Efficient linear optics quantum computation

Alexei Gilchrist
Macquarie University

Andrew Gerard White
The University of Queensland

Efficient Linear Optics Quantum Computation

E. Knill,[1,*] R. Laflamme,[1,†] and G. Milburn[2,‡]

[1]*Los Alamos National Laboratory, MS B265, Los Alamos, New Mexico 87545*

[2]*Center for Quantum Computer Technology, Department of Physics, University of Queensland, St. Lucia, Australia*

We investigate the computational power of passive and active linear optical elements and photo-detectors. We show that single photon sources, passive linear optics and photo-detectors are sufficient for implementing reliable quantum algorithms. Feedback from the detectors to the optical elements is required for this implementation. Without feedback, non-deterministic quantum computation is possible. A single photon source sufficient for quantum computation can be built with an active linear optical element (squeezer) and a photo-detector. The overheads associated with using only linear optics appear to be sufficiently low to make quantum computation based on our proposal a viable alternative.

I. INTRODUCTION

Quantum computers promise to greatly increase the efficiency of solving problems such as factoring large integers [1] and combinatorial optimization [2]. One of the greatest challenges now is to implement the basic quantum-computational elements in a physical system and demonstrate that they can be reliably and scalably controlled. One of the earliest proposals [3] for implementing quantum computation is based on encoding each qubit in two optical modes together containing exactly one photon. The main problem with this proposal is that it is extremely difficult to non-linearly couple two optical modes containing few photons. Here we consider the question of what can be accomplished in principle using various combinations of only the simplest optical elements: passive linear optics, photo-detectors, squeezers (an active linear optical element) and non-deterministic single photon sources. We show the surprising result that quantum computation is possible in principle using the first three of these. Only weak squeezing is required, and this only for single photon generation. Alternatively, any non-deterministic single photon source can be used. The optical elements must be controllable based on output from the photo-detectors. An alternative method relying on phase space based encodings, homodyne detection and an optical non-linearity in state preparation was independently presented by Gottesman and Preskill [4]. This establishes the principle of linear optics quantum computation (LOQC). Furthermore, the basic elements are testable in today's laboratories. Our non-deterministic optical gates may find immediate application in quantum communication, experiments with entanglement and optical state preparation. Spin-offs include near-deterministic quantum teleportation and a parity measurement for photon based qubits. Scalable quantum computation using our methods requires highly efficient photo-detectors, very low loss short term photon storage and long state preparation times to achieve the minimum accuracy required for reliable quantum computation. However, the theoretical overheads are sufficiently small compared to the implementation-independent requirements for scalability to suggest that LOQC is a viable proposal for implementing quantum computers.

We begin by briefly introducing the basic notions of bosonic modes and linear optics; give the representation of qubits using bosonic modes; describe the basic techniques required for implementing non-deterministic and and then deterministic quantum computation. We then consider scalability issues and argue that using quantum codes, the complexity of LOQC can be significantly reduced. We conclude with a discussion of the practical issues involved in using our methods. We assume some familiarity with quantum optics and quantum computation. An introduction to quantum optics can be found in [5]. An overview of quantum computation and implementation issues is in [6, 7].

II. BOSONIC MODES

To avoid issues surrounding the polarization states of photons we cast our work in terms of non-interacting spin-less bosons. Thus, the physical system of interest consists of a number of bosonic modes. A bosonic mode (or quantum harmonic oscillator) is a quantum system whose state space is spanned by the number states $|0\rangle, |1\rangle, |2\rangle, \ldots$. The modes are labeled and, with explicit labels, a number state of mode l is denoted by $|k\rangle_{l}$. The vacuum state, which satisfies that all modes are in state $|0\rangle$, is denoted by $|\mathbf{0}\rangle$. The observables for mode l can be constructed from the annihilation operator $\mathbf{a}^{(l)}$, which satisfies $\mathbf{a}^{(l)}|k\rangle_{l} = \sqrt{k}|k-1\rangle_{l}$ for $k \geq 1$ and $\mathbf{a}^{(l)}|0\rangle_{l} = 0$. $\mathbf{a}^{(l)\dagger}$ and $\mathbf{n}^{(l)} := \mathbf{a}^{(l)\dagger}\mathbf{a}^{(l)}$ are the creation and the number operator for this mode, respectively.

III. OPTICAL ELEMENTS

The most readily implementable processes are those given by passive linear optical elements. These are elements whose effect on the state of the mode are given by the following two Hamiltonians:

$$\begin{aligned} \mathbf{n}^{(l)} &:= \mathbf{a}^{(l)\dagger}\mathbf{a}^{(l)} && \text{(phase shifter)} \\ \mathbf{b}^{(lm)} &:= \mathbf{a}^{(l)}\mathbf{a}^{(m)\dagger} + \mathbf{a}^{(l)\dagger}\mathbf{a}^{(m)} && \text{(beam splitter).} \end{aligned} \tag{1}$$

