On photonic controlled phase gates

To cite this article: K Kieling et al 2010 New J. Phys. 12 013003

View the article online for updates and enhancements.

Related content
- Optical generation of matter qubit graph states
  S C Benjamin, J Eisert and T M Stace
- Quantum optical systems
  T C Ralph
- Photons as qubits
  G J Milburn

Recent citations
- Experimental Implementation of Optimal Linear-Optical Controlled-Unitary Gates
  Karel Lemr et al
- Scheme for a linear-optical controlled-phase gate with programmable phase shift
  Karel Lemr et al
- Resource-efficient generation of linear cluster states by linear optics with postselection
  D B Uskov et al
On photonic controlled phase gates

K Kieling\textsuperscript{1,4}, J L O'Brien\textsuperscript{2} and J Eisert\textsuperscript{1,3}

\textsuperscript{1} Institute of Physics and Astronomy, University of Potsdam, 14476 Potsdam, Germany
\textsuperscript{2} Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, UK
\textsuperscript{3} Institute for Advanced Study Berlin, 14193 Berlin, Germany
E-mail: kieling@qipc.org

\textit{New Journal of Physics} 12 (2010) 013003 (16pp)
Received 11 October 2009
Published 11 January 2010
Online at http://www.njp.org/
doi:10.1088/1367-2630/12/1/013003

Abstract. As primitives for entanglement generation, controlled phase gates have a central role in quantum computing. Especially in ideas realizing instances of quantum computation in linear optical gate arrays, a closer look can be rewarding. In such architectures, all effective nonlinearities are induced by measurements. Hence the probability of success is a crucial parameter of such quantum gates. In this paper, we discuss this question for controlled phase gates that implement an arbitrary phase with one and two control qubits. Within the class of post-selected gates in dual-rail encoding with vacuum ancillas, we identify the optimal success probabilities. We construct networks that allow for implementation using current experimental capabilities in detail. The methods employed here appear specifically useful with the advent of integrated linear optical circuits, providing stable interferometers on monolithic structures.

\textsuperscript{4} Author to whom any correspondence should be addressed.
1. Introduction

Linear optical architectures offer the potential for reliable realizations of small-scale quantum computing [1]. In the recent past, numerous proof-of-principle demonstrations have relied on the precise state manipulation that is available using linear optical elements. The development of better and brighter sources with good mode quality, as well as new types of detector, has opened up new perspectives [2] in state preparation and manipulation for six or more photons. Specifically, integrated optical circuits allow for state manipulation with few mode matching problems in interferometers [3].

Naturally, significant efforts have been made to realize instances of quantum gates. As primitives for such small-scale computing, two-partite quantum gates delivering a controlled phase shift of $\varphi$ have already been experimentally demonstrated (see [4]–[6] for $\varphi = \pi$ and [7] for general phases). In this paper, we focus on linear optical implementations of phase gates with arbitrary phases. In particular, we ask when arbitrary phases can be realized in the first place, and—one of the main figures of merit in linear optical applications—what the optimum probabilities of success are, as any nonlinear map is necessarily probabilistic. A realization of such gates seems interesting from the perspective of

(i) gaining an understanding of the probabilistic character of quantum gates as well as
(ii) serving as a proof-of-principle realization of a kind of quantum gate that has several applications in linear optical quantum information processing.

As far as the first aspect is concerned, one may well expect that there is a trade-off between the notorious problem of having a small probability of success and the phase that is being realized in the gate. In fact, the study in [8] suggests exactly such a behavior; the presented upper bounds to the probability of success increase from the minimum at $p_s(\varphi = \pi) = 1/4$ to $p_s(0) = 1$. To investigate such a trade-off is interesting in its own right and helps to further
understanding of the probabilistic behavior of linear optics. One may well develop the view that ‘large phases are costly’ as far as the probability of success and hence the overhead or repetition is concerned.

Further, concerning the second aspect, there are several applications for which such a trade-off is relevant. In linear optical architectures, it may be a good idea to have a smaller phase if one only has higher success probabilities. The new measurement-based quantum computational models [9] for example offer this perspective; one need not have controlled $\pi$ phase gates to prepare cluster states, but one would in principle also be able to work with smaller phases. This may well (but does not have to) be a significant advantage when preparing resources for measurement-based quantum computing other than cluster states [9, 10].

Of course, in standard gate-based quantum computing, one will typically encounter all kinds of controlled phase gates. For example, in the quantum Fourier transform [11], one has to implement several controlled phase gates. They can again be decomposed into other sets of universal gates (like CNOT or CZ and local unitaries). But, in terms of resource requirements, it is obviously an advantage to directly implement the relevant quantum gates with phases in the range $0 < \phi < \pi$. There are also interesting trade-offs between resource requirements and success probabilities in a number of related contexts, like non-local gates in distributed quantum computation [12, 13]. Cirac et al and Berry, for example, study distributed controlled phase gates requiring less entanglement and succeeding with a higher probability [13]. In the field of linear optics gates, numerical results on direct implementation of arbitrary two-qubit gates are known (see [14] and references therein).

