A scheme for efficient quantum computation with linear optics

E. Knill*, R. Laflamme* & G. J. Milburn†

* *Los Alamos National Laboratory, MS B265, Los Alamos, New Mexico 87545, USA*
† *Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Australia*

Quantum computers promise to increase greatly the efficiency of solving problems such as factoring large integers, combinatorial optimization and quantum physics simulation. One of the greatest challenges now is to implement the basic quantum-computational elements in a physical system and to demonstrate that they can be reliably and scalably controlled. One of the earliest proposals for quantum computation is based on implementing a quantum bit with two optical modes containing one photon. The proposal is appealing because of the ease with which photon interference can be observed. Until now, it suffered from the requirement for non-linear couplings between optical modes containing few photons. Here we show that efficient quantum computation is possible using only beam splitters, phase shifters, single photon sources and photo-detectors. Our methods exploit feedback from photo-detectors and are robust against errors from photon loss and detector inefficiency. The basic elements are accessible to experimental investigation with current technology.

Quantum information processing (QIP) uses quantum mechanics for information storage, communication and computation. It enables large improvements in computational efficiency and communication security by exploiting the superposition principle and non-classical correlations of quantum mechanics. Examples include Shor's quantum algorithm for factoring large integers[1], Grover's algorithm for accelerating combinatorial searches[2] and quantum cryptography for secure communication[3,4]. Initial concern that quantum coherence may be too fragile to be exploited has been dispelled by theoretical work showing that noise and decoherence are not fundamental obstacles to the implementation of QIP[5–10]. Consequently, increasing effort is being devoted towards physically realizing quantum computers, and there are many proposals for implementing the necessary quantum devices. Examples of promising technologies include ion traps, quantum dots, Josephson junctions, nuclear spins in silicon and nuclear spins in molecules[11].

Quantum effects are particularly easy to observe in optical systems, and it is therefore not surprising that one of the earliest proposals for QIP uses photons to implement quantum logic[12]. Optical systems currently constitute the only realistic proposal for long-distance quantum communication and underlie experimental implementations of quantum cryptography[13–15]. Until now the main obstacle to scalable optical QIP was the apparent need for nonlinear couplings between optical modes. Achieving such couplings at sufficient strengths is possible in principle but is technically difficult[16]. As a result, other proposals[17–19] for using linear optics to benchmark quantum algorithms require exponentially large physical resources.

Here we show the surprising[20] result that linear optics is sufficient for efficient QIP with photons. Efficiency in the sense of the theory of computation means with polynomial resources, and we achieve low linear resources. Our proposal for QIP with linear optics requires single photon sources (implementable with active linear optics[21]), beam splitters, phase shifters, photo-detectors, and feedback from photo-detector outputs. A quantum bit (qubit) is realized by one photon in two optical modes (such as horizontal or vertical polarization). Efficient QIP is established by means of three results, each of which constitutes a breakthrough in linear optics QIP. The first result implies that non-deterministic quantum computation[22] is possible with linear optics. It is based on a non-linear sign shift between two qubits that uses two additional photons and post-selection. The sign shift succeeds with probability 1/16, and whether or not it succeeded is known. Although there are no practical applications of non-deterministic quantum computation, it implies that linear optics has features not available to classical deterministic or probabilistic computation. The second result shows that the probability of success of the quantum gates can be increased arbitrarily close to one. The result is based on using entangled states prepared non-deterministically and quantum teleportation[23,24]. Thus quantum computation is possible in principle with linear optics. The resources needed to make the probability of success close to one with these methods are extremely demanding. The third result shows that with quantum coding, the resources for obtaining accurate encoded qubits are very efficient with respect to the accuracy achieved, thus completing the goal of efficient linear optics quantum computation (LOQC). The coding methods can be adapted to make LOQC fault-tolerant for photon loss, detector inefficiency and phase decoherence. As a result, LOQC can be robustly implemented with resources low enough to suggest practical scalability, making it as promising a technology for QIP as are other proposals.

Bosonic qubits and optical elements

The fundamental units of QIP are qubits, the quantum generalizations of classical bits. A qubit's state space consists of all superpositions $\alpha|0\rangle + \beta|1\rangle$ ($|\alpha|^2 + |\beta|^2 = 1$) of the basic states $|0\rangle$ and $|1\rangle$. A set of qubits can be realized by independent two-state subsystems of a physical system. Bosonic qubits are defined by states of optical modes. An optical mode is a physical system whose state space consists of superpositions of the number states $|n\rangle$, where $n = 0, 1, 2, \ldots$ gives the number of photons in the mode. When we consider several qubits or modes, we use labels to distinguish between them. For example, $|20\rangle_{lm}$ (short for $|2\rangle_l|0\rangle_m$) is a state where modes l and m have two and zero photons, respectively. The basic states of a bosonic qubit encoded in modes l_1 and l_2 are $|0\rangle \rightarrow |0\rangle_{l_1}|1\rangle_{l_2}$ and $|1\rangle \rightarrow |1\rangle_{l_1}|0\rangle_{l_2}$. For comprehensive treatments of quantum optics and QIP, see the references[25–27].

In addition to instances of an ideal quantum system, a complete implementation of a quantum computer requires a means for state preparation, the ability to apply sufficiently powerful quantum gates, and a readout method. To process information, these elements are combined in quantum networks (see Box 1). The initial state is the vacuum state $|\mathbf{0}\rangle$, in which there are no photons in any of

the modes to be used. The basic element that adds photons to the initial state is a single photon source. It can be used to set the state of any given mode to the one-photon state $|1\rangle$. It is sufficient to be able to prepare this state non-deterministically. This means that the state preparation has a non-zero probability of success, and whether or not it succeeded is known.