*knill@lanl.gov
†laflamme@lanl.gov
‡milburn@physics.uq.edu.au

Evolutions implementable by passive linear optics preserve the total number of bosons in the modes. It is therefore convenient to describe them by their effect on the creation operators. Specifically, if U is the unitary operator associated with the evolution, then U takes the state $\mathbf{a}^{(l)\dagger}|\mathbf{0}\rangle$ to

$$U\mathbf{a}^{(l)\dagger}|\mathbf{0}\rangle = U\mathbf{a}^{(l)\dagger}U^\dagger|\mathbf{0}\rangle \tag{2}$$

$$= \sum_m U_{ml}\mathbf{a}^{(m)\dagger}|\mathbf{0}\rangle, \tag{3}$$

using the fact that $U^\dagger|\mathbf{0}\rangle = |\mathbf{0}\rangle$. The matrix defined by the coefficients U_{ml} must be unitary, and furthermore, for all unitary U_{ml}, there is a sequence of phase shifter and beam splitter evolutions that implements the corresponding operation up to a global phase [8]. For a named optical element X, let $U(X)$ be the unitary matrix associated with X according to the above rules. The unitary matrices associated with phase shifters $P_\theta{}^{(l)}$ and beam splitters $B_\theta{}^{(lm)}$ are:

$$U(P_\theta{}^{(1)}) = e^{i\theta}$$

$$U(B_\theta{}^{(12)}) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

General linear optical elements have Hamiltonians that consist of terms at most quadratic in the annihilation and creation operators. We will make use of the squeezer, an active linear element whose Hamiltonian is

$$\mathbf{s}^{(lm)} := \mathbf{a}^{(l)}\mathbf{a}^{(m)} + \mathbf{a}^{(l)\dagger}\mathbf{a}^{(m)\dagger}. \tag{4}$$

A mode can be prepared in its vacuum state $|0\rangle$. A nondeterministic single boson source prepares a given mode in the state $|1\rangle$ with some probability of success. It is assumed that the information on whether the source was successful is available classically.

Measurement is accomplished by means of a particle detector, which destructively determines whether one or more bosons were present in a mode. We assume that measurement results can be used to control other optical elements. A more powerful detector is a destructive particle counter, which returns the number of bosons present in a mode. An approximate particle counter that suffices for our purposes can be designed by using N particle detectors operating on N modes $l_1, \ldots, l_N$. To measure mode l, use passive linear optics to transform $\mathbf{a}^{(l)\dagger} \to \frac{1}{\sqrt{N}}\sum_{m=1}^N \mathbf{a}^{(l_m)\dagger}$, Each of the N modes is then measured using the corresponding particle detector. If mode l has k bosons, then the probability that some output mode has two or more bosons is at most $1 - \frac{(N)_k}{N^k} \le \frac{k(k-1)}{2N}$, where we define $(N)_k$ as the k'th falling factorial of N, given by $N(N-1)\ldots(N-k+1)$. Provided that the maximum number of photons is not too large, the number of bosons is, with high probability, the number of particle detectors that detect a boson. The bound on the error probability is required for estimating the resources needed to achieve sufficiently high accuracy for reliable quantum computation.

IV. REPRESENTING QUBITS

A qubit is a quantum system with two distinguished basis states, $|0\rangle_q$ and $|1\rangle_q$. Thus, the state space of a qubit generalizes that of a classical bit by allowing superpositions of the classical states. To represent a qubit using bosonic modes requires mapping the basis states unitarily into two states of one or more modes. We choose the traditional encoding using two modes and one boson, where $|0\rangle_q \to |0\rangle_a|1\rangle_b$ and $|1\rangle_q \to |1\rangle_a|0\rangle_b$, and call this a "bosonic qubit". For example, the two modes can be two orthogonal polarization states of an optical mode, so that the polarization state of a photon encodes the state of a qubit. With this encoding, the one qubit ($U(2)$) rotations are easy to implement using passive linear optics. In the case of encoding in polarization states, polarization rotators can be used in place of beam splitters.

To complete the implementation of a standard quantum computer, it is necessary be able to prepare the state of a qubit in $|0\rangle_q$, to measure a qubit in the standard basis $|0\rangle_q, |1\rangle_q$, and, in addition to the rotations above, to implement a controlled-not (c-not) and/or a controlled-sign (c-sign) gate [7]. The state preparation is accomplished here by using a single boson source to prepare mode a in $|1\rangle_a$ and mode b in $|0\rangle_b$. To measure a bosonic qubit it suffices to use a photo-detector on the first mode. Unfortunately, linear optics is insufficient for implementing the two qubit gates c-not and c-sign, which are defined in terms of unitary matrices acting on the four dimensional two-qubit state space by

$$\text{c-not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{5}$$

$$\text{c-sign} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \tag{6}$$

where the ordering $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ is used for the basis. Thus c-not flips the second qubit conditional on the first, and c-sign flips the sign of the second qubit conditional on the first. A direct bosonic implementation using a suitable Hamiltonian requires strong optical non-linearities. For example the c-sign gate could be implemented with a non-linear phase shift on the second halves of two bosonic qubits. The task of this work is to show how these operations can be induced using only single particle sources and particle detectors.

We conclude this section by introducing one more useful gate, the Hadamard transform on one qubit, defined by the matrix

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{7}$$

H can be implemented by a balanced beam splitter on bosonic qubits (to within a global phase). Note that c-not can be obtained from c-sign by conjugating the second qubit with the Hadamard transform (which is its own inverse).

