Invited Paper

Quantum Computation based on Linear Optics

T.C.Ralph[a], W.J.Munro[b] and G.J.Milburn[a]

[a] Centre for Quantum Computer Technology,
University of Queensland, QLD 4072, Australia
[b] Hewlett Packard Laboratories, Filton Road, Stoke Gifford,
Bristol BS34 8QZ, U.K

ABSTRACT

We review recent theoretical progress in finding ways to do quantum processing with linear optics, non-classical input states and conditional measurements. We focus on a dual rail photonic scheme and a single rail coherent state scheme.

Keywords: Quantum Computation, Quantum Optics, Quantum Information

1. INTRODUCTION

Optics has played a major role in the testing of fundamental properties of quantum mechanics and, more recently, implementing simple quantum information protocols. This has been possible because photons are easily produced and manipulated and, as the electro-magnetic environment at optical frequencies can be regarded as vacuum, are relatively decoherence free. One of the earliest proposals[1] for implementing quantum computation was based on encoding each qubit in two optical modes, each containing exactly one photon (so-called dual rail logic). Unfortunately, 2 qubit gates would seem to require strong interactions between single photons. Such interactions would require massive, reversible non-linearities well beyond those presently available.

Knill , Laflamme and Milburn (KLM) found a way to circumvent this problem by showing that non-deterministic 2 qubit gates can be implemented using only linear optical networks and conditional photon number measurements.[2] Further, KLM showed that near deterministic gates could be created from these non-deterministic gates through the technique of teleporting gates.[3] Thus an efficiently scalable quantum computation scheme was devised using only single photon sources, photon counting and linear optics.

A number of groups around the world are now working on demonstrating KLM type gates and some first steps have been taken.[4] In section 2 we review the physics of the basic operation of the KLM gates and simplified test gate arrangements.[5] These test gates have the property that their operation can be confirmed with present, spontaneous photon source technology, but if fed with deterministic single photon sources could perform as true KLM gates.

Although KLM showed in principle that scale up is possible with such gates using only linear elements, the optical networks described by KLM are very complex. Thus there is considerable interest in finding simpler architectures based, perhaps on different encoding schemes. In section 3 of this manuscript we review a scheme of this type, based on a single rail (ie only one quantum optical mode) coherent state encoding.[6]

2. PHOTONIC QUBIT GATES

In this section we look at the physics of the KLM gates and simplifications to their construction and testing.

Further author information: (Send correspondence to TCR)
TCR: E-mail: ralph@physics.uq.edu.au

Quantum Optics in Computing and Communications, Songhao Liu, Guangcan Guo, Hoi-Kwong Lo,
Nobuyuki Imoto, Editors, Proceedings of SPIE Vol. 4917 (2002) © 2002 SPIE · 0277-786X/02/$15.00

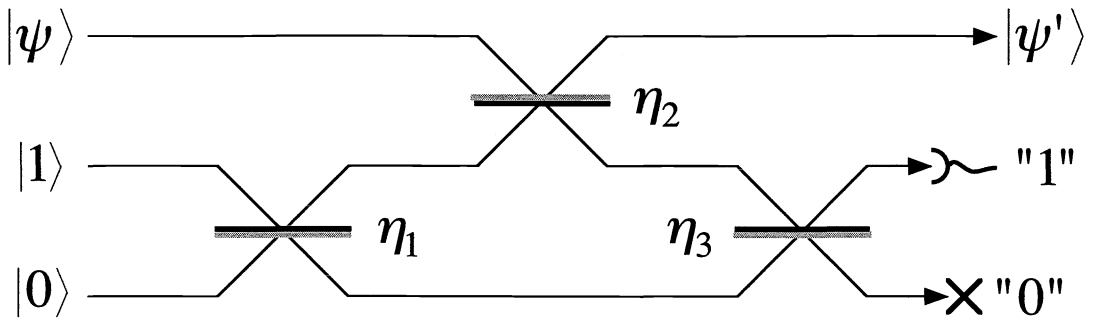

Figure 1. Schematic of NS gate. Grey indicates the surface from which a sign change occurs upon reflection. The use of this beamsplitter phase convention is convenient but not essential.

2.1. The NS Gate

The basic element in the construction of our non-deterministic CNOT gate is the nonlinear sign-shift (NS) gate.[2] This is a non-deterministic gate the operation of which is conditioned on the detection of an auxiliary photon. When successful the gate implements the following transformation on signal state $|\psi\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \rightarrow |\psi'\rangle = 0.5(\alpha|0\rangle + \beta|1\rangle - \gamma|2\rangle) \tag{1}$$

where the lack of normalization of the transformed state reflects the fact that the gate has a probability of success of $0.25 = (0.5)^2$. Fig.1 shows a realization of this gate. Two ancilla modes are required. A single photon is injected into one of the ancilla and the other is unoccupied. The first, second and third beamsplitters have intensity reflectivities η_1, η_2 and η_3 respectively. The beamsplitters are phase asymmetric: transmission from either side and reflection off the "black" surface of these beamsplitters results in no phase change, whilst reflection off the "grey" surface results in a sign change. When a single photon is counted at the "1" ancilla output and no photon is counted at the "0" ancilla output (as indicated in the figure) the transformation of Eq.1 is implemented if a suitable choice of beamsplitter reflectivities is made. Let us see how this works. Suppose first that the signal mode is in the vacuum state, i.e. $|\psi\rangle = |0\rangle$. The probability amplitude, C, for the ancilla photon to appear at the "1" output port is given by

$$C = \sqrt{\eta_1\eta_2\eta_3} + \sqrt{(1-\eta_1)(1-\eta_3)} \tag{2}$$

Now suppose the input is a single photon state, i.e. $|\psi\rangle = |1\rangle$. If a photon arrives at the "1" output port and no photon arrives at the "0" port then a single photon must have exited the signal output. We wish the probability amplitude for this event to also be C. This means

