Contents lists available at ScienceDirect

Reviews in Physics

journal homepage: www.elsevier.com/locate/revip

# The resurgence of the linear optics interferometer — recent advances & applications

Si-Hui Tan[a,b], Peter P. Rohde[c,*]

[a] *Singapore University of Technology and Design, Singapore University of Technology and Design, 8 Somapah Rd, Singapore 487372*
[b] *Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543, Singapore*
[c] *Centre for Quantum Software & Information (CQSI), Faculty of Engineering & Information Technology, University of Technology Sydney, NSW 2007, Australia*

ARTICLE INFO

*Article history*:

*2000 MSC:* 41A05, 41A10, 65D05, 65D17

*Keywords:* Keyword1, Keyword2, Keyword3

ABSTRACT

Linear optics has seen a resurgence for applications in quantum information processing owing to its miniaturisation on-chip, and increase in production efficiency and quality of single photons. Time-bin encodings have also become feasible owing to architectural breakthroughs, and new processing capabilities. Theoretical efforts have found new ways to implement universal quantum computations with linear optics requiring less resources, and to demonstrate the capabilities of linear optics without requiring a universal optical quantum computer.



## 1. Introduction

Linear optics play a prominent role in quantum information processing. Photons make fantastic 'flying' qubits, and are readily used for quantum communication [**bib:Northup14**] and quantum key distribution [**bib:Lo14**]. In 2001, Knill, Laflamme and Milburn (KLM) showed that efficient quantum computing is possible using only linear optical components, that is single photons, beamsplitters, phase shifters and photon counting [**bib:KLM01**]. Furthermore, an optical implementation of quantum protocols can potentially piggyback on existing communication infrastructure. Combined with the relative ease of transporting quantum states of light, as compared to say trapped ions or superconducting qubits, linear optics forms a powerful platform for quantum information processing.

The promises offered by linear optics have spearheaded many technical advancements. One of the major successes for linear optics is the paradigm shift from bulk optics to integrated photonics [**bib:Meany15**]. The advantage of using such integrated photonics over bulk optics is that it is more stable against phase fluctuations, and miniaturized. This has increased the scalability of optical implementations of quantum information protocols. Furthermore, it is now possible to have single-photon sources and detectors together with linear-optical networks on a silica chip [**bib:Sprengers11**, **bib:Silverstone14**]. Having all components on chip reduces coupling losses which would be crucial for fault-tolerance [**bib:Li15**].

*Corresponding author: dr.rohde@gmail.com ;http:// www.peterrohde.org

In the last decade, single photons have been produced mainly through a nonlinear optical process know as spontaneous parametric down-conversion (SPDC), a nonlinear optical process. SPDC produces single photons in correlated pairs that has been a staple source of entanglement. Through developments in production, the number of high quality indistinguishable photons that can be simultaneously produced have increased steadily over the years. Single-photon pairs, once a novelty, are now run-of-the-mill business for quantum optical labs, and three or four photons have become commonplace [**bib:Spagnolo12**, **bib:Tillmann13**, **bib:Spring13**, **bib:Broome13**]. Experiments using up to ten photons have been demonstrated [**bib:WangChen16**, **bib:Chen17**]. We have also seen the meteoric rise of quantum dots in the role for producing single photons [**bib:Ding16**, **bib:WangHe16**, **bib:213601**]. They are a scalable source of single photons which are highly indistinguishable, and are produced on demand–a significant advantage over SPDC which is an inherently probabilistic process.

Another approach to linear optics is to pack more features known as degrees of freedom onto a single photon, and to increase the degree of control over them. It is possible to manipulate degrees of freedom like polarization, time-of-arrival, and orbital angular momentum [**bib:Tillmann2015**, **bib:Bozinovic2013**, **bib:Nicolas2014**, **bib:Humphreys2013**, **bib:Donohue2013**]. Since KLM, new proposals for linear optical quantum computations (LOQC) have surfaced [**bib:Nielsen04**, **bib:BrowneRudolph05**, **bib:Gimeno-Segovia15**, **bib:Pant17**]. Some of them support new functionalities like secure delegated quantum computations [**bib:Barz12**, **bib:Fisher14**]. Others do not promise universality in their processing, but still performs tasks such as sampling [**bib:Aaronson11**], encrypted quantum walks [**bib:Rohde˙qw12**], and secure quantum computations [**bib:Tan16**] that might be hard or impossible with a classical system. Such methods open up new ways to engineer quantum states and quantum operations, and expand the toolbox of baseline resources we have for implementing quantum computations, which could prove crucial in the race to achieve quantum supremacy.

We begin in Section 2 with an overview of the mathematical treatment of linear optical transformation on single photons, and in Section 3 with a description of some commonly used qubit encodings. Any unitary transformation acting on the spatial label of single photons can be efficiently decomposed into a network of beamsplitters and phase-shifters. We discuss this, and an extension to handle additional internal states, in Section 4. For applying any linear optical circuit, one needs an accurate description of its unitary representation. A full quantum tomography is costly and time-consuming. Some practical methods have been devised to do this reconstruction without resorting to tomography, and these are described in Section 5. In Section 6, we recap the experimental breakthroughs in state preparation of single photons, and some entangled quantum states. This is followed by advances in time-bin based architecture for linear optical networks, and photodectors in Sections 7 and 8 respectively. Last, but not least, we review applications for linear optical interferometry in LOQC, BOSONSAMPLING, and quantum metrology.

