Quantum Circuit Completeness: Extensions and Simplifications

Alexandre Clément ✉ 🏠 ⓘ
Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria, LMF, 91190, Gif-sur-Yvette, France

Noé Delorme ✉ 🏠 ⓘ
Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

Simon Perdrix ✉ 🏠 ⓘ
Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

Renaud Vilmart ✉ 🏠 ⓘ
Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria, LMF, 91190, Gif-sur-Yvette, France

---- **Abstract** ----

Although quantum circuits have been ubiquitous for decades in quantum computing, the first complete equational theory for quantum circuits has only recently been introduced. Completeness guarantees that any true equation on quantum circuits can be derived from the equational theory.

We improve this completeness result in two ways: (i) We simplify the equational theory by proving that several rules can be derived from the remaining ones. In particular, two out of the three most intricate rules are removed, the third one being slightly simplified. (ii) The complete equational theory can be extended to quantum circuits with ancillae or qubit discarding, to represent respectively quantum computations using an additional workspace, and hybrid quantum computations. We show that the remaining intricate rule can be greatly simplified in these more expressive settings, leading to equational theories where all equations act on a bounded number of qubits.

The development of simple and complete equational theories for expressive quantum circuit models opens new avenues for reasoning about quantum circuits. It provides strong formal foundations for various compiling tasks such as circuit optimisation, hardware constraint satisfaction and verification.

1 Introduction

Introduced in the 80's by Deutsch [19], the quantum circuit[1] model is ubiquitous in quantum computing. Various quantum computing tasks – circuit optimisation, fault tolerant quantum computing, hardware constraint satisfaction, and verification – involve quantum circuit transformations [24, 34, 35, 36, 38]. It is therefore convenient to equip the quantum circuit formalism with an *equational theory* providing a way to transform a quantum circuit while

---

[1] Originally called *Quantum Computational Networks*, the term *quantum circuits* is nowadays unanimously used.

preserving the represented unitary map. When the equational theory is powerful enough to guarantee that any true property can be derived, it is said to be *complete*, in other words, any two circuits representing the same unitary map can be transformed into one another using the rules of the equational theory.

The first complete equational theory (denoted QC_{old} in the following) for quantum circuits has been introduced recently [12]. This equational theory has been derived from the LOv-calculus [11], a language for optical quantum computing. Before that, complete equational theories were only known for non-universal fragments of quantum circuits, such as Clifford+T circuits acting on two qubits [6, 16], Clifford+CS circuits acting on three qubits [7], the stabiliser fragment [33, 42], the CNot-dihedral fragment [1], or fragments of reversible circuits [25, 15, 14].

The quantum circuit model can naturally be extended to encompass ancillary qubits, measurements, or qubit discarding, in order to express more general evolutions like isometries and completely positive trace preserving maps. In a model of quantum circuits with ancillae, one can use an additional work space by adding fresh qubits, as well as releasing qubits when they are in a specific state. Even if the vanilla quantum circuits form a universal model of quantum computation,[2] this additional space is useful in many cases. It is for instance commonly used for the construction of quantum oracles.[3] Another important example is the parallelisation of quantum circuits: ancillae enable a better parallelisation of quantum gates, leading generally to a tradeoff between space (number of ancillae) and depth (parallel time) [37]. Notice that ancillae should be carefully used as the computation should leave a clean work space: one can only get rid of a qubit at the end of the computation if this qubit is in the $|0\rangle$-state.

We also consider another extension of quantum circuits where arbitrary qubits can be discarded (or traced out), whatever their states are. This extension allows for the representation of: (*i*) quantum measurements and more generally classically controlled computations; and (*ii*) arbitrary general quantum computations (CPTP maps[4]). Such quantum circuits can be used to deal with fault-tolerant quantum computing and error correcting codes which, by construction, require an additional workspace, measurements and corrections. One can also represent measurement-based quantum computation [43, 17] with this class of circuits. The study of hybrid quantum-classical models is also a subject of interest in algorithmic and complexity theory [22, 2].

Contributions. We address here the problem of simplifying the complete equational theory QC_{old}. Obtained through a non-trivial translation from the LOv-calculus, QC_{old} involves non-trivial equations (see Figure 3), in particular Equation (K_{old}^*) depicts a family of equations acting on an unbounded number of qubits, witness of the non-functoriality of the back and forth translations between quantum circuits and optical circuits, due to the fundamentally different interpretations of the parallel composition in the two circuit languages.

We show that several rules, including two of the three most intricate ones (Equations (12) and (13)), can actually be derived from the other rules, the third one (Equation (K_{old}^*)) being slightly simplified. This leads to a simpler, more compact and easier to use complete equational theory, which however still involves a family of equations acting on an unbounded number of qubits.

---

[2] Any n-qubit unitary transformation can be implemented by a n-qubit vanilla quantum circuit.
[3] Implementation of the n-qubit unitary transformation $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$ given a classical circuit implementing the boolean function f [39].
[4] Completely positive trace-preserving maps.

We consider the more expressive frameworks of quantum circuits with ancilla and/or discards. Several constructions for discarding [23, 9], measurements and quantum operations [45], allow one to turn the complete equational theory for vanilla quantum circuits into complete equational theories for quantum circuits with ancilla and/or discards, by adding a few extra equations. We then mainly show that in these more expressive setting, the unbounded family of equations (K_{old}^*) can be derived from bounded ones, leading to complete equational theories acting on a most three qubits.

Related work.   The first complete equational theory for a universal quantum computing model has been introduced in 2017 for the ZX-calculus [26]. Since then, complete equational theories have been introduced for other universal fragments of the ZX-calculus [27, 21, 28, 47, 29] and its variants ZH-, ZW-calculi [3, 20]. ZX-like languages differ from quantum circuits mainly in two ways: they are more expressive, allowing the representation of any matrix[5] so in particular those representing post-selected evolutions for instance; the second major difference – and the most important in our context – is that not all the generators are unitary, thus even if a ZX-diagram represents an overall unitary evolution, it does not provide in general a (deterministic) implementation by means of elementary gates contrary to the quantum circuit model. To circumvent this problem one can consider the so-called subclass of circuit-like ZX-diagrams which is in one-to-one correspondence with quantum circuits, however this class is not closed under the known complete equational theories of the ZX-calculus. In particular, the problem of transforming a ZX-diagram representing a unitary evolution into a circuit-like one has been studied in the context of circuit optimisation [30], leading to various heuristics [31, 4, 18]. However, this approach fails so far to lead to a complete equational theory for quantum circuits.

The paper is structured as follows. In Section 2, we consider vanilla quantum circuits together with a new equational theory QC. We prove the completeness of QC first for the fragment of 1-CNot circuits,[6] that we then use to derive the remaining equations of the already known complete equational theory QC_{old} introduced in [12]. In Section 3, we introduce an extension of vanilla quantum circuits with $|0\rangle$-state initialisation. Universal for isometries, such quantum circuits with initialisation are introduced as an intermediate step towards circuits with ancillae and/or discard. We add to the equational theory QC two basic equations involving qubit-initialisation, and provide a proof of completeness of the augmented equational theory QC_{iso} using a particular circuit decomposition based on the so-called cosine-sine decomposition of unitary maps. The completeness of QC_{iso} is extended to provide complete equational theories for quantum circuits with ancillae ($QC_{ancilla}$ in Section 4) – which additionally allow for the release of qubits when they are in a specific state – and for quantum circuits with qubit discarding ($QC_{discard}$ in Section 5) – which allows the tracing out of any qubits. Both extensions provide alternative representations of multi-controlled gates, allowing the simplification of the remaining intricate rule – which acts on an unbounded number of qubits – into its 2-qubit version.

Due to space constraints, we only sketch the proofs in the present paper. Please refer to the full version [13] for the detailed proofs together with all the required derivations.
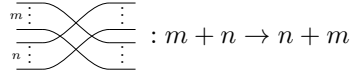
---

[5]   the only constraint is on the dimension of the matrices which must be a power of two for the qubit case, qudit versions also exist [8, 41]

[6]   The sub-class of quantum circuits made of at most one CNot gate.
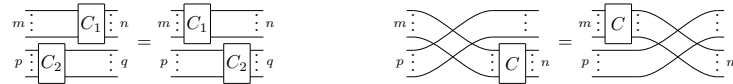
2   Vanilla quantum circuits

2.1   Graphical languages

We define quantum circuits using the formalism of props [32], which are, in category-theoretic terms, strict symmetric monoidal categories whose objects are generated by a single object, or equivalently with $(\mathbb{N}, +)$ as a monoid of objects. The prop formalism provides a formal and rigorous framework to describe graphical languages. The main features of props are recalled in the following. Circuits $C_1 : m \to n$ and $C_2 : p \to q$ in a prop, depicted as $m\ {\vdots}\ \boxed{C_1}\ {\vdots}\ n$ and $p\ {\vdots}\ \boxed{C_2}\ {\vdots}\ q$ can be composed: (1) "in sequence" $C_2 \circ C_1 : m \to q$ if $n = p$, graphically $m\ {\vdots}\ \boxed{C_1}\ \boxed{C_2}\ {\vdots}\ q$;

