



# Quantum Circuit Completeness: Extensions and Simplifications

Alexandre Clément, Noé Delorme, Simon Perdrix, Renaud Vilmart

## ► To cite this version:

Alexandre Clément, Noé Delorme, Simon Perdrix, Renaud Vilmart. Quantum Circuit Completeness: Extensions and Simplifications. International Conference on Computer Science Logic CSL 2024, Feb 2024, Naples, Italy. hal-04016498v2

**HAL Id: hal-04016498**

**<https://hal.science/hal-04016498v2>**

Submitted on 17 Aug 2023 (v2), 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.

# Quantum Circuit Completeness: Extensions and Simplifications

Alexandre Clément   

Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria, LMF, 91190, Gif-sur-Yvette, France

Noé Delorme   

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

Simon Perdrix   

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

Renaud Vilmart   

Université Paris-Saclay, ENS Paris-Saclay, CNRS, Inria, LMF, 91190, Gif-sur-Yvette, France

---

## Abstract

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

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

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

**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 [16], 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 [21, 31, 32, 33, 36]. 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 (denoted  $QC_{old}$  in the following) for quantum circuits has been introduced recently [10]. This equational theory has been derived from the LOv-calculus [9], a language for optical quantum computing. Before that, complete equational theories were only known for non-universal fragments of quantum circuits, such

---

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

as Clifford+T circuits acting on at most two qubits [6, 13], the stabiliser fragment [30, 40], the CNot-dihedral fragment [1], or fragments of reversible circuits [22, 12, 11].

The quantum circuit model can naturally be extended to encounter ancillary qubits, measurements, or qubit discarding, in order to express more general evolutions like isometries and completely positive trace preserving maps. In a model of quantum circuits with ancillae, one can use an additional work space by adding fresh qubits, as well as releasing qubits when they are in a specific state. Even if the vanilla quantum circuits form a universal model of quantum computation,<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) [34]. 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 [41, 14] with this class of circuits. The study of hybrid quantum-classical models is also a subject of interest in algorithmic and complexity theory [19, 2].

*Contributions.* We address here the problem of simplifying the complete equational theory  $\text{QC}_{\text{old}}$ . Obtained through a non-trivial translation from the LOv-calculus,  $\text{QC}_{\text{old}}$  involves non-trivial equations (see Figures 3 and 4), in particular Figure 4 displays a family of equations acting on an unbounded number of qubits, witness of the non-functoriality of the back and forth translations between quantum circuits and optical circuits, due to the fundamentally different interpretations of the parallel composition in the two circuit languages.

We show that several rules, including two of the three most intricate ones (Figure 3), can actually be derived from the other rules, the third one (Figure 4) being slightly simplified. This leads to a simpler, more compact and easier to use complete equational theory, which however still involves a family of equations acting on an unbound number of qubits.

We consider the more expressive frameworks of quantum circuits with ancilla and/or discards. Several constructions for discarding [20, 8], measurements and quantum operations [43], allow one to turn the complete equational theory for vanilla quantum circuits into complete equational theories for quantum circuits with ancilla and/or discards, by adding a few extra equations. We then mainly show that in these more expressive setting, the unbounded family of equations (Figure 4) can be derived from bounded ones, leading to complete equational theories acting on a most three qubits.

*Related work.* The first complete equational theory for a universal quantum computing model has been introduced in 2017 for the ZX-calculus [23]. Since then, 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  $f$  [37].

