametric down-conversion event. The polarization qubits can be converted into which-path qubits via the translation stage depicted in Fig. 14(b). Both the control and target qubits can be prepared in an arbitrary pure superposition of the computational basis states.

The gate is most easily understood in terms of dual spatial rails, Fig. 14(a). The two spatial modes that support the target qubit are mixed on a 50:50 beam splitter ($\theta_1=\pi/4$). One of these output modes is mixed with a spatial mode of the control qubit on a beam splitter with

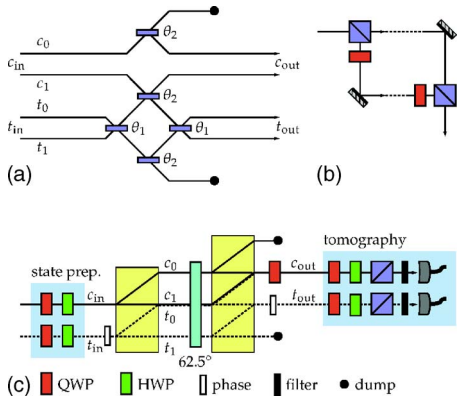

FIG. 14. (Color online) Schematic diagram of the CNOT gate demonstrated by O'Brien *et al.* (2003). (a) Concept of the two-qubit gate: The beam-splitter coefficients are $\theta_1=\pi/4$ and $\theta_2=\arccos(1/\sqrt{3})$. (b) Translation circuit for converting polarization and dual-rail qubits. (c) Schematic of the experimental setup. Simultaneous detection of a single photon at each detector heralds the successful operation of the gate.

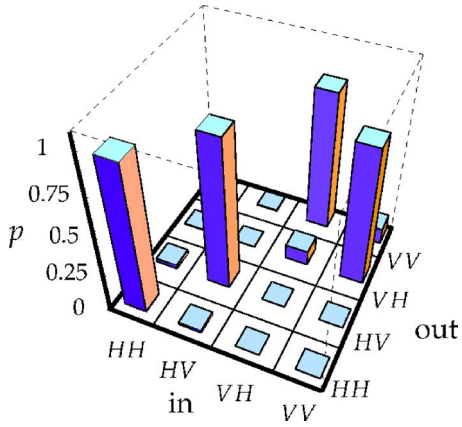

FIG. 15. (Color online) Experimental demonstration of the CNOT gate by O'Brien *et al.* (2003) in the logical qubit basis. The data are obtained by full state tomography of the output states.

$\cos\theta_2=1/\sqrt{3}$ (that is, a beam splitter with a reflectivity of $33\frac{1}{3}\%$). To balance the probability distribution of the CNOT gate, two dump ports consisting of another beam splitter with $\cos\theta_2=1/\sqrt{3}$ are introduced in one of the control and target modes. The gate works as follows: If the control qubit is in the state where the photon occupies the top mode c_0, there is no interaction between the control and target qubits. On the other hand, when the control photon is in the lower mode, the control and target photons interfere nonclassically at the central beam splitter with $\cos\theta_2=1/\sqrt{3}$. This two-photon quantum interference causes a π phase shift in the upper arm of the target interferometer t_0, and as a result the target photon is switched from one output mode to the other. In other words, the target state experiences a bit flip. The control qubit remains unaffected, hence the interpretation of this experiment as a CNOT gate. We do not always observe a single photon in each of the control and target outputs. However, when a control and a target photon are detected we know that the CNOT operation has been correctly realized. The success probability of such an event is 1/9. The detection of the control and target qubits could in principle be achieved by a quantum nondemolition measurement (see Sec. IV.A) and would not destroy the information encoded on the qubits. Experimentally, beam displacers are used to spatially separate the polarization modes and wave plates are used for beam mixing.

In Fig. 15, we show the truth table for the CNOT operation in the coincidence basis. The experimental fidelity of the gate is approximately 84% with conditional fringe visibilities exceeding 90% in nonorthogonal bases. This indicates that entanglement has been generated in the experiment: The gate can create entangled output states from separable input states.

The last experiment we consider in some detail is the realization of an optical CNOT gate by Gasparoni *et al.* (2004). The experiment is based on the four-photon logic gate of Pittman *et al.* (2001) depicted in Fig. 11.

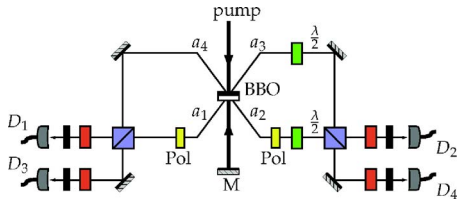

FIG. 16. (Color online) Schematic diagram of the four-photon CNOT gate by Gasparoni *et al.* (2004). A parametric down-conversion source is used to create the control and target input qubits in the spatial modes a_1 and a_2, as well as a maximally entangled ancilla pair in the spatial modes a_3 and a_4. Polarizing filters (Pol) can be used to destroy the initial entanglement in a_1 and a_2 if necessary.

The experiment of Gasparoni *et al.* employs a type-II parametric down-conversion source operated in a double-pass arrangement. The down-conversion process naturally produces close to maximally entangled photon pairs. This means that, depending on the input state for the control and target qubits, we may have to destroy or decrease any initial polarization entanglement. This is achieved by letting photons pass through appropriate polarization filters. After this, any two-qubit input state can be prepared. The gate depicted in Fig. 16 works as follows: The control qubit and one-half of the Bell state are sent into a polarizing beam splitter, while the target qubit with the second half of the Bell state is sent through a second polarizing beam splitter. The detection of ancilla photons heralds the operation of the CNOT gate (up to a known bit or sign flip on the control and/or target qubit). The probability of success of this gate is 1/4. Due to a lack of detectors that can resolve the difference between one and two photons and the rather low source and detector efficiencies, fourfold coincidence detection was employed to confirm the presence of photons in the output control and target ports. In principle, this postselection can be circumvented by using deterministic Bell pair sources and detectors that differentiate between one and two incoming photons.

The CNOT truth table for this experiment, based on fourfold coincidences, is shown in Fig. 17. This shows the operation of the CNOT gate. In addition, Gasparoni *et al.* showed that an equal superposition of H and V for the control qubit and H for the target qubit generated the maximally entangled state $|HH\rangle+|VV\rangle$ with an experimental fidelity of 81%. This clearly shows that the gate is creating entanglement.

As experiments become more sophisticated, more demonstrations of optical gates are reported. We cannot describe all of them here, but other recent experiments include the nonlinear sign shift (Sanaka *et al.*, 2004), a nondestructive CNOT (Zhao *et al.*, 2005), another CNOT gate (Fiorentino and Wong, 2004), and three-qubit optical quantum circuits (Takeuchi, 2000b, 2001). Four-qubit cluster states, which we will encounter later in this review, were demonstrated by Walther *et al.* (2005).

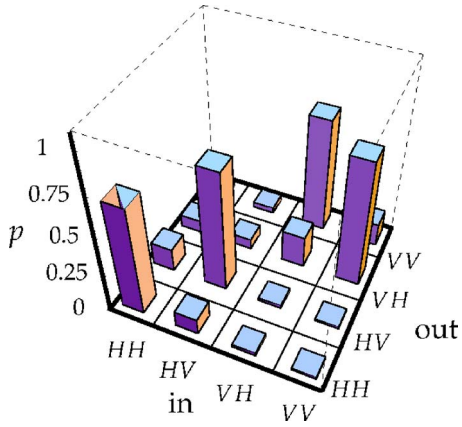

FIG. 17. (Color online) Experimental demonstration of the CNOT gate by Gasparoni *et al.* (2004). Fourfold coincidences for all combinations of inputs and outputs are shown.

D. Characterization of linear optics gates

In Sec. II.C, we showed the experimentally realized CNOT truth table for three different experimentally realized gates. However, the construction of the truth table is in itself not sufficient to show that a CNOT operation has been performed. It is essential to show the quantum coherence of the gate. One of the simplest ways to show coherence is to apply the gate to an initial separate state and show that the gate creates an entangled state (or vice versa). For instance, the operation of a CNOT gate on the initial state $(|H\rangle_c-|V\rangle_c)|V\rangle_t$ creates the maximally entangled singlet state $|H\rangle_c|V\rangle_t-|V\rangle_c|H\rangle_t$. This is sufficient to show the coherence properties of the gate. However, showing such coherences does not fully characterize the gate. To this end, we can perform state tomography. We show an example of this for the CNOT gate demonstrated by O'Brien *et al.* (2003) in Fig. 18. The reconstructed density matrix clearly indicates that a high-fidelity singlet state has been produced.

To fully understand the operation of a gate we need to create a complete map $\hat{\mathcal{E}}$ of all input states to output states:

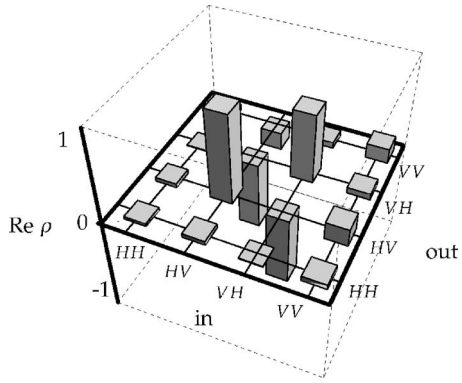

FIG. 18. Plot of the real part of the density matrix reconstructed from quantum process tomography for the input state $(|H\rangle_c-|V\rangle_c)|V\rangle_t$. This shows the highly entangled singlet state of the form $|H\rangle_c|V\rangle_t-|V\rangle_c|H\rangle_t$

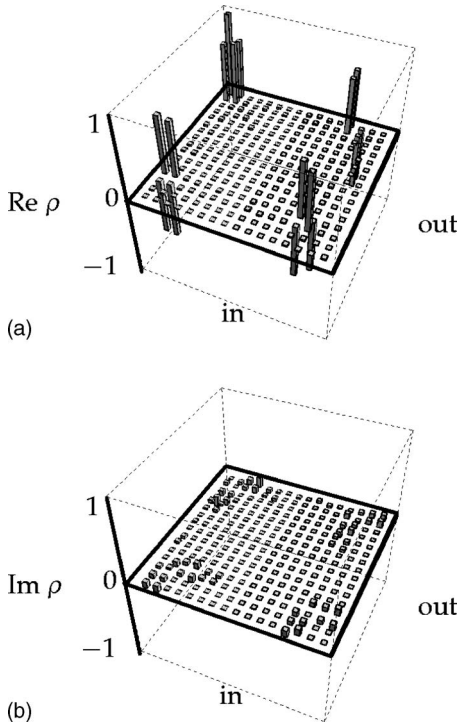

FIG. 19. Plot of the (a) real and (b) imaginary parts of the reconstructed process matrix of the CNOT gate by O'Brien *et al.* (2003). The ideal CNOT can be written as a coherent sum $\hat{U}_{\mathrm{CNOT}}=\frac{1}{2}(1\otimes 1+1\otimes X+Z\otimes 1-Z\otimes X)$ of the tensor products of Pauli operators $\{1,X,Y,Z\}$ acting on control and target qubits, respectively. The input abscissae are (from left to right) *II*, *IX*, *IY*, *IZ*, *XI*, *XX*, *XY*, *XZ*, *YI*, *YX*, *YY*, *YZ*, *ZI*, *ZX*, *ZY*, and *ZZ* while the output abscissae are (from left to right) *ZZ*, *ZY*, *ZX*, *ZI*, *YZ*, *YY*, *YX*, *YI*, *XZ*, *XY*, *XX*, *XI*, *IZ*, *IY*, *IX*, and *II*.

$$\hat{\mathcal{E}}(\rho)=\sum_{m,n=0}^{d-1}\chi_{mn}\hat{A}_m\rho\hat{A}_n^\dagger. \tag{31}$$

This map represents the process acting on an arbitrary input state ρ, where the operators $\hat{A}_m$ form a basis for the operators acting on ρ. The matrix χ describes completely the process $\hat{\mathcal{E}}$. Once this map has been constructed, we know everything about the process, including the purity of the operation and the entangling power of the gate. This information can then be used to fine-tune the gate operation. Experimentally, the map is obtained by performing *quantum process tomography* (Chuang and Nielsen, 1997; Poyatos *et al.*, 1997). A set of measurements is made on the output of the n-qubit quantum gate, given a complete set of input states. The input states and measurement projectors each form a basis for the set of n-qubit density matrices. For the two-qubit CNOT gate ($d=16$), we require 256 different settings of input states and measurement projectors.

In Fig. 19, we reproduce the reconstructed process matrix χ for the CNOT gate performed by O'Brien *et al.* (2003). The ideal CNOT can be written as a coherent sum $\hat{U}_{\mathrm{CNOT}}=\frac{1}{2}(1\otimes 1+1\otimes X+Z\otimes 1-Z\otimes X)$ of tensor products of Pauli operators $\{1,X,Y,Z\}$ acting on control and target qubits, respectively. The process matrix shows the populations and coherences between the basis operators making up the gate. The process fidelity for this gate exceeds 90% [see also O'Brien *et al.* (2004)]. For a general review of quantum state tomography with an emphasis on quantum information processing, see Lvovsky and Raymer (2005).

E. General probabilistic nonlinear gates

The two-qubit gates described above are special cases of N-ports acting on a set of input states, followed by a projective measurement. For quantum computing applications, however, we usually want the resulting nonlinear transformation M to be unitary. This is because nonunitary operations will reveal information about qubits in the projective measurement and hence corrupt the computation. We can derive a simple criterion that the N-ports and projective measurements must satisfy (Lapaire *et al.*, 2003).

Suppose the qubits undergoing M span a Hilbert space $\mathcal{H}_Q$ and the auxiliary qubits span $\mathcal{H}_A$. Furthermore, let U be the unitary transformation of the N-port in Eq. (10) and P_k the projector on the auxiliary states denoting the measurement outcome labeled by k. P_k must be a projector on the Hilbert space with dimension $\dim\mathcal{H}_A$ for M to be unitary. Given an arbitrary input state ρ of the qubits and a state σ of the auxiliary systems, the output state can be written as

$$\rho_{\mathrm{out}}^{(k)}=\frac{\mathrm{Tr}_A[U(\rho\otimes\sigma)U^\dagger P_k]}{\mathrm{Tr}_{QA}[U(\rho\otimes\sigma)U^\dagger P_k]}. \tag{32}$$

When we define $d(\rho)\equiv\mathrm{Tr}_{QA}[U(\rho\otimes\sigma)U^\dagger P_k]$, we find that M is unitary if and only if $d(\rho)$ is independent of ρ. We can then construct a test operator $\hat{T}=\mathrm{Tr}_A(\sigma U^\dagger P_k U)$. The induced operation on the qubits in $\mathcal{H}_Q$ is then unitary if and only if $\hat{T}$ is proportional to the identity or

$$\hat{T}=\mathrm{Tr}_A(\sigma U^\dagger P_k U)\propto 1\Leftrightarrow d(\rho)=d. \tag{33}$$

Given the auxiliary input state σ, the N-port transformation U, and the projective measurement P_k, it is straightforward to check whether this condition holds. The success probability of the gate is given by d.

In Eq. (32), the projective measurement was in fact a projection operator ($P_k^2=P_k$). However, in general, we might want to include generalized measurements, commonly known as positive operator-valued measures (POVM's). These are particularly useful when we need to distinguish between nonorthogonal states, and they can be implemented with N-ports as well (Myers and Brandt, 1997). Other optical realizations of nonunitary transformations were studied by Bergou *et al.* (2000).

The inability to perform a deterministic two-qubit gate such as the CNOT with linear optics alone is intimately related to the impossibility of complete Bell measurements with linear optics (Lütkenhaus *et al.*, 1999; Vaidman and Yoran, 1999; Calsamiglia, 2002). Since quantum computing can be cast into the shape of

single-qubit operations and two-qubit projections (Nielsen, 2003; Leung, 2004), we can approach the problem of making nonlinear gates via complete discrimination of multiqubit bases.

van Loock and Lütkenhaus gave straightforward criteria for the implementation of complete projective measurements with linear optics, photon counters, and arbitrary auxiliary states without feedforward (van Loock and Lütkenhaus, 2004). Suppose the basis states we want to identify without ambiguity are given by $\{|s_k\rangle\}$ and the auxiliary state is given by $|\psi_{\text{aux}}\rangle$. Applying the unitary N-port transformation yields the state $|\chi_k\rangle$. If the outgoing optical modes are denoted by a_j, with corresponding annihilation operators $\hat{a}_j$, then the set of conditions that have to be satisfied for $\{|\chi_k\rangle\}$ to be completely distinguishable are

$$\begin{aligned}
&\langle\chi_k|\hat{a}_j^\dagger\hat{a}_j|\chi_l\rangle = 0 \quad \forall\ j,\\
&\langle\chi_k|\hat{a}_j^\dagger\hat{a}_j\hat{a}_{j'}^\dagger\hat{a}_{j'}|\chi_l\rangle = 0 \quad \forall\ j,j',\\
&\langle\chi_k|\hat{a}_j^\dagger\hat{a}_j\hat{a}_{j'}^\dagger\hat{a}_{j'}\hat{a}_{j''}^\dagger\hat{a}_{j''}|\chi_l\rangle = 0 \quad \forall\ j,j',j'',\\
&\cdots .
\end{aligned} \tag{34}$$

Furthermore, when we keep the specific optical implementation in mind, we can use intuitive physical principles such as photon number conservation and group-theoretical techniques with the decomposition of U(N) into smaller groups. This gives us insight into the effects of the auxiliary states and photon detection on the (undetected) signal state (Scheel *et al.*, 2003).

So far we have generally focused on the means necessary to perform single-qubit rotations and CNOT gates. It is well known that such gates are sufficient for universal computation. However, it is not necessary to restrict ourselves to such a limited set of operations. Instead, it is possible to extend our operations to general circuits that can be constructed from linear elements, single-photon sources, and detectors. This is analogous to the shift in classical computing from a reduced instruction set computer (RISC) architecture to the complex instruction set computer (CISC) architecture. The RISC-based architecture in quantum computing terms could be thought of as a device built only from the minimum set of gates, while a CISC-based machine would be built from a much larger set: the natural set of gates allowed by the fundamental resources. The quantum SWAP operation illustrates this point. From fundamental gates, three CNOT's are required to build such an operation. However, from fundamental optical resources, only two beam splitters and a phase shifter are necessary. Scheel *et al.* (2003) focused their attention primarily on one- and two-mode situations, though the approach is easily extended to multimode situations. They differentiated between operations that are easy and those that are potentially difficult. For example, operations that cause a change in the Fock layers (for instance, the Hadamard operator) are generally difficult but not impossible.

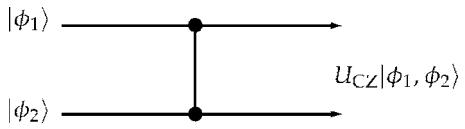

FIG. 20. The CZ applied to two qubits inside a quantum circuit. If it fails, then the two-qubit states are lost.

F. Scalable optical circuits and quantum teleportation

When the gates in a computational circuit succeed only with a certain probability p, then the entire calculation that uses N such gates succeeds with probability p^N. For large N and small p, this probability is minuscule. As a consequence, we have to repeat the calculation on the order of p^{-N} times or run p^{-N} such systems in parallel. Either way, the resources (time or circuits) scale exponentially with the number of gates. Any advantage that quantum algorithms might have over classical protocols is thus squandered on retrials or on the amount of hardware we need. In order to do useful quantum computing with probabilistic gates, we have to take the probabilistic elements out of the running calculation.

In 1999, Gottesman and Chuang proposed a trick that removes the probabilistic gate from the quantum circuit and places it in the resources that can be prepared off-line (Gottesman and Chuang, 1999). It is commonly referred to as the teleportation trick, since it teleports the gate into the quantum circuit.