V. NON-DETERMINISTIC QUANTUM COMPUTATION

A non-deterministic operation is one that succeeds only with probability <1, and whether it succeeded or not is known after it has been applied. It turns out that it is much easier to implement a non-deterministic non-linear phase shift rather than a deterministic one. These non-deterministic gates will also play a crucial role in preparing the states required for deterministic non-linear phase shifts. At the same time, having such a gate implies the ability to perform non-deterministic quantum computation (conditional on an acceptable measurement outcome at the end), general state preparation, and entanglement sharing through lossy systems. The basic nondeterministic gate we construct performs the transformation

$$NS_1 : \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle \;\rightarrow\; \alpha_0|0\rangle + \alpha_1|1\rangle - \alpha_2|2\rangle \quad \text{with probability } 1/4. \tag{8}$$

In order to implement the conditional sign flip c-sign on two bosonic qubits encoded in modes $1,2$ and $3,4$, respectively do the following: Apply the balanced beam splitter $B_{\pi/2}$ to modes 1 and 3. In the case where the two qubits are both in state $|1\rangle_q$, modes 1 and 3 are in the state $|11\rangle_{13}$, which transforms to $\frac{1}{\sqrt{2}}(|20\rangle_{13} + |02\rangle_{13})$. In none of the other cases do two bosons appear in the same mode. Now apply NS_1 to mode 1 and then to mode 3 and undo the balanced beam splitter. This has the desired effect with probability $1/16$.

The procedure for applying NS_1 to mode 1 begins with preparing the initial state $|10\rangle_{23}$ in ancilla modes 2 and 3. (The labels are chosen for convenience and are arbitrary.) Next a sequence of beam splitters is used to implement the symmetric unitary transformation

$$U = \begin{pmatrix} 1-2^{1/2} & 2^{-1/4} & (3/2^{1/2}-2)^{1/2} \\ 2^{-1/4} & 1/2 & 1/2-1/2^{1/2} \\ (3/2^{1/2}-2)^{1/2} & 1/2-1/2^{1/2} & 2^{1/2}-1/2 \end{pmatrix}. \tag{9}$$

Finally, modes 2 and 3 are measured, and the outcome is accepted only when the state is found to be $|10\rangle_{23}$, that is, the state is the same as the initial ancilla state. To check that this works, observe that due to particle conservation, the conditional state transformation is of the form

$$\alpha_0|0\rangle+\alpha_1|1\rangle+\alpha_2|2\rangle \rightarrow \lambda_0\alpha_0|0\rangle+\lambda_1\alpha_1|1\rangle+\lambda_2\alpha_2|2\rangle. \tag{10}$$

The λ_k are given by

$$\begin{aligned} \lambda_0 &= U_{22} \\ &= 1/2 \end{aligned} \tag{11}$$

$$\begin{aligned} \lambda_1 &= U_{11}U_{22} + U_{12}U_{21} \\ &= (1-2^{1/2})/2 + 2^{-1/2} \\ &= 1/2 \end{aligned} \tag{12}$$

$$\begin{aligned} \lambda_2 &= U_{11}(U_{11}U_{22} + 2U_{12}U_{21}) \\ &= U_{11}(U_{11}U_{22} + U_{12}U_{21}) + U_{11}U_{12}U_{21} \\ &= (1-2^{1/2})/2 + (1-2^{1/2})2^{-1/2} \\ &= -1/2 \end{aligned} \tag{13}$$

A direct calculation shows that U's columns are orthonormal.

VI. NEAR-DETERMINISTIC QUANTUM COMPUTATION

As noted earlier, it is in principle enough to implement a deterministic c-sign gate. Due to the results from fault tolerant quantum computing, it is acceptable for the gate to fail with a small probability (see Sect. VIII). The basic idea in implementing a near-deterministic c-sign gate with low error is to use ideas from quantum teleportation [9, 10]. The trick is to prepare an appropriate entangled state suitable for teleportation with the desired gate already applied, before using it for the teleportation protocol. The problem then becomes that of preparing the entangled state (which can be done non-deterministically) and implementing the requisite measurement in the protocol.

A. Quantum teleportation

A basic quantum teleportation protocol for transferring the state $\alpha_0|0\rangle_1 + \alpha_1|1\rangle_1$ to mode 3 first adjoins the "entangled" ancilla state $(|01\rangle_{23} + |10\rangle_{23})/\sqrt{2}$ to mode 1. Note that in this case, the ancilla state is easily generated from $|10\rangle_{23}$ by means of a beam splitter. The second step is to measure modes 1 and 2 in the basis $(|01\rangle_{12} \pm |10\rangle_{12})/\sqrt{2}, (|00\rangle_{12} \pm |11\rangle_{12})/\sqrt{2}$ (the "Bell basis"). We decompose the measurement into two steps. The first step determines the parity p of the number of bosons in modes 1 and 2 ("parity measurement"). The second determines the sign s in the superposition. Consider the case where $p=1$. Then if $s=$ '+', the state of mode 3 is $\alpha_0|0\rangle_3 + \alpha_1|1\rangle_3$. If $s=$ '-', the state is $\alpha_0|0\rangle_3 - \alpha_1|1\rangle_3$, which can be restored to the starting state by using a phase shifter. For $p=0$, the situation is similar except that $|0\rangle_3$ and $|1\rangle_3$ are flipped (and cannot be easily un-flipped using linear optics). The key property of quantum teleportation is that the input state appears in mode 3 up to a simple transformation without having interacted with mode 3 after the preparation of the initial ancilla state.

