Efficient Toffoli gates using qudits

T. C. Ralph,[1] K. J. Resch,[2,3] and A. Gilchrist[1]
[1]*Centre for Quantum Computer Technology, University of Queensland, Brisbane 4072, QLD, Australia*
[2]*Department of Physics, University of Queensland, Brisbane 4072, QLD, Australia*
[3]*Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

(Received 24 November 2006; published 16 February 2007)

The simplest decomposition of a Toffoli gate acting on 3 qubits requires *five* 2-qubit gates. If we restrict ourselves to controlled-sign (or controlled-NOT) gates this number climbs to 6. We show that the number of controlled-sign gates required to implement a Toffoli gate can be reduced to just 3 if one of the three quantum systems has a third state that is accessible during the computation—i.e., is actually a qutrit. Such a requirement is not unreasonable or even atypical since we often artificially enforce a qubit structure on multilevel quantums systems (e.g., atoms, photonic polarization plus spatial modes). We explore the implementation of these techniques in optical quantum processing and show that linear optical circuits could operate with much higher probabilities of success.

DOI: 10.1103/PhysRevA.75.022313 PACS number(s): 03.67.Lx, 42.50.Dv

I. INTRODUCTION

Quantum computing promises major increases in computing power but poses many experimental hurdles to its implementation [1]. Finding more efficient ways to implement quantum gates may allow small-scale quantum computing tasks to be demonstrated on a shorter time scale. A key quantum gate is the Toffoli gate. The Toffoli gate acts on three qubits and in conjunction with the Hadamard gate forms perhaps the simplest universal gate set in quantum computing [2].

In this paper we show that the number of two-qubit gates required to implement a Toffoli gate can be reduced by making one of the qubits in the circuit a qutrit (or, in the general case, a qudit). The qutrit nature will only manifest during the gate—after the gate only the qubit levels will be occupied. Remarkably, the additional space afforded by the extra level on one qubit provides a significant reduction in the resource requirements. This reduction is particularly dramatic for optical implementations where systems for applying the envisaged manipulations exist quite naturally. The paper is arranged in the following way. In the next section we introduce the scheme in an abstract, implementation-independent, way and demonstrate its increased efficiency. In Sec. III we consider various optical realizations and then summarize and conclude in our final section.

II. TOFFOLI GATE WITH QUDITS

We begin by showing how a Toffoli gate can be implemented using only three controlled sign (CS) gates plus single qubit unitaries by allowing one of the qubits to be a qutrit. To our knowledge the most efficient implementation that has been described using only qubits involves five 2-qubit gates [3,4]. If we restrict ourselves to using only CS gates, then six CS gates plus various single-qubit gates are needed [1].

Figure 1 shows the arrangement to implement a Toffoli-Sign (TS) gate—i.e., a three-qubit gate that applies a sign change on one and only one of the state components and the identity is implemented otherwise. It is of no consequence which state component is sign flipped, and the flipped component will vary between our various implementations. All such gates are locally equivalent and can be interconverted with straightforward single-qubit bit flips. The TS gate becomes a Toffoli gate by placing Hadamard gates before and after the gate on one of the qubits, which then becomes the target qubit. The two control qubits are labeled as usual with logical states **0** and **1** (where we reserve bold print for indicating logical values). The target is a qutrit for which we label the additional state **2**. We assume C-S gates and Hadamard gates are available. We note that a CNOT gate can be constructed from a C-S gate using a pair of Hadamard gates. We require one additional gate that we label X_A, which enables transitions between the **0** and **2** states. The C-S (and CNOT) gate act on the qubit levels in the usual way. If they act on a qutrit in the state **2** then both gates implement the identity regardless of the value of the control qubit. The first operation we perform is to apply an X_A gate to the target qutrit. The X_A gate is defined by the following actions on the basis states: $X_A|\mathbf{0}\rangle \to |\mathbf{2}\rangle$, $X_A|\mathbf{2}\rangle \to |\mathbf{0}\rangle$, $X_A|\mathbf{1}\rangle \to |\mathbf{1}\rangle$. Consider an arbitrary three-qubit state