The simplest optical elements are phase shifters and beam splitters. These elements generate the evolutions implementable by passive linear optics. These evolutions preserve the total photon number, and can be described by their effects on each mode's creation operator, which is defined by $\mathbf{a}^{(l)\dagger}|n\rangle_l = \sqrt{n+1}|n+1\rangle_l$. Let U be the unitary operator applied to a state by such an evolution. Using $U|\mathbf{0}\rangle = |\mathbf{0}\rangle$ gives $U\mathbf{a}^{(l)\dagger}|\mathbf{0}\rangle = U\mathbf{a}^{(l)\dagger}U^\dagger U|\mathbf{0}\rangle = U\mathbf{a}^{(l)\dagger}U^\dagger|\mathbf{0}\rangle = \Sigma_k u_{kl}\mathbf{a}^{(k)\dagger}|\mathbf{0}\rangle$. The coefficients u_{kl} introduced by these equations define a matrix u that must be unitary. Conversely, for every unitary u there is a sequence of phase shifters and beam splitters that implements the corresponding operation up to a global phase[28]. For a named optical element X, let $u(X)$ be the unitary matrix associated with X according to the above rules. The unitary matrix associated with phase shifter $\mathbf{P}_\theta$ is $u(\mathbf{P}_\theta) = e^{i\theta}$. The unitary matrix associated with beam splitter $\mathbf{B}_{\theta,\phi}$ is

$$u(\mathbf{B}_{\theta,\phi}) = \begin{pmatrix} \cos(\theta) & -e^{i\phi}\sin(\theta) \\ e^{-i\phi}\sin(\theta) & \cos(\theta) \end{pmatrix} \quad (1)$$

We define $\mathbf{B}_\theta = \mathbf{B}_{\theta,0}$.

Phase shifters and beam splitters applied to a bosonic qubit's modes preserve the qubit state space. Their effect can therefore be expressed in the qubit basis using the standard Pauli operators σ_x, σ_y and σ_z. For example, $\mathbf{P}_\theta^{(1)}$ applies $\exp(-i\sigma_z\theta/2)$ up to a global phase shift, and $\mathbf{B}_\theta^{(12)}$ applies $\exp(-i\sigma_y\theta)$. It follows that all one-qubit rotations can be implemented with linear optics. To achieve the full power of quantum computation we require a two-qubit gate such as the conditional sign flip c–z defined by $|a\rangle|b\rangle \rightarrow (-1)^{ab}|a\rangle|b\rangle$, where $a, b = 0,1$ and labels have been omitted.

Readout is accomplished by measuring a mode with a photo-detector, which destructively determines whether one or more photons are present in a mode. We assume that photo-detectors can be applied at any time and that the measurement result can be used to control other optical elements. We need a photon counter, which destructively counts the number of photons in a mode. An approximate photon counter that suffices for our purposes can be designed by using beam splitters and multiple photo-detectors. To measure a mode, we can use beam splitters to distribute the mode's photons evenly over N modes and use a photo-detector on each. The desired count is the number of detectors that 'see' photons. The probability of undercounting given that the photon number is k is at most $k(k-1)/(2N)$. For LOQC, $k \leqslant 4$.

Nondeterministic conditional sign flip

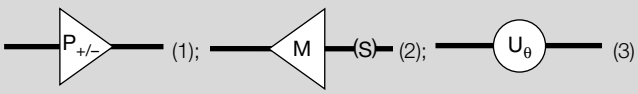
LOQC is based on a series of non-deterministic operations with increasing probability of success. The first operation is a non-deterministic nonlinear sign change on one mode defined by the operation NS: $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle \rightarrow \alpha_0|0\rangle + \alpha_1|1\rangle - \alpha_2|2\rangle$ (with probability 1/4), and can be implemented using the optical network of Fig. 1. Its main features are the use of two ancilla modes with one prepared photon and post-selection based on measuring the ancillas. This procedure can be experimentally verified using techniques similar to those used in a recent Greenberger–Horne–Zeilinger (GHZ) experiment[29] (see Supplementary Information). A conditional sign flip c–$z_{1/16}$ that succeeds with probability 1/16 can be

Box 1

Quantum gates and networks

Quantum information processing (QIP) is accomplished by applying quantum gates and measurements to prepared qubits. The gates evolve the state according to the laws of quantum mechanics. The power of QIP depends on the ability to implement enough evolutions using the available gates. If all unitary evolutions can be approximated up to a global phase, the set of gates is called universal. Standard quantum computation relies on universal gate sets where each gate acts on one or two qubits. One such gate set consists of the one-qubit rotations $U_\phi = \exp(-i\sigma_u\phi/2)$, $U = X, Y$ or Z, where ϕ can be restricted to $\phi = 45°$; and either the conditional sign flip (see text) or one of the 90° rotations $(UV)_{90°}^{(12)} = \exp(-i\pi\sigma_u^{(1)}\sigma_v^{(2)}/4)$, with $U, V = X, Y$ or Z.

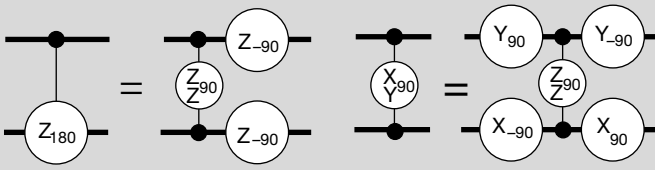
A sequence of state preparations, quantum gates and measurements is called a quantum network. Quantum networks can be depicted by time–space diagrams, with time lines of qubits given by lines running from left to right, and gates by elements that intercept the lines. Our conventions for depicting one qubit gates are:



(1) is a preparation gate, with $P = X, Y$ or Z corresponding to preparations of σ_x, σ_y or σ_z eigenstates. For example, if $P_\pm = Z_+$, the $|0\rangle$ state is prepared. (2) is a measurement gate, where $M = X, Y$ or Z corresponds to measurements in the eigenbasis of σ_x, σ_y or σ_z. The symbol S denotes the measurement outcome, which can be +1 or –1. (3) is a one-qubit rotation around $U = X, Y$ or Z by angle ϕ (in degrees by default). Two-qubit gates are denoted by

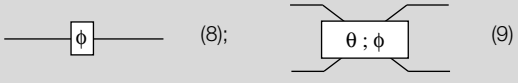
(4) is a conditional sign change by phase χ and applies χ only to the state $|11\rangle$. (5) is a $(ZY)_{90°}^{(12)}$ rotation.

Many of the gates are equivalent up to one-qubit rotations. Here are some equivalences used in the text:



(7) expresses one gate by conjugating another by $Y_{-90°}^{(1)}$ and $X_{90°}^{(2)}$.

Optical networks are similar to quantum networks except that the basic systems are optical modes. The basic elements of an optical network drawing are:



(8) shows a phase shifter $\mathbf{P}_\phi$ and (9) a beam splitter $\mathbf{B}_{\theta,\phi}^{(12)}$, where mode 1 is the top mode. If $\phi = 0$, only angle θ may be given in a diagram. State preparation is like (1), with $P_\pm$ replaced by 0 or 1, for the number of photons inserted into the mode. Measurement is like (2), with M replaced by $\mathbf{n}$ and S by R, for the number of photons detected.

implemented with two independent applications of the operation NS as shown in Fig. 2.

