LO_v-Calculus: A Graphical Language for Linear Optical Quantum Circuits

Alexandre Clément
Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

Nicolas Heurtel
Quandela, 7 Rue Léonard de Vinci, 91300 Massy, France
Université Paris-Saclay, CentraleSupélec, Inria, CNRS, ENS Paris-Saclay,
Laboratoire Méthodes Formelles, 91190 Gif-sur-Yvette, France

Shane Mansfield
Quandela, 7 Rue Léonard de Vinci, 91300 Massy, France

Simon Perdrix
Inria Mocqua, LORIA, CNRS, Université de Lorraine, F-54000 Nancy, France

Benoît Valiron
Université Paris-Saclay, CentraleSupélec, Inria, CNRS, ENS Paris-Saclay,
Laboratoire Méthodes Formelles, 91190 Gif-sur-Yvette, France

Abstract

We introduce the LO_v-calculus, a graphical language for reasoning about linear optical quantum circuits with so-called vacuum state auxiliary inputs. We present the axiomatics of the language and prove its soundness and completeness: two LO_v-circuits represent the same quantum process if and only if one can be transformed into the other with the rules of the LO_v-calculus. We give a confluent and terminating rewrite system to rewrite any polarisation-preserving LO_v-circuit into a unique triangular normal form, inspired by the universal decomposition of Reck *et al.* (1994) for linear optical quantum circuits.

2012 ACM Subject Classification Theory of computation → Quantum computation theory; Theory of computation → Axiomatic semantics; Hardware → Quantum computation; Hardware → Quantum communication and cryptography

Keywords and phrases Quantum Computing, Graphical Language, Linear Optical Circuits, Linear Optical Quantum Computing, Completeness

Digital Object Identifier 10.4230/LIPIcs.MFCS.2022.35

Related Version *Full Version*: `https://arxiv.org/abs/2204.11787`

Funding This work is funded by ANR-17-CE25-0009 SoftQPro, ANR-17-CE24-0035 VanQuTe, PIA-GDN/Quantex, and LUE / UOQ, the PEPR integrated project EPiQ ANR-22-PETQ-0007 part of Plan France 2030, and by *"Investissements d'avenir"* (ANR-15-IDEX-02) program of the French National Research Agency; the European Project NExt ApplicationS of Quantum Computing (NEASQC), funded by Horizon 2020 Program inside the call H2020-FETFLAG-2020-01(Grant Agreement 951821), and the HPCQS European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101018180.

1 Introduction

Quantum computing and information processing promise a variety of advantages over their classical analogues, from the potential for computational speedups (e.g. [33, 51]) to enhanced security and communication (e.g. [7, 28]). By encoding information into the states of physical systems that are quantum rather than classical, one can then process that information by

47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022).
Editors: Stefan Szeider, Robert Ganian, and Alexandra Silva; Article No. 35; pp. 35:1–35:16
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

evolving and manipulating the systems according to the laws of quantum mechanics. This opens up the possibility of exploiting non-classical behaviours available to quantum systems in order to process information in radically new and potentially advantageous ways.

The development of quantum technologies has proceeded at pace over the past number of years, with a variety of different physical supports for quantum information being pursued. These include matter-based systems like superconducting circuits, cold atoms, and trapped ions, as well as light-based systems, in which information is encoded in photons. Among these, photons have a privileged role in the sense that regardless of hardware choice it will eventually be necessary to network quantum processors, and (as the only sensible support for communicating quantum information) some quantum information will need to be treated photonically. Yet, in their own right, photons also offer viable approaches to quantum computation in the noisy intermediate-scale [40] and large-scale fault-tolerant [6] regimes.

The standard unit of quantum information is the quantum bit or qubit, and photons allow for a rich variety of ways to encode qubits. However it is also interesting to note that treating photons as informational units in their own right can be advantageous. A good example is BosonSampling, originally proposed by Aaronson and Arkhipov [1], a computational task that is $\#P$-hard but which can be efficiently solved by interacting photons in an idealised generic linear-optical circuit in which no qubit encoding need be imposed. At present, along with Random Circuit Sampling [2, 9], this provides one of the two main routes to experimental demonstrations of quantum computational advantage [3, 55, 53, 54], in which quantum devices have been claimed to outperform classical capabilities for specific tasks.

The usual semantics for quantum computation stemming from quantum mechanics is based on unitary matrices (or unitary operators in general) over Hilbert spaces. Although this faithfully models the extensional behaviour of a computation, it fails to address several key aspects that are of interest when considering the design and implementation of quantum algorithms. A first limitation is the intensional description of the computation: an algorithm or quantum computation in general consists of modular components that are composed and combined in specific way, and one wants to keep track of this information. One therefore needs a *language* for coding these. The other important aspect is the need to specify and verify the said code. Indeed, classically simulating a quantum process is a task that is exponentially costly in the size of the system, while running code on physical devices is expensive. If some limited testing techniques are available on quantum systems [29, 43], it is however highly desirable to be able to reason and prove the desired properties of the code upstream, and rely on *formal methods*. If text-based high-level languages oriented towards formal methods have successfully been proposed in the literature [32, 8, 37], we aim in this paper to explore a lower-level, graphical language, making contact with photonic hardware.

Graphical languages for quantum computation have a long history: since Feyman diagrams [30], graphical languages for representing (low-level) quantum processes have been considered as an answer to the limitations of plain unitary matrices. Quantum circuits – the quantum equivalent to classical, boolean circuits – are an obvious candidate for a graphical language, and indeed, several lines of research took them as their main object of study [32, 22, 46, 13]. Quantum circuits in particular form a natural medium for describing the execution flow of a computation. The main problem with the model of quantum circuits is the lack of a satisfactory equational presentation. If several attempts have been made for various subsets [20, 19, 36, 45], none of them provides a complete presentation.

A recent proposal responding to the shortfalls of quantum circuits as a model is the ZX-calculus [21], which, along with its variants [11, 4, 12], have proved to be particularly useful for reasoning about qubit quantum mechanics, for applications such as quantum circuit optimisation [25, 5], verification [26, 31, 35] and representation e.g. for MBQC patterns [27] or error-correction [27, 23]. However, while ZX-calculus is versatile and provides a welcomed formal semantics for quantum computation, it remains at an abstract level.

There is therefore a clear interest in developing a graphical language for quantum photonic processes, especially linear quantum optics, which is closer to photonic hardware and laboratory operations that are easily implementable in bulk optics, fibres, or in integrated photonic circuits. This would provide a more formal counterpart to software frameworks that have been proposed for defining and classically simulating such processes to the extent that it is tractable [39, 34]. The need for such a formal language is also evidenced, for example, by the appeal to diagrams to concisely illustrate equivalent unitaries in recent work in the physics literature [48]. Following on the trend for graphical quantum languages, the PBS-calculus [16, 10, 17] has been proposed as a first step towards an alternative to ZX dedicated to linear quantum optical computation (LOQC). The PBS-calculus makes it possible to reason on a small subset of linear optical components only acting on the polarisation of a photon. While it is enough to describe and analyse non causally-ordered computations, it falls short at expressing other aspects of LOQC typically considered in the physics community, such as the phase. Note that a recent, independent work[1] establishes some connections between the ZX-calculus and the photon preserving fragment of linear optics with multiple photons [24].