## 2. Mathematical background

A single photon in a quantum interferometer is described by its creation and annihilation operators, $\hat{a}_j^\dagger$ and $\hat{a}_j$ respectively, where $j$ is the mode label of the interferometer. These operators satisfy the bosonic comutation relationship $[\hat{a}_j, \hat{a}_k^\dagger] = \delta_{j,k}$. The action of a $2d$-port linear optical interferometer that has an equal number of input and output ports is expressed as an application of unitary operations on the creation operators,

$$b_i^\dagger = \sum_{j=1}^{d} U_{ij} a_j^\dagger \,, \tag{1}$$

where $a_j^\dagger$ and $b_i^\dagger$ are the creation operators of a single input and output photon in the $j$-th and $i$-th modes respectively, and $U \in SU(d)$. All such transformations can be expressed as sequences of beamsplitters and phase-shifters [**bib:Reck1994**] (see Section 4). By convention, the interferometer is assumed to act only on the spatial mode of the input state.

Additional quantum labels are added to the creation and annihilation operators when other degrees of freedom, such as polarization, orbital angular momentum, and time-bins, are present. In this case, their commutator relation is

$$[\hat{a}_{j,\alpha}, \hat{a}_{k,\beta}^\dagger] = \delta_{j,k}\delta_{\alpha,\beta} \,, \tag{2}$$

where $\alpha$ and $\beta$ represent these other degrees of freedom. As a consequence, quantum interference between multiple photons only occur when all quantum labels are the same. It is also possible to derive an analogous decomposition to

that of Reck *et al.* that realizes the unitary transformation on such photons as a sequence of beamsplitters and internal transformations.

Control of indistinguishability of these photons may enable future applications. Mathematical methods have been developed to deal with partial distinguishabilities among interfering photons, including those using group theory [**bib:Tan2013**, **bib:deGuise2014**, **bib:deGuise2015**], and quantum-to-classical transitions [**bib:Ra2013**]. Recently, by controlling multiple degrees of freedom of single photons, genuine three-photon interference that has no independent entanglement between any two subpairs of photons was demonstrated [**bib:Agne17**, **bib:Menssen17**].

## 3. Optical encoding of quantum information on single-photons

Using quantum states of light, there are a multitude of approaches to encoding quantum information. Beginning with a logical qubit,

$$|\psi\rangle_L = \alpha|0\rangle_L + \beta|1\rangle_L, \tag{3}$$

we now discuss the most prominent such encodings, which have been widely employed. We will specifically focus on single-photon encodings, as opposed to, for example, continuous variable encodings.

These encodings are all isomorphic to one another, but nonetheless, because they are represented using entirely different physical systems, they each exhibit their own unique advantages and disadvantages, and methods by which to implement operations upon them.

### *3.1. Polarisation*

In polarisation encoding, the polarisation of a single photon in a single spatial mode encodes a logical qubit. Specifically, we represent the logical qubit as,

$$|\psi\rangle_L = \alpha|H\rangle + \beta|V\rangle, \tag{4}$$

where $H$ ($V$) denotes a horizontally (vertically) polarised single photon.

Polarisation encoding has the elegance that the most common optical error mechanisms, such as loss or path-length mismatch, affect the two logical basis states equally. Furthermore, single-qubit operations may be directly implemented using wave-plates, which implement a rotation in polarisation space. Relevant to the preparation of large entangled states, such as cluster states, polarising beamsplitters can be employed to perform non-deterministic Bell state projections.

When physically constructing protocols based on polarisation-encoding, for obvious reasons it is extremely important that optical components be polarisation-preserving. Not doing so would obviously corrupt the logical state. Some waveguide technologies, for example, exhibit different refractive indices for the two polarisations.

### *3.2. Dual-rail*

In dual-rail encoding, a single photon encodes a logical qubit as a superposition across two spatial modes,

$$|\psi\rangle_L = \alpha|1,0\rangle + \beta|0,1\rangle, \tag{5}$$

where $|i,j\rangle$ is a two-mode state with $i$ ($j$) photons in the first (second) spatial mode. Using this encoding, phase-shifters and beamsplitters between the two spatial modes implement arbitrary single-qubit operations. Converting between polarisation- and dual-rail-encoding is trivial using polarising beamsplitters, which separate horizontal and vertical components into distinct spatial modes, or vice-versa.

Unfortunately, because the two basis states evolve via independent paths, our dual-rail qubits are susceptible to path-length-mismatch, a problem that does not affect polarisation encoding. Nonetheless, there are certain advantages to using two paths as opposed to one as is the case in single-rail encoding where the presence or absence of a photon denotes the logical bit. The loss of a photon in a dual-rail qubit is easily noted by its absence, whereas in a single-rail encoding, it would have been confused for one of the states. Moreover, a no-go result precludes universal quantum computation using just linear optics without the use of measurements in a single-rail encoding [**bib:Wu13**], thus making dual-rail encoding a more attractive alternative.

### *3.3. Time-bins*

Time-bin qubits encode quantum information into the time-of-arrival of single photons, which have fixed polarisation and reside in a single spatial mode. Effectively, we discretise the direction of propagation of photons into discrete bins, which are treated as orthogonal basis states. Specifically, we are employing the encoding,

$$|\psi\rangle_L = \alpha|1\rangle_t|0\rangle_{t+\tau} + \beta|0\rangle_t|1\rangle_{t+\tau}, \tag{6}$$

where $|0\rangle_t$ ($|1\rangle_t$) denotes the vacuum (single-photon) state with arrival time $t$. Here $\tau$ is the time-bin separation, which must be sufficiently large that the temporal envelopes of neighbouring photons do not overlap, thereby ensuring orthogonality of the logical basis states.

