A Complete Equational Theory for Quantum Circuits

Abstract—We introduce the first complete equational theory for quantum circuits. More precisely, we introduce a set of circuit equations that we prove to be sound and complete: two circuits represent the same unitary map if and only if they can be transformed one into the other using the equations. The proof is based on the properties of multi-controlled gates — that are defined using elementary gates — together with an encoding of quantum circuits into linear optical circuits, which have been proved to have a complete axiomatisation.

I. INTRODUCTION

Quantum computation is the art of manipulating the states of objects governed by the laws of quantum physics in order to perform computation. The standard model for quantum computation is the quantum co-processor model: an auxiliary device, hosting a quantum memory. This co-processor is then interfaced with a classical computer: the classical computer sends the co-processor a series of instructions to update the state of the memory. The standard formalism for these instructions is the circuit model [1]. Akin to boolean circuits, in quantum circuits wires represent quantum bits and boxes elementary operations — quantum gates. The mathematical model is however very different: quantum bits (qubits) correspond to vectors in a 2-dimensional Hilbert space, gates to unitary maps and parallel composition to the tensor product — the Kronecker product.

Quantum circuits currently form the de facto standard for representing low-level, logical operations on a quantum memory. They are used for everything: resource estimation [2], optimization [3]–[8], satisfaction of hardware constraints [9], [10], etc.

However, as ubiquitous to quantum computing as they are, the graphical language of quantum circuits has never been fully formalised. In particular, a complete equational theory has been a longstanding open problem for 30 years [11]. It would make it possible to directly prove properties such as circuit equivalence without having to rely on ad-hoc set of equations. So far, complete equational theories were only known for non-universal fragments, such as circuits acting on at most two qubits [12], [13], the stabilizer fragment [14], [15], the CNot-dihedral fragment [16], or fragments of reversible circuits [17]–[19].

Interestingly enough, other diagrammatic languages for quantum computation have been developed on sound foundations: it is reasonable to think that this could help in developing a complete equational theory for circuits. Arguably the strongest candidate has been the ZX-calculus [20], [21], equipped with complete equational theories [23]–[27]. The ZX-calculus shares the same underlying mathematical representation for states: wires corresponds to Hilbert spaces and parallel composition to the tensor operation. Nonetheless, the completeness of the ZX-calculus does not lead a priori to a complete equational theory for quantum circuits. The reason lies in the expressiveness of the ZX-calculus and the non-unitarity of some of its generators. Any quantum circuit can be straightforwardly seen as a ZX-diagram. On the other hand, a ZX-diagram does not necessarily represent a unitary map, and even when it does, extracting a corresponding quantum circuit is known to be a hard task in general [4], [28].

Another example of a quantum language with a complete equational theory is the LOv-calculus, a language for linear optical quantum circuits for which a simple complete equational theory has recently been introduced [29]. While both linear optical and regular quantum circuits are universal for unitary transformations, they do not share the same structure. In particular, if the parallel composition of quantum circuits corresponds to the tensor product, for linear optical circuits it stands for the direct sum.

In this paper, we introduce the first complete equational theory for quantum circuits, by first closing the gap between regular and linear optical quantum circuits. Despite the seemingly incompatible approaches to parallel composition, our completeness result derives from the completeness result for linear optical circuits. Indeed, unlike ZX-generators, linear optical components are unitary, making it possible to write a translation in both directions.

The complete equational theory for quantum circuits is derived from the completeness of the LOv-calculus as follows: equipped with maps for encoding (from quantum circuits to linear optical circuits) and decoding (from linear optical circuits to quantum circuits), one can roughly speaking prove completeness for quantum circuits as long as their equational theory is powerful enough to derive a finite number of equations, those corresponding to the decoding of the equations of the complete equational theory for linear optical circuits.

Due to the difference in its interpretation in both kinds of circuits, the parallel composition is not preserved by the encoding nor the decoding maps. The translations are actually based on a sequentialisation of circuits, since the translation of a local gate (acting on at most two wires) is translated as a piece of circuit acting potentially on all wires. Technically, it

1or its variants like ZH [22] and ZW [23], sharing several similar properties.
forces to work with a raw version of circuits, as a circuit may lead to a priori distinct translations depending on the choice of the serialisation. Moreover, a single linear optical gate like a phase shifter (which consists in applying a phase on a particular basis state) is decoded as a piece of circuits that can be interpreted as a multi-controlled gate acting on all qubits. As we choose to stick with the usual generators of quantum circuits acting on at most two qubits, multi-controlled gates are inductively defined and we introduce an equational theory powerful enough to prove the basic algebra of multi-controlled gates, necessary to finalise the proof of completeness. The paper is structured as follows. We first introduce a set of structural relations for quantum circuits generated by the standard elementary gates: Hadamard, Phase-rotations, and CNot. We define multi-controlled gates using these elementary gates, and show that the basic algebra of multi-controlled gates can be derived from the structural relations. In addition to the structural equations, we introduce Euler-angle-based equations. We then proceed to the proof of completeness, based on a back-and-forth translation from quantum circuits to linear optical circuits.

More complete proofs can be found in the appendix of the preprint version of the paper [30].

II. QUANTUM CIRCUITS

In quantum computation, circuits – such as quantum circuits or optical quantum circuits – are graphical descriptions of quantum processes. Akin to (conventional) boolean circuits, circuits in quantum computations are built from wires (oriented from left to right), representing the flow of information, and gates, representing operations to update the state of the system. Every circuit comes with a set of input wires (incoming the circuit from the left) and a set of output wires (exiting the circuit on the right).

A. Graphical languages

To provide a formal definition of circuits, we first use the notion of raw circuits. Given a set of generators, one can generate a raw circuit by means of iterative sequential (⊗) and parallel (⊕) compositions. For instance, given the elementary gates [QWH] and [PH/π/2] (with one input and one output) and [QWH/π/2] (with two inputs and two outputs), one can construct the raw circuit \[\text{QWH} \circ (\text{QWH} \otimes \text{PH/π/2}) \circ \text{QWH}.\] Notice that a sequential composition C' \circ C requires that the number of outputs of C' matches the number of inputs of C'. This raw circuit can be depicted by gluing the generators together and using boxes to witness how the generators have been composed:

To avoid the use of boxes and recover the intuitive notion of circuits, we formally define circuits as a prop [32], which consists in considering the raw circuits up to the rules given in Figure 1. More precisely, a prop generated by a set G of elementary gates is the collection of raw circuits generated by G \cup \{\text{CNOT}, \text{SWAP}, \text{Z}, \emptyset\} quotiented by the equations of Figure 1.

The use of the prop formalism guarantees that circuits can be depicted graphically without ambiguity. Circuits are thus defined up to deformations, as for instance:

\[\text{QWH} \circ (\text{QWH} \otimes \text{PH/π/2}) \circ \text{QWH}.\]

B. Quantum circuits: Syntax and semantics

We consider quantum circuits defined on the following standard set of generators: Hadamard, Control-Not, and Phase-gates together with global phases.

