



**HAL**  
open science

# Simple Complete Equational Theories for Quantum Circuits with Ancillae or Partial Trace

Alexandre Clément, Noé Delorme, Simon Perdrix, Renaud Vilmart

► **To cite this version:**

Alexandre Clément, Noé Delorme, Simon Perdrix, Renaud Vilmart. Simple Complete Equational Theories for Quantum Circuits with Ancillae or Partial Trace. 2023. hal-04016498v1

**HAL Id: hal-04016498**

**<https://hal.science/hal-04016498v1>**

Preprint submitted on 6 Mar 2023 (v1), last revised 4 Dec 2023 (v3)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Simple Complete Equational Theories for Quantum Circuits with Ancillae or Partial Trace

Alexandre Clément ✉ 🏠 

Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, 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, Inria, CNRS, 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.

Our contribution is twofold: (i) We simplify this 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) We extend the complete equational theory 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.

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.

**2012 ACM Subject Classification** Theory of computation → Quantum computation theory; Theory of computation → Equational logic and rewriting

**Keywords and phrases** Quantum Circuits, Completeness, Graphical Language

## 1 Introduction

Introduced in the 80's by Deutsch [10], the quantum circuit<sup>1</sup> 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 [11, 15, 16, 17, 20]. It is therefore convenient to equip the quantum circuit formalism with an *equational theory* providing a way to transform a quantum circuit while preserving the represented unitary map. When the equational theory is powerful enough to guarantee that any true property can be derived, it is said *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 for quantum circuits has been introduced recently [5]. Before that, complete equational theories were only known for non-universal fragments of quantum circuits, such as Clifford+T circuits acting on at most two qubits [3, 8], the stabiliser fragment [14, 23], the CNot-dihedral fragment [1], or fragments of reversible circuits [12, 7, 6].

---

<sup>1</sup> Originally called *Quantum Computational Networks*, the term *quantum circuits* is nowadays unanimously used.

Our contribution is twofold: (i) simplification of the complete equational theory and (ii) extension of the completeness result to more expressive quantum circuit models.

Indeed, we show that several rules, including two of the three most intricate ones (Figure 5), of the known complete equational theory for vanilla quantum circuits can actually be derived from the other rules, the third one (Figure 6) being slightly simplified. This leads to a simpler, more compact and easier to use complete equational theory.

Then, we consider more expressive quantum circuits by allowing ancillary qubits, a.k.a. ancillae, and qubit discarding. Indeed, *vanilla* quantum circuits do not allow for the addition or deletion of a qubit in any way: one can only apply elementary unitary gates that preserve the number of qubits.

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,<sup>2</sup> this additional space is useful in many cases. It is for instance commonly used for the construction of quantum oracles.<sup>3</sup> 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) [18]. 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<sup>4</sup>). 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 [24, 9] with this class of circuits.

In both cases – quantum circuits with ancillae and quantum circuits with qubit discarding – we introduce complete equational theories, derived from the one of vanilla quantum circuits together with a few simple additional equations associated with the new primitives (qubit initialisation and qubit discarding). We also show that in these more expressive settings the only remaining intricate rule from the equational theory of vanilla quantum circuits, can be greatly simplified.

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,<sup>5</sup> that we then use to derive the remaining equations of the already known complete equational theory introduced in [5]. 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 show the completeness of the augmented equational theory  $\text{QC}_{\text{iso}}$  using a particular circuit decomposition based on the so-called cosine-sine decomposition of unitary maps. The completeness of  $\text{QC}_{\text{iso}}$  is the cornerstone for providing complete equational

---

<sup>2</sup> Any  $n$ -qubit unitary transformation can be implemented by a  $n$ -qubit vanilla quantum circuit.

<sup>3</sup> 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  $f$  [21].

<sup>4</sup> Completely positive trace-preserving maps.

<sup>5</sup> The sub-class of quantum circuits made of at most one CNot gate.

theories for quantum circuits with ancillae ( $\mathbf{QC}_{\text{ancilla}}$  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 ( $\mathbf{QC}_{\text{discard}}$  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.

## 2 Vanilla quantum circuits

### 2.1 Graphical languages

We define quantum circuits using the formalism of props [13], 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  $C_1 : m \rightarrow n$  and  $C_2 : p \rightarrow q$  in a prop, depicted as  $m \text{---} \boxed{C_1} \text{---} n$  and  $p \text{---} \boxed{C_2} \text{---} q$  can be composed: (1) “in sequence”  $C_2 \circ C_1 : m \rightarrow q$  if  $n = p$ , graphically

$m \text{---} \boxed{C_1} \text{---} \boxed{C_2} \text{---} q$ ; (2) “in parallel”  $C_1 \otimes C_2 : m + p \rightarrow n + q$ , graphically  $m \text{---} \boxed{C_1} \text{---} n$  and  $p \text{---} \boxed{C_2} \text{---} q$ . The *unit* for

tensor product  $\otimes$  is the *empty circuit*:  $\boxed{\phantom{C}} : 0 \rightarrow 0$ . This means  $\boxed{\phantom{C}} \otimes C = C = C \otimes \boxed{\phantom{C}}$  for any  $C$ . The circuit  $\text{---} : 1 \rightarrow 1$  depicts the identity,  $\text{---} \text{---} : 2 \rightarrow 2$  is the identity on two wires and more generally  $\text{---}^{\otimes m} := \text{---} \otimes \text{---}^{\otimes m-1} : m \rightarrow m$  (with  $\text{---}^{\otimes 0} := \boxed{\phantom{C}}$ ) is the identity on  $m$  wires. Graphically, we obviously have  $\text{---}^{\otimes n} \circ C = C = C \circ \text{---}^{\otimes m}$  for any  $C : m \rightarrow n$ . Finally, a prop is also endowed with a particular circuit  $\text{---} \text{---} : 2 \rightarrow 2$  which graphically (and semantically in what follows) swaps places. By compositions, we may build

$$\begin{array}{c} \text{---} \\ \text{---} \end{array} \text{---} \text{---} : m + n \rightarrow n + m$$

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 without bending wires backwards”. For instance, the following identities are valid transformations:

$$\begin{array}{c} \text{---} \\ \text{---} \end{array} \text{---} \text{---} = \text{---} \text{---} \quad \begin{array}{c} m \text{---} \\ p \text{---} \end{array} \boxed{C_1} \text{---} \boxed{C_2} \text{---} \begin{array}{c} n \\ q \end{array} = \begin{array}{c} m \text{---} \\ p \text{---} \end{array} \boxed{C_2} \text{---} \boxed{C_1} \text{---} \begin{array}{c} n \\ q \end{array} \quad \begin{array}{c} m \text{---} \\ p \text{---} \end{array} \text{---} \text{---} \text{---} \text{---} = \begin{array}{c} m \text{---} \\ p \text{---} \end{array} \boxed{C} \text{---} \text{---} \text{---} \text{---} \begin{array}{c} n \\ n \end{array}$$

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 Hadamard, Phase gates, and CNot together with global phases:

► **Definition 1.** Let  $\mathbf{QC}$  be the prop generated by  $\text{---} \text{---} : 1 \rightarrow 1$ ,  $\text{---} \text{---} : 1 \rightarrow 1$ ,  $\text{---} \text{---} : 2 \rightarrow 2$ ,  $\text{---} : 0 \rightarrow 0$  for any  $\varphi \in \mathbb{R}$ .

► **Definition 2 (Semantics).** For any  $n$ -qubit quantum circuit  $C \in \mathbf{QC}$ , let  $\llbracket C \rrbracket : \mathbb{C}^{\{0,1\}^n} \rightarrow \mathbb{C}^{\{0,1\}^n}$  be the semantics of  $C$  inductively defined as the linear map  $\llbracket C_2 \circ C_1 \rrbracket = \llbracket C_2 \rrbracket \circ \llbracket C_1 \rrbracket$ ;  $\llbracket C_1 \otimes C_2 \rrbracket = \llbracket C_1 \rrbracket \otimes \llbracket C_2 \rrbracket$ ; and

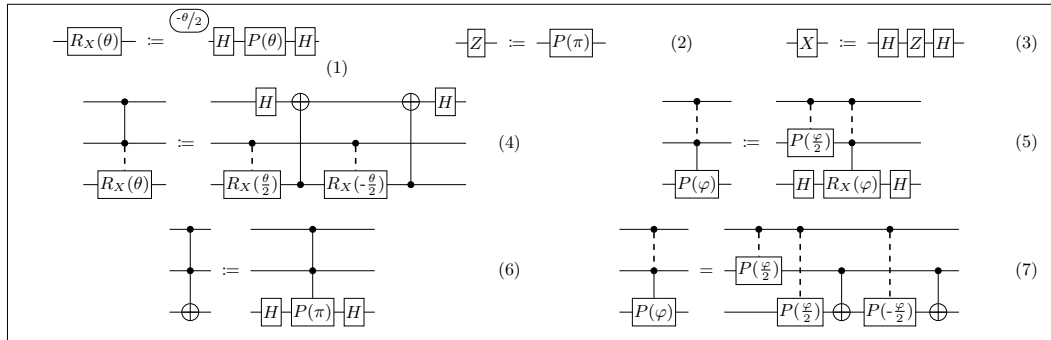
$$\begin{aligned} \llbracket \text{I} \rrbracket &= 1 \mapsto 1 & \llbracket \text{P}(\varphi) \rrbracket &= 1 \mapsto e^{i\varphi} & \llbracket \text{H} \rrbracket &= |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}} & \llbracket \text{P}(\varphi) \rrbracket &= |x\rangle \mapsto e^{ix\varphi} |x\rangle \\ \llbracket \text{CNOT} \rrbracket &= |x, y\rangle \mapsto |x, x \oplus y\rangle & \llbracket \text{X} \rrbracket &= |x\rangle \mapsto |x\rangle & \llbracket \text{CNOT} \rrbracket &= |x, y\rangle \mapsto |y, x\rangle \end{aligned}$$

Note that for any quantum circuit  $C \in \mathbf{QC}$ ,  $\llbracket C \rrbracket$  is unitary. Conversely, any unitary map acting on a finite number of qubits can be represented by a  $\mathbf{QC}$ -circuit:

► **Proposition 3 (Folklore).**  $\mathbf{QC}$  is universal, i.e. for any  $n$ -qubit unitary  $U : \mathbb{C}^{\{0,1\}^n} \rightarrow \mathbb{C}^{\{0,1\}^n}$  there exists a quantum circuit  $C \in \mathbf{QC}$  such that  $\llbracket C \rrbracket = U$ .

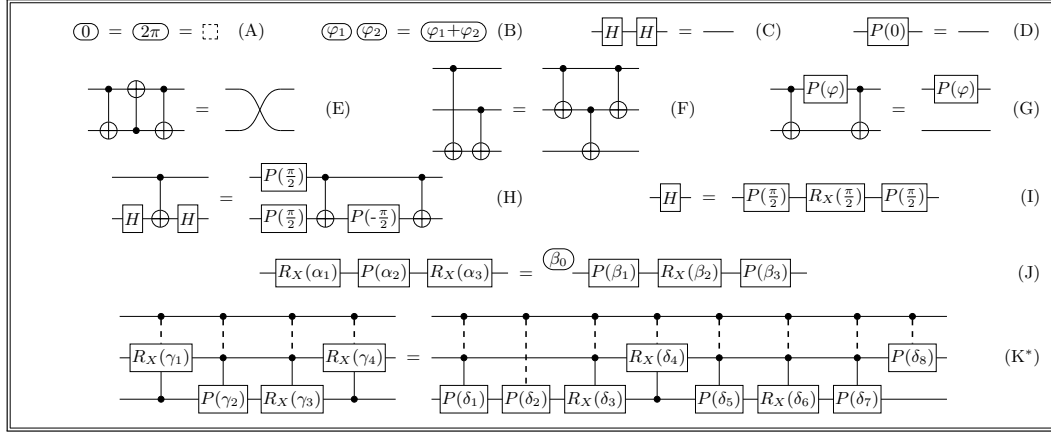
Quantum circuits only have four different kinds of generators, however, it is often convenient to use other gates that can be defined by combining them. For instance, following [2, 5], Pauli gates, Toffoli,  $X$ -rotations, and multi-controlled gates are defined in Figure 1. Note that while the phase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

We use the standard bullet-based notation for multi-controlled gates. For instance  $\text{CNOT}_{\text{P}(\varphi)}$  denotes the application of a phase gate  $\text{P}(\varphi)$  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.  $\text{CNOT}_{\text{P}(\varphi)}^{n+1}$  :  $n+1 \rightarrow n+1$  or simply  $\text{CNOT}_{\text{P}(\varphi)}^n$  :  $n+1 \rightarrow n+1$  have  $n \geq 0$  control qubits (possibly zero), whereas  $\text{CNOT}_{\text{P}(\varphi)}^{n+2}$  :  $n+2 \rightarrow n+2$  and  $\text{CNOT}_{\text{P}(\varphi)}^{1+n+1}$  :  $1+n+1 \rightarrow 1+n+1$  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 an alternative definition of the multi-controlled phase gate that is proved to be equivalent to Equation (5) in Appendix B.1.

We equip the vanilla quantum circuits with the equational theory  $\mathbf{QC}$  defined in Figure 2. We write  $\mathbf{QC} \vdash C_1 = C_2$  when  $C_1$  can be transformed into  $C_2$  using the equations of  $\mathbf{QC}$ . More formally,  $\mathbf{QC} \vdash \cdot = \cdot$  is the smallest congruence which satisfies the equations of Figure 2 together with the deformation rules that come with the prop formalism.  $\mathbf{QC}$  is sound, i.e. for any vanilla quantum circuits  $C_1, C_2 \in \mathbf{QC}$  if  $\mathbf{QC} \vdash C_1 = C_2$  then  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$ . This can be proved by observing that all equations of  $\mathbf{QC}$  are sound. We can prove the usual circuit identities of Figure 3 using the equations of  $\mathbf{QC}$  (the derivations are given in Appendix B.2). We can also prove the identities of Figure 4 about multi-controlled gates (see Appendix B.3) in  $\mathbf{QC}$ .



■ **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) is nothing but the well-known Euler-decomposition rule 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  $\beta_j$  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. Equation (K\*) can be seen as a generalisation of the Euler rule, using multi-controlled gates. 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  $\delta_j$  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  $\delta_5 = 0$ .

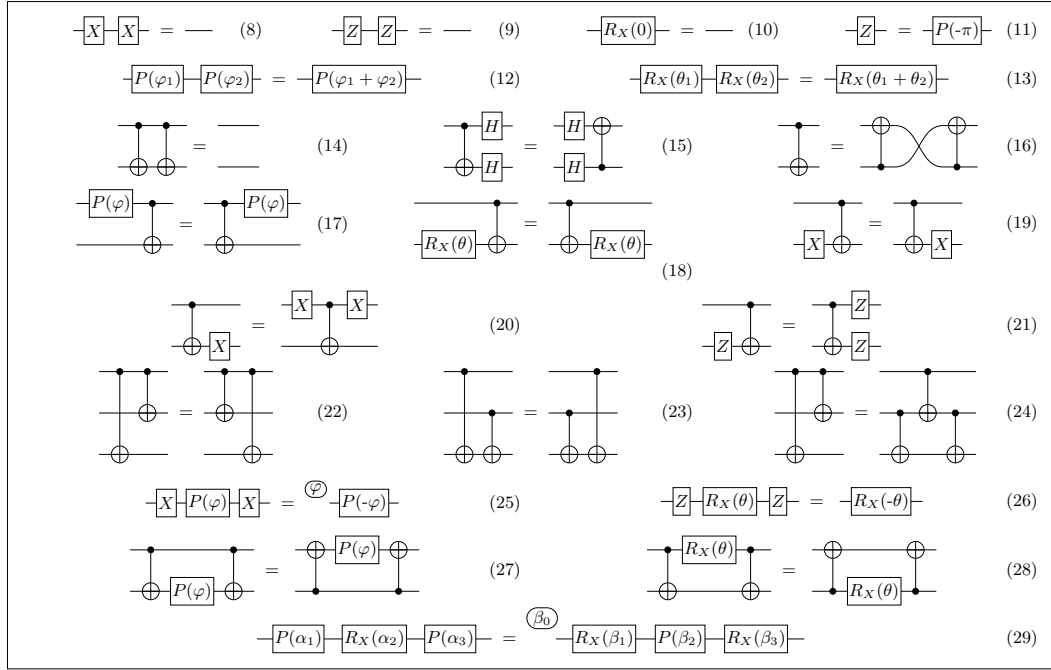
A complete equational theory for vanilla quantum circuits has been introduced in [5]. The rules of this original equational theory that are not in QC are Equations (14), (17), (20), (22), (38), (39) and (K\*<sub>old</sub>) (see Figures 3, 5, and 6).<sup>6</sup> Compared to the original equational theory, Equations (14) and (17) are now subsumed by Equation (G) in QC, Equation (K\*) is a slight simplification of Equation (K\*<sub>old</sub>) (with one less parameter in the RHS circuit), whereas Equations (20) and (22) (Figure 3) together with Equations (38) and (39) (Figure 5) have been removed, as we prove in the following that they can be derived in QC.

### 2.3 Reasoning on quantum circuits

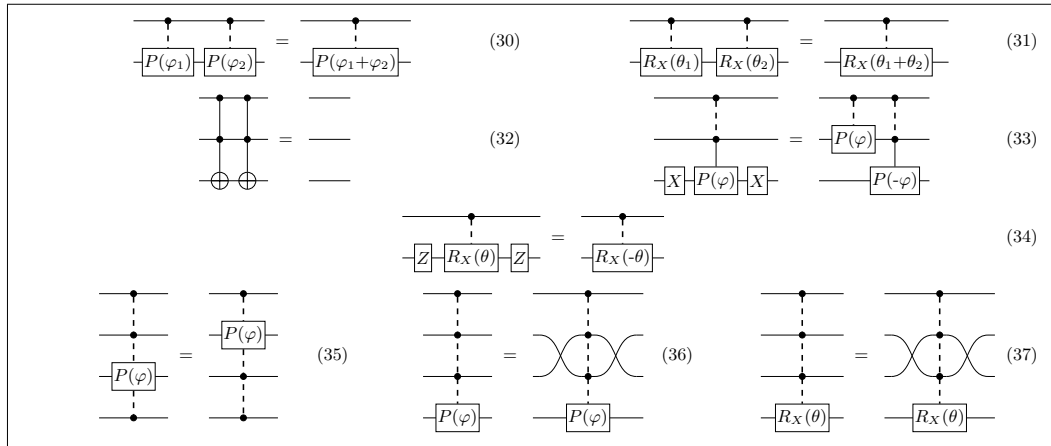
To derive an equation  $C_1 = C_2$  over quantum circuits, one can apply some rules of the equational theory to transform step by step  $C_1$  into  $C_2$ . In the context of vanilla quantum circuits, we can take advantage of the reversibility of generators to *simplify* equations. Indeed, intuitively, proving  $C_1 \circ \text{-H-} = C_2 \circ \text{-H-}$  is equivalent to proving  $C_1 = C_2$  as  $\text{-H-}$  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  $n$ -qubit quantum circuit  $C \in \mathbf{QC}$ , 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  $\varphi \in \mathbb{R}$ ,  $(\text{-}\varphi\text{-})^\dagger := \text{-}\varphi\text{-}$ ,  $(\text{-}P(\varphi)\text{-})^\dagger := \text{-}P(-\varphi)\text{-}$ , and  $g^\dagger := g$  for any other generator  $g$ .

<sup>6</sup> Notice that Equations (12) and (25) are in the original equational theory of [5] but are proved to be derivable in the same paper.



■ **Figure 3** Some usual identities provable in QC for any  $\varphi, \varphi_1, \varphi_2, \theta, \theta_1, \theta_2 \in \mathbb{R}$ . Equation (29) is the dual version of Equation (J) where the angles are computed in a similar way. All the proofs are given in Appendix B.2.



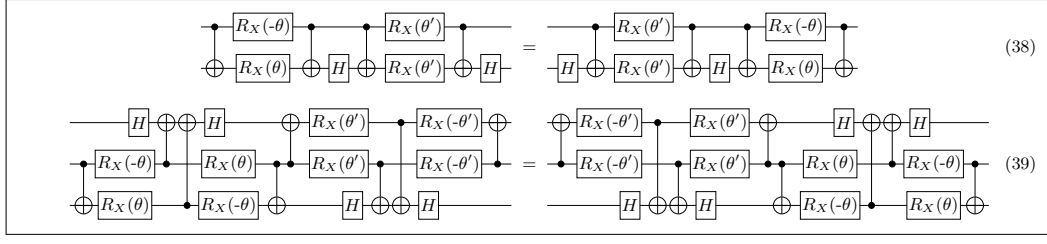
■ **Figure 4** Some usual identities over multi-controlled gates provable in QC for any  $\varphi, \varphi_1, \varphi_2, \theta, \theta_1, \theta_2 \in \mathbb{R}$ . All the proofs are given in Appendix B.3.

► **Proposition 5.**  $\llbracket C^\dagger \rrbracket = \llbracket C \rrbracket^\dagger$  for any vanilla quantum circuit  $C \in \mathbf{QC}$ , where  $\llbracket C \rrbracket^\dagger$  is the usual linear algebra adjoint of  $\llbracket C \rrbracket$ .

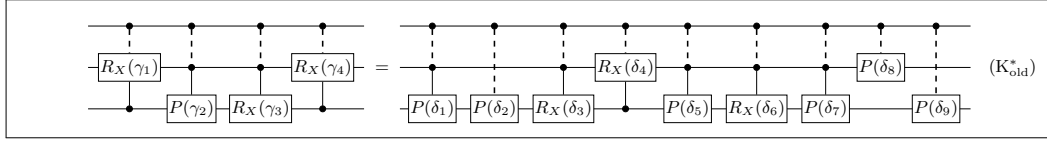
**Proof.** By induction on  $C$ . ◀

► **Proposition 6.**  $\mathbf{QC} \vdash C \circ C^\dagger = \text{---}^{\otimes n}$  and  $\mathbf{QC} \vdash C^\dagger \circ C = \text{---}^{\otimes n}$  for any  $n$ -qubit vanilla quantum circuit  $C \in \mathbf{QC}$ .

**Proof.** By induction on  $C$ . ◀



■ **Figure 5** Two of the equations of the complete equational theory introduced in [5] that are not in QC, defined for any  $\theta, \theta' \in \mathbb{R}$ .