Suppose we need to apply a probabilistic CZ gate to two qubits with quantum states $|\phi_1\rangle$ and $|\phi_2\rangle$, respectively. If we apply the gate directly to the qubits, we are very likely to destroy the qubits (see Fig. 20). However, suppose that we teleport both qubits from their initial mode to a different mode. For one qubit, this is shown in Fig. 21. Here x and z are binary variables, denoting the outcome of the Bell measurement, which determine the unitary transformation that we need to apply to the output mode. If $x=1$, we need to apply the σ_x Pauli operator (denoted by X), and if $z=1$, we need to apply σ_z (denoted by Z). If $x,z=0$, we do not apply the respective operator. For teleportation to work, we also need the entangled resource $|\Phi^+\rangle$, which can be prepared off-line. If we have a suitable storage device, we do not have to make $|\Phi^+\rangle$ on demand: we can create it with a probabilistic protocol using several trials and store the output of a successful event in the storage device.

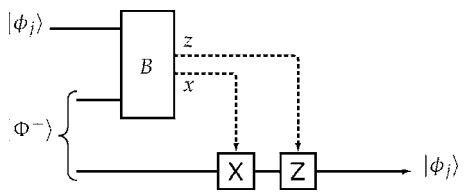

FIG. 21. The teleportation circuit. The state $|\phi_j\rangle$ is teleported via a Bell state $|\Phi^+\rangle$ and a Bell measurement B. The binary variables x and z parametrize the outcome of the Bell measurement and determine which Pauli operator is applied to the output mode.

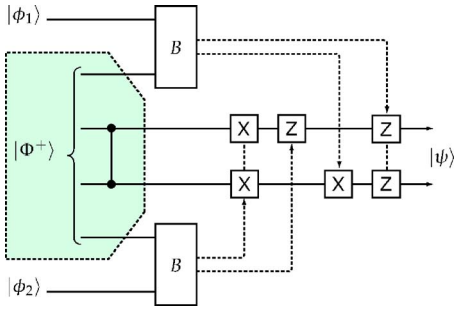

FIG. 22. (Color online) The CZ gate using teleportation: here $|\psi\rangle = U_{CZ}|\phi_1\phi_2\rangle$. By commuting the CZ gate through the Pauli gates from the computational circuit to the teleportation resources, we have taken the probabilistic part off-line. We can prepare the teleportation channel (the shaded area, including the CZ) in many trials, without disrupting the quantum computation.

When we apply the probabilistic CZ gate to the output of the two teleportation circuits, we effectively have again the situation depicted in Fig. 20, except that now our circuit is much more complicated. Since the CZ gate is part of the Clifford group, we can commute it through the Pauli operators X and Z at the cost of more Pauli operators. This is good news, because that means we can move the CZ gate from the right to the left at the cost of only the optically available single-qubit Pauli gates. Instead of preparing two entangled states $|\Phi^+\rangle$, we now have to prepare the resource $\mathbb{1}\otimes U_{CZ}\otimes\mathbb{1}|\Phi^+\rangle\otimes|\Phi^+\rangle$ (see Fig. 22). Again, with a suitable storage device, this can be done off-line with a probabilistic protocol. There are now no longer any probabilistic elements in the computational circuit.

G. The Knill-Laflamme-Milburn protocol

Unfortunately, there is a problem with the teleportation trick when applied to linear optics: In our qubit representation the Bell measurement (which is essential to quantum teleportation) is not complete and works at best only half of the time (Lütkenhaus *et al.*, 1999; Vaidman and Yoran, 1999). It seems that we are back where we started. This is one of the problems of linear optical quantum computing that was solved by Knill, Laflamme, and Milburn (2001).

In the KLM scheme, the qubits are chosen from the dual-rail representation. However, in the KLM protocol the teleportation trick applies to the single-rail state $\alpha|0\rangle+\beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ denote the vacuum and single-photon Fock state, respectively, and α and β are complex coefficients (this is because the CZ gate involves only one optical mode of each qubit). Linearity of quantum mechanics ensures that, if we can teleport this state, we can also teleport any coherent or incoherent superposition of it.

Choose the entangled state for teleportation to be the $2n$-mode state

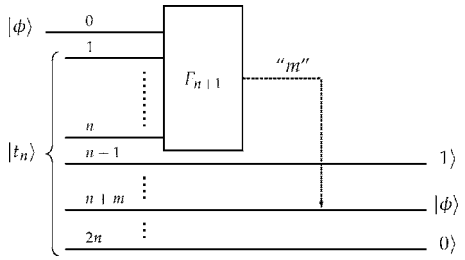

FIG. 23. Near-deterministic teleportation according to Knill, Laflamme, and Milburn. The input state $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$ is teleported to the mth outgoing mode, where m is the number of detected photons in the measurement of the $(n+1)$-point quantum Fourier transform. Note that $|\psi\rangle$ is a single-rail state; 0 and 1 denote photon numbers here.

$$|t_n\rangle = \frac{1}{\sqrt{n+1}}\sum_{j=0}^{n}|1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j}, \tag{35}$$

where $|k\rangle^j \equiv |k\rangle_1\otimes\cdots\otimes|k\rangle_j$. We can then teleport the state $\alpha|0\rangle+\beta|1\rangle$ by applying an $(n+1)$-point discrete quantum Fourier transform (QFT) to the input mode and the first n modes of $|t_n\rangle$ and count the number of photons m in the output mode. The input state will then be teleported to mode $n+m$ of the entangled state $|t_n\rangle$ (see Fig. 23).

The discrete quantum Fourier transform F_n can be written in matrix notation as

$$(F_n)_{jk} = \frac{1}{\sqrt{n}}\exp\left[2\pi i\frac{(j-1)(k-1)}{n}\right]. \tag{36}$$

It erases all path information of the incoming modes and can be interpreted as the n-mode generalization of the 50:50 beam splitter. To see how this functions as a teleportation protocol, it is easiest to consider an example.

Suppose we choose $n=5$, such that the state $|t_n\rangle$ describes ten optical modes, and assume further that we count two photons ($m=2$). This setup is given in Fig. 24. The two rows of zeros and ones (the bit values) denote two terms in the superposition $|t_5\rangle$. The five bit values on the left are the logical complement of the five bit values on the right (from which we will choose the outgoing qubit mode). It is clear from this diagram that when we find two photons, there are only two ways this could come about: either the input mode did not have a photon (associated with amplitude α), in which case the two

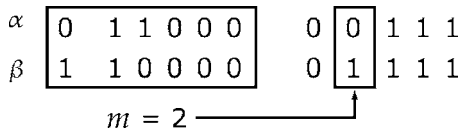

FIG. 24. The five-photon ancillary scheme for near-deterministic teleportation. The two rows correspond to two terms in the superposition state $|t_5\rangle$ that can yield two detected photons (including the unknown input state $\alpha|0\rangle+\beta|1\rangle$). The first six columns are detected, while the last five columns correspond to the freely propagating modes.

photons originated from $|t_5\rangle$, or the input mode did have a photon, in which case the state $|t_5\rangle$ provided the second photon. However, by construction of $|t_5\rangle$, the second mode of the five remaining modes must have the same number of photons as the input mode. And because we erased the which-path information of measured photons using the F_6 transformation, the two possibilities are added coherently. This means that we teleported the input mode to mode $5+2=7$. In order to keep the amplitudes of the output state equal to those of the input state, the relative amplitudes of the terms in $|t_n\rangle$ must be equal.

Sometimes this procedure fails, however. When we count either zero or $n+1$ photons in the output of the QFT, we collapse the input state onto zero or one photon, respectively. In those cases we have performed an unintentional measurement of the qubit in the computational basis, which indicates that the teleportation failed. The success rate of this protocol is $n/(n+1)$ (where we used that $|\alpha|^2+|\beta|^2=1$). We can make the success probability of this protocol as large as we like by increasing the number of modes n. The success probability for teleporting a two-qubit gate is then the square of this probability, $n^2/(n+1)^2$, because we need to teleport two qubits successfully. The quantum teleportation of a superposition state of a single photon with the vacuum was realized by Lombardi *et al.* (2002) using spontaneous parametric down-conversion.

Now that we have a (near-)deterministic teleportation protocol, we have to apply the probabilistic gates to the auxiliary states $|t_n\rangle$. For the CZ gate, we need the auxiliary state

$$|cz_n\rangle = \frac{1}{n+1}\sum_{i,j=0}^{n}(-1)^{(n-i)(n-j)}|1\rangle^i|0\rangle^{n-i} \times |0\rangle^i|1\rangle^{n-i}|1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j}. \quad (37)$$

The cost of creating this state is quite high. In the next section we will see how the addition of error-correcting codes can alleviate this resource count somewhat.

At this point, we should resolve a paradox: Earlier results have shown that it is impossible to perform a deterministic Bell measurement with linear optics. However, teleportation relies critically on a Bell measurement of some sort, and we have just shown that we can perform near-deterministic teleportation with only linear optics and photon counting. The resolution in the paradox lies in the fact that the impossibility proofs are concerned with exact deterministic Bell measurements. The KLM variant of the Bell measurement always has an arbitrarily small error probability ϵ. We can achieve scalable quantum computing by making ϵ smaller than the fault-tolerant threshold.

One way to boost the probability of success of the teleportation protocol is to minimize the amplitudes of the $j=0$ and $j=n$ terms in the superposition $|t_n\rangle$ of Eq. (35). At the cost of changing the relative amplitudes (and therefore introducing a small error in the teleported output state), the success probability of teleporting a single qubit can then be boosted to $1-1/n^2$ (Franson *et al.*, 2002). The downside of this proposal is that the errors become less well behaved: Instead of perfect teleportation of the state $\alpha|0\rangle+\beta|1\rangle$ with an occasional σ_z measurement of the qubit, the Franson variation will yield an output state $c_j\alpha|0\rangle+c_{j-1}\beta|1\rangle$, where j is known and c_j are the amplitudes of the modified $|t_n\rangle$. There is no simple two-mode unitary operator that transforms this output state into the original input state without knowledge about α and β. This makes error correction much harder.

Another variation on the KLM scheme, due to Spedalieri *et al.* (2006), redefines the teleported qubit $\alpha|0\rangle+\beta|1\rangle$ and Eq. (35). The vacuum state is replaced with a single horizontally polarized photon, $|0\rangle\rightarrow|H\rangle$, and the one-photon state is replaced with a vertically polarized photon, $|1\rangle\rightarrow|V\rangle$. There are now $2n$ rather than n photons in the state $|t_n\rangle$. The teleportation procedure remains the same, except that we now count the total number of vertically polarized photons. The advantage of this approach is that we know that we should detect exactly n photons. If we detect $m\neq n$ photons, we know that something went wrong, and this therefore provides us with a level of error detection (see also Sec. V).

Of course, having a near-deterministic two-qubit gate is all very well, but if we want to do arbitrarily long quantum computations, the success probability of the gates must be close to 1. Instead of making larger teleportation networks, it might be more cost effective or easier to use a form of error correction to make the gates deterministic. This is the subject of the next section.

H. Error correction of the probabilistic gates

As we saw in the previous section the success probability of teleportation gates can be increased arbitrarily by preparing larger entangled states. However, the asymptotic approach to unit probability is quite slow as a function of n. A more efficient procedure is to encode against gate failure. This is possible because of the well-defined failure mode of the teleporters. We noted in the previous section that the teleporters fail if zero or $n+1$ photons are detected because we can then infer the logical state of the input qubit. In other words, the failure mode of the teleporters is to measure the logical value of the input qubit. If we can encode against accidental measurements of this type, then our qubit will be able to survive gate failures and the probability of eventually succeeding in applying the gate will be increased.

KLM introduced the following logical encoding over two polarization qubits:

$$|0\rangle_L = |HH\rangle + |VV\rangle, \qquad |1\rangle_L = |HV\rangle + |VH\rangle. \quad (38)$$

This is referred to as parity encoding as the logical 0 state is an equal superposition of the even-parity states

and the logical 1 state is an equal superposition of the odd-parity states. Consider an arbitrary logical qubit $\alpha|0\rangle_L+\beta|1\rangle_L$. Suppose a measurement is made on one of the physical qubits, returning the result H. The effect on the logical qubit is the projection

$$\alpha|0\rangle_L + \beta|1\rangle_L \rightarrow \alpha|H\rangle + \beta|V\rangle. \tag{39}$$

That is, the qubit is not lost; the encoding is just reduced from parity to polarization. Similarly, if the measurement result is V, we have

$$\alpha|0\rangle_L + \beta|1\rangle_L \rightarrow \alpha|V\rangle + \beta|H\rangle. \tag{40}$$

Again the superposition is preserved, but this time a bit flip occurs. However, the bit flip is heralded by the measurement result and can therefore be corrected.

Suppose we wish to teleport the logical value of a parity qubit with the t_1 teleporter. We attempt to teleport one of the polarization qubits. If we succeed, we measure the value of the remaining polarization qubit and apply any necessary correction to the teleported qubit. If we fail, we can use the result of the teleporter failure (did we find zero photon or two photons?) to correct the remaining polarization qubit. We are then able to try again. In this way the probability of success of teleportation is increased from 1/2 to 3/4. At this point we have lost our encoding in the process of teleporting. However, this can be fixed by introducing the following entanglement resource:

$$|H\rangle|0\rangle_L + |V\rangle|1\rangle_L. \tag{41}$$

If teleportation is successful, the output state remains encoded. The main observation is that the resources required to construct the entangled state of Eq. (41) are much less than those required to construct $|t_3\rangle$. As a result, error encoding turns out to be a more efficient way to scale up teleportation and hence gate success.

Parity encoding of an arbitrary polarization qubit can be achieved by performing a CNOT gate between the arbitrary qubit and an ancilla qubit prepared in the diagonal state, where the arbitrary qubit is the target and the ancilla qubit is the control. This operation has been demonstrated experimentally (O'Brien *et al.*, 2005). In this experiment the projections given by Eqs. (39) and (40) were confirmed up to fidelities of 96%. In a subsequent experiment by Pittman *et al.*, the parity encoding was prepared in a somewhat different manner and, in order to correct the bit-flip errors, a feedforward mechanism was implemented (Pittman *et al.*, 2005).

To boost the probability of success further, we need to increase the size of the code. The approach adopted by Knill, Laflamme, and Milburn (2001) was to concatenate the code. At the first level of concatenation the parity code states become

$$\begin{aligned} |0\rangle_L^{(4)} &= |00\rangle_L + |11\rangle_L, \\ |1\rangle_L^{(4)} &= |01\rangle_L + |10\rangle_L. \end{aligned} \tag{42}$$

This is now a four-photon encoded state. At the second level of concatenation we would obtain an eight-photon state, etc. At each higher level of concatenation, corresponding encoded teleportation circuits can be constructed that operate with higher and higher probabilities of success.

If we are to use encoded qubits, we must consider a universal set of gates on the logical qubits. An arbitrary rotation about the x axis, defined by the operation $X_\theta = \cos(\theta/2)I - i\sin(\theta/2)X$, is implemented on a logical qubit by simply implementing it on one of the constituent polarization qubits. However, to achieve arbitrary single-qubit rotations we also require a $\pi/2$ rotation about the z axis, i.e., $Z_{\pi/2}=(1/\sqrt{2})(I-iZ)$. This can be implemented on the logical qubit by applying $Z_{\pi/2}$ to each constituent qubit and then applying a CZ gate between the constituent qubits. The CZ gate is of course nondeterministic, and so the $Z_{\pi/2}$ gate becomes nondeterministic for the logical qubit. Thus both the $Z_{\pi/2}$ and the logical CZ gate must be implemented with the teleportation gates in order to form a universal gate set for the logical qubits. In Knill *et al.* (2000) it is reported that the probability of successfully implementing a $Z_{\pi/2}$ gate on a parity qubit in this way is $P_Z=1-F_Z$, where

$$F_Z = \frac{f^2(2-f)}{1-f(1-f)} \tag{43}$$

and f is the probability of failure of the teleporters acting on the constituent polarization qubits. One can obtain the probability of success after concatenation iteratively. For example, the probability of success after one concatenation is $P_{Z1}=1-F_{Z1}$, where $F_{Z1}=F_Z^2(2-F_Z)/[1-F_Z(1-F_Z)]$. The probability of success for a CZ gate between two logical qubits is $P_{CZ}=(1-F_Z)^2$. Notice that, for this construction, an overall improvement in gate success is not achieved unless $f<1/2$. Using these results one finds that first level concatenation and t_3 ($f=1/4$) teleporters are required to achieve a CZ gate with better than 95% probability of success. It can be estimated that of order 10^4 operations would be required in order to implement such a gate (Hayes *et al.*, 2004).

So the physical resources for the original KLM protocol, albeit scalable, are daunting. For linear optical quantum computing to become a viable technology, we need more efficient quantum gates. This is the subject of the next section.

III. IMPROVEMENT ON THE KLM PROTOCOL

We have seen that the KLM protocol explicitly tells us how to build scalable quantum computers with single-photon sources, linear optics, and photon counting. However, showing scalability and providing a practical architecture are two different things. The overhead cost of a two-qubit gate in the KLM proposal, albeit scalable, is prohibitively large.

If linear optical quantum computing is to become a practical technology, we need less resource-intensive protocols. Consequently, there have been a number of proposals that improve the scalability of the KLM scheme. In this section we review these proposals. Sev-

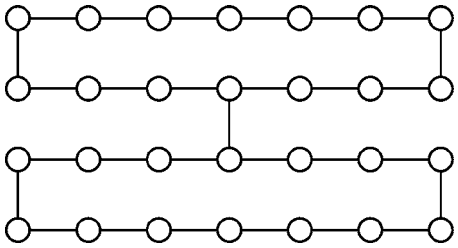

FIG. 25. A typical cluster state. Every circle represents a logical qubit, and the vertices represent CZ operations. A quantum computation proceeds by performing single-qubit measurements on the left column of qubits, thus removing them from the cluster and teleporting the quantum information through the cluster state. The vertical links induce two-qubit operations.

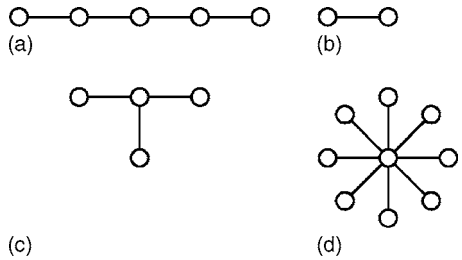

FIG. 26. Different cluster and graph states. (a) A linear cluster of five qubits. (b) A cluster representing the Bell states. (c) A four-qubit GHZ state. This state can be obtained by an X measurement of the central qubit in (a). (d) A general GHZ state.

eral improvements are based on cluster-state techniques (Yoran and Reznik, 2003; Nielsen, 2004; Browne and Rudolph, 2005), and recently a circuit-based model of optical quantum computing was proposed that circumvents the need for the very costly KLM-type teleportation (Gilchrist *et al.*, 2005). After a brief introduction to cluster-state quantum computing, we describe these different proposals.

A. Cluster states in optical quantum computing

In the traditional circuit-based approach to quantum computing, quantum information is encoded in qubits, which subsequently undergo single- and two-qubit operations. There is, however, an alternative model, called the cluster-state model of quantum computing (Raussendorf and Briegel, 2001), also known as one-way quantum computing or graph-state quantum computing. In this model, the quantum information encoded in a set of qubits is teleported to a new set of qubits via entanglement and single-qubit measurements. It uses a so-called cluster state in which physical qubits are represented by nodes and entanglement between the qubits is represented by connecting lines (see Fig. 25). Suppose that the qubits in the cluster state are arranged in a lattice. The quantum computation then consists of performing single-qubit measurements on a "column" of qubits, the outcomes of which determine the basis for the measurements on the next column. Single-qubit gates are implemented by choosing a suitable basis for the single-qubit measurement, while two-qubit gates are induced by local measurements of two qubits exhibiting a vertical link in the cluster state. The term graph state is often used to denote cluster states that do not exhibit a rectangular lattice structure. To avoid confusion, we will refer to all clusters and graphs as cluster states in this review.