Our goal here is to take a more bottom-up approach and to propose a new language which formalises the kinds of diagrammatics that are currently in use in the physics community. In practice this can find many uses including for the design, optimisation, verification, error-correction, and systematic study of linear optical quantum circuits for quantum information.

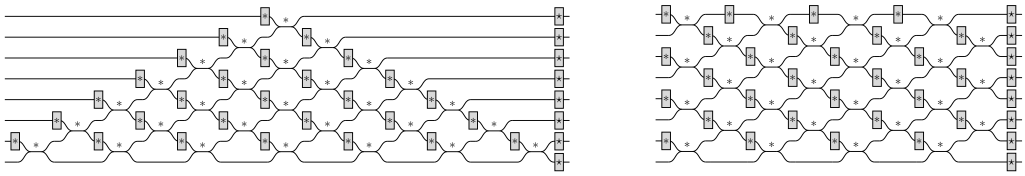
Contributions. Our main contributions are the following.

- A graphical language for LOQC featuring most of the physical apparatuses used in the physics literature. The language comes equipped with an equational theory that is sound and complete with respect to the standard semantics of LOQC.
- A strongly normalising and globally confluent rewrite system and normal form for the polarisation-preserving fragment, for which we recover the Reck *et al.* [49] decomposition as normal form (modulo 0-angled beam splitters and 0-angled phase shifters) with a novel proof of its uniqueness.

Finally, and maybe more importantly, our language makes it possible to formalise and reason within a common framework on various presentations of LOQC stemming from parallel research paths. Our semantics not only allow us to recover, extend and improve on some key results in LOQC such as the universal decompositions of Reck *et al.* [49] and Clements *et al.* [18], but it also gives a unifying language for the different formalisms from the literature. Furthermore, this result paves the way towards the design of complete equational theories for quantum circuits [14].

Plan of the paper. The article is structured as follows. In Section 2, we present the syntax and the semantics of the $\mathrm{LO_v}$-calculus. The equational theory and its soundness are given in Section 3. In Section 4 we present the strongly normalising and globally confluent rewrite system. This allows us to prove the completeness of the $\mathrm{LO_v}$-calculus in Section 5. Finally, we conclude in Section 6. More complete proofs can be found in the appendix of the technical report [15].

[1] The preprint version of [24] has been upladed to arXiv a few days after the one of the present paper [15].



(a) Triangular form [49]. **(b)** Rectangular form [18].

Figure 1 Triangular and rectangular forms for polarisation-preserving circuits.

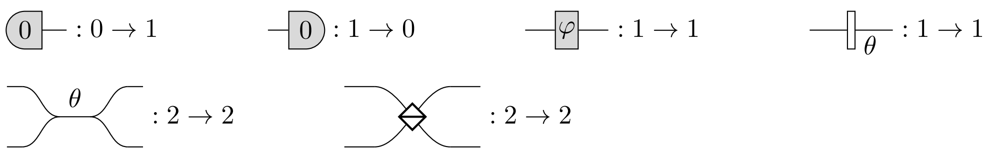
2 Linear Optical Quantum Circuits

A linear optical quantum computation [42, 41] (LOQC) consists of spatial modes through which photons pass – which may be physically instantiated by optical fibers, waveguides in integrated circuits, or simply by paths in free space (bulk optics) – and operations that act on the spatial and polarisation degrees of freedom of the photons, including in particular *beam splitters* ( ), *polarising beam splitters* ( ), *phase shifters* ( ), *wave plates* ( ), *pola-negations* ( ) and finally the *vacuum state sources* and *detectors* (and). Their action and the semantics are described in Section 2.2.

2.1 Syntax

In order to formalise linear optical quantum circuits, we use the formalism of PROPs [44]. A PRO is a strict monoidal category whose monoid of objects is freely generated by a single X: the objects are all of the form $X \oplus ... \oplus X$,[2] and simply denoted by n, the number of occurrences of X. PROs are typically represented graphically as circuits: each copy of X is represented by a wire and morphisms by boxes on wires, so that $\oplus$ is represented vertically and morphism composition "$\circ$" is represented horizontally. For instance, D_1 and D_2 represented as and can be horizontally composed as $D_2 \circ D_1$, represented by , and vertically composed as $D_1 \oplus D_2$, represented by . A PROP is the symmetric monoidal analogue of PRO, so it is equipped with a swap .

▶ **Definition 1.** **LO$_v$** *is the PROP of* LO$_v$*-circuits generated by*



where $\theta, \varphi \in \mathbb{R}$. When the parameters θ and φ are omitted we take them to be equal to $\pi/4$. We write as a shortcut notation for $\frac{\pi}{2}$ $-\frac{\pi}{2}$. The tensor of the monoidal structure is denoted with $\oplus$, and the identity, swap and empty circuit (unit of $\oplus$) are denoted as follows: $: 1 \to 1$, $: 2 \to 2$, $: 0 \to 0$.

▶ **Example 2.** An example of a linear optical quantum circuit using all of the connectives presented in Definition 1 is shown in Figure 2.

[2] Here we denote the monoidal product as $\oplus$ rather than $\otimes$ in order to better correspond to the semantics of LO$_v$-circuits (see Section 2.2).

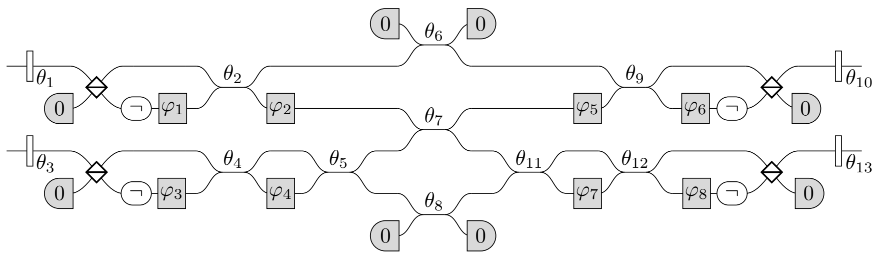


Figure 2 $\mathrm{LO_v}$-circuit implementing a variational quantum eigensolver [47], an algorithm with applications including calculation of ground-state energies in quantum chemistry.

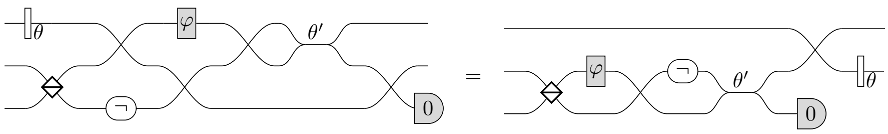
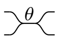


Figure 3 Two equivalent representations of the same $\mathrm{LO_v}$-circuit.

▶ Remark 3. The axioms of PROPs guarantee that linear optical quantum circuits are defined up to deformations: Figure 3 shows two equivalent circuits under the equations of PROPs.

Among the generators, the beam splitters and phase shifters are known to preserve the polarisation of the photons, as a consequence, we define a *polarisation-preserving* sub-PRO of $\mathrm{LO_v}$ as follows.

