An introduction to boson-sampling

In no particular order,[1] Peter P. Rohde,[1,*] Bryan Gard, Keith R. Motes, and Jonathan P. Dowling

[1] *Centre for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University, Sydney NSW 2113, Australia*

(Dated: May 26, 2014)

I. INTRODUCTION (BRYAN)

A. Motivation for linear optics quantum computing and boson-sampling

To-date, many different physical implementations and models for quantum computing have been proposed. These implementations include atom and ion trap quantum computing, superconducting qubits, nuclear magnetic resonance, quantum dots, nuclear spin, and optical quantum computing. When describing an implementation, one can use various models of computation. These include the gate model, cluster (or graph) states [1, 2], topological, adiabatic, quantum random walks [3], quantum Turing machines, permutational, and the one-clean qubit models (**PLEASE ADD REFERENCES FOR EACH OF THESE**). The most familiar and intuitive model is the gate model as it is most analogous to the classical circuit model of computation. We use this gate model in order describe linear optics quantum computing (LOQC) and eventually a special purpose subset, boson-sampling.

As stated, there exist many choices of implementations and computational models. Certain pairs of choices certainly have natural synergy but a fair question to ask is, which choice is likely to yield the first implemented quantum computer? The answer is likely not just one choice, but a composite of different choices for the various required components of a quantum computer. For this discussion we focus on LOQC for its main allure of 'simple' implementation.

There is a many year history in the physics community of investigations into the use of linear interferometers, particularly linear optics interferometers, as a type of quantum information processor. However in most of this early research the conclusion was that a linear optics interferometer (alone) could not be used to make a universal quantum computer, regardless of the input states. For example in 1994, one year before Shor's discovery of the now-famous quantum factoring algorithm, there appeared a paper by Černý that proposed to use a linear interferometer to solve **NP**-complete problems in polynomial time, but the scheme suffered from an exponential overhead in energy [4]. Along the same lines, in 1996, Clauser & Dowling showed that a linear optics Talbot interferometer could be used to factor integers in polynomial time but with either an exponential blow up in energy or physical size [5]. Then, also in 1996, Cerf, Adami & Kwiat showed how to construct a programmable linear optics interferometer that could perform any universal logic gate with single photon inputs but this scheme too suffered an exponential overhead in spatial dimension. In 2002 Bartlett *et al.* showed that even with quadratic non-linearities any interferometer that processes only Gaussian state inputs can be efficiently simulated classically, a continuous variable analog of the Gottesman-Knill theorem for discrete variables in the ordinary circuit quantum computation model [6].

This litany of 'no-go' theorems led to the widespread belief that linear interferometry alone could not provide a path to universal quantum computation and that, as a corollary, all linear optics interferometers are efficiently simulateable on a classical computer. For completeness we will introduce the LOQC approach of Knill, Laflamme & Milburn (KLM) [7, 8] in the following section, but the remaining focus of this chapter is instead on boson-sampling. That is because the KLM scheme set of universal gates requires intermediate measurements on ancilla photons with a feed-forward mechanism that imparts a type of effective Kerr nonlinearity on the system [9]. We explicitly only discuss linear optics implementations due to the fact that nonlinear Kerr media exhibit very poor efficiency for our purposes [10], and present-day Kerr mediums exhibit only very weak non-linearities.

Hence it came as a surprise to many of us in the quantum optics community when Aaronson & Arkhipov (AA) argued that, in general, the operation of a passive linear optics interferometer with Fock state inputs can very likely not be simulated by a classical computer [11]. In particular if one considers a sampling of the outputs, utilizing photon-number discriminating detectors, such a boson-sampling device cannot be predicted with a classical computer without an exponential overhead. This has become known in the computational complexity community as the boson-sampling problem.

The conclusion that computing the output of a linear optics interferometer with Fock state inputs is likely a computationally hard problem was independently reached by Gard *et al.*, in the context of trying to compute the related problem of multi-photon coincidence counts in the output of a linear optics interferometer implementation of a quantum random walk with multi-photon walkers [12]. In follow up papers, Gard *et al.* [13], as well as Motes *et al.* [14], argued from a physical (as opposed to computational complexity) point of view that this inability to simulate such interferometers arose from

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

two necessary requirements: (1) The photons 'interact' at the beamsplitters via a Hong-Ou-Mandel effect that gives rise to an exponentially large Hilbert space in the number-path degrees of freedom that rules out a brute force simulation of the interferometer; and (2) That the simulation of the interferometer is also tied to the need to compute the permanent of a large matrix with complex entries, a problem known to be in the complexity class **#P**-complete, that is thought to be an intractable problem not only classically but even on a universal quantum computer [15]. The reason for the second requirement is that, due to the Gottesman-Knill theorem, it is known that there are examples of quantum circuits with gates all in the Clifford algebra class that generate exponentially large amounts of qubit entanglement but are nevertheless and surprisingly classically simulateable. Sometimes there are shortcuts through the exponential Hilbert space and so by tying the simulation to the problem of the permanent solving we make is very unlikely that any such shortcuts exist. For example, the equivalent sampling problem with fermions rather than bosons is known to be classically easy to simulate, as the problem relates to matrix determinants rather than permanents, which are known to be in the complexity class **P** (**CITATION FOR FERMION SAMPLING**).

Since the first appearance of the AA paper in 2010 there has been an explosion of research into the field of boson-sampling. As we will discuss below there have been a number of experiments utilizing three photons from spontaneous parametric down conversion (SPDC) sources [16–21] (although these experiments are under debate as not all three photons were heralded single photons [22]). The experimental work has continued in parallel to a number of theoretical developments considering the effects of loss, noise, decoherence, non-Fock inputs, scalability of SPDC sources, ion-trap implementations, and so forth [14, 23–26]. We will discuss and summarize these results and more in the sections below.

