No-go theorem for passive single-rail linear optical quantum computing

Lian-Ao Wu[1], Philip Walther[2] & Daniel A. Lidar[3]

[1]Ikerbasque–Basque Foundation for Science and Department of Theoretical Physics and History of Science, The Basque Country University (EHU/UPV), PO Box 644, 48080 Bilbao, Spain, [2]Faculty of Physics, University of Vienna, Boltzmanngasse 5, Vienna A-1090, Austria, [3]Departments of Electrical Engineering, Chemistry, and Physics, Center for Quantum Information & Technology, University of Southern California, Los Angeles, California 90089, USA.

Photonic quantum systems are among the most promising architectures for quantum computers. It is well known that for dual-rail photons effective non-linearities and near-deterministic non-trivial two-qubit gates can be achieved via the measurement process and by introducing ancillary photons. While in principle this opens a legitimate path to scalable linear optical quantum computing, the technical requirements are still very challenging and thus other optical encodings are being actively investigated. One of the alternatives is to use single-rail encoded photons, where entangled states can be deterministically generated. Here we prove that even for such systems universal optical quantum computing using only passive optical elements such as beam splitters and phase shifters is not possible. This no-go theorem proves that photon bunching cannot be passively suppressed even when extra ancilla modes and arbitrary number of photons are used. Our result provides useful guidance for the design of optical quantum computers.

O ptical implementations of qubits have played an important role in quantum information science[1,2]. Photons exhibit an intrinsic lack of decoherence and are simple to control by standard off-the-shelf components. Furthermore, photonic qubits for quantum computation are particularly attractive because they can be used to interface to various quantum communication applications[3]. Due to the extremely small photon-photon coupling available in existing materials, it was at one point believed that optical qubits could not be used for scalable quantum computation. However, it is now understood that the process of photon detection itself can lead to effective photon-photon nonlinearities. In particular Knill, Laflamme, and Milburn (KLM)[4] launched the field of linear optics quantum computing (LOQC) by showing that deterministic single-photon sources and high-efficiency single-photon detectors allow the realization of scalable, probabilistic quantum computation purely with linear optical elements. This holds in spite of the fact that using linear optics alone, the success probability of the nonlinear sign shift gate used in the KLM scheme cannot be improved above $1/4$[5,6]. Since the original KLM proposal, a number of authors have suggested various simplifications, modifications, and optimizations[7–10]. Although these results formally show that scalable quantum computing is possible, the realization is very demanding in practice due to the large resource overhead arising from the required non-deterministic photon detection events. This becomes particularly apparent when considering beamsplitter-based two-photon gates, which are probabilistic in nature. In fact all optical two-qubit gates[11], including the promising nondestructive CNOT gate[12,13], fail in the case where more than one photon is emitted into the same optical output mode, due to photon bunching. One proposal to actively suppress such gate failure events in the polarization encoding uses the quantum Zeno effect, by coupling to the output light fields to atomic transitions[14,15].

While the previous discussion concerned mostly dual-rail qubits, less is known about single-rail photonic qubits. Here we address the natural question of whether linear optical elements alone can be used to establish quantum interference such that the photon-bunching effect, and thus the probability of gate failure, can be eliminated for the case of single-rail encoding. We show that this cannot be achieved in the sense that one cannot simultaneously and deterministically implement a linear optical two-photon entangling gate and decouple the double-occupancy states (in this work we are not concerned with single-photon nonlocality[16]). We thus prove a no-go theorem for photon bunching suppression via all-unitary linear optics. Our result is complementary to the recent proof that the single-photon fraction in any of the single-mode states resulting from purely linear optical processing (even including conditioning on results of detections) cannot be made to exceed the efficiency of the best available photon source[17]. We stress that our proof applies in the setting of deterministic LOQC; we do not address the possibility of simultaneously optimizing the suppression of photon bunching and the success

probability of LOQC gates in the single-rail setting. Nor do we address here what may be gained by adding measurements or other non-unitary operations[18].

Results

Problem formulation. In the standard circuit model of quantum computing any unitary transformation on n qubits can be decomposed as a product of gates, each of which acts nontrivially on at most two qubits, and is the identity on the other qubits[19]. Likewise, in the linear optics model, any unitary transformation on M modes can be decomposed into a product of "linear optical elements," each of which acts nontrivially on at most two modes, and is the identity on the other $M - 2$ modes[20,21]. As linear optical operations we consider just *passive* elements, in particular phase shifters and beam splitters, as they generate all linear optical elements [i.e., all 2×2 unitaries, the group U(2)] when acting on the same pair of modes. Moreover, when they are allowed to act on overlapping pairs of modes, the linear optical elements generate all $M \times M$ unitaries [i.e., the group U(M)][20].