$$\begin{aligned} C &= \sqrt{\eta_1\eta_3}(1-\eta_2) - (\sqrt{\eta_1\eta_2\eta_3} + \sqrt{(1-\eta_1)(1-\eta_3)})\sqrt{\eta_2} \\ &= \sqrt{\eta_1\eta_3}(1-\eta_2) - C\sqrt{\eta_2} \end{aligned} \tag{3}$$

and thus

$$C = \frac{\sqrt{\eta_1\eta_3}(1-\eta_2)}{1+\sqrt{\eta_2}} \tag{4}$$

Finally we consider the situation of a two photon input, i.e. $|\psi\rangle = |2\rangle$. If a single photon arrives at the "1" port and no photon arrives at the "0" port then two photons must have exited at the signal output. To obtain the

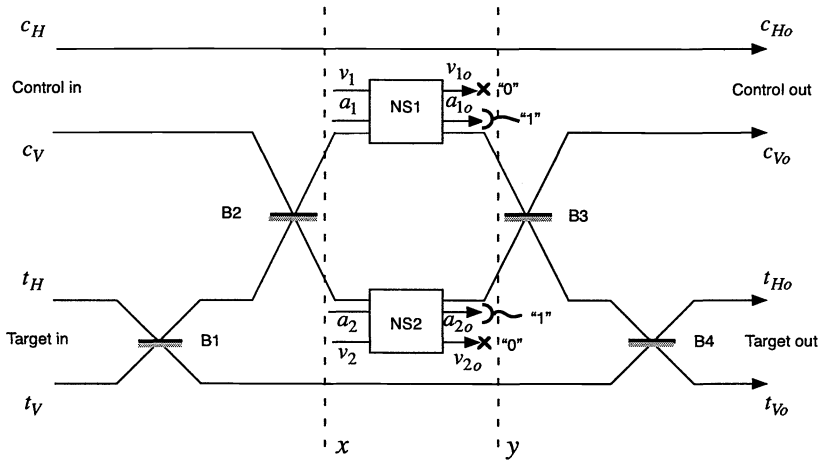

Figure 2. Schematic of CNOT gate. Grey indicates the surface from which a sign change occurs upon reflection. Note that if B1 and B4 were not present the gate would implement a control sign shift. B1 and B4 paly the role of Hadamard gates converting sign shift to CNOT operation

sign change of Eq.1 we require the probability amplitude for this event to be $-C$. This means

$$\begin{aligned} -C &= -\sqrt{\eta_1\eta_3\eta_2}(1-\eta_2) - \sqrt{\eta_2}(\sqrt{\eta_1\eta_3}(1-\eta_2) - (\sqrt{\eta_1\eta_2\eta_3} + \sqrt{(1-\eta_1)(1-\eta_3)})\sqrt{\eta_2}) \\ &= \eta_2 C - 2\sqrt{\eta_1\eta_2\eta_3}(1-\eta_2) \end{aligned} \tag{5}$$

Substituting Eq.4 into Eq.5 gives the result

$$\eta_2 = (\sqrt{2}-1)^2 \tag{6}$$

Substituting back into Eq.4 and Eq.2 we can solve for η_1, η_3 and C. The maximum value for C is achieved when

$$\eta_1 = \eta_3 = \frac{1}{(4-2\sqrt{2})} \tag{7}$$

and is

$$C = 0.5 \tag{8}$$

Thus the transformation of Eq.1 is implemented whenever a single photon is recorded at port "1" and no photon is found at port "0". On average this will occur 25% of the time since $|C|^2 = 0.25$.

2.2. The CNOT Gate

A conditional CNOT gate can now be implemented using two NS gates. The layout for doing this is shown schematically in Fig.2. We employ dual rail logic such that the "control in" qubit is represented by the two bosonic mode operators c_H and c_V. A single photon occupation of c_H with c_V in a vacuum state will be our logical 0, which we will write $|H\rangle$ (to avoid confusion with the vacuum state). Whilst a single photon occupation of c_V with c_H in a vacuum state will be our logical 1, which we will write $|V\rangle$. Of course superposition states can also be formed. Similarly the "target in" is represented by the bosonic mode operators t_H and t_V with the same interpretations as for the control. The beamsplitters, $B1$, $B2$, $B3$ and $B4$ are all 50:50.

The four modes c_H, c_V, t_H and t_V are all the same polarization. The use of the "H", "V" nomenclature alludes to the standard situation in which the two modes of the dual rail logic are orthogonal polarization modes. Conversion of a polarization qubit into the spatial encoding used to implement the CNOT gate can be

achieved experimentally by passing the the photon through a polarizing beamsplitter, to spatially separate the modes, and then using a half-wave plate to rotate one of the modes into the same polarization as the other. After the gate, the reverse process can be used to return the encoding to polarization.

The layout of Fig.2 contains two nested, balanced Mach-Zehnder interferometers. The target modes are combined and then re-separated forming the "T"interferometer. One arm of the T interferometer and the c_V mode of the control are combined to form another interferometer, the "C" interferometer. NS gates are placed in both arms of the C interferometer. The essential feature of the system is that if the control photon is in the c_H mode then there is never more that one photon in the C interferometer, so the NS gates do not produce a change, the T interferometer remains balanced and the target qubits exit in the same spatial modes in which they entered. On the other hand if the control photon is in mode c_V then there is a two photon component in the C interferometer which suffers a sign change due to the NS gates. This leads to a sign change in one arm of the T interferometer and the target qubit exits from the opposite mode from which it entered.