Consider the parity measurement. Applying a balanced beam splitter to modes 1 and 2 and then measuring the number of photons in the two modes successfully determines the parity, and if it is odd, the sign. As a result, this measurement method can be used to perform the teleportation with success probability $1/2$. We refer to this partial Bell-state measurement as *BM₁*.

Two teleportation steps using *BM₁* can be used to implement c-sign with success probability $1/4$. To see how to do this, observe that to implement c-sign on two bosonic qubits in modes $1,2$ and $3,4$ respectively, we could try to first teleport the second modes of each qubit to two new modes (labelled 6 and 8) and then apply c-sign to the new modes. The full teleportation procedure requires a correction step that consists of applying a Pauli operator (nothing, sign-flip, bit-flip, or their product) to each new mode. Since c-sign is in the normalizer of the group generated by the Pauli operators, the correction step can be deferred until after applying c-sign. Of course, now there is nothing preventing us from applying c-sign to the prepared entangled state before performing the measurement. Thus the implementation of c-sign is now reduced to the problem of preparing a modified four mode entangled state $|b'_4\rangle_{5678}$, then implementing the Bell measurement and correcting the resulting state in the new modes. The modified entangled state is given by

$$|b'_4\rangle = (|1010\rangle + |0110\rangle + |1001\rangle - |0101\rangle)/2. \quad (14)$$

$|b'_4\rangle$ can be generated with linear optics by following the sequence

$$\begin{aligned} |01\rangle|01\rangle &\rightarrow (|01\rangle + |10\rangle)(|01\rangle + |10\rangle)/2 \quad \text{(with two } B_{\pi/2}\text{)} \\ &\rightarrow |b'_4\rangle \quad \text{(with } NS_1\text{)}. \end{aligned} \quad (15)$$

The success probability of this procedure is $1/16$, which means that the expected effort for obtaining one instance of $|b'_4\rangle$ requires 16 trials of the sequence above. Once such an instance is obtained, we can use two BM_1 measurements followed by phase corrections to implement c-sign on two input bosonic qubits with success probability $1/4$. To increase the success probability further we can either change the teleportation procedure or improve on the parity measurement. We next show how to teleport nearly deterministically and how to use this for a near-deterministic c-sign.

B. Near-deterministic quantum teleportation with beam splitters

An initial entanglement that results in successful teleportation with probability of success $1/(n+1)$ is given by

$$|t_n\rangle = \sum_{j=0}^{n} |1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j}, \quad (16)$$

where we omitted normalization constants. The notation $|a\rangle^j$ means $|a\rangle|a\rangle\ldots$, j times. Note that if we label the modes $1\ldots 2n$ (left to right), the state exists in the space of n bosonic qubits, where the k'th qubit is encoded in modes k and $n+k$. Also, $|t_1\rangle$ is the same as the entanglement used in the basic teleportation protocol of the previous section.

The teleportation protocol using state $|t_n\rangle$ teleports mode 0 (say) in a superposition of $|0\rangle$ and $|1\rangle$ to one of the last n modes of $|t_n\rangle$ by a measurement BM_n involving only the mode to be teleported and the first n modes of $|t_n\rangle$. The measurement BM_n is implemented using an $n+1$ point Fourier transform. Let $\hat{F}_n$ be the unitary matrix defined by

$$(\hat{F}_n)_{kl} = \omega^{kl}/\sqrt{n+1}, \quad (17)$$

where $\omega = e^{i2\pi/(n+1)}$ and $k, l \in 0\ldots n$. $\hat{F}_n$ is unitary and therefore implementable with passive linear optics. Using the parallel fast Fourier transform (see page 795 of [11]), it can be implemented with $O(n\log(n))$ elements and depth $O(\log(n))$, for n a power of 2. Alternatively, a multiport interferometer can be used [12]. Denote the optical array for implementing $\hat{F}_n$ by F_n. To perform BM_n apply F_n to modes $0\ldots n$ and measure the number of bosons in each of these modes. Suppose we detect k bosons altogether. We claim that if $0 < k < n+1$, then the teleported state appears in mode $n+k$ and only needs to be corrected by applying a phase shift. The modes $2n-l$ are in state 1 for $0 \le l < (n-k)$ and can be reused in future preparations requiring single bosons. The modes are in state 0 for $n-k < l < n$. If $k=0$ we learn that the input state is measured and projected to $|0\rangle_0$ and if $k = n+1$, it is projected to $|1\rangle_0$. The probability of these two events is $1/(n+1)$, regardless of the input. We will make use of the fact that failure is detected and corresponds to measurements in the basis $|0\rangle, |1\rangle$ with the outcome known. Note that both the necessary correction and which mode we teleported to are unknown until after the measurement.

To prove the claim, observe that applying $P_{2\pi k/(n+1)}$ to mode k for $0 \le k \le n$ after applying F_n is equivalent to shifting modes $0\ldots n$ circularly right before applying F_n. This means that the states $|x_1\rangle = F_n|1\rangle^k|0\rangle^{n-k+1}$ and $|x_2\rangle = F_n|0\rangle|1\rangle^k|0\rangle^{n-k}$ differ only by phases in the number basis. Thus the measurement BM_n cannot distinguish between the two states. If the measurement detects r_j bosons in mode j ($\sum_j r_j = k$ in this case), then the relative phase of the second state is given by $\prod_j \omega^{r_j j}$. Because of the way $|t_n\rangle$ is entangled with the last n modes, the measurement outcome transfers a superposition of $|x_1\rangle$ and $|x_2\rangle$ in the entanglement to a superposition in mode $2n-k+1$. The remaining properties of the claim are immediate.