Instead of resorting to decompositions in the circuit model, one could gain by implementing unitaries in a fashion ‘natural’ to the respective architecture at hand. In the case of linear optics, it means leaving the computational sub-space given by the encoding of the qubits for the sake of taking a ‘shortcut’ through higher dimensions [7]. Given that the fundamental information carriers are implemented using bosonic modes, this will occur when mixing those modes in beam splitter networks, and is an inherent feature of genuine linear optics implementations, in contrast to decomposition into standard gate sets.

Here we study post-selected gates, which are not genuine ‘event-ready’ quantum gates, but—as is common in linear optical architectures, at least to date—those where one measures the output modes, and whether the gate actually succeeded is determined only a posteriori by accepting only those outcomes that lie in the computational dual-rail sub-space of the Hilbert space of $n$ photons on $2n$ modes. Incorporating fewer constraints, these gates concern only a relatively small number of modes and are still within the scope of current experimental capabilities. In principle, non-demolition measurements of the output would be required for an event-ready gate.

2. Controlled phase gates

2.1. Single beam splitter

In a post-selected phase gate on four modes in the standard dual-rail encoding, two of the modes are merely involved as ‘bystanders’, in that their amplitude is compensated for in exactly the same fashion as in [4]–[6]. In this section, we will therefore concentrate on two modes forming the ‘core’ of the scheme, giving rise to a two-qubit dual-rail phase gate on four physical modes. The core itself may be regarded as a single-rail phase gate in its own right. Later we will see that not breaking the network into core and bystander modes does not give any advantage.
Similarly to [4], we will briefly investigate the consequences of simply having a single beam splitter forming the core of the quantum gate. The action on the photonic creation operators of the two involved modes being mixed is described by the matrix

\[ U = \text{diag}(e^{i\phi_1}, e^{-i\phi_1}) \cdot B \cdot \text{diag}(e^{i\phi_2}, e^{-i\phi_2}) \]

with

\[ B = \begin{bmatrix} \sin(\vartheta) & \cos(\vartheta) \\ -\cos(\vartheta) & \sin(\vartheta) \end{bmatrix} \]

and appropriate phases \( \phi_1, \phi_2 \in [0, 2\pi) \) and mixing angle \( \vartheta \in [0, 2\pi) \). The phases can also be realized deterministically by local operations on the dual-rail qubits, which leaves the relevant part of the gate \( U' = B \). The matrix elements of the unitary \( U' \) belonging to \( U' \) for vacuum, single-photon operation and the two-photon component read

\[ \langle 0, 0 | U' | 0, 0 \rangle = 1, \]

\[ \langle 1, 0 | U' | 1, 0 \rangle = A_{1,1} = \sin(\vartheta), \]

\[ \langle 0, 1 | U' | 0, 1 \rangle = A_{2,2} = \sin(\vartheta), \]

\[ \langle 1, 1 | U' | 1, 1 \rangle = \text{per}(A) = \cos(2\vartheta) = 1 - 2\sin^2(\vartheta), \]

respectively. Since we are restricted to \( n \leq 2 \) modes, these four quantities determine the action of the core completely. With the constraint

\[ 1 - 2\sin^2(\vartheta) = \sin^2(\vartheta) \]

that ensures equal single- and two-photon amplitudes (equal probabilities for all dual-rail states), only the two solutions \( \vartheta = \pm \arcsin(3^{-1/2}) \) are possible, giving rise to \( \varphi = 0, \pi \), respectively.

Hence, one finds that in this way, one can implement quantum phase gates, but only two different ones; one is not doing anything, and the other one’s effect is a controlled phase of \( \pi \). This is precisely the gate of [4, 5]. In other words, without invoking at least a single additional mode, one cannot go beyond the known \( \pi \)-phase in this fashion.

### 2.2. Arbitrary phases

However, we can extend this scheme; the restriction to unitary two-mode beam splitters can be relaxed. Instead of starting with \( U \in SU(2) \), we use an arbitrary matrix \( A \in \mathbb{C}^{2 \times 2} \). Then we will embed the two-mode matrix into a higher dimensional unitary, so that an appropriately rescaled \( A \) forms a principle submatrix of a larger unitary matrix \( A' \). The optimal rescaling is simply dictated by the largest singular value of \( A \); any matrix the largest singular value of which is smaller than unity can be a principal submatrix of a unitary, as can easily be seen. An extension that has such a unit maximum singular value we will call optimal. Physically, such an embedding corresponds to adding vacuum modes to the input. We will see that in the two-mode case a single additional mode is already the most general extension, so the full set-up would consist of a transformation on three modes involving at most three beam splitters. In this class of gates, for each \( \varphi \) the one with the optimal probability of success \( p_s(\varphi) \) can be identified.
**Figure 1.** Optimal success probability $p_s(\varphi)$ of phase gates with vacuum ancillas (one vacuum ancilla is already optimal) versus the phase $\varphi$ (solid line). At $\varphi = \pi$ the result of [4, 5], $p_s(\pi) = 1/9$, is reproduced. The intuitive assumption of a monotonic $p_s(\varphi)$ is not fulfilled; indeed, the success probability is worse than $1/9$ in the interval $\pi/3 < \varphi < \pi$. Due to phases $\varphi < \pi$ not being implementable with a single beam splitter, the additional unitary extension requires further measurements and therefore decreases the probability of success near $\varphi = \pi$.