So then there come the questions – why is boson-sampling getting so much attention and what is it good for? The answer is that boson-sampling is a new example of a computationally complex mathematical problem that cannot be simulated on a classical computer, but which significantly reduces experimental requirements compared to universal quantum computing schemes. The appeal is that this is the first interesting example of a non-trivial quantum computing paradigm to be proposed in some while and the true scope and power of such machines is not yet fully understood.

Then the question arises; what is a boson-sampling machine good for other than boson-sampling? The boson-sampling problem itself, other than being a computational curiosity, has no known practical applications or 'killer apps' such as we find with the Shor factoring algorithm. But prior to 1994, when the Shor algorithm was invented, there the same question was asked; 'What is a quantum computer good for?' Feynman's work in the 1980s had hypothesized that an ordinary quantum computer could be used to carry out certain physics simulations without the exponential overhead required to do so on a classical computer but this hypothesis was not proved until Lloyd's work in 1996 [27, 28]. The first non-trivial application for an ordinary quantum computer was the Deutsch-Jozsa algorithm discovered in 1992, but this problem also had no practical applications [29]. So in many ways the boson-sampling quantum computer is like the ordinary circuit-based quantum computer pre-Shor. We have one example of an exponentially hard mathematical problem that the machine can solve but not one that is known to be useful for anything. The lure is that perhaps the linear optics interferometers, now that this hidden computational power has been uncovered, are good for something else besides the boson-sampling problem. This potential is what has captured the imagination of researchers in the field. As we arrive at our boson-sampling scheme by way of LOQC, we still maintain several of its benefits. These include no requirements for excessive cooling of the optical elements, long coherence times compared to the basic gate operations, and relatively simple to understand noise sources.

One final caveat; In almost all papers on the topic of boson-sampling the interferometer is described as a linear device with non-interacting bosons: photons in this case. However the Hong-Ou-Mandel effect (followed by a projective measurement) imparts an effective nonlinearity and hence an effective interaction at each beamsplitter. The presence or absence of a photon in one input mode radically changes the output state that a second photon in the other input mode will find itself in. This 'interaction' between indistinguishable particles, known as the exchange interaction, arises simply from the demand that the multi-particle wavefunction be properly symmetrized. While not a force in the usual sense it can give rise to quite noticeable effects. For example, the bound state of the neutral hydrogen molecule, the most common molecule in our Universe, arises from just such an exchange interaction. It is therefore a misnomer to describe these interferometers as linear devices with non-interacting bosons. The exchange interaction is just as real as tagging on an additional term in a Hamiltonian and if one adds postselection in the number basis to the mix this imparts an effective Kerr-like nonlinearity between the bosons to boot.

B. Introduction to linear optics quantum computing

We begin by defining some terminology and notation. The smallest amount of data that we can deal with in quantum computing, analogous to the classical computing bit, is the quantum 'qubit'. A qubit is defined as

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \, , \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \tag{1}$$

FIG. 1: Bloch sphere showing a way to visualize the rotations that the Pauli matrices apply to a state. Pure states lie on the sphere while mixed states are contained within the sphere.

for a zero and one qubit, respectively. One of the advantages of quantum computing over classical computing is, of course, the ability to use quantum effects. One of these effects is the ability to have a qubit in a superposition of zero and one, that is, in general

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,, \tag{2}$$

and with a specific choice for $\theta = \frac{\pi}{2}$ and $\phi = 0$ we can simplify this to

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,. \tag{3}$$

This superposition represents that our state, once measured, has a 1/2 probability of being in state zero and a 1/2 probability of being in state one. These superpositions can also be depicted on the Bloch sphere as shown in Fig. 1. One may initially want to view these superpositions as being in both states at once and while this idea is true, it is somewhat as once we measure this superposition state, it always takes either the value of zero or one. Before we measured the state however, we of course do not have any information about the state. It is the act of our measurement that forces the state to 'choose' a zero or one. Thus there is an attribute of these superposition states to contain some 'hidden' quantum information.

Also analogous to classical computing, we need a set of logic gates to perform operations on our quantum states [10]. Some of the most common gates are defined as

$$\begin{aligned}
\text{Controlled-NOT (CNOT):} &\quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \\
\text{Hadamard (H):} &\quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\
\text{Pauli-X } (\sigma_x)\text{:} &\quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
\text{Pauli-Y } (\sigma_y)\text{:} &\quad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\
\text{Pauli-Z } (\sigma_z)\text{:} &\quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\
\text{Phase:} &\quad \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \\
\frac{\pi}{8}\text{:} &\quad \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.
\end{aligned} \tag{4}$$

The first of these, the CNOT gate, is a maximally entangling two-qubit gate, which is the quantum equivalent of the classical XOR gate, whilst the latter gates are single qubit gates, which implement rotations on the Bloch sphere. The single qubit gates may be trivially implemented using waveplates in quantum optics, whilst the CNOT gate is far more challenging, requiring an effective Kerr non-linearity.

These gates form one choice of a universal gate set. Any choice for a universal gate set can approximate any other gate set to arbitrary precision. In broad terms there are three classes of problems to which quantum computation outperforms classical computing. These classes include algorithms that make use of the quantum Fourier transform such as Shor's algorithm for factoring and discrete logarithms. For $N = 2^n$ numbers, a classical fast Fourier transform would require $N \log N \approx 2^n n$ steps while a quantum computer could do this same transform in only $\log^2 N \approx n^2$ steps [10].