Let us consider the systems operation in more detail: If the control is in a logical 0 then the mode c_V will be in a vacuum state. Consider the line labeled x in Fig.2 lying just before the NS gates. The state of the system at this point is given by

$$|\psi\rangle_x = \frac{1}{\sqrt{2}}|1001\rangle \pm \frac{1}{2}(|1100\rangle - |1010\rangle) \tag{9}$$

where the left to right ordering is equivalent to the top to bottom ordering in Fig.2. The + occurs when the target input state is $|H\rangle$, the − occurs when the target input state is $|V\rangle$. Now consider the state of the system directly after the NS gates operate on the middle two modes (indicated by the line y in Fig.2). Substituting from Eq.1 we find $|\psi\rangle_y = 0.25|\psi\rangle_x$. That is the gates do not effect the states in the arms of the C interferometer (conditional on the detection of photons at the "1" ports of the NS gates). As both interferometers are balanced they will just return the same outputs as they had inputs. Thus c_{Vo} will be a vacuum mode, and if the target input photon was in t_H, it will emerge in t_{Ho}; or if it was in t_V, it will emerge in t_{Vo}. In other words the control and target qubits will remain in the same states.

On the other hand if the control is in a logical 1, then the c_V mode will contain one photon. The state at x is now

$$|\psi\rangle_x = \frac{1}{2}(|0101\rangle + |0011\rangle \pm (|0200\rangle - |0020\rangle)) \tag{10}$$

The two photon amplitudes suffer sign changes (conditional on the detection of photons at the "1" ports of the NS gates) such that the state at y, after the NS gates, is now

$$|\psi\rangle_y = 0.25(\frac{1}{2}(|0101\rangle + |0011\rangle \mp (|0200\rangle - |0020\rangle))) \tag{11}$$

This leads to a sign change in the returning beam of the T interferometer which in turn results in a swap between the inputs and outputs of the T interferometer. Thus if the target input photon was in t_H it will emerge in t_{Vo} or if it was in t_V it will emerge in t_{Ho}. The control output, c_{Vo} also suffers a sign change, but this does not change its logical status. In other words the control is unchanged but the target qubit will change states.

The truth table of the device is thus

$$\begin{aligned} |H\rangle_c|H\rangle_t &\rightarrow |H\rangle_c|H\rangle_t, \quad |H\rangle_c|V\rangle_t \rightarrow |H\rangle_c|V\rangle_t \\ |V\rangle_c|H\rangle_t &\rightarrow |V\rangle_c|V\rangle_t, \quad |V\rangle_c|V\rangle_t \rightarrow |V\rangle_c|H\rangle_t \end{aligned} \tag{12}$$

Which is CNOT logic.

It is useful to also look at this arrangement in the Heisenberg picture. Referring again to Fig.2 our input modes are c_H and c_V for the control, t_H and t_V for the target, and the ancilla modes a_1, a_2, v_1 and v_2. The initial state of c_i, t_j, a_1, a_2 is $|1,1,1,1\rangle$ where $i,j = H$ or V. The other modes are initially in the vacuum state

$|0,0,0,0\rangle$. We propagate these modes through the system and obtain the following expressions for the output modes

$$\begin{aligned} c_{Ho} &= c_H \qquad c_{Vo} = \frac{1}{\sqrt{2}}(d_1' + d_2') \\ t_{Ho} &= \frac{1}{\sqrt{2}}(t'' + t''') \qquad t_{Vo} = \frac{1}{\sqrt{2}}(t'' - t''') \\ a_{1o} &= \sqrt{\eta_3}a_1'' + \sqrt{1-\eta_3}v_1' \quad a_{2o} = \sqrt{\eta_3}a_2'' + \sqrt{1-\eta_3}v_2' \end{aligned} \tag{13}$$

where

$$\begin{aligned} t'' &= \frac{1}{\sqrt{2}}(d_1' - d_2') \qquad t''' = \frac{1}{\sqrt{2}}(t_H - t_V) \\ t' &= \frac{1}{\sqrt{2}}(t_H + t_V) \qquad a_1'' = \sqrt{\eta_2}a_1' + \sqrt{1-\eta_2}d_1 \\ a_2'' &= \sqrt{\eta_2}a_2' + \sqrt{1-\eta_2}d_2 \qquad a_1' = \sqrt{\eta_1}a_1 + \sqrt{1-\eta_1}v_1 \\ a_2' &= \sqrt{\eta_1}a_2 + \sqrt{1-\eta_1}v_2 \qquad v_1' = \sqrt{1-\eta_1}a_1 - \sqrt{\eta_1}v_1 \\ v_2' &= \sqrt{1-\eta_1}a_2 - \sqrt{\eta_1}v_2 \qquad d_1' = \sqrt{1-\eta_2}a_1' - \sqrt{\eta_2}d_1 \\ d_2' &= \sqrt{1-\eta_2}a_2' - \sqrt{\eta_2}d_2 \qquad d_1 = \frac{1}{\sqrt{2}}(c_V + t') \\ d_2 &= \frac{1}{\sqrt{2}}(c_V - t') \end{aligned} \tag{14}$$