The teleportation trick to improve the probability of success of c-sign can be used with $|t_n\rangle$ also. The necessary modification of $|t_n\rangle_{1\ldots 2n}|t_n\rangle_{2n+1\ldots 4n}$ to teleport two modes with an effective application of c-sign is accomplished by applying c-sign to each pair of modes $(n+k, 3n+l)$ with k and l in $1\ldots n$. This works up to qubit sign flips because the output modes that do not receive the teleported state are in known configurations after the procedure. Explicitly, the state that needs to be prepared is given by

$$\begin{aligned} |t'_n\rangle &= \sum_{i,j=0}^{n} (-1)^{(n-j)(n-i)} |1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j} \\ &\quad \times |1\rangle^i|0\rangle^{n-i}|0\rangle^i|1\rangle^{n-i}. \end{aligned} \quad (18)$$

We note a few features of this method of implementing c-sign that will prove useful when using quantum error-correction to boost reliability. The first step in the implementation of c-sign using $|t'_n\rangle$ is to perform BM_n on the first qubit and the first n modes of $|t'_n\rangle$. With probability $1/(n+1)$, the measurement fails, and the first qubit is measured in the standard basis with a known outcome. If this happen we do not attempt to complete the protocol so that the second qubit remains coherent. If the first measurement succeeds, the correction step is applied. Note that as it only adjusts the phase, it commutes with the implemented operation. Next BM_n is applied to the second qubit and the third n modes of $|t'_n\rangle$. With probability $1/(n+1)$, this fails and the second qubit is measured in the standard basis with known outcome. The outcome affects whether or not the first qubit experienced a sign flip, which can be corrected with a phase shifter to restore it to its original coherent state.

C. State preparation algorithm

We have reduced the problem of implementing a near-deterministic c-sign to generating the state $|t'_n\rangle$. Clearly this can be done by first generating two copies of $|t_n\rangle$ and then applying the $O(n^2)$ c-sign operations. Since $|t_n\rangle$ is a uniform superposition of simple bosonic qubit states (the unary numbers from 0 to n), it is not hard to see how to construct a quantum network with $O(n)$ gates from an initial state accessible with single boson sources. Together this gives $O(n^2)$ gates, which can be implemented non-deterministically. Although n needs to be no larger than some constant (pessimistically no more than 25, see Sect. VIII, implying existence of techniques with asymptotically efficient resource usage), both the number of gates and the way in which non-deterministic gates are used needs to be improved. The remainder of this section is dedicated to this task.

We begin by generating a variant of $|t_n\rangle$ with an ancilla bosonic qubit that contains parity information about the states in the superposition:

$$|tp_n\rangle \;=\; \sum_{j=0}^{n} |1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j} \times|(n-j) \bmod(2)\rangle_{a_1}|(n-j+1) \bmod(2)\rangle_{a_2}. \tag{19}$$

To prepare $|t'_n\rangle$ one can first prepare two copies of $|tp_n\rangle$, apply c-sign to the two ancilla qubits, apply $B_{\pi/2}$ to each ancilla qubit and measure them. There are four equiprobable outcomes to the measurement, which differ from the desired state $|t'_n\rangle$ only by signs, which can be undone by applying P_π to the last n modes of one or both halves of the component states. This involves $O(n)$ individual steps, only one of which requires a non-deterministic element.

To prepare state $|tp_n\rangle$, begin with the state $(|1\rangle^n|0\rangle^n + \sqrt{n}|1\rangle^{n-1}|0\rangle|0\rangle^{n-1}|1\rangle)(|01\rangle+|10\rangle)$, which can be generated from a product of single boson states by applying beam splitters to modes n and $2n$ and to the ancilla modes. Apply c-sign to modes $2n$ and $2n+1$. Let q_l be the qubit encoded in modes l and $n+l$ and a the ancilla qubit. The l'th step ($0 \le l \le n-1$) consists of

1 Conditionally on qubit q_{n-l} being in the state $|01\rangle$, apply B_{θ_l} to qubit q_{n-l-1}, with $\tan(\theta_l) = \sqrt{n-l-1}$.

2 Apply c-sign to modes $2n-l-1$ and $2n+1$.

At the end undo the beam splitter operation on the ancilla qubit. $O(n)$ operations are required for implementing this algorithm and $O(n)$ of these are based on gates that we can only do non-deterministically. The steps of the algorithm can be implemented with c-sign, beam splitters and phase shifters using (for example) the methods of [13]. For example, the conditional beam splitter is obtained by conjugating a beam splitter on the target by c-sign and following that with the inverse beam splitter. As this requires two c-sign operations, it may be more efficient to directly implement a conditional phase shift for phases other than -1 and then to conjugate this by a one qubit rotation to implement the required conditional beam splitter. If this is done by using an instance of our teleportation schemes (e.g. with $n=1$), then the built in error detection may be exploited to achieve some error recovery. In particular, of the two failure modes for a gate implemented by teleportation, one results in a state that is essentially a $|tp_l\rangle$ for $l < k$. This state can be used for improvements in the probability of success for the operations required when re-attempting the construction of $|tp_n\rangle$.