▶ **Definition 4.** $\mathbf{LO_{PP}}$ *is the PRO of* polarisation-preserving circuits *generated by beam splitters*  *and phase shifters*  *.*

Notice that we define polarisation-preserving circuits as a PRO rather than a PROP, thus they do not include swaps.

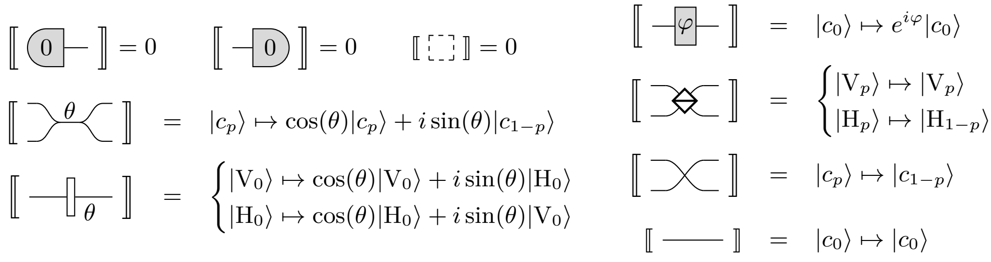
2.2 Single-Photon Semantics

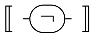
We will characterise photons by their spatial and polarisation modes. Spatial modes refer to position, and polarisation can be horizontal (H) or vertical (V). Note that the quantum formalism admits (normalised complex) superpositions of both spatial and polarisation modes. For any $n \in \mathbb{N}$, let $M_n = \{\mathrm{V}, \mathrm{H}\} \times [n]$, where $[n] = \{0, \dots n-1\}$, be the set of states (spatial and polarisation modes). The elements of M_n are denoted c_p with $c \in \{\mathrm{V}, \mathrm{H}\}$ and $p \in [n]$. The state space of a single photon is $\mathbb{C}^{M_n} = span(|\mathrm{V}_i\rangle, |\mathrm{H}_i\rangle \mid i \in [n])$. Notice that $\mathbb{C}^{M_0} = \mathbb{C}^{\emptyset} = \{0\}$ is the Hilbert space of dimension 0. For instance, on 2 spatial modes (i.e. 2 wires), there are four possible basis states: $\mathrm{H}_0, \mathrm{H}_1, \mathrm{V}_0, \mathrm{V}_1$. Indeed, a photon can be on one of the two wires, while in the horizontal or vertical polarisation. The state space is then a 4-dimensional Hilbert space. The semantics of a $\mathrm{LO_v}$-circuit is defined as follows.

▶ **Definition 5.** *For any* $\mathrm{LO_v}$*-circuit* $D : n \to m$*, let* $[\![D]\!] : \mathbb{C}^{M_n} \to \mathbb{C}^{M_m}$ *be the linear map inductively defined by Table 1*[3]*, and by* $[\![D_2 \circ D_1]\!] = [\![D_2]\!] \circ [\![D_1]\!]$, $[\![D_1 \oplus D_2]\!] = [\![D_1]\!] \oplus [\![D_2]\!]$, *where for all* $f \in \mathbb{C}^{M_n} \to \mathbb{C}^{M_m}$ *and* $g \in \mathbb{C}^{M_{n'}} \to \mathbb{C}^{M_{m'}}$, $(f \oplus g)(|c_k\rangle) = f(|c_k\rangle)$ *if* $k < n$ *and* $S_{m,m'}(g(|c_{k-n}\rangle))$ *if* $k \geq n$*, with* $S_{m,m'} : \mathbb{C}^{M_{m'}} \to \mathbb{C}^{M_{m+m'}} = |c_k\rangle \mapsto |c_{k+m}\rangle$ *a shift of the positions by* m*.*

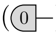
[3] There are many possible conventions for beam splitters. We have chosen this one as it is a symmetric

Table 1 Semantics of LO$_v$-circuits.

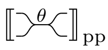


▶ **Example 6.** The negation inverts polarisation:  $: |V_0\rangle \mapsto |H_0\rangle$ and $|H_0\rangle \mapsto |V_0\rangle$.

▶ Remark 7. The semantics of the circuits is sound with respect to the axioms of PROPs. In other words two circuits that are equal up to deformation have the same semantics. More formally, $[\![.]\!] : \mathbf{LO_v} \to (\mathbf{Hilb}, \oplus, 0)$ is a monoidal functor where **Hilb** is the category of state spaces $\mathbb{C}^{M_n}$ and linear maps.

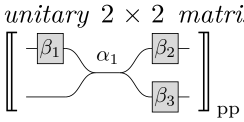
▶ Remark 8. All the generators of the LO$_v$-circuits are photon preserving, even the vacuum state sources () and detectors (). Indeed the vacuum state source produces no photons, whereas the semantics of the detector corresponds to a postselection on the case where no photons are detected.

▶ **Definition 9.** *For any* LO$_{\text{PP}}$*-circuit* $D : n \to n$*, we define* $[\![D]\!]_{\text{pp}} : \mathbb{C}^n \to \mathbb{C}^n$ *as the unique linear map such that* $[\![.]\!] \circ \iota = \iota \circ [\![.]\!]_{\text{pp}}$ *where* $\iota : \mathbb{C}^n \to \mathbb{C}^{M_n} = |k\rangle \mapsto |H_k\rangle$.

For instance  $= \begin{pmatrix} \cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & \cos(\theta) \end{pmatrix}$.

Polarisation-preserving circuits are universal for unitary transformations, this is a direct consequence of the result of Reck *et al.* [49]. Unitary transformations can actually be uniquely represented by LO$_{\text{PP}}$-circuits, as illustrated by the following two cases on 2 and 3 modes, the general case being proved in Section 4.

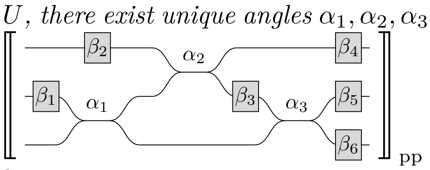
▶ **Lemma 10.** *For any unitary* 2×2 *matrix* U*, there exist unique* $\beta_1, \alpha_1 \in [0, \pi)$ *and* $\beta_2, \beta_3 \in [0, 2\pi)$ *such that*



$= U$*, and* $\alpha_1 \in \{0, \frac{\pi}{2}\} \Rightarrow \beta_1 = 0$.

Proof. The proof is given in [15]. ◀

▶ **Lemma 11.** *For any unitary* 3×3 *matrix* U*, there exist unique angles* $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in [0, \pi)$ *and* $\beta_4, \beta_5, \beta_6 \in [0, 2\pi)$ *such that*



$= U$ *where* $\forall i \in \{1, 2, 3\}, \alpha_i \in \{0, \frac{\pi}{2}\} \Rightarrow \beta_i = 0$*, and where* $\alpha_2 = 0 \Rightarrow \alpha_1 = 0$.

Proof. The existence of such a canonical form is shown in [49]. The uniqueness can then be derived by analysing the possible cases (See [15]). ◀

operation with good composition properties. The convention for the wave plate has been chosen for similar reasons.