Another class is quantum search algorithms which make use of the superposition quality to, in effect, speed search times. Discovered by Grover (**CITATION PLEASE**), a search of an unstructured database of N elements, one wants to find an element of that search space satisfying a specific property. On a classical computer this search would require $O(N)$ operations, whilst a quantum search could accomplish this in $O(\sqrt{N})$ operations.

The third type is simply quantum simulation, where one attempts to simulate a quantum system, thus requiring a quantum computer to simulate it efficiently. For a classical computer to simulate a quantum system with n distinct components, it would require c^n bits of memory, where c is a constant depending on the choice of the system. A quantum computer would only require $O(n)$ bits of memory however, where the proportionality constant depends on the choice of the physical system being simulated. We thus reduce an exponential use of resources to only a linear use of resources! For further discussion on quantum optics and quantum information processes see [30–32].

In computational terms, a computation is considered 'efficient' if the required resources are sub-exponential, such as polynomial. With only linear optical elements such as beamsplitters, phase-shifters, photo-detectors, and feedback from photodetector outputs, it can be shown that one can achieve this efficiency. This efficiency can be achieved by three requirements.

1. Non-deterministic quantum computation.

2. Probability of success of quantum gates must approach unity.

3. Ability to use quantum coding to accurately achieve encoded qubits.

(I DON'T UNDERSTAND WHAT THESE POINTS MEAN. COULD YOU REVISE THIS?)

Discussion of linear optics quantum gate efficiency, such as beamsplitters and the controlled phase gate are

discussed in Ref. [33] with the description of entanglement power and entanglement efficiency.

C. Linear optics quantum computing

In general, to fully achieve a true quantum computer we require a way to prepare quantum states, perform a universal gate set on the qubits, and measure the output state.

In order to generate a quantum state we use a single photon source which adds a photon to the vacuum state $|0\rangle$ and thus sets any vacuum mode to the $|1\rangle$ state. This process is non-deterministic but is sufficient for quantum computing.

The simplest optical elements are phase-shifters and beamsplitters. These elements are used to act as gate operations on our prepared states. Since both of these transformations are unitary we can write each of these elements in terms of their unitary matrix. A phase-shifter's unitary matrix is simply $P_\theta = e^{i\theta}$ while the unitary matrix for a beamsplitter is given by

$$B_{\theta,\phi} = \begin{pmatrix} \cos\theta & -e^{i\phi}\sin\theta \\ e^{-i\phi}\sin\theta & \cos\theta \end{pmatrix}, \tag{5}$$

in the basis of optical modes.

We can also represent both of these unitary matrices in terms of the familiar Pauli matrices, that is, a phase-shifter implements $P_\theta = \exp(-i\sigma_z\theta/2)$ and a beamsplitter implements $B_\theta = \exp(-i\sigma_y\theta)$ (**WE NEED TO EXPLAIN THE BASIS HERE. BOTH OF THESE MATRICES ARE TWO-BY-TWO BUT ONE OF THEM IS A SINGLE MODE OPERATION WHILST THE OTHER IS A TWO-MODE OPERATION. EXPLAIN THIS.**), where we omit any global phase and set $\phi = 0$. Since these Pauli matrices are simply rotations on the Bloch sphere, this shows that all one qubit rotations can be realized this way and thus can be implemented with linear optics elements.

In order to measure the state, we use photodetectors which destructively determine if a mode contains a photon or not. For states with more than one photon then, we need a photon counting detector, which can be implemented by using a series of beamsplitters and photodetectors. The beamsplitters act so that the photons are spread evenly over N modes, with each mode containing a photo-detector. The probability of under counting given that the photon number is k is at most $k(k-1)/(2N)$ but for our purposes $k \leq 4$ [7]. This is referred to as multiplexed photodetection (**CITATION**). Another alternative is to use photon-number-resolving detectors.

In addition to these single qubit rotations we also require a nonlinear sign flip gate (NS) [7]. This gate implements the transformation

$$\text{NS} : \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle \rightarrow \alpha_0|0\rangle + \alpha_1|1\rangle - \alpha_2|2\rangle, \tag{6}$$

and is the basis of implementing the CNOT gate. This two qubit gate along with the previously discussed single qubit gates form the required universal gate set to perform quantum computing. One only needs a set of one- and two-qubit universal gates in order to construct general multi-qubit gates. Specifically we only require the Hadamard, phase, $\pi/8$ and CNOT gates [10].

Using just linear optics and photodetection, implementing the NS gate is non-deterministic, which implies that with multiple gates in our circuit, the success probability of the computation drops exponentially with the number of gates. To overcome this, another useful tool in LOQC is the use of quantum teleportation to increase the probability of success of non-deterministic gates [7]. In order to teleport the state $\alpha_0|0\rangle + \alpha_1|1\rangle$ of mode 1 to mode 3, we first couple the entangled ancilla state $|t_1\rangle_{23} = |01\rangle_{23} + |10\rangle_{23}$. We then measure modes 1 and 2 in the Bell basis $|01\rangle_{12} \pm |10\rangle_{12}, |00\rangle_{12} \pm |11\rangle_{12}$. When measuring these modes, we first determine the parity of the number of photons present. We then determine the sign in the Bell basis ($\pm$). The following shows all combinations of these measurements:

$$\text{Odd parity} \begin{cases} + \text{ means mode 3 is } \alpha_0|0\rangle_3 + \alpha_1|1\rangle_3 \\ - \text{ means mode 3 is } \alpha_0|0\rangle_3 - \alpha_1|1\rangle_3 \end{cases}$$

$$\text{Even parity} \begin{cases} + \text{ means mode 3 is } \alpha_1|0\rangle_3 + \alpha_0|1\rangle_3 \\ - \text{ means mode 3 is } \alpha_1|0\rangle_3 - \alpha_0|1\rangle_3 \end{cases}$$

