

Quantum circuits for simulating linear interferometers

Hudson Leone 

Centre for Quantum Software and Information—[University of Technology Sydney](#), Sydney, Australia
and Australian Research Council Centre of Excellence for Quantum Computing and Communication Technology (CQC2T),
Sydney 2000, Australia

Peter S. Turner ^{*}

School of Mathematical and Physical Sciences, [Macquarie University](#), Sydney, New South Wales 2109, Australia
and Sydney Quantum Academy, 1 Eddy Avenue, Sydney, New South Wales 2000, Australia

Simon Devitt [†]

Centre for Quantum Software and Information—[University of Technology Sydney](#), Sydney, Australia
and InstituteQ, [Aalto University](#), 02150 Espoo, Finland



(Received 4 May 2025; accepted 10 November 2025; published 20 February 2026)

Motivated by recent proposals for quantum proof of work protocols, we investigate approaches for simulating linear optical interferometers using digital quantum circuits. We focus on a second quantization approach, where the quantum computer's registers represent optical modes. We can then use standard quantum optical techniques to decompose the unitary matrix describing an interferometer into an array of 2×2 unitaries, which are subsequently synthesized into quantum circuits and stitched together to complete the circuit. For an m -mode interferometer with n identical photons, this method requires approximately $\mathcal{O}(m \log(n))$ qubits and a circuit depth of $\mathcal{O}(mn^4 \log_2(n) \text{polylog}(n^4/\epsilon))$. We present a software package *aquinas* (a quantum interferometer assembler) that uses this approach to generate such quantum circuits. For reference, an arbitrary five-mode interferometer with two identical photons is compiled to a ten-qubit quantum circuit with a depth of 1972.

DOI: [10.1103/z513-z2dr](https://doi.org/10.1103/z513-z2dr)

I. INTRODUCTION

Linear optics has been at the forefront of quantum information research for many years. While interferometers natively execute certain types of high-fidelity quantum operations, they cannot be practical universal quantum computers unless some nonlinearity is introduced [1]. Nevertheless, there remains significant interest in linear quantum photonics, particularly on account of the seminal work of Aaronson and Arkhipov, which demonstrated that the interferometry problem of *boson sampling* is almost certainly classically intractable [2]. This stems from the fact that even approximating the output occupation probabilities of a boson sampling experiment requires one to calculate the permanents of large matrices, which is a famously #P-complete problem.

One implication of this is that linear optical interferometers, which are considerably easier to build than general-purpose quantum computers, could in principle be used to demonstrate genuine (albeit impractical) quantum computational supremacy. Significant work has therefore been

done to engineer interferometers that are both large enough and reliable enough to demonstrate an incontestable quantum advantage (see Ref. [3] for a review of progress). Of note is a recent result from Madsen *et al.* claiming supremacy using a variant of boson sampling that uses Gaussian states [4].

Although linear interferometry lacks the computational power of a general-purpose quantum computer, the proliferation of these experimental results has motivated research around finding practical applications for boson sampling. Some computational examples include locating dense subgraphs [5] and the graph isomorphism problem [6], though whether such algorithms can yield a tangible advantage in practice remains to be seen. An arguably more promising application for boson sampling is in distributed consensus between quantum computers. Recent work has indicated the suitability of coarse-grained boson sampling as a proof-of-work algorithm, which may see use in future quantum infrastructure [7].

Presently, to our knowledge, the best reported algorithm for simulating linear interferometers is the classical method from Heurtel *et al.*, which, despite savings over conventional permanent-based calculations, is still exponential in general (as expected) [8]. It is worth mentioning that a major practical issue with developing boson samplers is that of photon loss and distinguishability. Though the hardness of boson sampling remains unchanged when a constant number of photons are lost [9], losing a fraction of the total number of photons can render the sampling problem classically tractable [10,11].

^{*}Contact author: peter.turner@mq.edu.au[†]Contact author: simon.devitt@uts.edu.au

One may then ask how to go about simulating boson sampling (and linear optics more generally) on a conventional quantum computer. Of course, any quantum computer that can emulate boson sampling will generally be more powerful than an interferometer. Nevertheless, this could conceivably be useful for a quantum proof-of-work protocol, and simulating linear interferometers beyond what is experimentally feasible may be of fundamental interest.

In this paper, we report a software package called *aquinas* (a quantum interferometer assembler) [12] that expresses a given linear interferometer as a quantum circuit that accurately simulates ideal linear interferometry for up to a prespecified number of photons and modes. Broadly speaking, the algorithm works by first decomposing the given multi-mode interferometer into a network of interlaced two-mode beam splitters and phase shifters. Following this, the Hamiltonian of each two-mode piece is expressed in terms of ladder operators over the respective modes. By truncating the ladder operators at a fixed photon number (the total number of photons that enter the interferometer) and using some padding, we obtain a Hamiltonian that, when exponentiated, gives a unitary matrix that can be synthesized into a quantum subcircuit. These subcircuits are then knitted together in the configuration of the original beam splitters to form the interferometer circuit.