Single photon optical qubits come primarily in two varieties: single-rail[22,23], where a qubit is represented by the absence or presence of a single photon of fixed polarization in one optical mode, and dual-rail[19], where each qubit is encoded into the presence of a single photon in one or the other of two spatial optical modes. Polarization qubits[24]—where each qubit is represented by two orthogonal polarization modes—are formally equivalent to dual-rail qubits[11], so we will use both interchangeably (see Figure 1). Most LOQC proposals, including the original KLM scheme, use dual-rail qubits, but there is considerable interest in the single-rail encoding scheme as well, as evidenced by the numerous experiments devoted to preparation of arbitrary states of single-rail qubits[25–29]. In the dual-rail encoding single-qubit operations are straightforward while non-trivial two-qubits are challenging and are implemented probabilistically[4]. The reverse is true for single-rail encoding: it is easy to generate two-qubit entanglement deterministically, while single-qubit gates can be implemented probabilistically[30]. In both the single and dual-rail encodings two-qubit gate failure due to photon bunching is a major challenge standing in the way of scalability. Let us next explain this in more detail.

The subspace of interest in the single-rail encoding is spanned by the 6-dimensional Fock state basis $\mathcal{A} \cup \mathcal{B}$ where
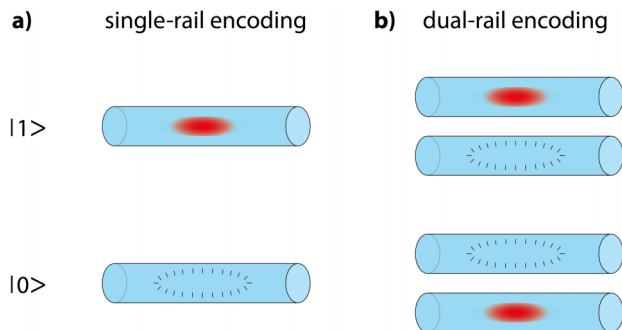

Figure 1 | Encoding of optical qubits. (a) Single-rail encoded qubits are represented by the absence or presence of a single photon of fixed polarization in one optical mode. This encoding allows for the deterministic generation of entangled states, but with the caveat that single-qubit gates can only be achieved probabilistically. (b) Dual-rail encoded qubits are represented by the presence of a single photon in one or the other of two spatial optical modes. Formally, polarization-encoded qubits are equivalent to the dual-rail encoding due to the basis comprising two orthogonal polarization modes, e.g., by defining $|1\rangle|0\rangle = |H\rangle$ and $|0\rangle|1\rangle = |V\rangle$ where $|H\rangle$ and $|V\rangle$ corresponds to a horizontally and vertically polarized photon state, respectively.

$$\mathcal{A} \equiv \left\{ 1, a_1^{\dagger}, a_2^{\dagger}, a_1^{\dagger} a_2^{\dagger} \right\} |0\rangle, \tag{1a}$$

$$\mathcal{B} \equiv \left\{ a_1^{\dagger 2}, a_2^{\dagger 2} \right\} |0\rangle \big/ \sqrt{2}. \tag{1b}$$

Here $|0\rangle$ is the global vacuum, $a_i^{\dagger}$, a_i, and n_i are the creation, annihilation, and number operator for mode i, respectively, satisfying the standard bosonic commutation relations. The subspace $\mathcal{A}$ is spanned by the computational basis of single-photon states in each of the two modes, while $\mathcal{B}$ is the subspace of "bunched" two photon states in either one of the two modes (double-occupation states). The latter are the problematic states causing computational errors in the single-rail encoding.

To define a basis for the polarization (i.e., dual rail) encoding consider the creation operators $a_{ip}^{\dagger}$, where $i \in \{1, 2\}$ is the spatial mode index, $p \in \{H, V\}$ is the polarization mode index, and all $a_{ip}^{\dagger}$ commute for all values of i and p. The ith qubit basis states are then $|0\rangle_i = a_{iH}^{\dagger}|0\rangle$ and $|1\rangle_i = a_{iV}^{\dagger}|0\rangle$, so that the computational and double-occupation (error) subspaces are, respectively,

$$\mathcal{A}' \equiv \left\{ a_{1H}^{\dagger} a_{2H}^{\dagger}, a_{1H}^{\dagger} a_{2V}^{\dagger}, a_{1V}^{\dagger} a_{2H}^{\dagger}, a_{1V}^{\dagger} a_{2V}^{\dagger} \right\} |0\rangle, \tag{2a}$$

$$\mathcal{B}' \equiv \left\{ a_{iH}^{\dagger 2} \big/ \sqrt{2}, a_{iV}^{\dagger 2} \big/ \sqrt{2}, a_{iH}^{\dagger} a_{iV}^{\dagger} \right\} |0\rangle, \quad i \in \{1, 2\} \tag{2b}$$

It is well known that linear optics is insufficient for generating non-trivial (entangling) two-qubit gates in the dual-rail encoding. Indeed, this, together with the inherent weakness of nonlinear photonic interactions such as the Kerr effect, is the *raison d'être* of the KLM scheme. The reason is a straightforward group-theoretic counting argument. Consider $m = 2K$ optical modes. If dual-rail linear optics could generate an entangling gate between one pair of qubits, which could then be swapped to all other pairs of qubits using beam splitters, the set of linear optical elements would generate the group U(2^K). However, this contradicts the fact that the set of linear optical elements can only generate U($2K$)[20,31]. This means that it is impossible to generate an entangling gate in the subspace $\mathcal{A}'$, irrespective of what happens in $\mathcal{B}'$. Another perspective on this is offered by results showing the unfeasibility of a linear optics Bell state analyzer, which rule out the implementation of a deterministic CNOT gate using dual-rail qubits[32,33]. However, these arguments cannot be applied in the single-rail case where a beam splitter suffices to generate two-qubit entanglement in the subspace $\mathcal{A}$. Since we are concerned in this work with deterministic gates we shall not consider the possibility of photon-bunching suppression and concurrent enhancement of the success probability of two-qubit gates in the dual-rail case. Instead, we devote the remainder of this work to the no-go theorem for deterministic gates in the single-rail case.