(**IN THIS DESCRIPTION WHAT DO + AND - REFER TO?**) It is clear that the first possible outcome is what is desired. The state in mode 1 is successfully teleported to mode 3 without actually interacting with mode 3. The second outcome in odd parity is a simple phase-shift transformation away from our desired outcome as well. The remaining two outcomes are not desirable and are not easily transformed into our desired state with linear optics. Thus we can see that if only using linear optics we can successfully implement this teleportation with a probability of 1/2. However, a teleporter can be bootstrapped to progressively increase the success probability of the teleportation, allowing asymptotically high success probabilities to be achieved. With such a teleporter, 'gate teleportation' may be implemented, which allows non-deterministic gates, such as the CNOT gate, to be implemented with arbitrarily high success probability [7], enabling scalable quantum computation.

D. Why is linear optics quantum computing hard?

All of this may lead one to ask, if this scheme, using only linear elements is so simple, what's the hold up in implementing it? To implement this scheme we require a myriad of technicalities. These include synchronization of pulses, mode-matching, quickly controllable delay lines, tunable beamsplitters and phase-shifters, single-photon sources, and accurate, fast, single photon detectors. Most of this list is not terribly unrealistic to adhere to but current efficiencies of photodetectors are not at the point at which they may realistically implement the teleportation

and the more complex gate operations (two qubit gates). The feedback control of these detectors must also be extremely fast in order to select proper state preparation before photon loss becomes an issue.

As an example, if we investigate actual implementation of a teleported (i.e high success probability) CNOT gate, which requires many individual non-deterministic CNOT gates, one can attain a probability of success in implementing this entangling operation of 95% with approximately 300 successful CNOT gates which translates to an excessively large number ($> 10^4$) of optical elements [34]. Whilst this may seem daunting, recent approaches using cluster states have reduced experimental requirements by orders of magnitude [35, 36], but nonetheless the experimental requirements are substantial and still require challenging technologies such as fast-feedforward and dynamic control.

Without accurate implementation of these protocols we likely lose our claim to universality, but we still retain our ability to investigate some interesting problems. This realm of LOQC without fast feedback control or unrealistically accurate photodetectors lead us into boson-sampling.

II. THE BOSON-SAMPLING FORMALISM

Unlike full LOQC, which requires active elements, the boson-sampling model is strictly passive, requiring only single-photon sources, passive linear optics (i.e beam-splitters and phase-shifters), and photodetection. No quantum memory or feedforward is required.

We begin by preparing an input state comprising n single photons in m modes,

$$\begin{aligned} |\psi_{\text{in}}\rangle &= |1_1, \ldots, 1_n, 0_{n+1}, \ldots, 0_m\rangle \\ &= \hat{a}_1^\dagger \ldots \hat{a}_n^\dagger \, |0_1, \ldots, 0_m\rangle \,, \end{aligned} \tag{7}$$

where $\hat{a}_i^\dagger$ is the photon creation operator in the ith mode. It is assumed that the number of modes scales quadratically with the number of photons, $m = O(n^2)$. The input state is evolved via a passive linear optics network, which implements a unitary map on the creation operators,

$$\hat{U}\hat{a}_i^\dagger\hat{U}^\dagger = \sum_{j=1}^{m} U_{i,j}\hat{a}_j^\dagger, \tag{8}$$

where U is a unitary matrix characterizing the linear optics network. It was shown by Reck *et al.* [37] that any U may be efficiently decomposed into $O(m^2)$ optical elements. The output state is a superposition of the different configurations of how the n photons could have arrived in the output modes,

$$|\psi_{\text{out}}\rangle = \sum_S \gamma_S \, |n_1^{(S)}, \ldots, n_m^{(S)}\rangle \,, \tag{9}$$

where S is a configuration, $n_i^{(S)}$ is the number of photons in the ith mode associated with configuration S, and γ_S is the amplitude associated with configuration S. The probability of measuring configuration S is given by $P_S = |\gamma_S|^2$. The full model is illustrated in Fig. 2

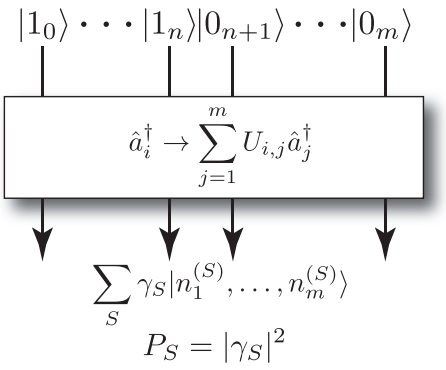

FIG. 2: The boson-sampling model. n single photons are prepared in m optical modes. These are evolved via a passive linear optics network $\hat{U}$. Finally the output statistics are sampled via coincidence photodetection. The experiment is repeated many times, reconstructing the output distribution P_S.

It was shown by Scheel [38] that the amplitudes γ_S are related to matrix permanents,

$$\gamma_S = \frac{\text{Per}(U_S)}{\sqrt{n_1^{(S)}! \ldots n_m^{(S)}!}}, \tag{10}$$

where U_S is an $n \times n$ sub-matrix of U, and $\text{Per}(U_S)$ is the permanent of U_S.

