Quantum computation with optical coherent states

T. C. Ralph,* A. Gilchrist, and G. J. Milburn
Centre for Quantum Computer Technology, Department of Physics, University of Queensland Brisbane, Queensland 4072, Australia

W. J. Munro
Hewlett Packard Laboratories, Filton Road Stoke Gifford, Bristol BS34 8QZ, United Kingdom

S. Glancy
Department of Physics, University of Notre Dame, Notre Dame, Indiana 46556, USA
(Received 28 May 2003; revised manuscript received 11 August 2003; published 20 October 2003)

We show that quantum computation circuits using coherent states as the logical qubits can be constructed from simple linear networks, conditional photon measurements, and ''small'' coherent superposition resource states.

DOI: 10.1103/PhysRevA.68.042319 PACS number(s): 03.67.Lx, 42.50.−p

I. INTRODUCTION

Quantum optics has proved a fertile field for experimental tests of quantum information science. However, quantum optics was not thought to provide a practical path to efficient and scalable quantum computation. This orthodoxy was challenged when Knill *et al.* [1] showed that, given single-photon sources and single-photon detectors, linear optics alone would suffice to implement efficient quantum computation. While this result is surprising, the complexity of the optical networks required is daunting.

More recently it has become clear that other, quite different versions of this paradigm are possible. In particular, by encoding the quantum information in multiphoton coherent states, rather than single-photon states, an efficient scheme which is elegant in its simplicity has been proposed [2]. The required resource, which may be produced nondeterministically, is a superposition of coherent states. Given this, the scheme is deterministic and requires only relatively simple linear optical networks and photon counting. Unfortunately, the amplitude of the required resource states is prohibitively large. Here we build on this idea and show that with only a moderate increase in complexity, a scheme based on much smaller superposition states is possible.

The idea of encoding quantum information on continuous variables of multiphoton fields [3] has led to a number of proposals for realizing quantum computation in this way [4–6]. One drawback of these proposals is that ''hard,'' nonlinear interactions are required ''in-line'' of the computation. These would be very difficult to implement in practice. In contrast, this proposal requires only ''easy,'' linear in-line interactions. The hard interactions are only required for ''off-line'' production of resource states. A related proposal is that of Gottesman *et al.* [7] in which superpositions of squeezed states are used to encode the qubits. In that proposal the hard interactions are only used for the initial-state preparation. However, quadratic, squeezing-type interactions are required in-line along with linear interactions.

This paper is laid out in the following way. We start by describing the basic principles of the scheme. In Secs. III and IV we describe realistic measurement and resource production techniques, respectively, based on photon counting and linear optics. In Sec. V we consider error correction and we conclude in Sec. VI.

II. BASIC SCHEME

The output of a single-mode, stabilized laser can be described by a coherent state $|\alpha\rangle$, where α is a complex number which determines the average field amplitude. Coherent states are defined by unitary transformation of the vacuum [8], $|\alpha\rangle = D(\alpha)|0\rangle$, where $D(\alpha)$ is the displacement operator. Let us consider an encoding of logical qubits in coherent states with $|0\rangle_L \equiv |-\alpha\rangle$ and $|1\rangle_L \equiv |\alpha\rangle$, where we take α to be real [9]. These qubits are not exactly orthogonal, but the approximation of orthogonality is good for α even moderately large as $|\langle\alpha|-\alpha\rangle|^2 = e^{-4\alpha^2}$. We will assume for most of this paper that $\alpha \geqslant 2$, which gives $|\langle\alpha|-\alpha\rangle|^2 \leqslant 1.1 \times 10^{-7}$. Measurement of the qubit values can be achieved with high efficiency by homodyne detection with respect to a local oscillator phase reference.

Of course, if one wished, an exactly orthogonal qubit code can easily be defined in terms of the orthogonal parity eigenstates, $\widetilde{|0\rangle}_L = |\alpha\rangle + |-\alpha\rangle$, $\widetilde{|1\rangle}_L = |\alpha\rangle - |-\alpha\rangle$. However, such states are only a single (nonunitary) qubit gate away from the code we propose to use. The issue is not so much the orthogonality of the qubit code, but rather the need to work outside the qubit space during qubit processing. As we shall now show, this can be done with negligible error.

Bit-flip gate. The logical value of a qubit can be flipped by delaying it with respect to the local oscillator by half a cycle. Thus the X or ''bit-flip'' gate is given by

$$X = \exp\{i\pi \hat{a}^\dagger \hat{a}\}. \tag{1}$$

This is a unitary gate. As already noted, the Hadamard gate (or its equivalents) which effects transformation from $|x\rangle_L$ to $\widetilde{|x\rangle}_L$ cannot be unitary. This is because the logical basis states are not orthogonal but the states $\widetilde{|x\rangle}_L$ are parity eigenstates

*Email address: ralph@physics.uq.edu.au

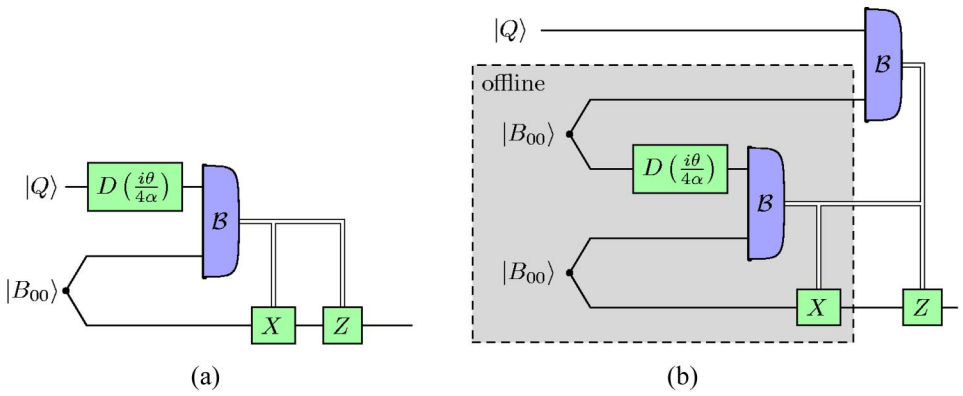

FIG. 1. Schematics of implementing the $R(Z,\theta)$ gate. (a) The bare gate; its operation is near deterministic for a sufficiently small value of θ/α. Repeated application of this gate can build up a finite rotation with high probability. (b) The teleported gate; its operation is deterministic, however, it may need to be applied several times in order to achieve the correct rotation. Determinism is achieved by preparing the entangled resource off line and only applying the gate to the qubit when the resource is available. In the diagrams, $\mathcal{B}$ represents a cat-Bell measurement.

which are orthogonal. For this reason we now consider nonunitary gates based on projective measurement. Gates based on projective measurements will be probabilistic in their operation.

Sign-flip gate. A bit flip in the superposition basis, i.e., a "sign flip" or Z gate, can be achieved via teleportation [10] as follows. A resource of coherent superposition states (commonly referred to as "cat" states), $1/\sqrt{2}(|-\sqrt{2}\alpha\rangle + |\sqrt{2}\alpha\rangle)$, is required. Splitting such a cat state on a 50:50 beam splitter produces the entangled Bell state, $1/\sqrt{2}(|-\alpha, -\alpha\rangle + |\alpha,\alpha\rangle)$. A Bell basis measurement is then made on the qubit state, $\mu|-\alpha\rangle+\nu|\alpha\rangle$, and one half of the entangled state (where μ and ν are arbitrary complex numbers). Depending on which of the four possible outcomes are found, the other half of the Bell state is projected into one of the following four states with equal probability:

$$\begin{aligned}&\mu|-\alpha\rangle+\nu|\alpha\rangle,\\ &\mu|-\alpha\rangle-\nu|\alpha\rangle,\\ &\mu|\alpha\rangle+\nu|-\alpha\rangle,\\ &\mu|\alpha\rangle-\nu|-\alpha\rangle.\end{aligned} \tag{2}$$

The bit-flip errors in the third and fourth results can be corrected using the X gate. After X correction the gate has two possible outcomes: either the identity has been applied, in which case we repeat the process, or else the required transformation

$$Z(\mu|-\alpha\rangle+\nu|\alpha\rangle)=\mu|-\alpha\rangle-\nu|\alpha\rangle \tag{3}$$

has been implemented. On average, this will take two attempts. We write

$$Z=T_X^p, \tag{4}$$

meaning that the teleportation transformation T with bit-flip correction X is applied p times, where p is outcome dependent.