(2) "in parallel" $C_1 \otimes C_2 : m + p \to n + q$, graphically $\begin{smallmatrix} m\ \vdots\ \boxed{C_1}\ \vdots\ n \\ p\ \vdots\ \boxed{C_2}\ \vdots\ q \end{smallmatrix}$. The *unit* for tensor product $\otimes$ is the *empty circuit*: $\square : 0 \to 0$. This means $\square \otimes C = C = C \otimes \square$ for any circuit C. The circuit $-\!\!-\,: 1 \to 1$ depicts the identity, $=\,: 2 \to 2$ is the identity on two wires and more generally $-\!\!-^{\otimes m} := -\!\!- \otimes (-\!\!-)^{\otimes m-1} : m \to m$ (with $(-\!\!-)^{\otimes 0} := \square$) is the identity on m wires. Graphically, we obviously have $-\!\!-^{\otimes n} \circ C = C = C \circ -\!\!-^{\otimes m}$ for any $C : m \to n$. Finally, a prop is also endowed with a particular circuit $\asymp : 2 \to 2$ which satisfies $\asymp\asymp\; = \;=$. Graphically (and semantically in what follows) $\asymp$ swaps places. By compositions, we may build the following family of circuits

$$\begin{smallmatrix} m\ \vdots \\ \\ n\ \vdots \end{smallmatrix}\!\!\!\!\bowtie\!\!\!\!\begin{smallmatrix} \vdots \\ \\ \vdots \end{smallmatrix} : m + n \to n + m$$

which exchanges m-sized and n-sized registers. In a prop, circuits satisfy a set of identities, that graphically translate as "being able to deform the circuit". For instance, the following identities are valid transformations:

$$\begin{smallmatrix} m\ \vdots\ \boxed{C_1}\ \vdots\ n \\ p\ \vdots\ \boxed{C_2}\ \vdots\ q \end{smallmatrix} = \begin{smallmatrix} m\ \boxed{C_1}\ \vdots\ n \\ p\ \vdots\ \boxed{C_2}\ q \end{smallmatrix} \qquad\qquad \begin{smallmatrix} m\ \vdots \\ \\ p\ \vdots \end{smallmatrix}\!\!\bowtie\!\!\begin{smallmatrix} \vdots \\ \boxed{C}\ n \\ \vdots \end{smallmatrix} = \begin{smallmatrix} m\ \boxed{C}\ \vdots \\ \\ p\ \vdots\ n \end{smallmatrix}\!\!\bowtie$$

In the following, all the considered theories will be props, and hence will have the empty, identity and swap circuits as basic generators.

2.2   Vanilla quantum circuits and their equational theory

We first consider the vanilla model of quantum circuits generated by the very standard gateset: Hadamard, Phase gates, and CNot, together with global phases:

▶ **Definition 1.** *Let* **QC** *be the prop generated by* $-\boxed{H}-\,: 1 \to 1$, $-\boxed{P(\varphi)}-\,: 1 \to 1$, $\underset{\oplus}{\overset{\bullet}{\mid}} : 2 \to 2$ *and* $\oslash : 0 \to 0$ *for any* $\varphi \in \mathbb{R}$.

We associate with any quantum circuit its standard interpretation as a unitary map:

▶ **Definition 2** (Semantics). *For any n-qubit* **QC**-*circuit C, let* $[\![C]\!] : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ *be the* semantics *of C inductively defined as the linear map satisfying* $[\![C_2 \circ C_1]\!] = [\![C_2]\!] \circ [\![C_1]\!]$; $[\![C_1 \otimes C_2]\!] = [\![C_1]\!] \otimes [\![C_2]\!]$; *and*
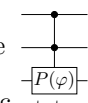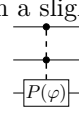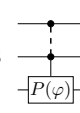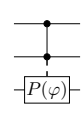
$$[\![\square]\!] = 1 \mapsto 1 \quad [\![\oslash]\!] = 1 \mapsto e^{i\varphi} \quad [\![-\boxed{H}-]\!] = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}} \quad [\![-\boxed{P(\varphi)}-]\!] = |x\rangle \mapsto e^{ix\varphi} |x\rangle$$

$$\left[\!\!\left[\underset{\oplus}{\overset{\bullet}{\mid}}\right]\!\!\right] = |x, y\rangle \mapsto |x, x \oplus y\rangle \qquad [\![-\!\!-]\!] = |x\rangle \mapsto |x\rangle \qquad [\![\asymp]\!] = |x, y\rangle \mapsto |y, x\rangle$$

Note that for any **QC**-circuit C, $[\![C]\!]$ is unitary. Conversely, it is well known that any unitary map acting on a finite number of qubits can be represented by a **QC**-circuit:

▶ **Proposition 3** (Universality). **QC** *is universal, i.e. for any unitary* $U : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ *there exists a* **QC**-*circuit* C *such that* $[\![C]\!] = U$.

Quantum circuits, as defined above, only have four different kinds of generators, however, it is often convenient to use other gates that can be defined by combining them. For instance, following [5, 12], Pauli gates, Toffoli, X-rotations, and multi-controlled gates are defined in Figure 1. Note that while the phase gate $-\boxed{P(\varphi)}-$ is 2π-periodic, the X-rotation $-\boxed{R_X(\theta)}-$ is 4π-periodic.

We use the standard bullet-based notation for multi-controlled gates. For instance denotes the application of a phase gate $-\boxed{P(\varphi)}-$ on the third qubit controlled by the first two qubits. With a slight abuse of notations, we use dashed lines for arbitrary number of control qubits, e.g. $: n+1 \to n+1$ or simply $: n+1 \to n+1$ have $n \geq 0$ control qubits (possibly zero), whereas $: n+2 \to n+2$ and $: 1+n+1 \to 1+n+1$ have at least one control qubit.
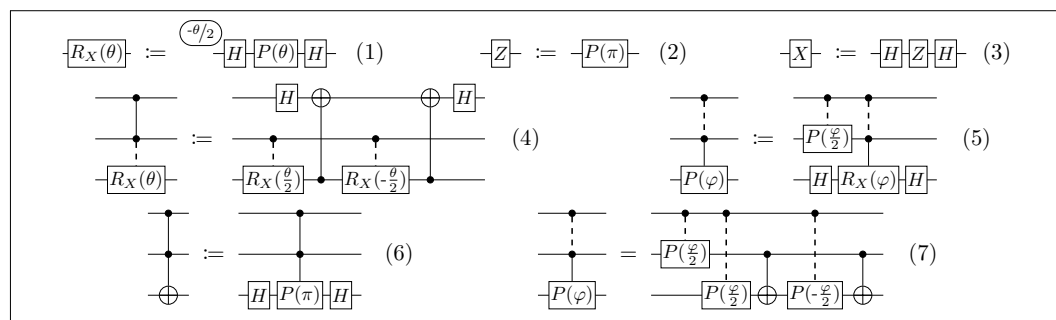
Figure 1 Shortcut notations for usual gates defined for any $\varphi, \theta \in \mathbb{R}$. Equation (1) defines X-rotations while Equations (2) and (3) define Pauli gates. Equations (4) and (5) are inductive definitions of multi-controlled gates. Equation (6) is the definition of the well known Toffoli gate. Equation (7) is a provably equivalent definition of the multi-controlled phase gate.

We equip the vanilla quantum circuits with the equational theory QC defined in Figure 2. We write $\text{QC} \vdash C_1 = C_2$ when C_1 can be transformed into C_2 using the equations of QC. More formally, $\text{QC} \vdash \cdot = \cdot$ is the smallest congruence which satisfies the equations of Figure 2 together with the deformation rules that come with the prop formalism. QC is sound, i.e. for any **QC**-circuits C_1, C_2 if $\text{QC} \vdash C_1 = C_2$ then $[\![C_1]\!] = [\![C_2]\!]$. This can be proved by observing that all equations of QC are sound.

Figure 3 depicts the complete equational theory QC_{old} for vanilla quantum circuits introduced in [12]. Compared to QC_{old}, Equations (8) and (9) are now subsumed by Equation (G) in QC, Equation (K*) is a slight simplification of Equation (K$_{\text{old}}^*$) with one less parameter in the RHS circuit, whereas Equations (10) and (11) together with Equations (12) and (13) have been removed, as we prove in the following that they can be derived in QC.
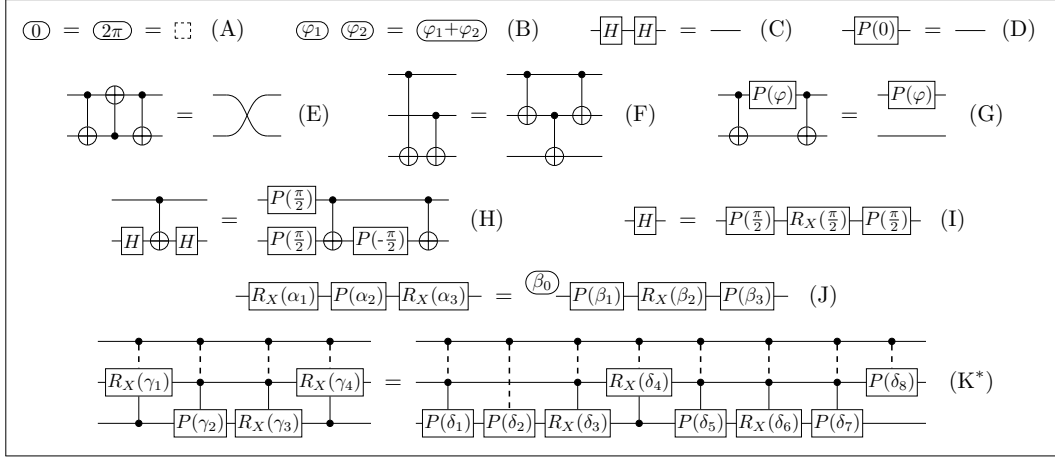
Figure 2 Equational theory QC. Equations (B) and (G) are defined for any $\varphi, \varphi_1, \varphi_2 \in \mathbb{R}$. In Equations (J) and (K*) the LHS circuit has arbitrary parameters which uniquely determine the parameters of the RHS circuit. Equation (J) follows from the well-known Euler-decomposition which states that any unitary can be decomposed, up to a global phase, into basic X- and Z-rotations. Thus for any $\alpha_i \in \mathbb{R}$, there exist $\beta_j \in \mathbb{R}$ such that Equation (J) is sound. We make the angles β_j unique by assuming that $\beta_1 \in [0, \pi)$, $\beta_0, \beta_2, \beta_3 \in [0, 2\pi)$ and if $\beta_2 \in \{0, \pi\}$ then $\beta_1 = 0$. Equation (K*) reads as follows: the equation is defined for any $n \geq 2$ input qubits, in such a way that all gates are controlled by the first $n-2$ qubits. Similarly to Equation (J), for any $\gamma_i \in \mathbb{R}$, there exist $\delta_j \in \mathbb{R}$ such that Equation (K*) is sound. We ensure that the angles δ_j are uniquely determined by assuming that $\delta_1, \delta_2, \delta_5 \in [0, \pi)$, $\delta_3, \delta_6, \delta_7, \delta_8 \in [0, 2\pi)$, $\delta_4 \in [0, 4\pi)$, if $\delta_3 = 0$ and $\delta_6 \neq 0$ then $\delta_2 = 0$, if $\delta_3 = \pi$ then $\delta_1 = 0$, if $\delta_4 \in \{0, 2\pi\}$ then $\delta_1 = \delta_3 = 0$, if $\delta_4 \in \{\pi, 3\pi\}$ then $\delta_2 = 0$, if $\delta_4 \in \{\pi, 3\pi\}$ and $\delta_3 = 0$ then $\delta_1 = 0$, and if $\delta_6 \in \{0, \pi\}$ then $\delta_5 = 0$.