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

theories have been introduced for other universal fragments of the ZX-calculus [24, 18, 25, 47, 26] and its variants ZH-, ZW-calculi [3, 17]. ZX-like languages differ from quantum circuits mainly in two ways: they are more expressive, allowing the representation of any matrix<sup>5</sup> so in particular those representing post-selected evolutions for instance; the second major difference – and the most important in our context – is that not all the generators are unitary, thus even if a ZX-diagram represents an overall unitary evolution, it does not provide in general a (deterministic) implementation by means of elementary gates contrary to the quantum circuit model. To circumvent this problem one can consider the so-called subclass of circuit-like ZX-diagrams which is in one-to-one correspondence with quantum circuits, however this class is not closed under the known complete equational theories of the ZX-calculus. In particular, the problem of transforming a ZX-diagram representing a unitary evolution into a circuit-like one has been studied in the context of circuit optimisation [27], leading to various heuristics [28, 4, 15]. However, this approach fails so far to lead to a complete equational theory for quantum circuits.

The paper is structured as follows. In Section 2, we consider vanilla quantum circuits together with a new equational theory QC. We prove the completeness of QC first for the fragment of 1-CNot circuits,<sup>6</sup> that we then use to derive the remaining equations of the already known complete equational theory QC<sub>old</sub> introduced in [10]. In Section 3, we introduce an extension of vanilla quantum circuits with  $|0\rangle$ -state initialisation. Universal for isometries, such quantum circuits with initialisation are introduced as an intermediate step towards circuits with ancillae and/or discard. We add to the equational theory QC two basic equations involving qubit-initialisation, and provide a proof of completeness of the augmented equational theory QC<sub>iso</sub> using a particular circuit decomposition based on the so-called cosine-sine decomposition of unitary maps. The completeness of QC<sub>iso</sub> is extended to provide complete equational theories for quantum circuits with ancillae (QC<sub>ancilla</sub> in Section 4) – which additionally allow for the release of qubits when they are in a specific state – and for quantum circuits with qubit discarding (QC<sub>discard</sub> 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 [29], 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  $\begin{smallmatrix} m \\ \vdots \\ \boxed{C_1} \\ \vdots \\ n \end{smallmatrix}$  and  $\begin{smallmatrix} p \\ \vdots \\ \boxed{C_2} \\ \vdots \\ q \end{smallmatrix}$  can be composed: (1) “in sequence”  $C_2 \circ C_1 : m \rightarrow q$  if  $n = p$ , graphically  $\begin{smallmatrix} m \\ \vdots \\ \boxed{C_1} \\ \vdots \\ \boxed{C_2} \\ \vdots \\ q \end{smallmatrix}$ ;

(2) “in parallel”  $C_1 \otimes C_2 : m + p \rightarrow n + q$ , graphically  $\begin{smallmatrix} m & p \\ \vdots & \vdots \\ \boxed{C_1} & \boxed{C_2} \\ \vdots & \vdots \\ n & q \end{smallmatrix}$ . The *unit* for tensor product

<sup>5</sup> the only constraint is on the dimension of the matrices which must be a power of two for the qubit case, qudit versions also exist [7, 39]

<sup>6</sup> The sub-class of quantum circuits made of at most one CNot gate.

$\otimes$  is the *empty circuit*:  $\boxed{\phantom{0}} : 0 \rightarrow 0$ . This means  $\boxed{\phantom{0}} \otimes C = C = C \otimes \boxed{\phantom{0}}$  for any circuit  $C$ . The circuit  $\text{---} : 1 \rightarrow 1$  depicts the identity,  $\text{---} : 2 \rightarrow 2$  is the identity on two wires and more generally  $\text{---}^{\otimes m} := \text{---} \otimes (\text{---})^{\otimes m-1} : m \rightarrow m$  (with  $(\text{---})^{\otimes 0} := \boxed{\phantom{0}}$ ) 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  $\text{---} \times \text{---} : 2 \rightarrow 2$  which satisfies  $\text{---} \times \text{---} = \text{---}$ . Graphically (and semantically in what follows)  $\text{---} \times \text{---}$  swaps places. By compositions, we may build the following family of circuits

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

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”. For instance, the following identities are valid transformations:

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

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 the very standard gateset: Hadamard, Phase gates, and CNot, together with global phases:

► **Definition 1.** Let **QC** be the prop generated by  $\boxed{H} : 1 \rightarrow 1$ ,  $\boxed{P(\varphi)} : 1 \rightarrow 1$ ,  $\bigoplus : 2 \rightarrow 2$  and  $\odot : 0 \rightarrow 0$  for any  $\varphi \in \mathbb{R}$ .