■ **Figure 6** The version of Equation (K\*) given in [5]. Similarly to Equation (K\*), 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  $\delta_j$  are uniquely determined by assuming that  $\delta_1, \delta_2, \delta_5 \in [0, \pi)$ ,  $\delta_3, \delta_4, \delta_6, \delta_7, \delta_8, \delta_9 \in [0, 2\pi)$ , 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  $\delta_4 = \pi$  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  $\delta_j$  for  $1 \leq j \leq 8$  are the same as in Equation (K\*) except for  $\delta_4$ , which is restricted to be in  $[0, 2\pi)$  instead of  $[0, 4\pi)$ , and for  $\delta_2$ , which has to be 0 when  $\delta_3 = 0$  even if  $\delta_6 = 0$ .

Formally, we say that an equation  $C_1 = C_2$  is QC-equivalent to another equation  $C_3 = C_4$ , denoted  $(C_1 = C_2) \sim_{\text{QC}} (C_3 = C_4)$ , if  $\text{QC} \vdash C_1 = C_2 \iff \text{QC} \vdash C_3 = C_4$ , i.e. proving one in QC implies that the other is provable in QC. Proposition 7 allows us to move gates from one side of the equation to the other.

► **Proposition 7.**  $(C_2 \circ C \circ C_1 = C') \sim_{\text{QC}} (C = C_2^\dagger \circ C' \circ C_1^\dagger)$  for any  $n$ -qubit vanilla quantum circuits  $C, C', C_1, C_2 \in \text{QC}$ .

**Proof.** W.l.o.g. assume  $\text{QC} \vdash C_2 \circ C \circ C_1 = C'$ , then, thanks to Proposition 6, we have  $\text{QC} \vdash C = C_2^\dagger \circ C_2 \circ C \circ C_1 \circ C_1^\dagger = C_2^\dagger \circ C' \circ C_1^\dagger$ . ◀

## 2.4 Completeness

We prove the completeness of QC by showing that every equation of the original complete equational theory introduced in [5] 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 8 (1-CNot completeness).** QC is complete for circuits containing at most one  $\begin{array}{c} \vdots \\ \oplus \\ \vdots \end{array}$ , i.e. for any quantum circuits  $C_1, C_2 \in \text{QC}$  with at most one  $\begin{array}{c} \vdots \\ \oplus \\ \vdots \end{array}$ , if  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$  then  $\text{QC} \vdash C_1 = C_2$ .

**Proof.** The idea of the proof is to conduct a semantic analysis to characterise the possible values of the unitaries represented by the 1-qubit circuits  $\begin{array}{c} \boxed{A_i} \\ \vdots \\ \oplus \\ \vdots \\ \boxed{B_i} \end{array}$ ,  $\begin{array}{c} \boxed{C_i} \\ \vdots \\ \oplus \\ \vdots \\ \boxed{D_i} \end{array}$  in the following equation:

$$\begin{array}{c} \boxed{A_1} \\ \vdots \\ \oplus \\ \vdots \\ \boxed{B_1} \end{array} \begin{array}{c} \bullet \\ \vdots \\ \oplus \\ \vdots \\ \bullet \end{array} \begin{array}{c} \boxed{C_1} \\ \vdots \\ \oplus \\ \vdots \\ \boxed{D_1} \end{array} = \begin{array}{c} \boxed{A_2} \\ \vdots \\ \oplus \\ \vdots \\ \boxed{B_2} \end{array} \begin{array}{c} \bullet \\ \vdots \\ \oplus \\ \vdots \\ \bullet \end{array} \begin{array}{c} \boxed{C_2} \\ \vdots \\ \oplus \\ \vdots \\ \boxed{D_2} \end{array}$$



It turns out that we can prove this equation in QC for any such unitaries (when the semantics coincide). We conclude the proof using the completeness of QC over 1-qubit circuits. The proof is given in Appendix C.1. ◀

► **Proposition 9.** *Equation (38) of Figure 5 can be derived in QC.*

**Proof.** Equation (38) is QC-equivalent to an equation whose circuits contain only one  $\text{CNOT}$ . The derivation is given in Appendix C.2. We conclude the proof using the completeness of QC for 1-CNot circuits (Lemma 8). ◀

► **Proposition 10.** *Equation (39) of Figure 5 can be derived in QC.*

**Proof.** It turns out that we can use Equation (38) to derive Equation (39) in QC. The derivation is given in Appendix C.3. ◀

► **Proposition 11.** *Equation  $(K_{\text{old}}^*)$  of Figure 6 can be derived in QC.*

**Proof.** We show that for semantic reasons, we have either the angle  $\delta_9$  in  $(K_{\text{old}}^*)$  in  $\{0, \pi\}$ , or  $\delta_2 = \delta_3 = \delta_5 = \delta_6 = 0$ . When  $\delta_9 = 0$ , Equation  $(K_{\text{old}}^*)$  can be trivially derived from Equation  $(K^*)$ . Otherwise, Equations  $(K^*)$  and  $(K_{\text{old}}^*)$  can be transformed one into the other using elementary properties of multi-controlled gates. Moreover, these transformations induce a bijection between the 8-tuples of angles  $\delta_j$  corresponding to right-hand sides of instances of Equation  $(K^*)$  and the 9-tuples corresponding to right-hand sides of instances of Equation  $(K_{\text{old}}^*)$ , so that the uniqueness of the  $\delta_j$  in Equation  $(K^*)$  follows from the uniqueness in Equation  $(K_{\text{old}}^*)$ . Details are given in Appendix C.4. ◀

► **Theorem 12.** *The equational theory QC, defined in Figure 2, is complete for QC-circuits, i.e. for any  $C_1, C_2 \in \mathbf{QC}$ , if  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$  then  $\mathbf{QC} \vdash C_1 = C_2$ .*

**Proof.** All the rules of the complete equational theory introduced in [5] that are not in QC are provable in QC: Equations (14), (17), (20), (22) are proved in Appendix B.2, Equations (38), (39) and  $(K_{\text{old}}^*)$  are proved in Propositions 9, 10 and 11 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 13.** *Let  $\mathbf{QC}_{\text{iso}}$  be the prop generated by  $\text{CNOT} : 0 \rightarrow 0$ ,  $\text{H} : 1 \rightarrow 1$ ,  $\text{P}(\varphi) : 1 \rightarrow 1$ ,  $\text{CNOT} : 2 \rightarrow 2$ ,  $\text{I} : 0 \rightarrow 1$  for any  $\varphi \in \mathbb{R}$ .*

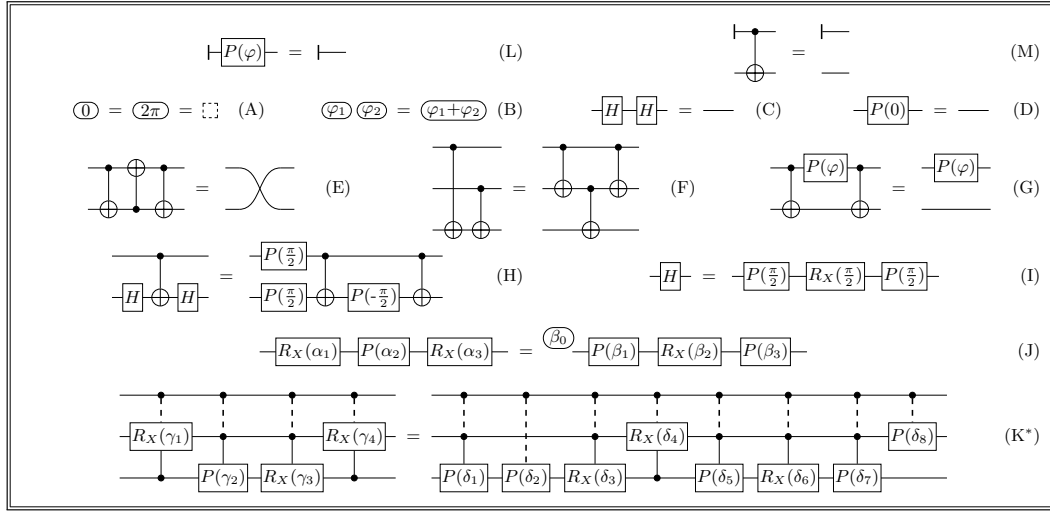
► **Definition 14 (Semantics).** *We extend the semantics  $\llbracket \cdot \rrbracket$  of vanilla quantum circuits (Definition 2) with  $\llbracket \text{I} \rrbracket = |0\rangle$ .*

► **Proposition 15.** *Any isometry<sup>7</sup>  $V : \mathbb{C}^{\{0,1\}^n} \rightarrow \mathbb{C}^{\{0,1\}^m}$  can be realised by a  $\mathbf{QC}_{\text{iso}}$ -circuit.*

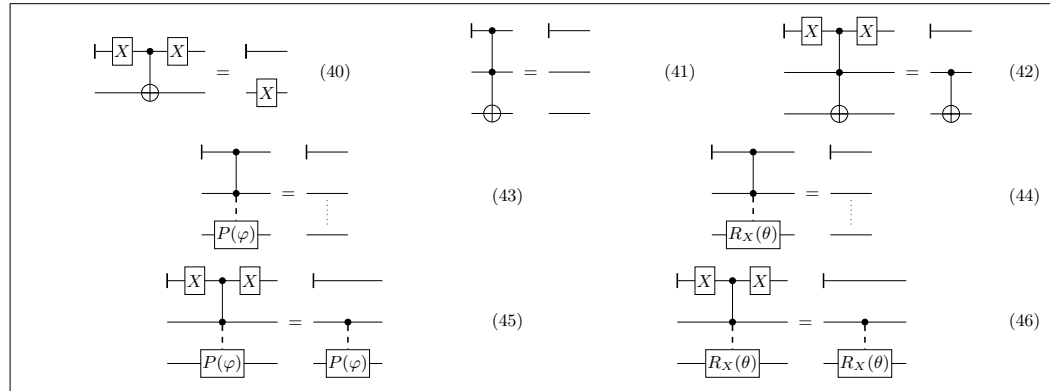
For instance, the so-called copies in the standard basis ( $|x\rangle \mapsto |xx\rangle$ ) and in the diagonal basis can be respectively represented as follows:



<sup>7</sup> An isometry is a linear map  $V$  s.t.  $V^\dagger \circ V$  is the identity.



■ **Figure 7** Equational theory  $\text{QC}_{\text{iso}}$ . It contains all the equations of  $\text{QC}$  together with Equation (L) (defined for any  $\varphi \in \mathbb{R}$ ) and Equation (M), which are new equations explaining the behaviour of the new generator  $\vdash$ .



■ **Figure 8** Some identities provable in  $\text{QC}_{\text{iso}}$  defined for any  $\varphi, \theta \in \mathbb{R}$ . Note that the proofs do not use Equation (K\*).

We consider the equational theory  $\text{QC}_{\text{iso}}$ , given in Figure 7, which is nothing but the equational theory  $\text{QC}$  augmented with the following two sound equations:

$$\vdash \boxed{P(\varphi)} = \vdash \quad (\text{L}) \qquad \vdash \begin{array}{c} \bullet \\ | \\ \oplus \end{array} = \vdash \quad (\text{M})$$

We show in the following that adding those two equations to a complete equational theory for  $\text{QC}$  gives a complete one for  $\text{QC}_{\text{iso}}$ . First we can show:

► **Lemma 16.** *Let  $C$  be a  $\text{QC}_{\text{iso}}$ -circuit such that  $\forall |\varphi\rangle \in \mathbb{C}^{2^n}$ ,  $\llbracket C \rrbracket |\varphi\rangle = |0\rangle \otimes |\varphi\rangle$ . Then:*

$$\text{QC}_{\text{iso}} \vdash \begin{array}{c} \vdots \\ | \\ \boxed{C} \\ | \\ \vdots \end{array} = \begin{array}{c} \vdash \\ | \\ \vdots \end{array}$$

**Proof.** The proof is in Appendix D. ◀

A direct corollary of Lemma 16 is the completeness of  $\mathbf{QC}_{\text{iso}}$  for quantum circuits with at most one initialisation. To show completeness of  $\mathbf{QC}_{\text{iso}}$  in general, we want to generalise this result 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  $\text{diag}(I, U)$ , 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  $\text{diag}(I, U)$  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  $\text{diag}(I, U)$  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 17.** Let  $U = \left( \begin{array}{c|cc} I & 0 & 0 \\ \hline 0 & U_{00} & U_{01} \\ \hline 0 & U_{10} & U_{11} \end{array} \right) \begin{array}{l} \}k \\ \}n-k \\ \}n \end{array}$  be unitary with  $U_{00}$  and  $U_{11}$  square.

Then, there exist:

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

such that:

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

The above decomposition is a variation on the *Cosine-Sine Decomposition* (CSD) [22], which has already proven useful in quantum circuit synthesis [25].

**Proof.** The proof itself is a variation of the proof for the usual CSD. It specifically involves the so-called RQ and SVD decompositions, which are introduced, alongside the full proof of the lemma, in Appendix D. ◀

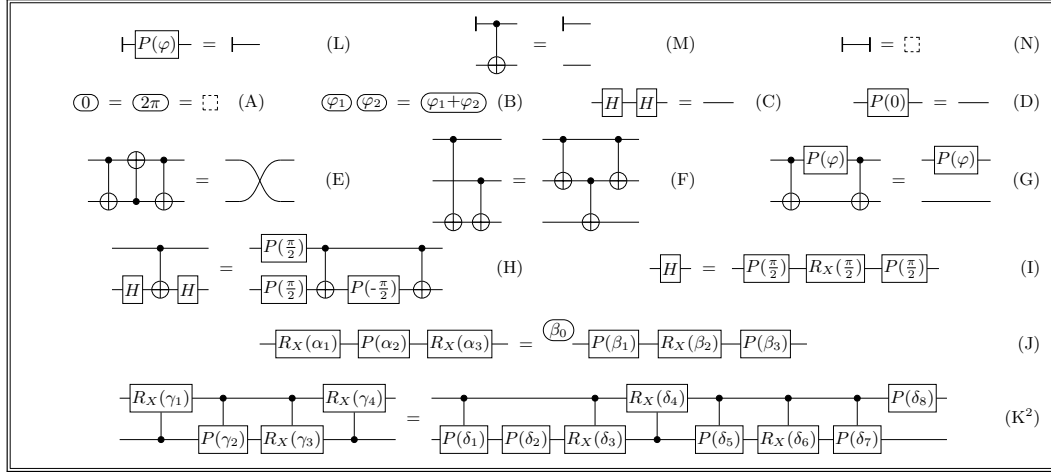
It is then possible to show the completeness of  $\mathbf{QC}_{\text{iso}}$ :

► **Theorem 18.** The equational theory  $\mathbf{QC}_{\text{iso}}$ , defined in Figure 7, is complete for  $\mathbf{QC}_{\text{iso}}$ -circuits.

**Proof.** The proof goes by showing that deriving equality between two  $\mathbf{QC}_{\text{iso}}$ -circuits amounts to generalising Lemma 16 to any number of qubit initialisations, which is shown inductively using the above variation of the CSD. The full proof is in Appendix D. ◀

## 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.



■ **Figure 9** Equational theory  $\mathbf{QC}_{\text{ancilla}}$ . It contains all the equations of  $\mathbf{QC}_{\text{iso}}$  where Equation (K<sup>\*</sup>) has been replaced by Equation (K<sup>2</sup>), together with Equation (N), which is a new equation that allows one to create ancillae.

To encounter 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 19.** Let  $\mathbf{QC}_{\text{pre-ancilla}}$  be the prop generated by  $\textcircled{0} : 0 \rightarrow 0$ ,  $\dashv\!-\!H\!-\! : 1 \rightarrow 1$ ,  $\dashv\!-\!P(\varphi)\!-\! : 1 \rightarrow 1$ ,  $\textcircled{2} : 2 \rightarrow 2$ ,  $\vdash : 0 \rightarrow 1$ ,  $\dashv : 1 \rightarrow 0$  for any  $\varphi \in \mathbb{R}$ .

► **Definition 20 (Semantics).** We extend the semantics  $\llbracket \cdot \rrbracket$  of  $\mathbf{QC}_{\text{iso}}$  (Definition 14) with  $\llbracket \dashv\!-\!H\!-\! \rrbracket = \langle 0 |$ .

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

► **Definition 21.** Let  $\mathbf{QC}_{\text{ancilla}}$  be the sub-prop of circuits  $C \in \mathbf{QC}_{\text{pre-ancilla}}$  such that  $\llbracket C \rrbracket$  is an isometry.

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 the  $\mathbf{QC}_{\text{ancilla}}$ -circuits with the equational theory  $\mathbf{QC}_{\text{ancilla}}$  given in Figure 9, which is nothing but the equational theory  $\mathbf{QC}_{\text{iso}}$  where Equation (K<sup>\*</sup>) is replaced by its 2-qubit version Equation (K<sup>2</sup>), together with a new elementary equation (N) governing the behaviour of the qubit removal generator  $\dashv$ .

$$\dashv\!-\!H\!-\! = \llbracket \textcircled{0} \rrbracket \quad (\text{N})$$

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  $C_f : n + 1 \rightarrow n + 1$

<sup>8</sup> 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.

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:

$$\boxed{C'_f} := \text{---} \begin{array}{c} \boxed{C_f} \\ \text{---} \\ \text{---} \end{array} \text{---} \\ \text{---} \boxed{X} \text{---} \boxed{H} \text{---} \boxed{C_f} \text{---} \boxed{H} \text{---} \boxed{X} \text{---} \text{---}$$

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 [18]. 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:

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \boxed{P(\varphi)} \end{array} = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \boxed{P(\varphi)} \\ \oplus \quad \oplus \end{array} \quad (47)$$

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

► **Proposition 22.** *The following two equations can be derived in  $\text{QC}_{\text{ancilla}}$ .*

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \boxed{P(\varphi)} \end{array} = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \boxed{P(\varphi)} \\ \oplus \quad \oplus \end{array} \quad (48)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \boxed{R_X(\theta)} \end{array} = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \boxed{R_X(\theta)} \\ \oplus \quad \oplus \end{array} \quad (49)$$

**Proof.** By induction on the number of qubits. The proof is given in Appendix E.1. ◀

► **Remark 23.** Notice that Equations (48) and (49) are actually derivable in  $\text{QC}_{\text{iso}}$ . However, in order to provide an alternative inductive definition of multi-control gates (like in Equation (47)), 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  $\text{QC}_{\text{ancilla}}$ , the equation  $(K^*)$  for any arbitrary number of controlled qubits:

► **Proposition 24.** *Equation  $(K^*)$  can be derived in  $\text{QC}_{\text{ancilla}}$ .*

**Proof.** Let  $(K^n)$  be Equation  $(K^*)$  acting on  $n$  qubits for any  $n \geq 2$ . Equation  $(K^2)$  is in  $\text{QC}_{\text{ancilla}}$ . 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  $(K^3)$ . The detailed proof is given in E.2 together with all necessary intermediate derivations. This technique is not applicable in the general case for any controlled 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  $\text{QC}_{\text{ancilla}}$  for any  $n \geq 4$  by induction on  $n$  using the alternative definition of multi-controlled gates (Proposition 22), which allows us to construct an instance of the LHS circuit of  $(K^{n-1})$  from the LHS circuit of  $(K^n)$ . The detailed proof is given in E.3. ◀

We are now ready to prove the completeness of  $\mathbf{QC}_{\text{ancilla}}$ :

► **Theorem 25.** *The equational theory  $\mathbf{QC}_{\text{ancilla}}$ , defined in Figure 9, is complete for  $\mathbf{QC}_{\text{ancilla}}$ -circuits.*

**Proof.** Proposition 24 implies that for any  $\dashv$ -free circuits  $C_0, C_1$ , if  $\mathbf{QC}_{\text{iso}} \vdash C_0 = C_1$  then  $\mathbf{QC}_{\text{ancilla}} \vdash C_0 = C_1$ . Using deformation of circuits, any  $\mathbf{QC}_{\text{ancilla}}$ -circuit  $C : n \rightarrow m$

can be written  $\begin{array}{c} \vdots \\ \boxed{C'} \\ \vdots \end{array}$ , where  $C' : n \rightarrow m+k$  is a  $\mathbf{QC}_{\text{iso}}$ -circuit. Since both  $\llbracket C \rrbracket$  and  $\llbracket C' \rrbracket$  are isometries and  $\llbracket C \rrbracket = (Id \otimes \langle 0^k |) \llbracket C' \rrbracket$ , we have  $\llbracket C' \rrbracket = \llbracket C \rrbracket \otimes |0^k\rangle$ . Given two  $\mathbf{QC}_{\text{ancilla}}$ -circuits  $C_0, C_1$  s.t.  $\llbracket C_0 \rrbracket = \llbracket C_1 \rrbracket$ , let  $C'_0 : n \rightarrow m+k$ , and  $C'_1 : n \rightarrow m+\ell$  be the corresponding  $\mathbf{QC}_{\text{iso}}$ -circuits. W.l.o.g. assume  $k \leq \ell$ , and pad  $C'$  with  $\ell - k$  qubit initialisations:  $C''_0 := C'_0 \otimes (\dashv)^{\otimes \ell - k}$ . We have  $\llbracket C''_0 \rrbracket = \llbracket C'_1 \rrbracket$ , so by completeness of  $\mathbf{QC}_{\text{iso}}$ ,  $\mathbf{QC}_{\text{ancilla}} \vdash C''_0 = C'_1$ , so  $\mathbf{QC}_{\text{ancilla}} \vdash C_0 \otimes (\dashv)^{\otimes \ell - k} = C_1$ . It suffices to apply the (N) rule to obtain  $\mathbf{QC}_{\text{ancilla}} \vdash C_0 = C_1$ . ◀

## 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 as follows:  $\dashv$ .

► **Definition 26.** *Let  $\mathbf{QC}_{\text{discard}}$  be the prop generated by  $\boxed{H} : 1 \rightarrow 1$ ,  $\boxed{P(\varphi)} : 1 \rightarrow 1$ ,  $\begin{array}{c} \vdots \\ \oplus \\ \vdots \end{array} : 2 \rightarrow 1$ ,  $\vdash : 0 \rightarrow 1$ ,  $\dashv : 1 \rightarrow 0$  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:

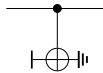
► **Definition 27 (Semantics).** *For any quantum circuit  $C : n \rightarrow m \in \mathbf{QC}_{\text{discard}}$ , let  $\langle C \rangle : \mathcal{M}_{2^n, 2^n}(\mathbb{C}) \rightarrow \mathcal{M}_{2^m, 2^m}(\mathbb{C})$  be the semantics of  $C$  inductively defined as the linear map  $\langle C_2 \circ C_1 \rangle = \langle C_2 \rangle \circ \langle C_1 \rangle$ ;  $\langle C_1 \otimes C_2 \rangle = \langle C_1 \rangle \otimes \langle C_2 \rangle$ ;  $\langle \dashv \rangle = \rho \mapsto \text{tr}(\rho)$  and for any other generator  $g$ ,  $\langle g \rangle = \rho \mapsto \llbracket g \rrbracket \rho \llbracket g \rrbracket^\dagger$ , where  $\text{tr}(M)$  is the trace of the matrix  $M$  and  $M^\dagger$  its adjoint.*

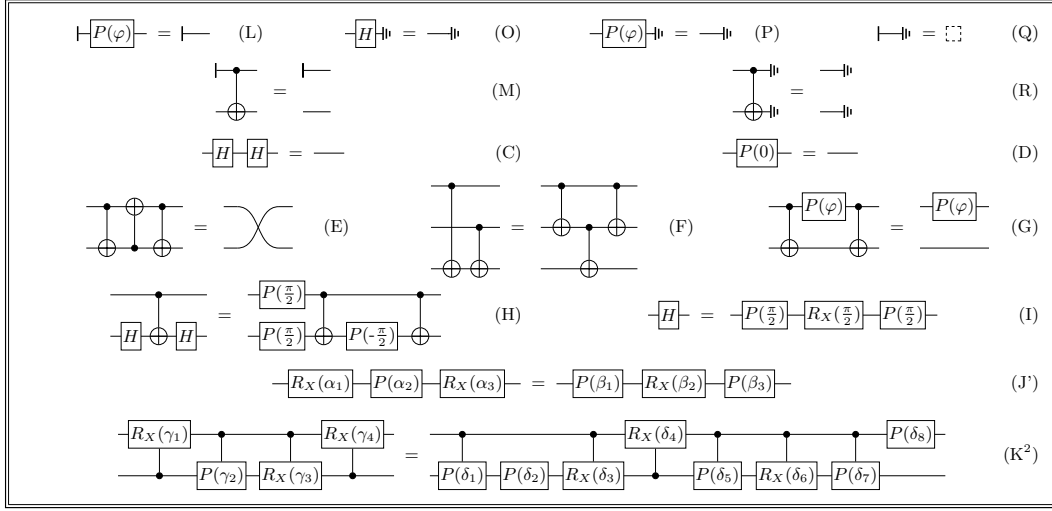
Notice that the global phase generator  $\odot$  is not part of the prop anymore. If it were, its interpretation would be  $\langle \odot \rangle = \rho \mapsto \llbracket \odot \rrbracket \rho \llbracket \odot \rrbracket^\dagger = e^{i\varphi} \rho e^{-i\varphi} = \rho$ , which is the same as that of the empty circuit.