This encoding is particularly resource-savvy, since a single spatial mode (e.g length of optical fibre) can encapsulate many time-bin qubits as a 'time-bin-train'. The amount of quantum information that can be encoded into the train is limited only by its physical length.

Unlike polarisation or dual-rail encoding, time-bin encoding does not lend itself to 'native' single-qubit operations. Rather, fast switching can be used to spatially separate neighbouring time-bins, implement a beamsplitter operation between them, before converting back to time-bin encoding. An experiment has built on this idea to implement a two-qubit gate by fast switching to a polarization basis [**bib:Humphreys2013**]. Another promising advance is an ultrafast measurement technique for time bins based on converting into frequency bins [**bib:Donohue2013**]. Scalable networks using time-bin encoding are also possible using a loop-based architecture [**bib:Motes14**]. This is discussed in more detail in Section 7.

## 4. Efficient circuit decompositions of linear optics networks

The task of implementing an arbitrary quantum computation on linear optics comes down to implementing an arbitrary $n \times n$ unitary matrix. If a non-unitary transformation is desired, it can be embedded within a unitary matrix with larger dimensions. An algorithm for expressing an arbitrary unitary matrix *exactly* in terms of a sequence of beamsplitters and phase-shifters was described by Reck *et al.* [**bib:Reck1994**]. This decomposition requires $O(n^2)$ linear optical elements, and the algorithm for finding the decomposition has polynomial runtime. Thus, such decompositions can always be determined and implemented efficiently. The layout for the original Reck *et al.* decomposition is shown in Fig. 1. However, since then a multitude of alternate decompositions have been found. A notable downside of the original decomposition is that different photons experience different circuit depth, i.e pass through different numbers of optical elements, resulting in asymmetry in losses and the accumulation of errors.

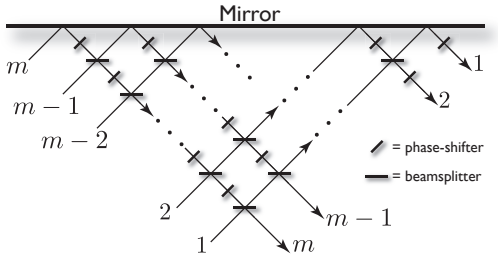



Fig. 1: Efficient decomposition of arbitrary linear optics networks into a sequence of beamsplitters and phase-shifters.

Alternatively, Mach-Zedner interferometers can also be employed as building blocks instead of beamsplitters and phase-shifters [**bib:Englert2001**]. Later, it was shown that any nontrivial beamsplitter, that does more than permuting modes or adding phases to them, is universal for linear optics [**bib:Bouland2014**]. However, they do not provide an explicit construction for arbitrary unitaries.

If the linear optical transformations is to be realized on various degrees of freedom of light, then it is possible to realize a $n \times n$ arbitrary unitary transformation, where $n = n_s n_p$ for $n_s$ spatial modes, and $n_p$ internal modes, by a sequence of $O(n_s^2 n_p)$ beamsplitters and $O(n_s^2)$ internal transformations [**bib:Dhand2015**]. This approach reduces the required number of beamsplitters but increases the total number of optical elements needed by a factor of 2.

## 5. Reconstructing the linear optical network

In many practical situations, the structure of a linear optical device in terms of its constituent beamsplitters and phase-shifters is known once it is built. However, owing to manufacturing imperfections, a precise characterization of these devices may still be needed post-production. One approach for achieving this is via quantum process tomography. However, quantum process tomography is an expensive approach in terms of the number of measurements required to characterize the network, with exponential overhead, becoming impractical for large optical networks which can contain hundreds of modes using present-day technology [**bib:Harris16**]. To mitigate this problem, alternative characterization protocols have been developed.

Generally, the unitary matrices of $d \times d$ linear optical devices are complex $U_{ij} = r_{ij}e^{i\theta_{ij}}$, where $0 \leq r_{ij} \leq 1$, and $0 \leq \theta_{ij} \leq 2\pi$. To characterize these numbers, one can do so by injecting one- and two-photon states into the network with correlated photon detection [**bib:Laing12**]. With some mathematical simplifications, the parameters can be solved for using the one-photon transmissions, and the visibility of two-photon inputs. An increased accuracy in the characterization is possible by estimating and correcting systematic errors that arise due to mode mismatch [**Dhand16**]. Others have used numerical methods to find the closest parameters that yield the observed visibilities [**bib:Spagnolo16**, **bib:Tillmann16**].

An alternative method uses coherent states to probe the interferometer [**bib:Rahimi-Keshari13**, **bib:Heilmann15**] instead of Fock states. Such states are produced by a standard laser source, thus reducing experimental resources. The $r_{jk}$ terms can be calculated from the ratios of output intensities at the $k$th port to the input intensity at the $j$th port. The remaining phases $\theta_{ij}$ are found by the interference pattern given by a two-mode coherent state $|\alpha\rangle|\alpha e^{\phi}\rangle$. When the states are injected into ports 1, and $j$ respectively, the output intensity at the $k$th port is

$$I_k = I(r_{1k}^2 + r_{jk}^2 + 2r_{1k}r_{kj}\cos(\phi + \theta_{jk}))\,, \tag{7}$$

where $\theta_{jk} = 0$ for $k = 1$, and $I$ is the intensity of the input coherent states. By scanning the phase shift $\phi$ and locating the maximum value of $I_k$ for $j = 2, \ldots, m$, all unknown phases can be found via $\theta_{jk} = 2\pi - \phi$. An elegant modification of this scheme removes the need for precise control of the phase-shift $\phi$ by suggesting instead to plot the output intensity $I_k$ with respect to the input intensity $I$ [**bib:Heilmann15**]. In time, the natural drift in the laser source will cause this plot to trace out an ellipse, known as a Lissajous figure, whose orientation and direction of evolution will give the phase $\theta_{jk}$ and its sign respectively.