Definition 1. Let QC be the prop generated by [QWH], [QWH/π], and for any \(\varphi \in \mathbb{R}\), \[\text{QWH/0} and \text{QWH/π}\] and for any \(\varphi \in \mathbb{R}\), \[\text{QWH}, \text{QWH/0} and \text{QWH/π}\] and for any \(\varphi \in \mathbb{R}\), \[\text{QWH}, \text{QWH/0} and \text{QWH/π}\].

The gates [QWH] and [QWH/π] have one input and one output, while \[\text{QWH/0}\] has two and \[\text{QWH/π}\] zero. A quantum circuit \(C\) with \(n\) inputs and \(n\) outputs is called a \(n\)-qubit circuit. Given an \(n\)-qubit circuit \(C\), the corresponding unitary map \([C]\) is acting on the Hilbert space \(\mathbb{C}^{(0,1)^n} = \text{span}\{ |x\rangle, x \in \{0, 1\}^n \} \).

Definition 2 (Semantics). For any \(n\)-qubit quantum circuit \(C\), let \([C] : \mathbb{C}^{(0,1)^n} \rightarrow \mathbb{C}^{(0,1)^n}\) be the linear map inductively defined as follows: \([C_2 \circ C_1] = [C_2] \circ [C_1], [C_1 \otimes C_3] = [C_1] \otimes [C_3], and \forall x, y \in \{0, 1\}, \forall \varphi \in \mathbb{R},\]

\[\text{QWH} = |x\rangle \mapsto (1/2)(|0\rangle + (-1)^x|1\rangle),\]

\[\text{QWH/0} = |x\rangle \mapsto e^{i\varphi}|x\rangle,\]

\[\text{QWH/π} = |x\rangle \mapsto |x\rangle,\]

\[\emptyset = |x, y\rangle \mapsto |x, x \oplus y\rangle,\]

\[\text{CNOT} = |x, y\rangle \mapsto |y, x\rangle,\]

\[\text{SWAP} = 1 \mapsto e^{i\varphi},\]

\[\text{Z} = 1 \mapsto 1.\]

Remark 3. Although the definition of \([.]\) relies on the inductive structure of raw quantum circuits, it is well-defined on quantum circuits as for any raw quantum circuits \(C, C'\), whenever \(C \equiv C'\) we have \([C] = [C']\).

Proposition 4 (Universality [33]). For any \(n\)-qubit unitary map \(U\) acting on \(\mathbb{C}^{(0,1)^n}\), there exists an \(n\)-qubit circuit \(C\) such that \([C] = U\).

We use standard shortcuts in the description of quantum circuits, given in Figure 2. In textual description, we sometimes use CNot, s(\(\varphi\)), X, P(\(\varphi\)), etc. to denote respectively \[\text{CNOT}, \text{SWAP}, \text{Z}, \emptyset, \text{X}, -P(\varphi), \text{etc.}\] Moreover, when the parameters (e.g. \(\varphi\)) are not specific values they can take arbitrary ones. We write \(R_X(\theta)\) for the so-called X-rotation [34], whereas the standard phase gate \(P(\varphi)\) is a Z-rotation only up to a global phase. As

\(^3\) denotes the identity, \(\text{SWAP}\) the swap and \(\emptyset\) the empty circuit.

\(^4\)We use the standard Dirac notations.
\[
\begin{align*}
\text{id}_k \circ C &= C = C \circ \text{id}_k & (t_1) \\
(C_3 \circ C_2) \circ C_1 &= C_3 \circ (C_2 \circ C_1) & (t_2) \\
\sigma_k \circ (C \circ \cdots) &= (\cdots \circ C) \circ \sigma_k & (t_4) \\
\sigma_0 := \ldots, \sigma_{k+1} := (\cdots \circ \text{id}_k) \circ (\cdots \circ \sigma_k).
\end{align*}
\]

where \( \text{id}_0 = \ldots \) and \( \text{id}_{k+1} = \text{id}_k \circ \cdots \), and \( \sigma_0 := \ldots \).

Fig. 1: Definition of \( \equiv \) for raw circuits (either raw quantum circuits or raw optical circuits).

\[
\begin{align*}
-Z &:= -P(\pi) & (1) \\
-X &:= -H -Z -H & (2) \\
-R_X(\theta) &:= \frac{\theta}{2} -H -P(\theta) -H & (3)
\end{align*}
\]

Fig. 2: Usual abbreviations of quantum circuits.

\[
\text{Equations (a) to (l) are fairly standard in quantum computing. Equation (m), which is used for instance in [35], describes two equivalent ways to define a controlled-Z gate. Notice that this equation cannot be derived from the other axioms as it is the only equation on 2 qubits which does not preserve the parity of the number of CNotS plus the number of swaps. Equations (n) and (o) are more involved and account for some specific commutation properties of controlled gates (see Proposition 16 and Proposition 17).}
\]

The axioms of QC0, i.e. the equations given in Figure 3, are sufficient to derive standard elementary circuit identities like those given in Figure 4.

One can also prove that some particular circuits, called phase-gadgets [36], can be flipped vertically:

\[
\begin{align*}
\text{QC}_0 \vdash P(\varphi) &= P(\varphi) & (6) \\
\text{QC}_0 \vdash R_X(\theta) &= R_X(\theta) & (7)
\end{align*}
\]

a consequence, they have a slightly different behaviour: \(P\) is 2\(\pi\)-periodic: \([P(2\pi)] = I\), whereas \(R_X\) is 4\(\pi\)-periodic, and we instead have \([R_X(2\pi)] = -I\).

C. Structural equations

We introduce a set QC0 of structural equations on quantum circuits in Figure 3. These equations are structural in the sense that the transformations on the parameters are only based on the fact that \(\mathbb{R}\) is an additive group. In particular, these equations are valid for any reasonable\(^3\) restriction on the angles.

We write QC0 \(\vdash C_1 = C_2\) when \(C_1\) can be transformed into \(C_2\) using the equations of Figure 3.\(^6\)

Proposition 5. The structural equations of Figure 3 are sound, i.e. if QC0 \(\vdash C_1 = C_2\) then \([C_1] = [C_2]\).

Proof. By inspection of the equations of Figure 3.\(\Box\)

\(^3\)I.e. which forms an additive group and contains \(\pi/2\).

\(^6\)More formally, QC0 \(\vdash \cdot = \cdot\) is defined as the smallest congruence which satisfies equations of Figures 1 and 3.
The derivations are given in [30]. Combining Equation (6) and Equation (i), one can easily prove the following equation, used for instance in [8] in the context of circuit optimisation:

\[ \text{QC}_0 \vdash \frac{\mathcal{P}(\varphi) \mathcal{P}(\varphi')} {\mathcal{P}(\varphi') \mathcal{P}(\varphi)} \]

Notice that when \( \varphi = -\varphi' = \alpha/2 \) the above circuits are two equivalent standard implementations of a controlled Z-rotation of angle \( \alpha \). We show in the next section how the basic algebra of (multi-) controlled gates can be derived.