The main advantage of this “divide-and-conquer” approach is that, by bringing compilation down to the level of individual beam splitters, the problem of synthesizing an interferometer circuit becomes computationally tractable with respect to both n , the number of photons, and m , the number of modes. As we will show, a clear drawback is that our circuits have an asymptotic depth that scales poorly with n . Our technique is therefore best suited for sparse interferometers with many modes and a limited number of photons. As a rule of thumb, a classically hard instance of boson sampling requires upward of $n \geq 30$ photons over $\mathcal{O}(n^2)$ modes [2]. Our circuit depths become prohibitively large even for relatively easy experiments (as we will see in Fig. 6). Nevertheless, we hope this work is a helpful first step toward simulating quantum optics with digital quantum computers.

In the following section, we describe how a linear interferometer evolves the creation operators of a photon number state and explain how these states can be described in either first or second quantization. In Sec. III, we limit our attention to the second quantization and detail our algorithm. Finally, in Sec. IV, we present numerical analysis that indicates our software is working correctly while allowing us to approximate circuit depths for moderate instances of boson sampling.

II. LINEAR OPTICS AND QUANTUM COMPUTATION BACKGROUND

Suppose we have a linear interferometer with m input and m output modes. Such a device is usually characterized in second quantization by an $m \times m$ unitary U that describes how creation operators are transformed for each mode. Specifically, if $\hat{a}_i^\dagger$ is the creation operator for the i th mode, we have

$$\hat{a}_i^\dagger \mapsto \sum_{i'=1}^m U_{ii'} \hat{a}_{i'}^\dagger, \quad (1)$$

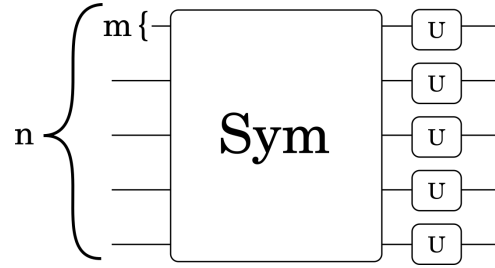


FIG. 1. A generic quantum circuit for simulating a linear interferometer in first quantization. The n registers are m -dimensional qudits that represent indistinguishable photons. Measurement in the computational basis indicates which of the m possible modes that photon is found in. By the symmetrization postulate for bosons, reordering the n registers cannot change the input state; this is implemented by the highly entangling *Sym* operation. Following this, the defining interferometer operation U is applied to each photon locally.

where $U_{ii'}$ are the matrix elements of U . For n photons, the output state is described by a degree- n polynomial in the creation operators. The coefficients turn out to be permanents of $n \times n$ matrices W , whose matrix elements are taken from U according to the input state and measurement outcome [13]:

$$\begin{aligned} & \hat{a}_{i_1}^\dagger \hat{a}_{i_2}^\dagger \cdots \hat{a}_{i_n}^\dagger \\ & \mapsto \left(\sum_{i'_1=1}^m U_{i_1 i'_1} \hat{a}_{i'_1}^\dagger \right) \left(\sum_{i'_2=1}^m U_{i_2 i'_2} \hat{a}_{i'_2}^\dagger \right) \cdots \left(\sum_{i'_n=1}^m U_{i_n i'_n} \hat{a}_{i'_n}^\dagger \right) \quad (2) \\ & = \sum_{i'_1 \leq i'_2 \leq \cdots \leq i'_n} \text{per} W_{i'_1 i'_2 \cdots i'_n}^{i_1 i_2 \cdots i_n}(U) \hat{a}_{i'_1}^\dagger \hat{a}_{i'_2}^\dagger \cdots \hat{a}_{i'_n}^\dagger. \quad (3) \end{aligned}$$

Quantum computation lends itself naturally to a first quantization picture, where a simulation circuit for such a linear interferometer consists of n quantum registers of dimension m . Thus, each register represents a photon, and measuring a register is analogous to learning the mode of that particular photon (see Fig. 1) [14]. Because these particles are indistinguishable, we require by the symmetrization postulate that our input state is invariant under photon permutation. Therefore, the input state of our circuit must be invariant under permutation of the registers. This means that the initial state must first be symmetrized, which is in general a nontrivial subroutine. One could implement this symmetrization on a quantum computer with, for example, the Schur transform, which is known to be efficiently implementable [15].

After symmetrization, however, simulating the interferometer is straightforward because photon interactions are extremely weak and can be safely ignored. Consequently, we can treat each photon of our symmetric state as if it were the only one passing through the interferometer. Since U can be interpreted as the transformation of a single photon, the final step for simulating in first quantization is to implement U on each of the n registers. A basic schematic of this protocol is presented in Fig. 1.