Quantum gates by teleportation

Quantum teleportation has proved to be a very versatile tool in QIP[23,24]. Here we use it to increase the probability of success of coupling gates by reducing the implementation of c–z to a state preparation problem. A basic quantum teleportation protocol $\mathbf{T}_1$ for transferring the state $\alpha_0|0\rangle_1 + \alpha_1|1\rangle_1$ of mode 1 to mode 3 begins by adjoining the 'entangled' ancilla state $|t_1\rangle_{23} = |01\rangle_{23} + |10\rangle_{23}$ (normalization constants omitted). Next, modes 1 and 2 are measured in the basis $|01\rangle_{12} \pm |10\rangle_{12}$, $|00\rangle_{12} \pm |11\rangle_{12}$ (a Bell basis). The measurement consists of two steps. The first determines the parity p of the number of photons in modes 1 and 2 (parity measurement). The second determines the sign s in the superposition. Consider the case where p is odd. 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 initial state by using a phase shifter. For even p, the situation is similar except that $|0\rangle_3$ and $|1\rangle_3$ are flipped (and cannot easily be 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.

The basic teleportation protocol can be implemented in linear optics with success probability 1/2 by applying a balanced beam splitter to modes 1 and 2 and then measuring the number of photons in the two modes. This partial Bell (or teleportation) measurement ($\mathbf{BM}_1$) determines the parity, and if it is odd, the sign. Using this method, it is possible to implement a conditional sign flip c–$z_{1/4}$ that succeeds with probability 1/4 (Fig. 3).

To reliably detect photon loss (in the single photon sources, in transmission or by undercounting in detectors), we give another method, $\mathbf{RT}_1$, for teleporting a bosonic qubit with success probability 1/2, which is shown in Fig. 4. The method for obtaining c–$z_{1/4}$ using $\mathbf{T}_1$ works with $\mathbf{RT}_1$, giving c–$z_{r,1/4}$ with identical failure behaviour (see the caption of Fig. 3). The implementation is in the Supplementary Information.

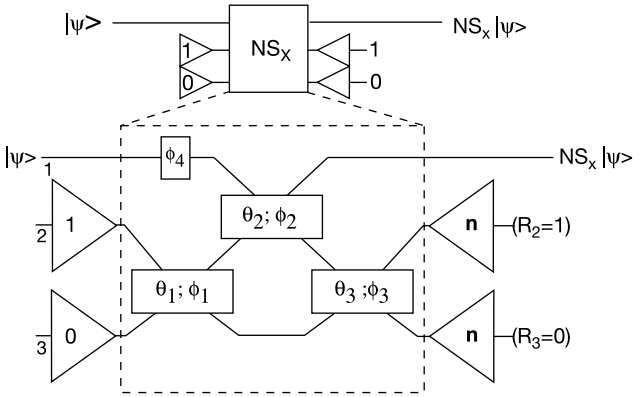


Figure 1 Nonlinear phase shifts on one mode. The numbers at the beginning of the horizontal mode line are their labels. The outlined optical element is abbreviated in future figures by using the top diagram as indicated. The output is accepted only if the photon counters detect one photon in mode 2 and none in mode 3. The subscript x in the top diagram is the phase shift applied and depends on the choice of phases in the optical elements. NS as defined in the text corresponds to $x = -1$ and requires $\theta_1 = 22.5°$, $\phi_1 = 0°$, $\theta_2 = 65.5302°$, $\phi_2 = 0°$, $\theta_3 = -22.5°$, $\phi_3 = 0°$ and $\phi_4 = 180°$. The probability of success is 0.25. Exact expressions for the angles of NS can be determined from the 3×3 unitary matrix u associated with the optical elements[28]:

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

A shift of $|2\rangle_1$ by $x = \exp(i\pi/2)$ is obtained by setting $\theta_1 = 36.53°$, $\phi_1 = 88.24°$, $\theta_2 = 62.25°$, $\phi_2 = -66.52°$, $\phi_3 = -36.53°$, $\phi_3 = -11.25°$ and $\phi_4 = 102.24°$. The probability of success is 0.18082.

Near-deterministic quantum teleportation and operations

To improve the probability of successful teleportation to $1 - 1/(n+1)$, we generalize the prepared entanglement by defining $|t_n\rangle_{1\ldots(2n)} = \Sigma_{j=0}^{n} |1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j}$. The notation $|a\rangle^j$ means $|a\rangle|a\rangle\ldots, j$ times. The modes are labelled from 1 to $2n$, left to right. The state exists in the space of n bosonic qubits, where the kth qubit is encoded in modes $n+k$ and k (in that order). Using the qubit bases, the state $|t_n\rangle$ is $\Sigma_{j=0}^{n}|o\rangle^j|1\rangle^{n-j}$. This representation can be used to obtain linear size quantum networks (which are implementable in LOQC) for preparing the state.

A procedure for teleporting the state $\alpha_0|0\rangle_0 + \alpha_1|1\rangle_0$ using $|t_n\rangle$ applies the measurement $\mathbf{BM}_n$, which consists of the $n+1$ point Fourier transform $\hat{\mathbf{F}}_{n+1}$ followed by measurement of modes $0\ldots n$. $\hat{\mathbf{F}}_{n+1}$ is determined by $u(\hat{\mathbf{F}}_{n+1})_{kl} = \omega^{kl}/\sqrt{n+1}$, where $\omega = \exp(i2\pi/(n+1))$ and $k, l \in 0\ldots n$. It has efficient linear optics implementations[30,31].

Suppose $\mathbf{BM}_n$ detects k photons 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 $0 \leqslant l < (n-k)$ and can be reused in future preparations requiring single photons. The modes $2n-l$ are in state 0 for $n-k < l < n$. If $k = 0$ we learn that the input state was $|0\rangle_0$ and if $k = n+1$, that it was $|1\rangle_0$. The probability of these two events is $1/(n+1)$, regardless of the input. Both the necessary correction and which mode we teleported to are unknown until after the measurement.