No-go theorem for two modes. We now proceed to prove the following no-go theorem: it is not possible to implement a deterministic entangling gate between two single-rail qubits while at the same time removing the "bunched" two-photon states using only linear optics. In this section we assume that only two photons in two modes are used; in the following section we allow for an arbitrary number of photons and modes.

The Hermitian beam-splitter generator is

$$X \equiv \frac{1}{2} \left(a_2^{\dagger} a_1 + a_1^{\dagger} a_2 \right), \tag{3}$$

and the Hermitian phase shifter generators are, for each mode,

$$n_1 = a_1^{\dagger} a_1, \quad n_2 = a_2^{\dagger} a_2. \tag{4}$$

Let us also define

$$Y \equiv \frac{i}{2} \left(a_2^{\dagger} a_1 - a_1^{\dagger} a_2 \right), \quad Z \equiv \frac{1}{2} (n_1 - n_2). \tag{5}$$

Then it is easily checked using the identities in the Methods section that the set of Hermitian operators $\{X, Y, Z\}$ is closed under commutation and moreover satisfies su(2) commutation relations. Therefore the beam-splitter generator X and the phase shifter generators (combined as Z) generate U(2). The most general unitary evolution operator we can then construct according to the Euler decomposition is the following composite gate:

$$U(\alpha,\beta,\gamma,\delta,\epsilon) = e^{i(\alpha n_1 + \beta n_2)} e^{i\epsilon X} e^{i(\gamma n_1 + \delta n_2)}, \tag{6}$$

where we have allowed a more general linear combination of the two phase shifter generators than Z, since they can be independently tuned.

We are interested in the (reducible) representation of the unitary operator (6) in the 6-dimensional Fock state basis $\mathcal{A} \cup \mathcal{B}$. We shall now show that if one demands that U does not couple $\mathcal{A}$ and $\mathcal{B}$, then without further assumptions it is not possible to implement an entangling gate between the two single-rail qubits. In the $\mathcal{A} \cup \mathcal{B}$ basis we have

$$U(\alpha,\beta,\gamma,\delta,\epsilon) = \mathrm{diag}\left(1, e^{i\alpha}, e^{i\beta}, e^{i(\alpha+\beta)}, e^{2i\alpha}, e^{2i\beta}\right) \begin{bmatrix} 1 & & \\ & A_1 & \\ & & B_1 \end{bmatrix} \times$$

$$\mathrm{diag}\left(1, e^{i\gamma}, e^{i\delta}, e^{i(\gamma+\delta)}, e^{2i\gamma}, e^{2i\delta}\right) = \begin{bmatrix} 1 & & \\ & A_2 & \\ & & B_2 \end{bmatrix}, \tag{7}$$

where diag denotes a diagonal matrix and where

$$A_1 = \begin{bmatrix} \cos\epsilon & i\sin\epsilon \\ i\sin\epsilon & \cos\epsilon \end{bmatrix},$$

$$A_2 = \begin{bmatrix} e^{i(\alpha+\gamma)}\cos\epsilon & ie^{i(\alpha+\delta)}\sin\epsilon \\ ie^{i(\beta+\gamma)}\sin\epsilon & e^{i(\beta+\delta)}\cos\epsilon \end{bmatrix},$$

$$B_1 = \begin{bmatrix} \cos 2\epsilon & \dfrac{1}{i\sqrt{2}}\sin 2\epsilon & \dfrac{1}{i\sqrt{2}}\sin 2\epsilon \\ \dfrac{1}{i\sqrt{2}}\sin 2\epsilon & \cos^2\epsilon & -\sin^2\epsilon \\ \dfrac{1}{i\sqrt{2}}\sin 2\epsilon & -\sin^2\epsilon & \cos^2\epsilon \end{bmatrix}, \tag{8}$$

$$B_2 =$$

$$\begin{bmatrix} e^{i(\alpha+\beta+\gamma+\delta)}\cos 2\epsilon & e^{i(\alpha+\beta+2\gamma)}\dfrac{\sin 2\epsilon}{i\sqrt{2}} & e^{i(\alpha+\beta+2\delta)}\dfrac{\sin 2\epsilon}{i\sqrt{2}} \\ e^{i(2\alpha+\gamma+\delta)}\dfrac{\sin 2\epsilon}{i\sqrt{2}} & e^{2i(\alpha+\gamma)}\cos^2\epsilon & -e^{2i(\alpha+\delta)}\sin^2\epsilon \\ e^{i(2\beta+\gamma+\delta)}\dfrac{\sin 2\epsilon}{i\sqrt{2}} & -e^{2i(\beta+\gamma)}\sin^2\epsilon & e^{2i(\beta+\delta)}\cos^2\epsilon \end{bmatrix}.$$