2.3 Reasoning on quantum circuits

To derive an equation $C_1 = C_2$ over quantum circuits, one can apply some rules of the equational theory to transform step by step C_1 into C_2. In the context of vanilla quantum circuits, we can take advantage of the reversibility of generators to *simplify* equations. Indeed, intuitively, proving $C_1 \circ \boxed{H} = C_2 \circ \boxed{H}$ is equivalent to proving $C_1 = C_2$ as $\boxed{H}$ is (provably) reversible. Similarly, proving $C_1 = C_2$ should be equivalent to proving $C_1 \circ C_2^\dagger = \text{---}$, where the adjoint of a circuit is defined as follows:

▶ **Definition 4.** *For any* **QC**-*circuit C, let $C^\dagger$ be the* adjoint *of C inductively defined as* $(C_2 \circ C_1)^\dagger := C_1^\dagger \circ C_2^\dagger$; $(C_1 \otimes C_2)^\dagger := C_1^\dagger \otimes C_2^\dagger$; *and for any* $\varphi \in \mathbb{R}$, $(\text{\textcircled{$\varphi$}})^\dagger := \text{\textcircled{$-\varphi$}}$, $(\boxed{P(\varphi)})^\dagger := \boxed{P(-\varphi)}$, *and $g^\dagger := g$ for any other generator g.*

▶ **Proposition 5.** $[\![C^\dagger]\!] = [\![C]\!]^\dagger$ *for any* **QC**-*circuit C, where $[\![C]\!]^\dagger$ is the usual linear algebra adjoint of $[\![C]\!]$.*

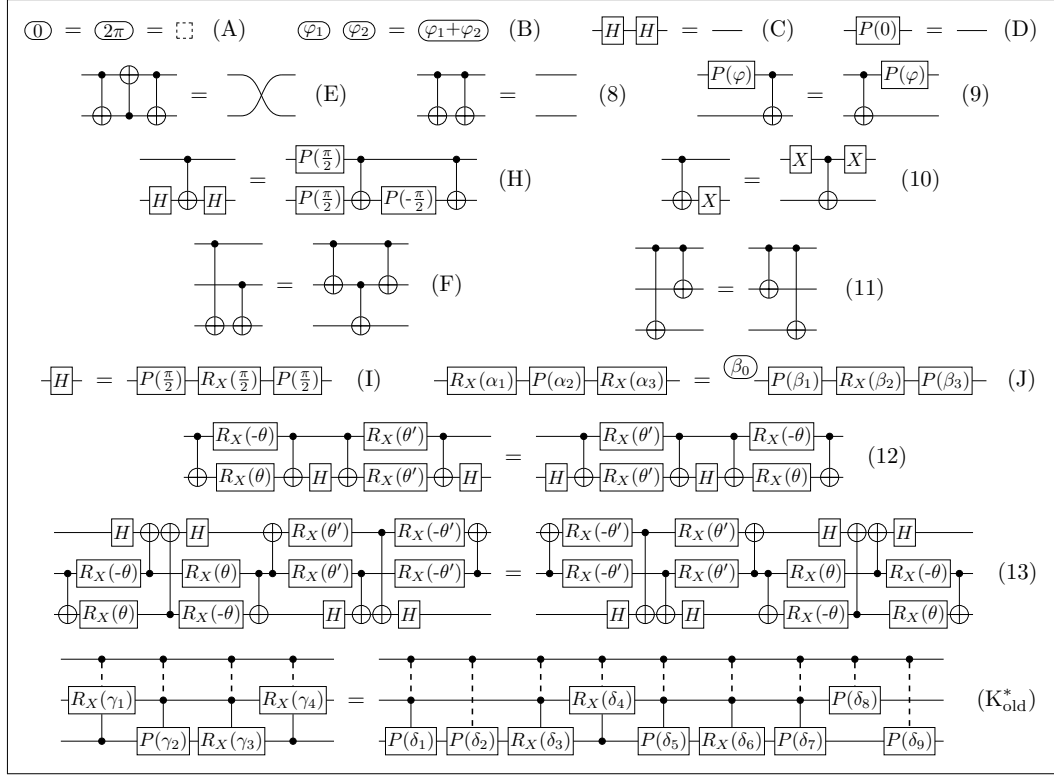**Proof.** By induction on C.   ◀

▶ **Proposition 6** (Simplification principle). *For any n-qubit* **QC**-*circuits C, C_1, C_2*

$$\text{QC} \vdash C \circ C_1 = C_2 \qquad \Leftrightarrow \qquad \text{QC} \vdash C_1 = C^\dagger \circ C_2$$

and

$$\text{QC} \vdash C_1 \circ C = C_2 \qquad \Leftrightarrow \qquad \text{QC} \vdash C_1 = C_2 \circ C^\dagger$$

Figure 3 Equational theory QC_{old} introduced in [12]. Equations (A),(B),(C),(D),(E),(H),(F),(I) are (J) are aslo in the equational theory QC. Equation (K_{old}^*) is the old version of Equation (K^*) with one more parameter, and where the uniqueness of the parameters δ_j is given by the conditions: $\delta_1, \delta_2, \delta_5 \in [0, \pi)$, $\delta_3, \delta_4, \delta_6, \delta_7, \delta_8, \delta_9 \in [0, 2\pi)$, if $\delta_3 = 0$ then $\delta_2 = 0$, if $\delta_3 = \pi$ then $\delta_1 = 0$, if $\delta_4 = 0$ then $\delta_1 = \delta_3 \ (= \delta_2) = 0$, if $\delta_4 = \pi$ then $\delta_2 = 0$, if $\delta_4 = \pi$ and $\delta_3 = 0$ then $\delta_1 = 0$, and if $\delta_6 \in \{0, \pi\}$ then $\delta_5 = 0$. Note that these conditions on the δ_j for $1 \leq j \leq 8$ are the same as in Equation (K^*) except for δ_4, which is restricted to be in $[0, 2\pi)$ instead of $[0, 4\pi)$, and for δ_2, which has to be 0 when $\delta_3 = 0$ even if $\delta_6 = 0$.

Proof. First we show by induction that $QC \vdash C \circ C^\dagger = \text{---}^{\otimes n}$ and $QC \vdash C^\dagger \circ C = \text{---}^{\otimes n}$ for any C. Then, w.l.o.g. we show that $(QC \vdash C \circ C_1 = C_2) \Rightarrow (QC \vdash C_1 = C^\dagger \circ C_2)$: assuming $QC \vdash C \circ C_1 = C_2$, we have $QC \vdash C_1 = C^\dagger \circ C \circ C_1 = C^\dagger \circ C_2$. ◀

2.4 Completeness

We prove the completeness of QC by showing that every equation of the original complete equational theory QC_{old} introduced in [12] can be derived in QC. To this end we first show the completeness of QC for the (modest) fragment of quantum circuits containing at most one CNot gate.

▶ **Lemma 7** (1-CNot completeness). QC *is complete for circuits containing at most one* ⊕̇, *i.e. for any* **QC**-*circuits* C_1, C_2 *with at most one* ⊕̇, *if* $[\![C_1]\!] = [\![C_2]\!]$ *then* $QC \vdash C_1 = C_2$.

Proof. First we can show that, for semantic reasons, it is enough to prove the statement for 2-qubit circuits containing no swap gate and exactly one CNot gate. Then, by the simplification principle (Proposition 6), it is sufficient to prove

whenever the equation is sound. By semantic analysis, we can show that there exist $\alpha, \beta, \gamma, \varphi, \theta \in \mathbb{R}$ and $k, \ell \in \{0, 1\}$ such that

$$\llbracket\, -\boxed{A}-\, \rrbracket = \llbracket\, @ -\boxed{P(\varphi)}\!-\!\boxed{X^k}-\, \rrbracket \qquad\qquad \llbracket\, -\boxed{C}-\, \rrbracket = \llbracket\, \oslash -\boxed{X^k}\!-\!\boxed{Z^\ell}\!-\!\boxed{P(-\varphi)}-\, \rrbracket$$

$$\llbracket\, -\boxed{B}-\, \rrbracket = \llbracket\, \circled{\beta} -\boxed{R_X(\theta)}\!-\!\boxed{Z^\ell}-\, \rrbracket \qquad\qquad \llbracket\, -\boxed{D}-\, \rrbracket = \llbracket\, \boxed{-\alpha - \beta - \gamma} -\boxed{X^k}\!-\!\boxed{Z^\ell}\!-\!\boxed{R_X(-\theta)}-\, \rrbracket$$

where $-\boxed{X^k}-$ (resp. $-\boxed{Z^\ell}-$) denotes $-\boxed{X}-$ (resp. $-\boxed{Z}-$) if $k = 1$ (resp. $\ell = 1$) and $-\!\!-$ if $k = 0$ (resp. $\ell = 0$). Then, using the completeness of QC for one-qubit circuits (which is a direct consequence of the fact that all equations acting on at most one qubit of QC_{old} are also in QC), it is straightforward to verify that Equations (A),(B),(23),(22),(32),(10),(9),(30),(18),(19),(D), and (25) capture all the possible cases. ◀

▶ **Proposition 8.** *Equation* (12) *can be derived in* QC.