The logical statements of Eq.12 can then be realized through measurements of 4-fold coincidences. Thus if the initial state is $|H\rangle_c|H\rangle_t$ then we find

$$\begin{aligned} \langle c_{Ho}^\dagger c_{Ho}\ t_{Ho}^\dagger t_{Ho}\ a_{1o}^\dagger a_{1o}\ a_{2o}^\dagger a_{2o}\rangle &= \frac{1}{16} \\ \langle c_{Ho}^\dagger c_{Ho}\ t_{Vo}^\dagger t_{Vo}\ a_{1o}^\dagger a_{1o}\ a_{2o}^\dagger a_{2o}\rangle &= 0 \\ \langle c_{Vo}^\dagger c_{Vo}\ t_{Vo}^\dagger t_{Vo}\ a_{1o}^\dagger a_{1o}\ a_{2o}^\dagger a_{2o}\rangle &= 0 \\ \langle c_{Vo}^\dagger c_{Vo}\ t_{Ho}^\dagger t_{Ho}\ a_{1o}^\dagger a_{1o}\ a_{2o}^\dagger a_{2o}\rangle &= 0 \end{aligned} \tag{15}$$

and similarly for the initial state $|H\rangle_c|V\rangle_t$ we find

$$\langle c_{Ho}^\dagger c_{Ho}\ t_{Vo}^\dagger t_{Vo}\ a_{1o}^\dagger a_{1o}\ a_{2o}^\dagger a_{2o}\rangle = \frac{1}{16} \tag{16}$$

with all other moments zero. However for initial state the $|V\rangle_c|H\rangle_t$ we find

$$\langle c_{Vo}^\dagger c_{Vo}\ t_{Vo}^\dagger t_{Vo}\ a_{1o}^\dagger a_{1o}\ a_{2o}^\dagger a_{2o}\rangle = \frac{1}{16} \tag{17}$$

with the other moments zero and for the initial state $|V\rangle_c|V\rangle_t$ we find

$$\langle c_{Vo}^\dagger c_{Vo}\ t_{Ho}^\dagger t_{Ho}\ a_{1o}^\dagger a_{1o}\ a_{2o}^\dagger a_{2o}\rangle = \frac{1}{16} \tag{18}$$

with the other moments zero. As expected the factor 1/16 appears as we have employed two NS gates each of which works on average 25% of the time. It can also be verified that injection of the control qubit in the superposition states $(1/\sqrt{2})(|H\rangle \pm |V\rangle)$ with the target in $|H\rangle$ or $|V\rangle$ produces correlations corresponding to the 4 entangled Bell states, as expected from quantum CNOT operation.

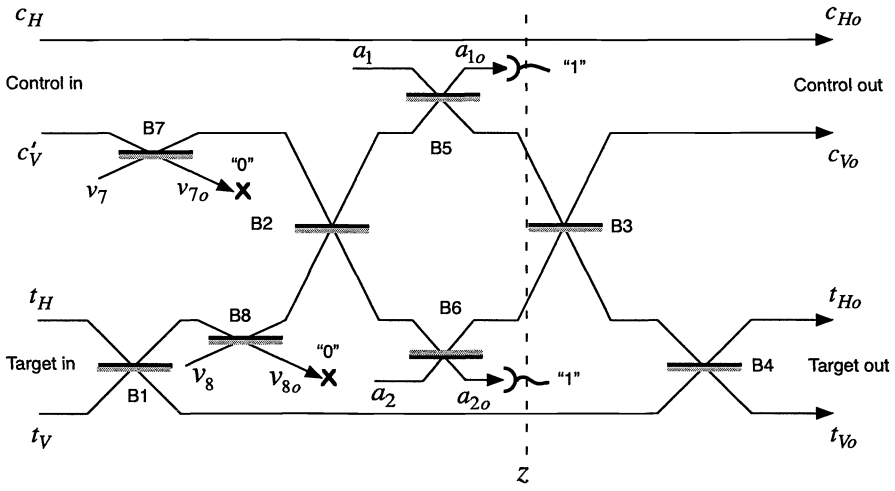

Figure 3. Schematic of simplified CNOT gate. Grey indicates the surface from which a sign change occurs upon reflection.

2.3. Simplified Gate Operation

A major experimental advantage to this set-up, as compared to the test circuit suggested in Ref.,[2] is that we can work in the coincidence basis. This allows low efficiency detectors and spontaneous single photon sources to be used to demonstrate the basic operation of the gate. Of course incorporating these gates in a scalable system as discussed in Section II requires one to know that the gate has successfully operated without destroying the output. It is straightforward to show from Eqs.13 that detection of one and only one photon in modes a_{1o} and a_{2o} and no photons in modes v_{1o} and v_{2o} is sufficient to ensure successful operation of the gate without disturbing the control and target outputs. However low-loss, 0, 1, 2-photon discriminating detection would be needed to operate in this way.

Even in the coincidence basis the above implementation represents a major technological challenge. Four nested interferometers must simultaneously be mode matched and locked to sub-wavelength accuracy over the operation time of the gate. A major simplification is achieved by operating the NS gates in a biased mode. The idea is to set the reflectivities η_1 and η_3 in the NS gates to one, i.e. totally reflective. This removes the interferometers from both the NS gates, greatly reducing the complexity of the gate. Summing over the paths as before we find that the NS operation becomes

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \rightarrow |\psi'\rangle = \sqrt{\eta_2}\alpha|0\rangle + (1-2\eta_2)\beta|1\rangle - \sqrt{\eta_2}(2-3\eta_2)\gamma|2\rangle \tag{19}$$

when $\eta_1 = \eta_3 = 1$. There is no solution such that the "0", "1" and "2" components scale equally, so the gate is biased. However this problem can be solved by placing an additional beamsplitter in the beam path with a vacuum input and conditioning on no photons appearing at its output. Now we find

$$|\psi'\rangle = \sqrt{\eta_2}\alpha|0\rangle + \sqrt{\eta_7}(1-2\eta_2)\beta|1\rangle - \eta_7\sqrt{\eta_2}(2-3\eta_2)\gamma|2\rangle \tag{20}$$

where η_7 is the reflectivity of the additional beamsplitter. Remarkably the additional degree of freedom allows the gate to be rebalanced such that exact NS operation is achieved without an interferometric element. The trade-off is a small reduction in the probability of success. Solving we find $\eta_2 = (3-\sqrt{2})/7$ and $\eta_7 = 5-3\sqrt{2}$ gives NS operation with a success probability of $\eta_2 \approx 0.23$.