► **Proposition 28.**  *$\mathbf{QC}_{\text{discard}}$  is universal for CPTP maps.*

**Proof.** According to the Stinespring dilation lemma [27], any CPTP map  $F : \mathcal{M}_{2^n, 2^n}(\mathbb{C}) \rightarrow \mathcal{M}_{2^m, 2^m}(\mathbb{C})$  can be purified as an isometry  $V : \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^{m+k}}$  such that for any  $\rho$ ,  $F(\rho) = \text{tr}_k(V\rho V^\dagger)$ , where  $\text{tr}_k(\cdot)$  is the partial trace of the last  $k$  qubits. By universality of  $\mathbf{QC}_{\text{iso}}$  there exists a circuit  $C$  such that  $\llbracket C \rrbracket = V$ . Let  $C'$  be the global-phase-free version of  $C$ , thus  $\llbracket C' \rrbracket = e^{i\theta} V$ . Seen as a  $\mathbf{QC}_{\text{discard}}$ -circuit,  $C'$  has the semantics  $\langle C' \rangle = \rho \mapsto (e^{i\theta} V)\rho(e^{i\theta} V)^\dagger = V\rho V^\dagger$ . Discarding the last  $k$  qubits of  $C'$  leads to a  $\mathbf{QC}_{\text{discard}}$ -circuit implementing  $F$ . ◀

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





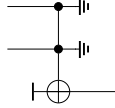
■ **Figure 10** Equational theory  $\mathbf{QC}_{\text{discard}}$ . It contains all the equations of  $\mathbf{QC}_{\text{ancilla}}$  except Equation (N) and where Equation (J) has been replaced by its global-phase free-version Equation (J'), together with Equations (O), (P) (defined for any  $\varphi \in \mathbb{R}$ ), (Q), (R), which are new equations explaining the behaviour of the new generator  $\neg$ .

Indeed we recover the semantics of the standard basis measurement:

$$\left( \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \oplus \\ \text{---} \end{array} \right) = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

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.

While [26] provides a way to get completeness for quantum circuits with measurements from a complete one for isometries, we instead use [4] 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  $\mathbf{QC}_{\text{discard}}$  with the equational theory defined in Figure 10, which is a global-phase-free version of  $\mathbf{QC}_{\text{ancilla}}$  where  $\neg$  replaces  $\neg$ , and with the addition of:

$$\begin{array}{lll} \neg H \dashv \vdash \text{---} & \text{(O)} & \neg P(\varphi) \dashv \vdash \text{---} & \text{(P)} & \dashv \vdash = \boxed{\phantom{0}} & \text{(Q)} \\ \begin{array}{c} \bullet \dashv \vdash \\ | \\ \oplus \\ \bullet \dashv \vdash \\ \text{---} \end{array} & = & \text{---} & & & \text{(R)} \end{array}$$

This observation allows us in particular to transport all the proofs using  $\text{QC}_{\text{ancilla}}$  into the present theory, the only two differences being that  $\dashv$  plays the role of  $\neg$  and that the  $\text{QC}_{\text{discard}}$  version of the proofs have no global phase  $\oplus$ .

► **Theorem 29.** *The equational theory  $\text{QC}_{\text{discard}}$ , defined in Figure 10, is complete for  $\text{QC}_{\text{discard}}$ -circuits.*

**Proof.** We can use the *discard construction* [4] to build  $\text{QC}_{\text{iso}}^{\dashv}$  from  $\text{QC}_{\text{iso}}$ , by adding equation:

$$\dashv^{\otimes m} \circ U = \dashv^{\otimes n} \quad (50)$$

for any  $\text{QC}_{\text{iso}}$ -circuit  $U : n \rightarrow m$ . The discard construction guarantees that  $\text{QC}_{\text{iso}}^{\dashv}$  is complete for CPTP maps (Proposition 2 in [4]). It remains to prove that all equations in  $\text{QC}_{\text{iso}}^{\dashv}$  derive from those of  $\text{QC}_{\text{discard}}$ . All equations of the former except  $(K^*)$  and Equation (50) appear as in  $\text{QC}_{\text{discard}}$ . Those are trivially derivable. As mentioned above, it is possible to prove  $(K^*)$  from  $\text{QC}_{\text{discard}}$  exactly as in the case of  $\text{QC}_{\text{ancilla}}$  by replacing each occurrence of  $\vdash = \square$  by  $\dashv = \square$ . This means all the equations of  $\text{QC}_{\text{iso}}$  are derivable. Finally, all the equations  $\dashv^{\otimes m} \circ U = \dashv^{\otimes n}$  for different isometries  $U$  can be derived from Equations (O), (P), (Q), and (R). ◀

## Acknowledgements

This work is supported by the PEPR integrated project EPiQ ANR-22-PETQ-0007 part of Plan France 2030, the ANR project SoftQPro ANR-17-CE25-0009-02, by the STIC-AmSud project Qapla' 21-STIC-10, and by the European projects NEASQC and HPCQS.

---

## 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. URL: <https://doi.org/10.4204/2Feptcs.266.5>, doi:10.4204/eptcs.266.5.
- 2 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. arXiv: [quant-ph/9503016](https://arxiv.org/abs/quant-ph/9503016), doi:10.1103/physreva.52.3457.
- 3 Xiaoning Bian and Peter Selinger. Generators and relations for 2-qubit Clifford+T operators. *arXiv preprint arXiv:2204.02217*, 2022.
- 4 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), dec 2021. URL: <https://doi.org/10.1145/3464693>, doi:10.1145/3464693.
- 5 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. A complete equational theory for quantum circuits. *arXiv preprint arXiv:2206.10577*, 2022.
- 6 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.
- 7 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.
- 8 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.



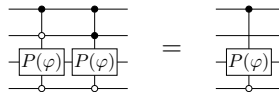
- 9 Vincent Danos, Elham Kashefi, Prakash Panangaden, and Simon Perdrix. Extended measurement calculus. *Semantic techniques in quantum computation*, pages 235–310, 2009.
- 10 D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 425(1868):73–90, 1989.
- 11 Toshinari Itoko, Rudy Raymond, Takashi Imamichi, and Atsushi Matsuo. Optimization of quantum circuit mapping using gate transformation and commutation. *Integration*, 70:43–50, 2020.
- 12 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.
- 13 Stephen Lack. Composing PROPs. In *Theory and Applications of Categories*, volume 13, pages 147–163, 2004. URL: <http://www.tac.mta.ca/tac/volumes/13/9/13-09abs.html>.
- 14 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.
- 15 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.
- 16 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.
- 17 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.
- 18 Cristopher Moore and Martin Nilsson. Parallel quantum computation and quantum codes. *SIAM journal on computing*, 31(3):799–815, 2001.
- 19 M. Möttönen and J.J. Vartiainen. *Decompositions of general quantum gates*. Nova Science Publishers Inc, United States, 2006.
- 20 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.
- 21 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.
- 22 C.C. Paige and M. Wei. History and generality of the cs decomposition. *Linear Algebra and its Applications*, 208-209:303–326, 1994. URL: <https://www.sciencedirect.com/science/article/pii/0024379594904464>, doi:[https://doi.org/10.1016/0024-3795\(94\)90446-4](https://doi.org/10.1016/0024-3795(94)90446-4).
- 23 André Ranchin and Bob Coecke. Complete set of circuit equations for stabilizer quantum mechanics. *Physical Review A*, 90(1):012109, 2014.
- 24 Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical review letters*, 86(22):5188, 2001.
- 25 Vivek Shende, Stephen Bullock, and Igor Markov. Synthesis of quantum logic circuits. (25), 2006-01-31 00:01:00 2006. URL: [https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=150894](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=150894).
- 26 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. URL: <https://doi.org/10.1145/2676726.2676999>, doi:10.1145/2676726.2676999.
- 27 W Forrest Stinespring. Positive functions on  $c^*$ -algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

- 28 Lloyd N. Trefethen and David Bau. *Numerical Linear Algebra*. Other Titles in Applied Mathematics. Society for Industrial and Applied Mathematics (SIAM, 3600 Market Street, Floor 6, Philadelphia, PA 19104), 1997. URL: <https://doi.org/10.1137/1.9780898719574>, doi:10.1137/1.9780898719574.
- 29 Farrokh Vatan and Colin Williams. Optimal quantum circuits for general two-qubit gates. *Physical Review A*, 69(3), mar 2004. URL: <https://doi.org/10.1103/PhysRevA.69.032315>, doi:10.1103/PhysRevA.69.032315.

### A Bullet-based graphical notation for multi-controlled gates

We use the standard bullet-based graphical notation for multi-controlled gates where the *negative control* (or *anti-control*)  $\ominus$  is a shortcut notation for  $\neg X \oplus X$ . For instance,  stands for the gate  $\text{P}(\varphi)$  on the third qubit positively controlled by the first and fourth qubits and negatively controlled by the second qubit. According to [5] we can simulate the expected behaviour of this bullet-based notation in QC without using Equation (K\*).

Combining a control and anti-control on the same qubit makes the evolution independent of this qubit. This is provable in QC without (K\*) and illustrated by the following example.



Another expected behaviour provable in QC without (K\*) is the fact that controlled and anti-controlled gates commute (even if the target qubits are not the same in both gates). This is illustrated by the two following examples.



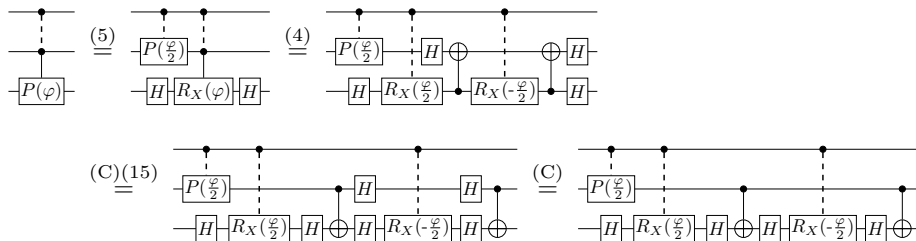
In the following, the use of such properties is denoted by  $(\diamond)$  and refers to Propositions 15, 16 and 17 (together with Propositions 10 and 11 in some cases) of [5].

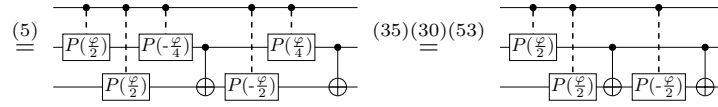
### B Proofs of circuit identities

The proofs are given in order of dependency, so as to guarantee that there is no circular reasoning.

#### B.1 Proofs of the equations of Figure 1

Proof of Equation (7).





## B.2 Proofs of the equations of Figure 3

**Proof of Equation (12) and Equation (25).** Those two equations are consequences of Equation (J). See Proposition 20 of [5].

**Proof of Equation (13).**

$$\begin{aligned} [R_X(\theta_1)] [R_X(\theta_2)] &\stackrel{(1)}{=} \left( \frac{-\theta_1 - \theta_2}{2} \right) [H] [P(\theta_1)] [H] [H] [P(\theta_2)] [H] \stackrel{(C)}{=} \left( \frac{-\theta_1 - \theta_2}{2} \right) [H] [P(\theta_1)] [P(\theta_2)] [H] \\ &\stackrel{(12)}{=} \left( \frac{\theta_1 + \theta_2}{2} \right) [H] [P(\theta_1 + \theta_2)] [H] \stackrel{(1)}{=} [R_X(\theta_1 + \theta_2)] \end{aligned}$$

**Proof of Equation (26).**

$$\begin{aligned} [Z] [R_X(\theta)] [Z] &\stackrel{(3)(1)}{=} \left( \frac{-\theta/2}{2} \right) [H] [X] [H] [H] [P(\theta)] [H] [H] [X] [H] \stackrel{(C)}{=} \left( \frac{-\theta/2}{2} \right) [H] [X] [P(\theta)] [X] [H] \\ &\stackrel{(25)}{=} \left( \frac{\theta/2}{2} \right) [H] [P(-\theta)] [H] \stackrel{(1)}{=} \left( \frac{\theta/2}{2} \right) \left( \frac{-\theta/2}{2} \right) [R_X(-\theta)] \stackrel{(B)(A)}{=} [R_X(-\theta)] \end{aligned}$$

**Proof of Equation (8).**

$$[X] [X] \stackrel{(D)}{=} [X] [P(0)] [X] \stackrel{(25)}{=} \textcircled{1} [P(0)] \stackrel{(D)(A)}{=} \text{---}$$

**Proof of Equation (9).**

$$[Z] [Z] \stackrel{(3)}{=} [H] [X] [H] [H] [X] [H] \stackrel{(C)}{=} [H] [X] [X] [H] \stackrel{(8)}{=} [H] [H] \stackrel{(C)}{=} \text{---}$$

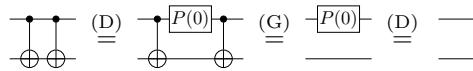
**Proof of Equation (10).**

$$[R_X(0)] \stackrel{(1)}{=} \textcircled{1} [H] [P(0)] [H] \stackrel{(D)(A)}{=} [H] [H] \stackrel{(C)}{=} \text{---}$$

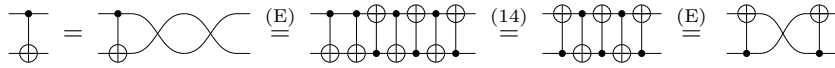
**Proof of Equation (11).**

$$[Z] \stackrel{(D)}{=} [P(0)] [Z] \stackrel{(12)}{=} [P(-\pi)] [P(\pi)] [Z] \stackrel{(2)}{=} [P(-\pi)] [Z] [Z] \stackrel{(9)}{=} [P(-\pi)]$$

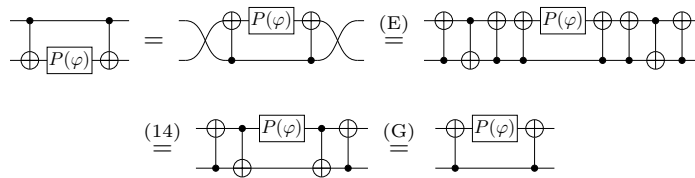
Proof of Equation (14).



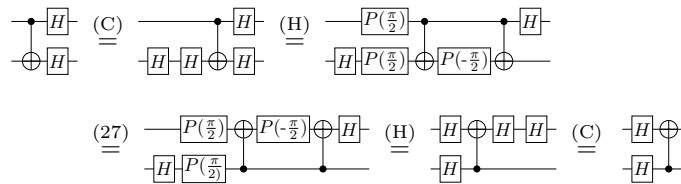
Proof of Equation (16).



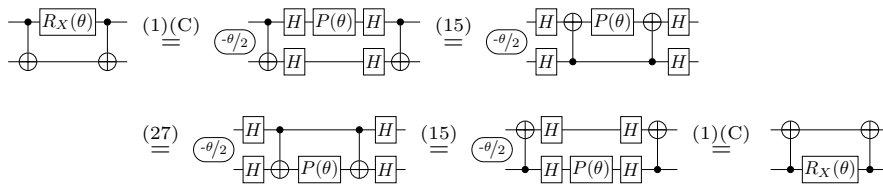
Proof of Equation (27).



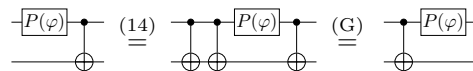
Proof of Equation (15).



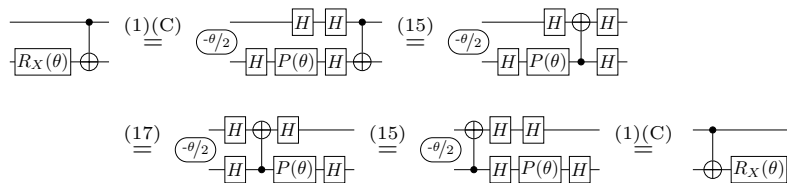
Proof of Equation (28).



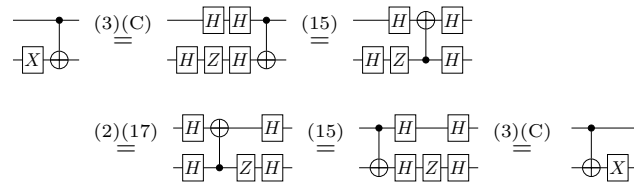
Proof of Equation (17).



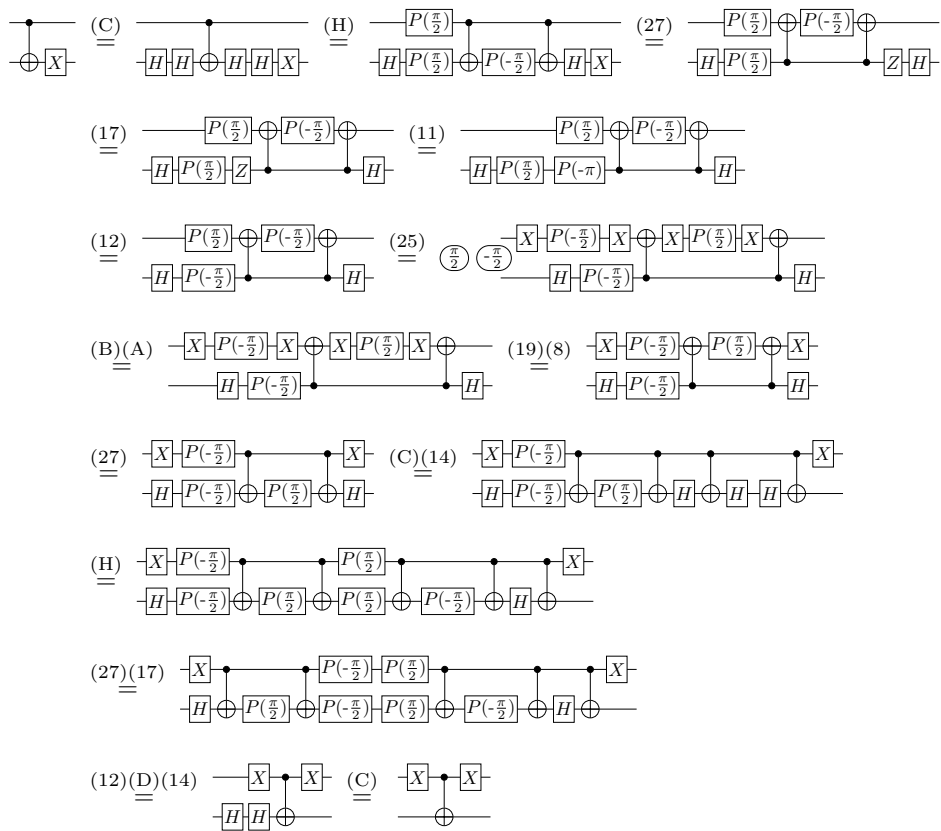
Proof of Equation (18).



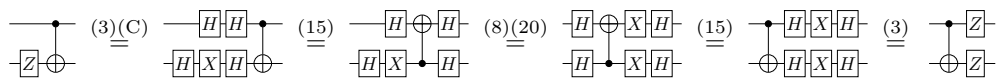
Proof of Equation (19).



Proof of Equation (20).



Proof of Equation (21).



Proof of Equation (22).

Proof of Equation (23).

Proof of Equation (24).

Proof of Equation (29).