The construction of c–$z_{1/4}$ and c–$z_{r,1/4}$ can be generalized using near-deterministic teleportation. To obtain a conditional sign flip c–$z_{n^2/(n+1)^2}$ that succeeds with probability $n^2/(n+1)^2$, the prepared entanglement consists of two copies of $|t_n\rangle$ modified by applied c–z operations as follows

$$|cs_n\rangle = \sum_{i,j=0}^{n} (-1)^{(n-i)(n-j)} |1\rangle^i|0\rangle^{n-i}|0\rangle^j|1\rangle^{n-i}|1\rangle^j|0\rangle^{n-j}|0\rangle^j|1\rangle^{n-j} \quad (2)$$

$$= \sum_{i,j=0}^{n} (-1)^{(n-i)(n-j)} |o\rangle^i|1\rangle^{n-i}|o\rangle^j|1\rangle^{n-j} \quad (3)$$

where the bosonic qubit encoding introduced earlier for $|t_n\rangle$ has been used for the second identity. The teleportation measurements involve the first modes of the two qubits to which c–z is to be

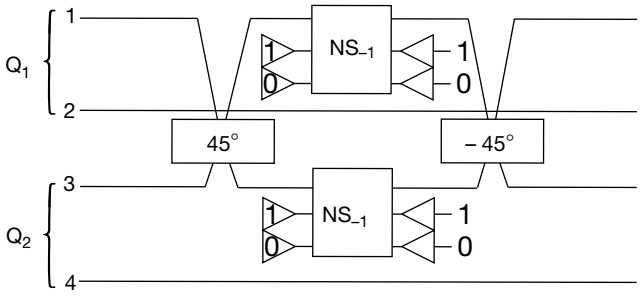


Figure 2 Conditional sign flip implemented with NS operations. Q_1 and Q_2 refer to the bosonic qubits encoded in modes 1, 2, and 3, 4, respectively. Consider the effect of the first beam splitter: When both qubits are in state $|1\rangle$, modes 1 and 3 are in the state $|11\rangle_{13}$, which transforms to $|20\rangle_{13} + |02\rangle_{13}$. In none of the other cases do two photons appear in the same mode. Thus $NS^{(1)}$ and $NS^{(3)}$ have the desired effect. Both of these operations must succeed, so c–$z_{1/16}$ succeeds with probability 1/16.

applied, and modes $1\ldots n$ and $2n+1\ldots 2n+n$ (left to right order), respectively. An additional phase correction is needed after the measurement, depending on which modes the output appears in.

To ensure detection of photon loss, the state $|\mathrm{rt}_n\rangle$, which generalizes $|\mathrm{rt}_1\rangle$, can be used: $|\mathrm{rt}_n\rangle = \Sigma_{j=}^{n}|0\rangle^{j}|1\rangle^{n-j}|0\rangle^{n-j}|1\rangle^{j}$, written in terms of the qubit encoding. As before, the total number of photons in the modes measured for teleportation is now fixed (at $n+1$), and any deviation from this results in a detected loss error. The state needed for the loss-detecting implementation of c–z, c–$z_{r,n^2/(n+1)^2}$ is:

$$|\mathrm{rcs}_n\rangle = \sum_{i,j=0}^{n}(-1)^{(n-i)(n-j)}|0\rangle^{i}|1\rangle^{n-i}|0\rangle^{n-i}|1\rangle^{i}|0\rangle^{j}|1\rangle^{n-j}|0\rangle^{n-j}|1\rangle^{j} \quad (4)$$

The failure-by-measurement behaviour for c–$z_{n^2/(n+1)^2}$ and c–$z_{r,n^2/(n+1)^2}$ can be made the same as that for c–$z_{1/4}$ (see Fig. 3).

Applications of the techniques introduced so far include near-deterministic non-destructive parity measurements, a method for

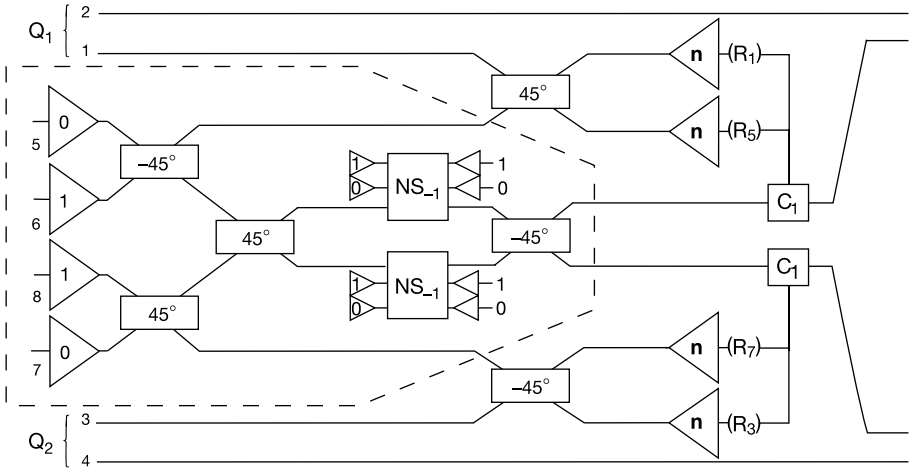


Figure 3 Conditional sign flip with success probability 1/4. The method may be derived as follows[24]: To implement c–z on two bosonic qubits in modes 1, 2 and 3, 4, respectively, we can teleport the first modes of each qubit to two new modes (labelled 6 and 8) and then apply c–z to the new modes. When using the basic teleportation protocol ($\mathbf{T}_1$), we may need to apply a sign correction. Since this commutes with c–z, it is possible to apply c–z to the prepared state before performing the measurements, reducing the implementation of c–z to a state-preparation (outlined) and two teleportations. The two teleportation measurements each succeed with probability 1/2, giving a net success probability of 1/4. The correction operations C_1 consist of applying the phase shifter $\mathbf{P}_{180°}$ when required by the measurement outcomes. The state preparation needs to be attempted 16 times on average before success, which corresponds to 32 attempted NS operations (without taking advantage of the ability to avoid an attempt if the first one in a pair failed).

The implementation of c–$z_{1/4}$ fails if one of the two teleportation measurements does not succeed. The following properties hold for failure of c–$z_{1/4}$: (1) the failed teleportation measurements result in an unintentional Z measurement of the corresponding bosonic qubit (2). The teleportation measurements fail independently. (Alternatively, to improve efficiency, one may attempt the measurements sequentially, so as not to perform the second one if the first one fails.) (3) By reintroducing a photon if necessary, the measurements can be assumed to be non-destructive. (4) By applying a phase shifter if necessary, it can be arranged that the effect on the successfully teleported qubit is as if the c–z operation succeeded before the unintentional measurement.