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

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


$$\llbracket \boxed{\phantom{0}} \rrbracket = 1 \mapsto 1 \quad \llbracket \odot \rrbracket = 1 \mapsto e^{i\varphi} \quad \llbracket \boxed{H} \rrbracket = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}} \quad \llbracket \boxed{P(\varphi)} \rrbracket = |x\rangle \mapsto e^{ix\varphi} |x\rangle$$

$$\llbracket \bigoplus \rrbracket = |x, y\rangle \mapsto |x, x \oplus y\rangle \quad \llbracket \text{---} \rrbracket = |x\rangle \mapsto |x\rangle \quad \llbracket \text{---} \times \text{---} \rrbracket = |x, y\rangle \mapsto |y, x\rangle$$

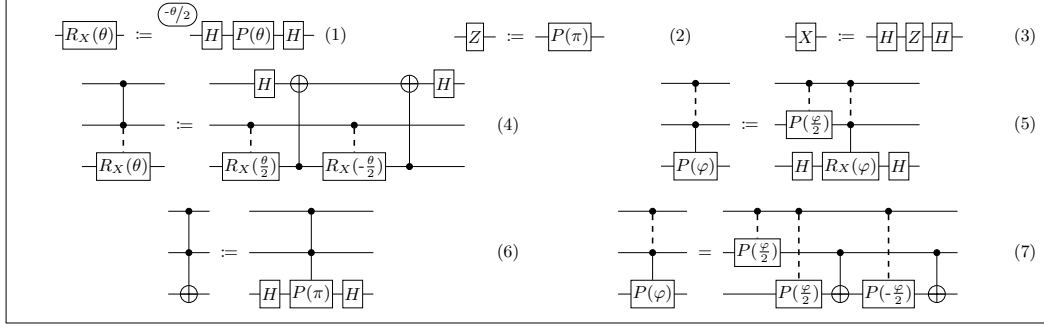
Note that for any **QC**-circuit  $C$ ,  $\llbracket C \rrbracket$  is unitary. Conversely, it is well known that any unitary map acting on a finite number of qubits can be represented by a **QC**-circuit:

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

Quantum circuits, as defined above, only have four different kinds of generators, however, it is often convenient to use other gates that can be defined by combining them. For instance, following [5, 10], Pauli gates, Toffoli, X-rotations, and multi-controlled gates are defined in Figure 1. Note that while the phase gate  $\boxed{P(\varphi)}$  is  $2\pi$ -periodic, the X-rotation  $\boxed{R_X(\theta)}$  is  $4\pi$ -periodic.

We use the standard bullet-based notation for multi-controlled gates. For instance  denotes the application of a phase gate  $\boxed{P(\varphi)}$  on the third qubit controlled by the first two

qubits. With a slight abuse of notations, we use dashed lines for arbitrary number of control qubits, e.g.  $\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} : n+1 \rightarrow n+1$  or simply  $\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} : n+1 \rightarrow n+1$  have  $n \geq 0$  control qubits (possibly zero), whereas  $\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} : n+2 \rightarrow n+2$  and  $\begin{array}{c} \text{---} \\ | \\ \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} \begin{array}{c} \bullet \\ | \\ \text{---} \end{array} : 1+n+1 \rightarrow 1+n+1$  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  $\text{QC}$  defined in Figure 2. We write  $\text{QC} \vdash C_1 = C_2$  when  $C_1$  can be transformed into  $C_2$  using the equations of  $\text{QC}$ . More formally,  $\text{QC} \vdash \cdot = \cdot$  is the smallest congruence which satisfies the equations of Figure 2 together with the deformation rules that come with the prop formalism.  $\text{QC}$  is sound, i.e. for any  $\text{QC}$ -circuits  $C_1, C_2$  if  $\text{QC} \vdash C_1 = C_2$  then  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$ . This can be proved by observing that all equations of  $\text{QC}$  are sound.