LO_v-circuits are more expressive than LO_{PP}-ones, they not only act on the polarisation but the use of detectors and sources allow the representation of non-unitary evolutions: For any LO_v-circuit $D : n \to m$, $[\![D]\!]$ is sub-unitary[4]. LO_v-circuits are actually universal for sub-unitary transformations:

▶ **Theorem 12** (Universality of LO_v). *For every sub-unitary map $U : \mathbb{C}^{M_n} \to \mathbb{C}^{M_m}$ (i.e. such that $U^\dagger U \sqsubseteq I$) there exists a diagram $D : n \to m$ s.t. $[\![D]\!] = U$.*

Proof. The proof given in [15] relies on the normal forms developed in Section 5. ◀

3 Equational Theory

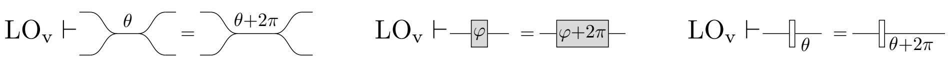
Two distinct LO_v-circuits may represent the same quantum evolution: for instance, composing two negations is equivalent to the identity. In order to characterise equivalences of LO_v-circuits, we introduce a set of equations, shown in Figure 4. They capture basic properties of LO_v-circuits, such as: detectors and sources essentially absorbing the other generators (Equations (9) to (12)); parameters forming a monoid (Equations (1) and (2)); and various commutation properties (Equations (15), (16)). Notice that there are two equations acting on 3 modes: Equation (6) and Equation (18). Equation (6) is a variant of the Yang-Baxter Equation [38], whereas Equation (18) is a property of decompositions into Euler angles. Indeed, in 3-dimensional space, the two sides of this equation correspond to two distinct decompositions in elementary rotations.

▶ **Definition 13** (LO_v-calculus). *Two LO_v-circuits D_1, D_2 are equivalent according to the rules of the LO_v-calculus, denoted $LO_v \vdash D_1 = D_2$, if one can transform D_1 into D_2 using the equations given in Figure 4. More precisely, $LO_v \vdash \cdot = \cdot$ is defined as the smallest congruence which satisfies the equations of Figure 4 in addition to the axioms of PROP.*

▶ **Proposition 14** (Soundness). *For any two LO_v-circuits D_1 and D_2, if $LO_v \vdash D_1 = D_2$ then $[\![D_1]\!] = [\![D_2]\!]$.*

Proof. Since semantic equality is a congruence it suffices to check that for every equation of Figure 4 both sides have the same semantics, which follows from Definition 5 and Lemma 11. ◀

▶ **Proposition 15.** *The rules of the LO_v-calculus imply that the parameters are 2π-periodic, i.e. for any $\theta, \varphi \in \mathbb{R}$:*



Proof. The proof is given in [15]. ◀

We now state one of our main results: the completeness of the LO_v-calculus.

▶ **Theorem 16** (Completeness). *For any two LO_v-circuits D_1 and D_2, if $[\![D_1]\!] = [\![D_2]\!]$ then $LO_v \vdash D_1 = D_2$.*

The proof of Theorem 16 is given in Section 5. As a step towards proving the theorem, we first consider the fragment of the LO_{PP}-circuits.

[4] U is sub-unitary (see for instance [50]) iff $U^\dagger U \sqsubseteq I$, where $\sqsubseteq$ is the Löwner partial order, i.e. $I - U^\dagger U$ is a positive semi-definite.

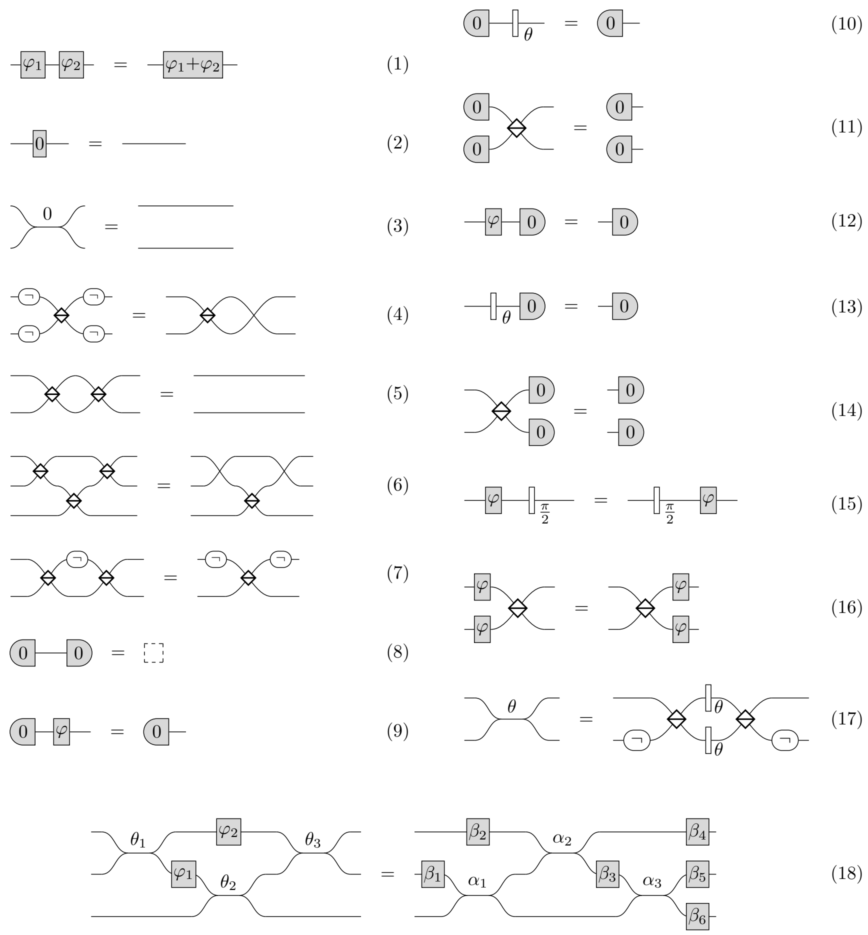


Figure 4 Axioms of the LO$_v$-calculus. The equations are valid for arbitrary parameters $\varphi, \varphi_i, \theta, \theta_i \in \mathbb{R}$. In Equation (18), the angles on the left-hand side can take any value while the right-hand side is given by Lemma 11 (where U is the $[\![.]\!]_{pp}$-semantics of the left-hand side of the equation).

4 Polarisation-Preserving Circuits

This section gives a universal normal form for any LO$_{PP}$-circuit. We prove the uniqueness of that form by introducing a strongly normalising and confluent polarisation-preserving rewrite system: PPRS.