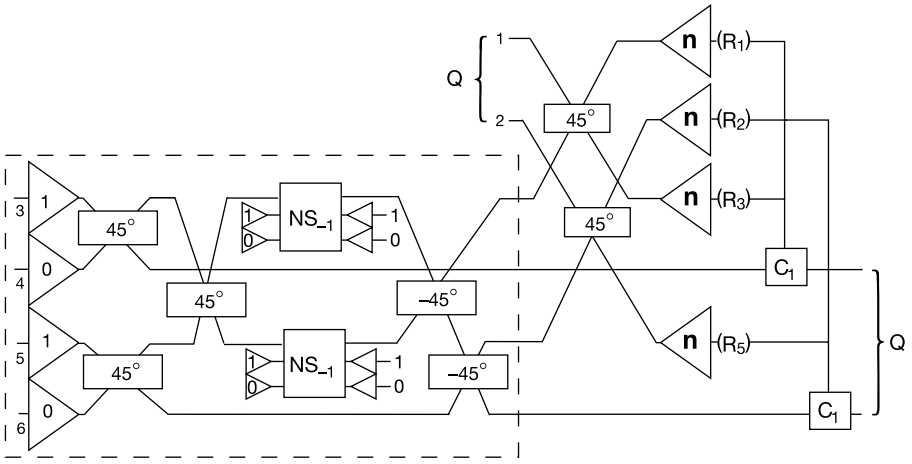


Figure 4 Teleportation with loss detection ($\mathbf{RT}_1$). The outlined box prepares the state $|\mathrm{rt}\rangle_{3456} = |01\rangle_{34}|10\rangle_{56} + |10\rangle_{34}|01\rangle_{56}$ using non-deterministic gates. This teleportation protocol has been experimentally tested[44,45], using down conversion with post-selection for preparing $|\mathrm{rt}_1\rangle$ instead of the preparation network shown above. Given $|\mathrm{rt}_1\rangle$, the protocol succeeds with probability 1/2. The pair of NS operations implements a c–$z_{1/16}$ on bosonic qubits encoded in modes 3, 4 and 5, 6, respectively. Thus 32 NS attempts are needed on average before successfully obtaining $|\mathrm{rt}_1\rangle$. Without loss, the number of photons in modes 1, 2, 3, 5 is two. Thus, loss is detected if $R_1 + R_2 + R_3 + R_5 \neq 2$. The teleportation succeeds if $R_1 + R_3 = 1$ and $R_2 + R_5 = 1$, in which case the qubit reappears in modes 4, 6. Failure not due to loss results in a Z measurement of the teleported qubit. Loss of a photon in the incoming qubit or from detector inefficiency is always detected. Assuming no loss in the prepared state or the detectors, $\mathbf{RT}_1$ detects if the input is not a bosonic qubit state (a leakage event) and returns a bosonic qubit. This is necessary for scalable quantum information processing (QIP).

creating entanglement by local measurements of uncorrelated photons shared with beam splitters, and nearly unconditional quantum teleportation and Bell-state measurements with linear optics.

The proof of the claim of this section, the teleportation network for the case $n = 2$, networks for preparing $|cs_2\rangle$ and $|rt_2\rangle$ and descriptions of the applications are in the Supplementary Information.

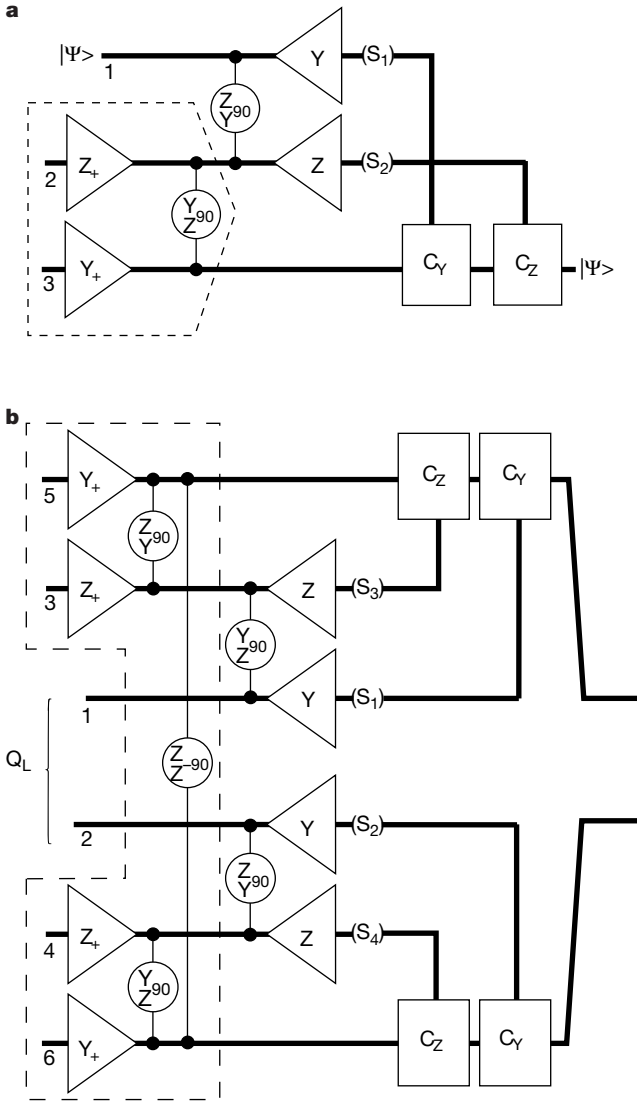


Figure 5 Teleportation networks for the code χ_2. **a**, Teleportation satisfying that failures of the teleportation step result at worst in a Z-measurement of qubit 1. The networks are based on a variation of the teleportation protocol that exploits the flexibility in the choices for initial states, rotations and measurements to ensure that it behaves well with respect to measurement failures. The correction operations are $C_Z = X_{180°}$ if $S_2 = 1$ and $C_Y = Z_{180°}$ if $S_1 = 1$. The state preparation is outlined and outputs a state denoted by $|tx_2\rangle$. **b**, Teleportation for applying $(Z^{(L)})_{90°}$. If $S_3S_4 = -1$, the phase needs to be corrected with a $Z_{180°}$ on both qubits. The prepared state (outlined) is obtained by applying $(ZZ)_{90°}$ to the destination qubits of two copies of $|tx_2\rangle$. The method for applying $(Z^{(L_1)}Z^{(L_2)})_{90°}$ is similar, using four copies instead. Both teleportations are attempted. The procedure can only fail with the logical qubit measured in Z. For simplicity, the following failure protocol can be used: If both teleportations fail in any way, we measure the qubits in Z on purpose (if that has not already happened), thus inducing a logical Z measurement. If only one fails, we ensure that the corresponding qubit is measured in Z, then follow the recovery protocol of Fig. 6 using the successfully teleported qubit. With this failure protocol, the logical failure probability for the $Z^{(L)}$ and $Z^{(L_1)}Z^{(L_2)}$ rotations is $f_2 = (1-(1-f)^2)^2 + 2(1-(1-f)^2)(1-f)^2 f_r$ with $f_r = f/(1-f(1-f))$ the probability of recovery failure (Fig. 6). Thus $f_2 < f$ whenever $f < 1/6.43$.