Note that $U(\alpha,\beta,\gamma,\delta,\epsilon)$ consists of three blocks (1, A_2, and B_2) of dimensions 1 (vacuum), 2 (one photon), and 3 (two photons), respectively. Therefore repeated applications of the composite gate U with different values for the angles $\alpha, \beta, \gamma, \delta, \epsilon$ will still have the same triple block structure. Hence our construction is general in the sense that we need only consider a single composite gate U.

Now, the problem is that the two-photon block includes $\mathcal{B}$. We would like to decouple these two states from the other four. Clearly, this can be done by setting the matrix elements $U_{4,5}$, $U_{4,6}$, $U_{5,4}$ and $U_{6,4}$ [i.e., the (1, 2), (1, 3), (2, 1), (3, 1) elements of B_2] to zero. As is clear from Eq. (8), a necessary and sufficient condition for this is

$$\sin 2\epsilon = 0. \tag{9}$$

This is achieved whenever ϵ is an integer multiple of $\pi/2$. If we pick an even multiple $2n$ of $\pi/2$ we have

$$U(\alpha,\beta,\gamma,\delta,n\pi) = \mathrm{diag}\left(1, (-1)^n e^{i(\alpha+\gamma)}, (-1)^n e^{i(\beta+\delta)}, \right.$$
$$\left. e^{i(\alpha+\beta+\gamma+\delta)}, e^{2i(\alpha+\gamma)}, e^{2i(\beta+\delta)}\right) \tag{10}$$

If we pick an odd multiple $2n + 1$ of $\pi/2$ we have

$$U\left(\alpha,\beta,\gamma,\delta,(2n+1)\frac{\pi}{2}\right) = \begin{bmatrix} 1 & & \\ & A_3 & \\ & & B_3 \end{bmatrix}, \tag{11}$$

where

$$A_3 = \begin{bmatrix} 0 & (-1)^n ie^{i(\alpha+\delta)} \\ (-1)^n ie^{i(\beta+\gamma)} & 0 \end{bmatrix} \tag{12a}$$

$$B_3 = \begin{bmatrix} -e^{i(\alpha+\beta+\gamma+\delta)} & 0 & 0 \\ 0 & 0 & -e^{2i(\alpha+\delta)} \\ 0 & -e^{2i(\beta+\gamma)} & 0 \end{bmatrix} \tag{12b}$$

In both cases U has a block-diagonal structure where the two-photons per mode states are decoupled from the other four states. Considering just the 4-dimensional block acting on span($\mathcal{A}$), we have for the even case

$$\mathrm{diag}\left(1, (-1)^n e^{i(\alpha+\gamma)}, (-1)^n e^{i(\beta+\delta)}, e^{i(\alpha+\beta+\gamma+\delta)}\right)$$
$$= \mathrm{diag}\left(1, (-1)^n e^{i(\beta+\delta)}\right) \otimes \mathrm{diag}\left(1, (-1)^n e^{i(\alpha+\gamma)}\right) \tag{13}$$

i.e., a tensor product of two single-qubit phase gates. Similarly, for the odd case we have

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & (-1)^n ie^{i(\alpha+\delta)} & 0 \\ 0 & (-1)^n ie^{i(\beta+\gamma)} & 0 & 0 \\ 0 & 0 & 0 & -e^{i(\alpha+\beta+\gamma+\delta)} \end{bmatrix} \tag{14}$$

$$= \mathrm{SWAP}\,\mathrm{diag}\left(1, (-1)^n ie^{i(\alpha+\delta)}\right) \otimes \mathrm{diag}\left(1, (-1)^n ie^{i(\beta+\gamma)}\right),$$

where $\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$, a non-entangling gate. Unfortun-

ately this means that, having decoupled span($\mathcal{B}$), the action of U on the $\mathcal{A}$ subspace is equivalent to a tensor product of two single-qubit phase gates, and therefore is no longer entangling.

The reason for this no-go result is straightforward: we are forced to set ϵ equal to a multiple of $\pi/2$ in order to prevent coupling to the span($\mathcal{B}$) subspace. Once we do this we are left with only four independent parameters ($\alpha, \beta, \gamma, \delta$), which are the parameters of the two phase shifters [see Eq. (6)]. The latter can only generate phase gates. To circumvent this result would require the use of some type of nonlinear optical element (see Figure 2).

No-go theorem for $M > 2$ modes. One might wonder whether the inclusion of additional modes and photons allows to circumvent the no-go theorem. In this section we show that this is not the case.