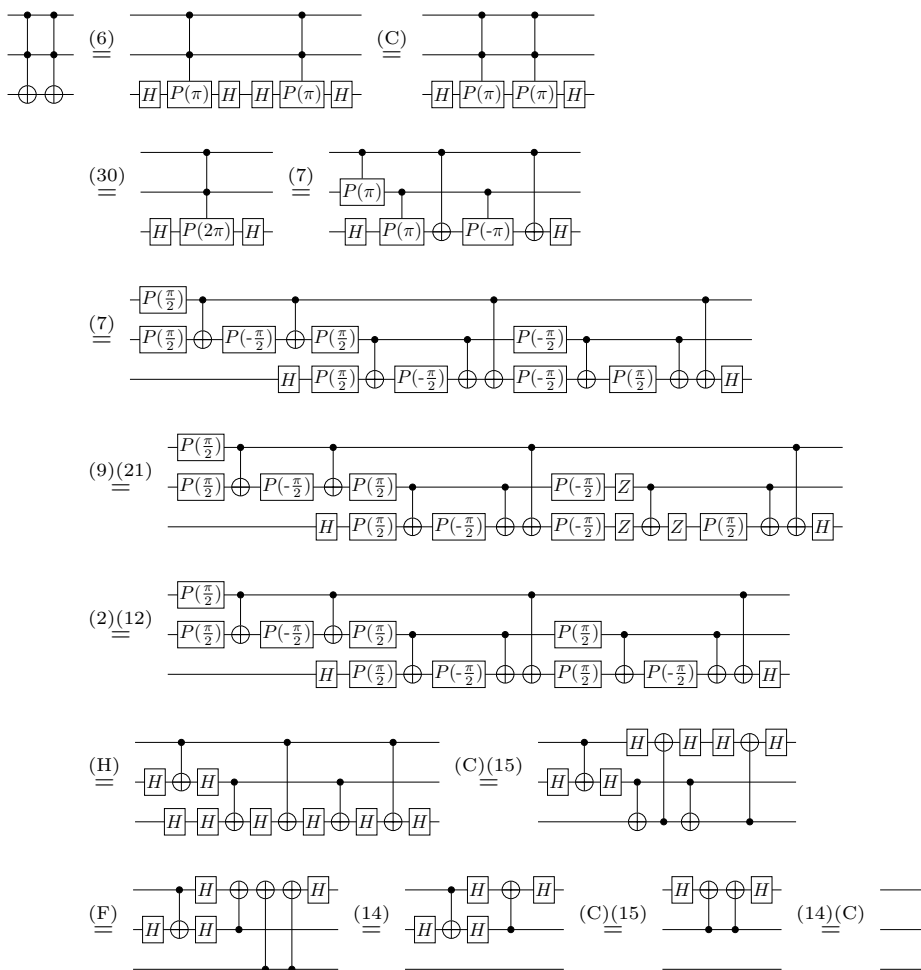
$$\begin{aligned}
 & \boxed{P(\alpha_1)} \boxed{R_X(\alpha_2)} \boxed{P(\alpha_3)} \quad \stackrel{(1)}{=} \quad \overset{\alpha_0}{\boxed{H}} \boxed{R_X(\alpha_1)} \boxed{H} \boxed{H} \boxed{P(\alpha_2)} \boxed{H} \boxed{H} \boxed{R_X(\alpha_3)} \boxed{H} \\
 & \quad \stackrel{(C)}{=} \quad \overset{\alpha_0}{\boxed{H}} \boxed{R_X(\alpha_1)} \boxed{P(\alpha_2)} \boxed{R_X(\alpha_3)} \boxed{H} \\
 & \quad \stackrel{(J)}{=} \quad \overset{\alpha_0 + \beta'_0}{\boxed{H}} \boxed{P(\beta_1)} \boxed{R_X(\beta_2)} \boxed{P(\beta_3)} \boxed{H} \\
 & \quad \stackrel{(1)}{=} \quad \overset{\beta_0}{\boxed{H}} \boxed{H} \boxed{R_X(\beta_1)} \boxed{H} \boxed{H} \boxed{P(\beta_2)} \boxed{H} \boxed{H} \boxed{R_X(\beta_3)} \boxed{H} \boxed{H} \\
 & \quad \stackrel{(C)}{=} \quad \overset{\beta_0}{\boxed{R_X(\beta_1)}} \boxed{P(\beta_2)} \boxed{R_X(\beta_3)}
 \end{aligned}$$

With  $\alpha_0 := \frac{\alpha_1 - \alpha_2 + \alpha_3}{2}$  and  $\beta_0 := \alpha_0 + \beta'_0 + \frac{\beta_1 - \beta_2 + \beta_3}{2}$ .

### B.3 Proofs of the equations of Figure 4

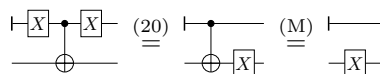
Equations (30) and (31) are proved in Proposition 13 of [5]. Equation (33) is proved in Lemma 53 of [5]. Equation (34) is proved in Lemma 47 of [5]. Equation (35) is proved in Proposition 12 of [5]. Equations (36) and (37) are proved in Proposition 11 of [5]. The proofs also hold for the equational theory QC because all the equations used are provable in QC.

Proof of Equation (32).

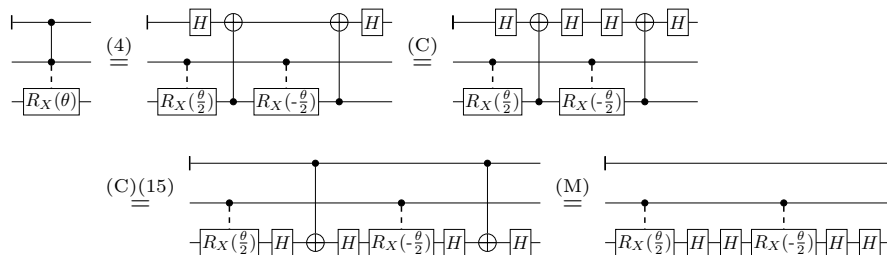


### B.4 Proofs of the equations of Figure 8

Proof of Equation (40).



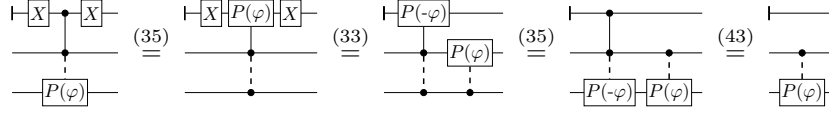
Proof of Equation (44).



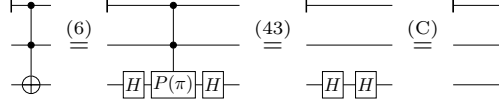




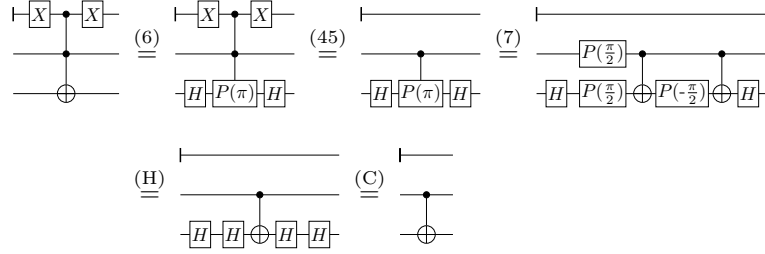
Proof of Equation (45).



Proof of Equation (41).



Proof of Equation (42).



## C Proofs used for the completeness of QC

### C.1 1-CNot completeness

In this Appendix,  $I, X, Z, \text{CNOT}, P(\varphi)$  and  $R_X(\theta)$  refers to the unitaries associated with the quantum gates  $\text{---}, \text{---}[X], \text{---}[Z], \text{---}\oplus, \text{---}[P(\varphi)]$  and  $\text{---}[R_X(\theta)]$  respectively.

► **Lemma 30** (1-qubit completeness). *QC is complete for 1-qubit quantum circuits, i.e. for any 1-qubit quantum circuits  $C_1, C_2 \in \text{QC}$ , if  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$  then  $\text{QC} \vdash C_1 = C_2$ .*

**Proof.** QC contains all the equations of the complete equational theory from [5] acting on at most one qubit. ◀

▷ **Claim 31.** By inputting and projecting the CNOT unitary on  $|0\rangle_1, |1\rangle_1, |+\rangle_2, |-\rangle_2$  and  $\langle 0|_1, \langle 1|_1, \langle +|_2, \langle -|_2$ , we get the following equations:

$$\begin{aligned} \text{CNOT } |0\rangle_1 &= (I \otimes I) |0\rangle_1 & \langle 0|_1 \text{CNOT} &= \langle 0|_1 (I \otimes I) \\ \text{CNOT } |1\rangle_1 &= (I \otimes X) |1\rangle_1 & \langle 1|_1 \text{CNOT} &= \langle 1|_1 (I \otimes X) \\ \text{CNOT } |+\rangle_2 &= (I \otimes I) |+\rangle_2 & \langle +|_2 \text{CNOT} &= \langle +|_2 (I \otimes I) \\ \text{CNOT } |-\rangle_2 &= (Z \otimes I) |-\rangle_2 & \langle -|_2 \text{CNOT} &= \langle -|_2 (Z \otimes I) \end{aligned}$$

► **Lemma 32.** *Let  $U \in \mathcal{U}_2$  be a 1-qubit unitary. If  $\langle 0|U|0\rangle = 0 \vee \langle 1|U|1\rangle = 0$  then there exist  $\varphi, \delta \in \mathbb{R}$  such that  $U = e^{i\delta}XP(\varphi)$ . Similarly, if  $\langle +|U|+\rangle = 0 \vee \langle -|U|-\rangle = 0$  then there exist  $\theta, \delta \in \mathbb{R}$  such that  $U = e^{i\delta}ZR_X(\theta)$ .*

**Proof.** First notice that  $\langle 0|U|0\rangle = 0$  iff  $\langle 1|U|1\rangle = 0$ . Then by unitarity there exists  $\delta, \phi \in \mathbb{R}$  such that  $U = \begin{pmatrix} 0 & e^{i\phi} \\ e^{i\delta} & 0 \end{pmatrix} = X \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\phi} \end{pmatrix} = e^{i\delta} X \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\phi-\delta)} \end{pmatrix}$ . And we are done by taking  $\varphi := \phi - \delta$ .

We prove the second statement by reducing it to the first one.  $\langle +|U|+\rangle = 0 \vee \langle -|U|-\rangle = 0$  iff  $\langle 0|HUUH|0\rangle = 0 \vee \langle 1|HUUH|1\rangle = 0$ . Thus there exists  $\theta, \phi \in \mathbb{R}$  such that  $HUUH = e^{i\phi}XP(\theta)$ . This implies that  $U = e^{i\phi}HXP(\theta)H = e^{i(\phi+\frac{\theta}{2})}ZR_X(\theta)$  and we are done by taking  $\delta := \phi + \frac{\theta}{2}$ . ◀

► **Lemma 33.** For any  $\varphi, \varphi', \theta, \theta', \delta \in \mathbb{R}$ , we have

$$\begin{cases} P(\varphi)P(\varphi') = e^{i\delta}I \Rightarrow \varphi' = -\varphi[2\pi] \\ R_X(\theta)R_X(\theta') = e^{i\delta}I \Rightarrow \theta' = -\theta[2\pi] \end{cases}$$

**Proof.** Let  $\varphi, \varphi', \theta, \theta', \delta \in \mathbb{R}$ . We prove the first statement as follows.

$$P(\varphi)P(\varphi') = e^{i\delta}I \Rightarrow \begin{cases} 1 = e^{i\delta} \\ e^{i(\varphi+\varphi')} = e^{i\delta} \end{cases} \Rightarrow \varphi' = -\varphi[2\pi]$$

We prove the second statement by reducing it to the first one as follows.

$$\begin{aligned} R_X(\theta)R_X(\theta') = e^{i\delta}I &\Rightarrow e^{-i(\frac{\theta}{2}+\frac{\theta'}{2})}HP(\theta)P(\theta')H = e^{i\delta}I \\ &\Rightarrow e^{-i(\frac{\theta}{2}+\frac{\theta'}{2})}P(\theta)P(\theta') = e^{i\delta}I \\ &\Rightarrow P(\theta)P(\theta') = e^{i(\delta+\frac{\theta}{2}+\frac{\theta'}{2})} \\ &\Rightarrow \theta' = -\theta[2\pi] \end{aligned}$$

► **Lemma 34.** Let  $A, B, C, D \in \mathcal{U}_2$  be 1-qubit unitaries, if  $(C \otimes D) \circ \text{CNOT} \circ (A \otimes B) = \text{CNOT}$  (see the following circuit representation) then there exist  $\varphi, \theta, \alpha, \beta, \gamma \in \mathbb{R}$  and  $k, l \in \{0, 1\}$  such that  $A = e^{i\alpha}X^kP(\varphi)$ ,  $B = e^{i\beta}Z^lR_X(\theta)$ ,  $C = e^{i\gamma}P(-\varphi)Z^lX^k$  and  $D = e^{i(-\alpha-\beta-\gamma)}R_X(-\theta)Z^lX^k$ .

$$\left[ \begin{array}{cc} \boxed{A} & \boxed{C} \\ \boxed{B} \oplus \boxed{D} & \end{array} \right] = \left[ \begin{array}{c} \bullet \\ \oplus \end{array} \right]$$

**Proof.** From the condition we derive four equations satisfied by  $A, B, C, D$  and we conduct a case distinction corresponding to the four possible assignments of  $k, l \in \{0, 1\}$ .

$$\begin{aligned} (C \otimes D) \circ \text{CNOT} \circ (A \otimes B) &= \text{CNOT} \\ &\Rightarrow \begin{cases} (C \otimes D) \circ \text{CNOT} \circ (I \otimes B) = \text{CNOT} \circ (A^\dagger \otimes I) \\ (C \otimes D) \circ \text{CNOT} \circ (A \otimes I) = \text{CNOT} \circ (I \otimes B^\dagger) \end{cases} \\ &\Rightarrow \begin{cases} \langle 0|_1 (C \otimes D) \circ \text{CNOT} \circ (I \otimes B) |0\rangle_1 = \langle 0|_1 \text{CNOT} \circ (A^\dagger \otimes I) |0\rangle_1 \\ \langle 1|_1 (C \otimes D) \circ \text{CNOT} \circ (I \otimes B) |1\rangle_1 = \langle 1|_1 \text{CNOT} \circ (A^\dagger \otimes I) |1\rangle_1 \\ \langle +|_2 (C \otimes D) \circ \text{CNOT} \circ (A \otimes I) |+\rangle_2 = \langle +|_2 \text{CNOT} \circ (I \otimes B^\dagger) |+\rangle_2 \\ \langle -|_2 (C \otimes D) \circ \text{CNOT} \circ (A \otimes I) |-\rangle_2 = \langle -|_2 \text{CNOT} \circ (I \otimes B^\dagger) |-\rangle_2 \end{cases} \\ \stackrel{\text{Claim 31}}{\Rightarrow} &\begin{cases} \langle 0|_1 (C \otimes D) \circ (I \otimes I) \circ (I \otimes B) |0\rangle_1 = \langle 0|_1 (I \otimes I) \circ (A^\dagger \otimes I) |0\rangle_1 \\ \langle 1|_1 (C \otimes D) \circ (I \otimes X) \circ (I \otimes B) |1\rangle_1 = \langle 1|_1 (I \otimes X) \circ (A^\dagger \otimes I) |1\rangle_1 \\ \langle +|_2 (C \otimes D) \circ (I \otimes I) \circ (A \otimes I) |+\rangle_2 = \langle +|_2 (I \otimes I) \circ (I \otimes B^\dagger) |+\rangle_2 \\ \langle -|_2 (C \otimes D) \circ (Z \otimes I) \circ (A \otimes I) |-\rangle_2 = \langle -|_2 (Z \otimes I) \circ (I \otimes B^\dagger) |-\rangle_2 \end{cases} \end{aligned}$$



$e^{i(\beta+\sigma)}R_X(\theta')ZZR_X(\theta) = e^{i\delta}I$ , which implies that  $\theta' = -\theta[2\pi]$  (Lemma 33). Then we can use the following derivation to get a new condition satisfied by  $A$  and  $C$ .

$$\left[ \begin{array}{c} \text{---} \boxed{A} \text{---} \boxed{C} \text{---} \\ \text{---} \boxed{R_X(\theta)} \text{---} \boxed{Z} \oplus \boxed{Z} \text{---} \boxed{R_X(-\theta)} \text{---} \\ \text{---} \end{array} \right] \stackrel{(21)}{=} \left[ \begin{array}{c} \text{---} \boxed{A} \text{---} \boxed{Z} \text{---} \boxed{C} \text{---} \\ \text{---} \boxed{R_X(\theta)} \text{---} \oplus \boxed{R_X(-\theta)} \text{---} \\ \text{---} \end{array} \right] \stackrel{(18)(13)(10)}{=} \left[ \begin{array}{c} \text{---} \boxed{A} \text{---} \boxed{Z} \text{---} \boxed{C} \text{---} \\ \text{---} \oplus \text{---} \\ \text{---} \end{array} \right]$$

We get  $e^{\beta+\sigma}(CZ \otimes I) \circ \text{CNOT} \circ (A \otimes I) = \text{CNOT}$  from which we obtain two new equations:

$$\begin{aligned} & e^{\beta+\sigma}(CZ \otimes I) \circ \text{CNOT} \circ (A \otimes I) = \text{CNOT} \\ \Rightarrow & \begin{cases} e^{\beta+\sigma} \langle +|_2 (CZ \otimes I) \circ \text{CNOT} \circ (A \otimes I) |+\rangle_2 = \langle +|_2 \text{CNOT} |+\rangle_2 \\ e^{\beta+\sigma} \langle -|_2 (CZ \otimes I) \circ \text{CNOT} \circ (A \otimes I) |-\rangle_2 = \langle -|_2 \text{CNOT} |-\rangle_2 \end{cases} \\ \Rightarrow & \begin{cases} e^{\beta+\sigma} \langle +|_2 (CZ \otimes I) \circ (I \otimes I) \circ (A \otimes I) |+\rangle_2 = \langle +|_2 (I \otimes I) |+\rangle_2 \\ e^{\beta+\sigma} \langle -|_2 (CZ \otimes I) \circ (Z \otimes I) \circ (A \otimes I) |-\rangle_2 = \langle -|_2 (Z \otimes I) |-\rangle_2 \end{cases} \\ & \Rightarrow \begin{cases} e^{\beta+\sigma}CZA = I \\ e^{\beta+\sigma}CZZA = Z \end{cases} \end{aligned}$$

This implies that  $CZA = CAZ$ , thus there exist  $\varphi, \alpha \in \mathbb{R}$  such that  $A = e^{i\alpha}P(\varphi)$  (because  $A = ZAZ$ ). The first equation implies  $C = e^{i(-\alpha-\beta-\sigma)}P(-\varphi)Z$ , and we are done by tacking  $k = 0, l = 1$  and  $\gamma := -\alpha - \beta - \sigma$ , which leads to  $\sigma = -\alpha - \beta - \gamma$ .

**Case  $\langle 0|A^\dagger|0\rangle = 0$  and  $\langle +|B^\dagger|+\rangle = 0$ .** It must also be the case that  $\langle 0|C|0\rangle = 0$  and  $\langle +|D|+\rangle = 0$ . Lemma 32 implies that there exist  $\varphi, \varphi', \theta, \theta', \alpha, \beta, \gamma, \delta \in \mathbb{R}$  such that  $A = e^{i\alpha}XP(\varphi)$ ,  $B = e^{i\beta}ZR_X(\theta)$ ,  $C = e^{i\gamma}P(\varphi')X$  and  $D = e^{i\delta}R_X(\theta')Z$ . Then we can use the following derivation to get a new condition satisfied by  $\varphi, \varphi', \theta, \theta'$ .

$$\left[ \begin{array}{c} \text{---} \boxed{P(\varphi)} \text{---} \boxed{X} \text{---} \boxed{P(\varphi')} \text{---} \\ \text{---} \boxed{R_X(\theta)} \text{---} \boxed{Z} \oplus \boxed{Z} \text{---} \boxed{R_X(\theta')} \text{---} \\ \text{---} \end{array} \right] \stackrel{(20)(21)}{=} \left[ \begin{array}{c} \text{---} \boxed{P(\varphi)} \text{---} \boxed{Z} \text{---} \boxed{P(\varphi')} \text{---} \\ \text{---} \boxed{R_X(\theta)} \text{---} \oplus \boxed{X} \text{---} \boxed{R_X(\theta')} \text{---} \\ \text{---} \end{array} \right]$$

We get  $e^{i(\alpha+\beta+\gamma+\delta)}(P(\varphi')Z \otimes R_X(\theta')X)\text{CNOT}(P(\varphi) \otimes R_X(\theta)) = \text{CNOT}$  from which we obtain two new equations:

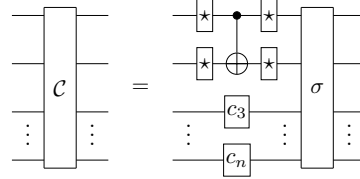
$$\begin{aligned} & e^{i(\alpha+\beta+\gamma+\delta)}(P(\varphi')Z \otimes R_X(\theta')X)\text{CNOT}(P(\varphi) \otimes R_X(\theta)) = \text{CNOT} \\ \Rightarrow & \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} \langle 0|_1 (P(\varphi')Z \otimes R_X(\theta')X)\text{CNOT}(P(\varphi) \otimes R_X(\theta)) |0\rangle_1 = \langle 0|_1 \text{CNOT} |0\rangle_1 \\ e^{i(\alpha+\beta+\gamma+\delta)} \langle +|_2 (P(\varphi')Z \otimes R_X(\theta')X)\text{CNOT}(P(\varphi) \otimes R_X(\theta)) |+\rangle_2 = \langle +|_2 \text{CNOT} |+\rangle_2 \end{cases} \\ \Rightarrow & \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} \langle 0|_1 (P(\varphi')Z \otimes R_X(\theta')X)(I \otimes I)(P(\varphi) \otimes R_X(\theta)) |0\rangle_1 = \langle 0|_1 (I \otimes I) |0\rangle_1 \\ e^{i(\alpha+\beta+\gamma+\delta)} \langle +|_2 (P(\varphi')Z \otimes R_X(\theta')X)(I \otimes I)(P(\varphi) \otimes R_X(\theta)) |+\rangle_2 = \langle +|_2 (I \otimes I) |+\rangle_2 \end{cases} \\ & \Rightarrow \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)}R_X(\theta')XR_X(\theta) = I \\ e^{i(\alpha+\beta+\gamma+\delta)}e^{-i(\theta+\theta')/2}P(\varphi')ZP(\varphi) = I \end{cases} \\ & \Rightarrow \begin{cases} R_X(\theta') = e^{-i(\alpha+\beta+\gamma+\delta)}R_X(-\theta)X \\ P(\varphi') = e^{-i(\alpha+\beta+\gamma+\delta)}e^{i(\theta+\theta')/2}P(-\varphi)Z \end{cases} \\ & \Rightarrow \begin{cases} R_X(\theta') = e^{-i(\alpha+\beta+\gamma+\delta)}e^{i\pi/2}R_X(\pi - \theta) \\ P(\varphi') = e^{-i(\alpha+\beta+\gamma+\delta)}e^{i(\theta+\theta')/2}P(\pi - \varphi) \end{cases} \\ & \stackrel{\text{Lemma 33}}{\Rightarrow} \begin{cases} \theta' = \pi - \theta[2\pi] \\ \varphi' = \pi - \varphi[2\pi] \end{cases} \end{aligned}$$

Hence, we get  $A = e^{i\alpha}XP(\varphi)$ ,  $B = e^{i\beta}ZR_X(\theta)$ ,  $C = e^{i\gamma}P(\pi - \varphi)X = e^{i\gamma}P(-\varphi)ZX$ ,  $D = e^{i(-\alpha-\beta-\gamma+\pi/2)}R_X(\pi - \theta)Z = e^{i(-\alpha-\beta-\gamma)}R_X(-\theta)ZX$  and we are done by taking  $k = l = 1$ .  $\blacktriangleleft$

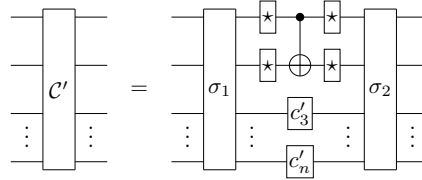
**Proof of Lemma 8 (1-CNot completeness).** Let  $\mathcal{C}, \mathcal{C}' \in \text{QC}$  be two 1-CNot quantum circuits, i.e. circuits containing at most one  $\text{CNot}$  gate each, such that  $\llbracket \mathcal{C} \rrbracket = \llbracket \mathcal{C}' \rrbracket$ .