The non-deterministic aspects of the method for preparing $|tp_n\rangle$ complicate the resource analysis. Let $S(n)$ be the expected number of elementary operations needed to prepare $|tp_n\rangle$. If we do not attempt to recover from failure, nor exploit improvements in the probability of success by using $|tp_k\rangle$ for $k < n$, then the probability of success would be $\frac{1}{4}^{O(n)}$, leading to $S(n) = 4^{O(n)}$ exponentially large.

Using $|tp_k\rangle$ recursively leads to a subexponential method as the following argument shows: Except for differences in rotation angles, the algorithm for preparing $|tp_n\rangle$ looks like the algorithm for preparing $|tp_{n-1}\rangle$ followed by $< C$ non-deterministic operations (for some constant C). Suppose we use $2C$ $|tp_{\sqrt{n}}\rangle$ for these operations. Each of these states requires $S(\sqrt{n})$ operations and their application has an additional overhead of $\le D\sqrt{n}$. The success probability is is now $1-1/\sqrt{n}$. Therefore, $S(n) \le (1-1/\sqrt{n})^{-2C}(S(n-1) + 2C(S(\sqrt{n}) + D\sqrt{n}))$. Under the assumption that $S(n) = \Omega(\sqrt{n})$, $S(n) \le (1+C_1/\sqrt{n})(S(n-1)+C_2S(\sqrt{n}))$ for suitable choices of the constants. This implies that $S(n) = 2^{O(\sqrt{n})}$.

D. Near-deterministic loss detection and non-destructive parity measurement

Our constructions so far assume essentially perfect optical gates and detectors. Unfortunately, loss of bosons is one of the primary error mechanisms. Since this implies "leakage" errors for the bosonic qubits, scalability requires a non-destructive method for detecting when the modes supporting a qubit are no longer in a state associated with the bosonic qubit and returning them to a qubit state. Fortunately, our methods can be adapted to yield a non-destructive parity measurement for the space spanned by the states $|00\rangle, |10\rangle, |01\rangle, |11\rangle$. In order to implement such a measurement, it is sufficient to follow the procedure used for teleporting the c-sign gate, but using instead of $|tp_n\rangle$ the state

$$|p'_n\rangle \;=\; \sum_{i,j:i+j=0(2)} |1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j} \times|1\rangle^i|0\rangle^{n-i}|0\rangle^i|1\rangle^{n-i}. \tag{20}$$

(21)

The measurement determines whether the number of bosons in the two input modes is even or odd, and the conditional state can be extracted from the output modes after suitable phase shifts. The state can be prepared using a simple variation of the method for preparing $|t'_n\rangle$, using only one ancilla qubit for keeping track of the total parity. Measurement of the ancilla at the end yields either $|p'_n\rangle$ or the odd variant, which is equally useful.

The above loss detection method is incomplete for detecting leakage in one respect: it does not detect when a mode has two or more bosons. However, it is sufficient for the experimental procedures to guarantee return to the coding state with sufficiently high probability, that is, the loss need not be detected by the user. Although the information is lost in the process without that loss being detected, this is in principle sufficient for meeting the scalability requirements. The teleportation methods described earlier for implementing various gates ensure that each output mode has at most one boson. By using them sufficiently frequently on both halves of a bosonic qubit, return to the state space where loss can be detected is thus adequately assured.

Another application of the non-destructive parity measurement is to the teleportation of a bosonic qubit using the traditional entangled state $|E\rangle = |0110\rangle - |1001\rangle$. The initial state is $(\alpha_0|01\rangle + \alpha_1|10\rangle)|E\rangle$ on modes $1, 2, 3, 4, 5$ and 6, say. The Bell measurement requires measuring in the basis $|0110\rangle \pm |1001\rangle$ and $|0101\rangle \pm |1010\rangle$ This has been implemented experimentally with some probability of failure [14, 15, 16]. A non-destructive parity measurement on modes 2 and 3 determines which of the two pairs of basis states are present. The sign can then be determined by applying two balanced beam splitters to modes $1, 2$ and $3, 4$ before measuring the four modes.

To conclude this section, observe that the entanglement needed for teleportation can be produced locally, non-deterministically by performing the non-destructive parity measurement on modes $1, 2$ of the non-traditional entangled state $(|01\rangle_{1,3} - |10\rangle_{1,3})(|01\rangle_{2,4} + |10\rangle_{2,4}$ and accepting if the parity is odd. Of course, an appropriate entangled state is still used locally inside the parity measurement, but this one may be generated locally, perhaps using the techniques of this paper. The curious feature is that the distribution of the entanglement requires only two independent bosons sent by means of beam splitters. The rest is taken care of by classical communication.

VII. SINGLE BOSONS USING ACTIVE LINEAR OPTICS

The need for non-linearities to create single boson states can be eliminated using weak squeezing and particle detectors [17]. A non-degenerate squeezer on modes 1 and 2 applies the Hamiltonian $\mathbf{s}^{(12)}$ given in Eq. 4. When applied to the vacuum, the output consists of a superposition of states with identical numbers of bosons in the two modes. Under weak squeezing conditions, the relative amplitudes of states with a total of $2n$ bosons decrease exponentially with n. Thus a single boson can be produced in mode 1 conditional on detection of at least one in mode 2. The output state has arbitrarily large overlap with the desired single boson state. The overlap is one in the limit of weak squeezing. If we can count bosons in mode 2, the reliability of the conditional output is even better.