There is considerable flexibility in how the simplified gate is employed in the CNOT. One of a number of possible scenarios is shown in Fig.3. The NS gates of Fig.2 have been replaced by the beamsplitters B5 and

B6 which have reflectivities η_2. Additional beamsplitters, B7 and B8, of reflectivities η_7 have been inserted in beams c_V and t' respectively. The state of the system at point z in Fig.3 (conditional on a single photon being detected at outputs a_{1o} and a_{2o} *and* no photons appearing at outputs v_{7o} and v_{8o}) is given by

$$|\psi\rangle_y = \frac{1}{\sqrt{2}}\eta_2|1001\rangle \pm \sqrt{\eta_2\eta_7}(1-2\eta_2)\frac{1}{2}(|1100\rangle - |1010\rangle) \tag{21}$$

if the control is initially in $|H\rangle$ and

$$|\psi\rangle_y = \frac{1}{2}(\sqrt{\eta_2\eta_7}(1-2\eta_2)(|0101\rangle + |0011\rangle) \mp (\eta_7\eta_2(2-3\eta_2)(|0200\rangle - |0020\rangle))) \tag{22}$$

if the control is initially in $|V\rangle$. Choosing as before $\eta_2 = (3-\sqrt{2})/7$ and $\eta_7 = 5-3\sqrt{2}$ we obtain CNOT operation with a probability $\eta_2^2 \approx 0.05$. The operation of the gate can also still be described by Eq.13 but with $\eta_1 = \eta_3 = 1$ and the substitutions

$$c_V = \frac{\sqrt{\eta_7}}{\sqrt{2}}c'_V + \sqrt{1-\eta_7}v_8, \quad t' = \frac{\sqrt{\eta_7}}{\sqrt{2}}(t_H + t_V) + \sqrt{1-\eta_7}v_7 \tag{23}$$

where now c'_V is the initial state of the control's vertical polarization mode. All the conditional moments of Eq.14-17 are reproduced but with the probabilities of the non-zero moments reduced from 1/16 to approximately 1/20. All other properties of the original gate are retained.

3. COHERENT STATE GATES

In this section we examine a scheme which, like KLM, requires only non-classical input states, conditional measurements and linear optical networks. Here the encoding is on multi-photon, coherent states.

3.1. Control Sign Gate

The idea of encoding quantum information on continuous variables of multi-photon fields has emerged recently[7] and a number of schemes have been proposed for realizing quantum computation in this way.[8–10] One drawback of these proposals is that "hard", non-linear interactions are required "in-line" of the computation. These would be very difficult to implement in practice. In contrast this proposal requires only "easy', linear in-line interactions. The hard interactions are only required for "off-line" production of resource states. A related proposal is that of Gottesman et al[11] in which superpositions of squeezed states are used to encode the qubits. There the hard interactions are only used for the initial state preparation. However, quadratic, squeezing type interactions, are required in-line along with linear interactions.

The output of a single mode, stabilized laser can be described by a coherent state, $|\alpha\rangle$ where α is a complex number which determines the average field amplitude. Coherent states are defined by unitary transformation of the vacuum,[12] $|\alpha\rangle = D(\alpha)|0\rangle$, where $D(\alpha)$ is the displacement operator. Let us consider an encoding of logical qubits in coherent states with "binary pulse code modulation", $|0\rangle_L = |0\rangle$ and $|1\rangle_L = |\alpha\rangle$, where we take α to be real.[13] The advantage of using such states is that detection is relatively easy, requiring only efficient homodyne detection.

These qubits are not exactly orthogonal, but the approximation of orthogonality is good for α even moderately large as $\langle\alpha|0\rangle = e^{-\alpha^2/2}$. We will assume for most of this paper that $\alpha >> 1$.

In single photon optics two qubit gates, in which the state of one photon controls the state of the other, represent a formidable challenge. Surprisingly, for our coherent state encoding, a non-trivial two qubit gate can be implemented using only a single beamsplitter. Consider the beamsplitter interaction given by the unitary transformation $U_{BS} = \exp[i\theta(ab^\dagger + a^\dagger b)]$, where a and b are the annihilation operators corresponding to two coherent state qubits $|\gamma\rangle_a$ and $|\beta\rangle_b$, with γ and β taking values of α or 0. It is well known that the output state produced by such an interaction is

$$U_{BS}|\gamma\rangle_a|\beta\rangle_b = |\cos\theta\gamma + i\sin\theta\beta\rangle_a|\cos\theta\beta + i\sin\theta\gamma\rangle_b \tag{24}$$

where $\cos^2\theta$ ($\sin^2\theta$) is the reflectivity (transmissivity) of the beamsplitter. Now consider the overlap between the output and input states. Using the relationship[12] $\langle\tau|\alpha\rangle = \exp[-1/2(|\tau|^2 + |\alpha|^2) + \tau^*\alpha]$ we find

$$\langle\gamma|_a\langle\beta|_b|\cos\theta\gamma + i\sin\theta\beta\rangle_a|\cos\theta\beta + i\sin\theta\gamma\rangle_b = \exp[-(\gamma^2+\beta^2)(1-\cos\theta) + 2i\sin\theta\gamma\beta] \tag{25}$$

Now suppose that θ is sufficiently small such that $\theta^2\alpha^2 << 1$ but that α is sufficiently large that $\theta\alpha^2$ is of order one. Physically this corresponds to an almost perfectly reflecting beamsplitter. Eq. 25 then approximately becomes

$$\langle\gamma|_a\langle\beta|_b|\cos\theta\gamma + i\sin\theta\beta\rangle_a|\cos\theta\beta + i\sin\theta\gamma\rangle_b \approx \exp[2i\theta\gamma\beta] \tag{26}$$

Eq.26 shows that the only difference between the input and output states of the beamsplitter is a phase shift proportional to the amplitudes of the input qubits, that is:

$$U_{BS}|\gamma\rangle_a|\beta\rangle_b \approx \exp[2i\theta\gamma\beta]|\gamma\rangle_a|\beta\rangle_b \tag{27}$$

If conditions are such that Eq.27 is a good approximation and we further require that $\theta\alpha^2 = \pi/2$ then this transformation produces a controlled sign shift gate.[14] That is if either or both of the qubits are in the logical zero state ($\gamma = 0$ and/or $\beta = 0$) the transformation produces no effect on the state. However if both modes are initially in the logical one state (i.e $\gamma = \beta = \alpha$) then a sign change is produced. Such a gate is a non-trivial two qubit gate.