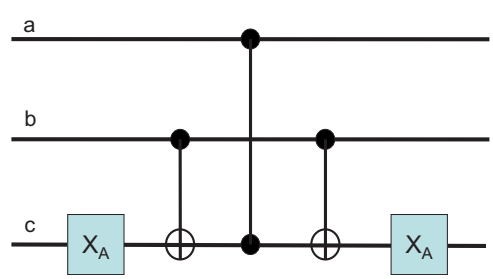

FIG. 1. (Color online) Realization of a TS gate using two qubits (a and b) and a qutrit (c). Controlled-NOT (CNOT) gates (first and last two-qubit gates) operate as normal on the qubit levels and implement the identity if the target is in the qutrit level ($|\mathbf{2}\rangle$). Similarly for the CS gate (middle two-qubit gate). The X_A gate flips the qutrit between the states **0** and **2**. The sign change occurs on the $|\mathbf{1},\mathbf{0},\mathbf{1}\rangle$ component.

 ©2007 The American Physical Society

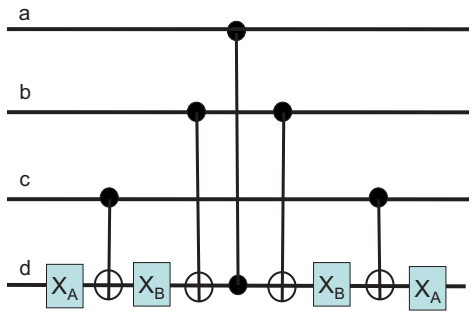

FIG. 2. (Color online) Realization of an ($n=3$) level TS gate using three qubits (a, b, and c) and a ququit (d). CNOT gates operate as normal on the qubit levels and implement the identity if the target is in the ququit levels (**2** or **3**). Similarly for the CS gate. The X_A gate flips the ququit between the states **0** and **2**. The X_B gate flips the ququit between the states **1** and **3**. The sign change occurs on the $|\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1}\rangle$ component.

$$\sum_{i,j,k=0,1} \alpha_{i,j,k}|i,j,k\rangle, \tag{1}$$

where $|i,j,k\rangle \equiv |i\rangle_a|j\rangle_b|k\rangle_c$ and the ket subscripts label the different qubits according to Fig. 1. After the application of the X_A gate on the qutrit (c) we have

$$\sum_{i,j=0,1} (\alpha_{i,j,0}|i,j,\mathbf{2}\rangle + \alpha_{i,j,1}|i,j,\mathbf{1}\rangle). \tag{2}$$

We now apply a CNOT gate between b and c to obtain

$$\sum_{i=0,1} (\alpha_{i,0,0}|i,\mathbf{0},\mathbf{2}\rangle + \alpha_{i,0,1}|i,\mathbf{0},\mathbf{1}\rangle + \alpha_{i,1,0}|i,\mathbf{1},\mathbf{2}\rangle + \alpha_{i,1,1}|i,\mathbf{1},\mathbf{0}\rangle). \tag{3}$$

Next a CS gate is applied between a and the c, resulting in

$$\begin{aligned}&\alpha_{0,0,0}|\mathbf{0},\mathbf{0},\mathbf{2}\rangle + \alpha_{1,0,0}|\mathbf{1},\mathbf{0},\mathbf{2}\rangle + \alpha_{0,0,1}|\mathbf{0},\mathbf{0},\mathbf{1}\rangle - \alpha_{1,0,1}|\mathbf{1},\mathbf{0},\mathbf{1}\rangle \\ &\quad + \alpha_{0,1,0}|\mathbf{0},\mathbf{1},\mathbf{2}\rangle + \alpha_{1,1,0}|\mathbf{1},\mathbf{1},\mathbf{2}\rangle \\ &\quad + \alpha_{0,1,1}|\mathbf{0},\mathbf{1},\mathbf{0}\rangle + \alpha_{1,1,1}|\mathbf{1},\mathbf{1},\mathbf{0}\rangle.\end{aligned} \tag{4}$$