In second quantization, the roles of particles and modes are reversed (see Fig. 2). Now, we have m registers of dimension $n+1$ that represent each of the possible modes. Each mode can be measured to detect up to n photons with an additional

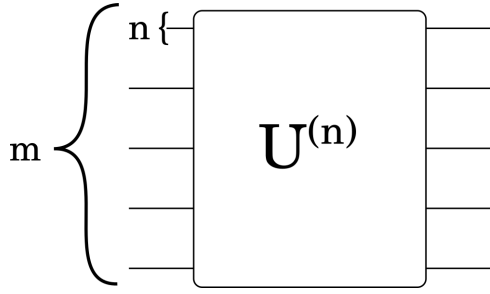


FIG. 2. A generic quantum circuit for simulating a linear interferometer in the second quantization picture. The m registers of the circuit are $(n + 1)$ -dimensional qudits that represent the m modes of an interferometer. Measuring in the computational basis reveals how many photons are present in that mode. The complexity of the second quantization approach is in constructing a circuit to implement $U^{(n)}$, which is the unitary matrix corresponding to the interferometer U acting in Fock space.

promise that there are n photons in total. Unlike the first quantization, there is no symmetrization step required in this picture since the modes only need to encode the number of particles present (the occupation). The difficulty of simulating in second quantization is constructing a circuit to implement $U^{(n)}$, which is the unitary describing how photon number states with up to n photons are transformed by the interferometer. This is the problem we consider in this paper.

III. SIMULATING IN THE SECOND QUANTIZATION

We recall from Fig. 2 that an optical simulation in the second quantization picture is realized with a quantum circuit that implements $U^{(n)}$; this unitary describes how photon number states containing up to n photons evolve through the interferometer. The primary difficulty of working in this quantization is finding a suitable way to construct this circuit. To make headway into this problem, let us first consider how $U^{(n)}$ is related to U . We begin by finding the Hamiltonian operator that generates U under exponentiation:

$$H = -i \log U. \quad (4)$$

Here, the above expression refers to the matrix logarithm. It is well known that such a Hamiltonian is a linear combination of number preserving terms quadratic in the ladder operators (i.e., these terms generate the Lie algebra for the group of interferometer unitaries).

For a fixed photon number n , each mode needs to only support the $n + 1$ occupations $0, 1, 2, \dots, n$. We therefore truncate the ladder operators, taking them from infinite-dimensional to $(n + 1)$ -dimensional matrices:

$$H \xrightarrow{\hat{a}_i \rightarrow \hat{a}_i^{(n)}} H^{(n)}. \quad (5)$$

Finally, we exponentiate to obtain the truncated unitary

$$U^{(n)} = e^{iH^{(n)}}. \quad (6)$$

There are at least two approaches for efficiently constructing a circuit for $U^{(n)}$. The first is Hamiltonian simulation, where the truncated Hamiltonian $H^{(n)}$ is decomposed into a

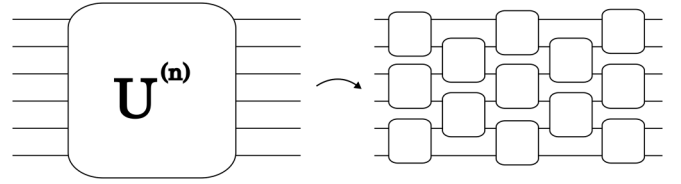


FIG. 3. Given a linear interferometer U , it is not computationally tractable to generate a circuit for the truncated operator $U^{(n)}$. In the “divide-and-conquer” approach, we use the decomposition of Ref. [17] to break U into a grid of 2×2 unitaries that are significantly smaller than the original interferometer matrix. As such, this method is best suited for simulating sparse linear interferometry where $n \ll m$, as in boson sampling.

polynomial-length sum of Pauli strings that are each “circuitized” and repeated to approximate the target unitary $U^{(n)}$. Sawaya *et al.* detail this approach in the context of quantum optics [16]. An alternative method, which is the one we present in this paper, is a “divide-and-conquer” approach wherein a standard decomposition of the interferometer [17] is used to break U into a grid of 2×2 unitaries (i.e., beam splitters, or two-mode interferometers) that have the form

$$U_{BS} = \begin{pmatrix} e^{i\phi} \cos \theta & -\sin \theta \\ e^{i\phi} \sin \theta & \cos \theta \end{pmatrix}. \quad (7)$$

Here, $\theta \in [0, \pi/2]$ is a parameter related to the *reflectivity* of the beam splitter. The device is transparent when $\theta = 0$ and is perfectly reflective when $\theta = \pi/2$. The $\phi \in [0, 2\pi]$ parameter is the relative phase shift introduced between the output modes.

To calculate the truncated counterparts of these unitaries, we follow the steps laid out in Eqs. (4)–(6). After synthesizing circuits for each of these simpler unitaries, we can take matrix products according to their original configuration to obtain a circuit for $U^{(n)}$ (see Fig. 3 for a schematic of the decomposition and Fig. 4 for an illustrative example of the basic circuit structure).