First notice that if both  $\mathcal{C}, \mathcal{C}'$  contains no CNot, then, according to Lemma 30 we have  $\text{QC} \vdash \mathcal{C} = \mathcal{C}'$ . If  $\mathcal{C}$  contains a CNot then one can show that  $\mathcal{C}'$  must contain a CNot otherwise they would not have the same semantics.

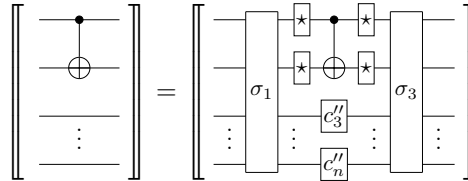
Then, w.l.o.g. we can suppose that the CNot is applied to the first two qubits in  $\mathcal{C}$ . We first show that the CNot is also applied to the first two qubits in  $\mathcal{C}'$ , and that the permutation of wires is the same in both circuits. Pushing all swaps to the right in  $\mathcal{C}$ , we get:



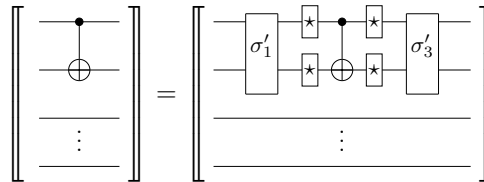
where  $\sigma$  is a permutation of wires. In  $\mathcal{C}'$ , using the prop equations to move the CNot on the first two qubits, we get:



By applying the inverse of all 1-qubit unitaries from  $\mathcal{C}$ , as well as the inverse of  $\sigma$ ,  $\llbracket \mathcal{C} \rrbracket = \llbracket \mathcal{C}' \rrbracket$  becomes equivalent to:



with  $\sigma_3 = \sigma_2 \circ \sigma^{-1}$ . It then becomes apparent that if  $\sigma_1(i) \geq 3$ , then  $\sigma_3(\sigma_1(i)) = i$ . Moreover, we get  $\llbracket \mathcal{C}'_i \rrbracket = \llbracket - \rrbracket$ . We then have:



Getting back to  $\mathcal{C}$  and  $\mathcal{C}'$ , we conclude that qubits that are not involved with the CNot have the same 1-qubit unitary applied to them on both sides, and are permuted with the rest in the same way. By completeness of QC for 1-qubit unitaries, it is now enough to show the result when  $\mathcal{C}$  and  $\mathcal{C}'$  are 2-qubit circuits.

We can now show that if a swap appears on one side, it also appears on the other side (i.e. that  $\sigma'_1 = \sigma'_3$  above). Indeed, suppose that  $\mathcal{C}$  has a swap and  $\mathcal{C}'$  does not. Using the prop equations, we can push the swap to the right, and get  $\mathcal{C} = \text{X} \circ \bar{\mathcal{C}}$ . Thus  $\llbracket \mathcal{C} \rrbracket = \llbracket \mathcal{C}' \rrbracket$  is then equivalent to  $\llbracket \text{X} \rrbracket = \llbracket \mathcal{C}' \circ \bar{\mathcal{C}}^\dagger \rrbracket$ . We hence have a circuit  $\mathcal{C}' \circ \bar{\mathcal{C}}^\dagger$  that implements  $\text{X}$ ,

using at most two CNOTs. This contradicts Theorem 6 of [29] that proves that the swap requires at least 3 CNOTs. Hence, if  $\mathcal{C}$  has a swap then so does  $\mathcal{C}'$ .

In the case where the two circuits have a swap, the equality between the two becomes QC-equivalent to the equality without swaps on both side. Hence, we can assume w.l.o.g. that  $\mathcal{C}$  and  $\mathcal{C}'$  are 2-qubit circuits containing one and only one CNOT and no swap. Moreover thanks to Equation (15) we can assume:

$$\begin{array}{|c|} \hline \mathcal{C} \\ \hline \end{array} = \begin{array}{|c|} \hline \boxed{A_1} \\ \hline \end{array} \bullet \begin{array}{|c|} \hline \boxed{C_1} \\ \hline \end{array} \\ \oplus \\ \begin{array}{|c|} \hline \boxed{B_1} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{D_1} \\ \hline \end{array} \quad \begin{array}{|c|} \hline \mathcal{C}' \\ \hline \end{array} = \begin{array}{|c|} \hline \boxed{A_2} \\ \hline \end{array} \bullet \begin{array}{|c|} \hline \boxed{C_2} \\ \hline \end{array} \\ \oplus \\ \begin{array}{|c|} \hline \boxed{B_2} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{D_2} \\ \hline \end{array}$$

for some 1-qubit circuits  $\boxed{A_i}$ ,  $\boxed{B_i}$ ,  $\boxed{C_i}$ ,  $\boxed{D_i}$ .

First, by QC-equivalence and Proposition 7, we reduce it to showing the following equation for any semantically correct 1-qubit circuits  $\boxed{A}$ ,  $\boxed{B}$ ,  $\boxed{C}$ ,  $\boxed{D}$ .

$$\begin{array}{|c|} \hline \boxed{A} \\ \hline \end{array} \bullet \begin{array}{|c|} \hline \boxed{C} \\ \hline \end{array} \\ \oplus \\ \begin{array}{|c|} \hline \boxed{B} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{D} \\ \hline \end{array} = \begin{array}{|c|} \hline \bullet \\ \hline \end{array} \oplus$$

Lemma 34 and Lemma 30 together with Equations (A) and (B) implies that this is always the case that this equation is QC-equivalent to one of the following equations:

$$\begin{array}{|c|} \hline \boxed{P(\varphi)} \\ \hline \end{array} \bullet \begin{array}{|c|} \hline \boxed{P(-\varphi)} \\ \hline \end{array} \\ \oplus \\ \begin{array}{|c|} \hline \boxed{R_X(\theta)} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{R_X(-\theta)} \\ \hline \end{array} = \begin{array}{|c|} \hline \bullet \\ \hline \end{array} \oplus \quad \begin{array}{|c|} \hline \boxed{P(\varphi)} \\ \hline \end{array} \boxed{X} \bullet \begin{array}{|c|} \hline \boxed{X} \\ \hline \end{array} \boxed{P(-\varphi)} \\ \oplus \\ \begin{array}{|c|} \hline \boxed{R_X(\theta)} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{X} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{R_X(-\theta)} \\ \hline \end{array} = \begin{array}{|c|} \hline \bullet \\ \hline \end{array} \oplus \\ \begin{array}{|c|} \hline \boxed{P(\varphi)} \\ \hline \end{array} \bullet \begin{array}{|c|} \hline \boxed{Z} \\ \hline \end{array} \begin{array}{|c|} \hline \boxed{P(-\varphi)} \\ \hline \end{array} \\ \oplus \\ \begin{array}{|c|} \hline \boxed{R_X(\theta)} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{Z} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{Z} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{R_X(-\theta)} \\ \hline \end{array} = \begin{array}{|c|} \hline \bullet \\ \hline \end{array} \oplus \quad \begin{array}{|c|} \hline \boxed{P(\varphi)} \\ \hline \end{array} \boxed{X} \bullet \begin{array}{|c|} \hline \boxed{X} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{Z} \\ \hline \end{array} \begin{array}{|c|} \hline \boxed{P(-\varphi)} \\ \hline \end{array} \\ \oplus \\ \begin{array}{|c|} \hline \boxed{R_X(\theta)} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{Z} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{X} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{Z} \\ \hline \end{array} \oplus \begin{array}{|c|} \hline \boxed{R_X(-\theta)} \\ \hline \end{array} = \begin{array}{|c|} \hline \bullet \\ \hline \end{array} \oplus$$

We conclude the proof by observing that we can derive all those equations for any  $\varphi, \theta \in \mathbb{R}$  using Equations (21),(20),(17),(18),(12),(13),(D), and (10). ◀

## C.2 Proof of Equation (38)

► **Lemma 35.** Equation (51) can be derived in QC.

$$\boxed{H} = \begin{array}{c} \textcircled{\frac{\pi}{4}} \\ \boxed{R_X(\frac{\pi}{2})} \end{array} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \quad (51)$$

**Proof.**

$$\begin{aligned} \boxed{H} &\stackrel{(D)(12)(10)(13)}{=} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{H} \\ &\stackrel{(I)}{=} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{H} \boxed{H} \\ &\stackrel{(C)}{=} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \\ &\stackrel{(1)}{=} \begin{array}{c} \textcircled{\frac{\pi}{4}} \\ \boxed{P(-\frac{\pi}{2})} \end{array} \boxed{H} \boxed{P(-\frac{\pi}{2})} \boxed{H} \boxed{P(-\frac{\pi}{2})} \\ &\stackrel{(I)}{=} \begin{array}{c} \textcircled{\frac{\pi}{4}} \\ \boxed{P(-\frac{\pi}{2})} \end{array} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \\ &\stackrel{(12)(D)}{=} \begin{array}{c} \textcircled{\frac{\pi}{4}} \\ \boxed{R_X(\frac{\pi}{2})} \end{array} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \end{aligned}$$

◀

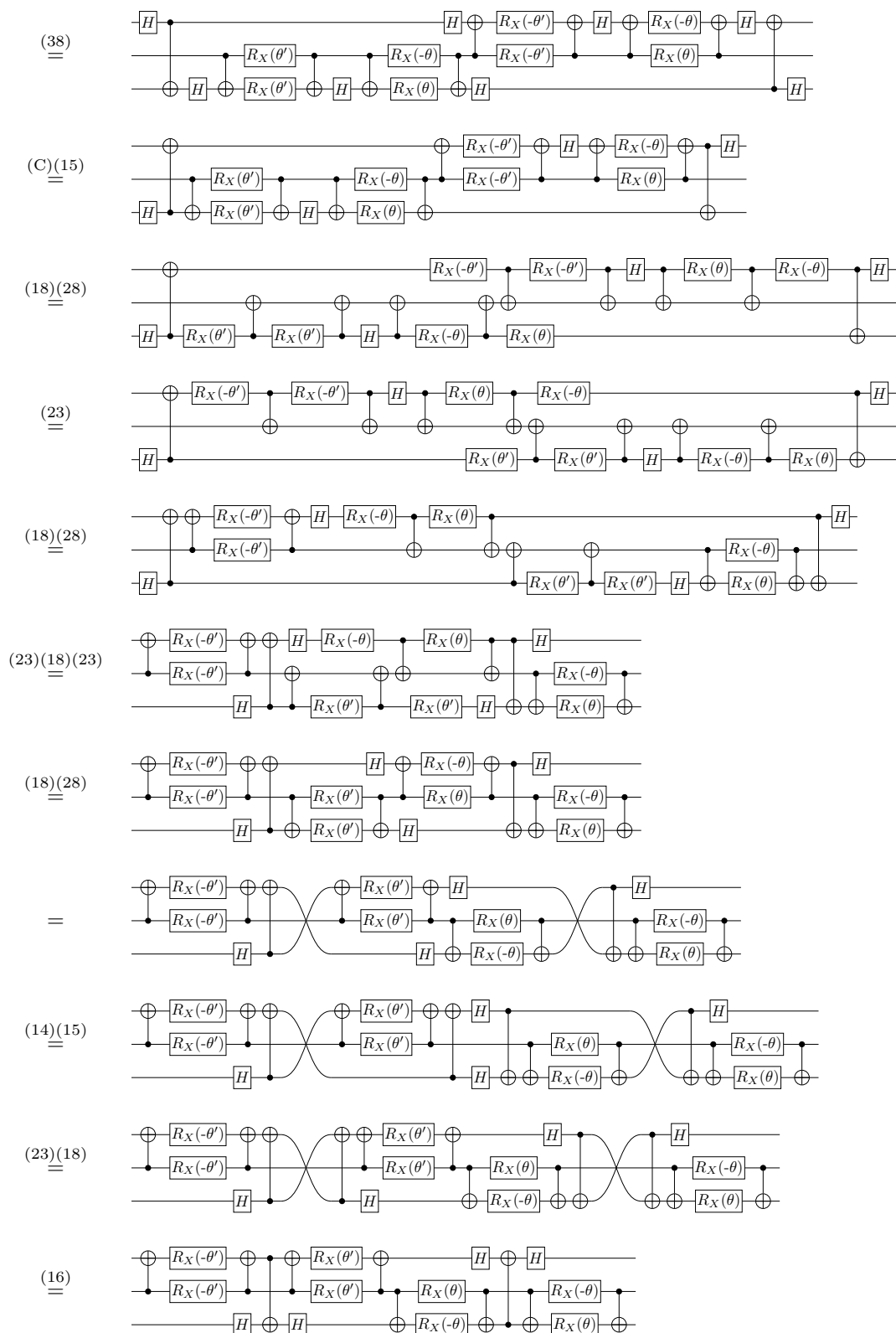


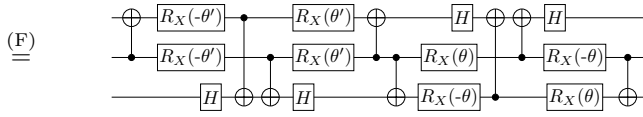
$$\begin{aligned}
 \sim_{\text{QC}} & \quad \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 & \quad \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \sim_{\text{QC}}^{(G)} & \quad \begin{array}{c} \text{---} \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} = \begin{array}{c} \text{---} \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}
 \end{aligned}$$

### C.3 Proof of Equation (39)

$$\begin{aligned}
 & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \stackrel{(F)}{=} & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \stackrel{(16)}{=} & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \stackrel{(23)(18)}{=} & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \stackrel{(15)(14)}{=} & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 = & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \stackrel{(18)(28)}{=} & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \stackrel{(23)(18)}{=} & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \\
 \stackrel{(28)(18)}{=} & \begin{array}{c} \text{---} \oplus \oplus \oplus \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}
 \end{aligned}$$





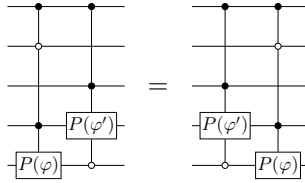


### C.4 Proof of Equation $(K_{\text{old}}^*)$ , existence and uniqueness of the RHS of Equation $(K^*)$

The proof uses some properties of multi-controlled gates:

► **Lemma 37.** *It follows from the equations of QC without Equation  $(K^*)$  that two multi-controlled  $P$  gates always commute, regardless of the colours and positions of their controls, and of the positions of their targets.*

For instance,



**Proof of Lemma 37.** This is a direct consequence of the results of [5], namely of Lemma 54 together with Propositions 11, 12 and 15. ◀

► **Lemma 38.** *The following equations are consequences of the equations of QC without Equation  $(K^*)$ :*

$$\begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{P(\varphi)} \\
 \vdots \\
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{R_X(\theta)}
 \end{array}
 =
 \begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{P(\varphi)} \\
 \vdots \\
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{R_X(\theta)}
 \end{array}
 \tag{52}$$

$$\begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{R_X(0)}
 \end{array}
 =
 \begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{P(0)}
 \end{array}
 =
 \begin{array}{c}
 \vdots \\
 \vdots \\
 \vdots \\
 \vdots
 \end{array}
 \tag{53}$$

► **Lemma 39.** *The following equation is a consequence of the equations of QC:*

$$\begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{P(2\pi)}
 \end{array}
 =
 \begin{array}{c}
 \vdots \\
 \vdots \\
 \vdots \\
 \vdots
 \end{array}
 \tag{54}$$

► **Lemma 40.** *The following equations are consequences of the equations of QC without Equation  $(K^*)$ , together with Equation (54):*

$$\begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{R_X(2\pi)}
 \end{array}
 =
 \begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{P(\pi)}
 \end{array}
 \tag{55}$$

$$\begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{P(\pi)} \quad \boxed{R_X(\theta)}
 \end{array}
 =
 \begin{array}{c}
 \bullet \\
 \vdots \\
 \bullet \\
 \vdots \\
 \bullet \\
 \boxed{R_X(2\pi-\theta)} \quad \boxed{P(\pi)}
 \end{array}
 \tag{56}$$

**Proof of Equation (52).** Equation (52) corresponds to Lemma 48 of [5], whose proof does not use Equation  $(K_{\text{old}}^*)$ . ◀

**Proof of Equation (53).** By a straightforward induction. ◀

**Proof of Equation (54).** The case with zero controls is a direct consequence of Equations (2), (9), and (12). For the case with one or more controls, it suffices to remark that the derivation given in [5] does not need  $\delta_9$ :

$$\begin{array}{c}
 \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \\ \boxed{P(2\pi)} \\ \text{---} \end{array} \quad \stackrel{(53)}{=} \quad \begin{array}{c} \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{---} \\ \boxed{R_X(0)} \quad \boxed{R_X(0)} \\ \vdots \quad \vdots \\ \text{---} \\ \boxed{P(2\pi)} \quad \boxed{R_X(0)} \\ \text{---} \end{array} \\
 \\
 \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \\ \boxed{P(0)} \\ \text{---} \end{array} \quad \stackrel{(K^*)}{=} \quad \begin{array}{c} \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{---} \\ \boxed{R_X(0)} \\ \vdots \\ \text{---} \\ \boxed{P(0)} \end{array} \\
 \\
 \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \\ \boxed{P(0)} \\ \text{---} \end{array} \quad \stackrel{(53)}{=} \quad \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \\ \text{---} \\ \text{---} \end{array}
 \end{array}$$

◀

**Proof of Equations (55) and (56).** Equations (55) and (56) correspond respectively to Lemmas 59 and 60 of [5], and it can be checked that their proofs given in [5] do not need the full power of Equation  $(K_{\text{old}}^*)$  but only Equation (54). ◀

Given an instance of Equation  $(K_{\text{old}}^*)$ , we prove that its right-hand side can be transformed into a circuit of the same form as the right-hand side of Equation  $(K^*)$ .

First, one can remark that

$$\langle 1\dots 101 | \left[ \begin{array}{c} \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{---} \\ \boxed{R_X(\gamma_1)} \quad \boxed{R_X(\gamma_4)} \\ \vdots \quad \vdots \\ \text{---} \\ \boxed{P(\gamma_2)} \quad \boxed{R_X(\gamma_3)} \\ \text{---} \end{array} \right] | 1\dots 110 \rangle = -\sin\left(\frac{\gamma_3}{2}\right) \sin\left(\frac{\gamma_4}{2}\right)$$

while

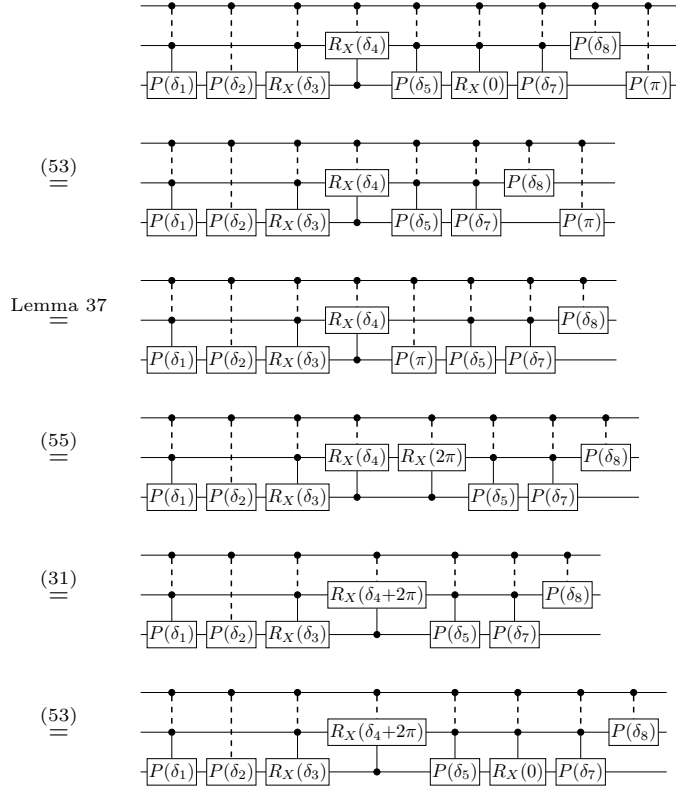
$$\langle 1\dots 101 | \left[ \begin{array}{c} \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{---} \\ \boxed{R_X(\delta_4)} \\ \vdots \\ \text{---} \\ \boxed{P(\delta_8)} \end{array} \right] | 1\dots 110 \rangle = -e^{i\delta_9} \sin\left(\frac{\delta_3}{2}\right) \sin\left(\frac{\delta_4}{2}\right).$$

■ If  $\sin\left(\frac{\delta_3}{2}\right) \sin\left(\frac{\delta_4}{2}\right) \neq 0$ , this implies that  $e^{i\delta_9}$  is a real number, which, since  $\delta_9 \in [0, 2\pi)$ , implies that  $\delta_9 \in \{0, \pi\}$ .