## 6. State preparation

The photonic states that are most commonly employed in linear optics protocols can be divided into Fock states (e.g single-photon), and entangled states, such as EPR, GHZ and cluster states. We will consider advances in each of these.

### *6.1. Fock states*

Sources of single photons for applications in quantum information processing can be separated into two main categories: those produced by spontaneous parametric down-conversion (SPDC), and those by solid-state emitters in a cavity. To-date, SPDC has been able to produce up to ten entangled photons [**bib:WangChen16**, **bib:Chen17**] that can in turn be converted into indistinguishable photons, and a quantum dot emitter in a microcavity has produced five photons [**bib:WangHe16**].

In SPDC, a nonlinear crystal with a large $\chi^{(2)}$ non-linearity is pumped with a laser source and with a small probability, the pump beam is absorbed by the crystal to produce two beams of lower energy known as the signal and idler. Owing to conservation of energy and momentum, the two beams have spatio-temporal correlations that can be engineered to produce twin-beam states with perfect photon number correlation, of the form

$$|\psi\rangle_{\text{SPDC}} = \sqrt{1-\chi^2}\sum_{n=0}^{\infty}\chi^n|n,n\rangle, \tag{8}$$

where $\chi$ is the squeezing parameter. If a single photon were to be detected in one of the modes, it is certain that the other mode would similarly contain a single photon.

Solid-state single photon sources are versatile and efficient sources of single photons, however, the photons they produce have suffered from the lack of indistinguishability that is necessary for typical quantum information processing applications. Recent developments using resonant excitation of quantum dots were able to overcome these limitations. Laser pulses are used to excite the electronic resonance of the quantum dots and trigger the emission of high quality single photons [**bib:WangHe16**]

### *6.2. Einstein-Podolsky-Rosen (EPR) pairs*

An EPR pair, or Bell pair, is one of the four states,

$$|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B, \text{ and } |1\rangle_A|0\rangle_B \pm |0\rangle_A|1\rangle_B \,, \tag{9}$$

which are all maximally entangled and locally equivalent to one another. These are the simplest examples of entangled states, and their preparation via SPDC has been the mainstay of entangled state preparation for quantum optical processing [**bib:Kim01**]. In some applications, it may be desired to have the EPR pairs conditionally prepared, *i.e.* successfully prepared only under certain measurement outcomes of auxiliary modes. Because the EPR qubits are not measured directly, they can be used subsequently. Several theoretical approaches have been proposed for this purpose [**bib:Pittman03**, **bib:Sliwa03**, **bib:Walther07**], and demonstrated [**bib:Wagenknecht10**, **bib:Barz10**].

### *6.3. Greenberger-Horne-Zeilinger (GHZ) states*

GHZ states form a class of entangled quantum states on multiple subsystems with at least three parties [**bib:GHZ89**]. For qubit encodings with $n$ subsystems, a GHZ state is of the form

$$|\Psi_n^{(\mathrm{GHZ})}\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}} \,. \tag{10}$$

These states are also non-local, and have been used extensively in experimental test for non-locality [**bib:JW00**, **bib:Zhang15**]. This has been a subject matter covered in detail by another review [**bib:JW12**]. To date, six- [**bib:Lu06**, **bib:Zhang15**], eight- [**bib:Huang11**, **bib:Yao12**], and ten-photons [**bib:WangChen16**, **bib:Chen17**] GHZ states have been produced.

The GHZ state is also known as the NOON state, because it is written as

$$|\psi_n^{(\mathrm{NOON})}\rangle = \frac{1}{\sqrt{2}}(|n,0\rangle + |0,n\rangle) \,, \tag{11}$$

in the second quantization representation. This notation is commonly used in quantum metrological applications.

### *6.4. Cluster states*

Cluster states form another class of multiparty entangled states, and were conceived in the context of arrays of qubits with an Ising-type interaction [**bib:Briegel01**]. These states can be represented as a graph, in which vertices are qubits initialized into the superposition state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, with CPHASE operation applied between edges, as shown in Fig. 2a. For this reason, such states are also referred to as graph states. The CPHASE operations generate entanglement between the qubits, and because they commute, are independent of ordering.

Cluster states are a resource state for a model of quantum computation known as measurement-based quantum computation (MBQC). Here, having such a state as a resource enables universal quantum computation using only single-qubit measurements [**bib:Raussendorf03**]. In fact, only (X,Y)-plane measurements are needed [**bib:Mantri17**]. Therefore, the preparation of such states is highly valuable, generating much interest in their efficient preparation.

Unfortunately, implementing CPHASE gates using linear optics is complicated and highly non-deterministic. A major improvement upon this is to use fusion gates-rotated polarising beamsplitters, which implement projections onto the Bell states. These operations fuse smaller cluster states, represented using polarisation encoding, into larger ones, consuming one (type-I fusion) or two (type-II fusion) photons in the process. These operations are shown in Fig. 2b. Although these operations are non-deterministic with a success probability of $1/2$, they require only a single beamsplitter, already a major improvement over directly implementing CPHASE gates. Furthermore, unlike CPHASE gates, fusion operations require only high Hong-Ou-Mandel visibility, rather than the Mach-Zehnder stability required within existing CPHASE gate implementations, a major experimental simplification.