**Observation 1** (Optimal post-selected dual-rail controlled phase gate). Consider linear optics, an arbitrary number of auxiliary vacuum modes and photon number resolving detectors. When post-selecting the state of the signal modes on to the computational sub-space and the auxiliary modes onto the vacuum, the optimal network on four modes implementing the gate represented in the computational basis of two dual-rail qubits by $U = \text{diag}(1, 1, 1, e^{i\varphi})$, $\varphi \in [0, \pi]$, has a success probability (shown in figure 1) of

$$p_s(\varphi) = \left(1 + 2\left|\sin \frac{\varphi}{2}\right| + 2\sin \frac{\pi - \varphi}{4}\sqrt{\left|\sin \frac{\varphi}{2}\right|}\right)^{-2}. \quad (8)$$

**Proof.** In order to find $p_s$—the same for all possible input states—we first construct the linear transformation of the relevant creation operators and then identify the optimal unitary extension.

- **Two-mode transformation:** The two-mode transformation resulting from solving equations (3)–(6) imposed by the gate we want to build is

$$A = p_s^{1/4} \begin{bmatrix} x & (e^{i\varphi} - 1) y/x \\ y/x & 1/x \end{bmatrix}. \quad (9)$$

$x$ and $y$ are free nonzero complex parameters. By writing

$$A = p_s^{1/4} \text{diag}(a, a^{-1}) \begin{bmatrix} 1 & e^{i\varphi} - 1 \\ 1 & 1 \end{bmatrix} \cdot \text{diag}(b, b^{-1}), \quad (10)$$

with $a = xy^{-1/2}$ and $b = y^{1/2}$ we see that the singular values of $A$ only depend on $|a|^2$ and $|b|^2$, so not on the phases of $a$, $b$, and $x$ and $y$. 

*New Journal of Physics* 12 (2010) 013003 (http://www.njp.org/)
The general solution to the dual-rail problem is actually composed of the transformation $A$, together with appropriate damping of the bystanders; the probability of success cannot be enhanced by considering a full transformation on all four modes. This can be seen by writing the polynomial system given by the dual-rail problem similar to (3)–(6), consisting of 16 quadratic equations in the matrix elements of $B \in \mathbb{C}^{4 \times 4}$. It emerges that by permuting modes and appropriate variable substitutions all solutions can be brought into the form $B \propto \mathbb{1}_2 \otimes A$, consisting of the two-mode core given in equation (9) and two bypassed modes.

- **Optimal extension:** Given the $2 \times 2$ matrix $A$ that realizes the transformation we are seeking, the optimal unitary extensions can be identified. Let us extend the first and second row vectors (denoted by $A_1$ and $A_2$) to dimension 3 by appending $A_{1,3}$ and $A_{2,3}$, respectively, in such a way as to allow for unitarity of the extended matrix, $A' \in \text{SU}(3)$. To see why a dimension of three is already sufficient, consider a linear transformation of the creation operators of $n$ modes, described by its (not necessarily unitary) matrix $A$. By using the singular value decomposition (SVD) it can be decomposed as $A = V D W^{-1}$, where $V$ and $W$ are unitary (and therefore have immediate interpretations as physical beam splitter matrices themselves), and $D = \text{diag}(d_1, \ldots, d_n)$ is a diagonal matrix with real non-negative entries $d_1 \geq d_2 \geq \cdots \geq d_n$, the singular values. In terms of linear optics $D$ can be interpreted as mixing each mode $k = 1, \ldots, n$ with an additional mode $n + k$ in the vacuum state which will be post-selected in the vacuum afterward [15, 16]. Then, $d_k$ describes the transmittivity of the beam splitter used to couple modes $k$ and $n_k$. Without loss of generality one can assume $d_1 = 1$, vacuum mixing for the first mode. This can be achieved by rescaling with the inverse of the largest singular value, so $A \mapsto d_1^{-1} A$, which implies $d_1 \mapsto d_1^{-1} d_k$. Note that such a ‘global’ rescaling of $A$ does not change the post-selected action on the computational sub-space, but only the success probability of it according to $p_s \mapsto d_1^{-2s} p_s$. Therefore, in general, there are $n - 1$ additional vacuum modes required to extend an $n$-mode linear transformation to a unitary, and thus physical, network. Also please note that the constraint $d_1 = 1$ has to be taken into account for any optimization of success probabilities of $A$. Here we will not explicitly use this decomposition further, but the constraint will be implemented implicitly by requiring the $n - 1$-mode extension to be unitary.

In our specific three-mode extension we choose $A_{1,3}$ and $A_{2,3}$ so that the new row vectors are orthogonal. By multiplying them by the root of the inverse of their respective norms, $|A_1'|$ and $|A_2'|$, they will be normalized. Finding a third orthogonal vector to fill the unitary matrix can be achieved with the complex cross product $(A_1' \times A_2')^*$, or in general by choosing a vector at random and orthogonalizing it with respect to the given ones.