Our remaining gates implement operations which may conveniently be described by the product operator notation

$$\begin{aligned}R(K_i\otimes K_j,\theta)&=e^{-i\theta/2K_i\otimes K_j}\\ &=\cos(\theta/2)I\otimes I-i\sin(\theta/2)K_i\otimes K_j,\end{aligned} \tag{5}$$

where $K_{i,j}$ can take on the values, X, Y, Z, or I (the Pauli sigma operators and the identity). For single-qubit operations we will drop the redundant identity I operation on the second qubit.

Phase rotation gate. Consider an arbitrary single-qubit rotation about Z, $R(Z,\theta)$. This can be implemented by shifting our qubit a small distance out of the computational basis and then using teleportation to project back. We begin by displacing our arbitrary input qubit by a small amount in the imaginary direction [see Fig. 1(a)],

$$\begin{aligned}&D\left(\frac{i\theta}{4\alpha}\right)(\mu|-\alpha\rangle+\nu|\alpha\rangle)\\ &\quad=e^{-i\theta/4}\mu\left|-\alpha\left(1-\frac{i\theta}{4\alpha^2}\right)\right\rangle+e^{i\theta/4}\nu\left|\alpha\left(1+\frac{i\theta}{4\alpha^2}\right)\right\rangle.\end{aligned} \tag{6}$$

Now consider the effect of teleporting this state. Using the relationship [8]

$$\langle\tau|\alpha\rangle=\exp[-1/2(|\tau|^2+|\alpha|^2)+\tau^*\alpha], \tag{7}$$

we find that the required projections are approximately given by

$$\begin{aligned}\left\langle\pm\alpha\left|\pm\alpha\left(1\pm\frac{i\theta}{4\alpha^2}\right)\right.\right\rangle&=e^{\pm i\theta/4}e^{-\theta^2/32\alpha^2},\\ \left\langle\mp\alpha\left|\pm\alpha\left(1\pm\frac{i\theta}{4\alpha^2}\right)\right.\right\rangle&=0,\end{aligned} \tag{8}$$

where we have assumed orthogonality and that $\theta^2/32\alpha^2 \ll 1$. The outcome of the sequence of displacement followed by teleportation is then found to be

$$T_X D\left(\frac{i\theta}{4\alpha}\right)(\mu|-\alpha\rangle+\nu|\alpha\rangle) = e^{-\theta^2/32\alpha^2}(e^{-i\theta/2}\mu|-\alpha\rangle \pm e^{i\theta/2}\nu|\alpha\rangle). \quad (9)$$

The "$\pm$" sign depends on the Bell state measurement outcome and can be corrected by the Z gate. The transformation is then $R(Z,\theta)$.

Notice, however, that the output state in Eq. (9) is unnormalized. This reflects the fact that because we are projecting back onto the qubit basis from outside, the probability of success is not unity. In other words, there is a probability $P=1-e^{-\theta^2/16\alpha^2}$ that the Bell state measurement will return a null result, in which case the gate will fail. In order to make the probability of failure as small as possible, we require $\theta^2 \ll 16\alpha^2$. One option would be to let α be large [2]. In this way θ can be a significant angle while $P\approx 1$ is still satisfied. However, this is undesirable because of the difficulty in producing cat states with large α.

A second option is to implement the gate with an incremental phase shift, repeatedly, to build up a significant angle. Let $\theta=n\phi$, then after n rotations by ϕ we have

$$\left[T_X D\left(\frac{i\phi}{4\alpha}\right)\right]^n(\mu|-\alpha\rangle+\nu|\alpha\rangle) = e^{-n\phi^2/32\alpha^2}(e^{-in\phi/2}\mu|-\alpha\rangle \pm e^{in\phi/2}\nu|\alpha\rangle). \quad (10)$$

The transformation is again $R(Z,\theta)$. The success probability is $P=e^{-\theta^2/16n\alpha^2}$, which can be made arbitrarily close to one for small α simply by choosing n sufficiently large. For example, with $\alpha=2$, $\theta=\pi/4$, and $n=8$ we find $P=0.9988$ (or $n=30$ gives $P=0.9997$). This is basically an application of the quantum Zeno effect [11].

A third option is to use the technique of gate teleportation [12]. In this case we place the gate inside a second teleporter as shown schematically in Fig. 1(b). The $R(Z,\theta)$ gate of Eq. (9) is implemented on one arm of a second Bell-cat state. If (and only if) the gate is successful, a Bell measurement is made between the qubit and the other arm of the entangled state. It is straightforward to show that the output state after X and Z corrections is

$$e^{\mp i\theta/2}\mu|-\alpha\rangle+e^{\pm i\theta/2}\nu|\alpha\rangle. \quad (11)$$

The signs in the arguments of the exponentials depend on the Bell state measurement results. The qubit is teleported with an equal probability of either $R(Z,\theta)$ or $R(Z,-\theta)$ applied. The operation is deterministic for the qubit as the second teleportation is only carried through if the first one is successful. In general, the result $R(Z,-\theta)$ can be corrected by applying the gate again, but this time attempting to apply $R(Z,2\theta)$. If this again fails, the process is continued by attempting to apply $R(Z,4\theta)$, etc. Symmetry can be exploited for certain angles. For example, for the "phase" gate $R(Z,\pi/2)$, only X and Z corrections are necessary.

Controlled phase gate. A nontrivial two-qubit gate $R(Z\otimes Z,-\phi)$ can be implemented in a way similar to the single-qubit rotation [see Fig. 2(a)]. Consider the beam splitter interaction given by the unitary transformation

$$U_{ab}=\exp\left[i\frac{\theta}{2}(ab^\dagger+a^\dagger b)\right], \quad (12)$$

where a and b are the annihilation operators corresponding to two coherent-state qubits $|\gamma\rangle_a$ and $|\beta\rangle_b$, with γ and β taking values of $-\alpha$ or α. It is well known that the output state produced by such an interaction is

$$U_{ab}|\gamma\rangle_a|\beta\rangle_b=\left|\cos\frac{\theta}{2}\gamma+i\sin\frac{\theta}{2}\beta\right\rangle_a\left|\cos\frac{\theta}{2}\beta+i\sin\frac{\theta}{2}\gamma\right\rangle_b, \quad (13)$$

where $\cos^2(\theta/2)$ $[\sin^2(\theta/2)]$ is the reflectivity (transmissivity) of the beam splitter. If both output beams are now projected using teleportation as for the single-qubit gate we find for an arbitrary input state

$$\begin{aligned} &T_{Xa}T_{Xb}U_{ab}(\nu|-\alpha\rangle_a|-\alpha\rangle_b+\mu|\alpha\rangle_a|-\alpha\rangle_b \\ &\quad+\tau|-\alpha\rangle_a|\alpha\rangle_b+\gamma|\alpha\rangle_a|\alpha\rangle_b) \\ &=e^{-\theta^2\alpha^2/4}(e^{i\theta\alpha^2}\nu|-\alpha\rangle_a|-\alpha\rangle_b \pm e^{-i\theta\alpha^2}\mu|\alpha\rangle_a|-\alpha\rangle_b \\ &\quad\pm e^{-i\theta\alpha^2}\tau|-\alpha\rangle_a|\alpha\rangle_b+e^{i\theta\alpha^2}\gamma|\alpha\rangle_a|\alpha\rangle_b, \end{aligned} \quad (14)$$

where, as before, we have assumed orthogonality, and that $\theta^2\alpha^2 \ll 1$ and the $\pm$ signs depend on the outcome of the Bell measurements. If we choose $\phi=2\theta\alpha^2=\pi/2$, then $R(Z\otimes Z,-\pi/2)$ is implemented, a gate that can easily be shown to be locally equivalent to a CNOT.