3.2. Hadamard Gate

For universal computation we require, in addition to the two qubit gate above, the ability to do arbitrary rotations that are diagonal in the computational basis, bit-flip operations, plus the Hadamard gate.[15] The Hadamard gate cannot be implemented unitarily with linear optics. However, we will show shortly that, provided the necessary quantum resource is possessed, it can be implemented using only linear optics and conditional measurements.

First let us consider some single qubit transformations that can be achieved with just linear optics. A *bit flip* gate flips the state of the system from a logical zero to a logical one, or vice versa and is equivalent to the pauli $\sigma_x \equiv X$ matrix, in the computational basis. The bit flip transformation operator, X, is equivalent to a displacement of $-\alpha$ followed by a π phase shift of the coherent amplitude: $X = U(\pi)D(-\alpha)$, where $U(\pi) = exp[i\pi a^\dagger a]$ is physically just a half-wavelength delay, whilst a displacement can be implemented by mixing a very strong coherent field with the qubit on a highly reflective beamsplitter.[7]

The *phase rotation* gate produces a rotation that is diagonal in the computational basis, $R_\phi(\mu|0\rangle_L + \nu|1\rangle_L) = \mu|0\rangle_L + e^{i\phi}\nu|1\rangle_L$. It can be implemented, to a good approximation, by imposing a small phase shift on the qubit. Using arguments similar to those leading to Eq.27 we find

$$\begin{aligned} U(\epsilon)|\alpha\rangle &= e^{i\epsilon a^\dagger a}|\alpha\rangle \\ &\approx e^{i\epsilon\alpha^2}|\alpha\rangle = R_\phi|\alpha\rangle \end{aligned} \tag{28}$$

with $\phi = \epsilon\alpha^2$ and as before we require $\epsilon^2\alpha^2 << 1$.

In addition to these gates, we require a Hadamard gate in order to achieve an arbitrary qubit rotation. The Hadamard gate, $\mathcal{H}$, induces the following transformations on the logical states: $\mathcal{H}|0\rangle_L = 1/\sqrt{2}(|0\rangle_L + |1\rangle_L) = 1/\sqrt{2}(|0\rangle + |\alpha\rangle)$ and $\mathcal{H}|1\rangle_L = 1/\sqrt{2}(|0\rangle_L - |1\rangle_L) = 1/\sqrt{2}(|0\rangle - |\alpha\rangle)$. The outputs are a superposition of two widely separated coherent states, commonly known as "cat" states. Such states are highly non classical and for unitary generation require a Kerr nonlinearity for which the Hamiltonian is proportional to $(a^\dagger a)^2$. Such interactions are typically very weak and do not have sufficient strength to produce the required superposition states. However we are not restricted to unitary transformations. A number of schemes have been suggested which can produce parity cat states[16] (of the form $|\beta\rangle \pm |-\beta\rangle$) non-unitarily and some experimental progress has been made in their production.[17] Perhaps more relevant in the short term to this discussion are non-deterministic proposals for optical cat state production.[18] The simpler of these schemes comprises a squeezed source split at a beamsplitter.

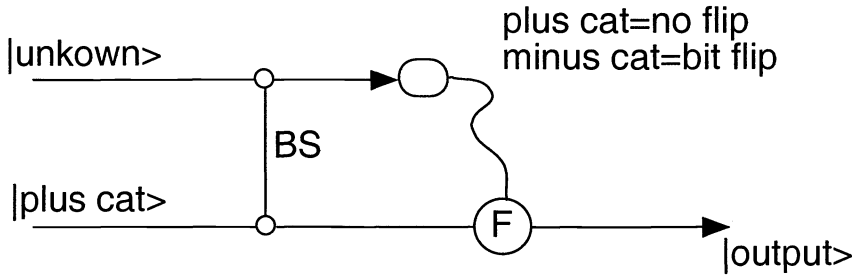

Figure 4. Schematic of Hadamard gate based on the two qubit beamsplitter gate (BS) and conditional implementation of the bit flip gate (F). If a plus cat is found then the output is in the desired state. If a minus cat is found a bit flip operation is needed to place the output in the correct state. The bit flip operation can be implemented by weakly mixing the beam with a powerful local oscillator on a beamsplitter and then introducing a π delay.

Photon counting on one output projects the other output into a coherent superposition state. For a sufficiently large photon count a parity cat is produced. A displacement operation could then be used to convert to the required state. In all these schemes it is necessary to distinguish between a photon (or phonon) number of n and $n \pm 1$. If cat states could be used as a resource to deterministically implement the Hadamard gate then these types of schemes would be sufficient for our purposes. We will now show this is true.