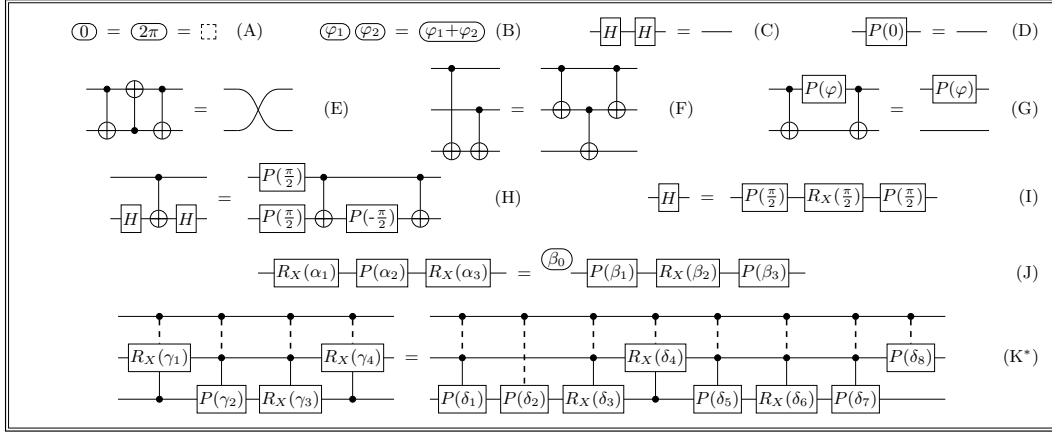
In Appendix B.2, we prove some usual circuit identities (Figure 8) using the equations of  $\text{QC}$ . We also prove in Appendix B.3 some identities about multi-controlled gates (Figure 9).

A complete equational theory  $\text{QC}_{\text{old}}$  for vanilla quantum circuits has been introduced in [10]. The rules of this original equational theory  $\text{QC}_{\text{old}}$  that are not in  $\text{QC}$  are Equations (20), (23), (26), (28), (8), (9) and  $(K_{\text{old}}^*)$  (see Figures 8, 3, and 4).<sup>7</sup> Compared to  $\text{QC}_{\text{old}}$ , Equations (20) and (23) are now subsumed by Equation (G) in  $\text{QC}$ , Equation  $(K^*)$  is a slight simplification of Equation  $(K_{\text{old}}^*)$  (with one less parameter in the RHS circuit), whereas Equations (26) and (28) (Figure 8) together with Equations (8) and (9) (Figure 3) have been removed, as we prove in the following that they can be derived in  $\text{QC}$ .

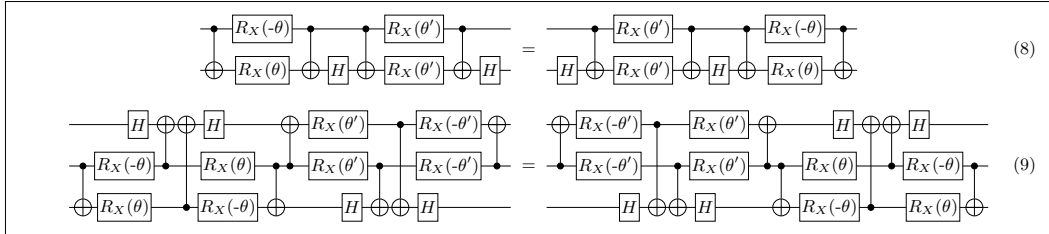
## 2.3 Reasoning on quantum circuits

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  $C_1 \circ \text{---}H\text{---} = C_2 \circ \text{---}H\text{---}$  is equivalent to proving  $C_1 = C_2$  as  $\text{---}H\text{---}$  is (provably)