### D. Controlled gates

Multi-controlled gates are useful to describe more elaborate quantum circuits. We use the notations “\( \lambda' \)” and “\( \Lambda' \)” for controls. Given a 1-qubit gate \( G \), \( \lambda^1 G \) is a 2-qubit positively controlled gate; if the control qubit (the top one) is in state \( |1\rangle \) (resp. \( |0\rangle \)) then \( G \) (resp. the identity) is applied on the target qubit (the bottom one). \( \lambda^2 G \) is a 3-qubit positively controlled gate, where the two upper qubits are controls: they both need to be in state \( |1\rangle \) for the gate \( G \) to fire on the bottom qubit. We also consider more general multi-controlled gates \( \Lambda^x_{\cdots} G \) with positive (when \( x_i = 1 \)) and negative (when \( x_i = 0 \)) controls: if the first qubit is in the state \( |x_1\rangle \) (resp. \( |\bar{x}_1\rangle \)) then \( \Lambda^{x_2 \cdots x_k} G \) (resp. the identity) is applied on the remaining qubits. Finally, \( \Lambda^{x_{\cdots} G \} \) denotes a multi-controlled gate with control qubits on both sides – above and below – of the target qubit.

We will follow a standard construction for multi-controllers using a decomposition into elementary 1- and 2-qubit gates (see for instance [33]). Note that we do not aim here at defining all controlled operators: as this construction is the main apparatus for the completeness result, we only focus on the operations \( s(\varphi), X, R_X(\theta) \) and \( P(\varphi) \). Other controlled operations can then be derived if needed.

We first define in Definition 6 circuits implementing regular, all-positive multi-controlled gates \( \lambda^n G \). We then present in Definition 7 how to handle positive and negative controls. In Definition 8 we finally introduce controlled gates with controls both above and below the gate \( G \).

**Definition 6 (Positively multi-controlled gates).** For all \( n \in \mathbb{N} \) and \( G \in \{ s(\varphi), X, R_X(\theta), P(\varphi) \} \), we define a quantum circuit \( \lambda^n G \). This circuit acts on \( n \) wires when \( G = s(\varphi) \) and \( n + 1 \) otherwise. We define each circuit \( \lambda^n G \) as follows.

---

1Note that \( G \) spans non-elementary gates, the constructor \( \lambda \) is not considered as a gate operator, and the fact that the circuit \( \lambda^n G \) happens to be related to \( G \) is a corollary of its definition, as discussed further in the article.
\begin{align*}
\lambda^n R_X(\theta) & \text{ is defined by induction:} \\
\lambda^0 R_X(\theta) & := R_X(\theta), \\
\lambda^{n+1} R_X(\theta) & := \lambda^n R_X(\frac{\pi}{2}) \lambda^n R_X(\frac{\pi}{2}) \lambda^n R_X(\frac{\pi}{2}) . \\
\lambda^n P(\varphi) & \text{ is defined by induction using } \lambda^n R_X(\varphi): \\
\lambda^0 P(\varphi) & := P(\varphi), \\
\lambda^{n+1} P(\varphi) & := \lambda^n P(\varphi) \lambda^n R_X(\frac{\pi}{2}) . \\
\lambda^n X & \text{ is a simple macro:} \\
\lambda^n X & := \lambda^n P(\pi) . \\
\text{Finally, } \lambda^n s(\psi) & := s(\psi) \text{ and } \lambda^{n+1} s(\psi) := \lambda^n P(\psi).
\end{align*}

\textbf{Definition 7} (Multi-controlled gates). For any \(k\)-length list of booleans \(x = x_1, \ldots, x_k\) \((x_i \in \{0,1\})\), for any \(G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}\) we define the quantum circuit \(\Lambda^x G\) as

\[ \Lambda^x G := \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots . \]

when \(G \in \{X, R_X(\theta), P(\varphi)\}\), and

\[ \Lambda^x s(\varphi) := \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]

where \(x = 1 - x\), \(X^1 = -X\), and \(X^0 = \).

\textbf{Definition 8} (General multi-controlled gates). Given two lists of booleans \(x \in \{0,1\}^k\) and \(y \in \{0,1\}^\ell\), if \(xy\) is the concatenation of \(x\) and \(y\) we define the two quantum circuits

- for any \(G \in \{X, R_X(\theta), P(\varphi)\}\)

\[ \Lambda^x y G := \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots . \]

- \(\Lambda^x y s(\varphi) := \Lambda^x y s(\varphi)\).

One can double check using the semantics that \(\Lambda^x y G\) is actually a multi-controlled gate:

\textbf{Proposition 9}. For any \(x, u, v \in \{0,1\}^k\), \(y, v \in \{0,1\}^\ell\), \(a \in \{0,1\}\) and \(G \in \{X, R_X(\theta), P(\varphi)\}\),

\[ [\Lambda^x y G] [u, a, v] = \begin{cases} [u] \otimes ([G] |a|) \otimes [v] & \text{if } uv = xy, \\
[u, a, v] & \text{otherwise,} \end{cases} \]

and

\[ [\Lambda^x y s(\varphi)] [u, v] = \begin{cases} e^{i\varphi} [u, v] & \text{if } uv = xy, \\
[u, v] & \text{otherwise.} \end{cases} \]

We use the standard bullet-based graphical notation for multi-controlled gates: the \(i\)th control is black (resp. white) when \(x_i = 1\) (resp. \(x_i = 0\)), and the \(j\)th from the end control is black (resp. white) when \(y_{n-j+1} = 1\) (resp. \(y_{n-j+1} = 0\)), e.g.:

\[ \Lambda^1_0 X : \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]

\[ \Lambda^{10} P(\varphi) : \begin{array}{c}
\begin{array}{c}
P(\varphi)
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]

\[ \Lambda^{01} X : \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]

\[ \Lambda^{010} P(\varphi) : \begin{array}{c}
\begin{array}{c}
P(\varphi)
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]

\[ \Lambda^{101} X : \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]

\[ \Lambda^{100} P(\varphi) : \begin{array}{c}
\begin{array}{c}
P(\varphi)
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]

\[ \Lambda^{1010} P(\varphi) : \begin{array}{c}
\begin{array}{c}
P(\varphi)
\end{array}
\end{array} \cdots \begin{array}{c}
\begin{array}{c}
X \times \cdots \times X
\end{array}
\end{array} \cdots , \]
To avoid ambiguity with CNot we will not use this notation in the particular case of $\Lambda^1 X$ and $\Lambda_1 X$. Notice however that $\Lambda^1 X$ is provably equivalent to CNot:

**Proposition 10.** $QC_0 \vdash \Lambda^1 X = \bigoplus_k$.  

*Proof.* The proof is given in [30].