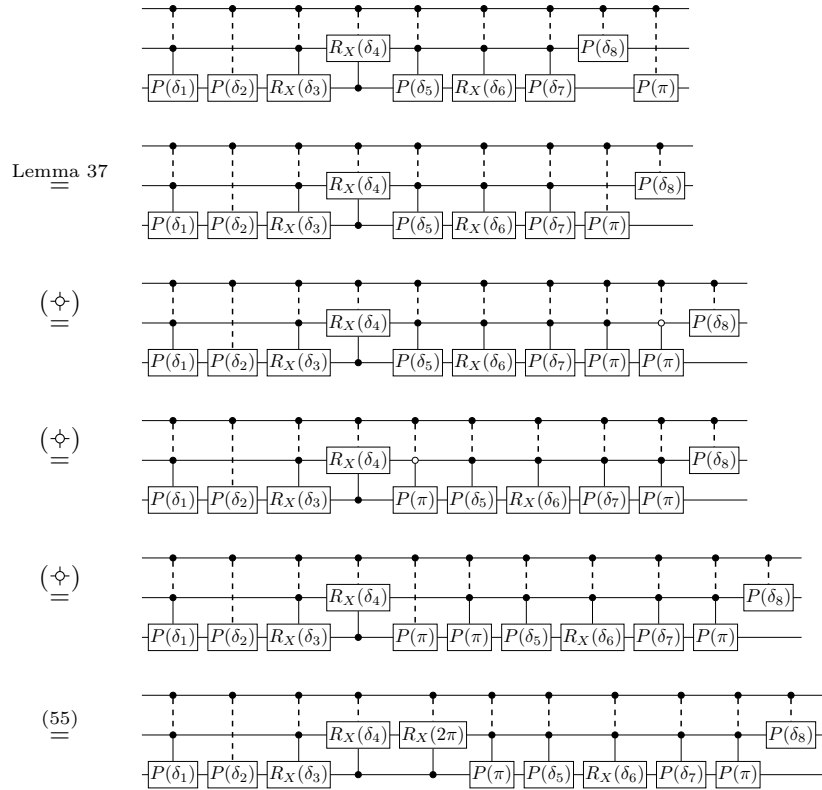
■ If  $\delta_9 = 0$ , then

$$\begin{array}{c} \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{---} \\ \boxed{R_X(\delta_4)} \\ \vdots \\ \text{---} \\ \boxed{P(\delta_8)} \end{array} \stackrel{(53)}{=} \begin{array}{c} \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \quad \text{---} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \text{---} \\ \boxed{R_X(\delta_4)} \\ \vdots \\ \text{---} \\ \boxed{P(\delta_8)} \end{array}$$

– If  $\delta_9 = \pi$  and  $\delta_6 = 0$ , then

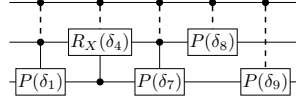


– If  $\delta_9 = \pi$  and  $\delta_6 \neq 0$ , then

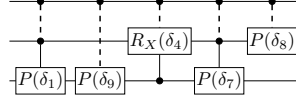




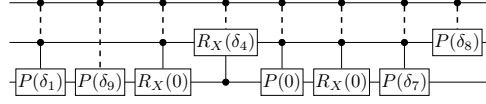
\* If  $\delta_9 \in [0, \pi)$ , then



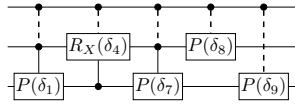
Lemma 37,  
(52)



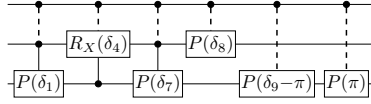
(53)



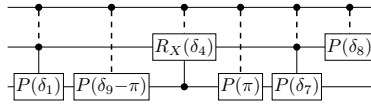
\* If  $\delta_9 \in [\pi, 2\pi)$ , then



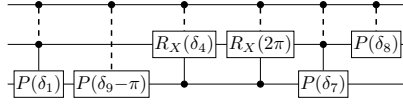
(30)



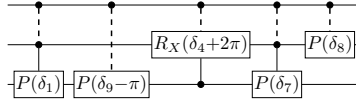
Lemma 37,  
(52)



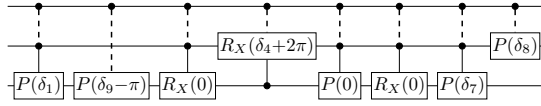
(55)



(31)



(53)



■ If  $\sin(\frac{\gamma_4}{2}) = 0$ , then  $\cos(\frac{\gamma_4}{2}) \in \{-1, 1\}$  and one has

$$\langle 1 \dots 101 | \left[ \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \end{array} \right] | 1 \dots 101 \rangle = \pm \cos(\frac{\gamma_1}{2})$$

while, since  $\delta_2 = 0$ ,

$$\langle 1 \dots 101 | \left[ \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \end{array} \right] | 1 \dots 101 \rangle = e^{i\delta_9} \cos(\frac{\delta_4}{2}).$$

\* If  $\cos(\frac{\delta_4}{2}) \neq 0$ , then this implies that  $e^{i\delta_9}$  is a real number, so that  $\delta_9 \in \{0, \pi\}$  and we can proceed as in the first case (where  $\sin(\frac{\delta_3}{2}) \sin(\frac{\delta_4}{2}) \neq 0$ ).



Since Equation  $(K_{\text{old}}^*)$  has been proved to be sound in [5] (that is, for any angles in its left-hand side, there exist a choice of angles in its right-hand side satisfying the conditions of Figure 6 that makes it sound), and it is easy to see that all equations of QC except maybe Equation  $(K^*)$  are sound, this implies that Equation  $(K^*)$  is sound.

Moreover, this proves that Equation  $(K_{\text{old}}^*)$  is a consequence of the equations of QC.

It remains to prove that for any choice of angles in the LHS of Equation  $(K^*)$ , the choice of angles in its RHS is unique. To this end, we now consider an instance of Equation  $(K^*)$  and transform its RHS into the RHS of the instance of  $(K_{\text{old}}^*)$  with same LHS. To make easier to differentiate between the parameters of the respective RHS of Equations  $(K^*)$  and  $(K_{\text{old}}^*)$ , we keep denoting those of Equation  $(K^*)$  as  $\delta'_k$ :

$$\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{R_X(\gamma_1)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\gamma_2)} \quad \boxed{R_X(\gamma_3)}
\end{array}
=
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{R_X(\delta'_6)} \quad \boxed{P(\delta'_7)}
\end{array}
\quad (K^*)$$

- If  $\delta'_4 \in [0, 2\pi)$  and either  $\delta'_3 \neq 0$  or  $\delta'_2 = 0$ , then

$$\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{R_X(\delta'_6)} \quad \boxed{P(\delta'_7)}
\end{array}
\stackrel{(53)}{=}
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{R_X(\delta'_6)} \quad \boxed{P(\delta'_7)} \quad \boxed{P(0)}
\end{array}$$

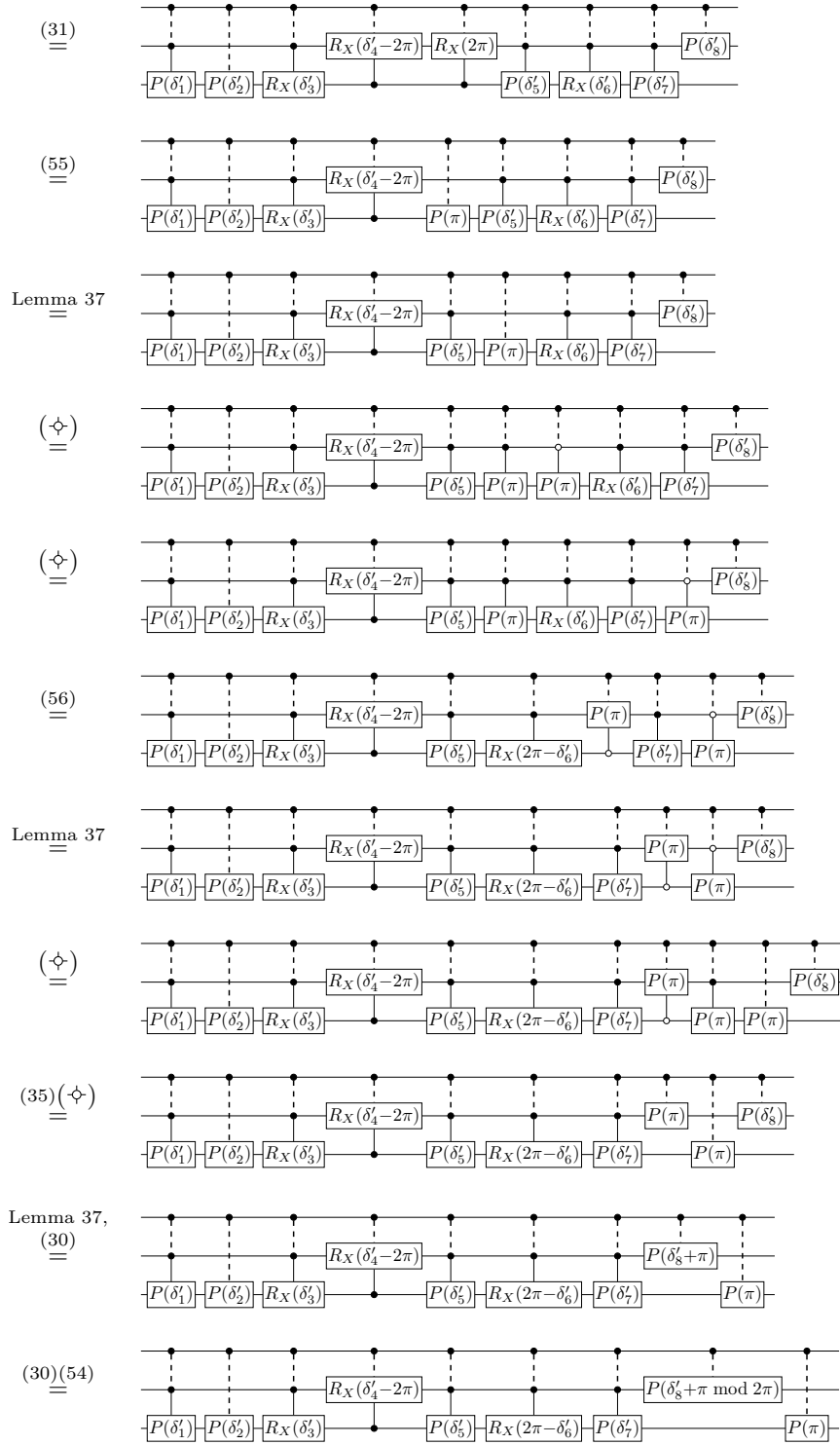
- If  $\delta'_4 \in [2\pi, 4\pi)$ , either  $\delta'_3 \neq 0$  or  $\delta'_2 = 0$ , and  $\delta'_6 = 0$ , then

$$\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{R_X(0)} \quad \boxed{P(\delta'_7)}
\end{array}
\stackrel{(53)}{=}
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{P(\delta'_7)}
\end{array}
\stackrel{(31)}{=}
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{P(\delta'_7)}
\end{array}
\stackrel{(55)}{=}
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\pi)} \quad \boxed{P(\delta'_5)} \quad \boxed{P(\delta'_7)}
\end{array}
\stackrel{\text{Lemma 37}}{=}
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{P(\delta'_7)} \quad \boxed{P(\pi)}
\end{array}
\stackrel{(53)}{=}
\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{R_X(0)} \quad \boxed{P(\delta'_7)} \quad \boxed{P(\pi)}
\end{array}$$

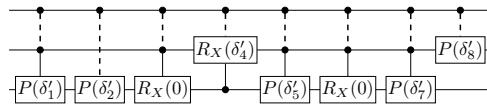
- If  $\delta'_4 \in [2\pi, 4\pi)$ , either  $\delta'_3 \neq 0$  or  $\delta'_2 = 0$ , and  $\delta'_6 \neq 0$ , then

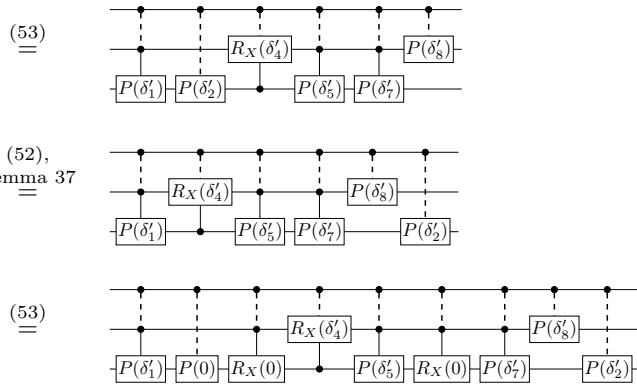
$$\begin{array}{c}
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\
\hline
\boxed{P(\delta'_5)} \quad \boxed{R_X(\delta'_6)} \quad \boxed{P(\delta'_7)}
\end{array}$$



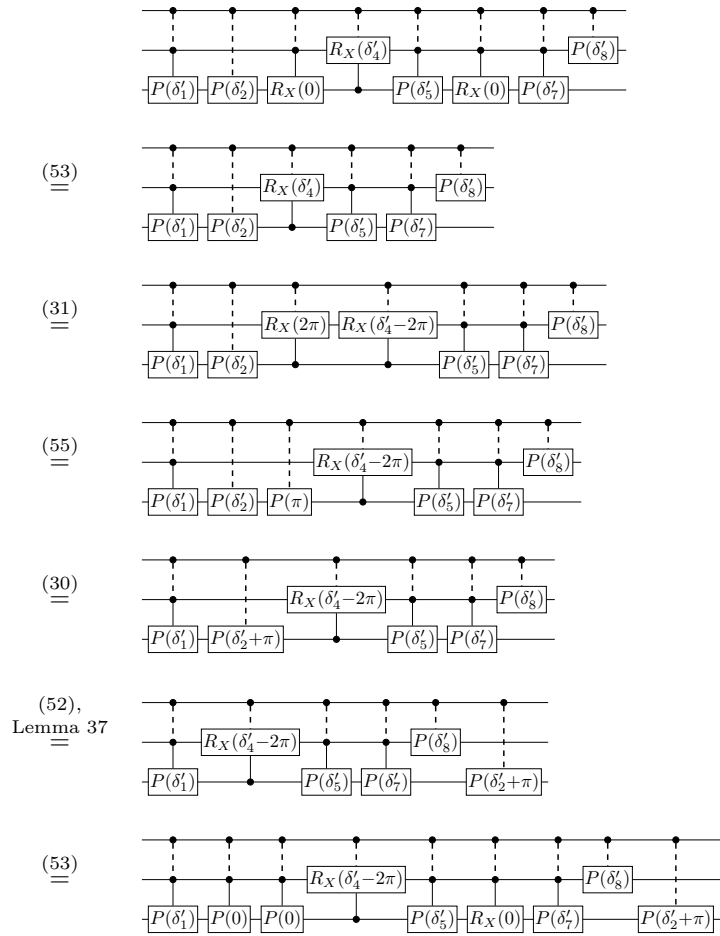


- If  $\delta'_4 \in [0, 2\pi)$  but  $\delta'_3 = 0$  and  $\delta'_2 \neq 0$ , then the conditions of Figure 2 imply that  $\delta'_6 = 0$ , so that

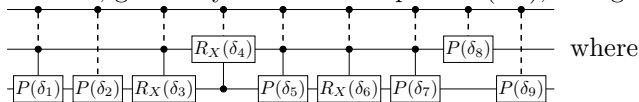




- If  $\delta'_4 \in [2\pi, 4\pi)$ ,  $\delta'_3 = 0$  and  $\delta'_2 \neq 0$ , then the conditions of Figure 2 still imply that  $\delta'_6 = 0$ , so that



Thus, given any instance of Equation  $(K^*)$ , its right-hand side can be transformed into



- $\delta_1 = \delta'_1$
- $\delta_3 = \delta'_3$
- $\delta_5 = \delta'_5$

$$\begin{aligned}
& \blacksquare \delta_7 = \delta'_7 \\
& \blacksquare \delta_2 = \begin{cases} 0 & \text{if } \delta'_3 = 0 \text{ and } \delta'_2 \neq 0 \\ \delta'_2 & \text{else} \end{cases} \\
& \blacksquare \delta_4 = \begin{cases} \delta'_4 & \text{if } \delta'_4 \in [0, 2\pi) \\ \delta'_4 - 2\pi & \text{if } \delta'_4 \in [2\pi, 4\pi) \end{cases} \\
& \blacksquare \delta_6 = \begin{cases} 2\pi - \delta'_6 & \text{if } \delta'_6 \neq 0 \text{ and } \delta'_4 \in [2\pi, 4\pi) \\ \delta'_6 & \text{else} \end{cases} \\
& \blacksquare \delta_8 = \begin{cases} \delta'_8 + \pi \bmod 2\pi & \text{if } \delta'_6 \neq 0 \text{ and } \delta'_4 \in [2\pi, 4\pi) \\ \delta'_8 & \text{else} \end{cases} \\
& \blacksquare \delta_9 = \begin{cases} \delta'_2 & \text{if } \delta'_3 = 0, \delta'_2 \neq 0 \text{ and } \delta'_4 \in [0, 2\pi) \\ \delta'_2 + \pi & \text{if } \delta'_3 = 0, \delta'_2 \neq 0 \text{ and } \delta'_4 \in [2\pi, 4\pi) \\ 0 & \text{if } (\delta'_3 \neq 0 \text{ or } \delta'_2 = 0) \text{ and } \delta'_4 \in [0, 2\pi) \\ \pi & \text{if } (\delta'_3 \neq 0 \text{ or } \delta'_2 = 0) \text{ and } \delta'_4 \in [2\pi, 4\pi) \end{cases} .
\end{aligned}$$

It is easy to check that these angles  $\delta_j$  satisfy the conditions of Figure 6 whenever the  $\delta'_j$  satisfy the conditions of Figure 2.

Let  $g$  be the function mapping any 8-tuple of angles  $\delta'_k$  corresponding to the RHS of some instance of Equation  $(K^*)$ , to the 9-tuple of angles  $\delta_j$  given by the formulas just above. Conversely, let  $f$  be the function mapping any 9-tuple of angles  $\delta_j$  corresponding to the right-hand side of some instance of Equation  $(K_{\text{old}}^*)$ , to the 8-tuple of angles  $\delta'_k$  given by the formulas given before.

Given any 8-tuple  $\vec{\delta}' := (\delta'_k)_{k \in \{1, \dots, 8\}}$  of angles corresponding to the right-hand side of some instance of Equation  $(K^*)$ , one has  $f(g(\vec{\delta}')) = \vec{\delta}'$ . Indeed, let  $(\delta_j)_{j \in \{1, \dots, 9\}} := g(\vec{\delta}')$  and  $(\delta''_k)_{k \in \{1, \dots, 8\}} := f(g(\vec{\delta}'))$ .

- By definition, one has  $\delta''_k = \delta'_k$  for  $j \in \{1, 3, 5, 7\}$ .
- Concerning  $\delta''_2$ :
  - If  $\delta'_3 \neq 0$  or  $\delta'_2 = 0$ , then  $\delta_2 = \delta'_2$ , and  $\delta_9$  is either 0 or  $\pi$  depending on  $\delta'_4$ , so that  $\delta''_2 = \delta_2 = \delta'_2$ .
  - If  $\delta'_3 = 0$ ,  $\delta'_2 \neq 0$  and  $\delta'_4 \in [0, 2\pi)$  then  $\delta_9 = \delta'_2 \in (0, \pi)$ , so that  $\delta''_2 = \delta_9 = \delta'_2$ .
  - If  $\delta'_3 = 0$ ,  $\delta'_2 \neq 0$  and  $\delta'_4 \in [2\pi, 4\pi)$  then  $\delta_9 = \delta'_2 + \pi \in (\pi, 2\pi)$ , so that  $\delta''_2 = \delta_9 - \pi = \delta'_2$ .
- Concerning  $\delta''_4$ :
  - If  $\delta'_4 \in [0, 2\pi)$ , then  $\delta_4 = \delta'_4$ , and  $\delta_9$  is either 0 or  $\delta'_2$ , which in any case is in  $[0, \pi)$ , so that  $\delta''_4 = \delta_4 = \delta'_4$ .
  - If  $\delta'_4 \in [2\pi, 4\pi)$ , then  $\delta_4 = \delta'_4 - 2\pi$ , and  $\delta_9$  is either  $\pi$  or  $\delta'_2 + \pi$ , which in any case is in  $[\pi, 2\pi)$ , so that  $\delta''_4 = \delta_4 + 2\pi = \delta'_4$ .
- Concerning  $\delta''_6$  and  $\delta''_8$ :
  - If  $\delta'_6 = 0$ , then  $\delta_8 = \delta'_8$ , and  $\delta_6 = \delta'_6 = 0$ , so that  $\delta''_6 = \delta_6 = \delta'_6 (= 0)$  and  $\delta''_8 = \delta_8 = \delta'_8$ .
  - If  $\delta'_4 \in [0, 2\pi)$ , then on the one hand,  $\delta_6 = \delta'_6$  and  $\delta_8 = \delta'_8$ , and on the other hand,  $\delta_9$  is either 0 or  $\delta'_2$ , which in any case cannot be equal to  $\pi$ , so that  $\delta''_6 = \delta_6 = \delta'_6$  and  $\delta''_8 = \delta_8 = \delta'_8$ .

- If  $\delta'_6 \neq 0$  and  $\delta'_4 \in [2\pi, 4\pi)$ , then the conditions of Figure 2 imply that we cannot have both  $\delta'_3 = 0$  and  $\delta'_2 \neq 0$ , so that  $\delta_9 = \pi$ ,  $\delta_6 = 2\pi - \delta'_6$ ,  $\delta''_6 = 2\pi - \delta_6 = \delta'_6$ ,  $\delta_8 = \delta'_8 + \pi \bmod 2\pi$ , and since  $\delta'_8 \in [0, 2\pi)$ ,  $\delta''_8 = \delta_8 + \pi \bmod 2\pi = \delta'_8$ .