Boosting success with quantum codes

Exponential improvements in the probability of success for gates and state preparation can be obtained by exploiting quantum codes and the failure behaviour of $c{-}z_{n^2/(n+1)^2}$. As a result, n need not be large and the difficulty of preparing states such as $|cs_n\rangle$ or $|rcs_n\rangle$ is lessened. We give a method based on a two-qubit code, χ_2. This method can be used to define logical qubits with greatly improved success probabilities and robustness, provided that the given qubits are sufficiently controllable. As a result it is possible to iterate the method to efficiently achieve essentially perfect QIP. This iteration is known as concatenation and underlies the accuracy-threshold theorems of fault-tolerant quantum computation[6–9].

From now on, we use qubit based quantum networks and rely on the following list of operations implementable in LOQC with bosonic qubits according to the techniques of the previous sections: (1) X, Y and Z eigenstate (eigenvalue +1 or −1) preparation; (2) X, Y and Z measurements; (3) $X_{180°}$, $Y_{180°}$ and $Z_{180°}$ rotations; (4) X_ϕ rotations; (5) $Z_{90°}$ rotation; (6) $(Z^{(1)}Z^{(2)})_{90°}$ rotation. For the moment we assume that the optical elements, single-photon sources and photon counters are error-free. Operations (1) to (4) always succeed. The $(Z^{(1)}Z^{(2)})_{90°}$ rotation fails independently on qubits 1 and 2 with probability f. If $c{-}z_{n^2/(n+1)^2}$ is used, then $f = 1/(n+1)$. The $Z_{90°}$ rotation always succeeds in LOQC, although after the first encoding it fails with probability f. A qubit on which an operation fails is measured in Z after the rotation has been applied. The $Y_{90°}$, $(YZ)_{90°}$ and $(YY)_{90°}$ rotations can be implemented by conjugation of $Z_{90°}$ or $(ZZ)_{90°}$ with failure-free X rotations. The failure mode of these rotations is similar to that for the $(ZZ)_{90°}$ rotation, with commuting Y measurements replacing Z measurements.

To encode a qubit we define its logical states $|0\rangle_L$ and $|1\rangle_L$ by $|0\rangle_L = |00\rangle + |11\rangle$ and $|1\rangle_L = |01\rangle + |10\rangle$. This is an instance of a stabilizer code[32–35]. In this context it is convenient to use the abbreviation $U = \sigma_u$ for $U = X, Y, Z$. With encoding qubits labelled 1, 2, the logical X, Y and Z operators are given by $X^{(L)} = X^{(1)} =_L X^{(2)}$, $Z^{(L)} = Z^{(1)}Z^{(2)} =_L -Y^{(1)}Y^{(2)}$ and $Y^{(L)} = Y^{(1)}Z^{(2)} =_L Z^{(1)}Y^{(2)}$, where we introduced the notation $=_L$ to denote identity when restricted to the code space spanned by $|0\rangle_L$, $|1\rangle_L$. To destructively measure one of the logical operators, it suffices to measure each qubit; it is straightforward to obtain nondeterministic state preparation networks (see the Supplementary Information). Any rotation $X_\phi^{(L)}$ can be implemented by applying $X_\phi^{(1)}$ or $X_\phi^{(2)}$. The 180° logical rotations can be applied by using the corresponding 180° rotations directly on the qubits, a feature satisfied by all stabilizer codes[36]. For example, to apply $Y_{180°}^{(L)}$ apply both $Y_{180°}^{(1)}$ and $Z_{180°}^{(2)}$.

The logical operations introduced so far can be done without failure. To implement the $Z_{90°}^{(L)}$ and $(ZZ)_{90°}^{(L_1L_2)}$ rotations with failure probabilities much less than f requires the teleportation networks shown in Fig. 5, which have the property that at worst, the teleported qubit is measured in Z. As described in the captions of Figs 5 and 6, the failure probability f_z of these logical rotations satisfies $f_z < O(f^2)$ and $f_z < f$ whenever $f < 1/6.43$.

The methods can be improved in three ways: first, by better exploiting the flexibility in state preparation and responses to failures; second, by using classical linear codes like the repetition codes; and third, by encoding more than one qubit into one block. With these techniques it is possible to achieve $f_z < f$ for $f < 1/2$ (see Supplementary Information).

Scalability and resource requirements

A scalable information processing system requires that one can deal with errors that occur in the physical implementation. For LOQC, dominant sources of errors are photon loss (at the single photon source or during processing), detector inefficiency (which can be

viewed as photon loss) and phase errors. Photon loss can be dealt with by using the loss-detecting implementations of c–z. The probability f_l of loss for an LOQC operation can be predicted from the characteristics of the optical devices. The possibility of loss introduces a new failure mode, where nothing is known about what happened to the state of the qubit. This is the erasure model of errors[37]. A good implementation of LOQC ensures that $f_l \ll f$, so that we can first improve f using the techniques already discussed, and then deal with the problem of erasures. Compensating for erasures is much easier than dealing with general errors, with pessimistic estimates of $f_l \lesssim 0.01$ (ref. 38) for quadratic improvements. Unlike photon loss, phase errors are not detected by the networks discussed so far. Happily, phase-error correction can be integrated into the methods for reducing f using codes that generalize χ_2 based on classical repetition codes. These codes can correct unknown phase errors in up to half the qubits. More details on erasure and phase error correcting codes are in the Supplementary Information.

The methods introduced so far suffice for implementing accurate quantum gates on logical qubits in the presence of intrinsic failures of LOQC, and sufficiently low photon loss and phase errors. Scalable quantum computation is possible provided that any remaining errors in the logical operations fall below a threshold. There is evidence that the relevant threshold may be above 0.0001 (D. Gottesman and J. Preskill, unpublished work). Achieving such low error is experimentally challenging for any device, although optimism is justified by the observations that many of the errors are due to improper calibration of classical control parameters, and these are often controllable well below the estimated threshold. An example is pulse phase in nuclear magnetic resonance. Another reason for optimism is that at least for quantum communication, the threshold is well above 0.01 (ref. 39). As all viable proposals for long-distance quantum communication are based on optics, this may be the first scalable application of LOQC.