Consider a linear optical system with M modes containing an arbitrary number of photons, of which only two modes–supporting two qubits–are the target of linear optical quantum computation. We therefore refer to these two modes as the "computational modes." Clearly the choice of which two modes are identified as
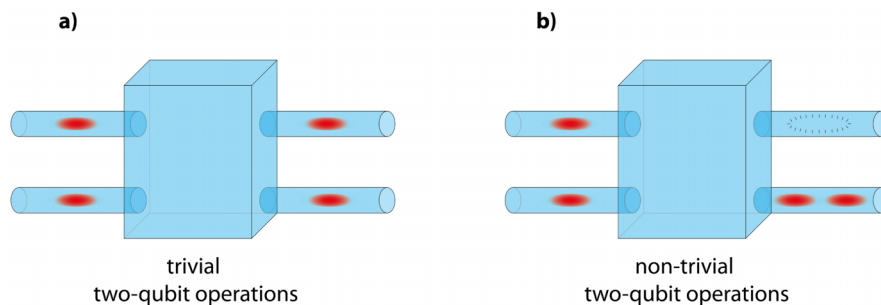
Figure 2 | Two-qubit operations for single-rail encoded qubits. (a) Only the restricted set of trivial two-qubit gates prohibits photon-bunching. (b) When using non-trivial two-qubit gates, such as the control-NOT or control-Phase gate, photon-bunching cannot be avoided and thus leads to gate errors or probabilistic success rates.

the computational modes is immaterial, so that without loss of generality we use the first two modes to this end. The computational basis still comprises only those states having either zero or one photons per mode in the first two modes, except that now an arbitrary number of photons is allowed in the ancillary modes 3, …, M. Let $\mathcal{C}_M \equiv \left\{ \Pi_{j=1}^{M} \frac{1}{\sqrt{n_j!}} \left(a_j^\dagger \right)^{n_j} |0\rangle \right\}$, where the occupation numbers $\{n_j\}_{j=1}^{M}$ are arbitrary. Then the computational basis states are the set $\mathcal{A}_M = \{\mathcal{C}_M | n_1, n_2 \in \{0,1\}\}$. The basis set for the problematic subspace of bunched states is now $\mathcal{B}_M = \{\mathcal{C}_M | n_1, n_2 \geq 2\}$. We assume that the photonic system is initialized in $\text{span}(\mathcal{A}_M)$. Furthermore, we assume that the initial state is a product state between the computational and ancilla modes, i.e., there is no initial entanglement between these two set of modes. Our proof does not apply otherwise, so that initialization errors are outside of the scope of this work and will have to be dealt with by other means.

Now let V be some arbitrary passive linear unitary optical transformation on all, or some subset, of the M modes. For example, V could be a product of phase shifters and beam splitters coupling any pair of modes. Its most general form is

$$V = \exp\left(i \sum_{i,j=1}^{M} \theta_{ij} a_i^\dagger a_j \right), \quad \theta_{ij} = \theta_{ji} \in \mathbb{R}, \quad (15)$$

an arbitrary element of U(M)[20]. The operator V replaces U [Eq. (6)] from our earlier two-mode discussion, and we shall show that even it cannot be used to decouple the computational basis states $\mathcal{A}_M$ from the bunched states $\mathcal{B}_M$ while simultaneously implementing an arbitrary unitary transformation on the computational modes. V has the following unitary representation in terms of the M × M matrix v = $\{v_{ij}\}$, in the basis of bosonic creation operators (see **Methods**):

$$V a_i^\dagger V^\dagger = \sum_{j=1}^{M} v_{ij} a_j^\dagger, \quad i \in \{1, \ldots, M\}, \quad (16)$$

Note that V commutes with the number operator, i.e., its only non-vanishing matrix elements are between Fock states with equal occupation numbers. Note also that if we write $V = \exp(i\Omega)$ where $\Omega = \sum_{i,j=1}^{M} \theta_{ij} a_i^\dagger a_j$, then $\Omega|0\rangle = 0$ due to the annihilation operator a_j, so that $V|0\rangle = |0\rangle$, and hence $\langle 0|V|0\rangle = 1$.

At first sight it might appear that the inclusion of ancilla modes could be useful. For example, one might hope that the bunched state $|200\rangle$ (for M = 3) can be transformed into the computational state $|002\rangle$, where the two photons have been transferred to the ancilla mode. However, this approach fails for passive all-unitary linear optics. The reason is that we must rule out the reverse process, i.e., we must impose the following necessary *"don't cause errors"* condition:

V cannot transfer any photons from the ancillary modes into the computational modes in a manner which transforms a valid computational basis state into a bunched state.