---

### E. Properties of multi-controlled gates

In a multi-qubit controlled gate, all control qubits play a similar role. This can be expressed as the following commuting property:

$$R_X(\theta) \circ R_X(\theta) = R_X(\theta) \circ R_X(\theta)$$

This property is provable in QC$_0$, considering three cases depending whether the exchanged control qubits are either above or below the target qubit:

**Proposition 11.** For any $x \in \{0, 1\}^k, y \in \{0, 1\}^\ell, z \in \{0, 1\}^m, a, b \in \{0, 1\}$ and any $G \in \{s(\psi), X, R_X(\theta), P(\varphi)\}$,

$$QC_0 \vdash \Lambda_x^{a b z} G = \Lambda_y^{a b z} G \quad \text{(20)}$$

**Proposition 12.** For any $x \in \{0, 1\}^k, y \in \{0, 1\}^\ell, G \in \{s(\psi), X, R_X(\theta), P(\varphi)\}$,

$$QC_0 \vdash \Lambda_x^{a b y} G = \Lambda_y^{a b y} G \quad \text{(21)}$$

$$QC_0 \vdash \Lambda_y^{a y G} = \Lambda_x^{a y G} \quad \text{(22)}$$

A peculiar property of controlled phase gates (and hence controlled scalars) is that the target qubit is actually equivalent to the control qubits, e.g.:

$$P(\varphi) \circ P(\varphi) = P(\varphi) \circ P(\varphi)$$

This property is also provable in QC$_0$:

**Proposition 13.** For any $x \in \{0, 1\}^k, y \in \{0, 1\}^\ell, G \in \{s(\psi), X, R_X(\theta), P(\varphi)\}$,

$$QC_0 \vdash \Lambda_x^y R_X(\theta') \circ \Lambda_y^x R_X(\theta) = \Lambda_x^y R_X(\theta + \theta'), \quad \text{for } G \in \{s(\psi), X, R_X(\theta), P(\varphi)\} \quad \text{(23)}$$

*Proof.* First, proving that multi-controlled gates with angle 0 are equivalent to the identity is straightforward by induction.

To prove the rest of the proposition, we first prove that $QC_0 \vdash \Lambda^{1-1} R_X(\theta') \circ \Lambda^{1-1} R_X(\theta) = \Lambda^{1-1} R_X(\theta + \theta')$. The proof is by induction: we unfold the two multi-controlled gates, use Equation (24) to put the multi-controlled gates with angles $\theta/2$ and $\theta'/2$ side by side, and merge them using the induction hypothesis. We use again Equation (24) to allow the combination of the multi-controlled gates with angle $-\theta/2$ and $-\theta'/2$, closing the case.

The cases with more general controls are derived from this one using Definitions 7 and 8. The cases of $P$ and $s$ are derived from the $R_X$ case using Definitions 6 and an ancillary lemma stating that a multi-controlled phase commutes with the controls of another multi-controlled gate. The details of the proof are given in [30].

**Remark 14.** Note that Proposition 13 does not imply the periodicity of controlled gates. The latter is proven in Proposition 22 with the help of the rules of Figure 5.

Combining a control and anti-control on the same qubit makes the evolution independent of this qubit, as in the following example in which the evolution is independent of
the second qubit: \(^8\)

\[
\begin{array}{c}
\begin{array}{c}
P(\varphi) \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
P(\varphi) \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
= \\
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
P(\varphi) \\
\end{array}
\end{array}

\end{array}
\]

Such simplifications can be derived in QC\(_0\):

**Proposition 15.** For any \(x \in \{0, 1\}^k\), \(y \in \{0, 1\}^l\), and \(G \in \{s(\varphi), X, R_X(\varphi), P(\varphi)\}\),

\[
\text{QC}_0 \vdash \Lambda_{x}^{0} G \circ \Lambda_{x}^{1} G = \bigotimes \Lambda_{x}^{0} G.
\]

**Proof.** Without loss of generality, we assume \(y\) as the empty string \(\epsilon\) and \(G = R_X(\varphi)\), as it can derive the other cases. The proof is by induction: we unfold the multi-controlled and multi-anti-controlled gates. We can then move the \(X\) gate through \(H\) and CNot gates due to the anti-control, changing the sign of an \(R_X\) rotation from \(-\theta/2\) to \(\theta/2\). The rest of the proof is similar to the one of Proposition 13, except that two \(R_X\) gates cancel out, leading to the identity on the first qubit and the desired multi-controlled gate on the second one. The details of the proof are given in [30]. \(\square\)

Proposition 15 shows how control and anti-control can be combined on the first qubit of a multi-controlled gate. Note, however, that it can be generalised to any control qubit thanks to Proposition 11.

Another useful property of multi-controlled gates is that they commute when there is a control and anti-control on the same qubit, as in the following example in which their controls differ on the third (and last) qubit:

\[
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\bigotimes \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
P(\varphi) \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
= \\
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
P(\varphi) \\
\end{array}
\end{array}

\end{array}
\]

When the target qubit is the same, such a commutation property can be derived in QC\(_0\), using in particular Equation (\(n\)):

**Proposition 16.** For any \(x, x' \in \{0, 1\}^k\), \(y, y' \in \{0, 1\}^l\), and \(G, G' \in \{X, R_X(\varphi), P(\varphi)\}\), if \(xy \neq x'y'\) then

\[
\text{QC}_0 \vdash \Lambda_{x}^{y} G \circ \Lambda_{x'}^{y'} G' = \Lambda_{x'}^{y'} G' \circ \Lambda_{x}^{y} G.
\]

**Proof.** The proof relies on a generalisation of Equation (24), and follows by an induction argument whose base case can be derived thanks to Equation (\(n\)). The details of the proof are given in [30]. \(\square\)

Controlled and anti-controlled gates also commute when the target qubits are not the same in both gates, as in:

\[
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
P(\varphi) \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
= \\
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
P(\varphi) \\
\end{array}
\end{array}

\end{array}
\]

This property can also be derived in QC\(_0\), using in particular Equation (\(o\)):

**Proposition 17.** For any \(a, b \in \{0, 1\}, x, x' \in \{0, 1\}^k\), \(y, y' \in \{0, 1\}^l\), \(z, z' \in \{0, 1\}^m\) and \(G, G' \in \{X, R_X(\varphi), P(\varphi)\}\), if \(xyz \neq x'y'z'\) then

\[
\text{QC}_0 \vdash \Lambda_{x}^{z} G \circ \Lambda_{x'}^{z'} G' = \Lambda_{x'}^{z'} G' \circ \Lambda_{x}^{z} G.
\]

**Proof.** The proof is also based on the generalisation of Equation (24), using an inductive argument whose base case can be derived thanks to Equation (\(o\)). The details of the proof are given in [30]. \(\square\)

**E. Euler angles and Periodicity**

QC\(_0\) is not complete. In particular equations based on Euler angles, which require non-trivial calculations on the angles, cannot be derived. As a consequence we add to the equational theory the three rules shown in Figure 5, leading to the equational theory QC. We write \(\text{QC} \vdash C_1 = C_2\) when \(C_1\) can be rewritten into \(C_2\) using equations of Figure 3 and Figure 5 (together with the deformation rules).