Proof. Using the simplification principle (Proposition 6), one can turn Equation (12) into an equivalent equation whose circuits contain only one $\overset{\bullet}{\underset{\oplus}{}}$. We conclude the proof using the completeness of QC for circuits containing at most one CNot (Lemma 7). The details are given in Appendix A. ◀

▶ **Proposition 9.** *Equation* (13) *can be derived in* QC.

Proof. It turns out that we can use Equation (12) to derive Equation (13) in QC. The derivation is given in Appendix A. ◀

▶ **Proposition 10.** *Equation* $(\text{K}^*_{\text{old}})$ *can be derived in* QC.

Proof. We show that for semantic reasons, we have either the angle δ_9 in $(\text{K}^*_{\text{old}})$ in $\{0, \pi\}$, or $\delta_2 = \delta_3 = \delta_5 = \delta_6 = 0$. When $\delta_9 = 0$, Equation $(\text{K}^*_{\text{old}})$ can be trivially derived from Equation (K^*). Otherwise, Equations (K^*) and $(\text{K}^*_{\text{old}})$ can be transformed into each other using elementary properties of multi-controlled gates. Moreover, these transformations induce a bijection between the 8-tuples of angles δ_j corresponding to the RHS of the instances of Equation (K^*) and the 9-tuples corresponding to the RHS of the instances of Equation $(\text{K}^*_{\text{old}})$, so that the uniqueness of the δ_j in Equation (K^*) follows from the uniqueness in Equation $(\text{K}^*_{\text{old}})$. ◀

▶ **Theorem 11** (Completeness). *The equational theory* QC, *defined in Figure 2, is complete for* **QC***-circuits, i.e. for any* **QC***-circuits* C_1, C_2, *if* $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$ *then* $\text{QC} \vdash C_1 = C_2$.

Proof. All the rules of the complete equational theory introduced in [12] that are not in QC are provable in QC: Equations (8), (9), (10), (11) are proved in Appendix A, Equations (12), (13) and $(\text{K}^*_{\text{old}})$ are proved in Propositions 8, 9 and 10 respectively. ◀

3   Quantum circuits for isometries

In this section we consider a first standard extension of the vanilla quantum circuits which consists in allowing qubit initialisation in a specific state, namely in the $|0\rangle$-state.

▶ **Definition 12.** *Let* $\textbf{QC}_{\text{iso}}$ *be the prop generated by* $\oslash : 0 \to 0$, $-\boxed{H}- : 1 \to 1$, $-\boxed{P(\varphi)}- : 1 \to 1$, $\overset{\bullet}{\underset{\oplus}{}} : 2 \to 2$ *and* $\vdash : 0 \to 1$ *for any* $\varphi \in \mathbb{R}$.

▶ **Definition 13** (Semantics). *We extend the semantics* $\llbracket \cdot \rrbracket$ *of vanilla quantum circuits (Definition 2) with* $\llbracket \vdash \rrbracket = |0\rangle$.

▶ **Proposition 14** (Universality). *Any isometry[7] $V : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^m}$ can be realised by a* $\mathbf{QC}_{\mathrm{iso}}$*-circuit $C : n \to m$ s.t. $[\![C]\!] = V$.*
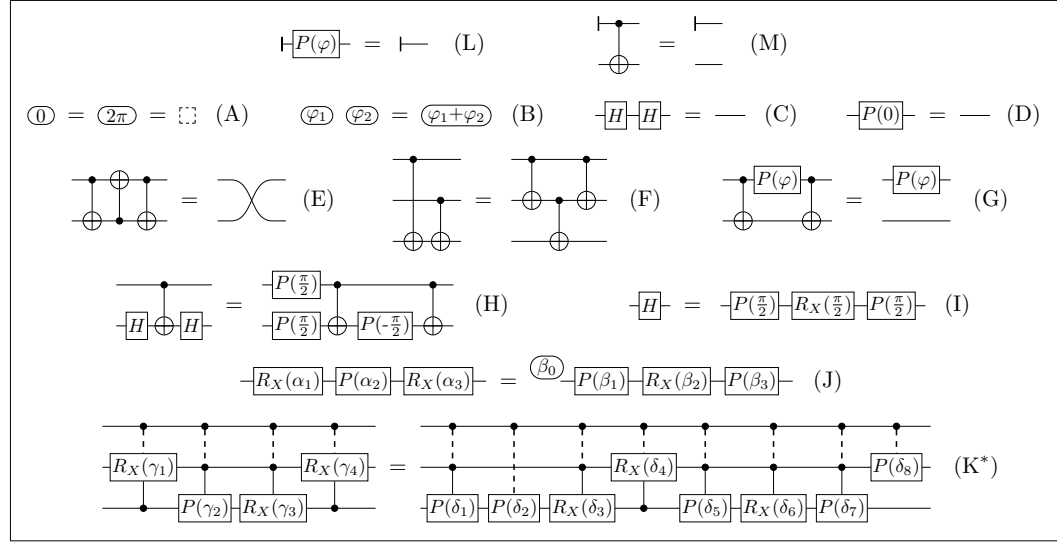
Figure 4 Equational theory $\mathrm{QC}_{\mathrm{iso}}$. It contains all the equations of QC together with Equation (L) (defined for any $\varphi \in \mathbb{R}$) and Equation (M), which are new equations governing the behaviour of the new generator $\vdash$.

For instance, the so-called copies in the standard basis ($|x\rangle \mapsto |xx\rangle$) and in the diagonal basis can be respectively represented as follows:

We consider the equational theory $\mathrm{QC}_{\mathrm{iso}}$, given in Figure 4, which is nothing but the equational theory QC augmented with the following two sound equations:

Viewing $-\boxed{P(\varphi)}-$ as a control-global-phase gate, Equations (L), (M) can be interpreted as instances of the following property: a control gate can be removed when one of its control qubit is initialised in the $|0\rangle$-state. This kind of properties can actually be derived within $\mathrm{QC}_{\mathrm{iso}}$.

▶ **Lemma 15.** *Let C be a* $\mathbf{QC}_{\mathrm{iso}}$*-circuit such that $\forall |\varphi\rangle \in \mathbb{C}^{2^n}$, $[\![C]\!] |\varphi\rangle = |0\rangle \otimes |\varphi\rangle$. Then:*

Proof. We prove that the above circuit necessarily is a **QC**-circuit together with a single qubit initialisation. The semantics of the **QC**-circuit forces it to be equivalent to a controlled circuit, which can be shown to be deletable by the qubit initialisation, thanks to Equations (L) and (M). ◀

---

[7] An isometry is a linear map V s.t. $V^\dagger \circ V$ is the identity.

A direct corollary of Lemma 15 is the completeness of $\mathrm{QC}_{\mathrm{iso}}$ for quantum circuits with at most one initialisation. Notice that one can then use Lemma 17 of [45] to essentially prove the completeness of $\mathrm{QC}_{\mathrm{iso}}$. However, as the semantics in [45] is based on CPTP maps rather than isometries (so global phases should be treated carefully), and moreover the proof of this Lemma 17 is not described, we provide a direct completeness proof of $\mathrm{QC}_{\mathrm{iso}}$ in the following.

To do so, we may want to generalise Lemma 15 to any number of qubit initialisations. However, the proof does not generalise. Indeed, it relies on the fact that, semantically, the vanilla circuit of which we initialize a single qubit is necessarily of the form $\mathrm{diag}(I, U)$, with I and U of the same dimension, so we can start with a circuit implementing U and control each of its gates to get a circuit implementing $\mathrm{diag}(I, U)$ with only controls and phases on the control wire. To generalise this notion to more than one qubit initialisation, where semantically we would need to implement $\mathrm{diag}(I, U)$ with U of dimensions larger than I's, we need a finer-grain decomposition of said matrix. We hence resort to the following unitary decomposition:

▶ **Lemma 16.** *Let* $U = \left(\begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & U_{00} & U_{01} \\ \hline 0 & U_{10} & U_{11} \end{array} \right) \begin{array}{l} \}k \\ \}n-k \\ \\ \}n \end{array}$ *be unitary with U_{00} and U_{11} square.*

Then, there exist:

- A_0, A_1, B_0, B_1 *unitary,*
- $C = \mathrm{diag}(c_1, ..., c_d)$ *and* $S = \mathrm{diag}(s_1, ..., s_d)$ *($c_i, s_i \geq 0$ and $d \leq n - k$).*

such that:

- $C^2 + S^2 = I$
- $U = \left(\begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & A_0 & 0 \\ \hline 0 & 0 & A_1 \end{array} \right) \left(\begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & C & 0 & -S \\ \hline 0 & 0 & I & 0 \\ \hline 0 & S & 0 & C \end{array} \right) \left(\begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & B_0 & 0 \\ \hline 0 & 0 & B_1 \end{array} \right)$

The above decomposition is a variation on the *Cosine-Sine Decomposition* (CSD) [40], which has already appeared to be useful in quantum circuit synthesis [44].