Two-dimensional cluster states, i.e., states with vertical as well as horizontal links, are essential for quantum computing, as linear cluster-state computing can be efficiently simulated on classical computers (Nielsen, 2006b). Since single-qubit measurements are relatively easy to perform when the qubits are photons, this approach is potentially suitable for linear optical quantum computing: Given the right cluster state, we need to perform only the photon detection and feedforward postprocessing. Verstraete and Cirac (2004) demonstrated how the teleportation-based computing scheme of Gottesman and Chuang could be related to clusters. They derived their results for generic implementations and did not address the special demands of optics.

Before we discuss the various proposals for efficient cluster-state generation, we present a few more properties of cluster states. Most importantly, a cluster such as the one depicted in Fig. 25 does not correspond to a unique quantum state: It represents a family of states that are equivalent up to local unitary transformations of the qubits. More precisely, a cluster state $|C\rangle$ is an eigenstate of a set of commuting operators S_i called the stabilizer generators (Raussendorf *et al.*, 2003):

$$S_i|C\rangle = \pm|C\rangle \quad \forall\ i. \tag{44}$$

Typically, we consider the cluster state that is a +1 eigenstate for all S_i. Given a graphical representation of a cluster state, we can write down the stabilizer generators by following a simple recipe: Every qubit i (node in the cluster) generates an operator S_i. Suppose that a qubit labeled q is connected to k neighbors labeled from 1 to k. The stabilizer generator S_q for qubit q is then given by

$$S_q = X_q kj = 1 \otimes Z_j. \tag{45}$$

For example, a (simply connected) linear cluster chain of five qubits labeled a, b, c, d, and e [Fig. 26(a)] is uniquely determined by the following five stabilizer generators: $S_a = X_a Z_b$, $S_b = Z_a X_b Z_c$, $S_c = Z_b X_c Z_d$, $S_d = Z_c X_d Z_e$, and $S_e = Z_d X_e$. It is easily verified that these operators commute. Note that this recipe applies to general cluster states, where every node (i.e., a qubit) can have an arbitrary number of links with other nodes. The rectangular-shaped cluster states are a subset of the set of cluster states.

Consider the following important examples of cluster states: The connected two-qubit cluster state is locally equivalent to the Bell states [Fig. 26(b)], and a linear three-qubit cluster state is locally equivalent to a three-qubit Greenberger-Horne-Zeilinger (GHZ) state. These are states that are locally equivalent to

$|0,\ldots,0\rangle+|1,\ldots,1\rangle$. In general, GHZ states can be represented by a star-shaped cluster such as shown in Figs. 26(c) and 26(d).

To build the cluster state that is needed for quantum computation, we can transform one cluster state into another using entangling operations, single-qubit operations, and single-qubit measurements. A Z measurement removes a qubit from a cluster and severs all the bonds that it had with the cluster (Raussendorf *et al.*, 2003; Hein *et al.*, 2004). An X measurement on a qubit in a cluster removes that qubit from the cluster, and transfers all the bonds of the original qubit to a neighbor. All the other neighbors become single qubits connected to the neighbor that inherited the bonds (Raussendorf *et al.*, 2003; Hein *et al.*, 2004).

There is a well-defined physical recipe for creating cluster states, such as the one shown in Fig. 25. First of all, we prepare all qubits in the state $(|0\rangle+|1\rangle)/\sqrt{2}$. Second, we apply a CZ gate to all qubits that are to be linked with a horizontal or vertical line, the order of which does not matter.

To make a quantum computer using the one-way quantum computer, we need two-dimensional cluster states (Nielsen, 2006b). Computation on linear cluster chains can be simulated efficiently on a classical computer. Furthermore, two-dimensional cluster states can be created with Clifford group gates. The Gottesman-Knill theorem then implies that single-qubit measurements implementing the quantum computation must include non-Pauli measurements.

It is the entangling operation that is problematic in optics, since a linear optical CZ gate in our qubit representation is inherently probabilistic. There have been, however, several proposals for making cluster states with linear optics and photon detection, and we discuss them in chronological order.

B. The Yoran-Reznik protocol

The first proposal for linear optical quantum computing along these lines by Yoran and Reznik (2003) is not strictly based on the cluster-state model, but it has many attributes in common. Most notably, it uses "entanglement chains" of photons in order to pass the quantum information through the circuit via teleportation.

First of all, for this protocol to work, the nondeterministic nature of optical teleportation must be circumvented. We have already remarked several times that complete (deterministic) Bell measurements cannot be performed in the dual-rail and polarization qubit representations of linear optical quantum computing. However, in a different representation this is no longer the case. Instead of the traditional dual-rail implementation of qubits, we can encode the information of two qubits in a single photon when we include both the polarization and the spatial degree of freedom. Consider the device depicted in Fig. 27. A single photon carrying specific polarization and path information is then transformed as (Popescu, 1995)

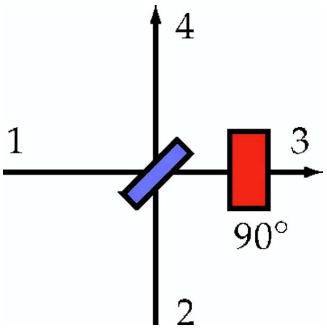

FIG. 27. (Color online) Using the "hyperentanglement" of the polarization and which-path observables, a single photon spans a four-dimensional Hilbert space $\{|H,1\rangle,|H,2\rangle,|V,1\rangle,|V,2\rangle\}$. A simple 50:50 beam-splitter and polarization rotation then furnishes a deterministic transformation from the computational basis to the Bell basis.

$$
\begin{aligned}
|H,1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|V,3\rangle+|H,4\rangle),\\
|V,1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|V,4\rangle-|H,3\rangle),\\
|H,2\rangle &\rightarrow \frac{1}{\sqrt{2}}(|H,4\rangle-|V,3\rangle),\\
|V,2\rangle &\rightarrow \frac{1}{\sqrt{2}}(|V,4\rangle+|H,3\rangle).
\end{aligned}
\tag{46}
$$

These transformations look tantalizingly similar to the transformation from the computational basis to the Bell basis. However, there is only one photon in this system. The second qubit is given by the which-path information of the input modes. By performing a polarization measurement of the output modes 3 and 4, we can project the input modes onto a Bell state. This type of entanglement is sometimes called hyperentanglement, since it involves more than one observable of a single system (Kwiat and Weinfurter, 1998; Barreiro *et al.*, 2005; Cinelli *et al.*, 2005). A teleportation experiment based on this mechanism was performed by Boschi *et al.* (1998).

It was shown by Yoran and Reznik how these transformations can be used to cut down on the number of resources: Suppose we want to implement the computational circuit given in Fig. 28. We will then create (highly entangled) chain states of the form

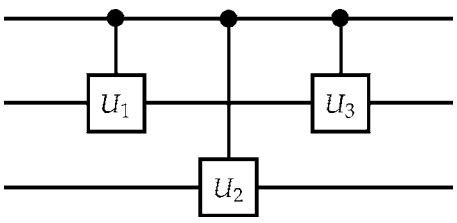

FIG. 28. A typical three-qubit quantum computational circuit.

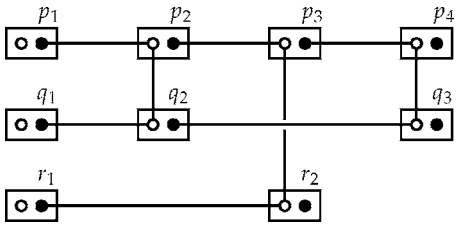

FIG. 29. The computational circuit of Fig. 28 in terms of the physical implementation by Yoran and Reznik (2003). This is reminiscent of the cluster-state model of quantum computing. The open and solid dots represent the polarization and which-path degrees of freedom, respectively.

$$(\alpha|H\rangle_{p_1}+\beta|V\rangle_{p_1})(|1\rangle_{p_1}|H\rangle_{p_2}+|2\rangle_{p_1}|V\rangle_{p_2})\times\cdots$$
$$\times(|2n-1\rangle_{p_n}|H\rangle_{p_{n+1}}+|2n\rangle_{p_n}|V\rangle_{p_{n+1}})|2n+1\rangle_{p_{n+1}}, \tag{47}$$

where the individual photons are labeled by p_j. This state has the property that a Bell measurement of the form of Eq. (46) on the first photon p_1 will teleport the input qubit $\alpha|H\rangle+\beta|V\rangle$ to the next photon p_2.

Let us assume that we have several of these chains running in parallel and that, furthermore, there are vertical "cross links" of entanglement between different chains, just where we want to apply the two-qubit gates U_1, U_2, and U_3. This situation is sketched in Fig. 28. The translation into optical chain states is given in Fig. 29. The open circles represent polarization and dots represent the path degree of freedom. In Fig. 30, the circuit that adds a link to the chain is shown. The unitary operators U_1, U_2, and U_3 are applied to the polarization degree of freedom of photons.

Note that we still need to apply two probabilistic CZ gates in order to add a qubit to a chain. However, whereas the KLM scheme needs the teleportation protocol to succeed with very high probability [scaling as $n^2/(n+1)^2$] in the protocol proposed by Yoran and Reznik the success probability of creating a link in the chain must be larger than one-half. This way, the entanglement chains grow on average. This is a very important observation and plays a key role in the protocols discussed in this section. Similarly, a vertical link between entanglement chains can be established with a two-qubit unitary operation on the polarization degree of freedom of both photons (cf. the vertical lines between the open dots in Fig. 29). If the gate fails, we can grow longer chains and try again until the gate succeeds.

C. The Nielsen protocol

A more explicit use of cluster-state quantum computing was made by Nielsen (2004). As Yoran and Reznik, Nielsen recognized that in order to build cluster states, the probability of adding a link to the cluster must be larger than one-half, rather than arbitrarily close to 1. Otherwise, the cluster will shrink on average. The KLM teleportation protocol allows us to apply a two-qubit

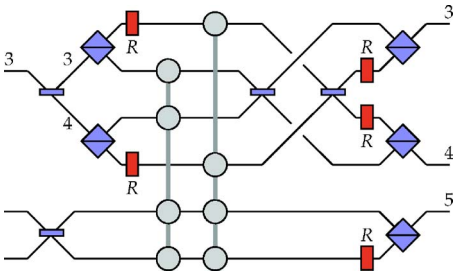

FIG. 30. (Color online) How to add a link to the Yoran-Reznik chain. This will create the state given in Eq. (47) with $n+1=5$. The four vertically connected gray circles represent the probabilistic CZ gate. Note that we need two of them.

gate with probability $n^2/(n+1)^2$, depending on the number n of ancillary photons. Let us denote a CZ gate with this success probability by $\mathrm{CZ}_{n^2/(n+1)^2}$. This gate can be used to add qubits to a cluster chain. When the gate fails, it removes a qubit from the cluster. This means that, instead of using very large n to make the CZ gate near deterministic, links can be added on average with a modest $\mathrm{CZ}_{9/16}$ gate, or $n=3$. This leads to similarly reduced resource requirements as the Yoran-Reznik protocol, while still keeping (in principle) error-free quantum computing. However, there is an extra gain in resources available when we try to add a qubit to a chain (Nielsen, 2004).

Suppose that we wish to add a single qubit to a cluster chain via the teleportation-based CZ gate. Instead of teleporting the two qubits simultaneously, we first teleport the disconnected qubit and second teleport the qubit at the end of the cluster. We know that a teleportation failure will remove the qubit from the cluster, so we attempt the second teleportation protocol only after the first has succeeded. The first teleportation protocol then becomes part of the off-line resource preparation, and the CZ gate effectively changes from $\mathrm{CZ}_{n^2/(n+1)^2}$ to $\mathrm{CZ}_{n/(n+1)}$. The growth requirement of the cluster state then becomes $n/(n+1)>1/2$, or $n=2$, and we make another substantial saving in resources.

Apart from linear cluster states, we also need the ability to make the two-dimensional clusters depicted in Fig. 25. This is equivalent to linking a qubit to two cluster chains and hence needs two successful CZ gates. Arguing along the same lines as before, it is easily shown that the success probability is $4/9$ for this procedure using two ancillae per teleportation gate. Since this is smaller than one-half, this procedure on average removes qubits from the cluster. However, we can first add extra qubits with the previous procedure, such that there is a buffer of qubits in the cluster state. This way, the average shrinkage of the cluster due to vertical links is absorbed by the buffer region.

Finally, Nielsen introduces so-called microclusters consisting of multiple qubits connected to the end point of a cluster chain. Such a microcluster is depicted in Fig. 26(d), where the central qubit is an end point of a cluster chain. Having such a fan of qubits at the end of a chain,

we can retry the entangling gate as many times as there are "dangling" qubits. This removes the lower limit on the success probability of the CZ gate at the cost of making large GHZ states (Nielsen and Dawson, 2004). Therefore, any optical two-qubit gate with arbitrary success probability p can be used to make cluster states efficiently.

D. The Browne-Rudolph protocol

There is still a cheaper way to grow cluster states. In order for a cluster chain to grow on average without using expensive microclusters, the success probability of adding a single qubit to the chain must be larger than one-half. However, if we can add small chains of qubits to the cluster, this requirement may be relaxed. Suppose that the success probability of creating a link between two cluster chains is p and that in each successful linking of two chains we lose d_s qubits from the chain. This might happen when the entangling operation joining the two clusters involves the detection of qubits in the cluster. Similarly, in an unsuccessful attempt, we may lose d_f qubits from the existing cluster chain (we do not count the loss of qubits in the small chain that is to be added). If our existing cluster chain has length N and the chain we wish to add has length m, then we can formulate the following growth requirement (Barrett and Kok, 2005; Browne and Rudolph, 2005):

$$p(N+m-d_s)+(1-p)(N-d_f)>N$$
$$\Leftrightarrow m>\frac{pd_s+(1-p)d_f}{p}. \tag{48}$$

Given a specific strategy (d_s,d_f) and success probability p, we need to create chains of length m off-line in order to make large cluster chains efficiently. Note that, again, there is no lower limit to the success probability p of the entangling operation in principle. This allows us to choose the optical gates with the most desirable physical properties (other than high success probability), and it means that we do not have to use the expensive and error-prone $\mathrm{CZ}_{n/(n+1)}$ gates.

Indeed, Browne and Rudolph introduced a protocol for generating cluster states using the probabilistic parity gates of Sec. II.B (Cerf *et al.*, 1998; Pittmann *et al.*, 2001; Browne and Rudolph, 2005). The notable advantage of this gate is that it is relatively easy to implement in practice (Pittman *et al.*, 2000b) and that it can be made robust against common experimental errors. Initially these gates were called parity gates, but following Browne and Rudolph we call these the type-I and type-II fusion *gates* (see Fig. 31).

Let us first consider the operation of the type-I fusion gate in Fig. 31(a). Given the detection of one and only one photon with polarization H or V in the detector D, the gate induces the following projection on the input state:

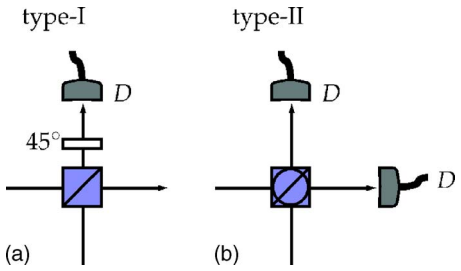

FIG. 31. (Color online) Two types of fusion operator: (a) The type-I fusion operator employs a polarization beam splitter (PBS1) followed by the detection D of a single output mode in the 45° rotated polarization basis. This operation determines the parity of the input mode with probability 1/2. (b) The type-II fusion operator uses a diagonal polarization beam splitter (PBS2), detects both output modes, and projects the input state onto a maximally entangled Bell state with probability 1/2.

$$\text{"H"}: \quad \frac{1}{\sqrt{2}}(|H\rangle\langle H,H|-|V\rangle\langle V,V|),$$
$$\text{"V"}: \quad \frac{1}{\sqrt{2}}(|H\rangle\langle H,H|+|V\rangle\langle V,V|). \tag{49}$$

It is easily verified that the probability of success for this gate is $p=1/2$. When the type-I fusion gate is applied to two photons belonging to two different cluster states containing n_1 and n_2 photons, respectively, a successful operation will generate a cluster chain of n_1+n_2-1 photons. However, when the gate fails, it effectively performs a σ_z measurement on both photonic qubits and the two cluster states both lose the qubit that was detected. The type-I fusion gate is therefore a (1,1) strategy, i.e., $d_s=d_f=1$ (recall that we count only the loss of qubits on one cluster to determine d_f). The ideal growth requirement is $m>1/p=2$.

Browne and Rudolph also introduced the type-II fusion operator [see Fig. 31(b)]. This operation involves the photon detection of both output modes of a polarization beam splitter, and a successful event is heralded by a detector coincidence (i.e., one photon with a specific polarization in each detector). When successful, this gate projects the two incoming qubits onto one of two polarization Bell states, depending on the detection outcome:

$$\text{"H,V" or "V,H"}: \quad \frac{1}{\sqrt{2}}(|H,H\rangle+|V,V\rangle),$$
$$\text{"H,H" or "V,V"}: \quad \frac{1}{\sqrt{2}}(|H,V\rangle+|V,H\rangle). \tag{50}$$

The success probability of this gate is $p=1/2$, and it is a (2,1) strategy (i.e., $d_s=2$ and $d_f=1$). The ideal growth requirement is thus $m>(1+p)/p=3$. The type-II fusion gate is essentially a version of the incomplete optical Bell measurement (Weinfurter, 1994; Braunstein and Mann, 1996).

Note that in order to grow long chains, we must be able to create chains of three qubits. Given a plentiful supply of Bell pairs as our fundamental resource, we can make three-qubit chains only with the type-I fusion gate, since the type-II gate necessarily destroys two qubits. This also indicates a significant difference between this protocol and the previous ones: Using only single-photon sources, the fusion gates alone cannot create cluster states. We can, however, use any method to create the necessary Bell pairs (such as the CZ gate in Sec. II.A), as they constitute an off-line resource.

Upon successful operation, both type-I and type-II fusion gates project two qubits that are part of a cluster onto a polarization Bell state. When we apply a Hadamard operation to one of the qubits adjacent to the detected qubit(s), the result will again be a cluster state. However, upon failure the characteristics of the fusion gates are quite different from each other. When the type-I gate fails, it performs a Z measurement on the input qubits. When the type-II gate fails, it performs an X measurement on the input qubits. Recall that there is a fundamental difference between a Z and an X measurement on qubits in cluster states: A Z measurement will break all bonds with the qubit neighbors and remove it from the cluster. An X measurement will also remove the qubit from the cluster, but it will join its neighbors into a redundantly encoded qubit. In terms of the clusters, this corresponds to a qubit with dangling bonds called leaves or cherries [see also Fig. 26(c)].

When the measured qubits are both end points of cluster states (i.e., they have only one link to the rest of the cluster), failing type-I and type-II fusion gates have similar effects on the cluster states: They remove the qubits from the cluster. However, when fusion gates are applied to two qubits inside a cluster (i.e., the qubits have two or more links to other qubits in the cluster), then the failure modes of the two fusion gates differ dramatically: In particular, when we apply the fusion gate to a qubit in a chain, a failed type-I gate will break the chain, while a failed type-II gate will only shorten the chain and create one redundantly encoded qubit next to the measured qubit. Since it is costly to reattach a broken chain, it is best to avoid the type-I gate for this purpose. The redundancy induced by a failed type-II fusion gate is closely related to the error correction model in Sec. V. We will explore this behavior further in the next section.