A. Two-mode interferometer

Before we analyze this approach numerically, let us illustrate with an example of how a truncated beam splitter unitary is calculated. Although AQUINAS uses the Clements decomposition to obtain a grid of 2×2 unitaries in the form of Eq. (7), we simplify our example by considering a different (but physically equivalent) beam splitter unitary [18]:

$$U_{BS} = \begin{pmatrix} \cos \theta & e^{i\phi} \sin \theta \\ -e^{-i\phi} \sin \theta & \cos \theta \end{pmatrix}. \quad (8)$$

The corresponding Hamiltonian is then

$$H_{BS} = -i \log U_{BS} = \begin{pmatrix} 0 & -ie^{i\phi}\theta \\ ie^{-i\phi}\theta & 0 \end{pmatrix}, \quad (9)$$

which, written in terms of two-mode ladder operators, has the form

$$H_{BS} = -ie^{i\phi}\theta \hat{a}_1^\dagger \hat{a}_2 + ie^{-i\phi}\theta \hat{a}_2^\dagger \hat{a}_1. \quad (10)$$

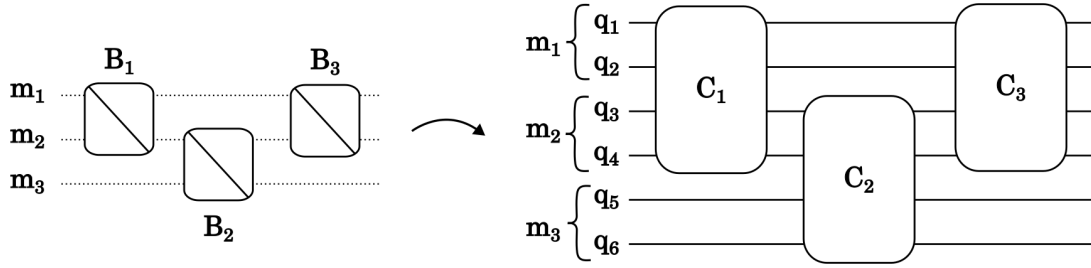


FIG. 4. An illustration of how the “divide-and-conquer” method translates a three-mode interferometer into a quantum circuit. Left: According to the Clements decomposition, an arbitrary linear interferometer with three spatial modes (m_1, m_2, m_3) contains three beam splitter elements (B_1, B_2, B_3). Right: Assuming a photon number $n < 4$, two qubits can be used to encode the photon number at each of the three modes. Qubits (q_1, q_2), for example, encode the photon number at mode m_1 . Individual beam splitters are translated into quantum circuits (C_1, C_2, C_3) that act between the respective modes. Here, the B_i beam splitter corresponds to the C_i circuit. The average circuit depth and cnot count for each C_i in this example are around 189 and 97, respectively (these values were calculated by first sampling 100 random beam splitters and building the corresponding circuits given $n = 3$).

Say, for example, we want to find the corresponding unitary with photon number $n = 2$. In this case, we would perform the following substitutions in Eq. (10):

$$\hat{a}_1^\dagger \hat{a}_2 \rightarrow \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \sqrt{2} & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \sqrt{2} \\ 0 & 0 & 0 \end{pmatrix} \quad (11)$$

$$\hat{a}_2^\dagger \hat{a}_1 \rightarrow \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \sqrt{2} \\ 0 & 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \sqrt{2} & 0 \end{pmatrix} \quad (12)$$

and then take the matrix exponential to obtain $U_{\text{BS}}^{(2)}$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \cos[\theta] & 0 & -e^{-i\phi} \sin[\theta] & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cos[\theta]^2 & 0 & -\sqrt{2}e^{-i\phi} \cos[\theta] \sin[\theta] & 0 & e^{-2i\phi} \sin[\theta]^2 & 0 & 0 & 0 \\ 0 & e^{i\phi} \sin[\theta] & 0 & \cos[\theta] & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2}e^{i\phi} \cos[\theta] \sin[\theta] & 0 & \cos[2\theta] & 0 & -\sqrt{2}e^{-i\phi} \cos[\theta] \sin[\theta] & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cos[2\theta] & 0 & -2e^{-i\phi} \cos[\theta] \sin[\theta] & 0 & 0 \\ 0 & 0 & e^{2i\phi} \sin[\theta]^2 & 0 & \sqrt{2}e^{i\phi} \cos[\theta] \sin[\theta] & 0 & \cos[\theta]^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & e^{i\phi} \sin[2\theta] & 0 & 0 & \cos[2\theta] & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (13)$$

Notice, however, that the size of this matrix is not equal to a power of 2 since the creation and annihilation operators we substituted in Eqs. (11) and (12) were not themselves powers of 2. We have two options for expanding into a qubit-friendly Hilbert space. The first and most obvious choice is to pick the next highest truncation that has a power-2 dimension. In this example, that would be $n = 3$:

$$\hat{a}^{\dagger(3)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 & 0 \\ 0 & 0 & \sqrt{3} & 0 \end{pmatrix}. \quad (14)$$

Alternatively, if one favors a slightly more sparse matrix, one can simply *pad* the creation, annihilation, and identity operators with zeros until the next power of 2 is reached. For example,

$$\hat{a}_{\text{padded}}^{\dagger(2)} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \sqrt{2} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (15)$$

To see the effect of this padding, consider a padded operator of the form $\hat{a}_i^\dagger \hat{a}_j$. When exponentiated, the action of the resulting unitary is seen with some effort to be idempotent on states with a photon number greater than the truncation depth.