For example, V is not allowed to take the computational basis state $\left(a_3^\dagger \right)^2 |0\rangle \in \mathcal{A}_M$ to $\left(a_1^\dagger \right)^2 |0\rangle \in \mathcal{B}_M$ (ignoring normalization). Thus, we impose the necessary conditions for all $i \in \{3, \ldots, M\}$

$$\langle 0| a_1^2 V \left(a_i^\dagger \right)^2 |0\rangle = 0, \quad (17a)$$

$$\langle 0| a_2^2 V \left(a_i^\dagger \right)^2 |0\rangle = 0 \quad (17b)$$

Then,

$$0 = \langle 0| a_1^2 V \left(a_i^\dagger \right)^2 |0\rangle = \langle 0| a_1^2 V a_i^\dagger V^\dagger V a_i^\dagger V^\dagger V |0\rangle \quad (18a)$$

$$= \sum_{k,l=1}^{M} v_{ik} v_{il} \langle 0| a_1^2 a_k^\dagger a_l^\dagger V |0\rangle \quad (18b)$$

$$= v_{i1}^2 \langle 0| a_1^2 a_1^\dagger a_1^\dagger |0\rangle + \sum_{k,l=2}^{M} v_{ik} v_{il} \langle 0| a_k^\dagger a_l^\dagger a_1^2 |0\rangle \quad (18c)$$

$$+ 2 \sum_{k=2}^{M} v_{ik} v_{il} \langle 0| a_k^\dagger a_1^2 a_1^\dagger |0\rangle$$

$$= v_{i1}^2 \langle 0| a_1^2 a_1^\dagger a_1^\dagger |0\rangle \quad (18d)$$

where to arrive at (18b) we used Eq. (16), and to arrive at (18c) we used $V|0\rangle = |0\rangle$ along with the standard bosonic commutation relations, and to arrive at (18d) we used the fact that both sums in (18c) vanish due to $\langle 0|a_k^\dagger = 0$. We can thus conclude that v_{i1} must vanish for all $i \in \{3, \ldots, M\}$. After we impose the additional necessary condition $\langle 0| a_2^2 V \left(a_i^\dagger \right)^2 |0\rangle = 0$, we find that v_{i2} must vanish for all $i \in \{3, \ldots, M\}$. In addition, it follows from unitarity of v that then also v_{1i} and v_{2i} must vanish for all $i \in \{3, \ldots, M\}$ (see **Methods**). That is, we have proved that the "don't cause errors" condition implies that v has a block-diagonal structure:

$$v = v_c \oplus v_a, \quad (19)$$

where v_c is a 2 × 2 block (over the computational modes $i, j \in \{1, 2\}$) and v_a is an (M − 2) × (M − 2) block (over the ancilla modes $i, j \in \{3, \ldots, M\}$). This, in turn, can be interpreted as "don't couple". It states that, subject to the "don't cause errors" condition, V cannot couple the computational and ancilla modes, and in particular cannot cause photons to leak from the ancilla modes into the computational, or *vice versa*. For example, V cannot couple the two computational basis states $|001\rangle$ and $|100\rangle$ (M = 3). It is conceptually clear that this implies that nothing is gained by the introduction of the ancilla modes. However, let us provide a formal proof as well.

Assume, as before, that the system is initially in a factorized state between the computational and ancilla modes: $G\left(a_3^\dagger,\ldots,a_M^\dagger\right) \times F\left(a_1^\dagger,a_2^\dagger\right)|\mathbf{0}\rangle$, where F and G are arbitrary polynomials in the creation operators, e.g., $F\left(a_1^\dagger,a_2^\dagger\right) = \sum_{m_1,m_2=0} c_{m_1,m_2}\left(a_1^\dagger\right)^{m_1}\left(a_2^\dagger\right)^{m_2}$, where c_{m_1,m_2} are arbitrary coefficients. Note that because of the block-diagonal structure of v it follows that

$$
\begin{aligned}
V\,F\left(a_1^\dagger,a_2^\dagger\right)V^\dagger &= \sum_{m_1,m_2=0} c_{m_1,m_2}\left(Va_1^\dagger V^\dagger\right)^{m_1}\left(Va_2^\dagger V^\dagger\right)^{m_2}\\
&= \sum_{m_1,m_2=0} c_{m_1,m_2}\left(\sum_{j=1}^2 v_{1j}a_j^\dagger\right)^{m_1}\left(\sum_{j'=1}^2 v_{2j'}a_{j'}^\dagger\right)^{m_2} \quad (20)\\
&= F'\left(a_1^\dagger,a_2^\dagger\right),
\end{aligned}
$$

where F' is a new polynomial. Here the key point is that the ancilla modes do not appear in F'. A similar calculation reveals that $V\,G\left(a_3^\dagger,\ldots,a_M^\dagger\right)V^\dagger = G\left(Va_3^\dagger V^\dagger,\ldots,Va_M^\dagger V^\dagger\right) = G'\left(a_3^\dagger,\ldots,a_M^\dagger\right)$, where G' is a new polynomial. Therefore the action of V on an arbitrary factorized initial state is

$$
V\,G\left(a_3^\dagger,\ldots,a_M^\dagger\right)F\left(a_1^\dagger,a_2^\dagger\right)|\mathbf{0}\rangle \tag{21a}
$$

$$
= \left[V\,G\left(a_3^\dagger,\ldots,a_M^\dagger\right)V^\dagger\right]\left[V\,F\left(a_1^\dagger,a_2^\dagger\right)V^\dagger\right]V|\mathbf{0}\rangle \tag{21b}
$$

$$
= G'\left(a_3^\dagger,\ldots,a_M^\dagger\right)F'\left(a_1^\dagger,a_2^\dagger\right)|\mathbf{0}\rangle. \tag{21c}
$$

For the computational modes this is equivalent to $V\,F\left(a_1^\dagger,a_2^\dagger\right)\times|\mathbf{0}\rangle = \left(a_1^\dagger,a_2^\dagger\right)|\mathbf{0}\rangle$, where the no-go theorem for $M=2$ holds.

