PHYSICAL REVIEW A **75**, 052328 (2007)

Efficient parity-encoded optical quantum computing

Alexei Gilchrist,[1,*] A. J. F. Hayes,[1] and T. C. Ralph[1]
[1]*Centre for Quantum Computer Technology and Physics Department, University of Queensland, QLD 4072, Brisbane, Australia*
(Received 15 September 2005; published 22 May 2007)

We present a linear optics quantum computation scheme with a greatly reduced cost in resources compared to that proposed by Knill, Laflamme, and Milburn (KLM). The scheme makes use of elements from cluster state computation but retains the circuit based approach of KLM.

DOI: 10.1103/PhysRevA.75.052328 PACS number(s): 03.67.Lx, 42.50.Dv

INTRODUCTION

There are a number of proposed physical systems for implementing quantum computation, and it is not yet clear which architecture would be most suitable. For initial steps toward quantum computation, optical systems have some appealing properties. The qubits are subject to low decoherence and single qubit unitaries can be implemented with passive linear elements.

The optical proposal by Knill, Laflamme, and Milburn (KLM) [1] attracted much attention as it demonstrated that scalable linear-optics quantum computation (LOQC) was possible. As a consequence, a number of experimental efforts are currently focused on testing the basic gates and protocols for LOQC [2–5]. KLM's proposal replaces the normally required large nonlinearities with nondeterministic (but heralded) schemes. They show that the nondeterminism can be effectively hidden by using a combination of teleportation (also nondeterministic) and error encoding. Although KLM showed that LOQC was possible, the resources consumed by their scheme are large. Given that the overall leanness in consuming resources will be one of the deciding factors in adopting a particular implementation [17], the longer term prospects for optical schemes did not appear so great.

This changed with the alternative approach to LOQC proposed by Nielsen [6]. This approach combined the model of cluster-state quantum computation [7] with the nondeterministic gates presented by KLM. Cluster-state computation divides the computation into two stages—first, preparing a massively entangled state (the cluster state), and second, performing the computation by a series of measurements on the cluster components. In Nielsen's scheme the cluster-state preparation is nondeterministic. Once the cluster state is prepared, the computation proceeds deterministically requiring only single qubit operations and measurements with feedforward. For a related scheme see also the approach by Yoran and Resnik [8]. There have also been several experimental demonstrations of cluster states [9,10].

Creating the cluster uses much fewer resources than the KLM proposal. Recently, a modified scheme for preparing an optical cluster was proposed which uses fewer resources still and is the most efficient implementation yet [11].

In this paper we present a method which combines the ideas in both approaches (KLM and cluster-state). We will use the teleported gates of KLM with the qubits especially encoded to protect from teleporter failures and computational basis measurements. To build up the encoding and perform gates on the encoded qubits we will use the incremental approach in [12]. The basic encoding gate is the same as the type-II fusion gate of [11] and the gate we will need for building the resource for teleportation is essentially the type-I gate. The resource preparation proceeds along the same lines as for preparing linear cluster states; the main difference is that for our encoding we link the nodes together with CNOT operations instead of CSIGN operations.

The motivation for this synthesis is that it retains the standard circuit model while attaining a large reduction in resources by borrowing techniques from the cluster-state approach. An efficient encoding against loss errors is also known for parity states [13].

NOTATION

Since we will deal with qubits at different levels of encoding some care needs to be taken to establish a clear notation. At the highest level, the *logical qubits* are encoded across many *physical qubits* in some encoding. We shall use the notation $|\psi\rangle^{(n)}$ to mean the logical state $|\psi\rangle$ of a qubit, which is encoded across n physical qubits. The basic physical qubits are the first level, and we will often drop the superscript for this level.