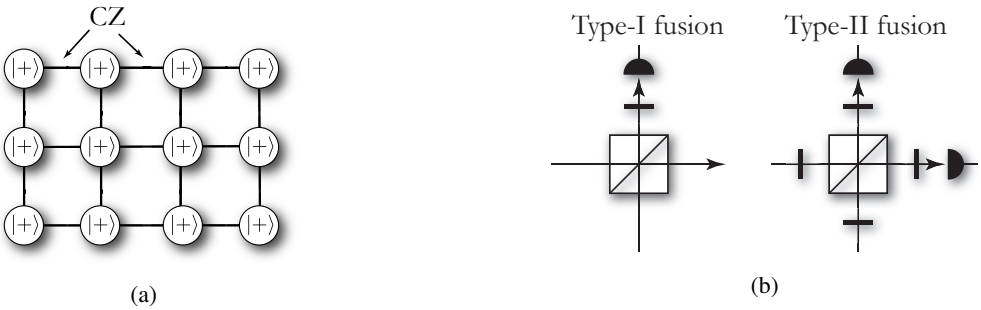



Fig. 2: (a) The representation of cluster states as a graph. Vertices represent qubits initialised into the $|+\rangle$ state, while edges represent the application on CPHASE gates, the ordering of which is irrelevant. (b) Fusion gates for joining smaller cluster states into larger ones. Both require only a single polarising beamsplitter, and waveplates. The type-I and -II fusion gates consume 1 or 2 qubits (photons) respectively, creating an edge between the remaining graphs. The type-I gate consumes one fewer photon, but requires number-resolved detection on the detected mode. The type-II gate requires only on/off photodetection, but consumes an additional photon. Thus, the type-I gate can be employed to fuse two Bell pairs into a 3-qubit cluster state, whereas the type-II gate will only grow clusters when beginning with at least 3 qubits per cluster.

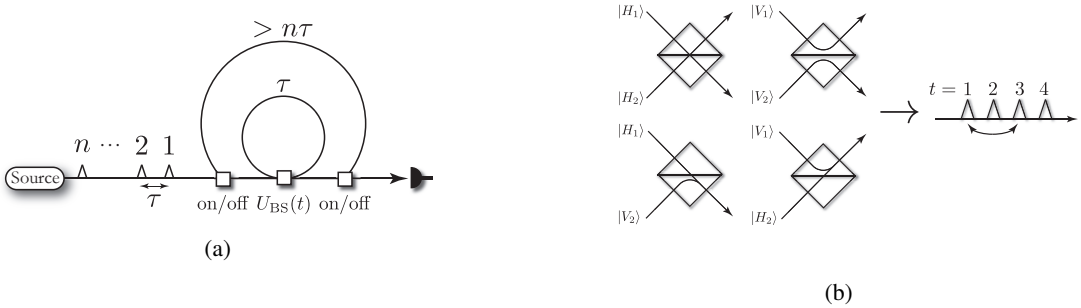



Fig. 3: (a) A fibre-loop architecture for implementing arbitrary linear optics operations upon a time-bin-encoded pulse-train. (b) Mapping between two polarisation-encoded qubits undergoing a polarising beamsplitter (PBS) operation, and its equivalent representation using 4 time-bins in a pulse-train. The PBS completely reflects (transmits) the vertical (horizontal) polarisations. The evolution of the four logical basis states, and their respective outputs, are shown explicitly. Writing out this PBS transformation in matrix form yields a permutation. Taking this permutation and relabelling the modes, we obtain the time-bin transformation shown underneath – a simple swap of two of the four time-bins.

Although these gates are non-deterministic and consume qubits, strategies have been described for efficiently preparing arbitrarily large cluster states of arbitrary topology, and using far fewer optical elements than by directly employing CPHASE gates [**bib:Nielsen04**, **bib:BrowneRudolph05**, **bib:Gimeno-Segovia15**, **bib:Pant17**]. Experimentally, small photonic cluster states have been demonstrated using both SPDC [**bib:Walther05a**, **bib:Lu06**, **bib:Prevedel07**, **bib:Tokunaga08**] and quantum dot sources [**bib:Schwartz16**]. To this end, continuous variable cluster states have fared better as large cluster states containing more than 10,000 entangled modes are possible [**bib:Yokoyama13**], with the caveat that it is difficult to address modes individually for processing.

## 7. Time-bin loop-based architecture for linear optical networks

Using time-bin encoding of optical qubits, the obvious question is how to perform operations upon them. In [**bib:Motes14**], a dual-loop architecture was presented for implementing arbitrary passive linear-optics on photonic pulse-trains with time-bin separation $\tau$, shown in Fig. 3a. The inner loop has length exactly $\tau$, while the outer one has length $> n\tau$ ($n$ is the number of optical modes). The architecture is controlled via three dynamically controlled beamsplitters. The first and last need only be on/off switches, whose sole purpose is to couple in the prepared pulse-train, keep it within the outer loop for the required duration, and then couple out of the outer loop, yielding the transformed pulse-train. The central beamsplitter must be able to implement arbitrary classically-controlled beamsplitter operations.