Proof. The proof itself is a variation of the proof for the usual CSD. It specifically involves the so-called RQ and SVD decompositions. ◀

It is then possible to show the completeness of $\mathrm{QC}_{\mathrm{iso}}$:

▶ **Theorem 17** (Completeness). *The equational theory* $\mathrm{QC}_{\mathrm{iso}}$, *defined in Figure 4, is complete for* **$\mathrm{QC}_{\mathrm{iso}}$**-*circuits.*

Proof. The proof goes by showing that deriving equality between two **$\mathrm{QC}_{\mathrm{iso}}$**-circuits amounts to generalising Lemma 15 to any number of qubit initialisations, which is shown inductively using the above variation of the CSD. ◀

4   Quantum circuits with ancillae

In this section, we consider quantum circuits which are implementing unitary maps (or isometries) using ancillary qubits, a.k.a. ancillae, as additional work space. To represent quantum circuits with ancillae, we not only need to be able to initialise fresh qubits, but also to release qubits when they become useless. Note that to guarantee that the overall evolution is an isometry, one can only release a qubit in the $|0\rangle$-state.

To encompass the notion of ancillary qubits we extend $\mathbf{QC}_{\text{iso}}$-circuits (already equipped with qubit initialisation $\vdash$) with a qubit removal generator denoted $\dashv$. Because of the constraint that removed qubits must be in the $|0\rangle$-state, we define the language of quantum circuits with ancillae in two steps.

▶ **Definition 18.** *Let* $\mathbf{QC}_{\text{pre-ancilla}}$ *be the prop generated by* $\mathcal{P} : 0 \to 0$, $-\boxed{H}- : 1 \to 1$, $-\boxed{P(\varphi)}- : 1 \to 1$, $\overset{\bullet}{\oplus} : 2 \to 2$, $\vdash : 0 \to 1$ *and* $\dashv : 1 \to 0$ *for any* $\varphi \in \mathbb{R}$.

▶ **Definition 19** (Semantics). *We extend the semantics* $\llbracket \cdot \rrbracket$ *of quantum circuits for isometries (Definition 13) with* $\llbracket \dashv \rrbracket = \langle 0|$.

Notice that the semantics of a $\mathbf{QC}_{\text{pre-ancilla}}$-circuit is not necessarily an isometry as $\llbracket \dashv \rrbracket$ is not isometric.[8] As a consequence, we define $\mathbf{QC}_{\text{ancilla}}$ as the subclass of $\mathbf{QC}_{\text{pre-ancilla}}$-circuits with an isometric semantics:

▶ **Definition 20.** *Let* $\mathbf{QC}_{\text{ancilla}}$ *be the sub-prop of* $\mathbf{QC}_{\text{pre-ancilla}}$*-circuit* C *such that* $\llbracket C \rrbracket$ *is an isometry.*
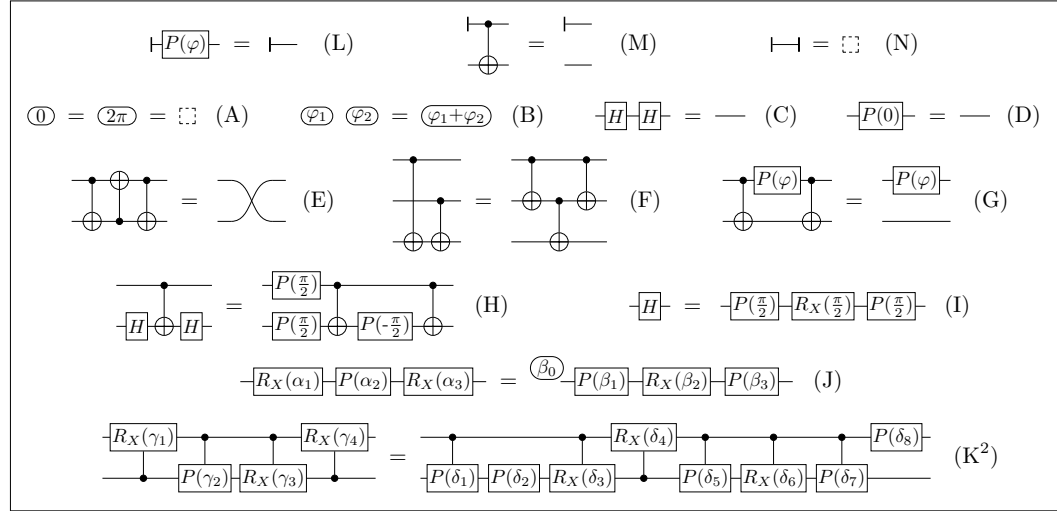
■ **Figure 5** Equational theory $\text{QC}_{\text{ancilla}}$. It contains all the equations of QC_{iso} where Equation (K*) has been replaced by Equation (K^2), together with Equation (N), which is a new equation that allows one to create ancillae.

Notice in particular that any $\mathbf{QC}_{\text{iso}}$-circuit is in $\mathbf{QC}_{\text{ancilla}}$, which implies the universality of $\mathbf{QC}_{\text{ancilla}}$ for isometries. We equip $\mathbf{QC}_{\text{ancilla}}$-circuits with the equational theory $\text{QC}_{\text{ancilla}}$ given in Figure 5, which is nothing but the equational theory QC_{iso} where Equation (K*) is replaced by its 2-qubit version Equation (K^2), together with a new elementary equation (N) governing the behaviour of the qubit removal generator $\dashv$.

$$\vdash\!\!\dashv \;=\; \square \quad (N)$$

---

[8] Actually any linear map L s.t. $L^\dagger L \sqsubseteq I$ can be implemented by a $\mathbf{QC}_{\text{pre-ancilla}}$-circuit, where $\sqsubseteq$ is the Löwner partial order. Thus $\mathbf{QC}_{\text{pre-ancilla}}$ can be seen as a language for postselected quantum computations.

Quantum circuits with ancillae form a standard model of quantum computing. They are for instance used in the context of quantum oracles: given a circuit $C_f : n + 1 \to n + 1$ whose semantics is $|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$ for some boolean function f, one can implement the corresponding phase oracle C'_f whose semantics is $|x\rangle \mapsto (-1)^{f(x)} |x\rangle$ as follows:

Quantum circuits with ancillae are also extensively used in the context of circuit parallelisation, as one can decrease the depth of a quantum circuit by adding ancillary qubits [37]. Finally, ancillary qubits can be used to provide an alternative realisation of multi-controlled gates, for instance a 3-qubit controlled gate can be implemented using an ancillary qubit, Toffoli gates, and the 2-qubit version of the gate:

(14)

This can be generalised to any multi-controlled gates with at least two control qubits:

▶ **Proposition 21.** *The following two equations can be derived in* $\mathrm{QC}_{\mathrm{ancilla}}$.

(15)

(16)

Proof. By induction on the number of qubits. ◀

Notice that Equations (15) and (16) are actually derivable in $\mathrm{QC}_{\mathrm{iso}}$. However, in order to provide an alternative inductive definition of multi-control gates (like in Equation (14)), it requires the presence of at least one fresh qubit which can always be created in the context of quantum circuits with ancillae thanks to Equation (N).

Thanks to the alternative representation of multi-controlled gates, one can derive, in $\mathrm{QC}_{\mathrm{ancilla}}$, the equation (K*) for any arbitrary number of controlled qubits:

▶ **Proposition 22.** *Equation* (K*) *can be derived in* $\mathrm{QC}_{\mathrm{ancilla}}$.

Proof. Let (K^n) be Equation (K*) acting on n qubits for any $n \geq 2$. Equation (K^2) is in $\mathrm{QC}_{\mathrm{ancilla}}$. We first prove that ($K^3$) can be derived from ($K^2$) by defining the Fredkin gate (or controlled-swap gate) and by pushing the two last wires of the LHS circuit of (K^3) into two fresh ancillae, which allow us to apply (K^2) and reverse the construction to get the RHS circuit of (K^3). This technique is not applicable in the general case for any circuit because if the Fredkin gates are not triggered, it could be the case that the gates pushed into the ancillae do not release the ancillae into the $|0\rangle$-state. The key observation is that this is possible for (K^3) as every involved gates are either phase gate or uniquely controlled gate (which both act as identity on the $|0\rangle$-state). Then, we prove that (K^n) is derivable in $\mathrm{QC}_{\mathrm{ancilla}}$ for any $n \geq 4$ by induction on n using the alternative definition of multi-controlled gates (Proposition 21), which allows us to construct an instance of the LHS circuit of (K^{n-1}) from the LHS circuit of (K^n). ◀

We are now ready to prove the completeness of $QC_{ancilla}$:

▶ **Theorem 23** (Completeness). *The equational theory* $QC_{ancilla}$*, defined in Figure 5, is complete for* $\mathbf{QC}_{ancilla}$*-circuits.*

Proof. Proposition 22 implies that for any ⊢-free circuits C_1, C_2, if $QC_{iso} \vdash C_1 = C_2$ then $QC_{ancilla} \vdash C_1 = C_2$. Using deformation of circuits, any $\mathbf{QC}_{ancilla}$-circuit $C : n \to m$ can be written ⋮ $\boxed{C'}$ ⋮ , where $C' : n \to m + k$ is a $\mathbf{QC}_{iso}$-circuit. Since both $[\![C]\!]$ and $[\![C']\!]$ are isometries and $[\![C]\!] = (Id \otimes \langle 0^k |) [\![C']\!]$, we have $[\![C']\!] = [\![C]\!] \otimes |0^k\rangle$. Given two $\mathbf{QC}_{ancilla}$-circuits C_1, C_2 s.t. $[\![C_1]\!] = [\![C_2]\!]$, let $C'_1 : n \to m + k$, and $C'_2 : n \to m + \ell$ be the corresponding $\mathbf{QC}_{iso}$-circuits. W.l.o.g. assume $k \leq \ell$, and pad C'_1 with $\ell - k$ qubit initialisations: $C''_1 := C'_1 \otimes (\vdash)^{\otimes \ell - k}$. We have $[\![C''_1]\!] = [\![C'_2]\!]$, so by completeness of QC_{iso}, $QC_{ancilla} \vdash C''_1 = C'_2$, so $QC_{ancilla} \vdash C_1 \otimes (\ \vdash\!\dashv\ )^{\otimes \ell - k} = C_2$. It suffices to apply Equation (N) to obtain $QC_{ancilla} \vdash C_1 = C_2$. ◀

5 Quantum circuits with discard for completely positive map

The last extension considered in this paper is the addition of a discard operator which consists in tracing out qubits. Contrary to quantum circuits with ancillae, any qubit can be discarded whatever its state is. Discarding a qubit is depicted by ⊣⊩.