ENCODING THE LOGICAL QUBITS

The basic physical states we will use to construct the logical qubits will be the polarization states of a photon so that $|0\rangle^{(1)} \equiv |H\rangle$ and $|1\rangle^{(1)} \equiv |V\rangle$. In fact, any physical qubits formed in a "dual-rail" fashion, i.e., by the occupation of one of two orthogonal modes, will do equally well and our results below can be easily cast in dual-rail form if desired. The advantage of this choice in optics, is that we can perform any single physical-qubit unitary *deterministically* with passive linear optical elements. It is interesting to note that with this choice unitary transformations will conserve energy (photon number).

The particular encoding we will use will be the even and odd parity states so that

$$|0\rangle^{(n)} \equiv (|+\rangle^{\otimes n} + |-\rangle^{\otimes n})/\sqrt{2},$$

$$|1\rangle^{(n)} \equiv (|+\rangle^{\otimes n} - |-\rangle^{\otimes n})/\sqrt{2}, \qquad (1)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. These states were used in the original KLM proposal to protect against teleporter failures.

*Electronic address: alexei@physics.uq.edu.au

A useful feature to note is that the parity states can be written as any sum where each term has the original parity, e.g., $|0\rangle^{(n)}=(|0\rangle^{(n-1)}|0\rangle+|1\rangle^{(n-1)}|1\rangle)/\sqrt{2}$. This choice of encoding means that a computational basis measurement of one of the physical qubits will not destroy the logical state, but will only reduce the level of encoding. To see this notice from Eq. (1) that $\langle 0|0\rangle^{(n)}=|0\rangle^{(n-1)}$ and $\langle 0|1\rangle^{(n)}=|1\rangle^{(n-1)}$, and thus $\langle 0|\psi\rangle^{(n)}=|\psi\rangle^{(n-1)}$. On the other hand, $\langle 1|0\rangle^{(n)}=|1\rangle^{(n-1)}$ and $\langle 1|1\rangle^{(n)}=|0\rangle^{(n-1)}$, and in this case a bit flip of the logical qubit has occurred. However, this can be easily corrected because a bit flip of any one physical qubit will bit flip the logical qubit. Thus $X\langle 1|\psi\rangle^{(n)}=|\psi\rangle^{(n-1)}$, where $X=|0\rangle\langle 1|+|1\rangle\langle 0|$ is the usual Pauli-X operator.

The key functional components in our scheme are two gates which we will call type-I (f_I) and type-II (f_{II}) fusion gates following the nomenclature of [11]. These gates are shown in Fig. 1 as polarization and dual-rail gates. The action of the gates can be represented in shorthand as positive operator-valued measure (POVM) measurement operators with the result being particular detector states denoted as d_{1010} for the detector sequence "1,0,1,0," etc. With this notation, the successful f_{II} operators are

$$|d_{1010}\rangle(\langle 00|+\langle 11|),|d_{0101}\rangle(\langle 00|+\langle 11|), \tag{2}$$

$$|d_{1001}\rangle(\langle 00|-\langle 11|),|d_{0110}\rangle(\langle 00|-\langle 11|), \tag{3}$$

and the unsucessful ones are

$$|d_{2000}\rangle\langle 01|,|d_{0200}\rangle\langle 01|,|d_{0020}\rangle\langle 10|,|d_{0002}\rangle\langle 10|. \tag{4}$$

Note that even without photon-number discriminating detectors these events are distinguishable. This is not true for f_I events which have the following successful operators:

$$|d_{10}\rangle(|0\rangle\langle 00|+|1\rangle\langle 11|), \tag{5}$$

$$|d_{01}\rangle(|0\rangle\langle 00|-|1\rangle\langle 11|), \tag{6}$$

and unsuccessful operators

$$|d_{20}\rangle|\ldots\rangle\langle 01|,|d_{02}\rangle|\ldots\rangle\langle 01|,|d_{00}\rangle|\ldots\rangle\langle 10|, \tag{7}$$

which all measure in the computational basis and project the remaining mode outside of that basis.