The dependence of the success probability on the extension is

$$p_s = (|A_1'||A_2'|)^2.$$  \hspace{1cm} (11)

Therefore, the objective is to

minimize $f = |A_1'|^2 |A_2'|^2$ \hspace{1cm} (12)

subject to $A_1'(A_2')^\dagger = A_1 A_2^\dagger + A_{1,3} A_{2,3}^* = 0$. \hspace{1cm} (13)

The first observation is that the row scaling by $x$ is already included in the norm of the row vectors, leaving us with one less parameter. By using the phase of $y$, we can
assure that $A_1A_2^*$ is real and positive and also $\arg(A_{1,3}) - \arg(A_{2,3}) = \pm \pi$. This constrained minimization problem in $A_{1,2}$ and $A_{1,3}$ can indeed be solved (by using Lagrange’s multiplier rule and showing constraint qualification) and we find $|y| = (2(1 - \cos \varphi))^{1/4}$. Then an optimal solution (phases chosen conveniently) is

$$A_{1,3} = A_{2,3}^* = e^{i \varphi/2} \left( \sqrt{2} \left| \sin \frac{\varphi}{2} \right| \sin \frac{\pi - \varphi}{4} \right)^{1/2}$$

with the probability of success given by

$$p_s(\varphi) = \left( 1 + |y|^2 + |y| \sqrt{2 - |y|^2} \right)^{-2} = \left( 1 + 2 \left| \sin \frac{\varphi}{2} \right| + 2 \sin \frac{\pi - \varphi}{4} \sqrt{\left| \sin \frac{\varphi}{2} \right|} \right)^{-2}.$$  \hspace{1cm} (14)

The reflectivities of the compensating beam splitters in the bypassed modes have to be chosen so that the success probability is constant for all dual-rail states, i.e.

$$r = p_s^{1/4}. \hspace{1cm} (16)$$

The success probability $p_s(\varphi)$ of this gate is shown in figure 1. Interestingly—and quite surprisingly—the worst success probability is not achieved for the sign flip ($\varphi = \pi$), but for $\varphi \approx 2.05$. This means that gates delivering a phase shift slightly smaller than $\pi$, and therefore generating less entanglement, will not give rise to a larger, but to a smaller, success probability. As expected, the success probability for very small phases increases and reaches unity for $\varphi = 0$; one can do nothing at all with unit success probability.

2.3. Integrated quantum photonics realizations

Sophisticated circuits such as the one shown in figure 5 can be built from bulk optical elements (mirrors, beam splitters, etc). Such circuits often require implementation of Sagnac interferometers (e.g. [18]), partially polarizing beam splitters (PPBSs) [6], or beam displacers [19, 30] to achieve interferometric stability. For the most complicated circuits a combination of these elements is required. Indeed a (non-optimal) implementation of a two-qubit controlled unitary gate used a combination of beam displacers and PPBSs [7]. However, such circuits are extremely challenging to align, are limited in performance by the quality of alignment, and are ultimately not scalable.

An alternative approach based on lithographically fabricated integrated waveguides on a chip has recently been developed [3]. This approach has demonstrated better performance in terms of alignment and stability, as well as miniaturization and scalability. The monolithic nature of these devices enables interferometers to be fabricated with precise phase and stability, making the Mach–Zehnder interferometer shown in figure 2 directly implementable without the need to stabilize the optical phase (either actively, or using the Sagnac-type architecture of figure 5), greatly simplifying the task of making complicated circuits; essentially the circuit one draws on the blackboard can be directly ‘written’ into the circuit. Indeed, integrated photonics circuits have been used to implement a circuit of several logic gates on four photons, to implement a compiled version of Shor’s quantum factoring algorithm in this way [20]. In fact,
Figure 2. Basic spatial-modes-based set-up obtained by translating an arbitrary $2 \times 2$ core into the language of linear optics. The core extension is provided by mixing with a vacuum mode on the central beam splitter. This mode, in turn, has to be post-selected in the vacuum state afterward. The upper and lower beam splitters implement the appropriate compensation by damping the bypassed modes (this is the same for both modes for the optimal solution we consider). The labels at the beam splitters will be used to identify them with the respective optical elements in figures 3–5. In general, the parameters (i.e. reflectivity and phases) of these elements depend on the gate’s phase $\phi$. Further, the notation $|0\rangle_i$ and $|1\rangle_i$ is used for the logical 0/1-modes of the $i$th qubit to avoid confusion with Fock states.

laser direct write techniques have been used to ‘write’ circuits in an even more direct fashion than the lithographic approach.

Another key advantage of integrated quantum photonics for the circuits described here is that on-chip phase control can be directly integrated with the circuit [21], which could allow measurement of the success probability curve (figure 1 or figure 6, for example) to be directly mapped by sweeping the applied voltage.

2.4. Experimental issues in free space

In order to render the proposed gates experimentally more feasible in free space, some simplifications have to be made, tailored to the specific physical implementation at hand. Waveguide-based setups would not need further simplification because stability of the interferometers would be ensured by the rigid substrate. Implementations more suitable for beam-displacer-based set-ups are known [7]. Influenced by the gate model, those gates include a controlled $\pi$-phase gate at the core. Operating at lower success probabilities, especially at phases $\phi$ approaching 0, the probability of success does not converge to 1.