A Hadamard gate can be implemented using the two qubit BS gate discussed earlier with one of the inputs being the arbitrary state we wish to transform and the second input being a known cat state. One of the outputs of the gate is measured in the "cat basis" (see below) and, depending on the result, a bit flip operation may be required. This is a specific example of quantum gate implementation via measurement. A general discussion of such techniques can be found in Reference.[15]

A possible arrangement is shown in Fig.4. Suppose the state we wish to transform, in the arbitrary state $\mu|0\rangle + \nu|\alpha\rangle$, is inserted into port 1 of the BS gate whilst a resource cat state $1/\sqrt{2}(|0\rangle + |\alpha\rangle)$ is inserted into port 2. The output state of the gate is

$$\frac{\mu}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |0\rangle_1|\alpha\rangle_2) + \frac{\nu}{\sqrt{2}}(|\alpha\rangle_1|0\rangle_2 - |\alpha\rangle_1|\alpha\rangle_2) \tag{29}$$

Now suppose we make a measurement on output port 1 which returns a dichotomic result telling us whether we have the same cat state as we inserted or the (near) orthogonal state $1/\sqrt{2}(|0\rangle - |\alpha\rangle)$. If the result is the same cat state then the state of output port 2 is projected into

$$\frac{1}{2}(\mu + \nu)|0\rangle + \frac{1}{2}(\mu - \nu)|\alpha\rangle \tag{30}$$

This is the required Hadamard transformation. On the other hand if the opposite cat is measured at the output as was inserted, then the projected output state is a bit flipped version of Eq.30. Thus the final step of the gate is to implement (if necessary) a bit flip on the output port.

A cat basis measurement can be implemented in the following way. First we displace by $-\alpha/2$. This transforms our "0", "α" superposition into "$\alpha/2$", "$-\alpha/2$" superposition:

$$D(-\alpha/2)1/\sqrt{2}(|0\rangle \pm |\alpha\rangle) = 1/\sqrt{2}(|-\alpha/2\rangle \pm |\alpha/2\rangle) \tag{31}$$

These new states are parity eigenstates. Thus if photon number is measured then an even result indicates detection of the state $1/\sqrt{2}(|\alpha/2\rangle + |-\alpha/2\rangle)$ and therefore $1/\sqrt{2}(|0\rangle + |\alpha\rangle)$ whilst similarly an odd result indicates detection of $1/\sqrt{2}(|0\rangle - |\alpha\rangle)$ as can be confirmed by direct calculation.[19]

Cat states can also be distinguished by homodyne detection looking at the imaginary quadrature. Cat states display fringes in the imaginary quadrature which are $\pi/2$ out of phase between the plus and minus

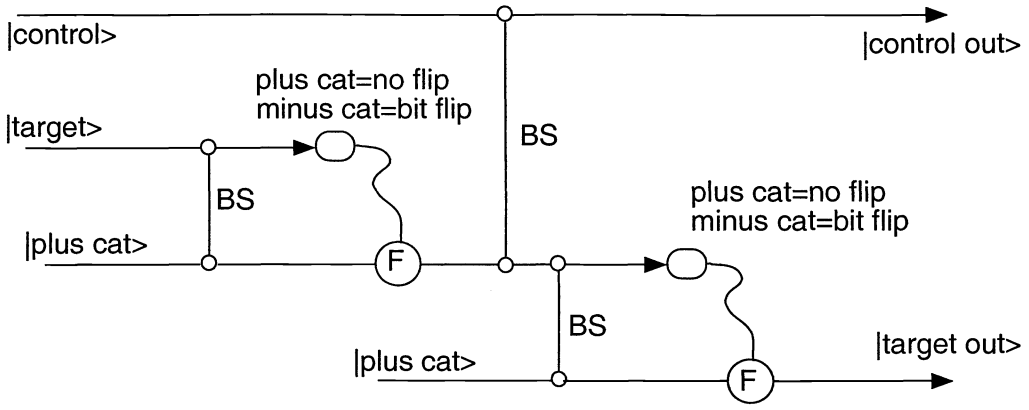

Figure 5. Schematic of CNOT gate based on two qubit beamsplitter gates (BS) and conditional implementation of bit flip gates (F).

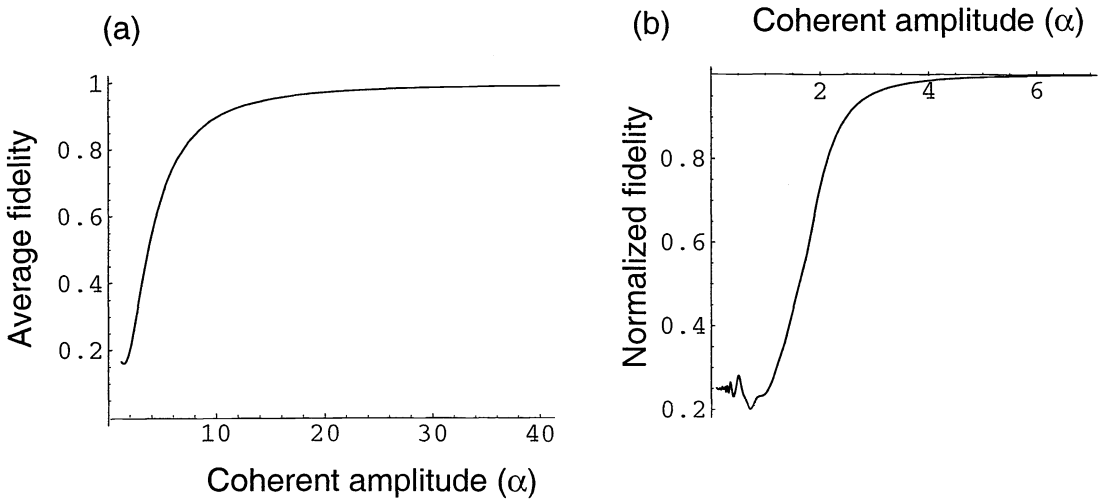

Figure 6. Performance of the CNOT gate as a function of the magnitude of α. The average fidelity is plotted against α in (a). In (b) the fidelity is renormalized against the success probability of the cat-basis measurements.

cats.[20] Therefore a measurement result that falls close to a fringe maximum can be identified with one or other cat with high probability. This technique gives inconclusive results some of the time (i.e. close to the fringe crossings) but could prove useful for initial experimental demonstrations.