Once again the probability of success is nonunit, and two options are possible for small α: repeated iterations of the gate for an incremental value of ϕ can be used to build up to a total angle of $\pi/2$ with a high probability of success via the quantum zeno effect or we can use gate teleportation to guarantee success. To achieve the second gate teleportation we must now nest the two-qubit gate inside two teleporters as shown schematically in Fig. 8(b). Only X and Z corrections are required.

Superposition gate. To complete our set of gates we now describe how to implement a rotation of $\pi/2$ about X, i.e., $R(X,\pi/2)$. This gate takes computational basis qubits into the diagonal, or superposition, basis and is locally equivalent to a Hadamard gate. The gate is shown schematically in Fig. 9(a). It is similar to the Z rotation except that now the displacement followed by Bell state measurement on the qubit and one of the Bell state modes is replaced by the beam splitter interaction used in the $R(Z\otimes Z,-\pi/2)$ gate, followed by single (as opposed to Bell-) cat measurements on the output modes from the beam splitter. The interaction produces the following output state from an arbitrary input:

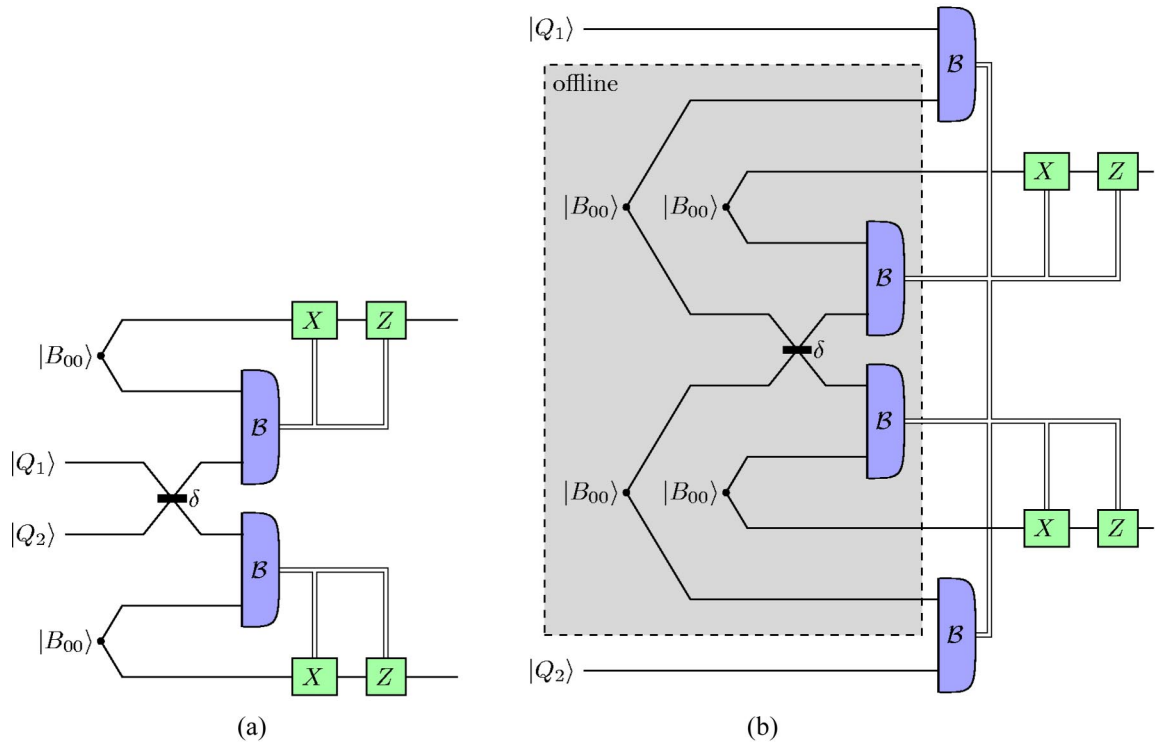

FIG. 2. Schematics of implementing the $R(Z\otimes Z,-\pi/2)$ gate. (a) The bare gate; its operation is near deterministic for a sufficiently small value of $\theta^2\alpha^2$ where the reflectivity of the beam splitter is $\delta=\cos^2(\theta/2)$. Repeated application of this gate can build up to a $\pi/2$ rotation with high probability. (b) The teleported gate; its operation is deterministic. Determinism is achieved by preparing the entangled resource off line and only applying the gate to the qubits when the resource is available. In the diagrams, $\mathcal{B}$ represents a cat-Bell measurement.

$$C_a C_b U_{BS}(\mu|-\alpha\rangle+\nu|\alpha\rangle)$$
$$=e^{-\theta^2\alpha^2/4}\{(e^{i\theta\alpha^2}\mu\pm e^{-i\theta\alpha^2}\nu)|-\alpha\rangle$$
$$+(\pm e^{-i\theta\alpha^2}\mu\pm e^{i\theta\alpha^2}\nu)|\alpha\rangle\}, \tag{15}$$

where C_a and C_b represent the cat state projections. The $\pm$ signs depend on the outcome of the cat state measurements. Using X and Z gates we can correct all the $\pm$'s to $+$'s. Choosing $2\theta\alpha^2=\pi/2$ then implements $R(X,\pi/2)$. As before, the gate is probabilistic for small α, working with a probability of $e^{-\theta^2\alpha^2/2}$. To achieve near determinism using the quantum Zeno effect, one would replace the beam splitter interaction [within the dashed box of Fig. 3(a)] with the $R(Z\otimes Z,-\phi)$ gate of Fig. 3(a), iterated sufficient times to give $\phi=\pi/2$ with high probability of success. The rest of the gate remains the same and will work deterministically. As before, we can also implement the gate deterministically using gate teleportation as depicted in Fig. 3(b). Only X and Z corrections are required.

The gates $R(Z,\theta)$, $R(X,\pi/2)$, and $R(Z\otimes Z,-\pi/2)$ form a universal set. An arbitrary single-qubit rotation can be constructed from $R(Z,\psi)R(X,\pi/2)R(Z,\phi)R(X,-\pi/2)$ and, as commented before, $R(Z\otimes Z,-\pi/2)$ is locally equivalent to a CNOT. This completes our basic discussion. In the following section we consider how the required cat and Bell state measurements can be performed.

III. CAT-BASIS MEASUREMENTS

We define a cat-basis measurement to be some procedure that projects the state of an optical mode onto one of the two states $(1/\sqrt{2})(|-\alpha\rangle\pm|\alpha\rangle)$. If our input state consists only of an arbitrary superposition of these two states then cat-basis measurement can be achieved by simply counting the photons in the mode. An even number of detected photons indicates measurement of the state $(1/\sqrt{2})(|-\alpha\rangle+|\alpha\rangle)$, and an odd number of photons indicates measurement of $(1/\sqrt{2})(|-\alpha\rangle-|\alpha\rangle)$. Of course, this will require very high quality photon detectors which can reliably distinguish n from $n+1$ photons when $n\sim\alpha^2$.

The cat states can also be distinguished to some extent by homodyne detection looking at the imaginary quadrature. Cat states display fringes in the imaginary quadrature which are $\pi/2$ out of phase between the plus and minus cats [13]. Therefore a measurement result that falls close to a fringe maximum can be identified with one or other cat with high probability. This technique gives inconclusive results some of the time (i.e., close to the fringe crossings) but could prove useful for initial experimental demonstrations.