In the following, we will discuss simplifications which will allow for easier free-space implementation of the networks introduced above, while still preserving optimality with respect to $p_s$. A straightforward set-up on dual-rail encoding that realizes a three-mode unitary and compensates for the amplitudes in the remaining modes is shown in figure 2. It includes one interferometer, but the whole gate would sit inside a double interferometer, because local unitaries on the input and output qubits would require classical interference. Thus, the complexity of this gate is best described as a nested three-fold interferometer. In this first stage, the parameters (reflectivities and phases) of all five beam splitters depend on $\phi$. 

New Journal of Physics 12 (2010) 013003 (http://www.njp.org/)
Figure 3. Set-up for a controlled phase gate on two polarization encoded dual-rail qubits. The logical modes of the two qubits are separated and re-united by means of polarizing beam splitters (PBS). Replacing the left and right beam splitters in figure 2 by wave plates $\lambda_1$ and $\lambda_2$, they become easier to tune to different $\varphi$, and provide better stability. The lower beam splitter, $\gamma$, implements compensation for both, $|0\rangle_1$ and $|0\rangle_2$, modes. $\lambda_V$ is taken care of by the PPBS (allowing for different reflectivities for the two polarizations, further explained in figure 4) in the center. Additionally, one of the qubits has to be flipped prior to and after the circuit, which is done here by acting with a wave plate on the second qubit.

To get rid of some of the interferometers, polarization encoding is convenient. Two modes can be united in one spatial mode, resulting in inherent stability (neglecting birefringence of the optical medium) of some interferometers. Rotations on these modes can be carried out easily using wave plates. Because the core acts on modes coming from different dual-rail qubits, these have to be combined into a single spatial mode beforehand. This is achieved with a polarizing beam splitter (PBS), thus permuting $H$ and $V$ modes. Damping of both bypassed modes can be done simultaneously by a single polarization insensitive beam splitter coupled to the vacuum. A straightforward translation of figure 2 into polarization encoding, thereby collapsing the network into a single interferometer, is shown in figure 3.

Due to the asymmetry of the core, a single PPBS is still used, the reflectivity of one polarization component of which actually depends on $\varphi$, the other one being 1. Figure 4 shows how a tunable PPBS can be constructed, introducing another interferometer.

Iterating the ideas that led to the compact PPBS implementation once more yields a collapsed form of the phase gate based on only two PBSs and a couple of wave plates. Due to the paths of light being very similar, this set-up should also be more robust.

2.5. Simple decomposition

In this subsection we aim at obtaining a simple decomposition and explicit $\varphi$-dependence of the involved elements of the full $3 \times 3$ unitary transformation $U \in \text{SU}(3)$. To do so, we interpret the effective core, acting on the $|1\rangle_1$ and $|1\rangle_2$ modes in figure 2, in a different way; in between $U_{\lambda_1}$ (the unitary beam splitter matrix of $\lambda_1$) and $U_{\lambda_2}$, there acts a diagonal mode transformation so that the first mode is unaffected and the amplitude of the second one is damped (due to $U_{\lambda_V}$ coupling it with reflectivity $r_V$ to a vacuum mode which will be projected onto the vacuum).

Now, considering the SVD of the matrix representing the core transformation, $A = V \Sigma W^\dagger$ we can identify $V = U_{\lambda_2}$, $W^\dagger = U_{\lambda_1}$ and $\Sigma = \text{diag}[1, r_V]$. As we have seen earlier, optimal
Figure 4. From left to right. (i) A PPBS implementing a beam splitter with polarization-dependent reflectivity. (ii) It is equivalent to an interferometer between two PBSs where the PPBS’s reflectivities are incorporated by means of wave plates, $\lambda_1$ and $\lambda_2$. (iii) By identifying the two PBSs, the interferometer collapses into a closed loop (which is more compact and more robust in experimental implementations), leaving only one PBS. In the second and third circuit, a polarization flip of the second qubit before and after the circuit is added using a wave plate.

Figure 5. Compact implementation of a controlled phase gate by using a single loop to implement the central PPBS and the compensation beam splitters simultaneously. Additionally, the two PBSs are identified, resulting in a second loop. All omitted modes are initialized in the vacuum and post-selected in the vacuum state (which will be achieved in practice by counting the photons in the other output).

extensions of $2 \times 2$ cores only require global rescaling, which commutes with the unitaries involved. Therefore, we can use the much simpler original form of $A$ in equation (9), and we choose $x = 1$ and $y = -(e^\phi - 1)^{1/2}$. We find the singular values of $A$

$$\sigma_\pm = \left( 1 + 2 \sin \frac{\phi}{2} \pm 2(2 - 2 \cos \phi)^{1/4} \cos \frac{\phi + \pi}{4} \right)^{1/2}.$$  (17)
Global rescaling amounts to fixing the largest singular value to unity, so the new singular values are 1 and $r_V = \sigma_-/\sigma_+$. 

Due to $\det U_{\lambda_1} = \det U_{\lambda_2} = 1$ we need to attach a phase to one singular values as well in order to apply the identification of the matrices introduced above. Then the SVD of $A$ yields

$$U_{\lambda_1} = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix}$$

and $U_{\lambda_2} = U_{\lambda_1}^{-1}e^{\phi_+\sigma_z}$ with

$$\phi_{\pm} = \arccot \left[ \cot \frac{\varphi + \pi}{4} \pm \left( (2 - 2 \cos \varphi)^{1/4} \sin \frac{\varphi + \pi}{4} \right)^{-1} \right],$$

where the order of rows and columns in the matrices is as in figure 2 from top to bottom.