The Euler decomposition of \(H\) (Equation (\(p\))) is not unique:

**Proposition 18.** QC \(\vdash \Lambda_{-\frac{\pi}{2}} = \bigotimes \left( \begin{array}{c}
\frac{1}{\sqrt{2}} \\
\frac{-i}{\sqrt{2}}
\end{array} \right) R_X(-\frac{\pi}{2}) \left( \begin{array}{c}
\frac{1}{\sqrt{2}} \\
\frac{-i}{\sqrt{2}}
\end{array} \right)
\]

**Proof.** The proof is given in [30]. \(\square\)

More generally the Euler angles are not unique, but can be made unique by adding some constraints on the angles, like choosing them in the appropriate intervals (see Figure 5).

**Proposition 19.** Equations (\(q\)) and (\(r\)) are sound. Moreover, the choice of parameters in the RHS-circuits to make the equations sound is unique (under the constraints given in Figure 5).

**Proof.** The soundness and uniqueness of Equation (\(q\)) are well-known properties. Regarding Equation (\(r\)), we first notice that the semantics of both circuits is of the form

\[
\begin{pmatrix}
I & 0 \\
0 & U^{-1}
\end{pmatrix}
\]

where \(U\) is a \(3 \times 3\) matrix. We then use the fact that this matrix can be decomposed into basic rotations that can be proved to be unique [29]. The details of the proof are given in [30]. \(\square\)

Notice that Equation (\(q\)) subsumes Equations (\(k\)) and (\(l\)), which can now be derived using the other axioms of QC.

**Proposition 20.** The following two equations of QC,

\[
\begin{array}{c}
\begin{array}{c}
P(\varphi_1) \bigotimes P(\varphi_2) \\
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
= \\
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
P(\varphi_1 + \varphi_2) \\
\end{array}
\end{array}

\end{array}
\]

\[
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
X \bigotimes P(\varphi) \\
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
= \\
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\Theta \\
\end{array}
\end{array}
\end{array}
\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
P(-\varphi) \\
\end{array}
\end{array}
\end{array}

\end{array}
\]

can be derived from the other axioms of QC.

**Proof.** The proofs are given in [30]. \(\square\)

The introduction of the additional equations of Figure 5 allows us to prove some extra properties about multi-controlled gates, like periodicity (for those with a parameter) in Proposition 22 and the fact that a multi-controlled \(X\) gate is self-inverse.
Proposition 21. For any \( x \in \{0, 1\}^k \), \( y \in \{0, 1\}^\ell \),
\[
QC \vdash \Lambda^y_x X \circ \Lambda^y_x X = id_{k+\ell+1}.
\]

Proof. The case \( x = y = \epsilon \) is a direct consequence of Equation (10). For the other cases, by Definitions 6 to 8, Equations (10) and (a), and Proposition 13, it is equivalent to show that, for any \( x \in \{0, 1\}^k \),
\[
QC \vdash \Lambda^x P(2\pi) = id_{k+1}.
\]

Without loss of generality, we can consider \( x \in \{1\}^k \). Then the result is a consequence of Proposition 13 and Equation (r). Indeed, by taking \( \gamma_1 = \gamma_3 = \gamma_4 = 0 \) and \( \gamma_2 = 2\pi \) in the LHS of Equation (r), the unique angles on the right are all zeros:
\[
\delta_1 = \delta_2 = \delta_3 = \delta_4 = \delta_5 = \delta_6 = \delta_7 = \delta_8 = \delta_9 = 0.
\]

By Proposition 13, any multi-controlled gate with zero angle is the identity, which gives us the desired equality. Further details can be found in [30].

Proposition 22. For any \( x \in \{0, 1\}^k \), \( y \in \{0, 1\}^\ell \), \( \theta \in \mathbb{R} \),
\[
QC \vdash \Lambda^y_x R_X(\theta + 4\pi) = \Lambda^y_x R_X(\theta)
\]
\[
QC \vdash \Lambda^y_x P(\theta + 2\pi) = \Lambda^y_x P(\theta)
\]
\[
QC \vdash \Lambda^y_x s(\theta + 2\pi) = \Lambda^y_x s(\theta)
\]

Proof. Following the additivity of Proposition 13, it is sufficient to show that for any \( x \in \{0, 1\}^k \), \( y \in \{0, 1\}^\ell \),
\[
QC \vdash \Lambda^y_x R_X(4\pi) = id_{k+\ell+1},
\]
\[
QC \vdash \Lambda^y_x P(2\pi) = id_{k+\ell+1},
\]
\[
QC \vdash \Lambda^y_x s(2\pi) = id_{k+\ell}.
\]

Also, with Equation (10) and Definitions 7 and 8, it is sufficient to show that for any \( x \in \{1\}^k \),
\[
QC \vdash \Lambda^x R_X(4\pi) = id_{k+1},
\]
\[
QC \vdash \Lambda^x P(2\pi) = id_{k+1},
\]
\[
QC \vdash \Lambda^x s(2\pi) = id_k.
\]

First, we prove the three cases with \( x = \epsilon \). Then, we use \( QC \vdash \Lambda^x P(2\pi) = id_{k+1} \) proven in Proposition 21 using Equation (r). We obtain the other statements as direct consequences of the 2\pi-periodicity of \( P \). Further details are provided in [30].

III. Completeness

In this section we prove the main result of the paper, namely the completeness of QC. To this end, a back and forth encoding of quantum circuits into linear optical quantum circuits is introduced. We use the graphical language for linear optical circuits introduced in [29].

A. Optical circuits

A linear optical polarisation-preserving (LOPP for short) circuit is an optical circuit made of beam splitters \( \varphi, \theta \in \mathbb{R} \) and phase shifters \( \theta \in \mathbb{R} \):

Definition 23. Let LOPP be the prop generated by \( \varphi, \theta \in \mathbb{R} \) with \( \varphi, \theta \in \mathbb{R} \).

Like quantum circuits, LOPP-circuits are defined as a prop: one can see them as raw circuits quotiented by the \( \equiv \)-equivalence given in Figure 1.
In the following, we consider the single-photon case, hence each input mode (or wire) represents a possible input position for the photon. The photon moves from left to right in the circuit. The state of the photon is entirely defined by its position, and as a consequence the state space is of the form \( \mathbb{C}^n \) when there are \( n \) possible modes. We consider the standard orthonormal basis \( \{|p\rangle\}_{p \in \{0, n\}} \) of \( \mathbb{C}^n \). The semantics is defined as follows.