Now a CNOT gate is again applied between b and c, and finally the X_A gate is again applied to the qutrit. The state is then

$$\begin{aligned}&\alpha_{0,0,0}|\mathbf{0},\mathbf{0},\mathbf{0}\rangle + \alpha_{1,0,0}|\mathbf{1},\mathbf{0},\mathbf{0}\rangle + \alpha_{0,0,1}|\mathbf{0},\mathbf{0},\mathbf{1}\rangle - \alpha_{1,0,1}|\mathbf{1},\mathbf{0},\mathbf{1}\rangle \\ &\quad + \alpha_{0,1,0}|\mathbf{0},\mathbf{1},\mathbf{0}\rangle + \alpha_{1,1,0}|\mathbf{1},\mathbf{1},\mathbf{0}\rangle \\ &\quad + \alpha_{0,1,1}|\mathbf{0},\mathbf{1},\mathbf{1}\rangle + \alpha_{1,1,1}|\mathbf{1},\mathbf{1},\mathbf{1}\rangle,\end{aligned} \tag{5}$$

as expected for a TS gate with the sign change implemented on the $|\mathbf{1},\mathbf{0},\mathbf{1}\rangle$ component. This technique can be generalized straightforwardly to higher-order n-control-bit Toffoli gates by introducing an $(n+1)$-level qudit as the target. Figure 2 shows an explicit construction of the next level up, the $n=3$, TS gate. In general the number of two-qubit gates required for this method is $2n-1$. This seems a significant improvement on previous estimates of optimal gate numbers for higher order Toffoli gates. For example, Ref. [5] finds that 64 two-qubit gates are required for a five-control-bit Toffoli while our qudit construction requires only 9. These results suggest that the computational depth of quantum processing circuits might be significantly reduced by employing these techniques. In the next section we discuss various ways in which the required manipulations can be realized in optics.

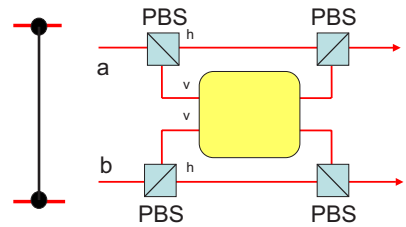

FIG. 3. (Color online) Schematic of the implementation of an optical CS gate using a strong cross-Kerr nonlinearity χ. PBS are polarizing beam splitters.

III. OPTICAL IMPLEMENTATIONS

We now turn specifically to an optical encoding and show that for this encoding the manipulations discussed in the previous section have natural physical realizations. First consider dual-rail encoding in which the logical qubit states are given as $|\mathbf{0}\rangle = |1\rangle_h \otimes |0\rangle_v$ and $|\mathbf{1}\rangle = |0\rangle_h \otimes |1\rangle_v$ where $|i\rangle_j$ is the ith Fock state of the jth optical mode (with plain text reserved for Fock state occupation number). The optical modes are orthogonal and may represent, for example, different polarization or spatial modes. To create a qutrit we simply add an extra mode such that, in the language of the previous section, $|0\rangle = |100\rangle$, $|\mathbf{1}\rangle = |010\rangle$, and $|\mathbf{2}\rangle = |001\rangle$, where we have simplified our nomenclature such that $|i\rangle_h \otimes |j\rangle_v \otimes |k\rangle_s = |ijk\rangle$, where s labels the new mode. In the following we will show that linear optical elements plus proposed two-qubit optical gates are sufficient to implement the operations used in the previous section. We begin by discussing deterministic two-qubit gates based on strong nonlinearities. We then consider heralded nondeterministic gates based on measurement-induced nonlinearities. Finally we consider demonstration gates based on post-selected measurement-induced nonlinearities. In each case we find considerable advantages to our qudit implementation.