Again, we need at least two-dimensional cluster states in order to achieve the level of quantum computing that cannot be simulated efficiently on a classical computer. Using the failure behavior of the type-II fusion gate, we can construct an efficient way of creating vertical links between linear cluster chains. We attempt a type-II fusion between two qubits that are part of different chains. If the gate succeeds, we have created a vertical link on the neighboring qubits. If the gate fails, one neighboring qubit to each detected qubit becomes redundantly encoded. The type-I fusion can now be attempted once more on the redundantly encoded qubits. If the gate succeeds, we established a vertical link. If the gate fails, we end up with two disconnected chains that are both two qubits shorter. Given sufficiently long linear cluster chains, we can repeat this protocol until we have succeeded in creating a vertical link. A proof-of-principle experiment demonstrating optical cluster-state quantum computing with four photons was performed in Vienna (Walther *et al.*, 2005).

Apart from constructing optimal two-qubit entangling gates, the classical strategies for creating cluster states can also be optimized. Kieling, Gross, and Eisert (2006) identified two possible global strategies called modesty and greed. Modesty denotes the rule that we always attempt a (type-I) fusion gate on the smallest available pieces of cluster state, while greed denotes the rule that we always attempt to fuse the largest available pieces. For a globally optimal strategy, the size Q of the cluster created with N Bell pairs is bounded by

$$Q(N) \leqslant \frac{N}{5} + 2. \tag{51}$$

It turns out that the modesty strategy is vastly superior to the greed strategy and is in fact close to the globally optimal strategy in Eq. (51).

E. Circuit-based optical quantum computing revisited

After all this, one might conclude that the cluster-state approach to linear optical quantum information processing has completely replaced the circuit-based model. However, such a conclusion would be premature. In fact, in a slightly altered form, the redundancy that we encountered in the Browne-Rudolph protocol can be used to make a scalable circuit-based optical quantum computer (Hayes *et al.*, 2004; Gilchrist *et al.*, 2005). We will now show how this is done.

We can encode a logical qubit in n physical qubits using the parity encoding we encountered earlier in Sec. II.H:

$$\begin{aligned} |0\rangle^{(n)} &\equiv \frac{1}{\sqrt{2}}(|+\rangle^{\otimes n} + |-\rangle^{\otimes n}), \\ |1\rangle^{(n)} &\equiv \frac{1}{\sqrt{2}}(|+\rangle^{\otimes n} - |-\rangle^{\otimes n}), \end{aligned} \tag{52}$$

where $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$. The superscript (n) denotes the level of encoding. This encoding has the attractive property that a computational-basis measurement of one of the physical qubits comprising the logical qubit $|\psi\rangle^{(n)}$ will yield $|\psi\rangle^{(n-1)}$, up to a local unitary on a single (arbitrary) physical qubit. In other words, no quantum information has been lost (Gilchrist *et al.*, 2005).

One way to generate this encoding is to use the type-II fusion operator without the two polarization

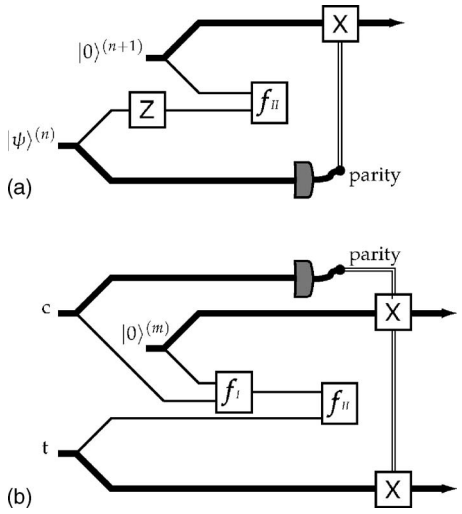

FIG. 32. The two probabilistic gates that complete a universal set. (a) The $Z_{\pi/2}$ gate uses a deterministic single-photon rotation and a single type-II fusion gate. (b) The CNOT gate uses one type-I and one type-II fusion gate. Both gates also need a parity measurement, which is implemented by σ_z measurements on the individual physical qubits.

rotations (half-wave plates) in the input ports of the polarizing beam splitter. This yields

$$f_{\mathrm{II}}|\psi\rangle^{(n)}|0\rangle^{(m)} \rightarrow \begin{cases} |\psi\rangle^{(n+m-2)} & \text{(success)} \\ |\psi\rangle^{(n-1)}|0\rangle^{(m-1)} & \text{(failure)}, \end{cases} \tag{53}$$

with $|\psi\rangle^{(n)} \equiv \alpha|0\rangle^{(n)} + \beta|1\rangle^{(n)}$. From this we can immediately deduce that, given a success probability p, the growth requirement for the redundancy encoding is $m > (1+p)/p$. This is exactly the same scaling behavior as the Browne-Rudolph protocol when clusters are grown with the type-II fusion gate.

In order to build circuits that are universal for quantum computing, we need a set of single-qubit operations and at least one two-qubit entangling gate at the level of the parity-encoded quits. As we have seen in Sec. II.H, we can perform the operations X_θ and Z deterministically: The operator $X_\theta \equiv \cos(\theta/2)\mathbb{1} + i\sin(\theta/2)\sigma_x$ can be implemented by applying this single-qubit operator to only one physical qubit of the encoding. The Z gate for an encoded qubit corresponds to a σ_z operation on all the physical qubits.

To complete the universal set of gates, we also need the single-qubit gate $Z_{\pi/2}$ and the CNOT. These gates cannot be implemented deterministically on parity-encoded qubits. In Fig. 32 we show how to implement these gates using the fusion operators. The thickness of the lines denotes the level of encoding. In addition to the fusion operators, we need to perform a parity measurement on one of the qubits by measuring σ_z on all the physical qubits in a circuit line. Since this measurement is performed on a subset of the physical qubits comprising a logical qubit, no quantum information is lost in this procedure. It should also be noted that we attempt the probabilistic fusion gates before the destructive parity measurement, so that in the case of a failed fusion operation we still have sufficient redundancy to try the fusion again. It has been estimated that universal gate operations can be implemented with greater than 99% probability of success with about 10^2 operations (Gilchrist *et al.*, 2005).

This circuit-based protocol for linear optical quantum computation has many features in common with the Browne-Rudolph protocol. Although the cluster-state model is conceptually different from the circuit-based model, they have similar resource requirements. The reader might also be wondering whether these schemes are tolerant to photon loss and other practical noise. The errors that we discussed so far originate from the probabilistic nature of linear optical photon manipulation, but can we also correct errors that arise from, e.g., detection inefficiencies? We will discuss the realistic errors of linear optical component in the next section and the possible fault tolerance of LOQC in the presence of these errors in Sec. V.

IV. REALISTIC OPTICAL COMPONENTS AND THEIR ERRORS

In order to build a real quantum computer based on linear optics, single-photon sources, and photon detection, our design must be able to deal with errors: The unavoidable errors in practical implementations should not erase the quantum information that is present in the computation. We have already seen that the teleportation trick in the KLM scheme employs error correction to turn the nondeterministic gates into near-deterministic gates. However, this assumes that the photon sources, the mode matching of the optical circuits, and the photon counting are all perfect. In the real world, this is far from true.

What are the types of errors that can occur in the different stages of the quantum computation? We can group them according to the optical components: detection errors, source errors, and circuit errors (Takeuchi, 2000a). In this section we will address these errors. In addition, we will address an assumption that has received little attention thus far: the need for quantum memories.

A. Photon detectors

In linear quantum optics, the main method for gaining information about quantum states is via photon detection. Theoretically, we can make a distinction between at least two types of detectors: ones that tell us exactly how many photons there are in an input state and ones that give a binary output "nothing" or "many." There are many more possible distinctions between detectors, but these two are the most important. The first type is called a number-resolving detector or a detector with single-photon resolution, while the second type is often called a bucket or vacuum detector. The original KLM proposal relies critically on the availability of number-

resolving detectors. On the other hand, typical photon detectors in LOQC experiments are bucket detectors. In recent years there has been a great effort to bridge the gap between the requirements of LOQC and available photon detectors, leading to the development of number-resolving detectors and LOQC protocols that rely less on high-photon-number counting. In this section, we state the common errors that arise in realistic photon detection and review some of the progress in the development of number-resolving detectors.

Real photon detectors of any kind can give rise to two different types of errors.

(i) The detector counts fewer photons than were actually present in the input state. This is commonly known as photon loss.

(ii) The detector counts more photons than were actually present in the input state. These are commonly known as dark counts.

Observe that it is problematic to talk about the number of photons "that were actually present" in the input state: When the input state is a superposition of different photon number states, the photon number in the state prior to detection is ill defined. However, we can give a general meaning to the concepts of photon loss and dark counts for arbitrary input states when we define the loss or dark counts as a property of the detector (i.e., independent of the input state). The detector efficiency $\eta \in [0,1]$ can be defined operationally as the probability that a single-photon input state will result in a detector count, while dark counts can be defined as the probability that a vacuum input state will result in a detector count.[4] Subsequently, these definitions can be modified to take into account non-Poissonian errors.

Whereas perfect number-resolving detectors can be modeled using projection operators onto the Fock states $|n\rangle\langle n|$, realistic detectors give rise to POVM's. A standard photon loss model is to have a perfect detector be preceded by a beam splitter with transmission coefficient η and reflection coefficient $1-\eta$. The reflected mode is considered lost (mathematically, this mode is traced over), so only a fraction η of the input reaches the detector. In this model, every incoming photon has the same probability of being lost, leading to Poissonian statistics. The POVM for a number-resolving photon detector corresponding to this model is (Scully and Lamb, 1969)

$$\hat{E}_n = \sum_{k=n}^{\infty} \binom{k}{n} \eta^n (1-\eta)^{k-n} |k\rangle\langle k|. \tag{54}$$

Using the same loss model, the POVM describing the effect of a bucket detector is (Kok and Braunstein, 2000b)

$$\hat{E}_0 = \sum_{n=0}^{\infty} (1-\eta)^n |n\rangle\langle n|,$$
$$\hat{E}_1 = \sum_{n=0}^{\infty} [1-(1-\eta)^n] |n\rangle\langle n|, \tag{55}$$

where 1 and 0 denote a detector click and no detector click, respectively. For an analysis including dark counts, see Lee, Yurtsever, *et al.* (2004).

Currently, the most common detectors in experiments on LOQC are avalanche photodiodes (APD's). When a photon hits the active semiconductor region of an APD, it will induce the emission of an electron into the conductance band. This electron is subsequently accelerated in an electric potential, causing an avalanche of secondary electrons. The resulting current tells us that a photon was detected. The avalanche must be stopped by reversing the potential, which leads to a dead time of a few nanoseconds in the detector. Any subsequent photon in the input mode can therefore not be detected, and this means that we have a bucket detector. A typical (unfiltered) detector efficiency for such a detector is 85% at a wavelength of 660 nm. Dark counts can be made as low as 6×10^3 Hz at room temperature and around 25 Hz at cryogenic temperatures.

Several attempts have been made to create a number-resolving detector using only bucket detectors and linear optics, but no amount of linear optics and bucket detection can lead to perfect, albeit inefficient, single-photon resolution (Kok, 2003). On the other hand, we can create approximate number-resolving detectors using only bucket detectors via detector cascading. In this setup, the incoming optical mode is distributed equally over N output modes, followed by bucket detection. When the number of modes in the cascade is large compared to the average photon number in the input state and the detector efficiencies of the bucket detectors are relatively high, then good fidelities for the photon number measurement can be obtained (Kok and Braunstein, 2001; Rohde, 2005). Detector cascading in the time domain using increasingly long fiber delays is called time multiplexing (Achilles *et al.*, 2003; Banaszek and Walmsley, 2003; Fitch *et al.*, 2003). However, the fiber length (and hence the detection time) must increase exponentially for this technique to work. Nemoto and Braunstein (2002) considered homodyne detection as a way to improve the efficiency of communication near the single-photon level, i.e., by simulating direct detection via homodyne detection. They found that the simulated direct detection strategy could provide limited improvement in the classical information transfer. Branczyk *et al.* (2003) proposed a photon number detector which uses an n-photon auxiliary Fock state and high-efficiency homodyne detection. The detector is nondeterministic, but, when successful, it has high fidelity. By sacrificing probability of operation, an excellent approximation to a photon number detector is achieved. When an (imperfect) quantum copier is available, extra information can

[4] In addition to this type of dark count, the detector can give a signal that is too large due to amplification noise. This is a multiplicative effect, rather than the additive effect we typically associate with dark counts, and it degrades the photon resolution of the detector.

be extracted from the qubits (Deuar and Munro, 2000a, 2000b).

Fully fledged number-resolving photon detectors are also being developed, such as the visible light photon counter (VLPC) (Kim *et al.*, 1999; Takeuchi *et al.*, 1999). An excellent recent introduction to this technology has been given by Waks *et al.* (2003). The VLPC's operate at a temperature of a few kelvin in order to minimize dark counts. They consist of an active area that is divided into many separate active regions. When a photon triggers such a region, it is detected while leaving the other regions fully operational. Once a region has detected a photon, it experiences a dead time in which no photon detection can take place. Multiple photon detections in different regions then generate a current that is proportional to the number of photons. The VLPC is thus effectively a large detector cascade ($N \approx 10^4$) with high detection efficiency (≈88% at 694 nm). The dark count rate of 2×10^4 Hz is about an order of magnitude higher than the dark count rate for off-the-shelf APD's.

An alternative technique uses a superconducting transition-edge sensor that acts as a calorimeter. It measures the rise in temperature of an absorber, which is quickly heated by incoming photons in the visible and near infrared range (Rosenberg *et al.*, 2005). This device operates at temperatures well below 100 mK and has a measured detection efficiency greater than 88%. The dark counts are negligible, but the repetition rate is rather slow (of the order of 10 kHz) due to the cooling mechanism after a photon has been detected. In addition to these experimental schemes, there are theoretical proposals for number-resolving detectors involving atomic vapors (James and Kwiat, 2002), electromagnetically induced transparency (Imamoğlu, 2002), and resonant nonlinear optics (Johnsson and Fleischhauer, 2003).

Finally, we briefly mention quantum nondemolition (QND) measurements. In the photon detectors that we described so far, the state of the electromagnetic field is invariably destroyed by the detector. However, in a QND measurement there is a freely propagating field mode after the measurement. In particular, the outcome of the QND measurement faithfully represents the state of the field after detection (Grangier *et al.*, 1998). Several schemes for single-photon QND measurements have been proposed, with either linear optics (Howell and Yeazell, 2000a; Kok *et al.*, 2002), optical quantum relays (Jacobs *et al.*, 2002), or other implementations (Brune *et al.*, 1990, 1992; Roch *et al.*, 1997; Munro, Nemoto, *et al.*, 2005). The experimental demonstration of a single-photon QND was reported by Nogues *et al.* (1999) using a cavity QED system, and a linear-optical (nondeterministic) QND measurement was performed by Pryde *et al.* (2004). However, this last experiment has led to a controversy about the nature of the fidelity measure that was used [see Kok and Munro (2005) and Pryde *et al.* (2005)].

So far, we have considered only photon number detection. However, in many implementations of LOQC the qubit is encoded in a single polarized photon. A qubit detector must therefore extract the polarization of the photon, which may have had unwanted interactions with the environment. A change in the polarization of the photon will then induce an error in the computational circuit.

One mechanism that leads to errors in polarization is inherent in any photon detector[5] and deserves a special mention here. In the Coulomb gauge, polarization is perpendicular to the direction of propagation and the plane of detection must therefore be perpendicular to the Poynting vector $\vec{k}$. A complication arises when we consider beams that are not perfectly collimated. We can write the $\vec{k}$ vector of the beam as

$$\vec{k}(\theta,\phi) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta). \tag{56}$$

A realistic, reasonably well-collimated beam will have a narrow distribution of θ and ϕ around θ_0 and ϕ_0. If we model the active area of a detector as a flat surface perpendicular to $\vec{k}(\theta_0,\phi_0)$, some modes in the beam will hit the detector at an angle. Fixing the gauge of the field in the detection plane then causes a mixing of left- and right-handed polarization. This introduces a detection error that is fundamental, since the uncertainty principle prevents the transverse momentum in a beam from being exactly zero (Peres and Terno, 2003). At first sight this effect might seem negligible, but later we will see that concatenation of error-correcting codes will amplify small errors. It is therefore important to identify all possible sources of errors.

B. Photon sources

The LOQC protocols described in this review all make critical use of perfect single-photon sources. In this section we wish to make more precise what is meant by a single-photon source. We have thus far considered interferometric properties of monochromatic plane waves with exactly one field excitation. Such states, while a useful heuristic, are not physical. Our first objective is to give a general description of a single-photon state followed by a description of current experimental realizations [see also Titulaer and Glauber (1966)].

The notion of a single photon conjures up an image of a single-particle-like object localized in space and time. However, it was conclusively demonstrated long ago by Newton and Wigner (1949), and also by Wightman (1962), that a single photon cannot be localized in the same sense that a single massive particle can. Here we are concerned only with temporal localization, which is ultimately due to the fact that the energy spectrum of the field is bounded from below. In this section we take a simpler operational view. A photon refers to a single detection event in a counting time window T. A single-photon source leads to a periodic sequence of single detection events with one, and only one, photon detected in each counting window. Further refinement of this

[5]It can equally well be argued that this is an imperfection of photon sources. This is a matter of convention.

definition, via the output counting statistics of interferometers, is needed to specify the kind of single-photon sources necessary for LOQC.

Consider a one-dimensional cavity of length L. The allowed wave vectors for plane-wave modes form a denumerable set given by $k_n = n\pi/L$, with corresponding frequencies $\omega_n = ck_n$. If we measure time in units of $\pi L/c$, the allowed frequencies may simply be denoted by an integer $\omega_n = n \in \mathbb{N}$. Similarly, if we measure length in units of π/L, the allowed wave vectors are also integers. We are primarily interested in multimode fields with an optical carrier frequency, $\Omega \gg 1$. We define the positive-frequency field component as

$$\hat{a}(t) = \sum_{n=1}^{\infty} \hat{a}_n e^{-int}. \tag{57}$$

The bosonic annihilation and creation operators are given by Eq. (2). From this point on we assume the detector is located at $x=0$ and thus evaluate all fields at the spatial origin. Following the standard theory of photodetection, the probability per unit time for detecting a single photon is given by

$$p_1(t) = \eta n(t), \tag{58}$$

where

$$n(t) = \langle \hat{a}^\dagger(t)\hat{a}(t) \rangle \tag{59}$$

and the parameter η characterizes the detector.

A single-photon state may be defined as

$$|1;f\rangle = \sum_{m=1}^{\infty} f_m \hat{a}_m^\dagger |0\rangle, \tag{60}$$

where $|0\rangle = \Pi_m |0\rangle_m$ is the multimode global vacuum state and we require that the single-photon amplitude f_m satisfies

$$\sum_{m=0}^{\infty} |f_m|^2 = 1. \tag{61}$$

The counting probability is then determined by

$$n(t) = \left| \sum_{k=1}^{\infty} f_k e^{-ikt} \right|^2. \tag{62}$$

This function is clearly periodic with a period 2π. As the spectrum is bounded from below by $n=1$, it is not possible to choose the amplitudes f_n so that the functions $n(t)$ have arbitrarily narrow support on $t \in [0, 2\pi)$.