The fusion gates act as partial Bell measurements on the input physical qubits, and are used to implement entangling operations. Such nondeterministic Bell measurements have been essential in attempting to use linear optics for quantum communication and computation. In 1994 Weinfurter [14] described an optical layout that used beam splitters and detectors to distinguish two of the four Bell states on spatially encoded qubits. It was observed that this configuration could be used to teleport qubits with a success probability of 50%. Soon after, Braunstein and Mann [15] published a similar scheme that acted on polarization-encoded qubits. The optical configuration they provide is equivalent to the f_{II} gate. In both papers, what we have referred to as a dual-rail Bell measurement was used, measuring both states that the photon could occupy. Calsamiglia and Lütkenhaus [16] later demonstrated that this 50% probability of uniquely distinguishing a Bell state was the best that could be achieved

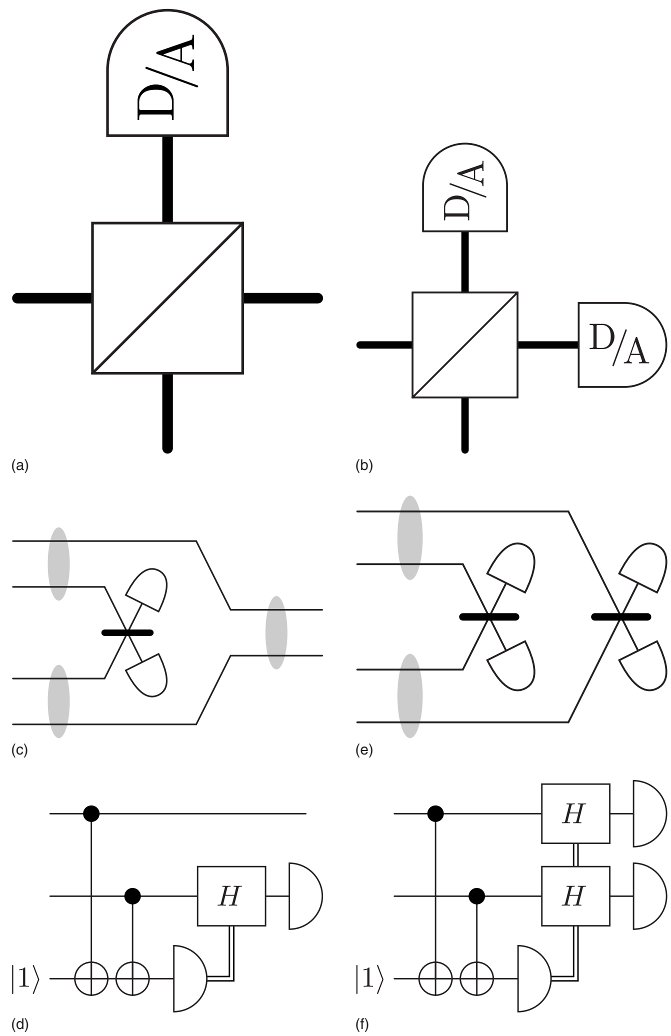

FIG. 1. (a) The type-I fusion (f_I) and (b) type-II fusion (f_{II}) gates, were the detectors analyzed in the diagonal-antidiagonal basis. Dual-rail forms of the f_I and f_{II} gates are shown in (c) and (d), respectively (the shaded ellipses represent the dual-rail physical qubit). (e) and (f) show equivalent circuit models for the fusion gates—an ancilla is used to detect the parity of the physical qubits; if the result is "1" Hadamard gates are applied prior to detection, possibly resulting in a phase-flip error that may need to be corrected (not shown); if the result is "0" the measurements will be in the computational basis and constitute a measurement error.

using linear optical components. However, as shown in KLM [1], the probability of successfully teleporting a qubit can be made arbitrarily high if sufficient resources are used.