A. Deterministic gates

It has long been known that a strong cross-Kerr nonlinearity enables the implementation of universal optical quantum gates on the encoding we have just introduced [6]. In particular a χ_3 nonlinear medium can be used to induce a cross-Kerr effect between the relevant photon modes. Ideally the cross-Kerr effect will produce the unitary evolution $\hat{U}_K = \exp[i\chi\hat{a}^\dagger\hat{a}\hat{b}^\dagger\hat{b}]$, where $\hat{a}$ is the annihilation operator for one optical mode and $\hat{b}$ another. Consider the schematic setup of Fig. 3. Two polarization-encoded qubits are converted into spatial dual rail qubits using polarizing beam splitters. One mode from each of the qubits is sent through the cross-Kerr material. The operation of this device on an arbitrary two-qubit input state is given by the following evolution:

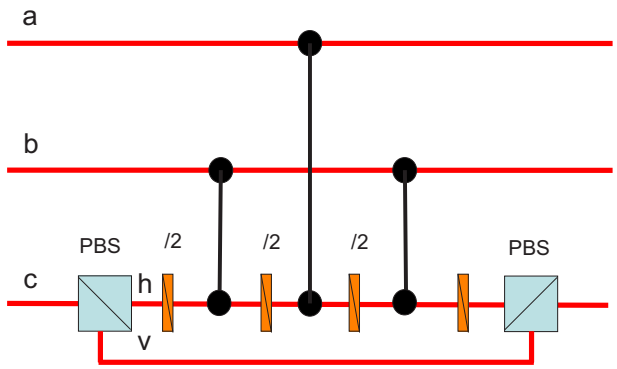

FIG. 4. (Color online) Optical realization of a TS gate. Polarizing beam splitters (PBS) act as X_A gates by accessing an additional spatial mode. The half-wave plates ($\lambda/2$) are set at 22.5° so as to act as Hadamard gates and the CS gates are implemented as per Fig. 3.

$$
\begin{aligned}
|\psi\rangle \to \hat{U}_K|\psi\rangle &= e^{i\chi\hat{a}_v^\dagger\hat{a}_v\hat{b}_v^\dagger\hat{b}_v}(\alpha|10\rangle_a|10\rangle_b + \beta|01\rangle_a|10\rangle_b \\
&\quad + \gamma|10\rangle_a|01\rangle_b + \delta|01\rangle_a|01\rangle_b) \\
&= \alpha|10\rangle_a|10\rangle_b + \beta|01\rangle_a|10\rangle_b + \gamma|10\rangle_a|01\rangle_b \\
&\quad + e^{i\chi}\delta|01\rangle_a|01\rangle_b. \qquad (6)
\end{aligned}
$$

Only when both modes entering the Kerr material are occupied is a phase shift induced. If we now choose the strength of the nonlinearity such that $\chi=\pi$, the effect is to flip the sign of one element of the superposition, producing a CS gate. We can introduce a third spatial mode by using polarization rotation and polarizing beam splitters and hence implement the control gate sequence required in Sec. I as shown in Fig. 4. Notice, from Eq. (6), that this CS gate implements the identity if both polarization modes are unoccupied as required. Only three χ_3 interactions are required compared with the five or six that would be needed to implement the Toffoli gate by the usual qubit gates. Thus the same saving is made as discussed for the abstract case.

Unfortunately Kerr materials with the required strength of nonlinearity are not presently available. As a result we now consider nondeterministic implementations based on measurement-induced nonlinearites.

B. Heralded gates

Knill, Laflamme, and Milburn have shown that scalable quantum gates can be implemented on optical qubits using linear elements, photon counters, and photon sources [7]. In particular, using linear optical elements, photon counters, and an entangled photon pair as resources, it is possible to implement the optical CS gate of the previous section nondeterministically with a probability of success of 1/4 [8]. Gate success is heralded by the photon counter signature obtained from the entangled pair after interaction with the qubits. If we used the direct method of implementing a Toffoli gate via a sequence of CS gates and single-qubit unitaries, we would require six entangled pairs and the probability of success would drop to $(1/4)^6=1/4096$. Recently Fiurášek [9] suggested a dedicated scheme requiring only three entangled pairs with a probability of success of 1/1065. His method offered significant reduction in the number of entangled pairs required, but only a modest increase in the success probability. Our method further reduces the number of additional entangled pairs and dramatically improves the success probability. In the following we will adapt our qutrit techniques to linear optics and obtain a heralded Toffioli gate requiring only two entangled pairs and working with a probability of success of 1/32.