As an example we take

$$f_m^N = \frac{1}{\sqrt{1-(1-\mu)^N}} \binom{N}{m}^{1/2} \mu^{m/2} (1-\mu)^{(N-m)/2}, \tag{63}$$

where we have introduced a cutoff frequency N, making infinite sums finite, and $0 \leqslant \mu \leqslant 0.5$. For $N \gg 1$ the normalization is very close to unity, so we will drop it in the following. The dominant frequency in this distribution is $\Omega = \mu N$, which we call the carrier frequency. In this case,

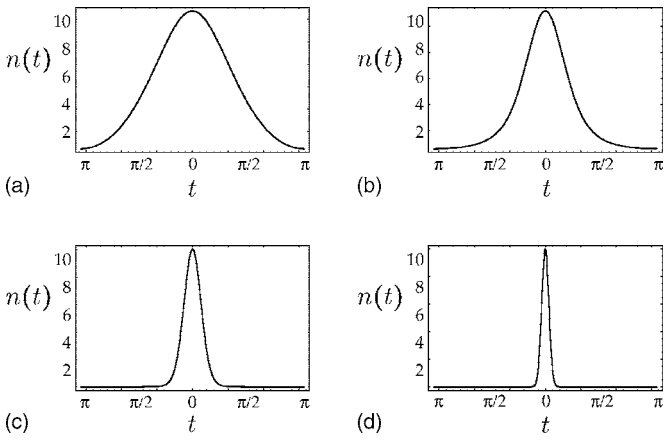

FIG. 33. The function $n(t)$ in arbitrary units in the domain $-\pi \leqslant t \leqslant \pi$ for different values of μ and $N=100$: (a) $\mu=0.001$, (b) $\mu=0.01$, (c) $\mu=0.05$, and (d) $\mu=0.49$.

$$n(t) = \left| \sum_{k=1}^{N} e^{-ikt} \binom{N}{k}^{1/2} \mu^{k/2} (1-\mu)^{(N-k)/2} \right|^2. \tag{64}$$

This function is shown in Fig. 33 for various values of μ. The probability per unit time is thus a periodic function of time, with period 2π and pulse width determined by μ when N is fixed. If we fix the carrier frequency $\Omega = \mu N$ and let N become large, we must let μ become small. In the limit $N \to \infty$, $\mu \to 0$ with Ω fixed we obtain a Poisson distribution for the single-photon amplitude.

A second example is the Lorentzian

$$f_n^N = \frac{1}{A} \frac{\sqrt{\mu}}{\mu + in}. \tag{65}$$

In the limit $N \to \infty$, the normalization constant is

$$A = \frac{\pi e^{\mu\pi}}{2\sinh(\mu\pi)} - \frac{1}{2\mu}. \tag{66}$$

While a field for which exactly one photon is counted in one counting interval, and zero in all others, is no doubt possible, it does not correspond to the more physical situation in which a source is periodically producing pulses with exactly one photon per pulse. To define such a field state we now introduce time-bin operators. For simplicity we assume that only field modes $n \leqslant N$ are excited and all others are in the vacuum state. It would be more physical to assume that only field modes are excited in some band, $\Omega - B \leqslant n \leqslant \Omega + B$. Here Ω is the carrier frequency and $2B$ is the bandwidth. However, this adds very little to the discussion.

Define the operators

$$\hat{b}_\nu = \frac{1}{\sqrt{N}} \sum_{m=1}^{N} e^{-i\tau m\nu} \hat{a}_m, \tag{67}$$

where $\tau = 2\pi/N$. This can be inverted to give

$$\hat{a}_m = \frac{1}{\sqrt{N}} \sum_{\nu=1}^{N} e^{i\tau m \nu} \hat{b}_\nu. \tag{68}$$

The temporal evolution of the positive-frequency components of the field modes then follows from Eq. (57):

$$\hat{a}(t) = \sum_{\mu=1}^{N} g_\mu(t) \hat{b}_\mu, \tag{69}$$

where

$$g_\mu(t) = \frac{1}{\sqrt{N}} [1 - e^{i(\mu\tau - t)}]^{-1}. \tag{70}$$

The time-bin expansion functions $g_\mu(t)$ are a function of $\mu\tau - t$ alone and thus are simple translations of the functions at $t=0$. The form of Eq. (69) is a special case of a more sophisticated way to define time-bin modes. If we were to regard $\hat{a}(t)$ as a classical signal, then the decomposition in Eq. (69) could be generalized as a wavelet transform where the integer μ labels the translation index for wavelet functions. In that case the functions $g_\mu(t)$ could be made rather less singular. In an experimental context, however, the form of the functions $g_\mu(t)$ depends upon the details of the generation process.

The linear relationship between the plane-wave modes a_m and time-bin modes b_ν is realized by a unitary transformation that does not change particle number, so the vacuum state for the time-bin modes is the same as the vacuum state for the global plane wave modes. We can then define a one-photon time-bin state as

$$|1\rangle_\mu = \hat{b}_\mu^\dagger |0\rangle. \tag{71}$$

The mean photon number for this state is

$$n(t) = |g_\mu(t)|^2. \tag{72}$$

This function is periodic with period 2π and corresponds to a pulse localized in time at $t=\mu\tau$. Thus the integer μ labels the temporal coordinate of the single-photon pulse.

We are now in a position to define an N-photon state with one photon per pulse. In addition to the mean photon number $n(t)$ we can now compute two-time correlation functions such as the second-order correlation function $G^{(2)}(\tau)$, defined by

$$G^{(2)}(T) = \langle \hat{a}^\dagger(t) \hat{a}^\dagger(t+T) \hat{a}(t+T) \hat{a}(t) \rangle. \tag{73}$$

The simplest example for $N=2$ is

$$|1_\mu, 1_\nu\rangle = \hat{b}_\mu^\dagger \hat{b}_\nu^\dagger |0\rangle, \quad \mu \neq \nu. \tag{74}$$

The corresponding mean photon number is

$$n(t) = |g_\mu(t)|^2 + |g_\nu(t)|^2, \tag{75}$$

as would be expected. The two-time correlation function is

$$G^{(2)}(T) = |g_\mu(t) g_\nu(t+T) + g_\nu(t) g_\mu(t+T)|^2. \tag{76}$$

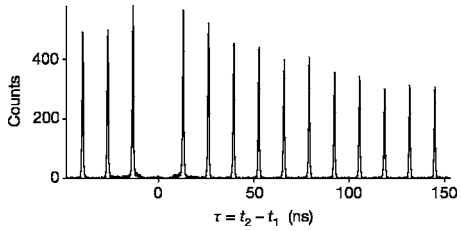

FIG. 34. The $G^{(2)}(\tau)$ for the InAs quantum dot single-photon source. Note that the variable T in the text is here replaced with τ. From Santori *et al.*, 2002b.

Clearly this has a zero at $T=0$, reflecting the fact that the probability of detecting a single photon immediately after a single-photon detection is zero, as the two pulses are separated in time by $|\mu - \nu|$. This is known as antibunching and is the first essential diagnostic for a sequence of single-photon pulses with one and only one photon per pulse. When $T=|\mu-\nu|\tau$, however, there is a peak in the two-time correlation function as expected. In Fig. 34 we have reproduced the experimental results for $G^{(2)}(T)$ from Santori *et al.* (2002b).

We now reconsider the Hong-Ou-Mandel interferometer introduced in Sec. II.A with single-photon input states. This example has been considered by Rohde and Ralph (2005). We label the two sets of modes by the Latin symbols a and b, so, for example, the positive-frequency parts of each field are simply $a(t)$ and $b(t)$. The coupling between the modes is described by a beam-splitter matrix connecting the input and output plane waves:

$$\hat{a}_n^{\text{out}} = \sqrt{v}\, \hat{a}_n + \sqrt{1-v}\, \hat{b}_n, \tag{77}$$

$$\hat{b}_n^{\text{out}} = \sqrt{v}\, \hat{b}_n - \sqrt{1-v}\, \hat{a}_n, \tag{78}$$

where $0 \leqslant v \leqslant 1$. The probability per unit time to find a coincidence detection of a single photon at each output beam is proportional to

$$C = \overline{\langle \hat{a}^\dagger(t) \hat{b}^\dagger(t) \hat{b}(t) \hat{a}(t) \rangle}. \tag{79}$$

The overbar represents a time average over a detector response time that is long compared to the period of the field carrier frequencies. In this example, we need only consider the case of one photon in each of the two distinguished modes, so we take the input state to be

$$|1\rangle_a \otimes |1\rangle_b = \sum_{m,n=1}^{\infty} \alpha_n \beta_m \hat{a}_n^\dagger \hat{b}_m^\dagger |0\rangle, \tag{80}$$

where α_n and β_n refer to the excitation probability amplitudes for modes a_n and b_n, respectively. This state is transformed by the unitary transformation U to give $|\psi\rangle_{\text{out}} = U(|1\rangle_a \otimes |1\rangle_b)$. In the case of a 50:50 beam splitter, for which $v=0.5$, this is given as $(U|0\rangle = |0\rangle)$

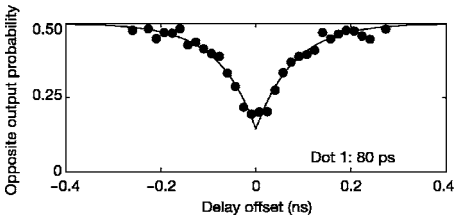

FIG. 35. The Hong-Ou-Mandel effect for the InAs quantum dot single-photon source. From Santori *et al.*, 2002b.

$$
\begin{aligned}
|\psi\rangle_{\text{out}} &= \sum_{n,m=1}^{\infty} \alpha_n \beta_m (U a_n^\dagger b_m^\dagger U^\dagger) U|0\rangle \\
&= \frac{1}{2} \sum_{n,m=1}^{\infty} \alpha_n \beta_m (a_n^\dagger + b_n^\dagger)(b_m^\dagger - a_m^\dagger)|0\rangle \\
&= \frac{1}{2} \sum_{n,m=1}^{\infty} \alpha_n \beta_m [|1\rangle_{a_n}|1\rangle_{b_m} - |1\rangle_{a_n}|1\rangle_{a_m}|0\rangle_b \\
&\quad + |1\rangle_{b_n}|1\rangle_{b_m}|0\rangle_a - |1\rangle_{b_n}|1\rangle_{a_m}].
\end{aligned}
$$

Note that the second and third terms in this sum have no photons in modes b and a, respectively. We then have that

$$
C = \frac{1}{2} - \frac{1}{2} \sum_{n,m=1}^{\infty} \alpha_n \alpha_m^* \beta_m \beta_n^*. \tag{81}
$$

If the excitation probability amplitudes at each frequency are identical $\alpha_n = \beta_n$, this quantity is zero. In other words, only if the two-single photon wave packets are identical do we see a complete cancellation of the coincidence probability. This is the second essential diagnostic for a single-photon source. Of course, in practice, complete cancellation is unlikely. The extent to which the coincidence rate approaches zero is a measure of the quality of a single-photon source as far as LOQC is concerned. Whether or not this is the case depends on the nature of the single-photon sources. In Fig. 35 we have reproduced the experimental results for the Hong-Ou-Mandel effect, shown with one of the InAs quantum dot single-photon sources of Santori *et al.* (2002b).

Broadly speaking, there are currently two main schemes used to realize single-photon sources: (I) conditional spontaneous parametric down-conversion and (II) cavity-QED Raman schemes. As discussed by Rohde and Ralph (2005), type I corresponds to a Gaussian distribution of α_n as a function of n and thus is the continuum analog of the binomial state defined by Eq. (63). The second scheme, type II, leads to a temporal pulse structure that is the convolution of the excitation pulse shape and the Lorentzian line shape of a cavity. If the cavity decay time is the longest time in the dynamics, the distribution α_n takes the Lorentzian form given by Eq. (65). An early single-photon source based on an optical emitter in a microcavity was proposed and demonstrated by De Martini *et al.* (1996).

Cavity-based single-photon sources are very complicated experiments in their own right, and instead most single-photon sources used in LOQC experiments are based on parametric down-conversion (PDC). In PDC a short-wavelength pump laser generates photon pairs of longer wavelength in a birefringent crystal. PDC can yield extremely high fidelities ($F > 0.99$) because the data are usually obtained via postselection: we take only those events into account that yield the right number of detector coincidents. In addition, PDC facilitates good mode matching due to energy and momentum conservation in the down-conversion process. The output of a noncollinear type-I PDC can be written as

$$
|\Psi_{\text{PDC}}\rangle = \sqrt{1 - |\lambda|^2} \sum_{n=0}^{\infty} \lambda^n |n,n\rangle, \tag{82}
$$

where $|n\rangle$ is the n-photon Fock state and λ is a measure for the amount of down-conversion. The probability for creating n photon pairs is $p(n) = (1 - |\lambda|^2)|\lambda|^{2n}$, which exhibits pair bunching. When λ is small, we can make a probabilistic single-photon gun by detecting one of the two modes. However, if we use only bucket detectors without single-photon resolution, then increasing λ will also increase the amplitudes for a two-photon pair and ultimately high-photon pairs in the output state. Consequently, the single-photon source will deteriorate badly. A detailed study of the mode structure of the conditional photon pulse has been undertaken by Grice *et al.* (2001).

Another consideration regarding parametric down-conversion is that photons in a pair are typically highly entangled in frequency and momentum. When we use a bucket detector that is sensitive over a broad frequency range to herald a single photon in the freely propagating mode, the lack of frequency information in the detector readout will cause the single-photon state to be mixed. In principle, this can be remedied by embedding the down-converting material in a microcavity such that only certain frequencies are allowed (Raymer *et al.*, 2005). The source will then generate photon pairs with frequencies that match the cavity, and a narrow-band bucket detector can herald a pure single-photon state with a small frequency linewidth.

Alternatively, we can use the following method of making single-photon sources (Migdall *et al.*, 2002; Pittman *et al.*, 2002c). Consider an array of PDC's with one output mode incident on a photon detector and the other entering the quantum circuit. We fire all PDC's simultaneously. Furthermore, all PDC's have small λ, but if there are approximately $|\lambda|^{-2}$ of them we still create a single photon on average. Given that in current PDC configurations $|\lambda|^2 \approx 10^{-4}$, this is quite an inefficient process. Nevertheless, since it contributes a fixed overhead per single photon to the computational resources, this technique is strictly speaking scalable. For a detailed description of parametric down-conversion as a photon source, see U'Ren *et al.* (2003).

To illustrate the experimental constraints on the generation of single-photon states, we now review an example of a cavity-QED Raman scheme implemented by Keller *et al.* (2004). Photon antibunching from resonance

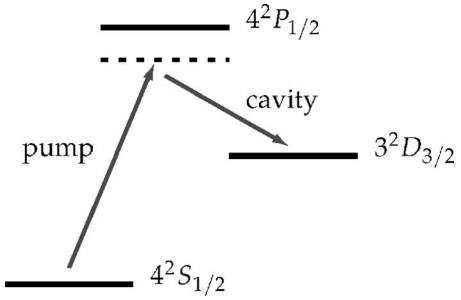

FIG. 36. The Raman process in a three-level atom. A classical pump field drives the transition $4\,^2S_{1/2} \rightarrow 4\,^2P_{1/2}$ off-resonantly, thus generating a photon in the cavity mode. The level $4\,^2P_{1/2}$ is adiabatically eliminated and hence never populated.

fluorescence was demonstrated long ago. If an atom decays spontaneously from an excited state to the ground state, a single photon is emitted, and a second photon cannot be emitted until the atom is reexcited. Unfortunately the photon is emitted into a dipole radiation pattern over a complete solid angle. Clearly we need to engineer the electromagnetic environment with mirrors, dielectrics, etc., to ensure a preferred mode for emission. However, as pointed out by Kiraz *et al.* (2004), this comes at a price. For example, a carefully engineered cavity around a single dipole emitter can change the free-field spectral density around the emitter such that a photon is indeed emitted in a preferred direction with an increased rate compared to free-space emission.

However, single-photon sources based on spontaneous emission are necessarily compromised by the random nature of spontaneous emission. As demonstrated by Rohde, Ralph, and Nielsen (2005), single-photon sources that create Gaussian wave packets are much more robust to mode mismatching than sources that create Lorentzian wave packets. Spontaneous emission processes fall in this last category. Clearly, we prefer a stimulated emission process yielding a Gaussian wave packet. To this end, a number of schemes based on stimulated Raman emission into a cavity mode have been proposed (Hennrich *et al.*, 2004; Maurer *et al.*, 2004). As an example, we discuss the experiment by Keller *et al.* (2004) in some detail.

Consider the three-level atomic system in Fig. 36. The ground state is coupled to the excited state via a two-photon Raman process mediated by a well-detuned third level. In the experiment by Keller *et al.* (2004), a calcium ion $^{40}Ca^+$ was trapped in a cavity via a rf ion trap. The cavity field is nearly resonant with the $4\,^2P_{1/2} \rightarrow 3\,^2D_{3/2}$ transition. Initially there is no photon in the cavity. An external laser is directed onto the ion and is nearly resonant with the $4\,^2S_{1/2} \rightarrow 4\,^2P_{1/2}$ transition. When this laser is switched on, the atom can be excited to the $3\,^2D_{3/2}$ level by absorbing one pump photon and emitting one photon in to the cavity. Since this is a stimulated Raman process, the time of emission of the photon into the cavity is completely controlled by the temporal structure of the pump pulse. The photon in the cavity then decays through the end mirror, again as a Poisson process, at a rate given by the cavity decay rate. This can be made very fast.

In principle one can now calculate the probability per unit time to detect a single photon emitted from the cavity. If we assume that every photon emitted is detected, this probability is simply $p_1(t) = \kappa\langle\hat{a}^\dagger(t)\hat{a}(t)\rangle$, where κ is the cavity decay rate, $\hat{a}$ and $\hat{a}^\dagger$ are the annihilation and creation operators for the intracavity field, and

$$\langle\hat{a}^\dagger(t)\hat{a}(t)\rangle = \mathrm{tr}[\rho(t)\hat{a}^\dagger\hat{a}], \tag{83}$$

with $\rho(t)$ the total density operator for the ion-plus-cavity-field system. This may be obtained by solving a master equation describing the interaction of electronic states of the ion and two fields, one of which is the time-dependent pump. Of course, for a general time-dependent pump pulse shape this can only be done numerically. Some typical examples are quoted by Keller *et al.* Indeed by carefully controlling the pump pulse shape considerable control over the temporal structure of the single-photon detection probability may be achieved. In the experiment the length of the pump pulse was controlled to optimize the single-photon output rate. The efficiency of emission was found to be about 8%, that is to say, 92% of the pump pulses did not lead to a single-photon detection event. This was in accordance with theoretical simulations. These photons are probably lost through the sides of the cavity. It is important to note that this kind of loss does not affect the temporal mode structure of the emitted (and detected) photons.

In a similar way we can compute the second-order correlation function via

$$G^{(2)}(T) = \kappa^2\mathrm{tr}\{\hat{a}^\dagger\hat{a}e^{\mathcal{L}T}[\hat{a}\rho(t)\hat{a}^\dagger]\}, \tag{84}$$

where $e^{\mathcal{L}T}$ is a formal specification of the solution to the master equation for a time T after the "initial" conditional state $a\rho(t)a^\dagger$. Once again, due to the nonstationary nature of the problem, this must be computed numerically. However, if the pump pulse duration is very short compared to the cavity decay time and the cavity decay time is the fastest decay constant in the system, the probability amplitude to excite a single photon in a cavity at frequency ω is very close to Lorentzian. The experiment revealed a clear suppression of the peak at $T=0$ in the normalized correlation function $g^{(2)}(T)$, thus passing the first test of a good single-photon source. Unfortunately, a Hong-Ou-Mandel interference experiment was not reported.

For a practical linear optical quantum computer, however, we need good microscopic single-photon sources that can be produced in large numbers. A recent review on this topic by Lounis and Orrit (2005) identifies six types of microscopic sources: (i) atoms and ions in the gaseous phase;[6] (ii) organic molecules at low temperature and room temperature;[7] (iii) chromophoric

[6] Kuhn *et al.*, 2002 and McKeefer *et al.*, 2004.

[7] Brunel *et al.*, 1999, Lounis and Moerner, 2000, Treussart *et al.*, 2002, and Hollars *et al.*, 2003.

systems;[8] (iv) color centers in diamond, such as nitrogen vacancy[9] or nickel nitrogen;[10] (v) semiconductor nanocrystals;[11] and (vi) self-assembled quantum dots and other heterostructures such as micropillars and micromesa;[12] quantum dots;[13] and electrically driven dots.[14] The typical physical mechanisms that reduce the indistinguishability of single-photon sources are dephasing of the optical transition, spectral diffusion, and incoherent pumping. An earlier review on this topic has been given by Greulich and Thiel (2001). The subject of single-photon sources using quantum dots was reviewed by Santori *et al.* (2004).