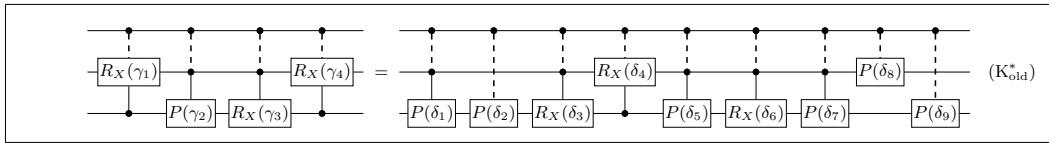
<sup>7</sup> Notice that Equations (18) and (31) are in the original equational theory  $\text{QC}_{\text{old}}$  of [10] but are proved to be derivable in the same paper.



■ **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  $\delta_5 = 0$ .



■ **Figure 3** Two of the equations of the complete equational theory  $\text{QC}_{\text{old}}$  introduced in [10] that are not in QC, defined for any  $\theta, \theta' \in \mathbb{R}$ .



■ **Figure 4** The version of Equation (K\*) given for  $\text{QC}_{\text{old}}$  in [10]. 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  $\delta_4 = \pi$  then  $\delta_2 = 0$ , if  $\delta_4 = \pi$  and  $\delta_3 = 0$  then  $\delta_1 = 0$ , and if  $\delta_6 \in \{0, \pi\}$  then  $\delta_5 = 0$ . Note that these conditions on the  $\delta_j$  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  $\delta_6 = 0$ .

reversible. Similarly, proving  $C_1 = C_2$  should be equivalent to proving  $C_1 \circ C_2^\dagger = \text{---}$ , where the adjoint of a circuit is defined as follows:

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

► **Proposition 5.**  $\llbracket C^\dagger \rrbracket = \llbracket C \rrbracket^\dagger$  for any QC-circuit  $C$ , where  $\llbracket C \rrbracket^\dagger$  is the usual linear algebra adjoint of  $\llbracket C \rrbracket$ .

**Proof.** By induction on  $C$ . ◀

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

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

and

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

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

## 2.4 Completeness

We prove the completeness of QC by showing that every equation of the original complete equational theory  $\text{QC}_{\text{old}}$  introduced in [10] can be derived in QC. To this end we first show the completeness of QC for the (modest) fragment of quantum circuits containing at most one CNot gate.

► **Lemma 7** (1-CNot completeness). QC is complete for circuits containing at most one  $\text{---}\text{---}\text{---}$ , i.e. for any QC-circuits  $C_1, C_2$  with at most one  $\text{---}\text{---}\text{---}$ , 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  $\text{---}\text{---}\text{---}$ ,  $\text{---}\text{---}\text{---}$ ,  $\text{---}\text{---}\text{---}$ ,  $\text{---}\text{---}\text{---}$  in the following equation:

$$\begin{array}{c} \text{---}\text{---}\text{---} \\ \text{---}\text{---}\text{---} \end{array} \quad \text{---}\text{---}\text{---} \quad \text{---}\text{---}\text{---} = \begin{array}{c} \text{---}\text{---}\text{---} \\ \text{---}\text{---}\text{---} \end{array} \quad \text{---}\text{---}\text{---} \quad \text{---}\text{---}\text{---}$$

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 8.** Equation (8) of Figure 3 can be derived in QC.

**Proof.** Using the simplification principle (Proposition 6), one can turn Equation (8) into an equivalent equation whose circuits contain only one  $\text{---}\text{---}\text{---}$ . The derivation is given in Appendix C.2. We conclude the proof using the completeness of QC for 1-CNot circuits (Lemma 7). ◀

► **Proposition 9.** Equation (9) of Figure 3 can be derived in QC.