Thus, given any instance of Equation  $(K_{\text{old}}^*)$ , the 8-tuple  $\vec{\delta}'$  of the angles of its RHS satisfies  $\vec{\delta}' = f(g(\vec{\delta}'))$ . Since we have proved that the 9-tuple  $g(\vec{\delta}')$  corresponds to the angles of the RHS of the instance of Equation  $(K_{\text{old}}^*)$  with same LHS, and it has been proved in [5] that this 9-tuple is uniquely determined by the LHS, this proves that the 8-tuple  $\vec{\delta}'$  is uniquely determined by the LHS as well.

## D Proofs used for the completeness of $\mathbf{QC}_{\text{iso}}$

**Proof of Lemma 16.** By assumption,  $C$  is a  $n \rightarrow n + 1$   $\mathbf{QC}_{\text{iso}}$ -circuit. The only generator of  $\mathbf{QC}_{\text{iso}}$  that does not preserve the number of qubits is qubit initialisation  $\vdash$ . As there is no generator that reduces the number of qubit, there is exactly one  $\vdash$  in the circuit. Using the axioms of prop, we can pull this qubit initialisation to the top left so as to get

$$\begin{array}{c} \vdash \\ \vdots \\ \boxed{C} \\ \vdots \\ \vdash \end{array} = \begin{array}{c} \vdash \\ \vdots \\ \boxed{C'} \\ \vdots \\ \vdash \end{array} \text{ where } C' \text{ is a } \mathbf{QC}\text{-circuit.}$$

Let  $U = \llbracket C' \rrbracket$ . Since  $U(|0\rangle \otimes Id) = |0\rangle \otimes Id$ ,  $U$  is of the form  $U = \left( \begin{array}{c|c} I & 0 \\ \hline 0 & U' \end{array} \right)$  with  $U'$  unitary. By universality of  $\mathbf{QC}$ -circuits (Proposition 3), there exists a  $\mathbf{QC}$ -circuit  $C_{U'}$  that implements  $U'$ , using only global phase, phases, Hadamards, CNOTs and swaps. One can

apply the following transformations  $\boxed{H} \rightarrow \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})}$  and  $\text{CNOT} \rightarrow \text{CNOT}$ , it

leads to  $H$ -free, swap-free circuit  $\tilde{C}_{U'}$  provably equivalent (with  $\mathbf{QC}$ ) to  $C_{U'}$ .

By controlling each of the gates constituting  $\tilde{C}_{U'}$  (using definitions in Figure 1, and taking  $P(\varphi)$  as the control of global phase  $\varphi$ ) with a fresh qubit, we get a circuit  $\Lambda\tilde{C}_{U'}$  such that  $\llbracket \Lambda\tilde{C}_{U'} \rrbracket = \llbracket C' \rrbracket$ , and where the fresh qubit only sees Phases  $P$  and the control part of some

gates. By completeness of  $\mathbf{QC}$  we have  $\mathbf{QC} \vdash C' = \Lambda\tilde{C}_{U'}$  so  $\mathbf{QC}_{\text{iso}} \vdash \begin{array}{c} \vdash \\ \vdots \\ \boxed{C} \\ \vdots \\ \vdash \end{array} = \begin{array}{c} \vdash \\ \vdots \\ \boxed{\Lambda\tilde{C}_{U'}} \\ \vdots \\ \vdash \end{array}$ .

Thus, one can push the initialisation of  $\begin{array}{c} \vdash \\ \vdots \\ \boxed{\Lambda\tilde{C}_{U'}} \\ \vdots \\ \vdash \end{array}$  through all the (controlled) gates using Equations 43, 44 and 41, leading to  $\begin{array}{c} \vdash \\ \vdots \\ \vdash \end{array}$ .  $\blacktriangleleft$

To show Lemma 17, we first introduce useful known decompositions, and recall as well the usual (balanced) CSD for reference:

► **Lemma 41** (Matrix Decompositions [28]).

- **RQ (QL):** Let  $A$  be a square matrix. There exists  $Q$  unitary and  $R$  upper triangular (with non-negative diagonal coefficients) such that  $A = RQ$ . There exists  $Q'$  unitary and  $L$  lower triangular (with non-negative diagonal coefficients) such that  $A = Q'L$ .

- **Singular Value (SVD):** For any matrix  $A$ , there exist  $U$  and  $V$  unitary, and  $D = \text{diag}(d_1, \dots, d_n)$  real diagonal with  $d_i \geq d_{i+1} \geq 0$ , such that  $A = UDV$ .

$\left( \begin{array}{c|c} I & 0 \\ \hline 0 & U \end{array} \right) \left( \begin{array}{c|c} I & 0 \\ \hline 0 & D \end{array} \right) \left( \begin{array}{c|c} I & 0 \\ \hline 0 & V \end{array} \right)$  is then an SVD of  $\left( \begin{array}{c|c} I & 0 \\ \hline 0 & A \end{array} \right)$ .

- **(balanced) Cosine-Sine (CSD):** Let  $U = \left( \begin{array}{c|c} U_{00} & U_{01} \\ \hline U_{10} & U_{11} \end{array} \right)$  be unitary with  $U_{ij}$  all of the same dimension. Then, there exist  $A_0, A_1, B_0, B_1$  unitary,  $C = \text{diag}(c_0, \dots, c_n)$  and  $S = \text{diag}(s_0, \dots, s_n)$  such that  $U = \left( \begin{array}{c|c} A_0 & 0 \\ \hline 0 & A_1 \end{array} \right) \left( \begin{array}{c|c} C & -S \\ \hline S & C \end{array} \right) \left( \begin{array}{c|c} B_0 & 0 \\ \hline 0 & B_1 \end{array} \right)$  and  $C^2 + S^2 = I$ .

A more general version of the CSD exists for “unbalanced” partitions of  $U$  i.e. when the  $U_{ij}$  do not not have the same dimensions, but we will not use it in this paper.

**Proof of Lemma 17.** This is a small variation on the usual CSD. Let us start with  $U = \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & U_{00} & U_{01} \\ \hline 0 & U_{10} & U_{11} \end{array} \right)$ . Let:

- $A_0 C_0 B_0$  be an SVD of  $U_{00}$ ,
- $A_1 R$  be a QL decomposition of  $\left( \begin{array}{c|c} 0 & U_{10} B_0^\dagger \end{array} \right)$  and
- $LB_1'$  be an RQ decomposition of  $\left( \begin{array}{c} 0 \\ \hline A_0^\dagger U_{01} \end{array} \right)$ .

The unitarity forces the diagonal components of  $C_0$  to be between 0 and 1. If 1s appear, they do so as the first diagonal components, as the SVD sorts them from largest to smallest. We then denote  $C$  the submatrix of  $C_0$  which has only  $< 1$  components. We

then have:  $U = \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & A_0 & 0 \\ \hline 0 & 0 & A_1 \end{array} \right) \left( \begin{array}{c|c|c} I & 0 & R \\ \hline 0 & C & \\ \hline L & & A_1^\dagger U_{11} B_1'^\dagger \end{array} \right) \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & B_0 & 0 \\ \hline 0 & 0 & B_1' \end{array} \right)$ . Notice

that since  $C \neq C_0$  in general,  $A_0$  and  $C$  may not be of the same dimensions. The orthonormality of the columns (resp. the rows) of the middle matrix forces it to be of the

form:  $\left( \begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & C & 0 & S' \\ \hline 0 & 0 & X_0 & 0 \\ \hline 0 & S & 0 & C' \end{array} \right)$  with  $C^2 + S^2 = C'^2 + S'^2 = I = C^2 + S'^2 = C'^2 + S'^2$ . Since

both  $S$  and  $S'$  are non-negative diagonal, this implies  $S = S'$ , which then, by unitarity, forces  $C' = -C$ . Moreover, by unitarity again,  $X_0$  itself is unitary. We hence have

$\left( \begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & C & 0 & S' \\ \hline 0 & 0 & X_0 & 0 \\ \hline 0 & S & 0 & C' \end{array} \right) = \left( \begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & C & 0 & -S \\ \hline 0 & 0 & I & 0 \\ \hline 0 & S & 0 & C \end{array} \right) \left( \begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & I & 0 & 0 \\ \hline 0 & 0 & X_0 & 0 \\ \hline 0 & 0 & 0 & -I \end{array} \right)$ . Wrapping it all up, we have:

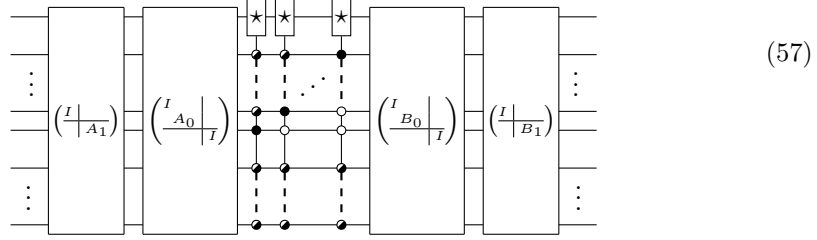
$$U = \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & A_0 & 0 \\ \hline 0 & 0 & A_1 \end{array} \right) \left( \begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & C & 0 & -S \\ \hline 0 & 0 & I & 0 \\ \hline 0 & S & 0 & C \end{array} \right) \left( \begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & I & 0 & 0 \\ \hline 0 & 0 & X_0 & 0 \\ \hline 0 & 0 & 0 & -I \end{array} \right) \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & B_0 & 0 \\ \hline 0 & 0 & B_1' \end{array} \right)$$

which gives the desired result with  $B_1 := \left( \begin{array}{c|c} X_0 & 0 \\ \hline 0 & -I \end{array} \right) B_1'$ . ◀

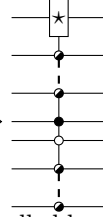
**Proof of Theorem 18.** Let  $C_1$  and  $C_2$  be two circuits of  $\mathbf{QC}_{\text{iso}}(n, n+k)$ , such that  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$ . Using the same reasoning as in the proof of Lemma 16, there exist two  $\mathbf{QC}$ -circuits



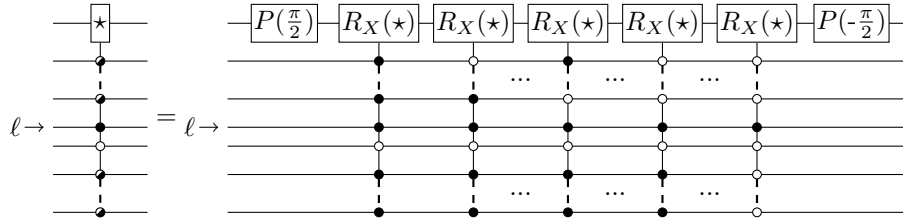
circuit:



where, similarly to [19], e.g.  $\ell \rightarrow$  is a syntactic sugar for the composition of all



rotations on the first qubit, controlled by the  $\ell$ -th qubit and anti-controlled by the  $\ell + 1$ -th qubit:



(notice that each  $R_X$  should be surrounded by  $P(\frac{\pi}{2})$  on the left and  $P(-\frac{\pi}{2})$  on the right, but all non-extremal ones simplify using (30) and (D).) By completeness of QC,  $C_U$  can be turned into the circuit in (57).

The first block (with  $A_1$ ) is such that its interpretation satisfies  $\forall |\varphi\rangle \in \mathbb{C}^{2^n}$ ,  $\left( \begin{array}{c|c} I & \\ \hline & A_1 \end{array} \right) (|0\rangle \otimes |\varphi\rangle) = |0\rangle \otimes |\varphi\rangle$ , hence using Lemma 16, it is provably deleted by intialisation on the first qubit, and a fortiori when the  $n + 1$  first qubits are initialised. Similarly, the last block (with  $B_1$ ) is deleted by the qubit initialisations.

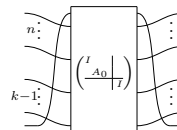
For the second block, notice that:

$$\left[ \begin{array}{c|c} \vdots & \\ \hline n & \\ \hline \vdots & \\ k-1 & \\ \hline \vdots & \end{array} \right] \left( \begin{array}{c|c} I & \\ \hline & A_0 \\ \hline & I \end{array} \right) = \left[ \begin{array}{c|c} \vdots & \\ \hline n & \\ \hline \vdots & \\ k-1 & \\ \hline \vdots & \end{array} \right]$$

which implies

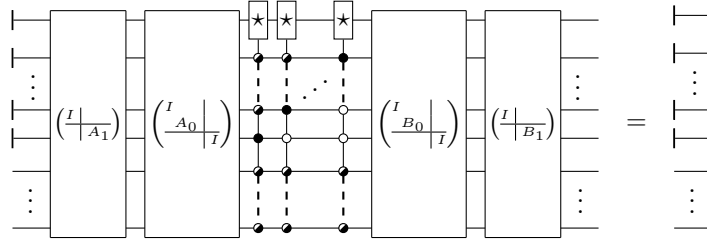
$$\left[ \begin{array}{c|c} \vdots & \\ \hline n & \\ \hline \vdots & \\ k-1 & \\ \hline \vdots & \end{array} \right] \left( \begin{array}{c|c} I & \\ \hline & A_0 \\ \hline & I \end{array} \right) = \left[ \begin{array}{c|c} \vdots & \\ \hline n & \\ \hline \vdots & \\ k-1 & \\ \hline \vdots & \end{array} \right]$$

We can hence apply the induction hypothesis on



from which we conclude

that the second block is deleted by initialisations on the  $n + 1$  first qubits. Similarly, the penultimate block (with  $B_0$ ) is deleted by initialisations on the first  $n + 1$  qubits. All the controlled rotations in the middle are deleted by the initialisations thanks to Lemma 16. Finally, it is provable that:



**E Proofs used for the completeness of  $QC_{\text{ancilla}}$**

**E.1 Proof of Proposition 22**

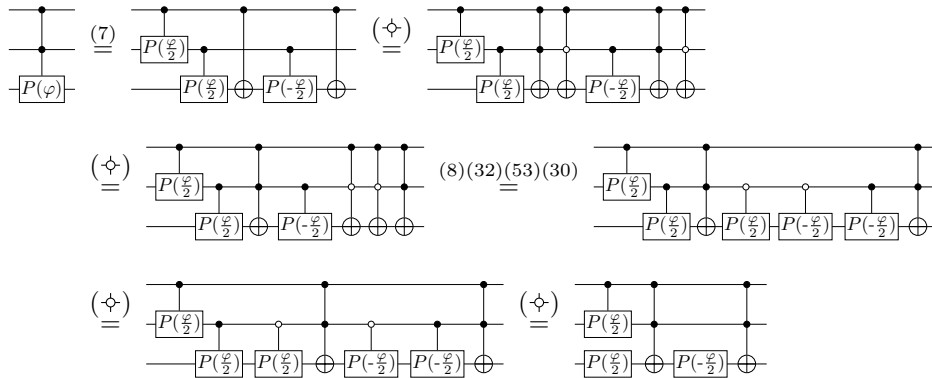
First, we derive the following equations. Equations (58) and (59) are alternative definitions of 2-controlled and 3-controlled phase gates. Equation (60) tells us how we can express a simply controlled gate with Toffoli gates and one 1-qubit gate using one ancilla.

$$\begin{array}{c}
 \text{---} \\
 \text{---} \\
 \text{---} \\
 \boxed{P(\varphi)} \\
 \text{---}
 \end{array}
 =
 \begin{array}{c}
 \text{---} \\
 \text{---} \\
 \text{---} \\
 \boxed{P(\frac{\varphi}{2})} \\
 \oplus \\
 \boxed{P(\frac{\varphi}{2})} \oplus \boxed{P(-\frac{\varphi}{2})} \oplus
 \end{array}
 \quad (58)$$

$$\begin{array}{c}
 \text{---} \\
 \text{---} \\
 \text{---} \\
 \text{---} \\
 \boxed{P(\varphi)} \\
 \text{---}
 \end{array}
 =
 \begin{array}{c}
 \text{---} \\
 \text{---} \\
 \text{---} \\
 \text{---} \\
 \boxed{P(\frac{\varphi}{2})} \\
 \oplus \\
 \boxed{P(\frac{\varphi}{2})} \oplus \boxed{P(-\frac{\varphi}{2})} \oplus
 \end{array}
 \quad (59)$$

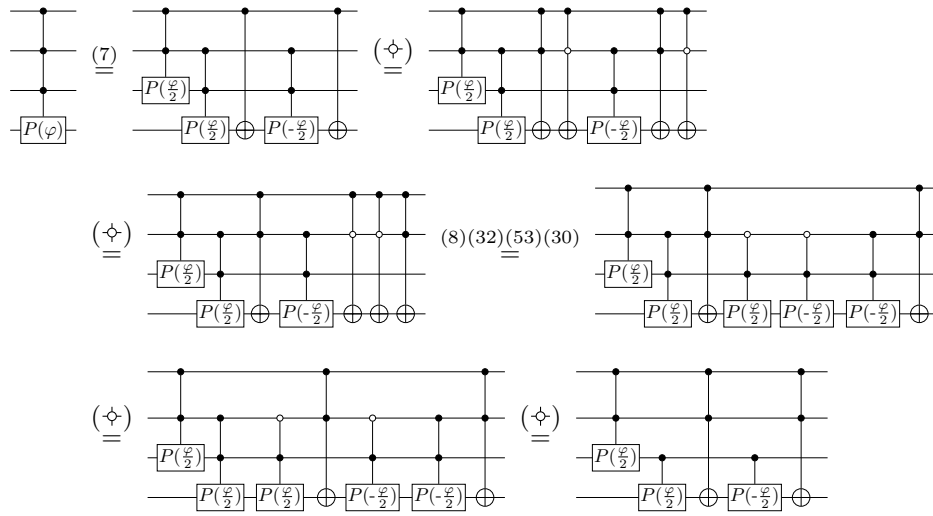
$$\begin{array}{c}
 \text{---} \\
 \text{---} \\
 \boxed{P(\varphi)} \\
 \text{---}
 \end{array}
 =
 \begin{array}{c}
 \text{---} \\
 \text{---} \\
 \text{---} \\
 \oplus \\
 \boxed{P(\varphi)} \oplus
 \end{array}
 \quad (60)$$

**Proof of Equation (58).**

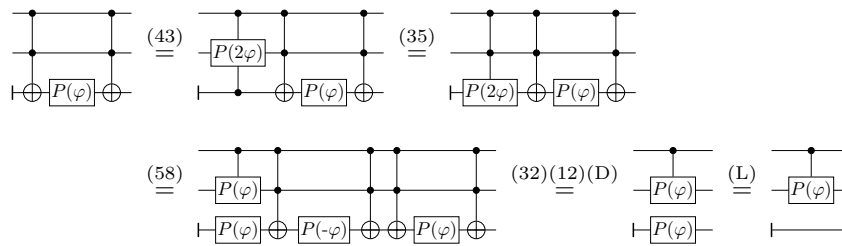




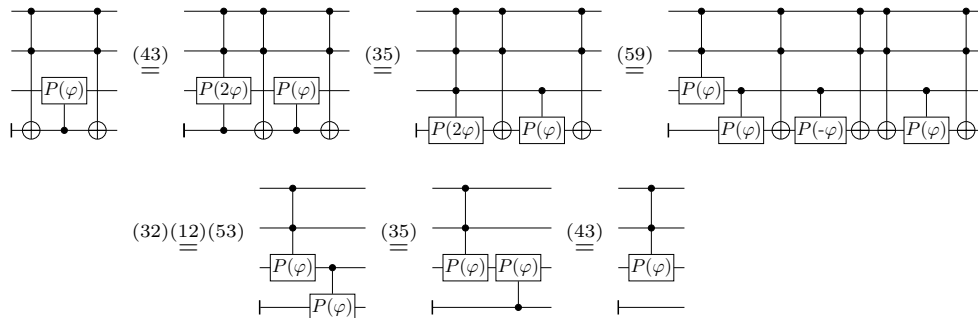
Proof of Equation (59).



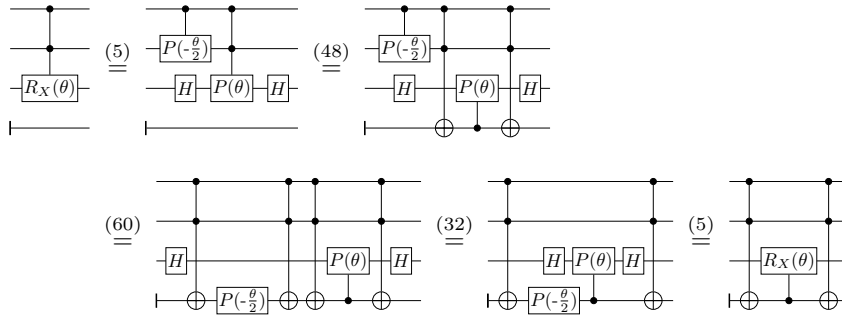
Proof of Equation (60).



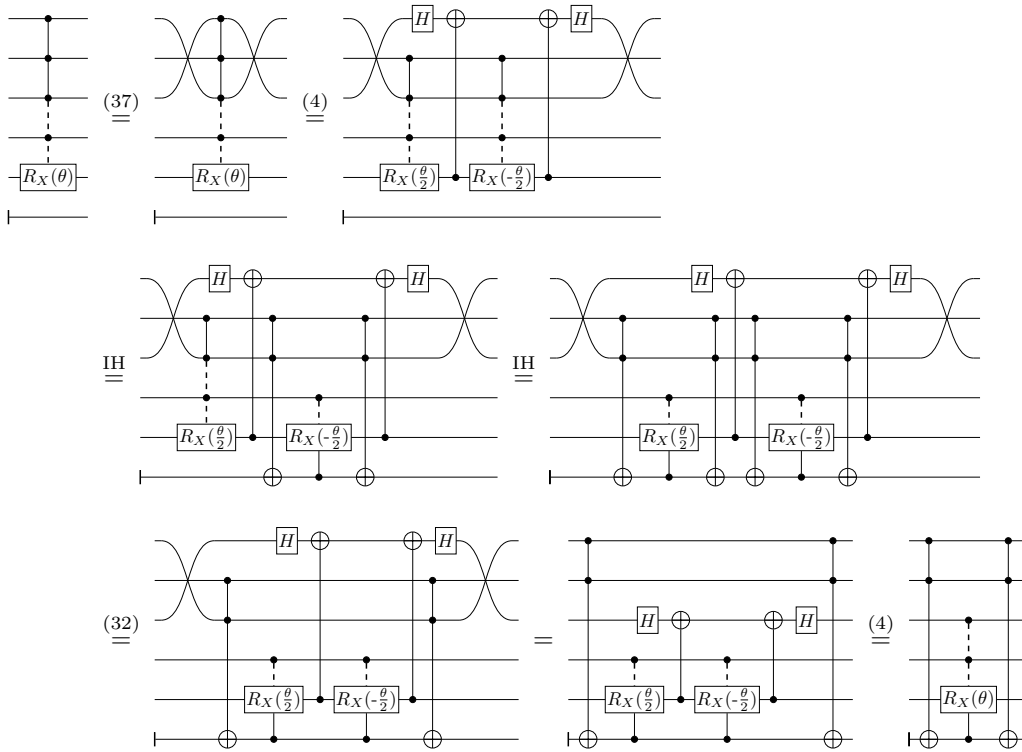
We first prove Equations (48) and (49) by induction on the number of qubits, whose base cases contains  $n = 4$  qubits. The base case for Equations (48) can be derived as follows.