The type-II fusion gate can be used to add n physical qubits to the encoded state by using a resource of $|0\rangle^{(n+2)}$. When successful (with probability 1/2), then the following takes place (with a bit flip applied in half the successful cases):

$$f_{II}|\psi\rangle^{(m)}|0\rangle^{(n+2)}\rightarrow\begin{cases}|\psi\rangle^{(m+n)} & \text{(success)}\\ |\psi\rangle^{(m-1)}|0\rangle^{(n+1)} & \text{(failure)}.\end{cases} \tag{8}$$

If the gate fails then a physical qubit is removed from the encoded state, and the resource state is left in the state

$|0\rangle^{(n+1)}$ which can be recycled. It will again be necessary to apply a bit-flip correction in half the cases. This encoding procedure is equivalent to a gambling game where we either lose one level of encoding, or gain n, depending on the toss of a coin.

GENERATING THE RESOURCE

Given a supply of Bell states ($|0\rangle^{(2)}$), the resource $|0\rangle^{(n)}$ can be built up using the same techniques as used to build up cluster states given in [11]. In fact, $|0\rangle^{(n)}$ is locally equivalent to a star shaped cluster state—all nodes linked to a central node.

To create the state $|0\rangle^{(3)}$, two $|0\rangle^{(2)}$ can be fused together using the f_I gate. When successful, the $|0\rangle^{(3)}$ state is produced; when unsuccessful, both bell states are destroyed. Since f_I functions with a probability of $1/2$, on average two attempts are necessary so on average each $|0\rangle^{(3)}$ consumes $4|0\rangle^{(2)}$.

Once there is a supply of $|0\rangle^{(3)}$ states, either f_I or f_{II} can be used to further build up the resource state via

$$Hf_I(H\otimes H)|0\rangle^{(n)}|0\rangle^{(m)} \rightarrow \begin{cases} |0\rangle^{(m+n-1)} & \text{(success)} \\ - & \text{(failure)}, \end{cases} \qquad (9)$$

$$f_{II}|0\rangle^{(n)}|0\rangle^{(m)} \rightarrow \begin{cases} |0\rangle^{(m+n-2)} & \text{(success)} \\ |0\rangle^{(m-1)}|0\rangle^{(n-1)} & \text{(failure)}. \end{cases} \qquad (10)$$

In the first case we use f_I with Hadamard gates and this approach has the advantage of losing only a single physical qubit from the input states, but the disadvantage of completely destroying the entanglement in both input states in the event of failure. In the second case, we use f_{II} to join the input states at the expense of losing two of the initial physical qubits. There are two advantages to the second scheme—in the case of failure we do not destroy the entanglement of the input states, just reduce their encoding by one; and we do not need photon number discriminating detectors to operate f_{II}.

Despite the advantages in using f_{II}, numerical exploration indicates that simply fusing two $|0\rangle^{(3)}$ with f_I to form a $|0\rangle^{(5)}$ is near optimal. This approach carries an average cost of $16|0\rangle^{(2)}$ per $|0\rangle^{(5)}$. Only once we have a supply of $|0\rangle^{(5)}$ is it advantageous to switch to another strategy using f_{II}, and incrementally add $|0\rangle^{(5)}$ to the resource.

GATES ON THE LOGICAL STATES

With the parity encoding we can deterministically perform any of the gates that can be achieved with the set $\{X_\theta, Z\}$ on a logical qubit. Here the notation is $X_\theta = \cos(\theta/2)I + i\sin(\theta/2)X$. The Z gate on a logical qubit can be performed by applying a Z gate on all the physical qubits. Since the number of sign flips obtained in this way will depend on the parity of the state, this will have the desired effect on the logical state. To perform an arbitrary X rotation on a logical qubit, we can apply that rotation to any of the physical qubits.

In order to get a universal set of gates we need to also perform the set $\{Z_{90}, \text{CNOT}\}$. These gates need to be performed nondeterministically on the encoded qubits, and performing these gates efficiently is the principal aim of this paper.