Discussion

We have shown that using linear optics alone it is not possible to cancel the photon bunching effect while at the same time implementing a deterministic universal set of logic gates using single-rail photonic qubits. In spirit our result agrees with previous theoretical work concerning the dual-rail encoding case[4,32,33], showing that passive linear optics does not involve particle interactions other than those imposed by statistics, and can be understood in terms of classical wave mechanics. One approach is to then consider additional non-linear operations such as photon-detection or absorption[14], the Kerr effect, or light squeezing, in order to enable universal linear optical quantum computing. However, our work leaves open the possibility that a more general analysis than we have considered here, in particular one which accounts for the possibility of a *probabilistic* enhancement (or even optimization) of both photon-bunching suppression and linear optical gate fidelity, might circumvent our no-go theorem. Nor did we consider measurements of the ancilla modes or other non-unitary transformations. For example, one might consider a non-unitary transformation with maps the bunched state $|200\rangle$ (on a total of three modes) to the computational basis state $|002\rangle$, without at the same time mapping $|002\rangle$ back into the computational subspace. In this sense the results presented here are thus a starting point for a study of the use of additional resources in linear optics quantum computing using single-rail qubits.

Methods

Unitary representation of V in the creation operator basis. To prove that the representation of V in Eq. (16) is unitary one can use the standard bosonic commutation relations along with the Baker-Hausdorff formula

$$
e^{\alpha A}Be^{-\alpha A} = B + \sum_{m=1}^\infty \frac{\alpha^m}{m!}[_mA,B], \tag{22}
$$

where $[_mA, B] := [A, [_{m-1}A, B]]$ and $[_1A, B] \equiv [A, B]$, for arbitrary operators A and B, and $\alpha \in \mathbb{C}$, to establish that $v = e^{-i\theta}$, where $\theta = \{\theta_{ij}\}$ is the orthogonal matrix of angles

appearing in Eq. (15). Indeed, setting $\alpha = i$, $A = \sum_{kj}\theta_{kj}a_k^\dagger a_j$, $B = a_i^\dagger$, and using the identity $\left[a_k^\dagger a_j, a_i^\dagger\right] = \delta_{ij}a_k^\dagger$, we have:

$$
[A,B] = \sum_j [\theta]_{ji}a_j^\dagger \tag{23a}
$$

$$
\begin{aligned}
[_2A,B] &= \sum_{jkm}\theta_{jk}\theta_{mi}\left[a_j^\dagger a_k, a_m^\dagger\right] = \sum_{jm}\theta_{jm}\theta_{mi}a_j^\dagger\\
&= \sum_j [\theta^2]_{ji}a_j^\dagger,
\end{aligned} \tag{23b}
$$

etc., so that $[_mA,B] = \sum_{j=1}^M [\theta^m]_{ji}a_j^\dagger$. Thus

$$
Va_i^\dagger V^\dagger = \sum_{m=0}^\infty \frac{i^m}{m!}\sum_{j=1}^M [\theta^m]_{ji}a_j^\dagger = \sum_{j=1}^M \left[e^{i\theta}\right]_{ji}a_k^\dagger, \tag{24}
$$

so that $v_{ij} = [e^{i\theta}]_{ji}$, whence $v = e^{-i\theta}$ as claimed.

Proof that "don't cause errors" implies "don't couple". Consider a unitary matrix v with the block structure

$$
v = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}, \tag{25}
$$

where x and z are square and y can be rectangular. The unitarity condition $v^\dagger v = I$ yields

$$
\begin{pmatrix} x^\dagger & 0 \\ y^\dagger & z^\dagger \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} x^\dagger x & x^\dagger y \\ y^\dagger x & y^\dagger y + z^\dagger z \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}, \tag{26}
$$

so that $x^\dagger x = I$ and $x^\dagger y = 0$. By unitarity of v the matrix X cannot be zero, so $x^{-1} = x^\dagger$ and hence also $xx^\dagger = I$. Thus $xx^\dagger y = y = 0$. In the context of our proof in the last section, we showed that the "don't cause errors" condition implies that both $v_{i1} = v_{i2} = 0$ for all $i \in \{3, \ldots, M\}$. This is the 0 block in Eq. (25). The vanishing of the y block then implies that also $v_{1i} = v_{2i} = 0$ for all $i \in \{3, \ldots, M\}$, which is the "don't couple" result.