In order to perform a Bell basis measurement on two modes (say, modes a and b) containing coherent-state qubits we can employ the following procedure [14,15]. Allow the two qubits to interfere at a 50:50 beam splitter $B_{a,b}=\exp[(\pi/4)(-a^\dagger b+ab^\dagger)]$, where a and b are the annihila-

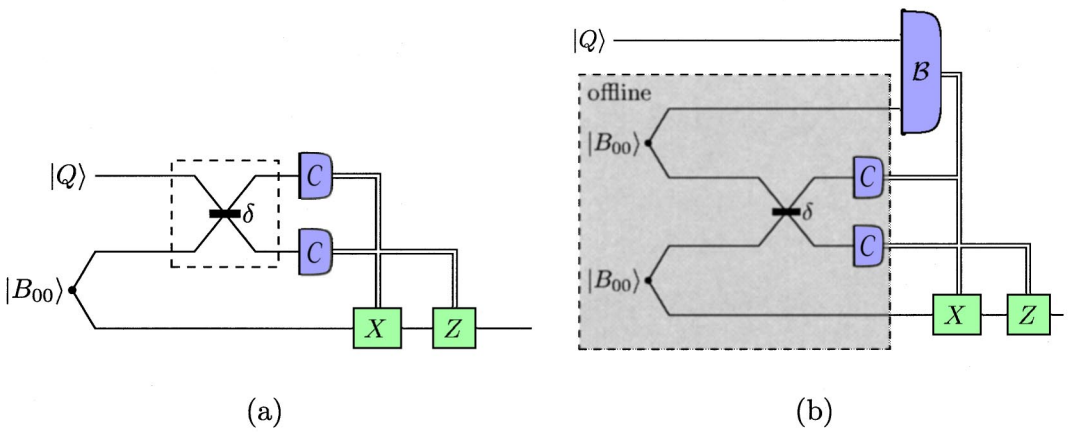

FIG. 3. Schematics of implementing the $R(X,\pi/2)$ gate. (a) The bare gate; its operation is near deterministic for a sufficiently small value of $\theta^2\alpha^2$. Replacement of the dashed section with the repeated application of the gate of Fig. 8(a) can build up to a $R(X,\pi/2)$ rotation with high probability. (b) The teleported gate; its operation is deterministic. Determinism is achieved by preparing the entangled resource off line and only applying the gate to the qubits when the resource is available. In the diagrams, $\mathcal{B}$ represents a cat-Bell measurement, and $\mathcal{C}$ represents a cat measurement.

tion operators for modes a and b. Then use photon counters to measure the number of photons in each mode. We can then identify the following four possible results: (1) an even number of photons in mode a and zero photons in mode b, (2) an odd number of photons in mode a and zero photons in mode b, (3) zero photons in mode a and an even number of photons in mode b, or (4) zero photons in mode a and an odd number of photons in mode b; corresponding to each of the following four Bell-cat states: (1) $|B_{00}\rangle=(1/\sqrt{2})(|-\alpha,-\alpha\rangle+|\alpha,\alpha\rangle)$, (2) $|B_{10}\rangle=(1/\sqrt{2})(|-\alpha,-\alpha\rangle-|\alpha,\alpha\rangle)$, (3) $|B_{01}\rangle=(1/\sqrt{2})(|-\alpha,\alpha\rangle+|\alpha,-\alpha\rangle)$, or (4) $|B_{11}\rangle=(1/\sqrt{2})(|-\alpha,\alpha\rangle-|\alpha,-\alpha\rangle t)$. Note that there is also a fifth possibility of detecting zero photons in both modes a and b, which indicates a failure of the measurement. Fortunately, this occurs with probability of only $\sim e^{-\alpha^2}$. The preceding discussion assumed that we were only differentiating between states within the computational basis. However, the gates discussed in Sec. II involved moving short distances outside this basis. Nevertheless, we will show in the following that these types of measurements are sufficient to implement our gates.

As an example, we will examine the use of this procedure for the Bell state measurement required when performing $R(Z,\theta)$. In order to perform this rotation, we must use the displacement $D(i\theta/4\alpha)$ on the qubit $|Q\rangle$ in mode a and append the Bell state $(1/\sqrt{2})(|-\alpha,-\alpha\rangle+|\alpha,\alpha\rangle)$ in modes b and c. When modes a and b meet in the beam splitter used for the Bell state measurement, their interference is incomplete and the resulting state is

$$\begin{aligned}|Q_D\rangle &= B_{a,b}D_a\left(\frac{i\theta}{4\alpha}\right)|Q\rangle|B_{00}\rangle \\ &= \mu e^{-i\theta/4}|-\sqrt{2}\alpha+i\delta,-i\delta,-\alpha\rangle \\ &\quad+\mu e^{-i\theta/4}|i\delta,\sqrt{2}\alpha-i\delta,\alpha\rangle \\ &\quad+\nu e^{i\theta/4}|i\delta,-\sqrt{2}\alpha-i\delta,-\alpha\rangle \\ &\quad+\nu e^{i\theta/4}|\sqrt{2}\alpha+i\delta,-i\delta,\alpha\rangle, \end{aligned} \tag{16}$$

where $\delta=\theta/4\sqrt{2}\alpha$. Because the qubit in mode a was corrupted by the displacement operator, now it is possible to detect photons in both modes a and b simultaneously. We now detect n_a photons in mode a and n_b photons in mode b, and this measurement leaves mode c in the pure state given by

$$\begin{aligned}\langle n_a|\langle n_b|Q_D\rangle &= \frac{1}{\sqrt{2}}\exp\left(-\alpha^2-\frac{\theta^2}{32\alpha^2}\right)\frac{1}{\sqrt{n_a!n_b!}}(\sqrt{2}\alpha)^{n_a+n_b} \\ &\quad\times[\mu e^{-i\theta/4}(-1)^{n_a+n_b}(1-i\epsilon)^{n_a}(i\epsilon)^{n_b}|-\alpha\rangle \\ &\quad+\mu e^{-i\theta/4}(i\epsilon)^{n_a}(1-i\epsilon)^{n_b}|\alpha\rangle \\ &\quad+\nu e^{i\theta/4}(-1)^{n_b}(i\epsilon)^{n_a}(1+i\epsilon)^{n_b}|-\alpha\rangle \\ &\quad+\nu e^{i\theta/4}(-1)^{n_b}(1+i\epsilon)^{n_a}(i\epsilon)^{n_b}|\alpha\rangle], \end{aligned} \tag{17}$$

where $\epsilon=\theta/8\alpha^2$, and we have ignored the normalization factor due to the nonorthogonality of the computational basis states. This state may need to be corrected with X or Z operations and properly normalized before we obtain the final result of the teleportation, which we will call $|Q_{n_a,n_b}\rangle$. We can see that this state is close to our goal by examining the limit when $\epsilon\ll 1$. In this case we are almost certain to measure one of n_a or n_b to be zero. The number of photons in the other mode is given by a probability distribution which is almost exactly equal to the Poisson distribution with a mean of $2\alpha^2$. This leaves us with the state

$$\approx \mu e^{-i\theta/4}(1-in\epsilon)|-\alpha\rangle+\nu e^{i\theta/4}(1+in\epsilon)|\alpha\rangle \tag{18}$$

$$\approx \mu e^{-i[(\theta/4)+n\epsilon]}|-\alpha\rangle+\nu e^{i[(\theta/4)+n\epsilon]}|\alpha\rangle \tag{19}$$

$$=R\left[Z,\frac{\theta}{4}\left(1+\frac{n}{2\alpha^2}\right)\right](\mu|-\alpha\rangle+\nu|\alpha\rangle). \tag{20}$$