When single-photon sources are less than ideal, linear optics might be employed in order to improve the output state. For example, if the source succeeds with probability p, then the output of the source might be $\rho = p|1\rangle\langle 1| + (1-p)|0\rangle\langle 0|$, where we assumed that the failure output results in a vacuum state. Using multiple copies of ρ, linear optics, and ideal photon detection, one may increase the probability up to $p=1/2$, but not higher (Berry *et al.*, 2005). A general discussion on improving single-photon sources with linear optical postprocessing has been given by Berry *et al.* (2004).

Not only must single-photon sources create clean single-photon states, in the sense described above, but all sources must also generate identical states in order to achieve good visibility in a Hong-Ou-Mandel test. Typical experiments demonstrating single-photon sources create subsequent single-photon states in the same source and employ a delay line to interfere the two photons. This way, two-photon quantum interference effects are demonstrated without having to rely on identical sources (Santori *et al.*, 2002b). de Riedmatten *et al.* demonstrated quantum interference by using identical pulse shapes triggering different photon sources (de Riedmatten *et al.*, 2003). In applications other than LOQC, such as cryptography, the requirement of indistinguishable sources may be relaxed. This leads to the concept of the suitability of a source for a particular application (Hockney *et al.*, 2003).

A variation on single-photon sources is the entangled-photon source. We define an ideal entangled-photon source as a source that creates a two-photon polarization Bell state. This is an important resource in both the Browne-Rudolph and Gilchrist-Hayes-Ralph protocols. It is known that these states cannot be created deterministically from single-photon sources, linear optics, and destructive photon detection (Kok and Braunstein, 2000a). Nevertheless, such states are very desirable, since they would dramatically reduce the cost of linear-optical quantum computing. The same error models for single-photon sources apply to entangled-photon sources. Again, a great variety of proposals for entangled-photon sources exist in the literature, using quantum dots (Benson *et al.*, 2000; Stace *et al.*, 2003) or parametric down-conversion (Śliwa and Banaszek, 2003). Two-photon states without entanglement have been created experimentally by Moreau *et al.* (2001), and Santori *et al.* (2002a), as have entangled-photon pairs (Kuzmich *et al.*, 2003; Yamamoto *et al.*, 2003).

C. Circuit errors and quantum memories

In addition to detector errors and errors in the single-photon sources, there is a possibility that the optical circuits themselves acquire errors. Probably the most important circuit error is mode mismatching. It occurs when nonidentical wave packets are used in an interferometric setup [e.g., the coefficients α_n and β_n in Eq. (81) are not identical]. There is a plethora of reasons why the coefficients α_n and β_n might not be equal. For example, the optical components might not do exactly what they are supposed to do. More precisely, the interaction Hamiltonian of the components will differ from its specifications. One manifestation of this is that there is a finite accuracy in the parameters in the interaction Hamiltonian of any optical component, leading to changes in phases, beam-splitter transmission coefficients, and polarization rotation angles. In addition, unwanted birefringence in the dielectric media can cause photoemission and squeezing. Inaccurate Hamiltonian parameters generally reduce the level of mode matching, leading, for example, to a reduced Hong-Ou-Mandel effect and hence inaccurate CZ gates. Indeed, mode matching is likely to be the main circuit error. Most of this effect is due to nonidentical photon sources, which we discussed in the previous section. The effect of frequency and temporal mode mismatching was studied by Rohde and Ralph (2005) and Rohde, Ralph, and Nielsen (2005).

A second error mechanism is that, typically, components such as beam splitters, half- and quarter-wave plates, etc., are made of dielectric media that have a (small) absorption amplitude. Scheel (2005) showed that there is a lower bound on the absorption amplitude in physical beam splitters. In addition, imperfect impedance matching of the boundaries will scatter photons back to the source. This amounts to photon loss in the optical circuit. In large circuits, these losses can become substantial.

A third error mechanism is due to classical errors in the feedforward process. This process consists of the readout of a photon detector, classical postprocessing, and conditional switching of the optical circuit. The detection errors have been discussed in Sec. IV.A and classical computing is virtually error free due to robust classical error correction. Optical switches, however, are still quite lossy (Thew *et al.*, 2002). In addition, when high-voltage Pockels cells are used, the repetition rate is slow

[8] Lee, Kumar, *et al.*, 2004.
[9] Kurtsiefer *et al.*, 2000, Beveratos *et al.*, 2002, and Jelezko *et al.*, 2002.
[10] Gaebel *et al.*, 2004.
[11] Lounis and Moerner, 2000, Michler *et al.*, 2000, and Messin *et al.*, 2001.
[12] Gérard *et al.*, 2002, Pelton *et al.*, 2002, Santori *et al.*, 2002b, and Vučković *et al.*, 2003.
[13] Hours *et al.*, 2003, Zwiller *et al.*, 2003, and Ward *et al.*, 2005.
[14] Yuan *et al.*, 2002.

(on the order of 10 kHz). This may become too slow, as photons need to be stored in a quantum memory (e.g., a delay loop), which itself may be lossy and needs feedforward processing. Feedforward control for LOQC was demonstrated by Giacomini *et al.* (2002) and Pittman *et al.* (2002a).

An important component of linear optical quantum computing that we have ignored so far is the quantum memory. When the probability of a successful (teleported) gate or addition to a cluster state becomes small, photons that are part of the circuit must be stored for a considerable time while the off-line preparation of entangled photons is taking place. The use of mere fiber loops then becomes problematic, as these induce photon losses (0.17 dB km^{-1} in a standard telecom fiber at 1550 nm). For example, storage of a photon for 100 μs in a fiber has a loss probability of $p \approx 0.54$. At present, all linear optical quantum computer proposals need some kind of quantum memory. This may be in the form of delay lines with error correction, atomic vapors, solid-state implementations, etc.

In general, the effect of a quantum memory error boils down to the inequality of the input state ρ_{in} and the (time-translated) output state ρ_{out}. A good figure of merit is the fidelity F_{qm}:

$$F_{qm} = [\mathrm{Tr}(\sqrt{\sqrt{\rho_{\text{in}}}\rho_{\text{out}}\sqrt{\rho_{\text{in}}}})]^2. \tag{85}$$

The absence of a photon in the output state is an obvious failure mechanism, but the memory can fail in other ways, include qubit decoherence and mode mismatching of the input/output modes. In this sense, the design specifications of a solid-state-based quantum memory are more stringent than those for solid-state single-photon sources: Not only does it need to produce a single photon with very high fidelity, it also needs the ability to couple a photon into the device with very high probability. Note that we do not have to couple a photonic qubit into a quantum memory: We can use two photon memories to store one qubit, provided the memory does not retain information about whether a photon was stored or not.

A proof of principle for a free-space delay line was given by Pittman and Franson (2002), and quantum memory delay lines using quantum error correction and QND measurements were proposed by Gingrich *et al.* (2003) and Ralph *et al.* (2005). A storage time of 125 μs for entangled photons in a telecom fiber was reported by Li *et al.* (2005), with subsequent fringe visibilities of 82%. Using the magnetic sublevels of the ground state of an atomic ensemble, Julsgaard *et al.* (2004) stored a weak coherent light pulse for up to 4 ms with a fidelity of 70%. The classical limit is 50%, showing that a true quantum memory was constructed. Other proposals include dark-state polaritons (Fleischhauer and Lukin, 2002), and single-photon cavity QED (Maître *et al.*, 1997).

V. GENERAL ERROR CORRECTION

To achieve quantum computing despite inevitable physical errors in the quantum computer, we have to employ error correction (EC). Typically, an error-correction protocol consists of a circuit that can correct for one or more types of error. However, these circuits will in turn introduce errors. For an EC protocol to be useful, the error in the circuit after the EC protocol must be smaller than the error before the EC protocol. Repeated nested application of the EC protocol (so-called concatenation) can then reduce the errors to arbitrarily small levels. In doing so, we must take care not to sacrifice the scaling behavior of the quantum computer. This is captured in the notion of fault tolerance. The magnitude of the errors for which fault tolerance breaks down is called the fault-tolerant threshold. For more details, see Nielsen and Chuang (2000).

General fault-tolerant thresholds for quantum computing have been derived by Steane (2003) and Knill (2005), and here we address LOQC specific error-correction and fault-tolerant thresholds. We have seen that the KLM scheme employs a certain level of error correction in order to turn high-probability teleported gates into near-deterministic gates, even though all-optical components are ideal. In this section, we discuss how an LOQC architecture can be developed with robustness against component errors.

Different error models will typically lead to different levels of robustness. For example, in the cluster-state approach of Browne and Rudolph, we can relax the condition of perfect photon counting given ideal photon sources. The type-II fusion operation described in Sec. III.D must give a coincidence count in the two detectors. Any other detector signature heralds an error. So if the photon detectors are lossy, the rate of coincidence counts is reduced. Since the fusion operation is already probabilistic, a reduced success rate translates into a larger overhead in the cluster-state generation. However, if the photon sources are not ideal and if there is a substantial number of dark counts in the detectors, then we rapidly lose quantum information. This raises two important questions: (i) Given a certain error model, what is the error-correcting capability for a given LOQC architecture? (ii) What is the realistic error model? This last question depends on the available photon sources, detectors, and memories, as well as the architecture of the optical quantum computer. Currently, theoretical research in LOQC is concentrating on these questions.

The three main errors that need to be coded against are inefficient detectors, noisy photon sources, and unfaithful quantum memories. There are other error mechanisms as well (see Sec. IV), and these will become important in concatenated error correction. In order to find the fault-tolerant level for a given architecture, these other errors must be taken into account. In the next section, we discuss how photon loss can be corrected in both the cluster-state model and the circuit-based model. In Sec. V.B we discuss fault-tolerant quantum computing in the cluster-state model.

A. Correcting for photon loss

We first consider photon loss. Its effect on the original teleportation component in the KLM protocol [Eq. (37)] was studied by Glancy *et al.* (2002), who found that in the KLM scheme a gate teleportation fidelity better than 99% requires detectors with an efficiency $\eta > 0.999\,987$. Using the seven-qubit CSS quantum code, the photon loss ϵ in the KLM scheme is allowed to be as large as $1.78\% \leqslant \epsilon \leqslant 11.5\%$, depending on the construction of the entangling gates (Silva *et al.*, 2005). Using type-I and type-II fusion gates in creating entanglement, the photon loss can be much higher: In the Browne-Rudolph protocol, a low detection efficiency merely reduces the rate with which the cluster state is created, whereas in the circuit-based model a low detection efficiency requires a higher level of encoding.

However, we need not only the ability to grow the cluster or the parity encoding efficiently, we also need to do the single-qubit measurements. Since in LOQC the single-qubit measurements amount to photon detection, we have a problem: Failing to measure a photon is also a single-qubit failure. Therefore, every logical qubit must be constructed with multiple photons, such that photon loss can be recovered from. In particular, this means that we can no longer straightforwardly remove redundant qubits in the cluster-state model if they are not properly encoded. In this section, we show how cluster states can be protected from photon loss by "planting trees" in the cluster (Varnava *et al.*, 2005), and we describe how an extra layer of encoding protects the circuit model of Ralph, Hayes, and Gilchrist (2005) from detection inefficiency, probabilistic sources, and memory loss.

Varnava, Browne, and Rudolph (2005) introduced a code exploiting the property that a cluster state is an eigenstate of every stabilizer generator and that the eigenvalue of each is known beforehand (we will assume that all eigenvalues are +1). This allows us to measure the value of a lost qubit as follows: Suppose we wish to measure a qubit in the computational basis; that is, we require a Z measurement. If that qubit is no longer present, we can choose $S_i = X_i \Pi_{j \in n(i)} Z_j$ such that our lost qubit is in the neighborhood $n(i)$ of the ith qubit. If we successfully measure X_i and all Z_j except for the lost qubit, we can multiply the eigenvalues to find either +1 or −1. Since the stabilizer generator has eigenvalue +1, this determines the Z eigenvalue, and therefore the Z eigenstate of our lost qubit. In Fig. 37(a), we show how an X measurement can be performed on a lost qubit by Z measurements on the adjacent qubits.

In cluster-state quantum computing, we need the ability to do single-qubit measurements in an arbitrary basis: $A = \cos\phi X + \sin\phi Y$. To this end, we use the cluster-state property that two adjacent X measurements remove the qubits from the cluster and transfer the bonds. This way, we can plant the qubit labeled A into the cluster [see Fig. 37(b)]. Instead of doing the A measurement on the in-line qubit, we perform the measurement on a qubit in the third (horizontal) level. When this measurement succeeds, we have to break the bonds with all other qubits in the tree. Therefore, we measure all remaining qubits in the third level as well as the qubits in the fourth level that are connected to the A qubit in the Z basis.

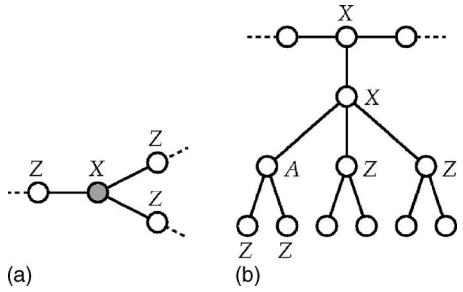

FIG. 37. Photon-loss-tolerant cluster states. (a) We can measure the Pauli operator X on the shaded (lost) qubit by measuring all the adjacent qubits in the Z basis. (b) Planting a cluster tree using two adjacent X measurements in order to do a single-qubit measurement in the basis A.

Sometimes the photon detection that constitutes the qubit measurement A will fail due to the detector inefficiency. In that case, we can attempt the A measurement on a second qubit in the third level. Again, the remaining qubits and the fourth-level qubits connected to the A qubit must be measured in the Z basis. Whenever such a Z measurement fails (as is the case for the qubit that failed the A measurement), we need to do an indirect Z measurement according to the method outlined above: When a photonic qubit is lost, we need to choose a stabilizer generator for which that photon was represented by a Z operator. The tree structure ensures that such an operator can always be found. We then measure all photons in this stabilizer generator to establish the Z eigenvalue for the lost photon. In the case of additional photon loss, we repeat this process until we succeed.

When the success probability of the measurement of a logical qubit is given by p, then the number of qubits in a tree n is given by

$$n = \text{polylog}\left(\frac{1}{1-p}\right). \tag{86}$$

Numerical simulations indicate that a detector loss of up to 50% can be corrected (Varnava *et al.*, 2005). Moreover, if more than 50% of photons were allowed to be lost, then we can imagine that all lost photons are collected by a third party who can perform a measurement complementary to A on the same qubit. Since this would violate various no-cloning bounds, such a strategy must be ruled out. Hence, a detection efficiency of 50% is the absolute minimum (Barrett, 2005).

In the circuit-based model by Gilchrist, Hayes, and Ralph, the lowest level of encoding consists of a polarized photon such that $|0\rangle \equiv |H\rangle$ and $|1\rangle \equiv |V\rangle$. The second level of encoding is the parity code $\{|0\rangle^{(n)}, |1\rangle^{(n)}\}$ of Eq. (52), which allows us to use the probabilistic fusion gates in a deterministic manner. The third level of encoding is

redundant encoding such that a logical qubit is encoded in a GHZ state of parity-encoded qubits (Ralph *et al.*, 2005):

$$|\psi\rangle_L \equiv \alpha|0\rangle_1^{(n)}\cdots|0\rangle_q^{(n)} + \beta|1\rangle_1^{(n)}\cdots|1\rangle_q^{(n)}. \tag{87}$$

To demonstrate that this code protects quantum information from photon loss, we show that heralded photon loss merely yields a recoverable error and that we can perform a universal set of deterministic quantum gates on these logical qubits.

First of all, we note that every pair of optical modes that constitutes the lowest-level qubit encoding must contain exactly one photon and no high number counting is required (contrary to the KLM scheme). This is also true for the Browne-Rudolph protocol. We therefore assume that we have bucket detectors with a certain detection efficiency η and a negligible dark count rate. The type-I and type-II fusion gates are then no longer (1,1) and (2,1) strategies, respectively. The type-I fusion gate ceases to yield pure output states, while the type-II gate yields a pure output state only if a detector coincidence is found (we assume perfect sources). Not only does failure remove the mode that was involved with the PBS, but we should also measure one mode in order to purify the cluster. Hence, the type-II fusion gate with bucket detectors is a (2,2) strategy and the growth requirement is $m>2/p$.

Suppose we wish to measure the value of the logical qubit $|\psi\rangle_L$ in the computational basis (as we discuss below, any other measurement can be performed by first applying a single-qubit rotation to $|\psi\rangle_L$). Since the logical qubit is a GHZ state, it is sufficient to measure only one parity qubit, e.g., the first one. Physically, this measurement constitutes a counting of horizontally and vertically polarized photons: if the number of vertically polarized photons is even, then the value of the parity qubit is $|0\rangle_1^{(n)}$, and if it is odd, then its value is $|1\rangle_1^{(n)}$. In order to successfully establish the parity, we therefore need to detect all n photons.

When we include photon loss in this measurement, there are three possible measurement outcomes for every optical mode: "horizontal," "vertical," or "detector failure." In the language of POVM's, this can be written as

$$\hat{E}^{(H)} = \eta|H\rangle\langle H|,$$

$$\hat{E}^{(V)} = \eta|V\rangle\langle V|, \tag{88}$$

$$\hat{E}^{(0)} = (1-\eta)(|H\rangle\langle H| + |V\rangle\langle V|).$$

These POVM's add up to unity in the subspace spanned by $|H\rangle$ and $|V\rangle$, as required. A particular measurement outcome on n modes can then be written as a string of n outcomes $s=(s_1,\ldots,s_n)$, where every $s_i\in\{H,V,0\}$. The optical state after finding a particular measurement outcome s is then

$$\rho_{2,\ldots,q} = \mathrm{Tr}_1[\hat{E}_1^{(s)}|\psi\rangle_L\langle\psi|]. \tag{89}$$

When all photons are detected, the qubit is projected onto its logical value. However, when one or more qubits are lost it is no longer possible to establish the parity. Therefore, as soon as a photon is lost the next photon is measured in a diagonal basis, thus disentangling the parity qubit from the other parity qubits. A few lines of algebra show that the remaining $q-1$ parity qubits are in the state

$$|\psi\rangle_L' = \alpha|0\rangle_2^{(n)}\cdots|0\rangle_q^{(n)} + \beta|1\rangle_2^{(n)}\cdots|1\rangle_q^{(n)}. \tag{90}$$

In other words, the encoding has become smaller but the quantum information has not been erased. We can therefore retry the measurement of the qubit q times.

Next, we have to show that we can perform deterministic one- and two-qubit gates using this redundant encoding. To this end, recall how deterministic gates were implemented in the parity encoding: A universal set of gates is $\{X_\theta^{(p)}, Z^{(p)}, Z_{\pi/2}^{(p)}, \mathrm{CNOT}^{(p)}\}$. We added a superscript (p) to indicate that these gates act on the parity qubit. As we have seen, the gates $Z_{\pi/2}^{(p)}$ and $\mathrm{CNOT}^{(p)}$ cannot be implemented deterministically, and have to be built using fusion gates.