Let us examine this relationship with the permanent more closely. Consider Fig. 3. Here the first two modes have single photons, with the remaining modes in the vacuum state. Let us consider the amplitude of measuring one photon at output mode 2 and another at output mode 3. Then there are two ways in which this could occur. Either the first photon reaches mode 2 and the second mode 3, or vice versa, i.e the photons pass straight through, or swap. Therefore there are $2! = 2$ ways in which the photons could reach the outputs. Thus, this amplitude may be written as,

$$\begin{aligned} \gamma_{\{2,3\}} &= \underbrace{U_{1,2}U_{2,3}}_{\text{walkers don't swap}} + \underbrace{U_{1,3}U_{2,2}}_{\text{walkers swap}} \\ &= \text{Per}\begin{bmatrix} U_{1,2} & U_{2,2} \\ U_{1,3} & U_{2,3} \end{bmatrix}, \end{aligned} \tag{11}$$

which is a 2×2 matrix permanent.

As a slightly more complex example, consider the three photon case shown in Fig. 4. Now we see that there are $3! = 6$ ways in which the three photons could reach the outputs, and the associated amplitude is given by a 3×3

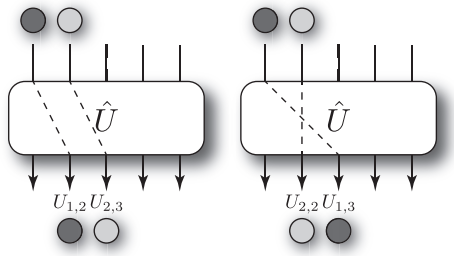

FIG. 3: Two-photon boson-sampling, where we wish to calculate the amplitude of measuring a photon at each of the output modes 2 and 3. There are two ways in which this may occur – either the photons pass straight through, or swap, yielding a sum of two paths.

matrix permanent,

$$\begin{aligned}\gamma_{\{1,2,3\}} &= U_{1,1}U_{2,2}U_{3,3} + U_{1,1}U_{3,2}U_{2,3} \\ &+ U_{2,1}U_{1,2}U_{3,3} + U_{2,1}U_{3,2}U_{1,3} \\ &+ U_{3,1}U_{1,2}U_{2,3} + U_{3,1}U_{2,2}U_{1,3} \\ &= \mathrm{Per}\begin{bmatrix} U_{1,1} & U_{2,1} & U_{3,1} \\ U_{1,2} & U_{2,2} & U_{3,2} \\ U_{1,3} & U_{2,3} & U_{3,3} \end{bmatrix}. \end{aligned} \tag{12}$$

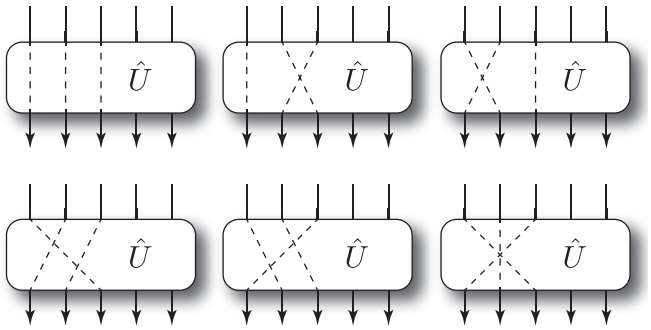

FIG. 4: Thee photon boson-sampling, where we wish to calculate the amplitude of measuring a photon at each of the output modes 1, 2 and 3. There are now $3! = 6$ possible routes for this to occur.

In general, with n photons, there will be $n!$ ways in which the photons could reach the outputs (assuming they all arrive at distinct outputs), and the associated amplitude will relate to an $n \times n$ matrix permanent. Calculating matrix permanents is known to be **#P**-complete, even harder than **NP**-complete, and the best known algorithm for calculating matrix permanents is by Ryser [15], requiring $O(2^n n^2)$ runtime. Thus, we can immediately see that if boson-sampling were to be classically simulated by calculating the matrix permanents, it would require exponential classical resources.

Because the number of modes scales quadratically with the number of photons, for large systems we are statistically guaranteed that all photons will arrive at different output modes. This implies that in this regime on/off (or 'bucket') detectors will suffice, and photon-number resolution is not necessary, a further experimental simplification compared to full-fledged LOQC.

The number of configurations in the output modes scales as,

$$|S| = \binom{n+m-1}{n}, \tag{13}$$

which is exponential is n. Thus, with an 'efficient' (i.e sub-exponential) number of trials, we are unlikely to sample from a given configuration more than once. This implies that we are unable to determine any given P_S with more than binary accuracy. Thus, boson-sampling does *not* let us *calculate* matrix permanents, as doing so would require determining amplitudes with a high level of precision, which would require an exponential number of measurements.

The experiment is repeated may times, each time performing a coincidence photodetection at the output modes. Thus, after each run we sample from the distribution P_S. This yields a so-called *sampling problem*, whereby the goal is to sample a statistical distribution using a finite number of measurements. This is in contrast to well-known *decision problems*, such as Shor's algorithm [39], which provide a well-defined answer to a well-posed question.

This sampling problem was shown by AA to be a computationally hard problem. That is, reconstructing the statistical distribution at the output to the boson-sampling device is computationally hard. However, whilst shown to be computationally hard, no known applications for boson-sampling have been described. Thus, boson-sampling acts as an interesting proof-of-principle demonstration that linear optics can outperform classical computers, but, based on present understanding, does not solve a problem of practical interest.