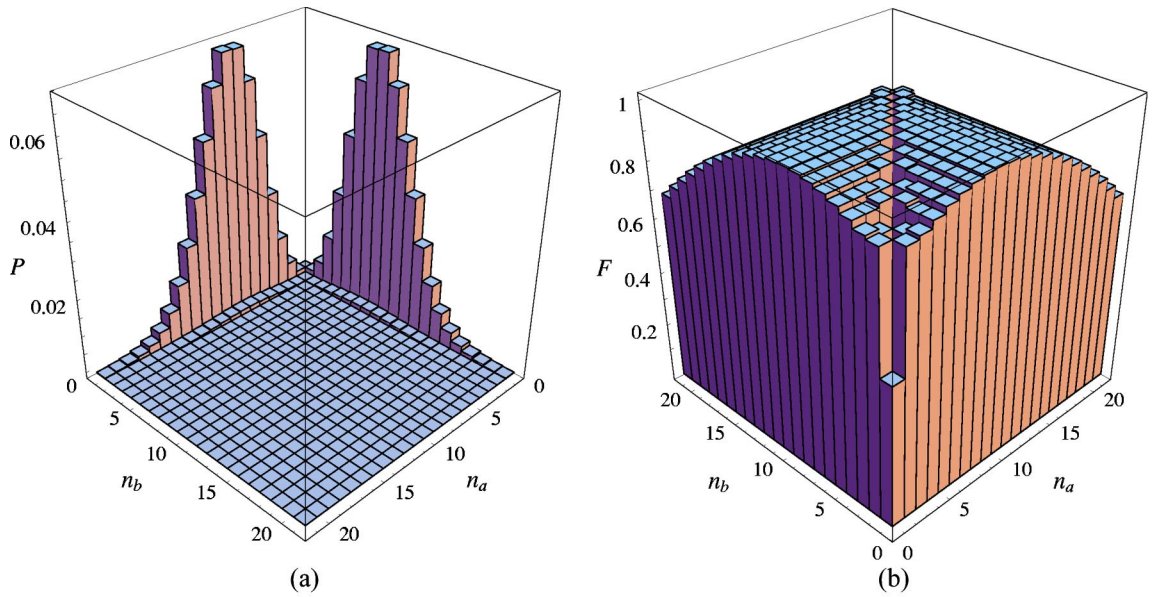

FIG. 4. Here we plot (a) the probability to detect the pair n_a, n_b when performing the $R(Z,\pi/2)$ rotation, and (b) $F=|\langle Q_{n_a,n_b}|Q_{goal}\rangle|^2$ as a function of n_a and n_b. We use the worst case input qubit and an $\alpha=2$.

To evaluate the effectiveness of this procedure without making such severe approximations, we examine $|Q_{n_a,n_b}\rangle$ in Fig. 4, where we calculate the fidelity $|\langle Q_{n_a,n_b}|Q_{goal}\rangle|^2$ and the probability to measure n_a and n_b. We use $\alpha=2$, the input qubit $|Q\rangle=(1/\sqrt{2})(|-\alpha\rangle+|\alpha\rangle)$, and a rotation angle $\theta=\pi/2$. These choices for $|Q\rangle$ and θ give the worst case scenario, in which we obtain the lowest fidelity with $|Q_{goal}\rangle=R(Z,\theta)|Q\rangle$. Because the Z operation is equivalent to $R(Z,\pi)$, we can reach any angle by using Z and $R(Z,\theta)$, where $\theta\leqslant\pi/2$. One can see that $|\langle Q_{n_a,n_b}|Q_{goal}\rangle|^2$ is very close to one in the regions where we are most likely to detect the pair n_a, n_b.

In order to compute the overall fidelity of this operation, we first construct the mixed state ρ representing the output of the teleportation operation for all measurement results,

$$\rho=\sum_{n_a=0}^{\infty}\sum_{n_b=0}^{\infty}P(n_a,n_b)|Q_{n_a,n_b}\rangle\langle Q_{n_a,n_b}|. \tag{21}$$

The fidelity is then given by

$$F=\langle Q_{goal}|\rho|Q_{goal}\rangle. \tag{22}$$

We plot $F(\alpha)$ for $\theta=\pi/2$ and $F(\theta)$ for $\alpha=2$ in Fig. 5. We can obtain a fidelity of 0.99 or above for any desirable angle if we can produce qubits with $\alpha=3$. A second strategy would be to limit our operation of $R(Z,\theta)$ to small angles. Larger rotations could be built from repeated applications of a high fidelity gate. For example the fidelity for $\theta=\pi/16$ is $F=0.999\,70$ when $\alpha=2$. Repeating this eight times implements $R(Z,\pi/2)$ with a fidelity of $F=0.999\,70^8=0.997\,56$. Compare this with the fidelity of 0.980 91 when performing $R(Z,\pi/2)$ in a single step.

Yet a third strategy emerges if we are willing to operate the logic gate in a nondeterministic fashion, in which the gate sometimes fails and must be repeated with a new copy of the qubit. Qubits can be protected from destruction if we use the gate teleportation scheme of Ref. [12] as pictured in Fig. 1 and discussed in the preceding section. We can then simply discard $R(Z,\theta)$ attempts for which the measurements of n_a and n_b yield low values for the product $|\langle Q_{n_a,n_b}|Q_{goal}\rangle|^2$. Suppose we choose a set S of (n_a,n_b)

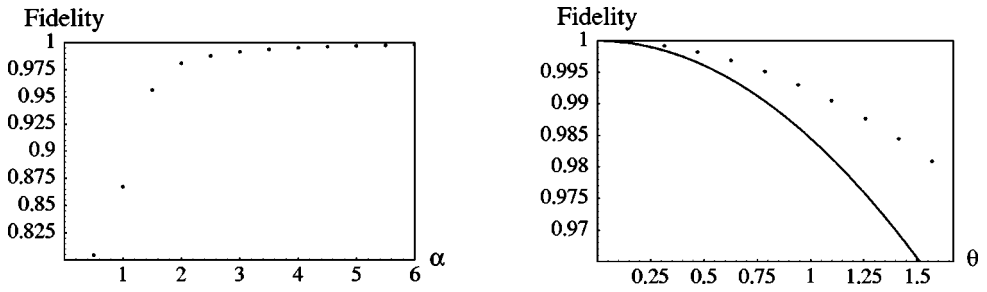

FIG. 5. Here we plot the fidelity of our procedure for performing the $R(Z,\theta)$ rotation as a function of α (using $\theta=\pi/2$) and as a function of θ (using $\alpha=2$). The dots show the fidelity after the teleportation and the curve shows the fidelity before teleportation. We use the worst case input qubit.

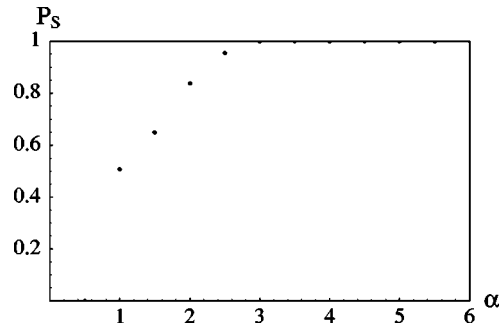

FIG. 6. Here we plot $P_S(\alpha)$, the probability that our implementation of $R(Z,\theta)$ succeeds, given that we demand it performs with a fidelity of 0.99. Here again we use $\theta=\pi/2$ and the worst case qubit.

pairs which are accepted as successful operations of the logic gate, and P_S is the probability to measure a member S during the teleportation. The total output of the logic gate (when it succeeds) is then the mixed state

$$\rho_S=\frac{1}{P_S}\sum_{(n_a,n_b)\in S} P(n_a,n_b)|Q_{n_a,n_b}\rangle\langle Q_{n_a,n_b}|. \qquad (23)$$

We can now operate this logic gate with a fidelity which is very close to one. Of course, this is limited by the maximum possible value of $|\langle Q_{n_a,n_b}|Q_{goal}\rangle|^2$ (0.999 999 9 for $\alpha=2$ and $\theta=\pi/2$ with the worst case qubit). Suppose we insist on performing $R(Z,\theta)$ with a fidelity of 0.99. In Fig. 6 we plot P_S as a function of α under this restriction. This allows us to make estimates of the number of Bell-cat states required to perform a single $R(Z,\theta)$. In the gate teleportation scheme, each attempt to perform $R(Z,\theta)$ requires two Bell-cat states, so on an average we need $2/P_S$ Bell cats. Because there is a 50% probability of performing $R(Z,-\theta)$ during the gate teleportation, we need additional $2/P_S$ Bell cats to correct this, and because Z commutes with $R(Z,\theta)$ it is not necessary to perform Z after each teleportation; instead we can wait and perform only one Z after all teleportations are complete. This makes a total of $4/P_S+1$ Bell cats on average, or 8.88 for $\alpha=1$, or 5.78 for $\alpha=2$.

Which of these three strategies, (i) using very large α, (ii) using only small θ, or (iii) operating the gate probabilistically and using gate teleportation, is ultimately most efficient is a complicated question that will depend on the constraints of Bell-cat production and photon counters. We hope to address this further in future research.

The other gates of the preceding section can similarly be implemented by replacing the projective measurements with photon counting measurements. In this way we are able to implement a universal set of quantum gates on the coherent-state qubits via linear optics, photon counting, and cat and Bell-cat state resources. We now examine how the cat and Bell-cat states may be produced.