The ‘complex singular values’ are 1 (the first mode is not affected) and $\sigma_-/\sigma_+ \exp \phi_+ + \phi_-$. The latter can be achieved by using the aforementioned coupling to the vacuum with a reflectivity of $r_V$ and a phase upon reflection of $\phi_+ + \phi_-$. The further ingredient is the beam splitters required for the ‘damping’ of the bystanders as discussed earlier. By confirming $1/\sigma_+^4 = p_\varphi$ in the range $0 \leq \varphi \leq \pi$, the optimality of this construction is assured.

### 3. Event-ready gates

Coming from post-selected gates, the next step towards scalable quantum computation would be to build gates not requiring measurements on the output modes. Intuitively, it is clear that the construction of a controlled phase gate in this class will be more demanding with respect to the resources (such as the number of auxiliary modes and photons, size and complexity of the network) involved.

In particular the number of additional photons will change drastically; having had none in the post-selected case of a controlled $\pi$-phase gate, two are required in the class of event-ready gates. We will use this example as motivation for a detour to discuss a number of different methods that could be useful for handling linear optics state preparation.

To do so, we notice that a controlled $\pi$-phase gate is more constrained than a device that creates EPR pairs from single photons. This is meant in the sense that it not only amounts to a state transformation from two single photons to an EPR pair, but a full unitary transformation on the entire computational state space in dual-rail encoding (and creating an EPR pair when applied to a certain product input corresponding to the product state of two photons). The following two sections concern different methods of describing linear optics state preparation, and we apply them to the specific example at hand (i.e. heralded dual-rail EPR pair generations from single photons).

It is established that the construction of an EPR pair out of single photons by means of linear optics, vacuum modes, one additional photon and detectors is not possible. Of course, directly solving the polynomial equations in the matrix elements of $A$ (generalization of equations (3)–(6)) yields the same result—no solutions unless two additional photons are involved. Having excluded the cases of zero and one auxiliary photons, a set-up with two of them is possible, proven by the existence of such a scheme (EPR construction [22] as well as controlled-Z gate [1]).
3.1. State transformations

An obvious way of looking at states of exactly two photons in $m$ bosonic field modes is the following. Such a state vector can be written as

$$|\psi_M\rangle = P(a^\dagger)|\text{vac}\rangle$$

$$= \sum_{i,j=1}^m M_{i,j} a_i^\dagger a_j^\dagger |\text{vac}\rangle = (a^\dagger)^T M a^\dagger |\text{vac}\rangle,$$

where $M$ is a symmetric $m \times m$ matrix. The application of a unitary mode-transformation $U$—representing a linear optical network—is reflected by

$$|\psi_M\rangle \mapsto |\psi_{M'}\rangle = (U a^\dagger)^T M (U a^\dagger)|\text{vac}\rangle$$

$$= (a^\dagger)^T M' a^\dagger |\text{vac}\rangle$$

with $M' = U^TMU$ again being clearly symmetric. As a special case of the SVD [23], a diagonal $M'$ can be achieved, given an arbitrary input state vector $|\psi_M\rangle$.

Now let us choose $U$ so that $M'$ is diagonal. Then, labelled by

$$\nu' = \text{rank}(M'),$$

there are $m$ different classes of state [16, 17], in each of which the state is composed by superpositions of two photons in either of $\nu'$ modes. These classes are separated by linear optical mode transformations requiring additional modes. Decreasing the rank is possible by allowing for auxiliary vacuum modes. However, to increase the rank by 1, one additional photon is required. Furthermore, the state matrix $M$ of two single photons on four modes has rank $\nu = 2$, while an EPR pair corresponds to a matrix with rank $\nu = 4$. Therefore, the desired state transformation requires at least two additional single photons.

3.2. Polynomial factorization

An alternative approach is the following [16]: the polynomial describing the objective state vector $|\psi\rangle = P(a^\dagger)|\text{vac}\rangle$ with

$$P(a^\dagger) = 2^{-1/2} \left( a_1^\dagger a_3^\dagger + a_2^\dagger a_4^\dagger \right)$$

(24)

does not factorize over $\mathbb{C}$. Using Lemmata 1 and 2 from [24], the property of factorization of a bivariate polynomial

$$p(x, y) = \sum_{i,j=0}^m p_{i,j} x^i y^j$$

(25)

over $\mathbb{C}$ can be tested by assessing the rank of a complex $2m(2m-1) \times (m+1)(2m-1)$ matrix. Furthermore, applying Lemma 7 of [25], this technique can be extended to multivariate polynomials. Now, a state can be constructed from a product state using linear optical gate arrays iff the corresponding polynomial is factorizable. In the case mentioned before (dual-rail EPR pair, so four variables), one can use the resulting $12 \times 9$ matrix to confirm in the language of polynomials of creation operators that additional resources are in fact required.