A. Sampling problems vs. decision problems (Peter)

B. Why is boson-sampling so much easier than linear optics quantum computing? (Peter)

C. Errors in boson-sampling (Johnny)

Discuss the 1/poly(n) bound

III. BOSON-SAMPLING AND THE EXTENDED CHURCH-TURING THESIS

Any model for quantum computation is subject to errors of some form. In the conventional circuit model, this includes errors such as dephasing. In linear optics, this includes photon loss and mode-mismatch. Let us consider a very generic error model for boson-sampling, where the

single-photon states are the desired single photon with probability p, otherwise are in some erroneous state [40]. This erroneous state could, for example, comprise terms with the wrong photon number (such as loss or second order excitations), or mode-mismatch. Then our input state is of the form,

$$\hat{\rho}_{\text{in}} = \left(\bigotimes_{i=1}^{n} [p \left|1\right\rangle \left\langle 1\right| + (1-p)\hat{\rho}_{\text{error}}^{(i)}] \right) \otimes [\left|0\right\rangle \left\langle 0\right|]^{\otimes^{m-n}}, \tag{14}$$

where $\hat{\rho}_{\text{error}}^{(i)}$ may be different for each input mode i. This is an independent error model, whereby each state is independently subject to an error channel. p stipulates the fidelity of the single photon states. When $p = 1$, the states are perfect single photons, and when $p < 1$, the state contain erroneous terms. We desire to sample from the distribution of Eq. 7, whereby none of the input states are erroneous. This occurs with probability p^n.

Let P be the probability that upon performing boson-sampling we have sampled from the correct distribution, otherwise we sample from noise. The complexity proof provided by AA only considered the regime where $P > 1/\text{poly}(n)$. Thus, for computational hardness, we require $p^n > 1/\text{poly}(n)$. Clearly in the asymptotic limit of large n, this bound can never be satisfied for any $p < 1$. Thus, with this independent error model, boson-sampling will always fail in the asymptotic limit.

Numerous authors [41–45] have claimed that large-scale demonstrations of boson-sampling could provide elucidation on the validity of the Extended Church-Turing (ECT) thesis – the statement that any physical system may be efficiently simulated on a Turing machine. However, it must be noted that the ECT thesis is by definition an asymptotic statement about arbitrarily large systems. Because the required error bound for boson-sampling is never satisfied in this limit, it is clear that boson-sampling cannot elucidate the validity of the ECT thesis as asymptotically large boson-sampling devices must fail under an independent error model.

This concern might be overcome in the future with either (1) a loosing of the error bound to $1/\exp(n)$, or (2) the development of fault-tolerance techniques for boson-sampling. However, to-date no such developments have been made. Thus, based on *present* understanding, boson-sampling will not answer the question as to whether the ECT thesis is correct or not. However, this is distinct from the question 'will boson-sampling yield *post-classical* computation?'. The answer to this question may very well be affirmative, as this only requires a finite sized device, just big enough to beat the best classical computers.

IV. BOSON-SAMPLING WITH OTHER CLASSES OF QUANTUM OPTICAL STATES (JOHNNY)

V. HOW TO BUILD A BOSON-SAMPLING DEVICE

In this section we explain the basic components required to build a boson-sampling device. This device consists of three basic components: (1) single-photon sources; (2) linear optics networks; and, (3) photodetectors. Each of these present their own engineering challenges. There are a range of technologies that could be employed for each of these components. However, although boson-sampling is much easier to implement than full-scale LOQC, it remains challenging to build a post-classical boson-sampling device.

A. Photon sources

add in citations

The first engineering challenge is to prepare an input state of the form of Eq. 7. This state may be generated using various photon source technologies. For a review of many of the photon sources see Ref. [46]. Presently, the most commonly employed photon source technology is spontaneous parametric down conversion (SPDC).

The SPDC source works by first pumping a non-linear crystal with a laser source. With some probability one of the laser photons interacts with the crystal and emits an entangled superposition of photons across two output modes, the *signal* and *idler*. The output of an SPDC source is of the form,

$$\left|\Psi_{\text{SPDC}}\right\rangle = \sqrt{1-\chi^2} \sum_{n=0}^{\infty} \chi^n \left|n\right\rangle_s \left|n\right\rangle_i, \tag{15}$$

where χ is the squeezing parameter, n is the number of photons, s represents the signal mode, and i represents the idler mode. For boson-sampling, we are interested in the $\left|1\right\rangle_s \left|1\right\rangle_i$ term of this superposition. The signal photons are measured by a photo-detector and because of the correlation in photon-number, we know that a photon is also present in the idler mode. The idler photons are then routed into one of the input ports of the boson-sampling device using a multiplexer [47–49].

There are several problems associated with SPDC sources, which limit the scalability of boson-sampling. The major problem is higher order photon-number terms. In the boson-sampling model we only want the $\left|1\right\rangle_s \left|1\right\rangle_i$ term, which is far from deterministic. The SPDC source is going to emit the zero-photon term with highest probability, with exponentially decreasing higher order terms. If the heralding photodetector does not have unit efficiency, then the heralded mode may contains higher order photon-number terms.

It was recently shown my Motes *et al.* [50] that SPDC sources are scalable in the asymptotic limit for boson-sampling. Specifically, if the photodetection efficiency is sufficient to guarantee post-selection at the output of the boson-sampling device with high probability then the heralded SPDC photons also have asymptotically high fidelity. The boson-sampling architecture with multiplexing is shown in Fig. 5.