1. Analysis of “divide and conquer”

At the start of Sec. III, we illustrated how the Clements decomposition can be used to decompose any interferometer into a grid of two-mode interferometers. Synthesizing circuits for each of these elements is significantly easier than finding a circuit for $U^{(n)}$ since fewer “active” qubits are required. To see how many exactly, first note that the minimum number of qubits needed to encode up to n photons in a single mode is $\lceil \log_2(n+1) \rceil$. A two-mode unitary truncated at a photon number of n therefore acts on $2\lceil \log_2(n+1) \rceil$ qubits. Recall that by the Solovay-Kitaev theorem, the number of gates required for a generic k qubit operator scales as (see Chap. 4, Sec. 5.4 of Ref. [19])

$$\mathcal{O}(4^k k^2 \log^c(4^k k^2 / \epsilon)), \quad (16)$$

where ϵ is the desired accuracy and c is a constant.

To find the asymptotic depth of a beam splitter circuit with respect to the photon number n , we make the approximation $k \approx 2 \log_2(n)$ and assume that the gates are uniformly distributed across the wires. The asymptotic circuit depth is therefore equal to the number of gates divided by the number of qubits:

$$\mathcal{O}(n^4 \log_2(n) \log^c(2n^4 \log_2^2(n)/\epsilon)), \quad (17)$$

which, to be succinct, we write as

$$\mathcal{O}(n^4 \log_2(n) \text{polylog}(n^4/\epsilon)). \quad (18)$$

Although the depth of a beam splitter circuit is evidently polynomial with respect to n , it remains to be seen whether the *compilation complexity* is polynomial (in other words, can these circuits be efficiently constructed with respect to n ?). To answer this question, it is sufficient to consider how the size of the Hilbert space grows with n . Because $2^{\lceil \log_2(n+1) \rceil}$ qubits are required to encode up to n photons per mode over two modes, the dimension of the “active” beam splitter Hilbert space is

$$\dim(\mathcal{H}) = 2^{2^{\lceil \log_2(n+1) \rceil}}, \quad (19)$$

which is asymptotically equivalent to $\mathcal{O}(n^2)$. Since the size of the Hilbert space grows quadratically with respect to n , we conclude that circuit synthesis is tractable for each beam splitter element.

Having established the width and depth of a *single* beam splitter circuit, we now consider the number of beam splitters that are required to decompose the interferometer. Well-established results in mathematics [20] and more recently in

the context of quantum optics [17,21] show that $m(m-1)/2$ two-mode interferometers are required to reconstruct an arbitrary m -mode interferometer, which immediately implies a depth of $\mathcal{O}(m)$ beam splitter elements and therefore a total circuit depth of $\mathcal{O}(mn^4 \log_2(n) \text{polylog}(n^4/\epsilon))$. In summary, the required number of qubits and the circuit depth of this second quantization approach are

Size	$\mathcal{O}(m \log(n))$
Depth	$\mathcal{O}(mn^4 \log_2(n) \text{polylog}(n^4/\epsilon))$

Moreover, since the number of beam splitters in a given interferometer decomposition is $\mathcal{O}(m^2)$, it follows that our divide-and-conquer approach also has a polynomial compilation complexity with respect to m .

IV. RESULTS

The AQUINAS software package [12] takes an $m \times m$ unitary matrix representing an m -mode linear interferometer and uses the method described in Sec. III A 1 to synthesize a quantum circuit that simulates the interferometer for any input state of up to n photons. To compensate for the fact that the dimensions of creation and annihilation operators truncated at photon number n generally are not a power of 2, we use the operator padding technique described in the worked example of Sec. III to ensure that $U^{(n)}$ can be implemented as a quantum circuit. (See Algorithm 1 for pseudocode.)

ALGORITHM 1. Pseudocode for the algorithm used by the aquinas software.

Inputs :

- n (The maximum photon number)
- U (An $m \times m$ unitary matrix describing how creation operators are transformed by an m mode interferometer)
- `sparsity_optimization == True` (If true, we perform an additional ‘padding’ step that slightly improves the sparsity of the circuit unitary when n is not a power of two.)