▶ **Definition 17.** *The rewrite system* PPRS *is defined on* LO$_{PP}$*-circuits with the rules of Figure 5.*

▶ **Lemma 18.** *If D_1 rewrites to D_2 using the* PPRS *rewrite system then* LO$_v$ $\vdash D_1 = D_2$*.*

Proof. The proof is given in [15]. ◀

▶ **Theorem 19.** *The rewrite system* PPRS *is strongly normalising.*

Proof. The proof is done by defining a lexicographic order on six distinct values: numbers of beam splitters of various angle ranges, count of specific patterns, numbers and positions of phase shifters. The order is shown to be decreasing with respect to the rewrite rules of PPRS. The complete proof is given in [15]. ◀

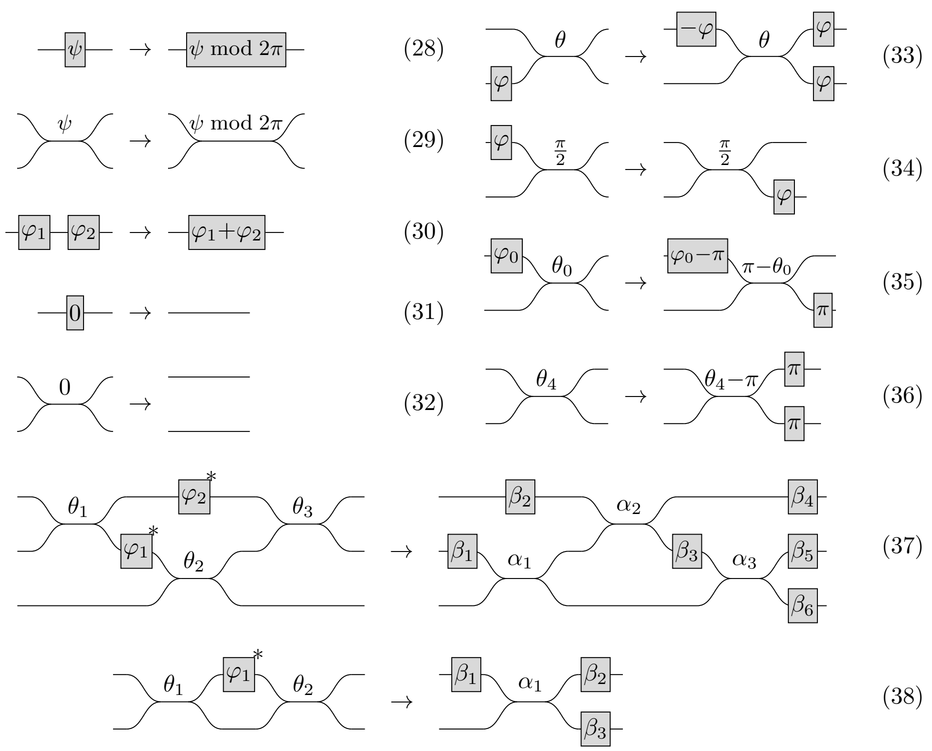


Figure 5 Rewriting rules of PPRS. $\psi \in \mathbb{R} \setminus [0, 2\pi)$, $\varphi, \varphi_1, \varphi_2 \in (0, 2\pi)$, $\varphi_0, \theta_4 \in [\pi, 2\pi)$, $\theta, \theta_0, \theta_1, \theta_2, \theta_3 \in (0, \pi)$, and $\theta_0 \neq \frac{\pi}{2}$. φ^* denotes either φ or ——. In Rules (37) and (38), the angles on the left-hand side can take any value while the right-hand side is given by Lemma 11 and Lemma 10 respectively.

As PPRS is terminating, we can therefore derive the existence of normal forms. The next step is to show that these normal forms are unique: this is derived from Theorem 20.

▶ **Theorem 20.** PPRS *is globally confluent.*

Proof. PPRS is locally confluent. Indeed, one can show by case analysis that the non-trivial peaks all use at most three wires. Each peak can be closed since for any polarisation-preserving $\mathrm{LO_v}$-circuit of size $n \in \{1, 2, 3\}$, PPRS terminates to a specific unique normal form: when $n = 1$, a simple phase-shift; when $n = 2$, the form shown in Lemma 10; when $n = 3$, the form shown in Lemma 11. See [15] for details. Finally, using Theorem 19, global confluence is deduced from Newman's lemma [52]. ◀

▶ **Definition 21.** *A* PPRS triangular normal form *is a circuit with a triangular shape similar to Figure 1a, but with all* 0*-angled generators replaced with identities and with additional conditions on the angles, as described in Figure 6.*

Figure 7 shows an example: the figure on the left is the "full" circuit with 0-angled beam splitters while on the right is the corresponding PPRS triangular normal form.

▶ **Lemma 22.** *Any irreducible* $\mathrm{LO_{PP}}$*-circuit is a PPRS triangular normal form.*

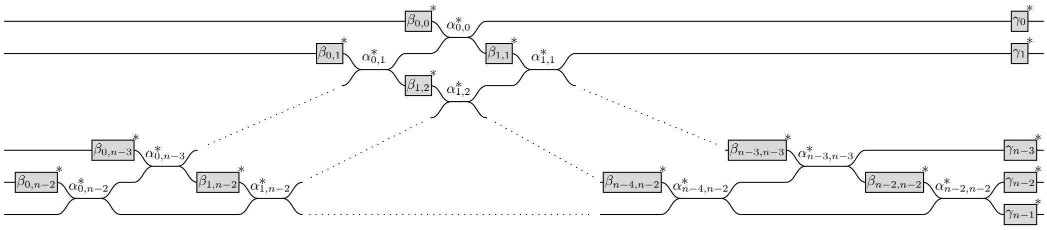


Figure 6 General scheme of a PPRS triangular normal form. The stars mean that any phase shifter or beam splitter with angle 0 is replaced by the identity. The conditions on the angles are the following: $\alpha_{i,j}, \beta_{i,j} \in [0, \pi)$; $\gamma_i \in [0, 2\pi)$; $\alpha_{i,j} = 0 \Rightarrow \forall j' > j, \alpha_{i,j'} = 0$; $\alpha_{i,j} \in \{0, \frac{\pi}{2}\} \Rightarrow \beta_{i,j} = 0$.

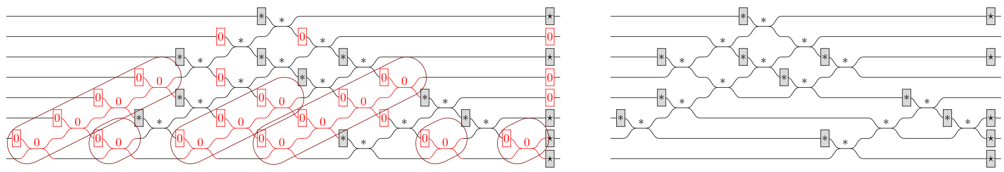


Figure 7 An example of a PPRS triangular normal form. In the figure on the left, the beam splitters and phase shifters with angle 0 in the corresponding triangular form are shown in red. In the figure on the right, they are replaced with identities.

Proof. This property can be proven by induction. First, we lay out the properties of any irreducible circuit that can be directly deduced from the PPRS rules of Figure 5. Then, we give two more properties characterising the PPRS triangular normal forms. By induction, we prove that any irreducible circuit respects those two properties, so that any irreducible circuit is a PPRS triangular normal form. See [15] for more details. ◀

▶ **Theorem 23.** *Any* LO$_{\text{PP}}$*-circuit, with the rules of* PPRS*, converges to a unique* PPRS *triangular normal form.*

Proof. PPRS is globally confluent and terminating: normal forms are unique. From Lemma 22, PPRS triangular normal forms are the only irreducible forms. Therefore, any polarisation-preserving circuit terminates to such a unique normal form. ◀

▶ Remark 24. In particular by using Equation (18) and by adding 0-angled beam splitters if necessary, one can turn any circuit in PPRS triangular normal form into a circuit in the rectangular form of [18] shown in Figure 1b. A schematic example of such a transformation is shown in [15].