The architecture is frugal in its use of optical components, requiring only three dynamic beamsplitters, and several lengths of fibre. The beauty of this architecture is that the experimental requirements do not increase with the number

of optical modes. The only parameter that scales with the number of optical modes is the outer loop, which must be at least long enough to house the entire time-bin-encoded pulse-train. Note, however, that the central beamsplitter must be controllable at sub-$\tau$ time-scales, so as to enable each temporal mode to be addressed individually, which is technically challenging.

The workings of the scheme can be thought of as follows: the inner loop allows arbitrary beamsplitter operations between neighbouring time-bins; the outer loop does nothing interferometric, but rather enables the pulse-train to undergo as many applications of the inner loops as necessary. It then follows that this scheme is universal for linear optics, as a sufficient number of beamsplitter operations between neighbouring modes enables universal decompositions, using for example, the Reck *et al.* decomposition described in Section 4.

As a simple example of how such time-bin encoding maps to other encodings, in Fig. 3b we show the isomorphism between the polarising beamsplitter operation and a pairwise temporal beamsplitter operation. This implies a direct mapping for implementing cluster state preparation within the time-bin scheme.

The above description applies to passive linear optics, which is sufficient for protocols such as BosonSampling, but insufficient for universal optical quantum computation, which requires the addition of ancillary states, and measurement with fast-feedforward. To address this, it was shown in [**Rohde15**] that by dynamically preparing ancillary pulse-trains (from the already-existing source), classically controlled by time-resolved measurements at the output, and changing the switching sequence, we can effectively couple in and out arbitrary subsets of the optical modes, enabling partial measurements to be implemented.

## 8. Photodetection

Broadly speaking, there are two main classes of photodetectors: non-photon-number-resolving (also referred to as bucket, or on/off) detectors, and photon-number-resolving (PNR) detectors. As the names suggest, non-PNR detectors only detect the presence or absence of photons in an incident beam, while PNR detectors are able to measure its number of photons. The outcomes of a PNR detector are described by the measurement projectors,

$$\hat{\Pi}_n = |n\rangle\langle n|, \; n = 0, 1, \dots \, , \tag{12}$$

while those of the non-photon-number-resolving detectors are given by

$$\hat{\Pi}_{\text{off}} = \hat{\Pi}_0, \text{ and } \hat{\Pi}_{\text{on}} = \hat{I} - \hat{\Pi}_{\text{on}} \, . \tag{13}$$

Detailed reviews have been written about these detectors [**bib:Hadfield09**, **bib:Eisaman11**], so we shall only outline a few important examples.

A common example of a non-PNR detector is the avalanche photodiode (APD). These devices are made up of semiconductor material, usually silicon, which generate an electron that quickly generates a cascade of electrons. This avalanche of electrons generate a current that can be measured. APDs are affordable, offer low dark count rates with reasonable efficiency, and can be made to operate in a broad spectrum of wavelengths. Superconducting nanowire single-photon detector (SNSPD) is another type of non-PNR detector. This detector operates in its superconducting phase just below the critical density, and it phase changes back to normal when a photon is absorbed. This causes a spike in current around it, which, when detected, would indicate the absorption of the photon.

PNR detectors are a wonderful addition to the linear optical toolbox. A notable example is the superconducting transition edge sensor (TES) which has an extremely high quantum efficiency. The principle it operates on is very similar to the SNSPD, but with a much higher sensitivity that allows it to detect the energy of single photons. The visible light photon counter (VLPC) is another kind of PNR detector. The way VLPC works is in principle very similar to the APD, but with an additional layer of silicon that is lightly doped with arsenic (As). Owing to the presence of the As, a single photon absorption event always create an electrical signal that is always of the same magnitude. Thus, the output electrical signal is just proportional to the number of detected photons. Last, PNR detectors can be created by connecting many non-PNR detectors in parallel to one another, and summing the signals at the output. For instance, like in the theoretical proposal of [**bib:Sperling12**]. Such an approach has been successfully demonstrated with SNSPD [**bib:Divochiy08**], and APDs [**bib:Kalashnikov12**, **bib:Chrapkiewicz14**, **bib:Heilmanndc15**].

## 9. Applications for linear optics interferometry

### *9.1. Linear optical quantum computation (LOQC)*

The advancements in linear optics have opened up avenues for implementation. One of the key requirements is nonlinear couplings between the different optical modes. Photons do not naturally interact with one another so some careful engineering is needed to achieve this coupling. Methods used include measurements and feedforwarding [**bib:KLM01**], and photon-atom interactions [**bib:Brod16**]. The former requires non-deterministic operations, which succeed only part of the time and have to be repeated. This can be challenging given the limited resources to begin with. Comprehensive reviews have been written previously to cover this topic [**bib:JW12**, **bib:Kok05**], hence we will focus on recent advances.

Integrated photonic circuits has greatly improved the feasibility of LOQC. Their small size and interferometric stability enable the requisite quantum interference to happen in certain LOQC settings. Programmable circuits that are reusable have also emerged [**bib:Metcalf14**, **bib:Carolan15**]. This saves resources and lead time for producing new circuits. Combining these chips with existing higher-efficiency sources and detectors will expand their capabilities. Loss can be mitigated by moving all components, *i.e.* sources and detectors, onto the same chip as the linear optical circuit [**bib:Sprengers11**, **bib:Silverstone14**]. What remains is to have fast feedforward also on chip. This might pose the greatest challenge yet for universal LOQC. The bottleneck is in the speed of modulation in the feedforward circuitry; only a handful of experiments have been able to implement adaptive feedforward for the purposes of LOQC [**bib:Prevedel07**, **bib:Xiao-Song12**, **bib:Mikova12**, **bib:Zhao14**].