1. O'Brien, J. L. Optical quantum computing. *Science* **318**, 1567–1570 (2007).
2. Aspuru-Guzik, A. & Walther, P. Photonic quantum simulators. *Nature Physics* **8**, 285–291 (2012).
3. O'Brien, J. L., Furusawa, A. & Vučković, J. Photonic quantum technologies. *Nature Photonics* **3**, 687 (2009).
4. Knill, E., Laflamme, R. & Milburn, G. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46 (2001).
5. Scheel, S. & Lütkenhaus, N. Upper bounds on success probabilities in linear optics. *New J. Phys.* **6**, 51 (2004).
6. Eisert, J. Optimizing linear optics quantum gates. *Phys. Rev. Lett.* **95**, 040502 (2005).
7. Pittman, T. B., Jacobs, B. C. & Franson, J. D. Probabilistic quantum logic operations using polarizing beam splitters. *Phys. Rev. A* **64**, 062311 (2001).
8. Knill, E. Quantum gates using linear optics and postselection. *Phys. Rev. A* **66**, 052306 (2002).
9. Ralph, T. C., White, A. G., Munro, W. J. & Milburn, G. J. Simple scheme for efficient linear optics quantum gates. *Phys. Rev. A* **65**, 012314 (2001).
10. Uskov, D. B., Kaplan, L., Smith, A. M., Huver, S. D. & Dowling, J. P. Maximal success probabilities of linear-optical quantum gates. *Phys. Rev. A* **79**, 042326 (2009).
11. Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79**, 135–174 (2007).
12. Pittman, T. B., Jacobs, B. C. & Franson, J. D. Demonstration of nondeterministic quantum logic operations using linear optical elements. *Phys. Rev. Lett.* **88**, 257902 (2002).
13. Pittman, T. B., Fitch, M. J., Jacobs, B. C. & Franson, J. D. Experimental controlled-not logic gate for single photons in the coincidence basis. *Phys. Rev. A* **68**, 032316 (2003).
14. Franson, J. D., Jacobs, B. C. & Pittman, T. B. Quantum computing using single photons and the zeno effect. *Phys. Rev. A* **70**, 062302 (2004).
15. Leung, P. M. & Ralph, T. C. Optical zeno gate: bounds for fault tolerant operation. *New J. Phys.* **9**, 224 (2007).
16. Dunningham, J. & Vedral, V. Nonlocality of a single particle. *Phys. Rev. Lett.* **99**, 180404 (2007).
17. Berry, D. W. & Lvovsky, A. I. Linear-optical processing cannot increase photon efficiency. *Phys. Rev. Lett.* **105**, 203601 (2010).
18. Verstraete, F., Wolf, M. M. & Ignacio Cirac, J. Quantum computation and quantum-state engineering driven by dissipation. *Nat Phys* **5**, 633–636 (2009).
19. Nielsen, M. & Chuang, I. *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
20. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58–61 (1994).
21. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics (2010). arXiv:1011.3245.

22. Pegg, D. T., Phillips, L. S. & Barnett, S. M. Optical state truncation by projection synthesis. *Phys. Rev. Lett.* **81**, 1604–1606 (1998).

23. Lee, H.-W. & Kim, J. Quantum teleportation and Bell's inequality using single-particle entanglement. *Phys. Rev. A* **63**, 012305 (2000).

24. Milburn, G. J. Quantum optical Fredkin gate. *Phys. Rev. Lett.* **62**, 2124–2127 (1989).

25. Lombardi, E., Sciarrino, F., Popescu, S. & De Martini, F. Teleportation of a vacuum one-photon qubit. *Phys. Rev. Lett.* **88**, 070402 (2002).

26. Resch, K. J., Lundeen, J. S. & Steinberg, A. M. Quantum state preparation and conditional coherence. *Phys. Rev. Lett.* **88**, 113601 (2002).

27. Lvovsky, A. I. & Mlynek, J. Quantum-optical catalysis: Generating nonclassical states of light by means of linear optics. *Phys. Rev. Lett.* **88**, 250401 (2002).

28. Babichev, S. A., Ries, J. & Lvovsky, A. I. Quantum scissors: Teleportation of single-mode optical states by means of a nonlocal single photon. *Europhys. Lett.* **64**, 1 (2003).

29. Babichev, S. A., Brezger, B. & Lvovsky, A. I. Remote preparation of a single-mode photonic qubit by measuring field quadrature noise. *Phys. Rev. Lett.* **92**, 047903 (2004).

30. Lund, A. P. & Ralph, T. C. Nondeterministic gates for photonic single-rail quantum logic. *Phys. Rev. A* **66**, 032307 (2002).

31. Wu, L.-A. & Lidar, D. A. Qubits as parafermions. *J. Math. Phys* **43**, 4506–4525 (2002).

32. Lütkenhaus, N., Calsamiglia, J. & Suominen, K.-A. Bell measurements for teleportation. *Phys. Rev. A* **59**, 3295–3300 (1999).

33. Calsamiglia, J. & Lütkenhaus, N. Maximum efficiency of a linear-optical Bell-state analyzer. *Appl. Phys. B* **72**, 67–71 (2001).

Acknowledgments

Authors contributions

All authors contributed equally.

Additional information

How to cite this article: Wu, L., Walther, P. & Lidar, D. No-go theorem for passive single-rail linear optical quantum computing. *Sci. Rep.* **3**, 1394; DOI:10.1038/srep01394 (2013).