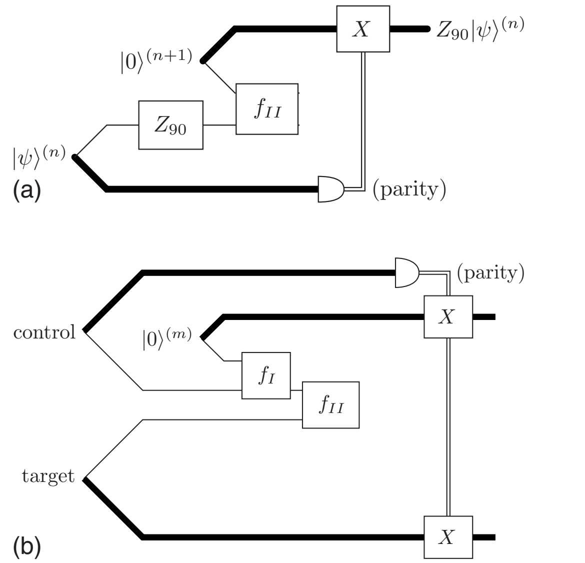

FIG. 2. (a) Implementation of the Z_{90} gate and (b) the CNOT gate. Depending on the outcomes of the fusion operations, phase flips may need to be applied to the eventual logical qubits (this is not shown on the figure for clarity). Note that for the CNOT, by choosing to measure the parity of the lower encoded qubit instead (with corresponding bit flips) the roles of target and control will be swapped.

The nondeterministic single logical-qubit gate we need is a straightforward extension of the encoding procedure. To perform the gate we first apply a Z_{90} gate on *one* of the physical qubits making up the encoded state and then fuse that qubit to a preprepared resource as depicted in Fig. 2(a). As before, if the fusion is unsuccessful we lose an encoding level from the logical qubit (the effect of the Z_{90} appears as a global phase shift in this case). If the fusion is successful on the other hand, we can now measure each remaining physical qubits of the original encoded logical qubit in the computational basis. If the parity of the result is odd, a bit flip needs to be applied to the new logical qubit. Note that it would be possible to perform a Z_θ in the same way but the parity measurement would randomly flip the angle to $-\theta$ half the time so this is not so useful.

Creating a CNOT proceeds along very similar lines to the Z_{90} gate. We first entangle the control, target, and a $|0\rangle^{(m+1)}$ resource with a combination of f_I and f_{II} fusion gates as shown in Fig. 2(b). Now by measuring the remaining physical qubits from the logical control qubit and applying a bit flip depending on the parity of the result, we perform the desired operation as follows:

$$|\psi\rangle^{(n,n)} \rightarrow \text{CNOT}|\psi\rangle^{(m,n-2)}. \qquad (11)$$

Instead of immediately reencoding the logical target or control qubits to the full amount, a nondeterministic Z_{90} operation can be incorporated into the process, thereby effectively getting it for free.

TABLE I. Success probabilities and resource usage. (a) Average number of Bell states consumed in forming $|0\rangle^{(m)}$ using f_I and no recycling. (b) Average number of Bell states consumed with recycling when advantageous. (c) Probability and (d) average resource usage of sucessfully performing Z_{90} and reencoding in one step. The resource usage is simply the cost of generating $2|0\rangle^{(n+1)}$, and involves no recycling. (e) Resource usage to performg Z_{90} using recycling. The values were calculated numerically from 500 000 runs.

m	(a)	(b)	(c)	(d)	(e)
3	4	4	87.48%	16	19
4	10	10	93.76%	28	25
5	16	16	96.96%	51	45
6	28	28	98.47%	76	53
7	40	38	99.20%	101	63
8	52	44	99.58%	126	78
9	64	57	99.80%	174	90
10	88	66	99.89%	222	100

We can employ the recycling of entangled states in our scheme as was done for the cluster-state proposal of [11]. The failure modes of the f_I and f_{II} fusion gates do not destroy the resource but reduce its encoding by one. This resource state can then be recycled for further attempts. It should be noted, however, that recycling may not be particularly useful in either scheme. The optics and control necessary to recycle these states without degradation will probably be more difficult than simply producing more resource states from scratch.

PROBABILITY AND RESOURCE

What level of encoding do we need to maintain? If we choose too low a level then there is a significant probability that we can destroy the logical qubit through a long string of failures. If the encoding is too high then this carries an unnecessarily high resource usage.