**Proof.** It turns out that we can use Equation (8) to derive Equation (9) in QC. The derivation is given in Appendix C.3. ◀



► **Proposition 10.** *Equation  $(K_{\text{old}}^*)$  of Figure 4 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 into each 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 11 (Completeness).** *The equational theory QC, defined in Figure 2, is complete for QC-circuits, i.e. for any QC-circuits  $C_1, C_2$ , if  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$  then  $\text{QC} \vdash C_1 = C_2$ .*

**Proof.** All the rules of the complete equational theory introduced in [10] that are not in QC are provable in QC: Equations (20), (23), (26), (28) are proved in Appendix B.2, Equations (8), (9) and  $(K_{\text{old}}^*)$  are proved in Propositions 8, 9 and 10 respectively. ◀

### 3 Quantum circuits for isometries

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

► **Definition 12.** *Let  $\text{QC}_{\text{iso}}$  be the prop generated by  $\oplus : 0 \rightarrow 0$ ,  $\boxed{H} : 1 \rightarrow 1$ ,  $\boxed{P(\varphi)} : 1 \rightarrow 1$ ,  $\oplus : 2 \rightarrow 2$  and  $\vdash : 0 \rightarrow 1$  for any  $\varphi \in \mathbb{R}$ .*

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

► **Proposition 14 (Universality).** *Any isometry<sup>8</sup>  $V : \mathbb{C}^{\{0,1\}^n} \rightarrow \mathbb{C}^{\{0,1\}^m}$  can be realised by a  $\text{QC}_{\text{iso}}$ -circuit  $C : n \rightarrow m$  s.t.  $\llbracket C \rrbracket = V$ .*

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

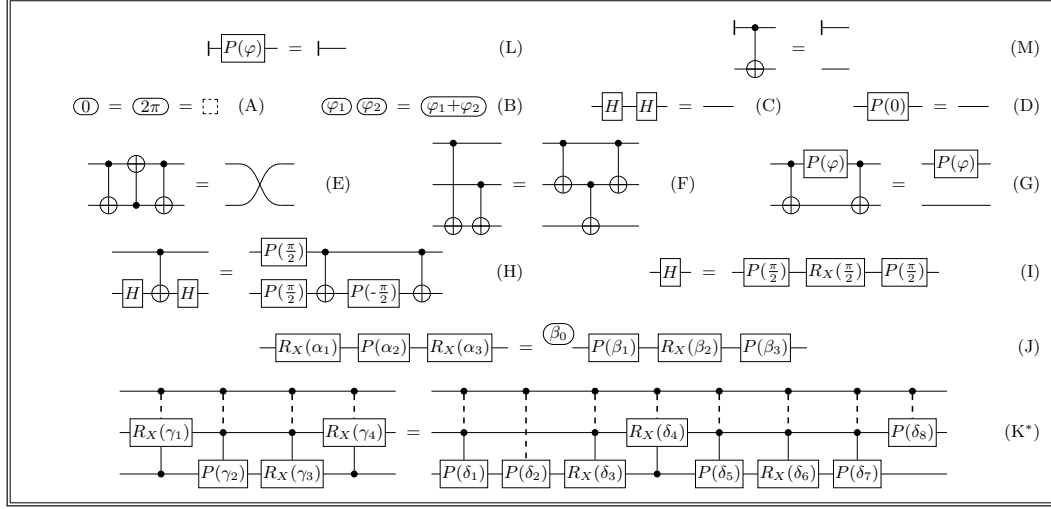


We consider the equational theory  $\text{QC}_{\text{iso}}$ , given in Figure 5, which is nothing but the equational theory QC augmented with the following two sound equations:

$$\vdash \boxed{P(\varphi)} = \vdash \quad (\text{L}) \qquad \vdash \text{ (dot on top, circle with plus on bottom) } = \vdash \quad (\text{M})$$

Viewing  $\boxed{P(\varphi)}$  as a control-global-phase gate, Equations (L), (M) can be interpreted as instances of the following property: a control gate can be removed when one of its control qubit is initialised in the  $|0\rangle$ -state. This kind of properties can actually be derived within  $\text{QC}_{\text{iso}}$  (see Figure 10 in Appendix B.4).