▶ **Definition 24.** *Let* $\mathbf{QC}_{discard}$ *be the prop generated by* $-\boxed{H}-$: $1 \to 1$, $-\boxed{P(\varphi)}-$: $1 \to 1$, $\overset{\bullet}{\oplus}$: $2 \to 2$, $\vdash$: $0 \to 1$ *and* ⊣⊩ : $1 \to 0$ *for any* $\varphi \in \mathbb{R}$.

The ability to discard qubits implies that the evolution represented by such a circuit is not pure anymore. As a consequence the semantics is a completely positive trace-preserving (CPTP) map acting on density matrices (trace 1 positive semi-definite Hermitian matrices). Formally the new semantics is defined as follows:

▶ **Definition 25** (Semantics). *For any quantum* $\mathbf{QC}_{discard}$*-circuit* $C : n \to m$*, let* $(\!|C|\!) :$ $\mathcal{M}_{2^n,2^n}(\mathbb{C}) \to \mathcal{M}_{2^m,2^m}(\mathbb{C})$ *be the* semantics *of* C *inductively defined as the linear map* $(\!|C_2 \circ C_1|\!) = (\!|C_2|\!) \circ (\!|C_1|\!)$*;* $(\!|C_1 \otimes C_2|\!) = (\!|C_1|\!) \otimes (\!|C_2|\!)$*;* $(\!|⊣⊩|\!) = \rho \mapsto tr(\rho)$ *and for any other generator* g*,* $(\!|g|\!) = \rho \mapsto [\![g]\!] \rho [\![g]\!]^\dagger$*, where* $tr(M)$ *is the trace of the matrix* M *and* $M^\dagger$ *its adjoint.*

Notice that the global phase generator ⓟ is not part of the prop anymore. If it were, its interpretation would be $(\!|ⓟ|\!) = \rho \mapsto [\![ⓟ]\!] \rho [\![ⓟ]\!]^\dagger = e^{i\varphi}\rho e^{-i\varphi} = \rho$, which is the same as that of the empty circuit. Thus, for this model the X-rotation can simply be defined as $-\boxed{R_X(\theta)}- := -\boxed{H}\!-\!\boxed{P(\theta)}\!-\!\boxed{H}-$ (the same definition as Figure 1 but without the global phase).

▶ **Proposition 26** (Universality). $\mathbf{QC}_{discard}$ *is universal for CPTP maps.*

Proof. According to the Stinespring dilation lemma [46], any CPTP map $F : \mathcal{M}_{2^n,2^n}(\mathbb{C}) \to \mathcal{M}_{2^m,2^m}(\mathbb{C})$ can be purified as an isometry $V : \mathbb{C}^{2^n} \to \mathbb{C}^{2^{m+k}}$ such that for any ρ, $F(\rho) = tr_k(V\rho V^\dagger)$, where $tr_k(.)$ is the partial trace of the last k qubits. By universality of $\mathbf{QC}_{iso}$ there exists a circuit C such that $[\![C]\!] = V$. Let C' be the global-phase-free version of C, thus $[\![C']\!] = e^{i\theta}V$. Seen as a $\mathbf{QC}_{discard}$-circuit, C' has the semantics $(\!|C'|\!) = \rho \mapsto (e^{i\theta}V)\rho(e^{i\theta}V)^\dagger = V\rho V^\dagger$. Discarding the last k qubits of C' leads to a $\mathbf{QC}_{discard}$-circuit implementing F. ◀

The new generator and new semantics allow us to model measurements. For instance, the standard basis measurement can be obtained via:

Indeed we recover the semantics of the standard basis measurement:

$$\left(\begin{array}{c} \quad \end{array}\right) = \left(\begin{array}{cc} a & c \\ b & d \end{array}\right) \mapsto \left(\begin{array}{cc} a & 0 \\ 0 & d \end{array}\right)$$

The output wire can be interpreted as a classical bit (encoded in a quantum bit), a (resp. d) being the probability to be 0 (resp. 1).

One can also encode classical gates, for instance the AND gate using Toffoli:

With the promise that the input is classical, i.e. the input density matrix is $\text{diag}(p_{00}, p_{01}, p_{10}, p_{11})$ (where p_{xy} is the probability for the input to be in the state $xy \in \{0,1\}^2$), the output state is $\text{diag}(p_{00}+p_{01}+p_{10}, p_{11})$ which corresponds to the behaviour of the AND gate.

More generally, one can represent classically controlled computation using the $\mathbf{QC}_{\text{discard}}$-circuits, allowing to reason on fault-tolerant computations, error correcting codes and measurement-based quantum computation for instance.
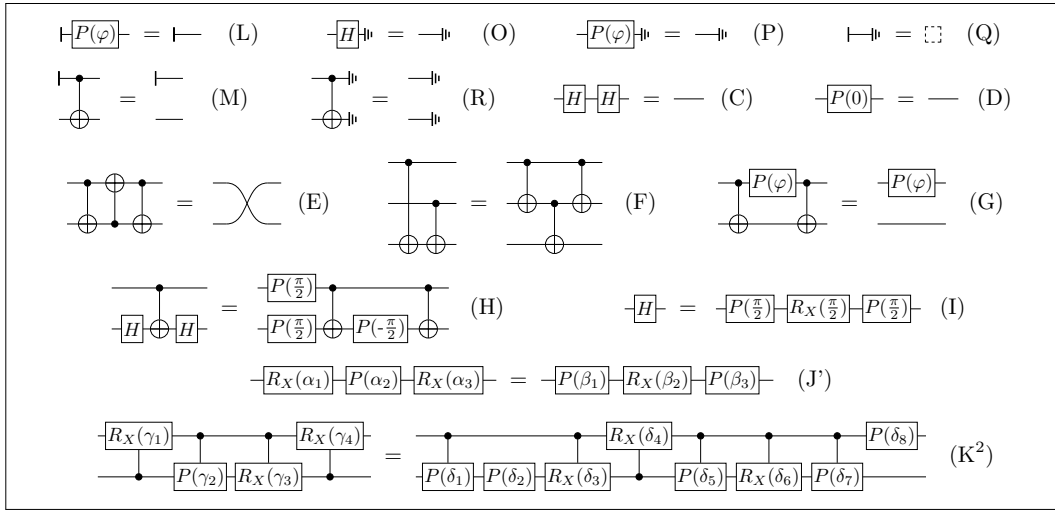
Figure 6 Equational theory $\text{QC}_{\text{discard}}$. It contains all the equations of $\text{QC}_{\text{ancilla}}$ except Equations (A), (B), (N) and where Equation (J) has been replaced by its global-phase free-version Equation (J'), together with Equations (O), (P) (defined for any $\varphi \in \mathbb{R}$), (Q) and (R), which are new equations governing the behaviour of the new generator ⊸.

While [45] provides a way to get completeness for quantum circuits with measurements from a complete one for isometries, we instead use [9] which provides a similar result but for isometries with discard, as the latter is a little bit more atomic than measurements. This leads us to equip $\mathbf{QC}_{\text{discard}}$-circuits with the equational theory $\text{QC}_{\text{discard}}$ defined in Figure 6, which is a global-phase-free version of $\text{QC}_{\text{ancilla}}$ where ⊸ replaces ⊣, and with the addition of:

$$-\boxed{H}\!\Vdash \;=\; -\!\Vdash \quad \text{(O)} \qquad -\boxed{P(\varphi)}\!\Vdash \;=\; -\!\Vdash \quad \text{(P)} \qquad \longmapsto\!\Vdash \;=\; \text{::} \quad \text{(Q)} \qquad \begin{array}{c} \!\Vdash \\ \oplus\!\Vdash \end{array} \;=\; \begin{array}{c} \!\Vdash \\ -\!\Vdash \end{array} \quad \text{(R)}$$

This observation allows us in particular to transport all the proofs using $\mathrm{QC_{ancilla}}$ into the present theory, the only two differences being that $\dashv\!\Vdash$ plays the role of $\dashv$ and that the $\mathrm{QC_{discard}}$ version of the proofs have no global phase φ.

▶ **Theorem 27** (Completeness). *The equational theory* $\mathrm{QC_{discard}}$, *defined in Figure 6, is complete for* $\mathbf{QC}_{\mathrm{discard}}$*-circuits.*

Proof. We can use the *discard construction* [9] to build $\mathrm{QC_{iso}^{\!\Vdash}}$ from $\mathrm{QC_{iso}}$, by adding equation:

$$\dashv\!\Vdash^{\otimes m} \circ\, U = \dashv\!\Vdash^{\otimes n} \tag{17}$$

for any $\mathbf{QC}_{\mathrm{iso}}$-circuit $U : n \to m$. The discard construction guarantees that $\mathrm{QC_{iso}^{\!\Vdash}}$ is complete for CPTP maps (Proposition 2 in [9]). It remains to prove that all equations in $\mathrm{QC_{iso}^{\!\Vdash}}$ derive from those of $\mathrm{QC_{discard}}$. All equations of the former except Equations (K^*) and (17) appear in $\mathrm{QC_{discard}}$. Those are trivially derivable. As mentioned above, it is possible to prove (K^*) from $\mathrm{QC_{discard}}$ exactly as in the case of $\mathrm{QC_{ancilla}}$ by replacing each occurrence of $\longmapsto\!\!\dashv = \text{::}$ by $\longmapsto\!\Vdash = \text{::}$. This means all the equations of $\mathrm{QC_{iso}}$ are derivable. Finally, all the equations $\dashv\!\Vdash^{\otimes m} \circ\, U = \dashv\!\Vdash^{\otimes n}$ for different isometries U can be derived from Equations (O), (P), (Q), and (R). ◀

6 Concluding remarks

We have simplified the complete equational theory for quantum circuits, and provided ones for standard extensions of quantum circuits, including qubit initialisation, ancillae, and/or qubit discarding. The equational theory can be simplified in these more general settings, leading in particular to equations acting on a bounded number of qubits, avoiding the use of controlled gates on arbitrary number of qubits. It is interesting to notice that increasing the expressive power of the model makes the equational theory simpler.