Output: A quantum circuit that simulates the interferometer for any photon number state containing up to (and including) n photons.

begin

Decompose U to obtain $m(m-1)/2$ many 2×2 unitary matrices. Remember their positions.

foreach 2×2 unitary B_i **do**

Calculate the corresponding Hamiltonian H_i (See section III 1 for an example)

Calculate $H_i^{(n)}$:

if `sparsity_optimization == False` **then**

$n := \text{next_highest_power_of_two}(n)$

Replace unbounded creation and annihilation operators ($\hat{a}^\dagger, \hat{a}$) with truncated counterparts ($\hat{a}^{\dagger(n)}, \hat{a}^{(n)}$)

else

Replace ($\hat{a}^\dagger, \hat{a}$) with ($\hat{a}^{\dagger(n)}, \hat{a}^{(n)}$)

Pad $\hat{a}^{(n)\dagger}$ and $\hat{a}^{(n)}$ with zeros until the shapes of each are a power of two. (See eq. 15)

Take the exponential of $H_i^{(n)}$ to obtain $U_i^{(n)}$

Convert $U_i^{(n)}$ into a quantum circuit (We use the `Qiskit.transpile()` method [22] at `optimization_level = 2` to synthesise circuits from the gateset $\{CNOT, U_3\}$)

Assemble the circuits as per the original decomposition

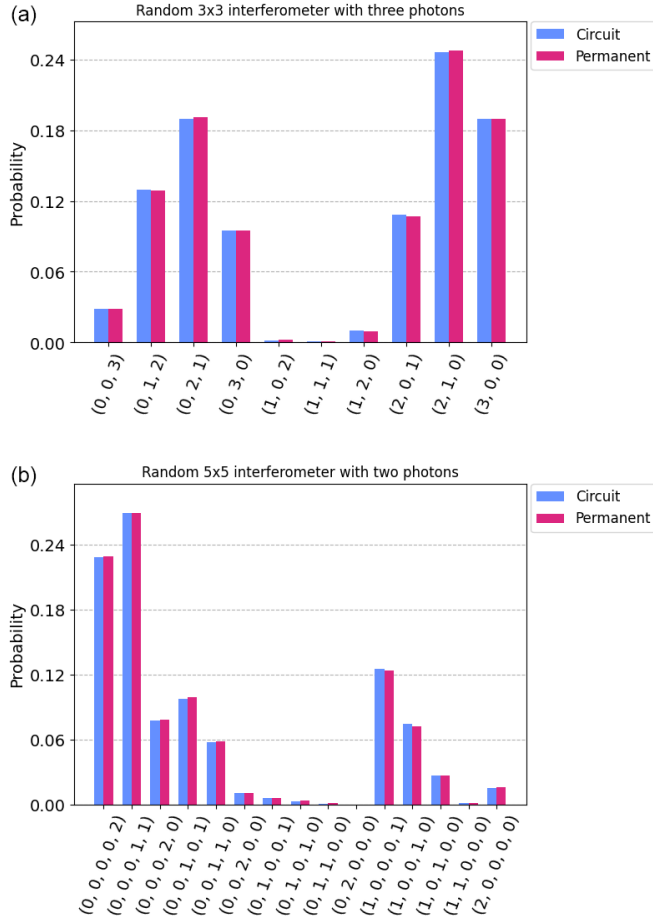


FIG. 5. Two numerical experiments in which the output statistics of interferometer circuits are compared with genuine expectation values (calculated via the matrix permanent method). The circuit statistics in blue were compiled by running each circuit 10 000 times. (a) A randomly selected 3×3 interferometer with up to three photons is simulated as a 6 qubit, depth 567 circuit. The initial photon configuration (2,1,0) is scrambled into one of 10 possible output distributions. (b) A randomly selected 5×5 interferometer with up to two photons is simulated as a 10 qubit, depth 1972 circuit. The initial photon configuration (2,0,0,0,0) is scrambled into 15 possible output distributions.

Our method is perhaps best described by way of examples—We present two numerically simulated interferometer experiments. In the first of these, we randomly selected a three-mode interferometer $U_{\text{rand}} \in \text{SU}(3)$ and began with three indistinguishable photons in the arbitrarily chosen configuration (2, 1, 0) (which is to say there are two photons in the first mode and one in the second mode). Using aquinas, we then constructed a quantum circuit that implements the transformation $U_{\text{rand}}^{(3)}$ using six qubits with a depth of 567. We simulated this circuit noiselessly using the qiskit [22] software package to obtain 10 000 measurement samples, which were then converted into estimates for the probabilities of observing each of the 10 possible output configurations. In order to validate these probabilities, we used the permanent method to calculate the expectation values for each outcome analytically.

We compare the estimated probabilities with the exact expectation values for this experiment using the histogram in