We can now prove the completeness of the polarisation-preserving fragment.

▶ **Theorem 25.** *For any* LO$_{\text{PP}}$*-circuits* C_1,C_2 *such that* $[\![C_1]\!]_{\text{pp}} = [\![C_2]\!]_{\text{pp}}$*, their normal forms are equal, i.e.* $N_1 = N_2$*, where* N_1 *(resp.* N_2*) is the unique normal form of* C_1 *(resp.* C_2*) given by Theorem 23.*

Proof. As the rewrite system preserves the semantics, it is sufficient to prove that $[\![N_1]\!]_{\text{pp}} = [\![N_2]\!]_{\text{pp}} \Rightarrow N_1 = N_2$. First, we can show by induction that $[\![N]\!]_{\text{pp}} = [\![I_n]\!]_{\text{pp}} \Rightarrow N = I_n$. Indeed, to have the semantics as the identity, we can show the upper beam splitter and phase shifters are necessarily 0-angled. The proof follows from induction, details are given in [15]. Let P be an inverse circuit of N_1 and N_2, that is, a polarisation-preserving circuit such that $[\![P]\!]_{\text{pp}} = [\![N_1]\!]_{\text{pp}}^{-1}$. The existence of such a circuit follows from [49]. As $[\![N_1 P]\!]_{\text{pp}} = [\![P N_2]\!]_{\text{pp}} = [\![I_n]\!]_{\text{pp}}$, the term $N_1 P N_2$ can both be reduced to N_1 (by reducing $P N_2$ first) and N_2 (by reducing $N_1 P$ first). By Theorem 23, $N_1 = N_2$. ◀

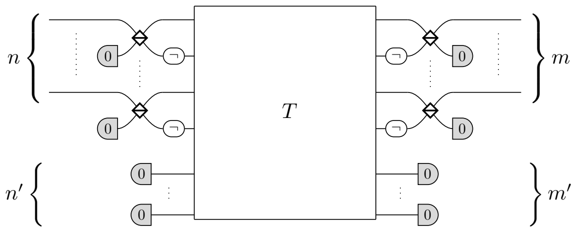


Figure 8 Shape of a circuit in normal form as of Definition 27.

▶ **Proposition 26** (Universality and uniqueness in the polarisation-preserving fragment)**.** *For any unitary* $U\colon \mathbb{C}^n \to \mathbb{C}^n$*, there exists a unique circuit* T *in* PPRS *triangular normal form such that* $[\![T]\!]_{\mathrm{pp}} = U$*.*

Proof. This follows directly from [49], Theorems 23 and 25 and the fact that all PPRS triangular normal forms are irreducible. ◀

5 Completeness of the $\mathrm{LO_v}$-Calculus

To prove the completeness of the $\mathrm{LO_v}$-Calculus (Theorem 16), we introduce the following notion of normal form.

▶ **Definition 27** (Normal form)**.** *A circuit in normal form* $N : n \to m$ *is a circuit of the form shown in Figure 8, where* T *is a PPRS triangular normal form (Definition 21). If* $n' = m' = 0$*, then* N *is said to be in* pure normal form.

▶ **Lemma 28** (Uniqueness of the pure normal form)**.** *If two circuits* N_1 *and* N_2 *in pure normal form are such that* $[\![N_1]\!] = [\![N_2]\!]$*, then* $N_1 = N_2$*.*

Proof. Let T_1 (resp. T_2) be the $\mathrm{LO_{PP}}$-circuit associated with N_1 (resp N_2) as in Figure 8. Notice that $[\![T_i]\!]_{\mathrm{pp}} \circ \mu = \mu \circ [\![N_i]\!]$ where $\mu : \mathbb{C}^{M_n} \to \mathbb{C}^{2n}$ is the isomorphism $|\mathrm{V}_k\rangle \mapsto |2k\rangle$ and $|\mathrm{H}_k\rangle \mapsto |2k+1\rangle$. Thus $[\![N_1]\!] = [\![N_2]\!]$ implies $[\![T_1]\!]_{\mathrm{pp}} = [\![T_2]\!]_{\mathrm{pp}}$ so that the result follows from Theorem 23. ◀

▶ **Lemma 29.** *For any circuit* D *without vacuum state sources or detectors there exists a circuit in pure normal form* N *such that* $\mathrm{LO_v} \vdash D = N$*.*

Proof. The proof is given in [15]. ◀

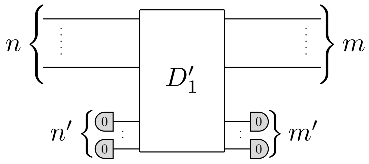
Completeness for circuits without vacuum state sources or detectors follows directly from Lemmas 28 and 29:

▶ **Proposition 30.** *Given any two circuits* D_1 *and* D_2 *without any* (0)– *or* –(0)*, if* $[\![D_1]\!] = [\![D_2]\!]$ *then* $\mathrm{LO_v} \vdash D_1 = D_2$*.*

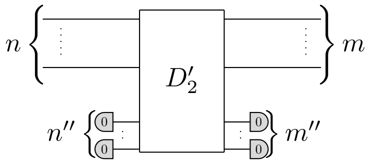
Proof. By Lemma 29, there exist two circuits in pure normal form N_1 and N_2 such that $\mathrm{LO_v} \vdash D_1 = N_1$ and $\mathrm{LO_v} \vdash D_2 = N_2$. By Proposition 14, one has $[\![N_1]\!] = [\![D_1]\!] = [\![D_2]\!] = [\![N_2]\!]$, so that by Lemma 28, $N_1 = N_2$. The result follows by transitivity. ◀

Proof of Theorem 16

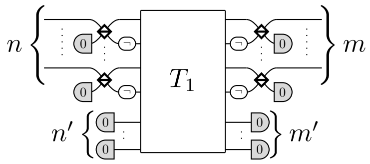
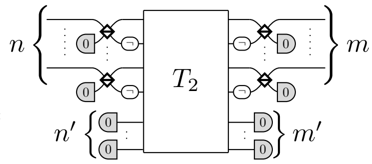
We now have the required material to to finish the proof of Theorem 16. Let $D_1, D_2 : n \to m$ be any two LO$_\mathrm{v}$-circuits such that $[\![D_1]\!] = [\![D_2]\!]$. By deformation, we can write them as



and



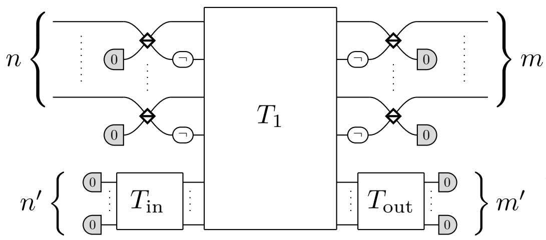
where D_1', D_2' do not contain (0)— or —(0). Up to using Equation (8), we can assume that $n'' = n'$. Since circuits without vacuum state sources and detectors necessarily have the same number of input wires as of output wires, this implies that $m'' = m'$. By Lemma 29, we can put D_1' and D_2' in pure normal form. Then by using Equations (9)–(14), we get two circuits in normal form

$D_1^{\mathrm{NF}} =$  and $D_2^{\mathrm{NF}} =$ 

with T_1 and T_2 in PPRS triangular normal form.