VIII. RELIABLE SCALABILITY

That quantum computing is scalable in principle is a consequence of the accuracy threshold theorem [18, 19, 20, 21]. According to this theorem, the main requirement for efficient scalability of a physical implementation of quantum computation is that the elementary operations can be implemented with a minimum accuracy, which is currently estimated to be less than $1 - 10^{-4}$ [22]. Although achieving such accuracy may seem like a daunting task, in practice, errors behave much more predictably than assumed in the general analyses, and experience shows that at least some aspects of many quantum experiments are controllable with accuracies above the threshold. A typical example is the phase of RF pulses in nuclear magnetic resonance. Such accuracies can be exploited to “boost” the accuracy of other gate parameters.

Achieving the necessary accuracy for the methods introduced in this work is clearly not practical without additional work. For example, to implement a single two qubit gate with error rate $< 10^{-4}$ would require $2 * 10^4$ modes, half of which are initially loaded with single bosons. To get the necessary prepared state would require a very large number of tries indeed. To avoid doing this we take advantage of the fact that ideally, it is always known when a gate fails. Thus, we begin by assuming that all optical operations (beam splitters, phase shifters, single boson state preparation, number state measurement) are perfect. Under this assumption, the threshold can be greatly improved by exploiting quantum erasure codes [23], yielding an “erasure threshold”. Given the special nature of the detected errors in our system, we are actually interested in an even more benign threshold T_d. This results in quantum code enhanced systems, where qubits are highly protected in specially coded states. One can then estimate how errors in the operations propagate to errors in specific instances of such systems and apply the general threshold to obtain an estimate of the minimum accuracy required. Most importantly, the overhead associated with using linear optics is directly related to T_d via the complexity of the necessary erasure code implementation. We pessimistically estimate T_d to be well below $.96$, which implies that scalability is achievable using our teleportation protocols with size parameter $n \leq 25$. This still implies substantial overheads, albeit far from what might have been expected. The quantum code constructions that lead to our estimate of T_d and more detailed resource analyses are in [24].

IX. EXPERIMENTAL REQUIREMENTS

A crucial question is to what extent the methods of the previous sections can be implemented experimentally. Although large scale quantum computation is clearly still out of reach with current technology, many of the elements can be tested using existing equipment. For example, the non-deterministic c-sign requires only three modes and one ancilla single photon. Similarly, the simplest methods for generating highly entangled states or for teleportation with parity measurements require reasonable overheads.

It is relatively easy to couple two optical modes at a single beam splitter. As subsequent beam splitters are added however careful spatial and temporal mode matching is required, otherwise unwanted modes could be mixed in representing loss channels. Fortunately a four mode experiment could be achieved using only two spatial modes together with the two polarization degrees of freedom for each. The price would be to add a requirement for polarizing beam splitters, together with controllable polarizers (Faraday rotators), to enable flexibility in linear coupling and to separate the polarization modes for detection.

The requirement of single photon sources is a more difficult constraint to satisfy with available technology. To some extent this is mitigated by the conditional preparation of the non deterministic phase shift; while the time at which the gate is applied is random, we do know when it has occurred. One way around this difficulty is to use a pulse-trigger to indicate that temporally correlated photon pairs are incident to the device. For example, in the case of the non-deterministic c-sign method, a three mode state with a total of three photons, together with an ancilla mode in the vacuum state is required. The three mode state can be generated using a method similar to that used to generate a GHZ state[25] via a type II parametric down converter with a suitable arrangement of polarizing beam splitters. To second order in the pump amplitude, the result is a four mode state with at most four photons in total. Conditioning on a single count in a time window for one of the four outputs distributes three photons across the other three modes. Subsequent processing could then yield the required input states to the non deterministic c-sign protocol. The considerable disadvantage of this approach is the very low probability of required states per run. Single photon sources however are not far away. The turnstile proposal of [26] or the SAW method of [27] could yield pulses of light with a predefined maximum number of photons per pulse, synchronized to an electronic clock signal. Optical delay line methods could then be used to bring single photon pulses together at a particular time and place. Of course single photon detectors with high quantum efficiency will be required in all cases.

In an experiment it would be necessary to be able to distinguish that the required controlled phase shift had been implemented in a successful run. The simplest way to do this is to use a double path interferometer with a controlled phase shift introduced in one arm only. The input signal state is then split at a 50/50 beam splitter at the input to the device, passes along two arms and is then recombined at an output beam splitter. In the absence of a phase shift the interferometer could be adjusted to transmit the input state with unit probability at a single output port. When the phase shift is introduced however this probability would change as “which path” information is imprinted by the conditional phase shift. In essence the total experiment, including the conditional state preparation, is a kind of four photon coincidence experiment.

X. DISCUSSION

The ability to implement quantum computation with linear optics and particle detectors realizes the dream of computing with non-interacting particles. The only particle interactions occur implicitly in the detectors and result in particle destruction. The present work shows how to do this for bosons, but similar techniques work for fermions, which have the property that the creation operators satisfy anti-commutation laws. This greatly improves on previous methods for implementing quantum networks with linear optics [28, 29, 30], which require an exponential number of modes to represent the state space of n qubits. It solves a problem we first learned from Paul Kwiat, who asked what the computational power of prepared entanglement in optics is. Other studies of quantum computation with harmonic oscillators or continuous variables have depended on non-linear effects either for quantum gates [3, 31, 32, 33] or for state preparation [4].