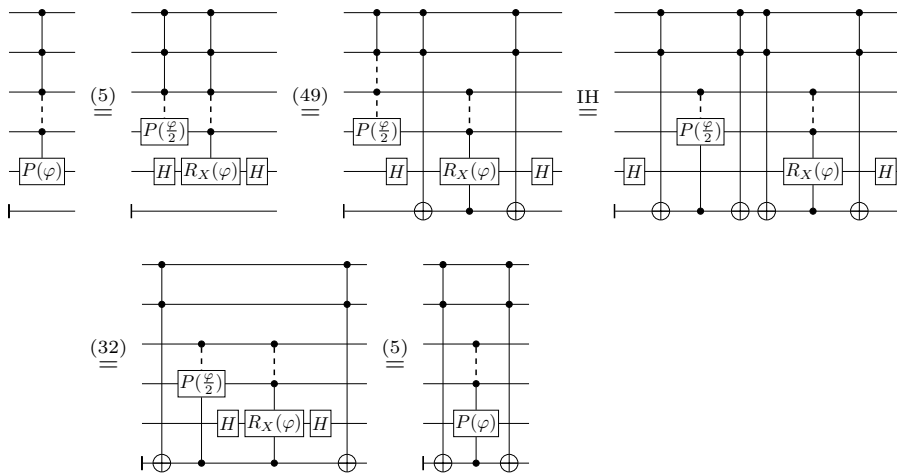
The base case for Equations (48) can be derived as follows.



The induction step for Equation (49) can be derived as follows.

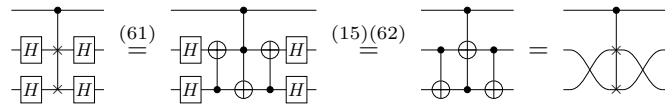


The induction step for Equation (48) can be derived as follows.

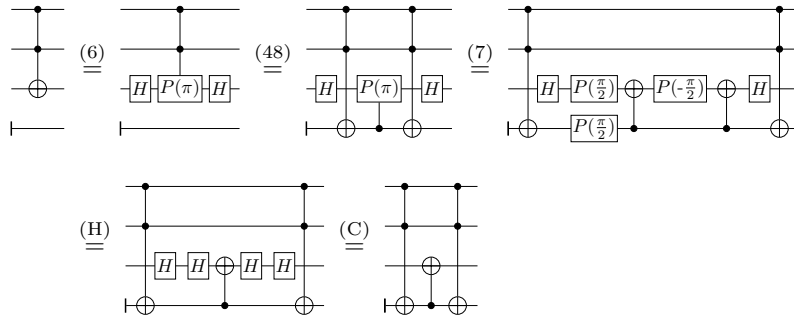




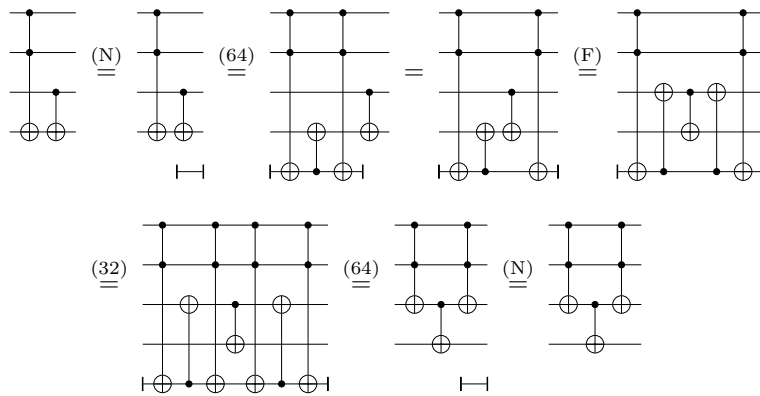
Proof of Equation (63).



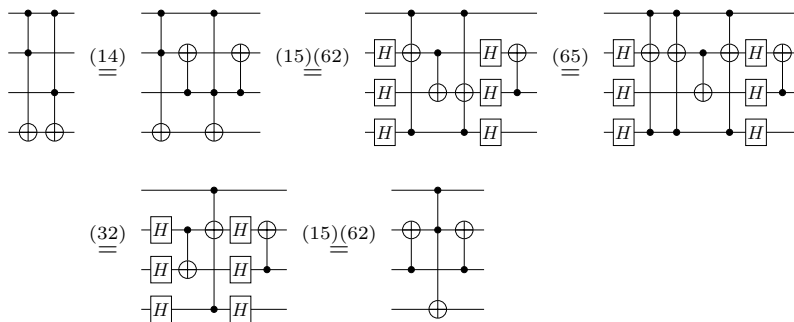
Proof of Equation (64).



Proof of Equation (65).



Proof of Equation (66).





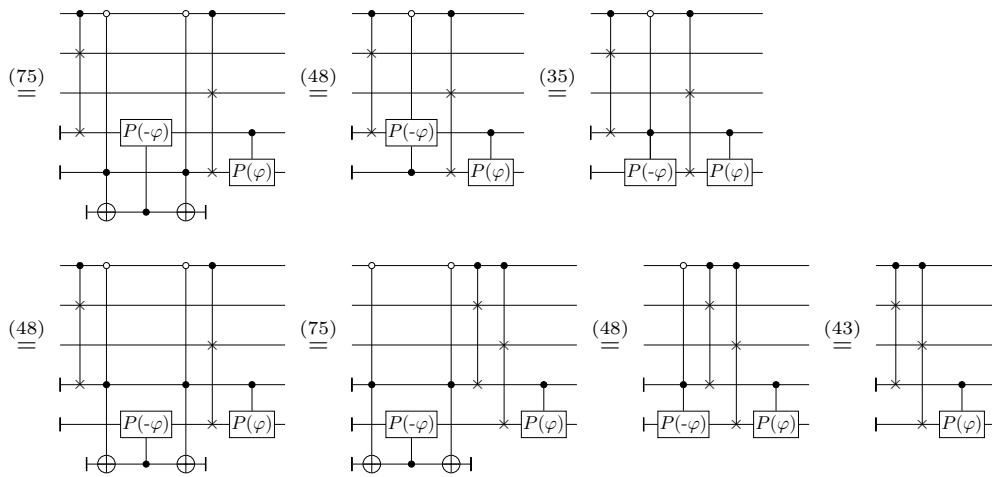


(77)

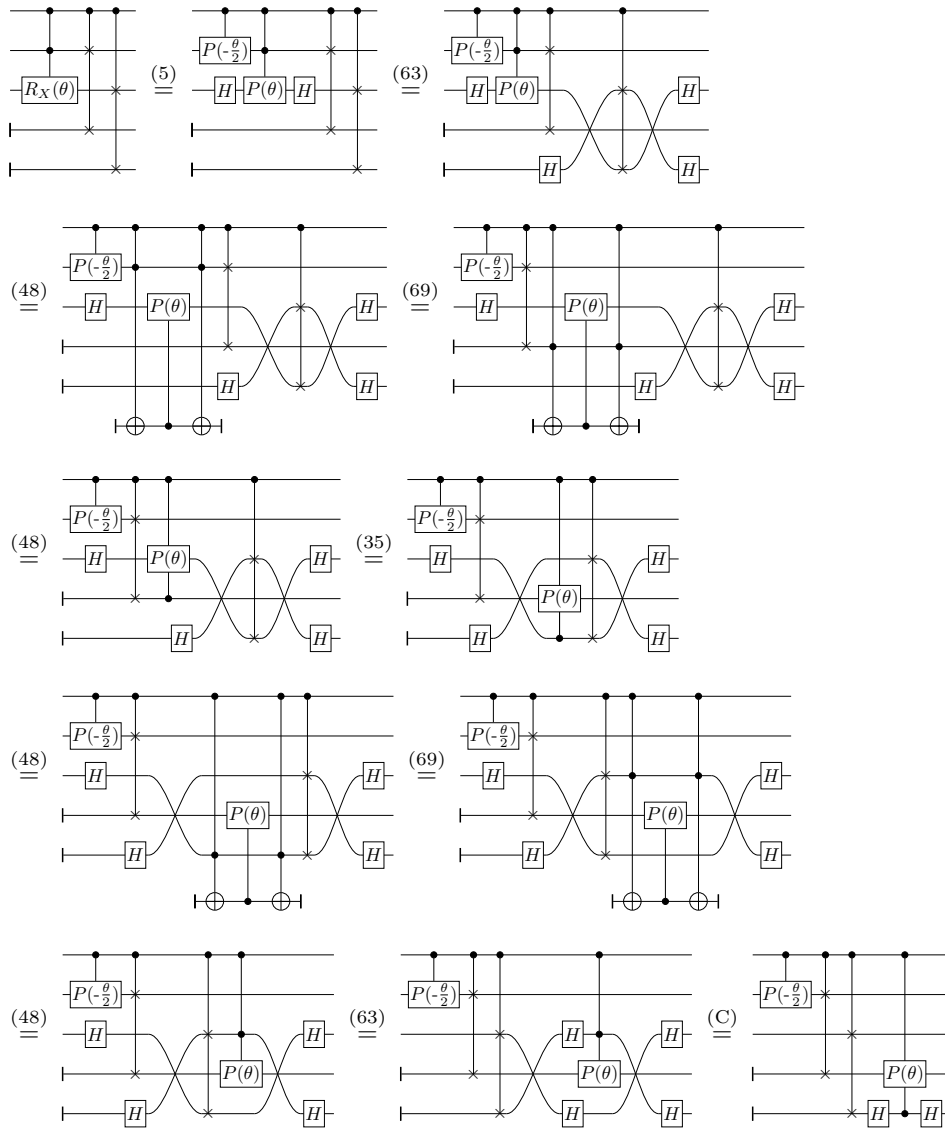
(78)

Proof of Equation (76).

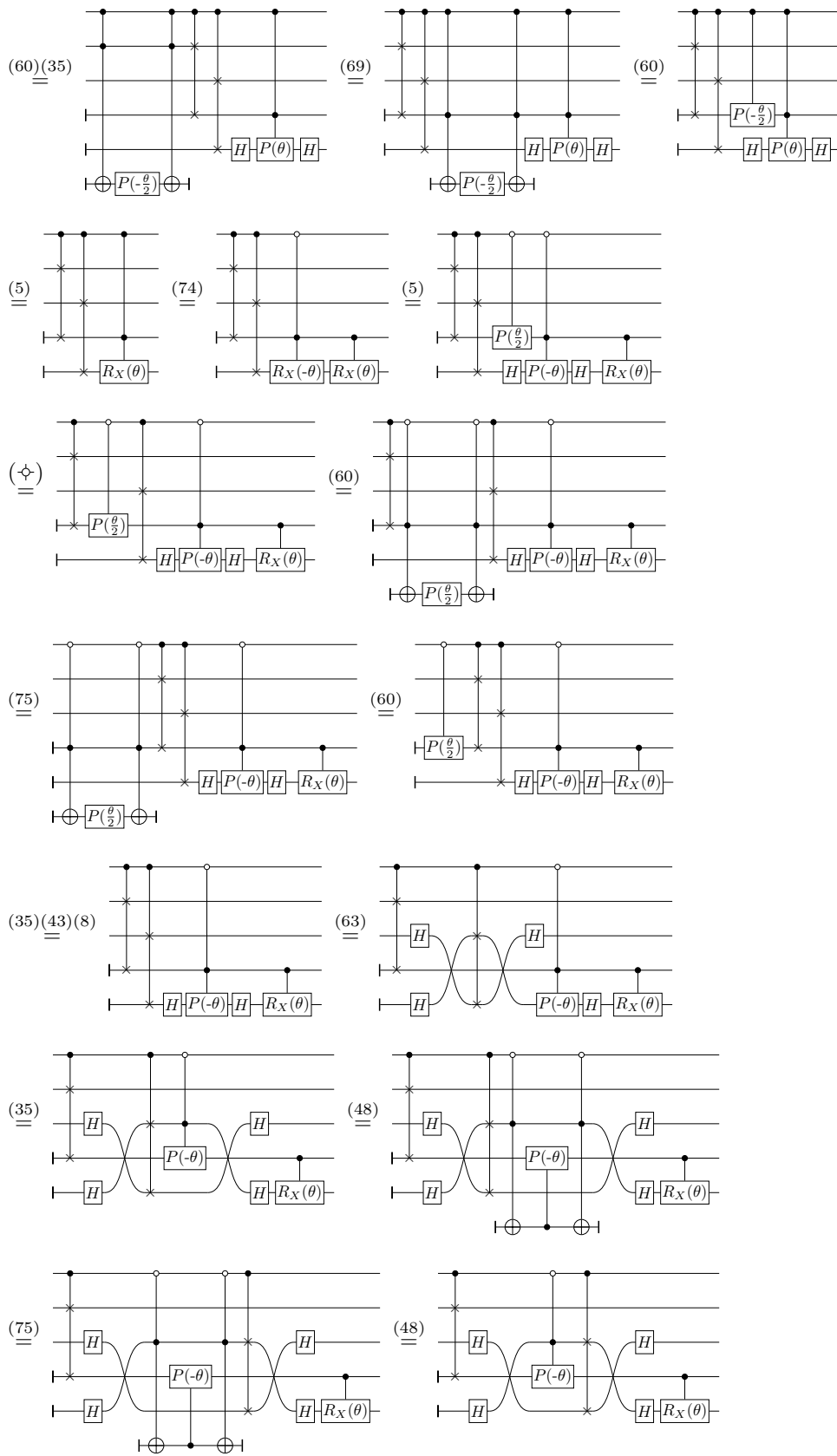
Proof of Equation (77).

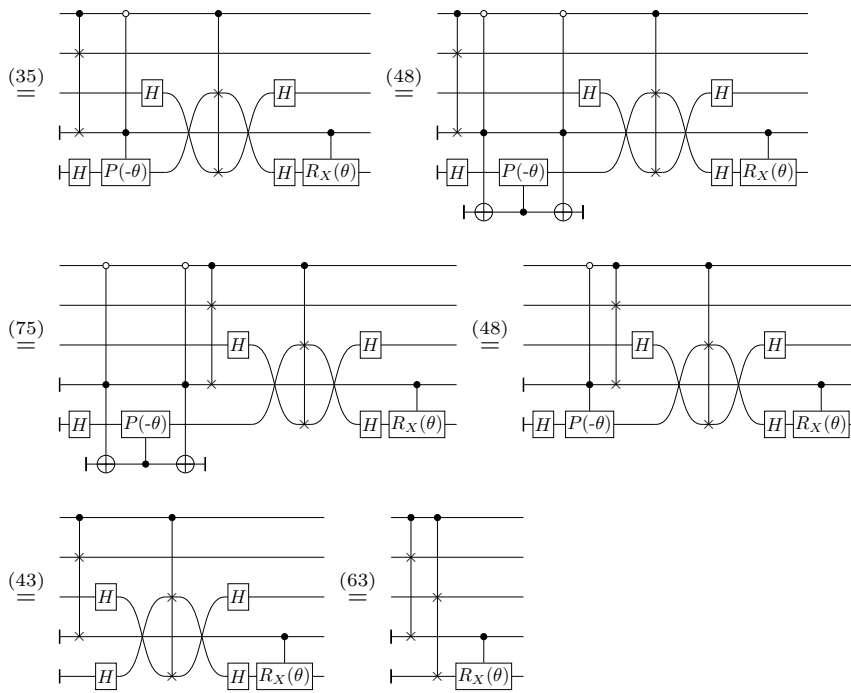


**Proof of Equation (78).**

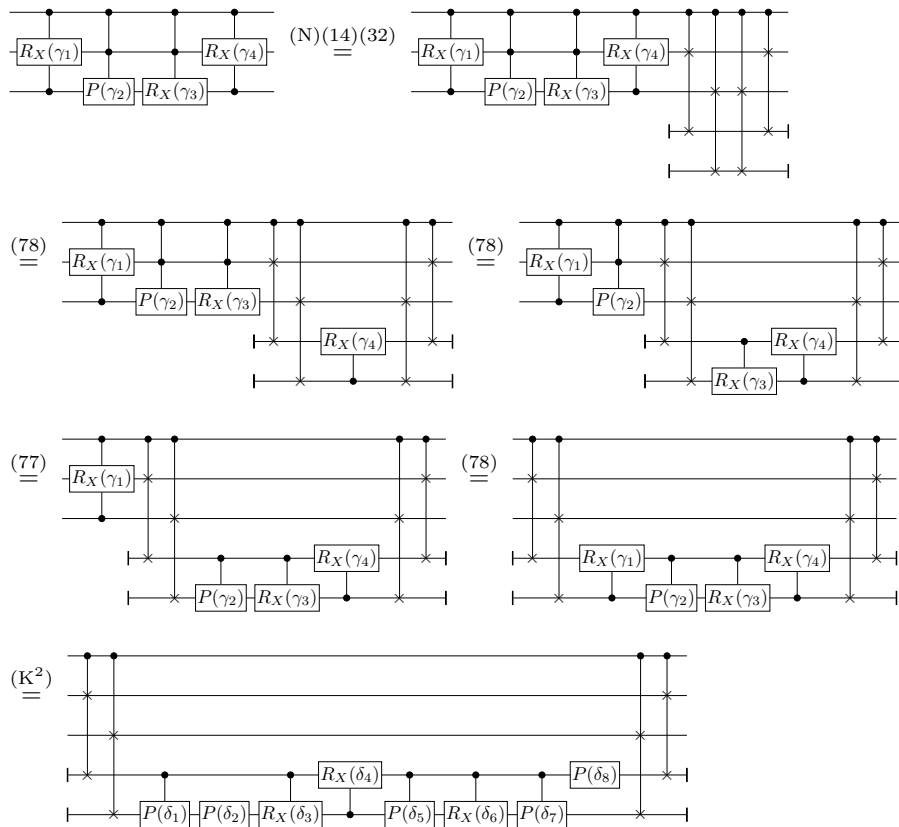


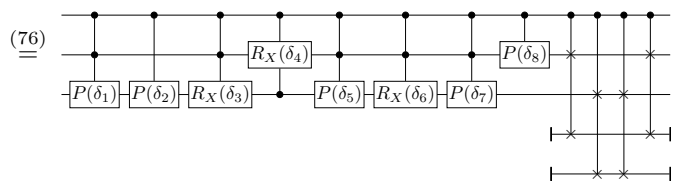
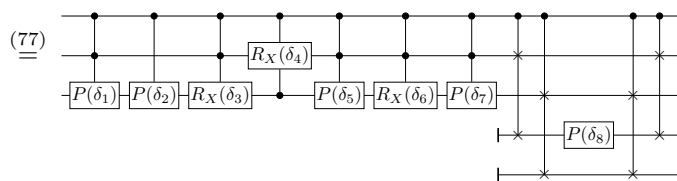
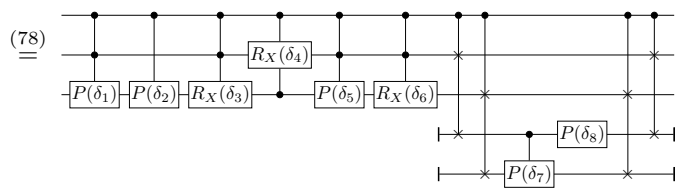
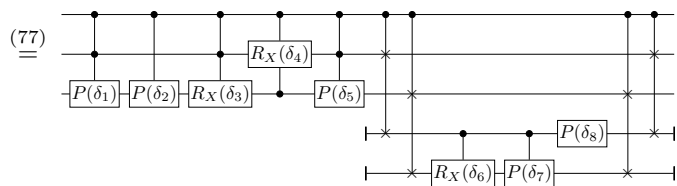
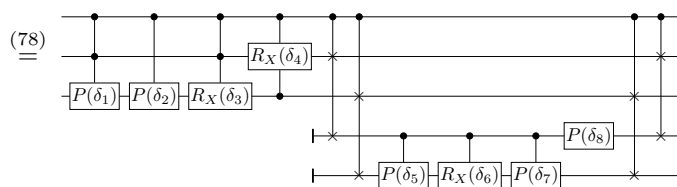
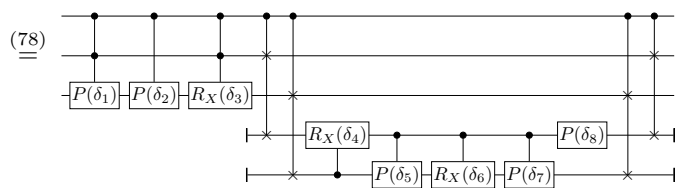
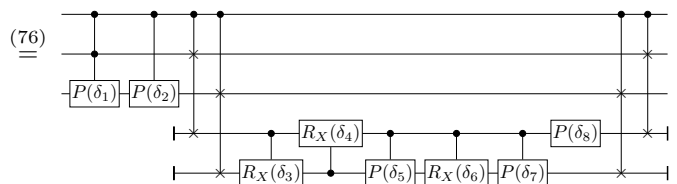
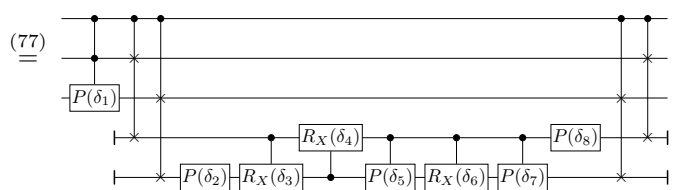


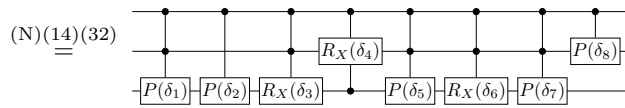




**Proof of Equation  $(K^3)$ .**







E.3 Induction step for the proof of Equation ( $K^*$ )