$[\![D_1]\!] = [\![D_2]\!]$ implies that $\pi \circ [\![T_1]\!]_{\mathrm{pp}} \circ \iota = \pi \circ [\![T_2]\!]_{\mathrm{pp}} \circ \iota$ where $\iota : \mathbb{C}^{2n} \to \mathbb{C}^{2n+n'}$ is the injection $|k\rangle \mapsto |k\rangle$ and $\pi : \mathbb{C}^{2m+m'} \to \mathbb{C}^{2m}$ is the projector s.t. $\pi|k\rangle = |k\rangle$ when $k < 2m$ and $\pi|k\rangle = 0$ otherwise. Thus there exists two unitaries Q, Q' s.t. $[\![T_2]\!]_{\mathrm{pp}} = (I \oplus Q') \circ [\![T_1]\!]_{\mathrm{pp}} \circ (I \oplus Q)$ (see [15]).

By Proposition 26, there exist two circuits T_{in} and T_{out} in PPRS triangular normal form such that $[\![T_{\mathrm{in}}]\!]_{\mathrm{pp}} = Q$ and $[\![T_{\mathrm{out}}]\!]_{\mathrm{pp}} = Q'$. Using the equational theory we can then make T_{in} and T_{out} appear, turning D_1^{NF} into



.

Since by construction, the middle part has the same single-photon semantics as T_2, by Proposition 30 we can transform it into T_2 using the axioms of the LO$_\mathrm{v}$-calculus, which means transforming D_1^{NF} into D_2^{NF}. The result follows by transitivity. ◀

6 Conclusion

In this paper, we presented the LO$_\mathrm{v}$-calculus, a graphical language for LOQC capturing most of the components typically considered in the physics community for linear optical quantum circuits. The language comes equipped with a sound and complete semantics, and we discussed how it provides a unifying framework for many of the existing approaches in the literature. We explained how several existing results can be ported in the LO$_\mathrm{v}$ framework.

An obvious direction for future work is to extend the language to allow for sources and detectors of a non-zero number of photons. A more exploratory research avenue is to add support for features such as squeezed states or continuous variables.

References

1 Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 9(4):143–252, 2013. doi:10.4086/toc.2013.v009a004.

2 Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments, 2016. arXiv:1612.05903.

3 Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

4 Miriam Backens and Aleks Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity. *Electronic Proceedings in Theoretical Computer Science*, 287:23–42, 2019.

5 Miriam Backens, Hector Miller-Bakewell, Giovanni de Felice, Leo Lobski, and John van de Wetering. There and back again: A circuit extraction tale. *Quantum*, 5:421, 2021.

6 Sara Bartolucci, Patrick Birchall, Hector Bombin, Hugo Cable, Chris Dawson, Mercedes Gimeno-Segovia, Eric Johnston, Konrad Kieling, Naomi Nickerson, Mihir Pant, Fernando Pastawski, Terry Rudolph, and Chris Sparro. Fusion-based quantum computation, 2021. arXiv:2101.09310.

7 Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. doi:10.1016/j.tcs.2014.05.025.

8 Benjamin Bichsel, Maximilian Baader, Timon Gehr, and Martin T. Vechev. Silq: a high-level quantum language with safe uncomputation and intuitive semantics. In Alastair F. Donaldson and Emina Torlak, editors, *Proceedings of the 41st ACM SIGPLAN International Conference on Programming Language Design and Implementation, PLDI'20*, pages 286–300. ACM, 2020. doi:10.1145/3385412.3386007.

9 Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15(2):159–163, 2019. doi:10.1038/s41567-018-0318-2.

10 Cyril Branciard, Alexandre Clément, Mehdi Mhalla, and Simon Perdrix. Coherent control and distinguishability of quantum channels via PBS-diagrams. In Filippo Bonchi and Simon J. Puglisi, editors, *Proceedings of the 46th International Symposium on Mathematical Foundations of Computer Science, MFCS 2021*, volume 202 of *LIPIcs*, pages 22:1–22:20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2021. doi:10.4230/LIPIcs.MFCS.2021.22.

11 Titouan Carette, Dominic Horsman, and Simon Perdrix. SZX-calculus: Scalable graphical quantum reasoning. In Peter Rossmanith, Pinar Heggernes, and Joost-Pieter Katoen, editors, *Proceedings of the 44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019*, volume 138 of *LIPIcs*, pages 55:1–55:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.MFCS.2019.55.

12 Titouan Carette, Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Completeness of graphical languages for mixed states quantum mechanics. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming, ICALP 2019*, volume 132 of *LIPIcs*, pages 108:1–108:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.ICALP.2019.108.

13 Christophe Chareton, Sébastien Bardin, François Bobot, Valentin Perrelle, and Benoît Valiron. An automated deductive verification framework for circuit-building quantum programs. In Nobuko Yoshida, editor, *Programming Languages and Systems*, volume 12648 of *Lecture Notes in Computer Science (LNCS)*, pages 148–177, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-72019-3_6.

14 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. A complete equational theory for quantum circuits, 2022. doi:10.48550/ARXIV.2206.10577.

15 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. LOv-calculus: A graphical language for linear optical quantum circuits, 2022. arXiv:2204.11787.

16 Alexandre Clément and Simon Perdrix. PBS-calculus: A graphical language for coherent control of quantum computations. In Javier Esparza and Daniel Kráľ, editors, *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, volume 170 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:14, Dagstuhl, Germany, August 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.MFCS.2020.24.

17 Alexandre Clément and Simon Perdrix. Minimising resources of coherently controlled quantum computations, 2022. Accepted at MFCS 2022. arXiv:2202.05260.

18 William R. Clements, Peter C. Humphreys, Benjamin J. Metcalf, W. Steven Kolthammer, and Ian A. Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, December 2016. doi:10.1364/OPTICA.3.001460.

19 Robin Cockett and Cole Comfort. The category TOF. In Peter Selinger and Giulio Chiribella, editors, *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018*, volume 287 of *EPTCS*, pages 67–84, 2019.

20 Robin Cockett, Cole Comfort, and Priyaa Srinivasan. The category CNOT. In Peter Selinger and Giulio Chiribella, editors, *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018*, volume 287 of *EPTCS*, pages 258–293, 2019. doi:10.4204/EPTCS.266.18.

21 Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017. doi:10.1017/9781316219317.

22 Ugo Dal Lago, Claudia Faggian, Benoît Valiron, and Akira Yoshimizu. The geometry of parallelism: Classical, probabilistic, and quantum effects. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages*, POPL 2017, pages 833–845, New York, NY, USA, 2017. Association for Computing Machinery. doi:10.1145/3009837.3009859.