**Definition 24 (Semantics).** For any \( n \)-mode LOPP-circuit \( C \), let \( \|C\| : \mathbb{C}^n \rightarrow \mathbb{C}^n \) be a linear map inductively defined as follows: \( \|C_2 \circ C_1\| := \|C_2\| \circ \|C_1\| \), \( \|C_1 \otimes C_3\| := \|C_1\| \oplus \|C_3\| \).

\[\|\bigtriangleup\| := |p\rangle \iff \cos(\theta) |p\rangle + i \sin(\theta) |1-p\rangle = \begin{pmatrix} \cos(\theta) & i \sin(\theta) \\ i \sin(\theta) & \cos(\theta) \end{pmatrix} \] \[\|\bigtriangledown\| := |p\rangle \iff |1-p\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \] \[\|\bigcirc\| := e^{i \phi} \quad \|\bigbox\| := 1 \quad \|\bigboxdot\| := 0 \]

**Remark 25.** The definition of \( \|\cdot\| \) relies on the inductive structure of raw LOPP-circuits, it is however well-defined on LOPP-circuits as for any raw LOPP-circuits \( C, C' \), \( C \equiv C' \) implies \( \|C\| = \|C'\| \).

We consider a simple equational theory for LOPP-circuits (Figure 6), which is derived from the rewriting system introduced in [29]. Contrary to the rewriting system of [29], the swap is part of LOPP-circuits. Moreover, the most elaborate equation – Equation (G) – is slightly simplified in the present paper to have one parameter less.

We use the notation LOPP \( \vdash C_1 = C_2 \) whenever \( C_1 \) can be transformed into \( C_2 \) using the equations of Figure 6 (and circuit deformations of Figure 1).

**Theorem 26.** The equational theory given by Figure 6 is sound and complete: for any LOPP-circuits \( C_1, C_2 \), LOPP \( \vdash C_1 = C_2 \) iff \( \|C_1\| = \|C_2\| \).

**Proof.** The soundness can be shown with the semantics given in Definition 24. Regarding completeness, we show that we can derive from Figure 6 the rules of the strongly normalising rewriting system of [29]. The full proof is given in [30].

### B. Forgetting the monoidal structure

The proof of completeness for quantum circuits is based on a back and forth translation from linear optical circuits. While both kinds of circuits form a prop, so both have a monoidal structure, these monoidal structures do not coincide. The monoidal structure of quantum circuits corresponds to the tensor product, whereas that of linear optical circuits is a direct sum. Hence the translations do not preserve the monoidal structure.

As a consequence there is a technical issue around defining the translation directly on circuits. We instead define the transformations on raw circuits (cf. Section II-A). The collection of raw quantum (resp. LOPP) circuits is denoted \( \text{QC}_{\text{raw}} \) (resp. \( \text{LOPP}_{\text{raw}} \)). Notice that we recover the standard circuits by considering the raw circuits up to the equivalence relation \( \equiv \) given in Figure 1: \( \text{QC} = \text{QC}_{\text{raw}}/\equiv \) and \( \text{LOPP} = \text{LOPP}_{\text{raw}}/\equiv \).

To avoid ambiguity in the graphical representation of raw circuits one can use boxes like \( X \) for \((X \otimes X) \circ (X \otimes X)\). We also use box-free graphical representation that we interpret as a layer-by-layer description of a raw circuit, more precisely we associate with any box-free graphical representation, a raw-circuit of the form \( C = (\ldots \left((L_1 \circ L_2) \circ L_3\right) \circ \ldots) \circ L_k \) where \( L_i = (\ldots ((g_{i,1} \otimes g_{i,2} \otimes g_{i,3} \otimes \ldots) \otimes g_{i,k}) \).

For instance, \((|id_1 \otimes id_1\rangle \circ X) \circ (\text{CNot} \otimes H)\) is:

\[
\begin{array}{c}
|id_1 \otimes id_1\rangle \\
\circ \\
X \\
\circ \\
H \\
\end{array}
\]

We extend the notation \( \text{QC} \vdash \cdot = \cdot \) and \( \text{LOPP} \vdash \cdot = \cdot \) to raw circuits. For any raw quantum circuits (resp. raw optical circuits) \( C_1, C_2 \), we write \( \text{QC} \vdash C_1 = C_2 \) (resp. \( \text{LOPP} \vdash C_1 = C_2 \)) if \( C_1 \) and \( C_2 \) are equivalent by the congruence defined in Figure 3, Figure 5 and Figure 1 (resp. Figure 6 and Figure 1).\(^{10}\)

Notice that there exists a derivation between two circuits if and only if there exists a derivation between two of their representative raw circuits. Indeed, intuitively the only difference is that the derivation on raw circuits is more fine-grained as the equivalence relation \( \equiv \) is made explicit.

### C. Encoding quantum circuits into optical ones

We are now ready to define the encoding of (raw) quantum circuits into (raw) linear optical circuits. For dimension reasons, an \( n \)-qubit system is encoded into \( 2^n \) modes. One can naturally choose to encode \( |x\rangle \), with \( x \in \{0, 1\}^n \), into the mode \( |\chi\rangle \) where \( \chi = \sum_{i=1}^{2^n} x_i 2^{n-i} \) is the usual binary encoding. Alternatively, we use Gray codes to produce circuits with a simpler connectivity, in particular two adjacent modes encode basis qubit states which differ on exactly one qubit.

**Definition 27 (Gray code).** Let \( \mathcal{G}_n : \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{(0,1)^n} \) be the map \( |k\rangle \mapsto |G_n(k)\rangle \) where \( G_n(k) \) is the Gray code of \( k \), inductively defined by \( G_0(0) = \epsilon \) and

\[
G_n(k) = \begin{cases} 0G_{n-1}(k) & \text{if } k < 2^{n-1}, \\ 1G_{n-1}(2^n - 1 - k) & \text{if } k \geq 2^{n-1}. 
\end{cases}
\]

For instance \( G_3 \) is defined as follows:

| 0 | 000 | 4 | 110 |
| 1 | 001 | 5 | 111 |
| 2 | 011 | 6 | 101 |
| 3 | 010 | 7 | 100 |

\(^{10}\)In this context, the circuits depicted in Figures 3, 5 and 6 are interpreted as box-free graphical representations of raw circuits.
In order to get around the fact that the encoding an n-qubit circuit into a 2n-mode optical circuit cannot preserve the parallel composition, we proceed by “sequentialising” the circuit: roughly speaking, an n-qubit circuit is seen as a sequential composition of layers, each layer being an n-qubit circuit made of an elementary gate g acting on at most two qubits in parallel with the identity on all other qubits, e.g. \( id_k \otimes g \otimes id_l \). The encoding of such a layer, denoted \( E_{k,l}(g) \), is a 2n-mode optical circuit acting non-trivially on potentially all the modes.