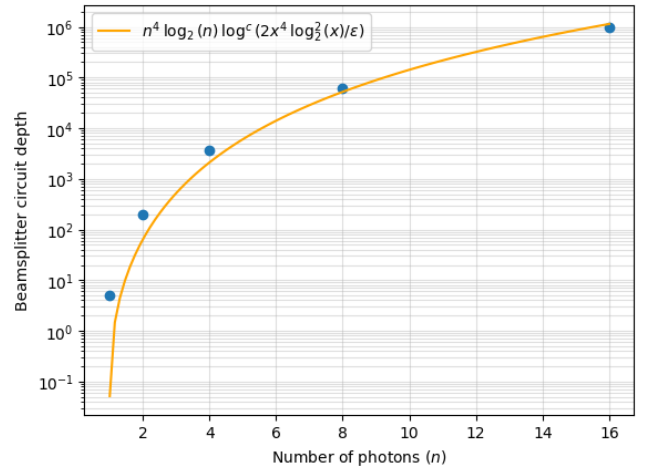


FIG. 6. Circuit depths for a randomly selected two-mode interferometer for various numbers of photons. The orange curve is placed as a visual aid to show the approximate trend of the data points. Its vertical coordinates are equal to $\mathcal{O}(n^4 \log_2(n) \log^c(2n^4 \log_2^2(n)/\epsilon))$, where n is the photon number, ϵ is an error term (assumed to be 1×10^{-15} since the numerical errors reported in Sec. IV have the same order of magnitude), and $c \approx 0.377$ (which was selected using nonlinear least squares regression).

the upper part of Fig. 5. From inspection, it appears that our estimates converge on the genuine expectation values with minor variations that may possibly be attributed to sampling uncertainty. To verify that this convergence was genuine, we began by using qiskit’s built-in `Operator` class to transform the circuit into a $2^6 \times 2^6$ matrix. After this, we calculated the expectation values of a random assortment of output probabilities by “looking up” the appropriate matrix element:

$$p_{\text{out}} = |\langle \psi_{\text{out}} | U_{\text{rand}}^{(3)} | \psi_{\text{out}} \rangle|^2. \quad (20)$$

With this, we were able to quickly verify that the expectation values of the circuit were accurate to an error of around $\epsilon \approx 3 \times 10^{-15}$.

The second experiment was virtually identical to the first, with the only difference being that we instead simulated a five-mode interferometer with two photons in the starting configuration (2, 0, 0, 0, 0). In this case, the resulting ten-qubit circuit has a depth of 1972. The estimated probabilities of the 15 possible output distributions from 10 000 circuit samples are plotted in the bottom part of Fig. 5 together with the analytical expectation values. As before, we see convincing evidence of genuine convergence that we confirmed by manually checking the expectation values of the operator corresponding to the circuit. As before, we compared the expectation values of this circuit to the analytical values and found a somewhat higher error of around $\epsilon \approx 6 \times 10^{-15}$.

In order to calculate the depth of aquinas’s circuits with respect to m and n , it is sufficient to calculate the depths of the beam splitter circuits with respect to n . This is because every circuit with $m > 2$ modes is composed of multiple beam splitter circuits arranged in a predictable pattern (recall Fig. 3). A scatterplot of these depths is presented in Fig. 6.

V. CONCLUSION AND OUTLOOK

In this work, we looked at approaches for simulating linear optics in first and second quantization pictures. We presented a divide-and-conquer strategy in the second quantization picture based on decomposing the interferometer into beam splitters and phase shifters, which are more easily synthesized into circuits. We wrote software to construct interferometer circuits according to this method and found that the asymptotic circuit size and depth were $\mathcal{O}(m \log(n))$ and $\mathcal{O}(n^4 \log_2(n) \text{polylog}(n^4/\epsilon))$, respectively. Finally, we validated our efforts by presenting two numerical experiments in Fig. 5.

Although we initially hoped that this *divide-and-conquer* method might be able to generate feasible circuits for nontrivial instances of boson sampling (upward of $n = 30$ and $m = \mathcal{O}(n^2)$ [2]), it is clear from our numerical data (Fig. 6) that the circuit depths for individual beam splitters are prohibitively large. A 16-photon beam splitter, for example, requires a depth of around 10^6 (see Fig. 6). Consequently, it is unlikely that *divide and conquer* will see any practical use, even with further optimizations.

One promising direction for further research is to simulate in the first quantization picture instead. As mentioned in Sec. II, the main difficulty with this approach is the preparation of symmetric states. Recently, Berry *et al.* proposed various methods for efficiently preparing *antisymmetric states*

[23]. Using a sorting network called an *odd-even mergesort*, they indicate that it is possible to prepare an m -mode, n -particle antisymmetric state using $\mathcal{O}(m \log^c m \log n)$ ancilla qubits and a circuit depth of $\mathcal{O}(\log^c m \log \log n)$. With further work, it is possible their techniques could be used to generate symmetric states.

In this work, we have limited our discussion to the circuit model of quantum computation. Whether or not there is an advantage in considering a measurement-based framework is an open question. Our work can be used as a first step in this direction by noting that aquinas circuits can be translated into equivalent graphs using the jabilizer package by Vijayan *et al.* [24].

ACKNOWLEDGMENTS

We thank Professor Gavin Brennen and Dr. Peter Rhode for helpful discussions. The lead author extends a special thanks to our resident computer wizard Dr. Alan Robertson for helping fix a particularly nasty bug. H.L. acknowledges support from the ARC Center of Excellence for Computing and Communications Technology (CQC2T).

DATA AVAILABILITY

The data supporting this study's findings are available within the article.