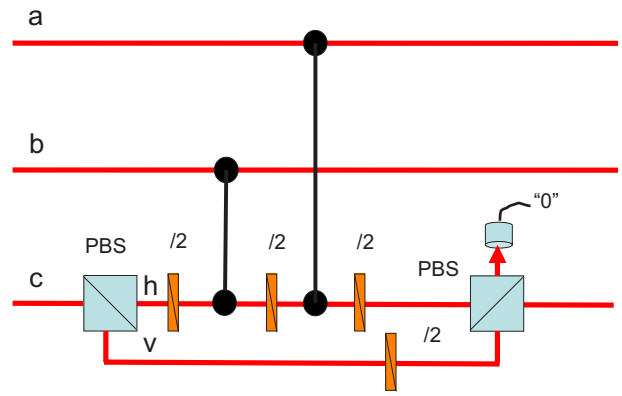

FIG. 5. (Color online) Nondeterministic, but heralded, optical realization of a TS gate. Polarizing beam splitters (PBS) act as X_A gates by accessing an additional spatial mode. The half-wave plates ($\lambda/2$) act as Hadamard gates and the CS gates are implemented using heralded nondeterministic gates. The sign change occurs on the $|\mathbf{0},\mathbf{0},\mathbf{1}\rangle$ component.

The proposed setup is shown in Fig. 5. It is similar to the deterministic gate setup except that the CS gates are assumed nondeterministic and the final two-qubit gate is replaced with a passive quantum filter. Notice that, because we are also exploiting the polarization degree of freedom on the second spatial mode, the target is now effectively a ququit (a four-level quantum system). Each two-qubit gate works with a probability of success 1/4 and requires an entangled pair for their operation. The filter succeeds with probability 1/2 and does not require any ancilla qubits for its operation. The gate works in the following way: the state after the second CS gate (see Fig. 5) is

$$
\begin{aligned}
&\alpha_{0,0,0}|H,H,\text{vac},H\rangle + \alpha_{1,0,0}|V,H,\text{vac},H\rangle + \alpha_{0,0,1}|H,H,V,\text{vac}\rangle \\
&\quad - \alpha_{1,0,1}|V,H,V,\text{vac}\rangle + \alpha_{0,1,0}|H,V,\text{vac},H\rangle \\
&\quad + \alpha_{1,1,0}|V,V,\text{vac},H\rangle + \alpha_{0,1,1}|H,V,H,\text{vac}\rangle \\
&\quad + \alpha_{1,1,1}|V,V,H,\text{vac}\rangle, \qquad (7)
\end{aligned}
$$

conditional on the correct photon counting outcomes from the previous two CS gates (probability of success 1/16). Here H and V refer to horizontally and vertically polarized single-photon states, respectively, and "vac" refers to the vacuum state (both polarization modes unoccupied)—i.e., $|H\rangle=|10\rangle\equiv|\mathbf{0}\rangle$, $|V\rangle=|01\rangle\equiv|\mathbf{1}\rangle$, and $|\text{vac}\rangle=|00\rangle$. The initial state is as defined in Eq. (1) and the ordering of the kets corresponds to top to bottom in Fig. 5. Instead of using a third CS gate as in the deterministic scheme, half-wave plates oriented at 22.5° are applied to both target modes, leading to the state

$$\alpha_{0,0,0}|H,H,\text{vac},D\rangle + \alpha_{1,0,0}|V,H,\text{vac},D\rangle + \alpha_{0,0,1}|H,H,A,\text{vac}\rangle - \alpha_{1,0,1}|V,H,A,\text{vac}\rangle + \alpha_{0,1,0}|H,V,\text{vac},D\rangle + \alpha_{1,1,0}|V,V,\text{vac},D\rangle + \alpha_{0,1,1}|H,V,D,\text{vac}\rangle + \alpha_{1,1,1}|V,V,D,\text{vac}\rangle, \quad (8)$$