IV. THE GENERATION OF SMALL SCHRÖDINGER CAT STATES

Let us now turn our attention to how small amplitude Schrödinger cat states required for our universal quantum

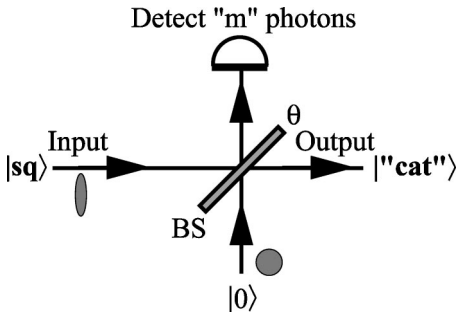

FIG. 7. Schematic diagram for the generation of Schrödinger-like cat states by means of a conditional photon number measurement on a beam splitter. A single-mode squeezed state is used as an input into one port of a variable reflectivity beam splitter with the other input being a vacuum state. A definite measurement of m photons (with $m>0$) on one output port of the beam splitter prepares the required state to a good approximation.

computation schemes can be realized using technologies currently available or likely in the near future. More specifically, how do we generate states of the form

$$|\Psi_\pm\rangle=\frac{1}{\sqrt{\mathcal{N}_\pm}}[|-\alpha\rangle\pm|\alpha\rangle], \qquad (24)$$

where the $\mathcal{N}_\pm=2\pm2e^{-2|\alpha|^2}$. As we have seen, the amplitude of these cat states need not be large ($\alpha\approx2$ is sufficient). An elegant proposal was made by Dakna *et al.* [16] (see also Ref. [17]) for generating such states by means of a conditional measurement on a beam splitter. Their scheme is depicted in Fig. 7 and works as follows: A squeezed state of the form $|\Psi_{sq}\rangle=(1-|\lambda|^2)^{1/4}\Sigma_n[\sqrt{(2n)!}/n!](\lambda/2)^n|2n\rangle$ (with squeezing parameter λ) and a vacuum state $|0\rangle$ are combined on a variable transmissivity θ beam splitter. On the second output port from the beam splitter, a definite photon number measurement, which can be modeled by the projector $|m\rangle\langle m|$, is performed giving a result m. The conditional state of the remaining output mode is then

$$|\Psi_m\rangle=\frac{1}{\sqrt{\mathcal{N}_m}}\sum_n c_{n,m}\left(\frac{\lambda\cos^2\theta}{2}\right)^{(n+m)/2}|n\rangle, \qquad (25)$$

with $c_{n,m}=(n+m)![1+(-1)^{n+m}]/[\sqrt{n!}\Gamma([(n+m)/2]+1)]$ and $\mathcal{N}_m=\Sigma_n c_{n,m}^2|\lambda\cos^2\theta/2|^{n+m}$. The mean photon number for Eq. (25) is

$$\langle\overline{n}\rangle=\frac{1}{\mathcal{N}_m}\sum_n nc_{n,m}^2\left|\frac{\lambda\cos^2\theta}{2}\right|^{n+m}. \qquad (26)$$

Equation (25) can be broken into two cases: the state resulting from an even m result and the state from an odd m (which will not be considered here). For m even, Eq. (25) has only even photon numbers and can be written in the simplified form

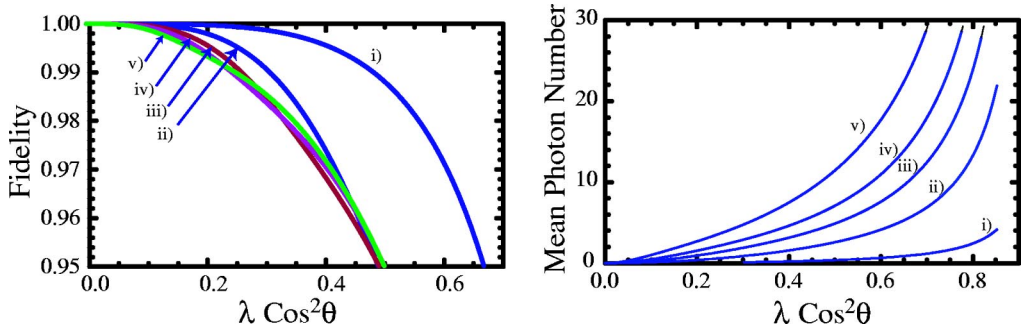

FIG. 8. Plot of the fidelity of the state, Eq. (25), compared with Eq. (24) and mean photon number of Eq. (25) vs $\lambda \cos^2\theta$ for (i) $m=0$, (ii) $m=2$, (iii) $m=4$, (iv) $m=6$, and (v) $m=10$.

$$|\Psi_m\rangle = \frac{1}{\sqrt{\mathcal{N}_m}} \sum_n \frac{(2n+m)! \left(\frac{\lambda \cos^2\theta}{2}\right)^{[n+(m/2)]}}{\left(n+\frac{m}{2}\right)! \sqrt{(2n)!}} |2n\rangle. \tag{27}$$

For $\lambda \cos^2\theta$ small, this expression can be further approximated as

$$|\Psi_m\rangle \approx |0\rangle + \lambda \cos^2\theta \frac{1+m}{\sqrt{2}} |2\rangle + \cdots. \tag{28}$$

Here we observe that as m increases, so does the population in the $|2\rangle$ (and higher) states compared with the $m=0$ situation. Thus for small $\lambda \cos^2\theta$, the mean photon number increases as m increases. As a cautionary note, we must emphasize that the scheme here requires the detection of an exact number of photons to generate the approximate single-mode cat state. Currently, detectors are not that efficient but good progress is being made.

Now let us determine how good an approximation, Eq. (25), is with the Schrödinger cat states given by Eq. (24). This can be achieved by calculating the overlap $F = |\langle \Psi_+ | \Psi_m \rangle|^2$ between the two states. To this end, we plot in Fig. 8 both the mean photon number of the state of Eq. (25) and the fidelity for various even m. It is interesting to observe that a good fidelity ($>95\%$) can be achieved for quite a range of $\lambda \cos^2\theta$ and m. In fact, for $\lambda \cos^2\theta \leqslant 0.3$ the fidelity between the two states we are comparing exceeds 99%. However, to achieve a cat state with a moderate mean photon number we either need m large or $\lambda \cos^2\theta \geqslant 0.5$. As m increases, the overlap between Eqs. (24) and (25) for the same mean photon number increases. There is a potential regime where Eq. (25) has moderate mean photon number and a high overlap with the state in Eq. (24). However, there is a trade-off in that the initial probability of generating the state in Eq. (25) with λ fixed decreases as m increases. The probability of successfully generating the state in Eq. (25) is given by

$$P_m = \sqrt{\frac{1-\lambda^2}{1-\lambda^2 \cos^4\theta}} \left[\frac{\lambda^2 \sin^2 2\theta}{4(1-\lambda^2 \cos^4\theta)}\right]^m \times \sum_{l=0}^{m/2} \frac{m!}{(m-2l)!\, l!^2 (2\lambda \cos^2\theta)^{2l}} \tag{29}$$

and is shown in Fig. 9 for various m. As m increases, the probability of successfully generating our required state significantly decreases but the success probability is reasonable for $\lambda = 0.6$ with either $m=2$ or 4. With such parameters we can generate a Schrödinger cat like state with a fidelity greater than 95% with a probability of success greater than 1%.