-
- [1] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Linear optical quantum computing with photonic qubits, *Rev. Mod. Phys.* **79**, 135 (2007).
 - [2] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing, STOC'11* (Association for Computing Machinery, New York, 2011), pp. 333–342.
 - [3] D. J. Brod, E. F. Galvão, A. Crespi, R. Osellame, N. Spagnolo, and F. Sciarrino, Photonic implementation of boson sampling: A review, *Adv. Photonics* **1**, 034001 (2019).
 - [4] L. S. Madsen, F. Laudenbach, M. F. Askarani, F. Rortais, T. Vincent, J. F. F. Bulmer, F. M. Miatto, L. Neuhaus, L. G. Helt, M. J. Collins, A. E. Lita, T. Gerrits, S. W. Nam, V. D. Vaidya, M. Menotti, I. Dhand, Z. Vernon, N. Quesada, and J. Lavoie, Quantum computational advantage with a programmable photonic processor, *Nature (London)* **606**, 75 (2022).
 - [5] J. M. Arrazola and T. R. Bromley, Using Gaussian boson sampling to find dense subgraphs, *Phys. Rev. Lett.* **121**, 030503 (2018).
 - [6] K. Brádler, S. Friedland, J. Izaac, N. Killoran, and D. Su, Graph isomorphism and Gaussian boson sampling, *Spec. Matrices* **9**, 166 (2021).
 - [7] D. Singh, G. Muraleedharan, B. Fu, C.-M. Cheng, N. R. Newton, P. P. Rohde, and G. K. Brennen, Proof-of-work consensus by quantum sampling, *Quantum Sci. Technol.* **10**, 025020 (2025).
 - [8] N. Heurtel, S. Mansfield, J. Senellart, and B. Valiron, Strong simulation of linear optical processes, *Comput. Phys. Commun.* **291**, 108848 (2023).
 - [9] S. Aaronson and D. J. Brod, BosonSampling with lost photons, *Phys. Rev. A* **93**, 012335 (2016).
 - [10] M. Oszmaniec and D. J. Brod, Classical simulation of photonic linear optics with lost particles, *New J. Phys.* **20**, 092002 (2018).
 - [11] A. E. Moylett, R. García-Patrón, J. J. Renema, and P. S. Turner, Classically simulating near-term partially-distinguishable and lossy boson sampling, *Quantum Sci. Technol.* **5**, 015001 (2019).
 - [12] H. Leone, Aquinas, version 1.0, GitHub, <https://github.com/FalafelGood/Aquinas>, accessed 30 August 2024.
 - [13] S. Scheel and S. Y. Buhmann, Macroscopic quantum electrodynamics—concepts and applications, *Acta Phys. Slovaca* **58**, 675 (2008).
 - [14] A. E. Moylett and P. S. Turner, Quantum simulation of partially distinguishable boson sampling, *Phys. Rev. A* **97**, 062329 (2018).
 - [15] D. Bacon, I. L. Chuang, and A. W. Harrow, Efficient quantum circuits for Schur and Clebsch-Gordan transforms, *Phys. Rev. Lett.* **97**, 170502 (2006).
 - [16] N. P. D. Sawaya, T. Menke, T. H. Kyaw, S. Johri, A. Aspuru-Guzik, and G. G. Guerreschi, Resource-efficient digital quantum simulation of d -level systems for photonic, vibrational, and spin- s Hamiltonians, *npj Quantum Inf.* **6**, 49 (2020).
 - [17] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, Optimal design for universal multiport interferometers, *Optica* **3**, 1460 (2016).
 - [18] The reason this unitary was chosen is that it can be expressed as a time-independent Hamiltonian. It is worth noting though that the Clements unitary given in Eq. (7) can be written as a *product* of time-independent Hamiltonians [see Eq. (4.13) in Ref. [25]].

This is needlessly complex for the sake of our example, which is why we use the Eq. (8) unitary instead.

- [19] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2012), 10th anniversary ed.
- [20] A. Hurwitz, Über die Erzeugung der Invarianten durch Integration, *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl.* **1897**, 71 (1897).
- [21] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Experimental realization of any discrete unitary operator, *Phys. Rev. Lett.* **73**, 58 (1994).
- [22] A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. Nation, L. S. Bishop, A. W. Cross, B. R. Johnson, and J. M. Gambetta, Quantum computing with Qiskit, [arXiv:2405.08810](https://arxiv.org/abs/2405.08810).
- [23] D. W. Berry, M. Kieferová, A. Scherer, Y. R. Sanders, G. H. Low, N. Wiebe, C. Gidney, and R. Babbush, Improved techniques for preparing eigenstates of fermionic Hamiltonians, *npj Quantum Inf.* **4**, 22 (2018).
- [24] M. Krishnan Vijayan, A. Paler, J. Gavriel, C. R. Myers, P. P. Rohde, and S. J. Devitt, Compilation of algorithm-specific graph states for quantum circuits, *Quantum Sci. Technol.* **9**, 025005 (2024).
- [25] I. Arrazola, Design of light-matter interactions for quantum technologies, Ph.D. thesis, University of the Basque Country, Leioa, 2020.