where $|D\rangle=(1/\sqrt{2})(|H\rangle+|V\rangle)$ and $|A\rangle=(1/\sqrt{2})(|H\rangle-|V\rangle)$. The third and fourth modes are then recombined on a polarizing beam splitter and the output mode is conditioned on a zero detection at the second output port of the polarizing beam splitter. The probability of the zero detection is 1/2, producing the conditional output state

$$\alpha_{0,0,0}|H,H,H\rangle + \alpha_{1,0,0}|V,H,H\rangle - \alpha_{0,0,1}|H,H,V\rangle + \alpha_{1,0,1}|V,H,V\rangle + \alpha_{0,1,0}|H,V,H\rangle + \alpha_{1,1,0}|V,V,H\rangle + \alpha_{0,1,1}|H,V,V\rangle + \alpha_{1,1,1}|V,V,V\rangle. \quad (9)$$

Hence we have produced a TS gate with the phase flip occurring on the $|H,H,V\rangle$ component. The probability of success is $1/16\times 1/2=1/32$.

The proposed heralded circuit represents a five-photon experiment. Such experiments are feasible, but difficult [10]. In the following section we propose an in principle demonstration requiring only three photons.

C. Post-selected gates

We now consider the construction of a post-selected gate. By this we mean a gate in which the photons act as their own ancilla, with success heralded by successful detection of a photon for each qubit, so-called coincidence detection. In this way a TS gate requiring only the three photons needed to represent the three qubits could be constructed. For example, we could substitute post-selected CS gates [11,12] into the circuit of Fig. 5. These gates operate with a probability of success of 1/9, so this would produce a post-selected TS gate requiring only three photons and working with a probability of success of $1/9\times 1/9\times 1/2=1/162$. However, it turns out the gate can be optimized for maximum success probability by using the techniques for chaining post-selected CS gates described in Ref. [13] and in this way achieves a success probability of 1/72 as we now describe. Fiurášek also considered this problem and proposed a different architecture with a success probability of about 1/133 [9].

Our proposed setup is shown in Fig. 6. The important part of the circuit is the central string of two interferometers created from the top target mode (T). First, if this mode is unoccupied, photons can only emerge in all three output qubits if they remain in their respective modes. In this case no phase flip occurs. If the top target mode is occupied, we must consider passage of the photon through the central interferometers. The first interferometer is antibalanced if the bottom mode of the first control mode $C1$ is unoccupied. As a result the photon couples completely into the bottom mode of the second interferometer with a phase flip. On the other hand, if the bottom mode of the first control is occupied, there will be no phase change at the one-third beam splitter in the first interferometer due to two-photon interference (assuming a single photon exits from each port of the beam splitter). In this case the first interferometer is balanced and the photon will couple completely into the top mode of the second interferometer. Now we turn to the second interferometer. If the top mode of the second control mode $C2$ is unoccupied, then passage through the bottom mode of the interferometer induces a phase flip. But recall that this will only occur if the photon has undergone a phase flip in the first interferometer. Thus, if the photon subsequently makes it into the output target mode, it will not have undergone a phase flip. Similarly, if the target photon couples into the top mode of the second interferometer, then it will not have undergone a phase flip in the first interferometer and will not undergo any further phase flip if it subsequently makes it to the output target mode, regardless of the state of the $C2$ control mode. Finally, if the photon couples into the bottom mode of the second interferometer (meaning that control mode $C1$ had its bottom mode unoccupied and the photon has picked up a phase flip) and mode $C2$ has its top mode occupied, two-photon interference at the one-third beam splitter in the second interferometer then leads to no phase flip. Thus, if the target photon subsequently makes it to the output, this state component will carry a phase flip. Summarizing, we find that the only state component that will carry a phase flip will be the one in which every qubit was in its logical 0 state, where we take occupation of the top mode to be logical 0. The beam splitter ratios are picked such that all state components have equal probability to lead to an event with a photon appearing in all the output qubits. That probability turns out to be 1/72.