Let us now determine if the Dakna cat state can be used to generate the entangled cat state $|\alpha\rangle|\alpha\rangle + |-\alpha\rangle|-\alpha\rangle$ required in the teleportation step of the various fundamental gates. Such a state can be generated by combining it with the vacuum state on a 50/50 beam splitter (here we need to choose the amplitude β of the original single-mode cat to be $\sqrt{2}\alpha$). Using the Dakna state cat as the input to this beam splitter, we plot in Fig. 10(a) the overlap between the resulting two mode-state and the two-mode entangled state. We observe that for both $m=2,4$ we have the fidelity exceeding 95% for a wide range of parameters. This indicates that to a very good approximation we can generate the two-mode entangled cat state required for our basic gate operations. Given this entangled resource we can now investigate one such gate operation. We consider the operation of the $R(Z,\phi)$ gate illustrated in Fig. 1 using the Dakna cat state to generate both the entangled resource and the state $|Q\rangle$. In Fig. 10(b) we

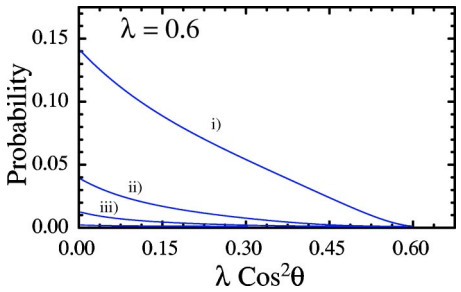

FIG. 9. Plot of the probability of generating Eq. (25) vs $\lambda \cos^2\theta$ for $\lambda = 0.6$ with (i) $m=2$, (ii) $m=4$, and (iii) $m=6$.

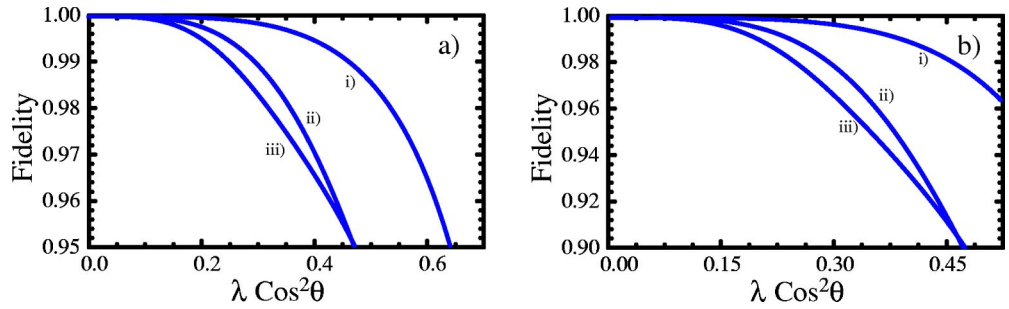

FIG. 10. Plot of the fidelity for the (a) Dakna two-mode cat state vs $|\alpha\rangle|\alpha\rangle+|-\alpha\rangle|-\alpha\rangle$ and (b) the state $e^{i\phi}|\alpha\rangle+e^{-i\phi}|-\alpha\rangle$ resulting from the action of the gate $R(Z,\phi)$ with $\phi=\pi/32$ vs $\lambda\cos^2\theta$ for (i) $m=0$, (ii) $m=2$, and (iii) $m=4$.

show the fidelity for performing the gate operation to transform the state $|Q\rangle$ to $e^{i\phi}|\alpha\rangle+^{-i\phi}|-\alpha\rangle$ for small ϕ. These results show the feasibility of performing, in principle, experiments to demonstrate quantum logic.

V. ERROR CORRECTION

A viable quantum computation scheme must be capable of incorporating error correction. We now briefly discuss the issue of error correction. The major sources of error in our scheme are expected to be, in order of increasing significance, (i) errors due to nonorthogonal code states, (ii) errors due to moving outside the qubit basis, (iii) errors due to random optical phase shifts, and (iv) photon loss.

Sources (i) and (ii) are equivalent. As discussed in Sec. II we could use the cat states as orthogonal code states. These states are a single-qubit gate away from the coherent-state code. Such a gate must be nonunitary and we have given a method based on teleportation to achieve this. Single-qubit manipulations in the cat state basis require us to move outside the qubit basis and rely on teleportation to project back into the computational basis. We have shown that errors introduced in this process due to nonorthogonality of coherent states are exponentially small in amplitude and in any case are heralded by the teleportation process itself. If we see an error, we can repeat the teleportation process which, as the errors can be made so small, is very likely to succeed after a couple of trials. We will thus not consider these sources of error further.

Optical phase-shift errors will occur due to timing errors between different qubits and between qubits and the local oscillator. Such errors may arise from path-length fluctuations in the circuit. These can be monitored and corrected through classical optical interferometric techniques. Such locking techniques are a mature technology and can be extremely precise. We will assume that sufficient classical control is exercised to make these errors negligible.

Photon loss error, however, is a more serious problem as it is never heralded and increases quadratically with α. In this case we must turn to error correction coding to mitigate the effect. Photons are lost from a coherent state at Poisson distributed times at a rate determined by $\gamma\langle a^\dagger a\rangle$, where γ is the single-photon loss rate. Obviously, if a photon is lost, the system has one less photon. The effect of photon loss from a pure state is thus given by $|\psi\rangle\rightarrow a|\psi\rangle$, where a is the Bose annihilation operator.

The Poisson distributed nature of photon loss means that even when no photons are lost from a coherent state, the state must change. Not seeing a photon emitted up to time t indicates that the state is increasingly likely not to contain any photons at all, and thus we must continuously adjust our description of the state to reflect this knowledge.

We can put the description of photon loss on a more formal basis by asking for the conditional state of the system, given an entire history of photon loss events. This is a list of times $\{t_1<t_2<\cdots<t_n\leqslant t\}$ at which photons are lost. The (un-normalized) conditional state [18] is

$$\begin{aligned}|\psi(t|t_1,t_2,\ldots,t_n)\rangle &= \gamma^{n/2}e^{-\gamma(t-t_n)\hat{a}^\dagger\hat{a}/2}\hat{a}e^{-\gamma(t_n-t_{n-1})\hat{a}^\dagger\hat{a}/2}\\ &\quad\times\hat{a}\cdots e^{-\gamma(t_2-t_1)\hat{a}^\dagger\hat{a}/2}\hat{a}e^{-\gamma t_1\hat{a}^\dagger\hat{a}/2}|\psi(0)\rangle. \qquad (30)\end{aligned}$$

The norm of this unconditional state is the probability for this history.

If we start in the coherent state $|\alpha\rangle$ and lose no photons up to time t, the conditional state is $|\kappa\alpha\rangle$ where $\kappa=e^{-\gamma t/2}$. The important fact here is that the state remains a coherent state even though the amplitude is decreased. This kind of error takes us out of the code space, but can be corrected by teleportation. Consider the state

$$|\Psi\rangle=(\mu|-\kappa\alpha\rangle_1+\nu|\kappa\alpha\rangle_1)(|\alpha,\alpha\rangle_{23}+|-\alpha,-\alpha\rangle_{23}). \qquad (31)$$

If we mix modes 1 and 2 on a beam splitter, and count $n\neq 0$ photons in mode 1 and 0 photons in mode 2, the conditional state of mode 3 is found to be $\mu|-\alpha\rangle+\nu|\alpha\rangle$. If κ is small enough, this will occur with high probability. In fact, letting $\kappa=1-\epsilon$, the probability for this event is very close to

$$P(n_1\neq 0,n_2=0)=e^{-\epsilon^2|\alpha|^2/2}, \qquad (32)$$

the teleportation projects us back into the qubit basis with high probability as it is most likely that n_1 is near $2|\alpha|^2$. Failure of the protocol is heralded by $n_1=0,n_2\neq 0$ and thus the gate can be repeated if necessary. The dominant term in the failure probability is approximately given $e^{-2|\alpha|^2}$. In

fact, this resetting of the amplitude happens as a matter, of course, in all the teleportation-based gates we have discussed. Thus it may not be necessary to explicitly introduce additional gates for this purpose.

If a photon is lost from a coherent state, the state is unchanged up to a phase as $a|\alpha\rangle=\alpha|\alpha\rangle$, which when normalized produces only a phase shift given by the phase of α [19]. This means that, in the qubit code space, photon loss is equivalent to an erroneous application of the Z gate, which induces a sign-flip error. A sign flip error may be converted into a bit-flip error by performing a Hadamard gate and working in the conjugate basis $|\pm\rangle=|\alpha\rangle\pm|-\alpha\rangle$, (that is, the cat states). To prepare a code state to protect sign-flip errors, we thus first prepare the standard three-qubit code [20],

$$|0\rangle_L=|-\alpha,-\alpha,-\alpha\rangle, \quad |1\rangle_L=|\alpha,\alpha,\alpha\rangle, \tag{33}$$

and then perform a Hadamard gate on each mode separately. Sign-flip errors will now appear as bit-flip errors and can be corrected using the standard three-qubit circuit [21].