Better single-photon sources (see Section 6.1) are part of the solution. Improvement in control of their degrees of freedom have also led to more efficient designs of circuits [**bib:Zhou11**, **bib:Lanyon09**] that enabled the optical implementation of quantum teleportation of the state of a single photon [**bib:Wang15**]. In this way, three-qubit [**bib:Lanyon09**, **bib:Micuda13**, **bib:Patel16**] and four-qubit [**bib:Starek16**] gates have also been implemented using LOQC.

Cross-Kerr nonlinearity is a type of nonlinearity implemented through atom-photon interactions. It has been thought for some time that fundamental noise limits in atom-photon interactions will prevent any help for LOQC [**bib:Shapiro06**, **bib:Shapiro07**, **bib:Gea-Banacloche10**]. However, this belief has been countered by the construction of a CPHASE gate using photons that undergo cross-Kerr interaction [**bib:Brod16**]. Regardless of who is right in this debate, stronger Kerr nonlinearities have been achieved in the last five years [**bib:Hoi13**, **bib:Venkataraman13**, **bib:Feizpour15**, **bib:Beck16**], and this avenue remains a tantalizing possibility for deterministic quantum gates.

Although there has been tremendous progress in linear optics, it seems likely that an efficient, and fault-tolerant universal quantum computer will require a hybrid system. Nonetheless, linear optics remains fascinating platform for applications and foundation work.

### *9.2. Boson-sampling*

The difficulty in producing nonlinear operations required for universal LOQC led researchers to seek out alternative ways for demonstrating its power in the near term. BOSONSAMPLING is the result of such an effort. It is a restricted model of non-universal quantum computation [**bib:Aaronson11**] that constitutes sampling the photocounts from the probability distribution of identical bosons scattered by a passive linear optical interferometer. While not universal, the BOSONSAMPLING scheme is strongly believed to implement a classically hard task. Consider such a circuit of $m$ input (and output) modes that is injected with $n$ indistinguishable single photons such that $m \sim O(n^2)$. Then, the boson-sampling task consists of generating a sample from the probability distribution of single-photon measurements at the output of the circuit. The probability of detecting $s_j$ photons at the $j$th output mode is

$$p(s_1, \ldots, s_m) = \frac{|\mathrm{Per}(U_S)|^2}{s_1! \ldots s_n!} , \tag{14}$$

where Per() denotes the permanent of a matrix, $S = \{s_1, \ldots, s_m\}$ denotes an output photon-number configuration, and $U_S$ is obtained from the interferometer unitary $U$ by keeping its first $n$ columns and repeating its $j$th row $s_j$ times. The appearance of the permanent, which is #P-hard in general (a complexity class even harder than NP-hard), in this statistics contributes to the hardness of the boson-sampling problem. Note that the number of configurations $|S| = \binom{n+m-1}{n}$ in the output superposition scales exponentially with $m$. For this reason, the boson sampler does not let us *calculate* matrix permanents, as this would require knowing individual amplitudes with high precision, which would require an

exponential number of samples. Rather, the boson sampler samples across a distribution of permanents without actually revealing any of them to the experimenter. Nonetheless, this is a classically intractable problem. It is also known that boson-sampling is as hard as stimulating the short time evolution of a certain Hamiltonian[**bib:Peropadre17**].

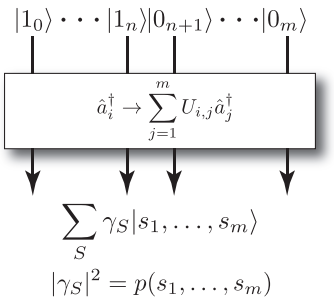



Fig. 4: The Boson-Sampling model. A string of n single photons is prepared in m optical modes. They are evolved via a passive interferometer $U$. Finally the photon-statistics are sampled from the distribution $p(s_1, \ldots, s_m)$.

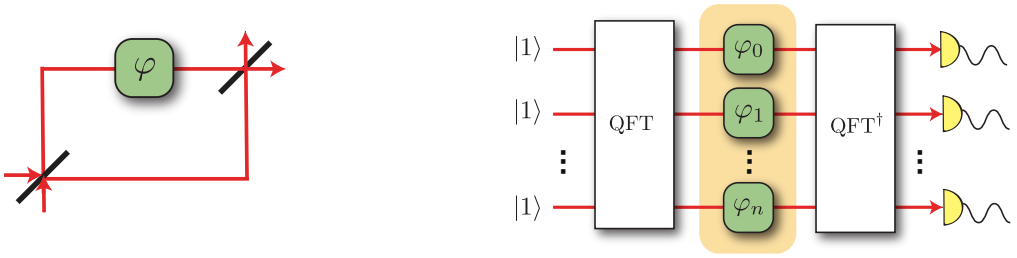
Owing to the simplicity of BosonSampling and its overarching implications for computer science, multiple experiments were reported shortly after its theoretical conception [**bib:Tillmann13**, **bib:Spring13**, **bib:Broome13**, **bib:Crespi13**]. A recent experiment showed a bosonsampling machine beating an early computer [**bib:WangHe16**]. BosonSampling has piqued so much interest, that a complete discussion would make up its own review, so we shall only outline some main developments here. One variant, known as scattershot bosonsampling, proposes using pumped SPDC heralded photon sources to increase the rate of generating input photons [**bib:Lund14**, **bib:Bentivegna15**], by inputting an SPDC source into *every* mode rather than just the first $n$, thereby boosting the probability of preparing the desired $n$ photons. Others varied the source input to cat-states [**bib:Rohde15**] and thermal states [**bib:Tamma14˙thermal**] . An exciting modification allows the determination of molecular vibronic spectra [**bib:Huh15**], a task that goes beyond demonstrating a computationally hard task.