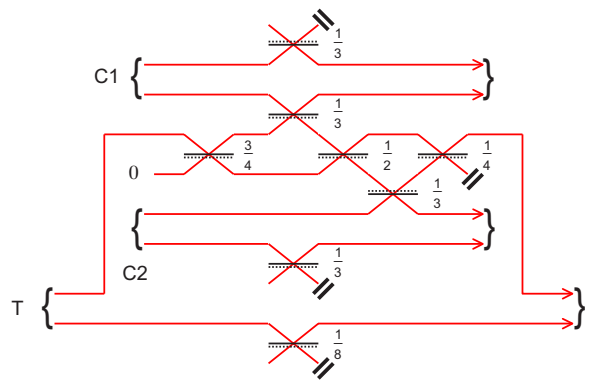

FIG. 6. (Color online) Nondeterministic, post-selected, optical realization of a TS gate. In contrast to the other figures all optical modes are shown explicitly; thus, each input qubit is represented by two modes. Note that in the central part of the diagram there are a total of seven modes, due to the introduction of an additional target mode. Beam splitters are represented as black lines with their reflectivity indicated to the right. The beam splitters are assumed to be asymmetric; i.e., a phase flip is induced by reflection off one surface but all other components suffer no phase change. The surface for which the phase flip occurs is indicated by a dotted line. If we take occupation of the top mode of each qubit to represent logical 0 and occupation of the bottom mode to represent logical 1, then the circuit implements a TS gate in which a phase flip is only applied to the element $|\mathbf{000}\rangle$. The figure is represented, for clarity, as if all modes are spatial. In an experimental realization polarization modes would be utilized where ever possible.

IV. CONCLUSION

We have discussed the implementation of Toffoli gates in circuits where one of the qubits is allowed to be a qutrit, or more generally a qudit, and shown that increased gate efficiency can be achieved. In particular we showed that instead of six CS gates, as required for a qubit only circuit, introducing a qutrit allows this to be reduced to three CS gates. For an n-control-bit Toffoli gate the required gate number is $2n-1$ if a $(n+1)$-level qudit is available. We showed that for deterministic optical quantum processing a natural implementation method could be identified. For nondeterministic optical approaches further simplifications could be identified, leading to a heralded Toffoli gate with a probability of success of $1/32$ and a post-selected gate with a probability of success of $1/72$. These latter results open the door to experimental optical demonstrations of Toffoli gates in the near future and make small-scale applications appear more feasible. It is interesting to note that a nonuniversal set of qubit gates, CS plus Hadamard gates (an additional $\pi/8$ gate is required to make this a universal set), becomes universal, Toffoli plus Hadamard, gates when a single additional quantum level is introduced.

ACKNOWLEDGMENTS

We thank J. L. Dodd, G. J. Pryde, and J. L. O'Brien for useful discussions. This work was supported by the Australian Research Council, the Queensland State Government and the DTO-funded U.S. Army Research Office Contract No. W911NF-05-0397.

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK 2000).
[2] Yaoyun Shi, e-print quant-ph/0205115.
[3] A. Barenco, C. H. Bennett, R. Cleve, D. P. Divincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolen, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[4] We note that a 3 two-qubit gate construction does exist for the so-called "simplified Toffoli gate" that differs from the true Toffoli gate by a nontrivial phase factor: N. Margolus, in *Collision Based Computation*, edited by A. Adamatzky (Springer-Verlag, Berlin, 2002), p. 107.
[5] D. Maslov and G. W. Dueck, e-print quant-ph/0403053.
[6] G. J. Milburn, Phys. Rev. Lett. **62**, 2124 (1989).
[7] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[8] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **64**, 062311 (2001).
[9] J. Fiurášek, Phys. Rev. A **73**, 062313 (2006).
[10] Q. Zhang, A. Goebel, C. Wagenknecht, Y.-A. Chen, B. Zhao, T. Yang, A. Mair, J. Schmiedmayer, and J.-W. Pan, Nat. Phys. **2**, 678 (2006).
[11] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, Phys. Rev. A **65**, 062324 (2002).
[12] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature (London) **426**, 264 (2003).
[13] T. C. Ralph, Phys. Rev. A **70**, 012312 (2004).