Resources contributing toward a logical quantum gate based on LOQC can be counted in two ways: as total and as conditional resources. The total resources are given by the number of optical operations required on average. This depends on the success probabilities of the component state preparations and the desired success probability for the logical operations. As most of the resources are used in independent state preparation steps, an implementation of LOQC can be based on massively parallel state factories. It is thus natural to consider the conditional resources, which are the number of optical operations that successfully contribute toward a logical quantum gate. Their significance is that the error of an operation conditional on success can be estimated by multiplying the conditional error of the optical elements by the conditional resource count. Detailed resource analyses are yet to be done. However, it can be shown that failure probabilities below 5% can be achieved using only two iterations of χ_2, requiring about 300 successful c–$z_{9/16}$ operations per logical two-qubit gate[38].

An implementation of LOQC requires careful mode matching, rapidly controllable delay lines or good synchronization of pulses, tunable beam splitters and phase shifters, single photon sources and high-efficiency fast photo-detectors for single photon detection. Speed is needed to be able to select successful state preparations before photon loss becomes too large. Tunable optical elements can be made using polarizers and polarizing beam splitters. Non-deterministic single photon sources can be constructed with parametric down converters[21], although a better method is to use one of the schemes for single photon sources that have recently been proposed[40,41]. The best photon counters currently have efficiencies of about 0.9 at optical frequencies[42]. This is sufficient for experimentally implementing the basic elements of LOQC. Higher efficiencies are required for implementing the more complex teleportation and quantum gate operations with sufficiently low error conditional on success.

The preliminary resource counts discussed above imply large but not excessive resource overheads per reliable quantum gate. The need for robustness requires non-trivial resource overheads in all implementations of QIP, so this suggests that scalable quantum computation using LOQC is comparable in complexity to other proposals. LOQC has the advantage in several respects. In particular, there is no need for low temperature for the basic optical elements (except perhaps in the single photon sources and the photo-detectors, depending on implementation), and photons naturally maintain their coherence over timescales that are long compared to the basic control operations. Furthermore, the sources of noise are better understood and do not depend on difficult-to-predict or difficult-to-measure thermal interactions. However, all proposals until now, including LOQC, require that various technologies can be made to work together to obtain high fidelities in operations.

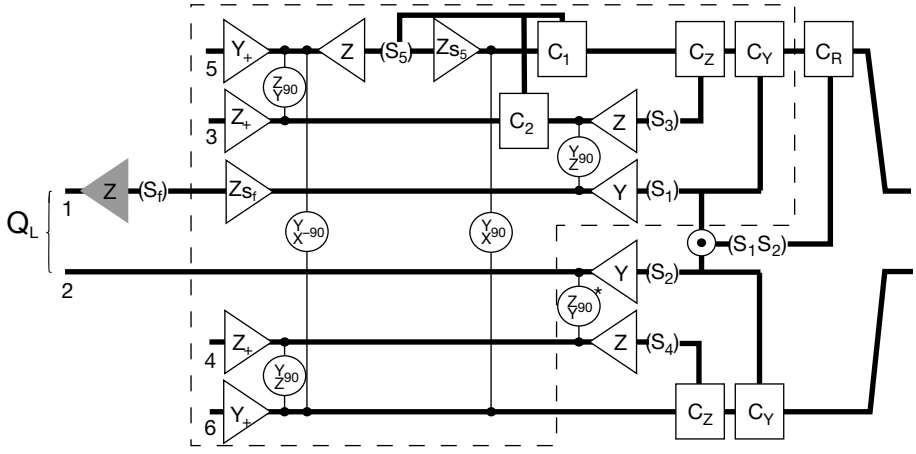


Figure 6 Recovery from Z measurement. A state is prepared using two instances of $|\mathrm{tx}_2\rangle$ modified by projecting with $I + XX$. The gates C_1 and C_2 correct for measuring $S_5 = -1$ by applying $C_1 = Z_{180°}$ to qubit 5 and $C_2 = X_{180°}$ to qubit 3. The two teleportations are then attempted. The network assumes that we need to recover from a Z measurement of qubit 1 (shown in grey). In this case, qubit 1 can be absorbed into a state preparation; which one depends on the measurement outcome. This avoids being affected by failures in the top teleportation. The parts of the network which can be performed in a non-deterministic state preparation are outlined. An XX measurement of the teleported qubits becomes recorded in the teleportation measurements. The recovered state is obtained by applying $C_R = Z_{180°}$ if $S_1S_2 = -1$. If the pre-measurement coupling gate marked by an asterisk fails with a Y-measurement only, then we can retry the recovery process using a new prepared state. The probability of this failure event is $f(1-f)$, so the total failure probability f_r of recovery satisfies $f_r = f + f(1+f)f_r$, whence $f_r = f/(1-f(1-f))$.

Discussion

Linear optics was believed to be insufficient for quantum computation because every implementable evolution can be understood in terms of a small unitary matrix, contrary to expectations of exponential complexity. Furthermore, passive linear optics does not involve particle interactions other than those imposed by statistics and can be understood in terms of classical wave mechanics. There is, however, a hidden non-linearity in LOQC (in the photo-detectors) and our techniques effectively transfer this non-linearity to the bosonic qubits, thus enabling universal quantum computation.

There are other options for implementing LOQC. Particularly interesting is an idea[43] that involves encoding qubits in the phase space of a mode. Universal computation in this system requires active linear optics and a nonlinearly prepared state, but has the advantage of being intrinsically robust against errors involving shifts in the canonically conjugate variables. It may be possible to combine approaches to achieve robust and efficient LOQC even more easily. □

Received 24 July; accepted 13 November 2000.