For instance, consider a 3-qubit layer which consists in applying \( P(\varphi) \) on the second qubit. Its semantics is \( |x,y,z\rangle \mapsto e^{i\varphi y} |x,y,z\rangle \). Such a circuit is encoded into an 8-mode optical circuit \( E_{1,1}(P(\varphi)) \) made of 4 phase shifters acting on the modes \( p \in \{2,5\} \) (those s.t. \( G_2(p) = x1z \)). Indeed, the semantics of \( E_{1,1}(P(\varphi)) \) is \( |p\rangle \mapsto \begin{cases} e^{i\varphi} |p\rangle & \text{if } p \in \{2,5\} \\ |p\rangle & \text{otherwise} \end{cases} \).

The encoding map is formally defined as follows:

**Definition 28 (Encoding).** Let \( E : QC_{raw} \rightarrow LOPP_{raw} \) be defined as follows: for any n-qubit circuit \( C \), \( E(C) = E_{0,0}(C) \) where \( E_{k,l} \) is inductively defined as:

- \( E_{k,l}(C_1 \otimes C_2) = E_{k+l,n_1,n_2}(C_1) \otimes E_{k+l,n_1,n_2}(C_2) \), where \( C_1 \) (resp. \( C_2 \)) is acting on \( n_1 \) (resp. \( n_2 \)) qubits;
- \( E_{k,l}(C_1 \circ C_2) \) is acting on \( n_1 \) qubits.

Let us define \( \sigma_{k,n,l} \) as a \( 2k+n+\ell \)-mode linear optical circuit made only of swaps (that is, without any \( 0 \)- or \( \uparrow \)-) such that \( 0_n \circ [\sigma_{k,n,l}] \circ 0_n^{-1} \) acts on \( |x,y,z\rangle \) for any \( x \in \{0,1\}^k \), \( y \in \{0,1\}^n \) and \( z \in \{0,1\}^\ell \). We then define\(^{11}\)

\[
E_{k,l}(\bigotimes) = \sigma_{k,2,\ell} \circ E_{k+1,2,1} \circ \sigma_{k,2,\ell},
E_{k,l}(\bigotimes) = (---) \otimes 2^{k+\ell},
\]

\(^{11}\)Note that we are making an abuse of notation by writing products of three raw circuits without parentheses, since composition is not associative on raw circuits. This can be solved by taking a convention similarly to the box-free representation of circuits. Note however that our proofs actually do not depend on the convention chosen.

\[
E_{k,l}(\bigotimes) = (---) \otimes 2^{k+\ell},
\]

where \( C^\otimes n \) means \( C \) n times in parallel: \( C^\otimes 0 = [] \) and \( C^\otimes n+1 = C \otimes C^\otimes n \).

For the remaining generators, we have:

\[
E_{0,0}(\bigotimes) = \bigotimes_{i=1}^\ell |y_i\rangle \langle y_i| \circ \sigma_{1,1,\ell},
E_{0,0}(\bigotimes) = \bigotimes_{i=1}^\ell |\bar{y}_i\rangle \langle \bar{y}_i| \circ \sigma_{1,1,\ell},
\]

and whenever \( (k, \ell) \neq (0,0) \):

\[
E_{k,l}(\bigotimes) = \sigma_{k,1,l} \circ \bigotimes_{i=1}^{\ell} |y_i\rangle \langle y_i| \circ \sigma_{1,1,\ell},
E_{k,l}(\bigotimes) = \sigma_{k,1,l} \circ \bigotimes_{i=1}^{\ell} |\bar{y}_i\rangle \langle \bar{y}_i| \circ \sigma_{1,1,\ell},
\]

**Remark 29.** Note that for any n-qubit circuit \( C \), \( E_{k,l}(C) \) is a \( 2k+n+\ell \)-mode optical circuit. Also note that \( \sigma_{k,n,l} \) is nothing but a permutation of wires. By Lemma 36 – which is independent of the definition of \( E \) – any actual circuit satisfying the above property \( (\Phi_n \circ [\sigma_{k,n,l}] \circ \Phi_n^{-1} \) is convenient for our purposes. A formal definition of \( \sigma_{k,n,l} \) is however given in [30].

**Example 30.** Consider the simple circuit \( C_0 = \bigotimes \). The encoding is as shown in Figure 7. Using the topological rules...
The encoding of quantum circuits into linear optical circuits preserves the semantics, up to Gray codes.

**Proposition 31.** For any $n$-qubit quantum circuit $C$,

\[
\mathcal{G}_n \circ \|E(C)\| = \|C\| \circ \mathcal{G}_n
\]

**Proof.** By induction. \(\square\)

### D. Decoding

Regarding the decoding, i.e. the translation back from linear optical circuits to quantum circuits, we use the same sequentialisation approach. Note that such a decoding is defined only for optical circuits with a power of two number of modes.

The decoding of a $2^n$-mode layer $id_k \otimes g \otimes id_l$ is an $n$-qubit circuit denoted $D_{k,n}(g)$. For instance consider a 16-mode layer which consists in applying $\frac{\pi}{2}$ on the fourth mode.

The encoding of quantum circuits into linear optical circuits is inductively defined as follows:

**Definition 32** (Decoding). Let $D : \text{LOPP}_\text{raw} \rightarrow \text{QC}_\text{raw}$ be defined as follows: for any $2^n$-mode circuit $C$, $D(C) = D_{0,n}(C)$ where for any $n,k,\ell$ with $k+\ell \leq 2^n$ and $C : \ell \rightarrow \ell$, $D_{k,n}(C)$ is inductively defined as follows.

- $D_{k,n}(C_1 \otimes C_2) = D_{k+\ell_1,n}(C_2) \circ D_{k,n}(C_1)$, where $C_1$ is acting on $\ell_1$ modes;
- $D_{k,n}(C_2 \circ C_1) = D_{k,n}(C_2) \circ D_{k,n}(C_1)$;
- $D_{k,n}(\mathbf{id}_n) = \mathbf{id}_n$.

The remaining generators are treated as follows.

\[
D_{k,n}(\varphi) = \frac{\pi}{2}, \quad D_{k,n}(\varphi) = \Lambda^{G_n(k)}(\varphi),
\]

\[
D_{k,n}(\emptyset) = \Lambda^{G_n(k)}(\varphi), \quad D_{k,n}(\emptyset) = \Lambda^{G_n(k)}(\varphi)
\]

where $x_{2k,n} := G_{n-1}(k)$, $y_{2k,n} := s$ and $y_{2k+1,n} := w$ and $w \in \{0,1\}$ are such that $G_n(2k+1) = w\alpha.0^q$ for some $\alpha \in \{0,1\}$.

**Example 33.** We consider the optical circuit $C_1$ obtained in Example 30. With all of the gates $P$ and $R_X$ parametrised with $\frac{\pi}{2}$, we can show that $D(C_1) \equiv \frac{\pi}{2}$. Similarly to the encoding function, the decoding function preserves the semantics up to Gray codes.