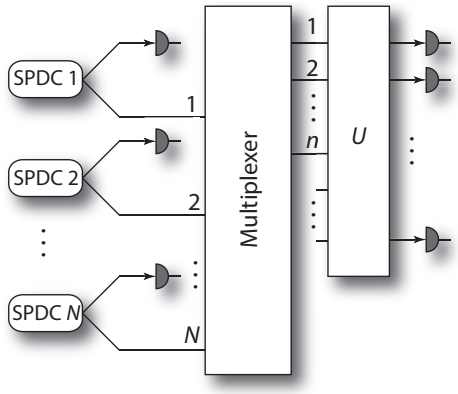

FIG. 5: Boson-sampling architecture using SPDC sources with an active multiplexer. N sources operate in parallel, each heralded by an inefficient single-photon number-resolving detector. It is assumed that $N \gg n$, which guarantees that at least n photons will be heralded. The multiplexer dynamically routes the successfully heralded modes to the first n modes of the unitary network U. Finally, photodetection is performed and the output is post-selected on the detection on all n photons.

Another problem is that photons from SPDC sources have uncertainty in their temporal distribution. If a boson-sampling device is built using multiple SPDC sources it is difficult to temporally align each of the n photons entering the device. The error term associated with this scales exponentially with n, yielding an error model consistent with Eq. 14, which undermines operation in the asymptotic limit.

B. Linear optics networks

After the input state has been prepared it is evolved via a linear optics network, $\hat{U}$. $\hat{U}$ transforms the input state as per Eq. 8 and may be completely characterized before the experiment using coherent state inputs [51]. $\hat{U}$ is composed of an array of discrete elements, namely, beam-splitters and phase-shifters. A beamsplitter with phase-shifters may be represented as a two-mode unitary of the form [52],

$$U_{\rm BS}(t) = \begin{pmatrix} e^{i(\alpha-\frac{\beta}{2}-\frac{\gamma}{2})}\cos\left(\frac{\delta}{2}\right) & -e^{i(\alpha-\frac{\beta}{2}+\frac{\gamma}{2})}\sin\left(\frac{\delta}{2}\right) \\ e^{i(\alpha+\frac{\beta}{2}-\frac{\gamma}{2})}\sin\left(\frac{\delta}{2}\right) & e^{i(\alpha+\frac{\beta}{2}+\frac{\gamma}{2})}\cos\left(\frac{\delta}{2}\right) \end{pmatrix}, \tag{16}$$

where $0 \leq \alpha \leq 2\pi$ and $0 \leq \{\beta, \gamma, \delta\} \leq \pi$ are arbitrary phases. It was shown by Reck *et al.* [37] that an arbitrary unitary $\hat{U}$ can be constructed with $O(m^2)$ optical elements, where m is the number of inputs to the boson-sampling device.

For a $\hat{U}$ that implements a classically hard problem one would need hundreds of discrete optical elements. Constructing an arbitrary $\hat{U}$ using the traditional linear optics approach of setting and aligning each optical element would be extremely cumbersome. Thus, using discrete optical elements is not a very promising route towards scalable boson-sampling.

One method to simplify the construction of the linear optics network is to use integrated waveguides. Quantum interference was first demonstrated with this technology by Peruzzo *et al.* [53]. This technology requires more frugal space requirements, is more optically stable, and far easier to manufacture, allowing the entire linear optics network to be integrated onto a small chip [54–56]. The main issue with integrated waveguides is achieving sufficiently low loss rates inside of the waveguide and in the coupling of the waveguide to the photon-sources and photo-detectors. Presently, the loss rates in these devices are extremely high and post-selection upon n photons at the output occurs with very low probability. It is foreseeable that photon-sources and photodetectors will eventually be integrated into the waveguide which would eliminate coupling loss rates, substantially improving scalability.

Another potential route to simplifying the linear optics network is to use time-bin encoding in a loop based architecture [57]. The major advantage of this architecture is that it only requires two delay loops, two on/off switches, and one controllable phase-shifter as shown in Fig. 6. This possibility eliminates the problem of aligning hundreds of optical elements and has fixed experimental complexity, irrespective of the size of the boson-sampling device. A major problem with this architecture however is that it remains difficult to control a dynamic phase-shifter with high fidelity at a rate that is on the order of the time-bin width τ.

C. Photodetection

The final requirement in the boson-sampling device is sampling the output distribution. With linear optics this is done using photo-detectors. For a review on photodetection see Ref. [46].

There are two general types of photo-detectors – photon-number resolving detectors and bucket detectors. The former counts the number of incident photons. These are much more difficult to make and more expensive in general than bucket detectors. Bucket detectors, on the other hand, simply trigger if any non-zero number of photons are incident on the detector.

As discussed earlier, in the limit of large boson-sampling devices, we are statistically guaranteed that we never measure more than one photon per mode, since the number of modes scales as $m = O(n^2)$. Thus, bucket de-

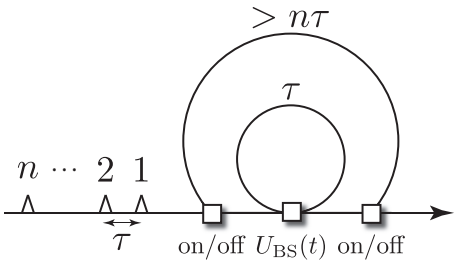

FIG. 6: Time-bin encoding architecture for implementing a boson-sampling device. Single photons arrive in a train of time-bins instead of in spatial modes. Each time-bin corresponds to spatial modes in the boson-sampling scheme and are separated by time τ. The photon train is coupled into the loop by the first switch. The photons then transverse the inner loop such that each time-bin may interact. The first (last) photon is coupled completely in (out). The outer loop allows an arbitrary number of the smaller loops to be applied consecutively which is determined by the third switch. Finally, the photon train is measured at the output using time-resolved detection.

tectors are sufficient for large boson-sampling devices, a significant experimental simplification compared to universal LOQC protocols.