The $m = 4$ case was used previously in [28, 29]. We thank D. Uskov for pointing out the nice structure of this.
4. Toffoli gates

In the same way as above, we can consider a generalized Toffoli gate, the effect of which on the computational basis realized as dual-rail encodings can be described by the unitary

$$U = \text{diag}(1, 1, 1, 1, 1, 1, e^{i\phi}).$$

The solutions to the polynomial equations describing the action on the three-mode core—up to mode permutations—can be parametrized by $x, y \in \mathbb{R}$ and are given by the matrix

$$A = p_s^{1/6} \begin{bmatrix} 1 & e^{ix} - 1 & 0 \\ \frac{xy}{e^{ix}} & 1 & y \\ x & 0 & 1 \end{bmatrix}.$$  \hspace{1cm} (27)

This has to be understood in a similar way to the two-mode core used by the controlled phase gate. However, here we do not solve the full optimization problem, but only consider global rescaling.

For a unitary extension all singular values of $A$ have to be at most 1. In order to avoid formulating cubic singular values explicitly, we use the following constraints. Let $p_{AA^\dagger}(\lambda) = \text{det}(AA^\dagger - \lambda I_3)$ be the characteristic polynomial of $AA^\dagger$, the roots $\lambda_{1,2,3}$ of which are the squared singular values of $A$. By requiring $p_{AA^\dagger}(1) = 0$, one of the singular values has to be 1. If the roots of $p_{AA^\dagger}$ are real valued and non-negative, the condition that all other singular values are not larger than 1 is equivalent to the condition that all derivatives of $p_{AA^\dagger}$ have the same sign at $\lambda = 1$. More formally, this results in further constraints of the form

$$(-1)^{\alpha} p_{AA^\dagger}^{(k)}(1) = (-1)^{\alpha} \frac{d p_{AA^\dagger}(\lambda)}{d\lambda} \bigg|_{\lambda=1} \geq 0$$  \hspace{1cm} (28)

for $1 \leq k < n$ where $\alpha = 0, 1$ is fixed by the condition of $k = n$. For $\varphi = \pi$ the optimal $p_s$ compliant with these conditions is

$$p_s(\pi) = 1 + 3 \left(2^{1/3} - 2^{2/3}\right) \approx 1/57.$$  \hspace{1cm} (29)

See figure 6 for the maximum success probability in the range $0 \leq \varphi \leq \pi$. The corresponding networks could be constructed in the same way as above. However, they would consist of three-mode cores (an interferometer composed of three partially polarizing beam splitters) inside separate interferometers for each of the three qubits. For free space experiments more appealing approaches for the specific choice of $\varphi = \pi$ are presented in [26, 27], but these lead only to success probabilities of at most 1/72.

5. Remarks on process tomography

Process tomography amounts to characterizing (or sometimes certifying) an unknown physical process. In practice, the task is to identify a completely positive map that is closest to the data with respect to some meaningful figure of merit. To accomplish this task, one has to consider a tomographically complete set of inputs, and look at Hilbert–Schmidt scalar products of the output with observables, to faithfully reconstruct the matrix form of the channel [30, 31]. Practically, the closest physical process can then be found by solving a convex optimization problem. Formally equivalently, and in instances in an experimentally simpler fashion, one can, instead of sending in a full set of input states, submit half of a single fixed maximally entangled
Figure 6. Optimal success probabilities of generalized Toffoli gates. The features exhibited by $p_s(\phi)$ are similar to the ones observed at the controlled phase gate (figure 1); there is a shallow dip between $\phi = \pi/2$ and $\pi$ below $p_s(\pi) = p_s(\pi/2)$, and a steep incline (more pronounced than for the controlled phase gate) for small phases towards $p_s(0) = 1$.

state, and hence reconstruct the channel from the Choi matrix, then referred to as entanglement-assisted process tomography.

The latter technique can clearly also be applied in the case of a post-selected quantum gate such as a phase gate. Yet, even without entangled inputs and including the actual measurement, one can reconstruct the resulting POVM elements, to which essentially post-selected gates amount to when one also faithfully includes the actual measurement in the black-box description of the process. If one has a well-characterized source at hand, then the statistics of

$$p_{j,k} = \text{tr}[\rho_j A_k]$$

uniquely characterize the process, where $\{\rho_j\}$ form a tomographically complete well-characterized input set, and $A_1, \ldots, A_K \geq q$ constitute a POVM, i.e.

$$\sum_{k=1}^K A_k = 1$$

(for an experimental realization of such an approach, see [32]). In practice, one uses methods of convex optimization to identify the closest physical process to the given data.

For the purposes of the present work, one of the outcomes $k = 1$, that is, a specific pattern $A_1$ of detection, then gives rise to the actual post-selected linear optical quantum gate. In this way, one can reconstruct post-selected quantum gates, without using an ancilla-based approach, even faithfully including the final measurement as part of the process.

6. Conclusion

We have shown how to obtain the maximum probability of success of controlled phase- and Toffoli-like gates in the class of post-selected linear optics dual-rail gates without additional photons. Further, constructions of networks for the smaller gates suitable for experimental
implementation have been given, and techniques elaborated upon that allow for the assessment of the possibility of certain linear optical schemes. For further progress concerning the eventual full optimization of linear optical processes it would be interesting to investigate (i) optimal constructions with respect to a class of gates inherently incorporating such experimental constraints or (ii) identify further decomposition techniques from a given linear optics mode transformation into suitable physical networks, respecting these constraints.