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26,** 1484–1509 (1997).
2. Grover, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **79,** 325–328 (1997).
3. Wiesner, S. Conjugate coding. *(Original Manuscript ~ 1969) Sigact News* **15,** 78–88 (1983).
4. Bennett, C., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptol.* **5,** 3–28 (1992).
5. Shor, P. W. in *Proceedings of the 37th Symposium on the Foundations of Computer Science (FOCS)* 56–65 (IEEE Press, Los Alamitos, 1996).
6. Aharonov, D. & Ben-Or, M. in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computation (STOC)* 176–188 (ACM Press, New York, 1996).
7. Kitaev, A. Y. Quantum computations: algorithms and error correction. *Russian Math. Surv.* **52,** 1191–1249 (1997).
8. Knill, E., Laflamme, R. & Zurek, W. H. Resilient quantum computation. *Science* **279,** 342–345 (1998).
9. Preskill, J. Reliable quantum computers. *Proc. R. Soc. Lond. A* **454,** 385–410 (1998).
10. Steane, A. Efficient fault-tolerant quantum computing. *Nature* **399,** 124–126 (1999).
11. Experimental proposals for quantum computation. (Special focus issue) *Fort. Phys.* **48,** 767–1138 (2000).
12. Milburn, G. J. Quantum optical Fredkin gate. *Phys. Rev. Lett.* **62,** 2124–2127 (1988).
13. Hughes, R. J., Morgan, G. L. & Peterson, C. G. Quantum key distribution over a 48 km optical fibre network. *J. Mod. Optics* **47,** 533–547 (2000).
14. Tittle, W., Brendel, J., Gisin, N. & Zbinden, H. Long-distance Bell-type tests using energy-time entangled photons. *Phys. Rev. A* **59,** 4150–4163 (1999).
15. Townsend, P., Rarity, J. & Tapster, P. Single photon interference in 10 km long optical fibre interferometer. *Electron. Lett.* **29,** 1291–1293 (1993).
16. Turchette, Q. A., Hood, C. J., Lange, W., Mabuchi, H. & Kimble, H. J. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.* 4710–4713 (1995).
17. Cerf, N. J., Adami, C. & Kwiat, P. G. Optical simulation of quantum logic. *Phys. Rev. A* **57,** R1477–R1480 (1998).
18. Howell, J. C. & Yeazell, J. A. Reducing the complexity of linear optics quantum circuits. *Phys. Rev. A* **61,** 052303/1–5 (2000).
19. Kwiat, P. G., Mitchell, J. R., Schwindt, P. D. D. & White, A. G. Grover's search algorithm: An optical approach. *J. Mod. Optics* **47,** 257–266 (2000).
20. Lütkenhaus, N., Calsamiglia, J. & Suominen, K.-A. Bell measurements for teleportation. *Phys. Rev. A* **59,** 3295–3300 (1999).
21. Hong, C. K. & Mandel, L. Experimental realization of a localized one-photon state. *Phys. Rev. Lett.* **56,** 58–60 (1986).
22. Adleman, L. M., DeMarrais, U. & Huang, M.-D. A. Quantum computability. *SIAM J. Comput.* **26,** 1524–1540 (1997).
23. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895–1899 (1993).
24. Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402,** 390–393 (1999).
25. Walls, D. F. & Milburn, G. J. *Quantum Optics* (Springer, Berlin, 1994).
26. Aharonov, D. in *Annual Reviews of Computational Physics VI* (ed. Stauffer, D.) (World Scientific, Singapore, 1999).
27. DiVincenzo, D. The physical implementation of quantum computation. *Fort. Phys.* **48,** 771–793 (2000).
28. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of an discrete unitary operator. *Phys. Rev. Lett.* **73,** 58–61 (1994).
29. Bouwmeester, D., Pan, J.-W., Daniell, M., Weinfurter, H. & Zeilinger, A. Observation of three-photon Greenberger-Horne-Zeilinger entanglement. *Phys. Rev. Lett.* **82,** 1345–1349 (1999).
30. Weihs, G., Reck, M., Weinfurter, H. & Zeilinger, A. All-fiber three-path Mach-Zehnder interferometer. *Opt. Lett.* **21,** 302–304 (1996).
31. Cormen, T. H., Leiserson, C. E. & Rivest, R. L. *Introduction to Algorithms* 795 (MIT Press, Cambridge, MA, 1990).
32. Shor, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **52,** 2493–2496 (1995).
33. Steane, A. Multiple particle interference and quantum error correction. *Proc. R. Soc. Lond. A* **452,** 2551–2577 (1996).
34. Calderbank, A., Rains, E., Shor, P. & Sloane, N. Quantum error correction and orthogonal geometry. *Phys. Rev. A* **78,** 405–408 (1997).
35. Gottesman, D. A class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A* **54,** 1862–1868 (1996).
36. Gottesman, D. A theory of fault-tolerant quantum computation. *Phys. Rev. A* **57,** 127–137 (1998).
37. Grassl, M., Beth, T. & Pellizari, T. Codes for the quantum erasure channel. *Phys. Rev. A* **56,** 33–38 (1997).
38. Knill, E., Laflamme, R. & Milburn, G. Thresholds for linear optics quantum computation. Preprint quant-ph/0006120 at ⟨xxx.lanl.gov⟩ (2000).
39. Dür, W., Briegel, H.-J., Cirac, J. I. & Zoller, P. Quantum repeaters based on entanglement purification. *Phys. Rev. A* **59,** 169–181 (1999).
40. Kim, J., Benson, O., Kan, H. & Yamamoto, Y. A single-photon turnstile device. *Nature* **397,** 500–503 (1999).
41. Foden, C. L., Talyanskii, V. I., Milburn, G. J., Leadbeater, M. L. & Pepper, M. High frequency acousto-electric single photon source. *Phys. Rev. A* **62,** 011803(R)/1–4 (2000).
42. Takeuchi, S., Yamamoto, Y. & Hogue, H. H. Development of a high-quantum-efficiency single-photon counting system. *Appl. Phys. Lett.* **74,** 1063–1065 (1999).
43. Gottesman, D., Kitaev, A. & Preskill, J. Encoding a qubit in an oscillator. Preprint quant-ph/0008040 at ⟨xxx.lanl.gov⟩ (2000).
44. Bouwmeester, D., Pan, J., Mattle, K., Eibl, M., Weinfurter, H. & Zeilinger, A. Experimental quantum teleportation. *Nature* **390,** 575–579 (1997).
45. Boschi, D., Branca, S., Martini, F. D., Hardy, L. & Popescu, S. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels. *Phys. Rev. Lett.* **80,** 1121–1125 (1998).

Supplementary information is available on *Nature*'s World-Wide Web site (http://www.nature.com) or as paper copy from the London editorial office of *Nature*.

Acknowledgements

We thank P. Kwiat and A. White for help and discussions.

Correspondence and requests for materials should be sent to E. Knill (e-mail: knill@lanl.gov).