3.3. CNOT Gate

The control not gate (CNOT) is ubiquitous in quantum processing tasks. It is also the simplest two-qubit gate whose operation can easily be experimentally verified in the computational basis. A CNOT gate will flip the state of one of the input qubits, the "target", only if the other qubit, the "control", is in the logical one state. If the control is in the logical zero state the target is unchanged. A CNOT gate can be implemented as shown in Fig.5 by first applying a Hadamard gate to the target state followed by the BS gate applied to the control and target. Finally another Hadamard gate is applied to the target. For arbitrary control and target input qubits we find:

$$\mathcal{H}_t U_{BS} \mathcal{H}_t (\mu|0\rangle + \nu|\alpha\rangle)_c (\gamma|0\rangle + \tau|\alpha\rangle)_t = \mu\gamma|0\rangle|0\rangle + \mu\tau|0\rangle|\alpha\rangle + \nu\tau|\alpha\rangle|0\rangle + \nu\gamma|\alpha\rangle|\alpha\rangle \quad (32)$$

which displays CNOT logic. The result of Eq.32 assumes $\alpha >> 1$. To evaluate just how large α needs to be we use the exact expression for the BS gate, as given in Eq.24, to calculate the output state of the CNOT. We assume ideal bit flip operations, cat state preparation and projective measurements. Our figure of merit is the average fidelity between the exact output and the ideal output, as given by Eq.32.

The results are shown in Fig.6(a) where the average fidelity is plotted as a function of α. We see that the fidelities do indeed asymptote to one for large α, though rather slowly with fidelities greater than 0.95 requiring $\alpha \geq 20$. To produce, control and measure cat states of such sizes would be extremely difficult. However much of the reduction in fidelity at low α's is simply due to one, or both of the cat basis measurements not returning a result and hence the gate failing. This means that the gate can still operate non-deterministically at low α's. Fig.6(b) shows the CNOT fidelities renormalized against the probability that the cat basis measurements actually give a result. Now we find that fidelities greater than 0.95 only require $\alpha \geq 3$, a far more realistic testing ground. This result is not restricted to projective measurements but works equally well for parity measurements by only accepting certain photon counts as valid.

4. CONCLUSION

We have reviewed the operation of quantum gates in two linear optical scenarios, one the dual rail photonic scheme of KLM and the second a single rail coherent scheme. In the photonic scheme we have shown how to construct and test 2 qubit gates with current technology. In the coherent scheme we have demonstrated a simpler scalable architecture which may have advantages over KLM in the medium to long term. We have concentrated on the simplest implementation of the coherent scheme which unfortunately requires uncomfortably large α. However with a modest increase in complexity the non-deterministic operation of the gates at low α can form the basis of a scalable system using the technique of gate operation via deterministic teleportation[3] (as opposed to the near deterministic technique in KLM).

ACKNOWLEDGMENTS

This work was supported by the Australian Research Council and ARDA.

REFERENCES

1. G. J. Milburn, Phys.Rev.Lett. **62**, 2124 (1988).
2. E. Knill, R. Laflamme and G. Milburn, Nature **409**, 46, (2001).
3. D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).
4. T. B. Pittman, B. C. Jacobs and J. D.Franson, Phys.Rev.Lett. **88**, 257902 (2002).
5. T. C. Ralph, A. G. White, W. J. Munro and G. J. Milburn, Phys.Rev.A **65**, 012314 (2002).
6. T. C. Ralph, W. J. Munro and G. J. Milburn, quant-ph/0110115.
7. A. Furasawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble and E. S. Polzik, Science **282**, 706 (1998)
8. S. Lloyd, S. L. Braunstein, Phys.Rev.Lett. **82**, 1784 (1999).
9. S. D. Bartlett, Hubert de Guise, B. C. Sanders , quant-ph/0109066 (2001).
10. H. Jeong and M. S. Kim, quant-ph/0109077 (2001).
11. D. Gottesman, A. Kitaev, J. Preskill, Phys.Rev.A **64**, 012310 (2001).
12. D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 1994).
13. "Taking α real" means that the field is in phase with the local oscillator which is used to make the displacements required for some of the gates. The intensity of a logical one pulse is $I = \hbar\omega|\alpha|^2$ per bandwidth with ω the optical frequency.
14. Note that Eq.25 only considers on-diagonal terms. Given $\alpha >> 1$ and $\theta^2\alpha^2 << 1$, the off-diagonal terms are approximately zero as required.
15. M. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, UK 2000).
16. B. Yurke and D. Stoler, Phys.Rev.Lett. **57**, 13 (1986).

17. C. Monroe, *et al* , Science **272**, 1131 (1996), M. Brune *et al*, Phys.Rev.Lett. **77**, 4887 (1996); J. F. Roch *et al*, Phys.Rev.Lett. **78**, 634 (1997), Q. A. Turchette *et al*, Phys.Rev.Lett. **75**, 4710 (1995).
18. S. Song, C. M. Caves and B. Yurke, Phys.Rev.A **41**, 5261 (1990), M. Dakna *et al*, Phys.Rev.A **55**, 3184 (1997).
19. A slight complication in implementing the photon counting determination of the cat-state is that the required displacement results in a phase rotation. As a result the Hadamard actually implements $\frac{1}{2}(\mu + \nu)|0\rangle + \exp[i\pi/4]\frac{1}{2}(\mu - \nu)|\alpha\rangle$. This is easily corrected with a phase rotation to the output.
20. L. Krippner, W. J. Munro, and M. D. Reid, Phys.Rev.A **50**, 4330 (1994).