How can these gates be used to form a universal set on the redundantly encoded (logical) qubit? First, the single-qubit gate Z is still implemented deterministically: $Z=Z^{(p)}=n\sigma_z$. Therefore, in order to apply a Z gate, a σ_z operation must be applied to all n photons in one and only one parity qubit. Second, the gate $Z_{\pi/2}$ is diagonal in the computational basis and can therefore be implemented using one $Z_{\pi/2}^{(p)}$. Third, the X_θ gate on the redundantly encoded qubit is somewhat problematic, since the gate transforms separable states of parity qubits into highly entangled GHZ states. However, if we apply $q-1$ $\mathrm{CNOT}^{(p)}$ gates, we can decode the qubit such that its state is $(\alpha|0\rangle_1^{(n)}+\beta|1\rangle_1^{(n)})\otimes|0\rangle_2^{(n)}\cdots|0\rangle_q^{(n)}$. We can then apply the deterministic gate $X_\theta^{(p)}$ to the first parity qubit and use another set of $q-1$ $\mathrm{CNOT}^{(p)}$ gates to reencode the qubit. Therefore, the gate X_θ "costs" $2(q-1)$ $\mathrm{CNOT}^{(p)}$ gates. Finally, the CNOT gate on the redundantly encoded qubit can be implemented using q $\mathrm{CNOT}^{(p)}$ gates.

Since every single-qubit operation can be constructed from X_θ and $Z_{\pi/2}$, we can perform arbitrary single-qubit measurements. We now have a universal set of gates on our logical qubit, together with computational-basis readout and an efficient encoding mechanism. Numerical simulations indicate that this method allows for detector, source, and memory efficiencies of $\eta>82\%$ (Ralph *et al.*, 2005).

Note that there seem to be conflicting requirements in this code: In order to execute successful fusion gates, we want n to be reasonably large. On the other hand, we want n to be as small as possible such that the probability of measuring all n photons $p=\eta^n$ is not too small. We assumed that every parity qubit is encoded with the same number of photons n, but this is not necessary. In principle, this method works when different parity qu-

bits have different-sized encodings. However, some care should be taken to choose every n_i as close to the optimal value as possible.

B. General error correction in LOQC

As we mentioned before, photon loss is not the only error in LOQC, and creating large cluster trees or a sizable redundant encoding in the circuit model will actually amplify other errors, such as dephasing. A truly fault-tolerant quantum computer architecture must therefore be able to handle the actual physical noise that will be present. Given a certain noise model and error-correcting codes, we can derive fault-tolerant thresholds: The errors must be smaller than the threshold value for concatenated error correction to eliminate them all. Knill *et al.* (2000) considered a combination of photon loss and dephasing in their original proposal and found that the accuracy threshold for optical components in that scheme was higher than 99%.

Dawson, Haselgrove, and Nielsen (2005, 2006) performed an extensive numerical study of fault-tolerant thresholds for linear optical cluster-state quantum computing. The computational model they adopted is Nielsen's microcluster approach, described in Sec. III.C, with type-I fusion gates instead of KLM-type CZ gates. The physical operations in this model are Bell-state preparation, single-photon gates and memories, type-I fusion gates, and photon measurements. The computation proceeds in time steps, with exactly one operation at each step. Furthermore, it is assumed that any two single-photon qubits in the computation can serve as inputs of the fusion gate. In other words, we have a direct interaction between qubits. In addition, parallel operations are allowed to speed up the computation and minimize the use of quantum memories. Finally, the classical computation needed to control the cluster-state computing is taken to be sufficiently fast.

The noise model adopted by Dawson *et al.* consists of the inherent probabilistic nature of the fusion gates, as well as photon loss and depolarization at every time step in the computation. The photon loss is characterized by a uniform loss probability γ, and the depolarization comes in two flavors: Single-qubit operations have a probability $\epsilon/3$ of undergoing a Pauli operation X, Y, or Z. After the Bell-state preparation and before the fusion gate input, the two photons undergo a correlated depolarizing noise: With probability $1-\epsilon$ nothing happens to the qubits, while with probability $\epsilon/15$ any of the remaining 15 two-qubit Pauli operators are applied. This is a completely general model for the noise that can affect optical cluster-state quantum computing, and the resulting fault-tolerance simulation gives an accuracy threshold region on γ and ϵ. Thresholds were obtained for both a seven-qubit CSS error correction code and a 23-qubit Golay error correction code. The study shows that scalable quantum computing with the 23-qubit code is possible for a maximum loss probability of $\gamma<3\times10^{-3}$ and a maximum depolarizing probability of $\epsilon<10^{-4}$.

Even though this noise model accounts for general noise and the fault-tolerant threshold puts a bound on its magnitude, it is clearly a simplification of the physical noise that is expected in cluster-state LOQC. It is argued that the difference between correlated two-qubit noise and independent noise does not change the threshold much. Similarly, using one parameter to describe both photon absorption and detector efficiency will not have a dramatic effect on the threshold (Nielsen, 2006a). The next milestone for establishing fault-tolerance thresholds is to adopt a noise model in which the parameters are measurable quantities, such as the visibility in a Hong-Ou-Mandel experiment and photon loss probabilities.

When various parameters in a noise model differ significantly, it might be beneficial to diversify the error correction codes. EC codes that correct specific errors such as photon loss or depolarization may be smaller than generic EC codes and therefore introduce less noise. A round of special error correction might be used to reduce large errors, and subsequent generic error correction will further reduce the errors below the fault-tolerant threshold.

In addition, certain types of errors or noise might be naturally suppressed by a suitable alteration in the architecture. For example, there is a way to create high-fidelity four-photon GHZ states with lossy bucket detectors and inefficient sources (Gilchrist, 2005). Assume that the Bell-pair source creates a state of the form $p_s|0\rangle\langle 0|+(1-p_s)|\Psi^-\rangle\langle\Psi^-|$, where $|\Psi^-\rangle$ is the two-photon polarization singlet state. This is a reasonable error model when the source obeys selection rules that prevent single-photon components to contribute to the output state (cf. Benson *et al.*, 2000). In order to make a three-photon GHZ state using these sources we use a type-I fusion gate and postselect on a single detector click. The detector click indicates that at least one source created a photon pair. However, if only one photon pair was created, the output mode of the type-I fusion gate must necessarily be empty. By taking the output modes of two type-I fusion gates in two separate three-photon GHZ creation attempts and leading them into a type-II fusion gate, we can postselect on finding two detector clicks. As a result, high-fidelity four-photon GHZ states are produced.

Several other specialized circuits have been proposed that either detect errors or correct them. For example, Ralph (2003) proposed a simple demonstration circuit that detects and corrects bit-flip errors on a single qubit using the encoded qubit state $\alpha|0\rangle|0\rangle+\beta|1\rangle|1\rangle$ and an ancilla qubit $|0\rangle$. However, since this is a probabilistic protocol, this circuit cannot naively be inserted in a quantum computing circuit. If we assume the availability of perfectly efficient detectors (not necessarily photon-number resolving), deterministic polarization-flip detection for distributing entanglement can be achieved (Kalamidas, 2004). In a similar fashion, a single-qubit error-correction circuit can be constructed with polarizing beam splitters, half-wave plates, and Pockels cells (Kalamidas, 2005). Here we assume that these passive

optical elements do not induce additional noise. A full analysis would have to take this noise into account.

VI. OUTLOOK: BEYOND LINEAR OPTICS

We have seen in this review that it is possible to construct a quantum computer with linear optics, single-photon sources, and photon detection alone. Knill, Laflamme, and Milburn (2001) overturned the conventional wisdom that a lack of direct photon-photon interactions prohibits scalability. Since the work of KLM, several groups have proposed modifications to building a linear optical quantum computer with reduced resources and realistic (noisy) components.

The basic principles of LOQC have all been demonstrated experimentally, predominantly using parametric down-conversion and bucket photon detection. Due to the small efficiency of PDC photon sources, however, these techniques cannot be considered scalable in a practical sense. Currently, there is a concerted effort to build the necessary single-photon sources, photon detectors, and quantum memories for a scalable linear optical quantum computer. On the theoretical front, there is an ongoing effort to design more efficient architectures and effective error correction codes tailored to the noise model that is relevant to LOQC.

Nevertheless, constructing the necessary components and using fault-tolerant encoding is hard, and several extensions to LOQC have been proposed. In this last section we sketch a few additions to the linear optical toolbox that can make quantum computing a little bit easier.

First, we have seen in Sec. I.D that cross-Kerr nonlinearity can be used to induce a photon-photon interaction and how two-qubit quantum gates can be constructed using such a nonlinearity. Unfortunately, natural Kerr nonlinearities are extremely small, and this is not a practical method for creating optical gates. However, recently it was suggested that a small nonlinearity might still be used for quantum computing. It was shown by Munro, Nemoto, *et al.* (2005) how such nonlinearities can make a number-resolving QND detector, and Barrett *et al.* (2005) showed how a small cross-Kerr nonlinearity can be used to perform complete Bell measurements without destroying photons. Subsequently, it was realized by Nemoto and Munro (2004) that this technique can also be used to create a deterministic CNOT gate on photonic qubits [see also Munro, Nemoto, and Spiller (2005)]. Recent work in electromagnetically induced transparencies by Lukin and Imamoğlu (2000, 2001) suggests that the small but not tiny nonlinearities needed for this method are on the threshold of becoming practical. Alternatively, relatively large nonlinearities can be obtained in photonic band-gap materials (Friedler *et al.*, 2004).

Second, if we have high-fidelity single-photon sources and memories, it might become beneficial to engineer these systems such that they support coherent single-qubit operations. This way, we can redefine our qubits as isolated static systems, and we have circumvented the problem of qubit loss. When these matter qubits emit a qubit-dependent photon, they can in turn be entangled using techniques from linear optical quantum computing. It was shown by Barrett and Kok (2005) that such an architecture can support scalable quantum computing, even with current realistic components. Independently, Lim *et al.* (2005a, 2005b) showed how a similar setup can be used to implement deterministic two-qubit quantum gates. Recently, these two methods were combined in a fault-tolerant, near-deterministic quantum computer architecture (Lim *et al.*, 2005a).

Third, Franson, Jacobs, and Pittman proposed the implementation of a two-qubit $\sqrt{\text{SWAP}}$ gate using the quantum Zeno effect: Two optical fibers are fused and split again, such that the input modes overlap in a small section of the fiber. This acts as a beam splitter on the modes in the input and output fibers. At regular intervals inside the joint fiber we place atoms with a two-photon transition. This transition acts as a two-photon measurement, while single-photon wave packets propagate through the fiber undisturbed. Furthermore, the single-photon wave packets maintain coherence. This repeated two-photon measurement effectively suppresses the Hong-Ou-Mandel effect via the quantum Zeno effect. In this way, two single-photon qubits in the input modes are transformed into two single-photon qubits in the output modes and undergo a $\sqrt{\text{SWAP}}$ gate.

Finally, an alternative approach to linear optical quantum computing involves encoding qubits in squeezed or coherent states of light (Gottesman *et al.*, 2001; Ralph *et al.*, 2003). Linear elements take on a new capability in these implementations. For example, Bell measurements and fan-out gates become deterministic elements (Jeong *et al.*, 2001; van Enk and Hirota, 2002). The downside is that it is difficult to produce the superposition states that are required as resources in such schemes, although considerable theoretical and experimental progress has been made recently (Lund *et al.*, 2004; Wenger *et al.*, 2004). If this problem is solved, considerable savings in resources could result from adopting such implementations.

Whatever the ultimate architecture of quantum computers will be, there will always remain a task for (linear) optical quantum information processing: In order to distribute quantum information over a network of quantum computers, the qubit of choice will most likely be optical. We therefore believe that the techniques reviewed here are an important step toward full-scale distributed quantum computing—the quantum internet.

ACKNOWLEDGMENTS

We would like to thank James Franson, Andrew White, Geoff Pryde, Philip Walther, and their coworkers for providing us with the experimental data of their respective CNOT gates. P.K. wishes to thank Sean Barrett and Dan Browne for stimulating discussions, Radu Ionicioiu, Michael Raymer, and Colin Williams for valuable comments, and Michael Nielsen for extensive correspondence on fault tolerance in LOQC. This work

was supported by ARO, the Australian Centre for Quantum Computer Technology, DTO, the Hearne Institute, JSPS, LSU BOR-LINK, MEXT, NSA, the QIPIRC, and the EU RAMBOQ Project.

REFERENCES

Achilles, D., C. Silberhorn, C. Śliwa, K. Banaszek, and I. A. Walmsley, 2003, Opt. Lett. **28**, 2387.

Banaszek, K., and I. A. Walmsley, 2003, Opt. Lett. **28**, 52.

Barnett, S. M., J. Jeffers, A. Gatti, and R. Loudon, 1989, Phys. Rev. A **57**, 2134.

Barreiro, J. T., N. K. Langford, N. A. Peters, and P. G. Kwiat, 2005, Phys. Rev. Lett. **95**, 260501.

Barrett, S. D., 2005 (private communication).

Barrett, S. D., P. Kok, K. Nemoto, R. G. Beausoleil, W. J. Munro, and T. P. Spiller, 2005, Phys. Rev. A **71**, 060302(R).

Barrett, S. D., and P. Kok, 2005, Phys. Rev. A **71**, 060310(R).

Benson, O., C. Santori, M. Pelton, and Y. Yamamoto, 2000, Phys. Rev. Lett. **84**, 2513.

Bergou, J. A., M. Hillery, and Y. Q. Sun, 2000, J. Mod. Opt. **47**, 487.

Berry, D. W., S. Scheel, C. R. Meyers, B. C. Sanders, P. L. Knight, and R. Laflamme, 2004, New J. Phys. **6**, 93.

Berry, D. W., S. Scheel, B. C. Sanders, and P. L. Knight, 2004, Phys. Rev. A **69**, 031806(R).

Beveratos, A., S. Kühn, R. Brouri, T. Gacoin, J. P. Poizat, and P. Grangier, 2002, Eur. Phys. J. D **18**, 191.

Biedenharn, L. C., and J. D. Louck, 1981, *Angular Momentum in Quantum Physics*, Encyclopedia of Mathematics and Its Applications, Vol. 8 (Addison-Wesley, Reading, MA).

Boschi, D., S. Branca, F. De Martini, L. Hardy, and S. Popescu, 1998, Phys. Rev. Lett. **80**, 1121.

Branczyk, A. M., T. J. Osborne, A. Gilchrist, and T. C. Ralph, 2003, Phys. Rev. A **68**, 043821.

Braunstein, S. L., and A. Mann, 1996, Phys. Rev. A **51**, R1727.

Braunstein, S. L., and P. van Loock, 2005, Rev. Mod. Phys. **77**, 513.

Browne, D. E., and T. Rudolph, 2005, Phys. Rev. Lett. **95**, 010501.

Brune, M., S. Haroche, V. Lefevre, J. M. Raimond, and N. Zagury, 1990, Phys. Rev. Lett. **65**, 976.

Brunel, C., B. Lounis, P. Tamarat, and M. Orrit, 1999, Phys. Rev. Lett. **83**, 2722.

Calsamiglia, J., 2002, Phys. Rev. A **65**, 030301(R).

Cerf, N. J., C. Adami, and P. G. Kwiat, 1998, Phys. Rev. A **57**, R1477.

Chuang, I. L., and M. A. Nielsen, 1997, J. Mod. Opt. **44**, 2455.

Chuang, I. L., and Y. Yamamoto, 1995, Phys. Rev. A **52**, 3489.

Cinelli, C., M. Barbieri, F. De Martini, and P. Mataloni, 2005, Laser Phys. **15**, 124.

Clausen, J., L. Knöll, and D. G. Welsch, 2002, J. Opt. B: Quantum Semiclassical Opt. **4**, 155.

Clausen, J., L. Knöll, and D. G. Welsch, 2003, Phys. Rev. A **68**, 043822.

Clauser, J. F., and J. P. Dowling, 1996, Phys. Rev. A **53**, 4587.

d'Ariano, G. M., C. Macchiavello, and L. Maccone, 2000, Fortschr. Phys. **48**, 573.

Dawson, C. M., H. L. Haselgrove, and M. A. Nielsen, 2005, Phys. Rev. Lett. **96**, 020501.

Dawson, C. M., H. L. Haselgrove, and M. A. Nielsen, 2006, Phys. Rev. A **73**, 052306.

De Martini, F., G. Di Giuseppe, and M. Marrocco, 1996, Phys. Rev. Lett. **76**, 900.

de Riedmatten, H., I. Marcikic, W. Tittel, H. Zbinden, and N. Gisin, 2003, Phys. Rev. A **67**, 022301.

Deuar, P., and W. J. Munro, 1999, Phys. Rev. A **61**, 010306(R).

Deuar, P., and W. J. Munro, 2000, Phys. Rev. A **62**, 042304.

Dowling, J. P., 1998, IEE Proc.-J: Optoelectron. **145**, 420.

Eisert, J., 2005, Phys. Rev. Lett. **95**, 040502.

Ekert, A., 1998, Phys. Scr. **T76**, 218.

Englert, B. G., C. Kurtsiefer, and H. Weinfurter, 2001, Phys. Rev. A **63**, 032303.

Fearn, H., and R. Loudon, 1987, Opt. Commun. **64**, 485.

Fiorentino, M., and F. N. C. Wong, 2004, Phys. Rev. Lett. **93**, 070502.

Fitch, M. J., B. C. Jacobs, T. B. Pittman, and J. D. Franson, 2003, Phys. Rev. A **68**, 043814.

Fleischhauer, M., and M. D. Lukin, 2002, Phys. Rev. A **65**, 022314.

Franson, J. D., M. M. Donegan, M. J. Fitch, B. C. Jacobs, and T. B. Pittman, 2002, Phys. Rev. Lett. **89**, 137901.

Franson, J. D., B. C. Jacobs, and T. B. Pittman, 2003, Fortschr. Phys. **51**, 369.

Franson, J. D., and T. B. Pittman, 1999, Lect. Notes Comput. Sci. **1509**, 383.

Friedler, I., G. Kurizki, and D. Petrosyan, 2004, Europhys. Lett. **68**, 625.

Gaebel, T., I. Popa, A. Gruber, M. Domhan, F. Jelezko, and J. Wrachtrup, 2004, New J. Phys. **6**, 98.

Gasparoni, S., J. W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, 2004, Phys. Rev. Lett. **93**, 020504.

Gérard, J. M., I. Robert, E. Moreau, M. Gallart, and I. Abram, 2002, J. Phys. IV **12**, 29.

Giacomini, S., F. Sciarrino, E. Lombardi, and F. De Martini, 2002, Phys. Rev. A **66**, 030302(R).

Gilchrist, A., 2005, private communication with Dan E. Browne.

Gilchrist, A., A. J. F. Hayes, and T. C. Ralph, 2005, e-print quant-ph/0505125.

Gilchrist, A., W. J. Munro, and A. G. White, 2003, Phys. Rev. A **67**, 040304(R).

Gingrich, R. M., P. Kok, H. Lee, F. Vatan, and J. P. Dowling, 2003, Phys. Rev. Lett. **91**, 217901.

Glancy, S., J. M. LoSecco, H. M. Vasconcelos, and C. E. Tanner, 2002, Phys. Rev. A **65**, 062317.

Gottesman, D., and I. L. Chuang, 1999, Nature (London) **402**, 390.

Gottesman, D., A. Kitaev, and J. Preskill, 2001, Phys. Rev. A **64**, 012310.

Grangier, P., J. A. Levenson, and J. P. Poizat, 1998, Nature (London) **396**, 537.

Greulich, K. O., and E. Thiel, 2001, Single Mol. **2**, 5.

Grice, W. P., A. B. U. Ren, and I. A. Walmsley, 2001, Phys. Rev. A **64**, 063815.

Hayes, A. J. F., A. Gilchrist, C. R. Myers, and T. C. Ralph, 2004, J. Opt. B: Quantum Semiclassical Opt. **6**, 533.

Hein, M., J. Eisert, and H. J. Briegel, 2004, Phys. Rev. A **69**, 062311.

Hennrich, M., T. Legero, A. Kuhn, and G. Rempe, 2004, New J. Phys. **6**, 86.

Hockney, G. M., P. Kok, and J. P. Dowling, 2003, Phys. Rev. A **67**, 032306.

Hofmann, H. F., K. Kojima, S. Takeuchi, and K. Sasaki, 2003, J. Opt. B: Quantum Semiclassical Opt. **5**, 218.