LOQC is related to the observation that in the usual model of quantum computation, it suffices to be able to implement operations in the normalizer of the Pauli group, provided one non-stabilizer state can be generated, such as the state $\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ [20], or a non-stabilizer measurement can be performed, such as that of the Hadamard operator H. Linear optical elements generate the normalizer of the continuous version of the Pauli group. This group is given by products of operators of the form $e^{-it(\mathbf{a}+\mathbf{a}^\dagger)}$ and $e^{-t(\mathbf{a}-\mathbf{a}^\dagger)}$, which correspond to translations in phase space. From this point of view, the vacuum state preparation and particle detectors serve the purpose of the non-stabilizer state and measurement, respectively.

Even though LOQC is no more practical given current technology than any of the other proposals, many of the basic elements can be tested, and there are numerous other applications in quantum information processing. For example, our methods can be used to generate complex entangled states with higher efficiency than is possible by using sequential down-conversion sources. The non-destructive parity measurement can be used for implementing standard quantum teleportation essentially unconditionally. In general our methods yield complex quantum non-demolition measurements. Since quantum communication is substantially less demanding than quantum computation (as demonstrated by its much better thresholds [34]), our methods are closer to being practical for implementations of quantum channels, particularly when relatively low success probabilities are acceptable, such as in quantum cryptography. Note that quantum optics is likely to dominate the important communication sector of quantum information processing regardless of how quantum computation is finally implemented.

Another approach to implementing quantum computation optically is to use non-linear optical elements. Assuming that such elements are available, though perhaps with high losses, it may be possible to combine techniques from LOQC with these elements to significantly reduce the introduced errors.

More work is required to optimize the resources required for LOQC. Clearly the suggestions made here are just the beginning and we believe that significant improvements are possible. From a theoretical point of view it would be nice to establish lower bounds on the complexity of various elementary gates depending on the desired probability of failure.

Acknowledgments: We thank the Aspen Center for Physics for its hospitality. We are grateful to Paul Kwiat for his suggesting the problem to us and for his help with the references. E.K. and R.L. received support from the NSA and from the DOE (contract W-7405-ENG-36).

[1] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
[2] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[3] G. J. Milburn, Phys. Rev. Lett. **62**, 2124 (1988).
[4] D. Gottesman and J. Preskill (2000), talk at the Aspen Physics Center, June 7, 2000.
[5] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 1994).
[6] Y. Aharonov and J. Anandan, *Meaning of the Density Matrix* (1998), quant-ph/9803018.
[7] D. DiVincenzo, *The Physical Implementation of Quantum Computation* (2000), to appear in *Fort. Phys.*, special issue on “Experimental Proposals for Quantum Computation”. quant-ph/0002077.
[8] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[9] C. H. Bennett, G. Brassard, C. Crepau, R. Josza, A. Peres, and W. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).
[10] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).
[11] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introcution to Algorithms* (MIT Press, Cambridge, Mass, 1990).
[12] G. Weihs, M. Reck, H. Weinfurter, and A. Zeilinger, Opt. Lett. **21**, 302 (1996).
[13] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[14] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature **390**, 575 (1997).
[15] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).
[16] A. Furusawa, J. L. Sorenson, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).
[17] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986).
[18] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)* (ACM Press, New York, New York, 1996), pp. 176–188.
[19] A. Y. Kitaev, Uspekhi Mat. Nauk. **52**, 53 (1997).
[20] E. Knill, R. Laflamme, and W. H. Zurek, Science **279**, 342 (1998).
[21] J. Preskill, Proc. R. Soc. Lond. A **454**, 385 (1998).
[22] D. Gottesman and J. Preskill (1999), unpublished analysis of the accuracy threshold.
[23] M. Grassl, T. Beth, and T. Pellizari, Phys. Rev. A **56**, 33 (1997).
[24] E. Knill, R. Laflamme, and G. Milburn, *Thresholds for Linear Optics Quantum Computation* (2000), available by request from `knill@lanl.gov`.
[25] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
[26] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature **397**, 500 (1999).
[27] C. L. Foden, V. I. Talyanskii, G. J. Milburn, M. L. Leadbeater, and M. Pepper, *High Frequency Acousto-electric Single Photon Source* (2000), quant-ph/0004079.
[28] N. J. Cerf, C. Adami, and P. G. Kwiat, Phys. Rev. A **57**, R1477 (1998).
[29] J. C. Howell and J. A. Yeazell, Phys. Rev. A **61**, 052303/1 (2000).
[30] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White, J. Mod. Optics **47**, 257 (2000).
[31] J. C. Howell and J. A. Yeazell, *Quantum Communication Through Entangling Single Photons In Multipath Interferometers* (2000), to appear.
[32] S. L. Braunstein, Nature **394**, 47 (1998).
[33] S. Lloyd and S. M. Braunstein, Phys. Rev. Lett. **82**, 1784 (1998).
[34] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum Repeaters for Communication* (1998), quant-ph/9803056.