This simplification of the equational theory is a step towards a minimal equational theory (i.e. an equational theory where each equation provably cannot be derived from the other ones). Notice that based on the present work, a minimal complete equational theory for vanilla quantum circuits has been introduced recently [10], showing in particular that equations acting on an unbounded number of qubits are necessary for vanilla quantum circuits. The question of the minimality in the context of quantum circuits with qubit initialisation, ancillae, and/or qubit discarding remains open.

Getting rid of Equation (K^*) eases also the practical implementation of the rewriting rules as it avoids to consider a family of rules acting on an unbounded of qubits. Notice that regarding practical considerations, various equations presented in this paper have parameters, e.g. $-\boxed{R_X(\alpha_1)}\boxed{P(\alpha_2)}\boxed{R_X(\alpha_3)}- \;=\; -\boxed{P(\beta_1)}\boxed{R_X(\beta_2)}\boxed{P(\beta_3)}-$ that should be read as follows: for any angle α_i on the LHS, there exist β_j on the RHS so that the equation holds. β_j can be computed using fairly simple trigonometric operations. Notice that even if the equation looks non-symmetric, one can show conversely that for any β_j there exist α_i angles such that the equation holds (see Equation (21)).

References

1 Matthew Amy, Jianxin Chen, and Neil J. Ross. A finite presentation of CNOT-dihedral operators. *Electronic Proceedings in Theoretical Computer Science*, 266:84–97, February 2018. `doi:10.4204/eptcs.266.5`.

2 Atul Singh Arora, Andrea Coladangelo, Matthew Coudron, Alexandru Gheorghiu, Uttam Singh, and Hendrik Waldner. Quantum depth in the random oracle model. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1111–1124. ACM, 2023. `doi:10.1145/3564246.3585153`.

3 Miriam Backens, Aleks Kissinger, Hector Miller-Bakewell, John van de Wetering, and Sal Wolffs. Completeness of the ZH-calculus. *Compositionality*, 5, July 2023. `doi:10.32408/compositionality-5-5`.

4 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, March 2021. `doi:10.22331/q-2021-03-25-421`.

5 Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, November 1995. `doi:10.1103/physreva.52.3457`.

6 Xiaoning Bian and Peter Selinger. Generators and relations for 2-qubit Clifford+T operators. *Proceedings of QPL'22, Electronic Proceedings in Theoretical Computer Science*, 394:13–28, November 2023. `doi:10.4204/eptcs.394.2`.

7 Xiaoning Bian and Peter Selinger. Generators and relations for 3-qubit Clifford+CS operators. *Proceedings QPL'23, Electronic Proceedings in Theoretical Computer Science*, 384:114–126, August 2023. `doi:10.4204/eptcs.384.7`.

8 Robert I. Booth and Titouan Carette. Complete ZX-Calculi for the Stabiliser Fragment in Odd Prime Dimensions. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:15, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.MFCS.2022.24`.

9 Titouan Carette, Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Completeness of graphical languages for mixed state quantum mechanics. *ACM Transactions on Quantum Computing*, 2(4), December 2021. `doi:10.1145/3464693`.

10 Alexandre Clément, Noé Delorme, and Simon Perdrix. Minimal equational theories for quantum circuits, 2023. `arXiv:2311.07476`.

11 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. LO$_v$-Calculus: A Graphical Language for Linear Optical Quantum Circuits. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 35:1–35:16, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.MFCS.2022.35`.

12 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. A complete equational theory for quantum circuits. In *Logic in Computer Science (LICS)*, 2023.

13 Alexandre Clément, Noé Delorme, Simon Perdrix, and Renaud Vilmart. Quantum circuit completeness: Extensions and simplifications, 2023. `arXiv:2303.03117`.

14 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.

15 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`.

16   Bob Coecke and Quanlong Wang. ZX-rules for 2-qubit Clifford+T quantum circuits. In *International Conference on Reversible Computation*, pages 144–161. Springer, 2018.

17   Vincent Danos, Elham Kashefi, Prakash Panangaden, and Simon Perdrix. Extended measurement calculus. *Semantic techniques in quantum computation*, pages 235–310, 2009.

18   Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and Effective Techniques for T-Count Reduction via Spider Nest Identities. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:23, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. `doi:10.4230/LIPIcs.TQC.2020.11`.

19   D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 425(1868):73–90, 1989.

20   Amar Hadzihasanovic. *The algebra of entanglement and the geometry of composition.* PhD thesis, University of Oxford, 2017.

21   Amar Hadzihasanovic, Kang Feng Ng, and Quanlong Wang. Two complete axiomatisations of pure-state qubit quantum computing. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 502–511, New York, NY, USA, 2018. ACM. `doi:10.1145/3209108.3209128`.

22   Atsuya Hasegawa and François Le Gall. An optimal oracle separation of classical and quantum hybrid schemes. In Sang Won Bae and Heejin Park, editors, *33rd International Symposium on Algorithms and Computation, ISAAC 2022, December 19-21, 2022, Seoul, Korea*, volume 248 of *LIPIcs*, pages 6:1–6:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. `doi:10.4230/LIPIcs.ISAAC.2022.6`.

23   Mathieu Huot and Sam Staton. Universal properties in quantum theory. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 213–223, 2019. `doi:10.4204/EPTCS.287.12`.

24   Toshinari Itoko, Rudy Raymond, Takashi Imamichi, and Atsushi Matsuo. Optimization of quantum circuit mapping using gate transformation and commutation. *Integration*, 70:43–50, 2020.

25   Kazuo Iwama, Yahiko Kambayashi, and Shigeru Yamashita. Transformation rules for designing CNOT-based quantum circuits. In *Proceedings of the 39th annual Design Automation Conference*, pages 419–424, 2002.

26   Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 559–568. ACM, 2018. `doi:10.1145/3209108.3209131`.

27   Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 569–578. ACM, 2018. `doi:10.1145/3209108.3209139`.

28   Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A generic normal form for ZX-diagrams and application to the rational angle completeness. In *34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, Vancouver, BC, Canada, June 24-27, 2019*, pages 1–10. IEEE, 2019. `doi:10.1109/LICS.2019.8785754`.

29   Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Completeness of the ZX-Calculus. *Logical Methods in Computer Science*, Volume 16, Issue 2, June 2020. `doi:10.23638/LMCS-16(2:11)2020`.

30   Aleks Kissinger and John van de Wetering. PyZX, 2018. URL: `https://github.com/Quantomatic/pyzx`.

31 Aleks Kissinger and John van de Wetering. Reducing the number of non-Clifford gates in quantum circuits. *Phys. Rev. A*, 102:022406, August 2020. `doi:10.1103/PhysRevA.102.022406`.

32 Stephen Lack. Composing PROPs. In *Theory and Applications of Categories*, volume 13(9), pages 147–163, 2004. URL: `http://www.tac.mta.ca/tac/volumes/13/9/13-09abs.html`.

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

34 Dmitri Maslov, Gerhard W Dueck, D Michael Miller, and Camille Negrevergne. Quantum circuit simplification and level compaction. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 27(3):436–444, 2008.

35 Dmitri Maslov, Christina Young, D Michael Miller, and Gerhard W Dueck. Quantum circuit simplification using templates. In *Design, Automation and Test in Europe*, pages 1208–1213. IEEE, 2005.

36 D Michael Miller, Dmitri Maslov, and Gerhard W Dueck. A transformation based algorithm for reversible logic synthesis. In *Proceedings of the 40th annual Design Automation Conference*, pages 318–323, 2003.

37 Cristopher Moore and Martin Nilsson. Parallel quantum computation and quantum codes. *SIAM journal on computing*, 31(3):799–815, 2001.

38 Yunseong Nam, Neil J Ross, Yuan Su, Andrew M Childs, and Dmitri Maslov. Automated optimization of large quantum circuits with continuous parameters. *npj Quantum Information*, 4(1):1–12, 2018.

39 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

40 C.C. Paige and M. Wei. History and generality of the CS decomposition. *Linear Algebra and its Applications*, 208-209:303–326, 1994. `doi:10.1016/0024-3795(94)90446-4`.

41 Boldizsár Poór, Quanlong Wang, Razin A. Shaikh, Lia Yeh, Richie Yeung, and Bob Coecke. Completeness for arbitrary finite dimensions of ZXW-calculus, a unifying calculus. In *LICS*, pages 1–14, 2023. `doi:10.1109/LICS56636.2023.10175672`.

42 André Ranchin and Bob Coecke. Complete set of circuit equations for stabilizer quantum mechanics. *Physical Review A*, 90(1):012109, 2014.

43 Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical review letters*, 86(22):5188, 2001.

44 Vivek Shende, Stephen Bullock, and Igor Markov. Synthesis of quantum logic circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 25, 2006-01-31 00:01:00 2006. URL: `https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=150894`.

45 Sam Staton. Algebraic effects, linearity, and quantum programming languages. In *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '15, pages 395–406, New York, NY, USA, 2015. Association for Computing Machinery. `doi:10.1145/2676726.2676999`.