**Proposition 34.** For any $2^n$-mode optical circuit $C$,

\[
\|D(C)\| \circ \mathcal{G}_n = \mathcal{G}_n \circ \|C\|.
\]

**Proof.** The proof is by induction. \(\square\)

### E. Quantum circuit completeness

The proof of completeness is based on the encoding/decoding of quantum circuits into optical circuits. Intuitively, given two quantum circuits representing the same unitary map, one can encode them as linear optical circuits. Since the encoding preserves the semantics and LOPP is complete, there exists a derivation proving the equivalence of the encoded circuits. In order to lift this proof to quantum circuits, it remains to prove that the decoding of an encoded quantum circuit is provably equivalent to the original quantum circuit, and that each axiom of LOPP can be mimicked in QC. Notice that since the encoding/decoding is defined on raw circuits, an extra step in the proof consists in showing that the axioms of $\equiv$ can also be mimicked in QC.

Examples 30 and 33 point out that composing encoding and decoding does not lead, in general, to the original circuit,
the decoded circuit being made of multi-controlled gates. However, we show that the equivalence with the initial circuit can always be derived in QC:

**Lemma 35.** For any $n$-qubit raw quantum circuit $C$, $\text{QC} \vdash D(E(C)) = C$.

**Proof.** We prove by structural induction on $C$ that

$$\forall k, \ell, \text{QC} \vdash D(E_{k,\ell}(C)) = id_k \otimes C \otimes id_\ell.$$

For any two $n$-qubit raw circuits $C_1, C_2$, one has

$$D(E_{k,\ell}(C_2 \circ C_1)) = D(E_{k,\ell}(C_2)) \circ D(E_{k,\ell}(C_1))$$

and for any $m$-qubit raw circuit $C_3$,

$$D(E_{k,\ell}(C_1 \otimes C_3)) = D(E_{k+n,\ell}(C_3)) \circ D(E_{k,\ell+m}(C_1)).$$

Hence, it remains the base cases, which are proved in [30].

Note that in general, the decoding function does not preserve the topological equivalence. For instance, with the raw circuits $C_1 = X \otimes X \otimes X$ and $C_2 = Y \otimes Y$, we have $C_1 \equiv C_2$ but $D(C_1) = X \otimes X \otimes X$ and $D(C_2) = R_x(\pi)$. Thus, the topological rules also have to be mimicked in QC:

**Lemma 36.** For any $2^n$-mode raw optical circuits $C_1, C_2$, if $C_1 \equiv C_2$ then $\text{QC} \vdash D(C_1) = D(C_2)$.

**Proof.** The proof consists intuitively in verifying that the decoding of every equation of Figure 1 is provable in QC. The proof is given in [30].

**Lemma 37.** For any $2^n$-mode raw optical circuits $C_1, C_2$, if $\text{LOPP} \vdash C_1 = C_2$ then $\text{QC} \vdash D(C_1) = D(C_2)$.

**Proof.** The proof consists intuitively in verifying that the decoding of every equation of Figure 6 is provable in QC. The proof is given in [30].

We are now ready to prove the main result of the paper.

**Theorem 38 (Quantum circuit completeness).** QC is a complete equational theory for quantum circuits: for any quantum circuits $C_1, C_2$, if $[C_1] = [C_2]$ then $\text{QC} \vdash C_1 = C_2$.

**Proof.** Given two quantum circuits $C_1, C_2$ s.t. $[C_1] = [C_2]$, let $C'_1$ (resp. $C'_2$) be a raw quantum circuit, representative of $C_1$ (resp. $C_2$). Thanks to Proposition 31 we have $[E(C'_1)] = [E(C'_2)]$. The completeness of LOPP implies $\text{LOPP} \vdash E(C'_1) = E(C'_2)$. By Lemma 37, we have QC $\vdash D(E(C'_1)) = D(E(C'_2))$. Moreover Lemma 35 implies QC $\vdash C'_1 = C'_2$. From this derivation we obtain a derivation of QC $\vdash C_1 = C_2$, where the steps corresponding to the equivalence relation $\equiv$ are trivialised.

IV. DISCUSSIONS

We have introduced the first complete equational theory for quantum circuits. Although this equational theory is fairly simple, Equation (r) is an unbounded family of equations – one for each possible number of control qubits. Such a family of equations is a natural byproduct of our proof technique: The decoding of each axiom of LOPP produces an equation made of multi-controlled gates that has to be derived using QC. It is actually quite surprising that Equation (r) is the only remaining equation with multi-controlled gates.

Notice that one can get rid of these multi-controlled gates by extending the context rule as described below. Indeed, Equation (r) can be derived from its 2-qubit case

$$R_x(\pi), R_x(\pi) = R_x(\pi), R_x(\pi)$$

if one allows the following control context rule $\vdash \Lambda C_1 = \Lambda C_2$ when $C_1 = C_2$. Notice that it requires extending the λ-bernstein to any circuit – which can be done in an inductive way like $\Lambda(C_2 \circ C_1) = \Lambda(C_2 \circ C_1)$ and $\Lambda(C_1 \otimes C_2) = (\Lambda C_1 \otimes id_m) \circ (id_1 \otimes \sigma_{n,m}) \circ (\Lambda C_2 \otimes id_n) \circ (id_1 \otimes \sigma_{m,n})$.

A natural application of the completeness result is to design procedures for quantum circuit optimisation based on this equational theory. One can take advantage of the terminating and confluent rewriting system for optical circuits [29] by mimicking the applications of the rewrite rules on quantum circuits. However, the exponential blowup of the encoding map makes this approach probably inefficient as it is and requires some improvements.

Another future work is to prove (upper or lower) bounds on the size of a derivation between two given equivalent circuits, as well as a bound on the size of the intermediate quantum circuits. This might be useful for providing a verifiable quantum advantage, in particular if there exist polysize quantum circuits requiring exponentially many rewrites [11].

REFERENCES

[1] D. Deutsch, “Quantum computational networks,” Proceedings of the Royal Society of London, Series A. Mathematical and Physical Sciences, vol. 425, no. 1968, pp. 73–90, 1989.

[2] A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger, and B. Valiron, “Quipper: A scalable quantum programming language,” in Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI’13, H.-J. Boehm and C. Flanagan, Eds. ACM, 2013, pp. 333–342.

[3] M. Amy, D. Maslov, and M. Mosca, “Polynomial-time T-depth optimization of Clifford-T circuits via matroid partitioning,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 10, pp. 1476–1489, 2014.

[4] R. Duncan, A. Kissinger, S. Perdrix, and J. Van De Wetering, “Graph-theoretic simplification of quantum circuits with the ZX-calculus,” Quantum, vol. 4, p. 279, 2020.

[5] A. Kissinger and J. van de Wetering, “Reducing the number of non-Clifford gates in quantum circuits,” Phys. Rev. A, vol. 102, p. 022406, Aug. 2020. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.102.022406

[6] D. Maslov, C. Young, D. M. Miller, and G. W. Dueck, “Quantum circuit simplification using templates,” in Design, Automation and Test in Europe. IEEE, 2005, pp. 1208–1213.