Certifying that a bosonsampling task has been correctly performed is non-trivial. Some efforts look into discriminating between a valid bosonsampling and a uniform distributions [**bib:Gogolin13**, **bib:Aaronson13**]. Another shows how to discriminate data arising from either indistinguishable or distinguishable photons [**bib:Spagnolo14**, **bib:Carolan14**]. More general benchmark standards have also been instituted [**bib:Walschaeprs16**]. Another approach to verify that the interferometer is behaving as expected is to make use of suppression laws [**bib:Tichy14**] together with fully reconfigurable optical circuits. When the circuits are tuned to implement certain unitary matrices, specific input and output combinations are suppressed [**bib:Crespi16**]. Last but not least, a bound for the transition amplitudes for bosonsampling indicates that an approximation algorithm for the permanent is possible [**bib:Yung16**]. Such an algorithm can help with verifying the sampling distribution, but their proof does not construct the algorithm needed for this to happen.

As experimental imperfections threaten the scalability of bosonsampling, there have been efforts to look into its error tolerance [**bib:Rohde12˙tol**], fault-tolerance [**bib:Leverrier15**], and experimental artefacts [**bib:Shchesnobich14**, **bib:Tamma16**]. Some works have resulted in interesting connections to exotic mathematical entities like immanants [**bib:Tan2013**, **bib:deGuise2014**] and the multi-dimensional permanent [**bib:Tichy15**]. A time-bin implementation of bosonsampling [**bib:Motes14**] seems particularly attractive in terms of robustness [**bib:Motes15˙timebin**].

### *9.3. Quantum metrology*

An archetypal task for quantum metrology is the following: Given a Mach-Zedner interferometer, with an unknown phase shift of magnitude $\varphi$ inserted in one of the two paths (see Fig. 5a), can one deduce $\varphi$ via a judicious use of quantum states and measurements with a higher sensitivity than that of a completely classical interferometer? Indeed, one can, and the standard deviation, $\Delta\varphi$, after $N$ trials using quantum estimation is $\Delta\varphi = 1/N$, which gets a factor of $\sqrt{N}$ improvement over classical phase estimation. As this sensitivity is also a fundamental limit arising from Heisenberg's uncertainty principle, *i.e.* we cannot measure definitively the phase, it is known as the Heisenberg limit. Most famously, NOON states achieve this limit using $N$ photons in a single trial. Many reviews have been written for quantum metrology and Heisenberg-limited quantum phase estimation [**bib:Giovannetti04**, **bib:Dowling08**,




(a) (b)

Fig. 5: (a) A schematic diagram of the Mach-Zehnder interferometer comprising of two 50/50 beamsplitters with a phase shift $\varphi$ in one of its two paths. (b) Architecture of the quantum Fourier transform interferometer for metrology using single-photon states. QFT: Quantum Fourier transform circuit, and $\varphi_k = (k-1)\varphi$. Single photons are injected into the input modes on the left-hand-side, and a $N$-fold coincidence measurement is conducted at the output on the right-hand-side.

**bib:Giovannetti11**] so we will not dwell on the history of this application. Instead, we will discuss new paradigms for quantum metrology that have been made possible by the aforementioned advancements in linear optics.

As discussed in Section 9.2, the resources needed for Boson-sampling is readily available, but executes a task that is believed to be hard classically. Surprisingly, an entanglement between a large number of path labels is possible with single photons in a passive linear optical device. Motes *et al.* harnessed this so-called number-path entanglement for quantum metrology without the use of entangled states [**bib:Motes15˙LOQM**]. Here, the phase shift to be estimated, $\varphi$, manifests itself as a linear phase gradient across $N$ modes (See Fig. 5b). By straddling these modes among a quantum Fourier transform and its conjugate operation, it is possible to achieve $\Delta\varphi = O(N^{-3/2})$ using a coincidence measurement with just a string of $N$ single photons, for up to at least $N = 25$ modes.

Quantum multi-parameter estimation is the extension of quantum phase estimation to sense multiple phases in a multi-arm interferometer [**bib:Szczykulska16**]. Theoretical work has shown that it is favorable to probe all phases simultaneously rather than individually [**bib:Baumgratz16**, **bib:Ciampini16**], and it remains to realize existing proposals for implementation [**bib:Spagnolo12**]. Nonetheless, for a Heisenberg-limited sensitivity, entangled states and joint measurements across modes are likely to be required.

## 10. Conclusion

Linear optical interferometry has become a leading contender for the implementation of quantum information processing protocols. The preparation, manipulation and measurement of photonic quantum information has become mainstream and widely employed, with impressive experimental accuracies.

We have discussed the various ways in which quantum information can be represented in photonics, how they can be manipulated and detected, and some of their leading applications.

Although there are countless physical architectures for the implementation of quantum information processing, and it is far from certain which will win ‘the quantum race for supremacy, optics will always find a home as the only contender for applications involving quantum communication. For this reason, the future of linear optics interferometry is a bright one, which will find inevitable applicability in the future quantum world.

## Acknowledgments

P.P.R. is funded by an ARC Future Fellowship (project FT160100397). This research was supported in part by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01. ST acknowldeges support from the Air Force Office of Scientific Research under AOARD grant FA2386-15-1-4082.

paper