Some of the various types of photo-detectors are:

Number-resolving:

Bucket:

- List different types of detectors
- don't need to be number resolving.
- be sure to describe issues to overcome

VI. CONCLUSION (JON)

Acknowledgments

This research was conducted by the Australian Research Council Centre of Excellence for Engineered Quantum Systems (Project number CE110001013).

[1] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[2] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[3] Y. Aharonov, L. Davidovich, and N. Zagury, Phys. Rev. A **48**, 1687 (1993).
[4] V. Cerny, Phys. Rev. A **48**, 116 (1993).
[5] J. Clauser and J. Dowling, Phys. Rev. A **53**, 4587 (1996).
[6] S. Bartlett, B. Sanders, S. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88** (2002).
[7] E. Knill, R. Laflamme, and G. Milburn, Nature **409**, 46 (2001).
[8] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Reviews of Modern Physics **79**, 135 (2007).
[9] G. Lapaire, P. Kok, J. Dowling, and J. Sipe, Phys. Rev. A **68** (2003).
[10] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[11] S. Aaronson and A. Arkhipov, Theory of Computing **9 (4)**, 143 (2013).
[12] B. T. Gard, R. M. Cross, P. M. Anisimov, H. Lee, and J. P. Dowling, J. Optical Soc. Am. B **30**, 1538 (2013).
[13] B. T. Gard, J. P. Olson, R. M. Cross, M. B. Kim, H. Lee, and J. P. Dowling, Phys. Rev. A **89** (2014).
[14] K. R. Motes, J. P. Dowling, and P. P. Rohde, Phys. Rev. A **88** (2013).
[15] H. J. Ryser, Combinatorial Mathematics, Carus Mathematical Monograph No. 14 (1963).
[16] T. C. Ralph, Nature Photonics **7**, 514 (2013).
[17] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Science **339**, 794 (2013).
[18] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, et al., Science **339**, 798 (2013).
[19] Anonymous, Photonics Spectra **47**, 33 (2013).
[20] M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Nature Photonics **7**, 540 (2013).
[21] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Nature Photonics **7**, 545 (2013).
[22] J. P. Dowling (2013), URL http://quantumpundit.blogspot.com/2013/07/sampling-schmampling.html.
[23] P. P. Rohde, Phys. Rev. A **86** (2012).
[24] P. P. Rohde and T. C. Ralph, Phys. Rev. A **85** (2012).
[25] Z. Jiang, M. D. Lang, and C. M. Caves, Phys. Rev. A **88** (2013).
[26] V. S. Shchesnovich, Phys. Rev. A **89** (2014).
[27] R. P. Feynman, International Journal Of Theoretical Physics **21**, 467 (1982).
[28] S. Lloyd, Science **273**, 1073 (1996).
[29] D. D and J. R, Proceedings of the Royal Society of London Series A-Mathematical Physical and Engineering Sciences **439**, 553 (1992).
[30] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).
[31] D. Aharonov, *Annual Reviews of Computational Physics VI (ed. Stauffer, D.)* (World Scientific, Singapore, 1999).
[32] D. DiVincenzo, Fort. Phys. **48**, 771 (2000).
[33] K. Lemr, A. Černoch, J. Soubusta, and M. Dušek, arXiv:1207.5756v1.
[34] M. A. Nielsen, Phys. Rev. Lett. **93** (2004).
[35] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[36] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
[37] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[38] S. Scheel (2004), quant-ph/0508189.
[39] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
[40] P. P. Rohde, K. R. Motes, P. A. Knott, and W. J. Munro (2014), arXiv:1401.2199.

[41] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Science **339**, 6121 (2013).
[42] C. Shen, Z. Zhang, and L.-M. Duan (2013), arXiv:1310.4860.
[43] S. Aaronson and A. Arkhipov (2013), arXiv:1309.7460v2.
[44] V. S. Shchesnovich (2013), arXiv:1311.6796.
[45] M. C. Tichy, K. Mayer, A. Buchleitner, and K. Mølmer (2013), arXiv:1312.3080.
[46] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Review of Scientific Instruments **82**, 071101 (2011).
[47] A. Migdall, D. Branning, and S. Castelletto, Physical Review A **66**, 053805 (2002).
[48] T. Meany, L. A. Ngah, M. J. Collins, A. S. Clark, R. J. Williams, B. J. Eggleton, M. J. Steel, M. J. Withford, O. Alibart, and S. Tanzilli, Laser & Photonics Reviews (2014), ISSN 1863-8899.
[49] X.-S. Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger, Phys. Rev. A **83**, 043814 (2011).
[50] K. R. Motes, J. P. Dowling, and P. P. Rohde, Physical Review A **88**, 063822 (2013).
[51] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[52] C. C. Gerry and P. L. Knight, *Introductory quantum optics* (Cambridge University Press, 2005).
[53] A. Peruzzo, A. Laing, A. Politi, T. Rudolph, and J. L. O'Brien, Nature communications **2**, 224 (2011).
[54] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, Science **320**, 646 (2008).
[55] J. C. Matthews, A. Politi, A. Stefanov, and J. L. O'Brien, Nature Photonics **3**, 346 (2009).
[56] A. Politi, J. C. F. Matthews, and J. L. O'Brien, Science **325**, 1221 (2009).
[57] K. R. Motes, A. Gilchrist, J. P. Dowling, and P. P. Rohde, arXiv:1403.4007 (2014).