The encoding is easily done in linear optics by an extension of the technique previously discussed for producing Bell entanglement. Two beam splitters suffice to implement the transformation

$$(\mu|-\beta\rangle_1+\nu|\beta\rangle_1)|0\rangle_2|0\rangle_3 \rightarrow\left(\mu\left|\frac{-\beta}{\sqrt{3}}\right\rangle_1\left|\frac{-\beta}{\sqrt{3}}\right\rangle_2\left|\frac{-\beta}{\sqrt{3}}\right\rangle_3+\nu\left|\frac{\beta}{\sqrt{3}}\right\rangle_1\left|\frac{\beta}{\sqrt{3}}\right\rangle_2\left|\frac{\beta}{\sqrt{3}}\right\rangle_3\right). \tag{34}$$

At the first beam splitter, with reflectivity amplitude of $1/\sqrt{3}$, modes 1 and 2 are combined, subsequently, modes 2 and 3 are combined at a 50:50 beam splitter. Thus by choosing $\beta=\sqrt{3}\alpha$ we can immediately prepare the entangled state $\mu|-\alpha,-\alpha,-\alpha\rangle+\nu|\alpha,\alpha,\alpha\rangle$.

Any logical operation may be performed on an arbitrary state in the code space,

$$|\psi\rangle_L=\mu|-\alpha,-\alpha,-\alpha\rangle+\nu|\alpha,\alpha,\alpha\rangle, \tag{35}$$

by extending the teleportation gates for the single-mode case to the multimode case. Displacements can easily be done for one mode at a time. The teleportation steps in the gates will require a six-mode entangled resource of the form

$$|\alpha,\alpha,\alpha,\alpha,\alpha,\alpha\rangle+|-\alpha,-\alpha,-\alpha,-\alpha,-\alpha,-\alpha\rangle. \tag{36}$$

Such a state could be prepared by an obvious generalization of the method used in Eq. (34), however, the amplitude of the initial cat state is becoming uncomfortably large. We now show how to avoid this problem.

Consider the resource state

$$|-\alpha,-\sqrt{2}\alpha\rangle+|\alpha,\sqrt{2}\alpha\rangle, \tag{37}$$

which can be produced from a cat state of amplitude $\sqrt{3}\alpha$ by splitting it on a beam splitter of reflectivity $1/\sqrt{3}$. Suppose this state is used as the entanglement in a teleportation protocol, with the smaller amplitude arm being mixed with the input state and measured. The result of the teleportation is the transformation

$$\mu|-\alpha\rangle+\nu|\alpha\rangle\rightarrow\mu|-\sqrt{2}\alpha\rangle+\nu|\sqrt{2}\alpha\rangle, \tag{38}$$

where we have assumed that the necessary bit-flip and sign-flip corrections have been made. That is, the state is amplified while preserving the superposition. If the amplified state is then split on a 50:50 beam splitter, an entangled state of the same amplitude as the original will be produced. By repeating this process many times, multimode encoded states or entangled resource states can be produced deterministically without the need to produce ''large'' cats.

Finally, we note that the preceding analysis has ignored the effect of gate errors due to photon loss. For the phase rotation gate and the control phase gate [$R(Z,\theta)$ and $R(Z\otimes Z,-\phi)$], the effect of photon loss is similar to that discussed above for the propagating qubit, that is, it produces sign flips in the computational basis. In reaching this conclusion we have considered loss events occurring, to the resource states, at the measurement site and, at the displacement. Hence errors in these gates can be corrected by the code discussed above. However, photon loss events in the superposition gate [$R(X,\pi/2)$] can produce bit flips in the computational basis if they occur at the measurement site. As a result, protecting a general circuit will require error correction for both sign flips and bit flips. This can be achieved by using the standard nine-qubit code [21] which can be implemented by a straightforward generalization of the techniques outlined in the preceding discussion.

It is likely that the application of more efficient codes [22] and optimization, in particular, exploiting the rarity of bit-flip vs sign-flip errors in a general circuit, can reduce the complexity of the required error correcting codes. We leave an investigation of this and the general question of fault tolerance levels for future research.

VI. CONCLUSION

In this paper we have presented a quantum computation scheme based on encoding qubits as coherent states of equal absolute amplitude but opposite sign. The optical networks required to manipulate the qubits are conceptually simple and require only linear interactions and photon counting, provided coherent superposition ancilla states are available (cat states). We have shown that qubits with amplitude $|\alpha|=2$ and resource cat states of amplitude $|\alpha|=\sqrt{6}$ would be sufficient. Accurate photon counting measurements of up to about ten photons would also be necessary.

We have discussed how the cat-state resources could be produced from squeezed sources, linear interactions, and photon counting in a simple scheme. This scheme appears capable of producing states suitable for proof of principle experiments. It seems likely though that more sophisticated schemes would be necessary for scalable systems.

The power of the scheme stems from the ability to generate entangled states and make Bell basis measurements with

simple linear interactions. This means teleportation protocols of various forms can be implemented deterministically to great effect.

A disadvantage of the scheme is that the multiphoton nature of the qubits makes them more susceptible to photon loss than single-photon qubits. However, we have shown how error correction can be employed in a straightforward way to counter this effect.

Being a simple optical system, the decoherence and control issues are well understood and with sufficient effort realistic evaluations of the resources and precision needed can be made. This level of understanding is not a feature of all quantum computer candidates. In addition to the long term goal of quantum computation, nearer term applications in quantum communication protocols appear possible.

ACKNOWLEDGMENTS

We thank Charles Hill for careful reading. S.G. acknowledges support from the Arthur J. Schmitt Foundation and thanks John LoSecco and Hilma Vasconcelos for valuable discussions. W.J.M. acknowledges funding in part by the European project EQUIP (Grant No. IST-1999-11053). A.G. was supported by the New Zealand Foundation for Research, Science and Technology under Grant No. UQSL0001. The Australian Research Council and ARDA supported this work.

[1] E. Knill, L. Laflamme, and G.J. Milburn, Nature (London) **409**, 46 (2001).
[2] T.C. Ralph, W.J. Munro, and G.J. Milburn, Proc. SPIE **4917**, 1 (2002); e-print quant-ph/0110115.
[3] S.L. Braunstein and H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[4] S. Lloyd and S.L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).
[5] S.D. Bartlett, Hubert de Guise, and B.C. Sanders, Phys. Rev. A **65**, 052316 (2002).
[6] H. Jeong and M.S. Kim, Phys. Rev. A **65**, 042305 (2002).
[7] D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A **64**, 012310 (2001).
[8] D.F. Walls and G.J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 1994).
[9] "Taking α real" means that the field is in phase with the local oscillator which is used for qubit measurement and to make the displacements required for some of the gates. The average intensity of all logical pulses is $I=\hbar\omega|\alpha|^2$ per bandwidth with ω the optical frequency.
[10] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[11] B. Misra and E.C.G. Sudarshan, J. Math. Phys. **18**, 756 (1977).
[12] D. Gottesman and I.L. Chuang, Nature (London) **402**, 390 (1999); M.A. Nielsen and I.L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[13] L. Krippner, W.J. Munro, and M.D. Reid, Phys. Rev. A **50**, 4330 (1994).
[14] S.J. van Enk and O. Hirota, Phys. Rev. A **64**, 022313 (2001).
[15] H. Jeong, M.S. Kim, and J. Lee, Phys. Rev. A **64**, 052308 (2001).
[16] M. Dakna *et al.*, Phys. Rev. A **55**, 3184 (1997).
[17] S. Song, C.M. Caves, and B. Yurke, Phys. Rev. A **41**, 5261 (1990).
[18] M.D. Srinivas and E.B. Davies, Opt. Acta **28**, 981 (1981).
[19] P. Cochrane, G.J. Milburn, and W.J. Munro, Phys. Rev. A **59**, 2631 (1999).
[20] D. Gottesman, Phys. Rev. A **54**, 1862 (1996); **57**, 127 (1998).
[21] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[22] R. Laflamme, C. Miquel, J.P. Paz, and W.H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).