Consider performing a Z_{90} gate on a logical qubit encoded across n physical qubits. Since the fusion gates fail with probability $1/2$, and assuming we will reencode to the full amount n in one hit, then the success probability of the gate will be $1-(1/2)^n$. The average resource requirements will just be twice the resource requirements needed to generate the state $|0\rangle^{(n+1)}$. These figures are shown in Table I(b).

If we are reencoding in multiple smaller steps then this figure will be an *upper* bound on the success probability. The advantage of reencoding in smaller steps is that we can consume fewer resources. Probabilities and resources for an alternative reencoding strategy is shown in Table I(c).

TABLE II. Success probabilities and resource usage for a CNOT. Both logical qubits initially are encoded across n physical qubits. The strategy involved preencoding the control (with resource size $|0\rangle^{(8)}$ for all except $n=6$ where it was $|0\rangle^{(7)}$) if it fell below 6 party qubits; using $|0\rangle^{(5)}$ in the actual gate itself; and postencoding back up to the initial n encoding level once the gate was successful. (a) Probability of operation. Average resources consumed with (b) no recycling and (c) with recycling are also shown. The values were calculated numerically from 100 000 runs.

n	(a)	(b)	(c)
6	96.4%	181	115
7	97.6%	190	117
8	98.2%	196	121
9	98.6%	208	126
10	98.9%	228	151

For the CNOT gate depicted in Fig. 2(b), when the encoding is sufficient that there are no boundary effects, the success probability is simply $1-(3/4)^n$ since both the f_I and f_{II} gates have to succeed. At the conclusion of the gate the logical control qubit is left encoded across m physical qubits (assuming a resource $|0\rangle^{(m+1)}$), and the target will on average lose two physical qubits from the encoding.

The success probability can be boosted by first preencoding the top logical qubit of Fig. 2(b) to boost the size of the parity code. After the gate is successful, the measurement of parity can be delayed and the size of the top logical qubit can again be increased by appending some more resources. The results of a strategy implementing this are shown in Table II.

CONCLUSION

In this paper we have presented a method for KLM-style optical quantum computation which dramatically reduces the resource usage over the original scheme. We borrow the circuit based approach and parity encoding from the KLM proposal, and the method of resource preparation from the cluster-state approach.

ACKNOWLEDGMENTS

We would like to acknowledge helpful discussions with Bill Munro and Stefan Scheel. This work was supported by the Australian Research Council and QLD State Government. We acknowledge partical support by the DTO-funded U.S. Army Research Office Contract No. W911NF-05–0397.

[1] E. Knill, R. Laflamme, and G. Milburn, Nature (London) **409**, 46 (2001).
[2] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).
[3] N. K. Langford, T. J. Weinhold, R. Prevedel, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White, Phys. Rev. Lett. **95**, 210504 (2005).
[4] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter,

Phys. Rev. Lett. **95**, 210505 (2005).

[5] R. Okamoto, H. F. Hofmann, S. Takeuchi, and K. Sasaki, Phys. Rev. Lett. **95**, 210506 (2005).

[6] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).

[7] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[8] N. Yoran and B. Reznik, Phys. Rev. Lett. **91**, 037903 (2003).

[9] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature (London) **434**, 169 (2005).

[10] C.-Y. Lu, X.-Q. Zhou, O. Guhne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, Nat. Phys. **3**, 91 (2007).

[11] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).

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

[13] T. C. Ralph, A. J. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).

[14] H. Weinfurter, Europhys. Lett. **25**, 559 (1994).

[15] S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995).

[16] J. Calsamiglia and N. Lütkenhaus, Appl. Phys. B: Lasers Opt. **72**, 67 (2001).

[17] Of course, there is some ambiguity in specifying what are to be the resources. For instance, whether we count single photon states consumed or Bell states will depend on the nature of the sources that are developed. In this paper, we shall follow the example of [11] and count the number of Bell states consumed as the primary resource in our scheme.