46 W Forrest Stinespring. Positive functions on c^*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

47 Renaud Vilmart. A near-minimal axiomatisation of ZX-calculus for pure qubit quantum mechanics. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–10, 2019. `doi:10.1109/LICS.2019.8785765`.

A   Derivations of the equations of QC$_{\mathrm{old}}$

In this appendix, we derive the equations of QC$_{\mathrm{old}}$ that are not in QC, namely Equations (8),(9),(10),(11),(12) and (13) (the proof of Equation (K$^*_{\mathrm{old}}$) can be found in the full version of the present paper [13]). In addition, we prove some other useful equations (depicted

in Figure 7) that are used as intermediate steps. Note that QC contains all equations of QC$_{\text{old}}$ acting on at most one qubit, thus QC is complete for one-qubit circuits and all equations of Figure 7 on one qubit are derivable. The proofs of the remaining equations are given below.
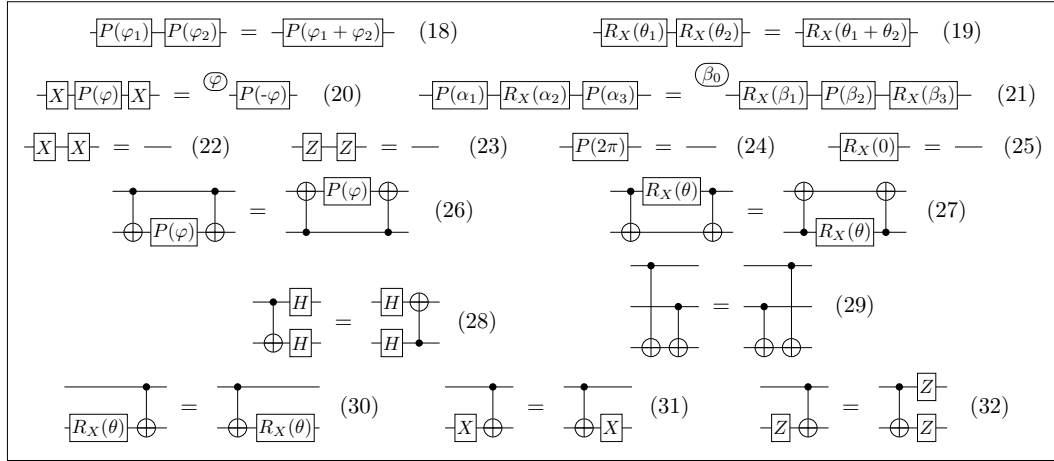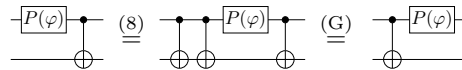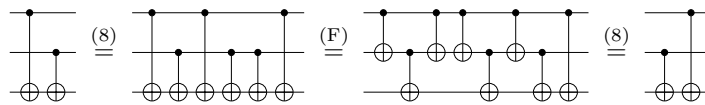

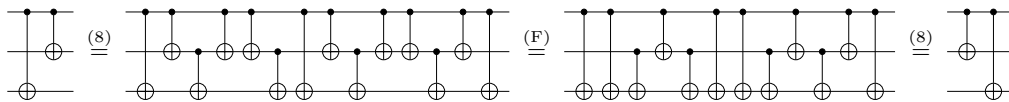**Figure 7** Useful intermediate equations.

Proof of Equation (8).
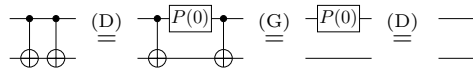
Proof of Equation (9).

Proof of Equation (29).

Proof of Equation (11).

Proof of Equation (26).

Proof of Equation (28).

◀
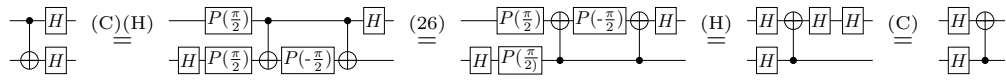
Proof of Equation (31).

◀
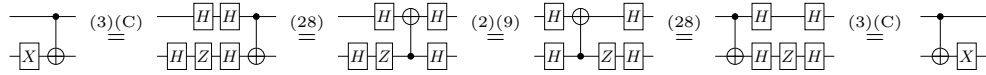
Proof of Equation (30).

◀
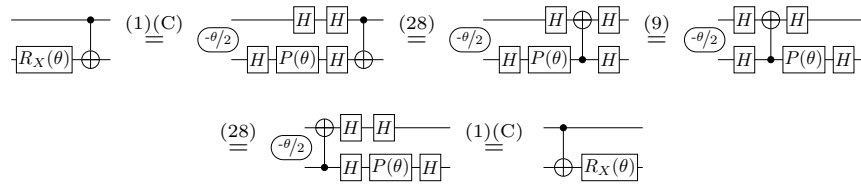
Proof of Equation (27).

◀
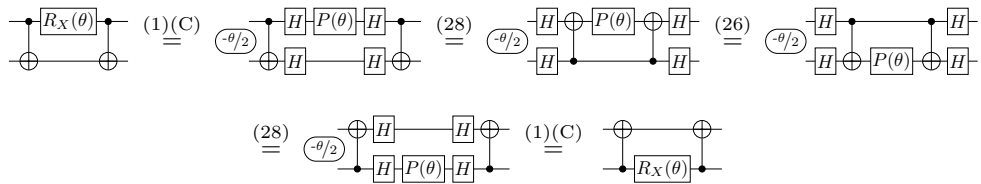
Proof of Equation (10).

◀

Proof of Equation (32).

$$\text{[circuit derivation]} \quad \overset{(3)(C)}{=} \quad \overset{(28)}{=} \quad \overset{(22)(10)}{=} \quad \overset{(28)}{=} \quad \overset{(3)}{=} \quad \blacktriangleleft$$

Proof of Equation (12). We first show that any circuits (containing four CNot gates) of the form [circuit with C_1, C_2, C_3, C_4, C_5 and four CNot gates] can always be transformed in QC into a circuit (containing only two CNot gates) of the form [circuit φ with C_6, C_7, C_8] where $-\boxed{C_i}-$ denotes a one-qubit circuit. This uses the fact (referenced $(*)$ below) that any one-qubit circuit can be transformed in QC into a circuit of the form $\overset{\alpha_0}{}\boxed{R_X(\alpha_1)}\boxed{P(\alpha_2)}\boxed{R_X(\alpha_3)}$ or $\overset{\beta_0}{}\boxed{P(\beta_1)}\boxed{R_X(\beta_2)}\boxed{P(\beta_3)}$ (by the completeness of QC for one-qubit circuits and the well-know Euler-decomposition). The derivation goes as follows.

$$\text{[circuit with } C_1, C_2, C_3, C_4, C_5 \text{]}$$

$$\overset{(*)(B)}{=} \quad \boxed{\alpha_0 + \beta_0}\ C_1\ P(\alpha_1)\ R_X(\alpha_2)\ P(\alpha_3)\ C_3\ P(\beta_1)\ R_X(\beta_2)\ P(\beta_3)\ C_5$$

$$\overset{(9)}{=} \quad \boxed{\alpha_0 + \beta_0}\ C_1\ P(\alpha_1)\ R_X(\alpha_2)\ P(\alpha_3)\ C_3\ P(\beta_1)\ R_X(\beta_2)\ P(\beta_3)\ C_5$$

$$\overset{(*)(B)}{=} \quad \boxed{\alpha_0 + \beta_0 + \gamma_0}\ C_1\ P(\alpha_1)\ R_X(\alpha_2)\ R_X(\gamma_1)\ P(\gamma_2)\ R_X(\gamma_3)\ R_X(\beta_2)\ P(\beta_3)\ C_5$$

$$\overset{(27)(30)}{=} \quad \boxed{\alpha_0 + \beta_0 + \gamma_0}\ C_1\ P(\alpha_1)\ R_X(\gamma_1)\ R_X(\alpha_2)\ P(\gamma_2)\ R_X(\beta_2)\ R_X(\gamma_3)\ P(\beta_3)\ C_5$$

$$\overset{(G)}{=} \quad \boxed{\alpha_0 + \beta_0 + \gamma_0}\ C_1\ P(\alpha_1)\ R_X(\gamma_1)\ R_X(\alpha_2)\ P(\gamma_2)\ R_X(\beta_2)\ R_X(\gamma_3)\ P(\beta_3)\ C_5$$

Then, using Equations (30) and (27), Equation (12) becomes

$$\boxed{R_X(\theta)}\ R_X(\text{-}\theta)\ H\ R_X(\theta')\ R_X(\theta')\ H \quad = \quad H\ R_X(\theta')\ R_X(\theta')\ H\ R_X(\text{-}\theta)\ R_X(\theta)$$

We can then use the above derivation to transform both circuits into circuits of the form [circuit φ with C_6, C_7, C_8]. Then, by using the simplification principle (Proposition 6), we can push the RHS circuit to the end of the LHS circuit, which leads to a circuit of the form [circuit with C_1, C_2, C_3, C_4, C_5] (up to a global phase) from which we can apply again the above derivation, leading to a circuit containing only two CNot gates. Then, by using the simplification principle again, we can turn the equation into an equivalent equation with only one CNot on both sides. Finally, the completeness of QC for circuits containing at most one CNot gate (Lemma 7) concludes the proof. $\blacktriangleleft$

Proof of Equation (13).

$$\text{[three-qubit circuit with } H, R_X(\text{-}\theta), R_X(\theta), R_X(\theta'), R_X(\text{-}\theta') \text{ gates]}$$

$$\overset{(30)}{\underset{(27)}{=}}$$

$$\overset{(29)}{\underset{(30)}{=}}$$

$$\overset{(30)}{\underset{(27)}{=}}$$

$$=$$

$$\overset{(8)}{\underset{(28)}{=}}$$

$$\overset{(29)}{\underset{(30)}{=}}$$

$$\overset{(8)}{\underset{(E)}{=}}$$

$$\overset{(F)}{=}$$

◄