Hofmann, H. F., and S. Takeuchi, 2002, Phys. Rev. A **66**,

024308.
Hollars, C. W., S. M. Lane, and T. Huser, 2003, Chem. Phys. Lett. **370**, 393.
Hong, C. K., Z. Y. Ou, and L. Mandel, 1987, Phys. Rev. Lett. **59**, 2044.
Hours, J., S. Varoutsis, M. Gallart, J. Bloch, I. Robert-Philip, A. Cavanna, I. Abram, F. Laruelle, and J. M. Gérard, 2003, Appl. Phys. Lett. **82**, 2206.
Howell, J. C. and J. A. Yeazell, 2000a, Phys. Rev. A **62**, 032311.
Howell, J. C. and J. A. Yeazell, 2000b, Phys. Rev. Lett. **85**, 198.
Howell, J. C., and J. A. Yeazell, 2000c, Phys. Rev. A **61**, 052303.
Hutchinson, G. D., and G. J. Milburn, 2004, J. Mod. Opt. **51**, 1211.
Imamoğlu, A., 2002, Phys. Rev. Lett. **89**, 163602.
Imoto, N., H. A. Haus, and Y. Yamamoto, 1985, Phys. Rev. A **32**, 2287.
Jacobs, B. C., T. B. Pittman, and J. D. Franson, 2002, Phys. Rev. A **66**, 052307.
James, D. F. V., and P. G. Kwiat, 2002, Phys. Rev. Lett. **89**, 183601.
Jelezko, F., I. Popa, A. Gruber, C. Tietz, and J. Wrachtrup, 2002, Appl. Phys. Lett. **81**, 2160.
Jeong, H., M. S. Kim, and J. Lee, 2001, Phys. Rev. A **64**, 052308.
Jex, I., S. Stenholm, and A. Zeilinger, 1995, Opt. Commun. **117**, 95.
Johnsson, M., and M. Fleischhauer, 2003, Phys. Rev. A **67**, 061802(R).
Julsgaard, B., J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, 2004, Nature (London) **432**, 482.
Kalamidas, D., 2004, Phys. Lett. A **321**, 87.
Kalamidas, D., 2005, Phys. Lett. A **343**, 331.
Keller, M., B. Lange, K. Hayasaka, W. Lange, and H. Walther, 2004, Nature (London) **431**, 1075.
Kieling, K., D. Gross, and J. Eisert, 2006, e-print quant-ph/0601190.
Kim, J., S. Takeuchi, Y. Yamamoto, and H. H. Hogue, 1999, Appl. Phys. Lett. **74**, 902.
Kiraz, A., M. Atatüre, and A. Immamoğlu, 2004, Phys. Rev. A **69**, 032305.
Knill, E., 2002, Phys. Rev. A **66**, 052306.
Knill, E., 2003, Phys. Rev. A **68**, 064303.
Knill, E., 2005, Nature (London) **434**, 39.
Knill, E., R. Laflamme, and G. J. Milburn, 2000, e-print quant-ph/0006120.
Knill, E., R. Laflamme, and G. J. Milburn, 2001, Nature (London) **409**, 46.
Koashi, M., T. Yamamoto, and N. Imoto, 2001, Phys. Rev. A **63**, 030301(R).
Kok, P., 2003, IEEE J. Sel. Top. Quantum Electron. **9**, 1498.
Kok, P., and S. L. Braunstein, 2000a, Phys. Rev. A **62**, 064301.
Kok, P., and S. L. Braunstein, 2000b, Phys. Rev. A **61**, 042304.
Kok, P., and S. L. Braunstein, 2001, Phys. Rev. A **63**, 033812.
Kok, P., and S. L. Braunstein, 2006, Int. J. Quantum Inf. **4**, 119.
Kok, P., H. Lee, and J. P. Dowling, 2002, Phys. Rev. A **66**, 063814.
Kok, P., and W. J. Munro, 2005, Phys. Rev. Lett. **95**, 048901.
Kuhn, A., M. Hennrich, and G. Rempe, 2002, Phys. Rev. Lett. **89**, 067901.
Kurtsiefer, C., S. Mayer, P. Zarda, and H. Weinfurter, 2000, Phys. Rev. Lett. **85**, 290.
Kuzmich, A., W. P. Bowen, A. D. Boozer, A. Boca, C. W. Chou, L. M. Duan, and H. J. Kimble, 2003, Nature (London) **423**, 731.
Kwiat, P. G., J. R. Mitchell, P. D. D. Schwindt, and A. G. White, 2000 J. Mod. Opt. **47**, 257.
Kwiat, P. G., and H. Weinfurter, 1998, Phys. Rev. A **58**, R2623.
Lapaire, G. G., P. Kok, J. P. Dowling, and J. E. Sipe, 2003, Phys. Rev. A **68**, 042314.
Lee, H., U. Yurtsever, P. Kok, G. M. Hockney, C. Adami, S. L. Braunstein, and J. P. Dowling, 2004, J. Mod. Opt. **51**, 1517.
Lee, T. H., P. Kumar, A. Mehta, K. Xu, R. M. Dickson, and M. D. Barnes, 2004, Appl. Phys. Lett. **85**, 100.
Leonhardt, U., 1997, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, England).
Leonhardt, U., 2003, Rep. Prog. Phys. **66**, 1207.
Leonhardt, U., and A. Neumaier, 2004, J. Opt. B: Quantum Semiclassical Opt. **6**, L1.
Leung, D. W., 2004, Int. J. Quantum Inf. **2**, 33.
Li, X., P. L. Voss, J. Chen, J. E. Sharping, and P. Kumar, 2005, Opt. Lett. **30**, 1201.
Lim, Y. L., S. D. Barrett, A. Beige, P. Kok, and L. C. Kwek, 2006, Phys. Rev. A **73**, 012304.
Lim, Y. L., A. Beige, and L. C. Kwek, 2005, Phys. Rev. Lett. **95**, 030505.
Lloyd, S., 1995, Phys. Rev. Lett. **75**, 346.
Lloyd, S., and S. L. Braunstein, 1999, Phys. Rev. Lett. **82**, 1784.
Lombardi, E., F. Sciarrino, S. Popescu, and F. De Martini, 2002, Phys. Rev. Lett. **88**, 070402.
Lounis, B., and W. E. Moerner, 2000, Nature (London) **407**, 491.
Lounis, B., and M. Orrit, 2005, Rep. Prog. Phys. **68**, 1129.
Lukin, M. D., and A. Imamoğlu, 2000, Phys. Rev. Lett. **84**, 1419.
Lukin, M. D., and A. Imamoğlu, 2001, Nature (London) **413**, 273.
Lund, A. P., T. B. Bell, and T. C. Ralph, 2003, Phys. Rev. A **68**, 022313.
Lund, A. P., H. Jeong, and T. C. Ralph, and M. S. Kim, 2004, Phys. Rev. A **70**, 020101(R).
Lund, A. P. and T. C. Ralph, 2002, Phys. Rev. A **66**, 032307.
Lütkenhaus, N., J. Calsamiglia, and K. A. Suominen, 1999, Phys. Rev. A **59**, 3295.
Lvovsky, A. I., and M. G. Raymer, 2005, e-print quant-ph/0511044.
Maître, X., E. Hagley, G. Nogues, C. Wunderlich, P. Goy, M. Brune, J. M. Raimond, and S. Haroche, 1997, Phys. Rev. Lett. **79**, 769.
Maurer, C., C. Becher, C. Russo, J. Eschner, and R. Blatt, 2004, New J. Phys. **6**, 94.
McKeefer, J., A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble, 2004, Science **303**, 1992.
Messin, G., J. P. H. ans E. Giacobino, P. Desboilles, and M. Dahan, 2001, Opt. Lett. **26**, 1891.
Michler, P., A. Kiraz, C. Becher, W. V. Schoenfeld, P. Petroff, L. D. Zhang, E. Hu, and A. Imamoğlu, 2000, Science **290**, 2282.
Migdall, A. L., D. Branning, and S. Castelletto, 2002, Phys. Rev. A **66**, 053805.
Milburn, G. J., 1989, Phys. Rev. Lett. **62**, 2124.
Munro, W. J., K. Nemoto, R. G. Beausoleil, and T. P. Spiller, 2005, Phys. Rev. A **71**, 033819.
Munro, W. J., K. Nemoto, and T. P. Spiller, 2005, New J. Phys. **7**, 137.

Myers, C. R., and R. Laflamme, 2005, e-print quant-ph/0512104.
Myers, J. M. and H. E. Brandt, 1997, Meas. Sci. Technol. **8**, 1222.
Nemoto, K., and S. L. Braunstein, 2002, Phys. Rev. A **66**, 032306.
Nemoto, K., and W. J. Munro, 2004, Phys. Rev. Lett. **93**, 250502.
Newton, T. D., and E. P. Wigner, 1949, Rev. Mod. Phys. **21**, 400.
Nielsen, M. A., 2003, Phys. Lett. A **308**, 96.
Nielsen, M. A., 2004, Phys. Rev. Lett. **93**, 040503.
Nielsen, M. A., 2006a, private communication.
Nielsen, M. A., 2006b, Rep. Math. Phys. **57**, 147.
Nielsen, M. A., and I. L. Chuang, 2004, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England).
Nielsen, M. A., and C. M. Dawson, 2004, Phys. Rev. A **71**, 042323.
Nogues, G., A. Rauschenbeutel, S. Osnaghi, M. Brune, J. M. Raimond, and S. Haroche, 1999, Nature (London) **400**, 239.
O'Brien, J. L., G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White, 2004, Phys. Rev. Lett. **93**, 080502.
O'Brien, J. L., G. J. Pryde, A. G. White, and T. C. Ralph, 2005, Phys. Rev. A **71**, 060303(R).
O'Brien, J. L., G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, 2003, Nature (London) **426**, 264.
Paris, M. G. A., 2000, Phys. Rev. A **62**, 033813.
Paris, M. G. A., G. M. d'Ariano, P. L. Presti, and P. Perinotti, 2003, Fortschr. Phys. **51**, 449.
Pelton, M., C. Santori, J. Vučković, B. Y. Zhang, G. S. Solomon, J. Plant, and Y. Yamamoto, 2002, Phys. Rev. Lett. **89**, 233602.
Peres, A., and D. R. Terno, 2003, J. Mod. Opt. **50**, 1165.
Pittman, T. B., and J. D. Franson, 2002, Phys. Rev. A **66**, 062302.
Pittman, T. B., M. J. Fitch, B. C. Jacobs, and J. D. Franson, 2003, Phys. Rev. A **68**, 032316.
Pittmann, T. B., B. C. Jacobs, and J. D. Franson, 2001, Phys. Rev. A **64**, 062311.
Pittman, T. B., B. C. Jacobs, and J. D. Franson, 2002a, Phys. Rev. A **66**, 052305.
Pittman, T. B., B. C. Jacobs, and J. D. Franson, 2002b, Phys. Rev. Lett. **88**, 257902.
Pittman, T. B., B. C. Jacobs, and J. D. Franson, 2002c, Phys. Rev. A **66**, 042303.
Pittman, T. B., B. C. Jacobs, and J. D. Franson, 2005, Phys. Rev. A **71**, 052332.
Popescu, S., 1995, e-print quant-ph/9501020.
Poyatos, J. F., J. I. Cirac, and P. Zoller, 1997, Phys. Rev. Lett. **78**, 390.
Pryde, G. J., J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph, 2004, Phys. Rev. Lett. **92**, 190402.
Pryde, G. J., J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph, 2005, Phys. Rev. Lett. **95**, 048902.
Ralph, T. C., 2003, IEEE J. Sel. Top. Quantum Electron. **9**, 1495.
Ralph, T. C., 2004, Phys. Rev. A **70**, 012312.
Ralph, T. C., A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, 2003, Phys. Rev. A **68**, 042319.
Ralph, T. C., A. J. F. Hayes, and A. Gilchrist, 2005, Phys. Rev. Lett. **95**, 100501.
Ralph, T. C., N. K. Langford, T. B. Bell, and A. G. White, 2002, Phys. Rev. A **65**, 062324.
Ralph, T. C., A. G. White, W. J. Munro, and G. J. Milburn, 2002, Phys. Rev. A **65**, 012314.
Raussendorf, R., and H. J. Briegel, 2001, Phys. Rev. Lett. **86**, 5188.
Raussendorf, R., D. E. Browne, and H. J. Briegel, 2003, Phys. Rev. A **68**, 022312.
Raymer, M. G., J. Noh, K. Banaszek, and I. A. Walmsley, 2005, Phys. Rev. A **72**, 023825.
Reck, M., A. Zeilinger, H. J. Bernstein, and P. Bertani, 1994, Phys. Rev. Lett. **73**, 58.
Resch, K. J., J. S. Lundeen, and A. M. Steinberg, 2002, Phys. Rev. Lett. **89**, 037904.
Roch, J. F., K. Vigneron, P. Grelu, A. Sinatra, J. P. Poizat, and P. Grangier, 1997, Phys. Rev. Lett. **78**, 634.
Rohde, P. P., 2005, J. Opt. B: Quantum Semiclassical Opt. **7**, 82.
Rohde, P. P., and T. C. Ralph, 2005, Phys. Rev. A **71**, 032320.
Rohde, P. P., T. C. Ralph, and M. A. Nielsen, 2005, Phys. Rev. A **72**, 052332.
Rosenberg, D., A. E. La, A. J. Miller, and S. W. Nam, 2005, Phys. Rev. A **71**, 061803(R).
Rudolph, T., and J. W. Pan, 2001, e-print quant-ph/0108056.
Sanaka, K., T. Jennewein, J. W. Pan, K. Resch, and A. Zeilinger, 2004, Phys. Rev. Lett. **92**, 017902.
Santori, C., D. Fattal, M. Pelton, G. S. Solomon, and Y. Yamamoto, 2002, Phys. Rev. B **66**, 045308.
Santori, C., D. Fattal, J. Vučković, G. S. Solomon, and Y. Yamamoto, 2002, Nature (London) **419**, 594.
Santori, C., D. Fattal, J. Vučković, G. S. Solomon, and Y. Yamamoto, 2004, New J. Phys. **6**, 89.
Scheel, S., 2004, e-print quant-ph/0406127.
Scheel, S., 2005, e-print quant-ph/0508189.
Scheel, S., and K. M. R. Audenaert, 2005, New J. Phys. **7**, 149.
Scheel, S., and N. Lütkenhaus, 2004, New J. Phys. **6**, 51.
Scheel, S., W. J. Munro, J. Eisert, K. Nemoto, and P. Kok, 2006, Phys. Rev. A **73**, 034301.
Scheel, S., K. Nemoto, W. J. Munro, and P. L. Knight, 2003 Phys. Rev. A **68**, 032310.
Scheel, S., J. Pachos, E. A. Hinds, and P. L. Knight, 2004, e-print quant-ph/0403152.
Schmidt, H., and A. Imamoğlu, 1996, Opt. Lett. **21**, 1936.
Scully, M. O., and W. E. Lamb, 1969, Phys. Rev. **179**, 368.
Silva, M., M. Rötteler, and C. Zalka, 2005, Phys. Rev. A **72**, 032307.
Simon, R., and N. Mukunda, 1990, Phys. Lett. A **143**, 165.
Śliwa, C., and K. Banaszek, 2003, Phys. Rev. A **67**, 030101(R).
Spedalieri, F. M., H. Lee, and J. P. Dowling, 2006, Phys. Rev. A **73**, 012334.
Spiller, T. P., W. J. Munro, S. D. Barrett, and P. Kok, 2006, Contemp. Phys. (to be published).
Spreeuw, R. J. C., 1998, Found. Phys. **28**, 361.
Stace, T. M., G. J. Milburn, and C. H. W. Barnes, 2003, Phys. Rev. B **67**, 085317.
Steane, A. M., 2003, Phys. Rev. A **68**, 042322.
Stenholm, S., 1996, Opt. Commun. **123**, 287.
Summhammer, J., 1997, Phys. Rev. A **56**, 4324.
Takeuchi, S., 2000a, Phys. Rev. A **61**, 052302.
Takeuchi S., 2000b, Phys. Rev. A **62**, 032301.
Takeuchi, S., 2001, Electron. Commun. Jpn., Part 2: Electron. **84**, 52.
Takeuchi, S., J. Kim, Y. Yamamoto, and H. H. Hogue, 1999, Appl. Phys. Lett. **74**, 1063.

Thew, R. T., S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, 2002, Phys. Rev. A **66**, 062304.
Titulaer, U. M., and R. M. Glauber, 1966, Phys. Rev. **145**, 1041.
Törmä P., I. Jex, and S. Stenholm, 1996, J. Mod. Opt. **43**, 245.
Törmä P., and S. Stenholm, 1996, Phys. Rev. A **54**, 4701.
Törmä P., S. Stenholm, and I. Jex, 1995, Phys. Rev. A **52**, 4853.
Treussart F., R. Alléaume, V. Le Floc'h, L. T. Xiao, J. M. Courty, and J. F. Roch, 2002, Phys. Rev. Lett. **89**, 093601.
Turchette, Q. A., C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, 1995, Phys. Rev. Lett. **75**, 4710.
U'Ren, A. B., K. Banaszek, and I. A. Walmsley, 2003, Quantum Inf. Comput. **3**, 480.
Vaidman, L., and N. Yoran, 1999, Phys. Rev. A **59**, 116.
van Enk, S. J., and O. Hirota, 2002, Phys. Rev. A **64**, 022313.
van Loock, V., and N. Lütkenhaus, 2004, Phys. Rev. A **69**, 012302.
Varnava, M., D. E. Browne, and T. Rudolph, 2005, e-print quant-ph/0507036.
Verstraete, F., and J. I. Cirac, 2004, Phys. Rev. A **70**, 060302(R).
Vučković, J., D. Fattal, C. Santori, and G. S. Solomon, 2003, Appl. Phys. Lett. **82**, 3596.
Waks, E., K. Inoue, W. D. Oliver, E. Diamanti, and Y. Yamamoto, 2003, IEEE J. Sel. Top. Quantum Electron. **9**, 1502.
Walther, P., K. J. Resch, T. Rudolph, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, 2005, Nature (London) **434**, 169.
Ward, M. B., O. Z. Karimov, D. C. Unitt, Z. L. Yuan, P. See, D. G. Gevaux, A. J. Shields, P. Atkinson, and D. A. Ritchie, 2005, Appl. Phys. Lett. **86**, 201111.
Weihs, G., M. Reck, H. Weinfurter, and A. Zeilinger, 1996, Opt. Lett. **21**, 302.
Weinfurter, H., 1994, Europhys. Lett. **25**, 559.
Wenger, J., R. Tualle-Brouri, and P. Grangier, 2004, Phys. Rev. Lett. **92**, 153601.
Wightman, A. S., 1962, Rev. Mod. Phys. **34**, 845.
Yamamoto, Y., M. Kitagawa, and K. Igeta, 1988, in *Proceedings of the 3rd Asia-Pacific Physics Conference*, edited by Y. W. Chan, A. F. Leung, C. N. Yang, and K. Young (World Scientific, Singapore), pp. 779–799.
Yamamoto T., M. Koashi, Ş. Özdemir, and N. Imoto, 2003, Nature (London) **421**, 343.
Yoran, N., and B. Reznik, 2003, Phys. Rev. Lett. **91**, 037903.
Yuan, Z. L., B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, 2002, Science **295**, 102.
Zeilinger, A., 1981, Am. J. Phys. **49**, 882.
Zhao, Z., A. N. Zhang, Y. A. Chen, H. Zhang, J. F. Du, T. Yang, and J. W. Pan, 2005, Phys. Rev. Lett. **94**, 030501.
Zou, X. B., K. Pahlke, and W. Mathis, 2002, Phys. Rev. A **65**, 064305.
Zwiller, V., T. Aichele, W. Seifert, J. Persson, and O. Benson, 2003, Appl. Phys. Lett. **82**, 1509.