Acknowledgments

For insightful discussions concerning current experimental capabilities we would like to thank M Dušek, W Wieczorek, C Schmid and J Matthews. KK was supported by Microsoft Research through the European PhD Programme and the EU (MINOS), and JE by the EU (QAP, COMPAS, MINOS) and the EURYI award.

References

[1] Knill E, Laflamme R and Milburn G J 2001 Nature 409 46
[2] Munro W J, Nemoto K, Spiller T P, Barrett S D, Kok P and Beausoleil R G 2005 J. Opt. B: Quantum Semiclass. Opt. 7 S135
   O’Brien J L 2007 Science 318 1567
   Walmsley I A 2008 Science 319 1211
   Aspelmeyer M and Eisert J 2008 Nature 455 180
[3] Politi A, Cryan M J, Rarity J G, Yu S and O’Brien J L 2008 Science 320 646
   Smith B J, Kundys D, Thomas-Peter N, Smith P G R and Walmsley I A 2009 Opt. Exp. 16 13516
[4] Hofmann H F and Takeuchi S 2002 Phys. Rev. A 66 024308
[5] Ralph T C, Langford N K, Bell T B and White A G 2002 Phys. Rev. A 65 062324
[6] Langford N K, Weinhold T J, Prevedel R, Resch K J, Gilchrist A, O’Brien J L, Pryde G J and White A G 2005 Phys. Rev. Lett. 95 210504
   Kiesel N, Schmid C, Weber U, Ursin R and Weinfurter H 2005 Phys. Rev. Lett. 95 210505
   Okamoto R, Hofmann H F, Takeuchi S and Sasaki K 2005 Phys. Rev. Lett. 95 210505
[7] Lanyon B P, Barbieri M, Almeida M P, Jennewein T, Ralph T C, Resch K J, Pryde G J, O’Brien J L, Gilchrist A and White A G 2009 Nat. Phys. 5 134
[8] Eisert J 2005 Phys. Rev. Lett. 95 040502
   Scheel S and Lütkenhaus N 2004 New J. Phys. 6 51
[9] Gross D and Eisert J 2007 Phys. Rev. Lett. 98 220503
[10] Raussendorf R and Briegel H J 2001 Phys. Rev. Lett. 86 5188
[11] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[12] Eisert J, Jacobs K, Papadopoulos P and Plenio M B 2000 Phys. Rev. A 62 052317
[13] Cirac J I, Duer W, Kraus B and Lewenstein M 2001 Phys. Rev. Lett. 86 544
   Berry D W 2007 Phys. Rev. A 75 032349
[14] Uskov D B, Smith A M and Kaplan L 2009 arXiv:0908.2482
[15] VanMeter N M, Lougovski P, Uskov D B, Kieling K, Eisert J and Dowling J P 2007 Phys. Rev. A 76 063808
[16] Kieling K 2008 PhD Thesis Imperial College London
[17] Kieling K 2010 Linear Optics State Transformations in preparation
[18] Nagata T, Okamoto R, O’Brien J L, Sasaki K and Takeuchi S 2007 Science 316 726
[19] O’Brien J L, Pryde G J, White A G, Ralph T C and Branning D 2003 Nature 426 264
[20] Politi A, Matthews J C F and O’Brien J L 2009 Science 325 1221

New Journal of Physics 12 (2010) 013003 (http://www.njp.org/)
[21] Smith B J, Kundys D, Thomas-Peter N, Smith P G R and Walmsley I A 2009 Opt. Exp. 17 13516
Matthews J C F, Politi A, Stefanov A and O’Brien J L 2009 Nat. Phot. 3 346
[22] Zhang Q, Bao X-H, Lu C-Y, Zhou X-Q, Yang T, Rudolph T and Pan J-W 2008 Phys. Rev. A 77 062316
[23] Horn R A and Johnson C R 1985 Matrix Analysis (Cambridge: Cambridge University Press)
[24] Ruppert W 1999 J. Number Theory 77 62
[25] Kaltofen E 1995 J. Comput. Syst. Sci. 50 274
[26] Ralph T C, Resch K J and Gilchrist A 2007 Phys. Rev. A 75 022313
[27] Fiurášek J 2006 Phys. Rev. A 73 062313
[28] Lütkenhaus N, Calsamiglia J and Suominen K-A 1999 Phys. Rev. A 59 3295
[29] Calsamiglia J 2002 Phys. Rev. A 65 030301
[30] O’Brien J L, Pryde G J, Gilchrist A, James D F V, Langford N K, Ralph T C and White A G 2004 Phys. Rev. Lett. 93 080502
[31] Černoch A, Soubusta J, Bartušková, Dušek M and Fiurášek J 2008 Phys. Rev. Lett. 100 180501
Wieczorek W, Schmid C, Kiesel N, Pohlner R, Guehne O and Weinfurter H 2008 Phys. Rev. Lett. 101 010503
[32] Lundeen J S, Feito A, Coldenstrodt-Ronge H, Pregnell K L, Silberhorn Ch Ralph T C, Eisert J, Plenio M B and Walmsley I A 2009 Nat. Phys. 5 27