23 Niel de Beaudrap and Dominic Horsman. The ZX calculus is a language for surface code lattice surgery. *Quantum*, 4:218, 2020. arXiv:1704.08670.

24 Giovanni de Felice and Bob Coecke. Quantum linear optics via string diagrams, 2022. arXiv:2204.12985.

25 Ross Duncan, Aleks Kissinger, Simon Perdrix, and John Van De Wetering. Graph-theoretic simplification of quantum circuits with the ZX-calculus. *Quantum*, 4:279, 2020.

26 Ross Duncan and Maxime Lucas. Verifying the Steane code with Quantomatic. In Bob Coecke and Matty J. Hoban, editors, *Proceedings of the 10th International Workshop on Quantum Physics and Logic, QPL 2013*, volume 171 of *EPTCS*, pages 33–49, 2013. doi:10.4204/EPTCS.171.4.

27 Ross Duncan and Simon Perdrix. Rewriting measurement-based quantum computations with generalised flow. In *International Colloquium on Automata, Languages, and Programming*, pages 285–296. Springer, 2010.

28 Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, August 1991. doi:10.1103/PhysRevLett.67.661.

29 Yuan Feng, Ernst Moritz Hahn, Andrea Turrini, and Lijun Zhang. QPMC: a model checker for quantum programs and protocols. In Nikolaj Bjørner and Frank S. de Boer, editors, *Proceedings of the 20th International Symposium on Formal Methods (FM 2015)*, volume 9109 of *Lecture Notes in Computer Science*, pages 265–272. Springer, 2015. doi:10.1007/978-3-319-19249-9_17.

30 Richard P. Feynman and Albert R. Hibbs. *Quantum Mechanics and Path Integrals*. McGraw-Hill Publishing Company, 1965.

31 Liam Garvie and Ross Duncan. Verifying the smallest interesting colour code with quantomatic. *Electronic Proceedings in Theoretical Computer Science, EPTCS*, 266:147–163, 2018.

32 Alexander S. Green, Peter LeFanu Lumsdaine, Neil J. Ross, Peter Selinger, and Benoît Valiron. Quipper: A scalable quantum programming language. In Hans-Juergen Boehm and Cormac Flanagan, editors, *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI'13*, pages 333–342. ACM, 2013. `doi:10.1145/2491956.2462177`.

33 Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. Association for Computing Machinery. `doi:10.1145/237814.237866`.

34 Nicolas Heurtel, Andreas Fyrillas, Grégoire de Gliniasty, Raphaël Le Bihan, Sébastien Malherbe, Marceau Pailhas, Boris Bourdoncle, Pierre-Emmanuel Emeriau, Rawad Mezher, Luka Music, et al. Perceval: A software platform for discrete variable photonic quantum computing, 2022. `arXiv:2204.00602`.

35 Anne Hillebrand. *Quantum Protocols involving Multiparticle Entanglement and their Representations in the zx-calculus.* PhD thesis, University of Oxford, 2011.

36 Christian Hutslar, Jacques Carette, and Amr Sabry. A library of reversible circuit transformations (work in progress). In Jarkko Kari and Irek Ulidowski, editors, *Proceedings of the 10th International Conference on Reversible Computation, RC 2018*, volume 11106 of *Lecture Notes in Computer Science*, pages 339–345. Springer, 2018. `doi:10.1007/978-3-319-99498-7_24`.

37 Ali Javadi-Abhari, Shruti Patil, Daniel Kudrow, Jeff Heckey, Alexey Lvov, Frederic T. Chong, and Margaret Martonosi. ScaffCC: Scalable compilation and analysis of quantum programs. *Parallel Computing*, 45:2–17, 2015. `doi:10.1016/j.parco.2014.12.001`.

38 Michio Jimbo. Introduction to the Yang-Baxter equation. *International Journal of Modern Physics A*, 4(15):3759–3777, 1989.

39 Nathan Killoran, Josh Izaac, Nicolás Quesada, Ville Bergholm, Matthew Amy, and Christian Weedbrook. Strawberry fields: A software platform for photonic quantum computing. *Quantum*, 3:129, 2019.

40 Emanuel Knill, Raymond Laflamme, and Gerald J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001. `doi:10.1038/35051009`.

41 Pieter Kok and Brendon W. Lovett. *Introduction to Optical Quantum Information Processing.* Cambridge University Press, 2010.

42 Pieter Kok, William J. Munro, Kae Nemoto, Timothy C. Ralph, Jonathan P. Dowling, and Gerald J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79:135–174, January 2007. `doi:10.1103/RevModPhys.79.135`.

43 Gushu Li, Li Zhou, Nengkun Yu, Yufei Ding, Mingsheng Ying, and Yuan Xie. Projection-based runtime assertions for testing and debugging quantum programs. *Proceedings of the ACM on Programming Languages*, 4(OOPSLA):150:1–150:29, 2020. `doi:10.1145/3428218`.

44 Saunders MacLane. Categorical algebra. *Bulletin of the American Mathematical Society*, 71(1):40–106, 1965. `doi:bams/1183526392`.

45 Justin Makary, Neil J. Ross, and Peter Selinger. Generators and relations for real stabilizer operators. In Chris Heunen and Miriam Backens, editors, *Proceedings of hte 18th International Conference on Quantum Physics and Logic, QPL 2021*, volume 343 of *EPTCS*, pages 14–36, 2021. `doi:10.4204/EPTCS.343.2`.

46 Jennifer Paykin, Robert Rand, and Steve Zdancewic. QWIRE: a core language for quantum circuits. In Giuseppe Castagna and Andrew D. Gordon, editors, *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages, POPL'17*, pages 846–858. ACM, 2017. `doi:10.1145/3009837.3009894`.

47 Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, and Jeremy L O'brien. A variational eigenvalue solver on a photonic quantum processor. *Nature communications*, 5(1):1–7, 2014.

48 Mathias Pont, Riccardo Albiero, Sarah E. Thomas, Nicolò Spagnolo, Francesco Ceccarelli, Giacomo Corrielli, Alexandre Brieussel, Niccolo Somaschi, Hêlio Huet, Abdelmounaim Harouri, Aristide Lemaître, Isabelle Sagnes, Nadia Belabas, Fabio Sciarrino, Roberto Osellame, Pascale Senellart, and Andrea Crespi. Quantifying n-photon indistinguishability with a cyclic integrated interferometer, 2022. arXiv:2201.13333.

49 Michael Reck, Anton Zeilinger, Herbert J. Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73:58–61, July 1994. doi:10.1103/PhysRevLett.73.58.

50 Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004. doi:10.1017/S0960129504004256.

51 Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. doi:10.1109/SFCS.1994.365700.

52 Terese. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2003.

53 Yulin Wu, Wan-Su Bao, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, et al. Strong quantum computational advantage using a superconducting quantum processor. *Physical Review Letters*, 127(18):180501, 2021.

54 Han-Sen Zhong, Yu-Hao Deng, Jian Qin, Hui Wang, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Dian Wu, Si-Qiu Gong, Hao Su, et al. Phase-programmable Gaussian boson sampling using stimulated squeezed light. *Physical Review Letters*, 127(18):180502, 2021.

55 Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.