<sup>8</sup> An isometry is a linear map  $V$  s.t.  $V^\dagger \circ V$  is the identity.



■ **Figure 5** 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 governing the behaviour of the new generator  $\vdash$ .

► **Lemma 15.** *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:*

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

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

A direct corollary of Lemma 15 is the completeness of  $\text{QC}_{\text{iso}}$  for quantum circuits with at most one initialisation. Notice that one can then use Lemma 17 of [43] to essentially prove the completeness of  $\text{QC}_{\text{iso}}$ . However, as the semantics in [43] is based on CPTP maps rather than isometries (so global phases should be treated carefully), and moreover the proof of this Lemma 17 is not described, we provide a direct completeness proof of  $\text{QC}_{\text{iso}}$  in the following.

To do so, we may want to generalise Lemma 15 to any number of qubit initialisations. However, the proof does not generalise. Indeed, it relies on the fact that, semantically, the vanilla circuit of which we initialize a single qubit is necessarily of the form  $\text{diag}(I, U)$ , 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 16.** *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:

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

The above decomposition is a variation on the *Cosine-Sine Decomposition* (CSD) [38], which has already proven useful in quantum circuit synthesis [42].

**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 17** (Completeness). *The equational theory  $\mathbf{QC}_{\text{iso}}$ , defined in Figure 5, 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 15 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.

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

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

Notice that the semantics of a  $\mathbf{QC}_{\text{pre-ancilla}}$ -circuit is not necessarily an isometry as  $\llbracket \dashv \rrbracket$  is not isometric.<sup>9</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 20.** Let  $\mathbf{QC}_{\text{ancilla}}$  be the sub-prop of  $\mathbf{QC}_{\text{pre-ancilla}}$ -circuit  $C$  such that  $\llbracket C \rrbracket$  is an isometry.

<sup>9</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. Thus  $\mathbf{QC}_{\text{pre-ancilla}}$  can be seen as a language for postselected quantum computations.



(11)

(12)

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

► **Remark 22.** Notice that Equations (11) and (12) are actually derivable in  $\mathbf{QC}_{\text{iso}}$ . However, in order to provide an alternative inductive definition of multi-controlled gates (like in Equation (10)), 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  $\mathbf{QC}_{\text{ancilla}}$ , the equation  $(K^*)$  for any arbitrary number of controlled qubits:

► **Proposition 23.** *Equation  $(K^*)$  can be derived in  $\mathbf{QC}_{\text{ancilla}}$ .*

**Proof.** Let  $(K^n)$  be Equation  $(K^*)$  acting on  $n$  qubits for any  $n \geq 2$ . Equation  $(K^2)$  is in  $\mathbf{QC}_{\text{ancilla}}$ . 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  $\mathbf{QC}_{\text{ancilla}}$  for any  $n \geq 4$  by induction on  $n$  using the alternative definition of multi-controlled gates (Proposition 21), which allows us to construct an instance of the LHS circuit of  $(K^{n-1})$  from the LHS circuit of  $(K^n)$ . The detailed proof is given in E.3. ◀

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

► **Theorem 24 (Completeness).** *The equational theory  $\mathbf{QC}_{\text{ancilla}}$ , defined in Figure 6, is complete for  $\mathbf{QC}_{\text{ancilla}}$ -circuits.*

**Proof.** Proposition 23 implies that for any  $\neg$ -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  $\begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array} \left[ \begin{array}{c} C' \\ \vdots \\ \vdots \\ \vdots \end{array} \right] \begin{array}{c} \vdots \\ \vdots \\ \vdots \end{array}$ , 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:  $C''_0 := C'_0 \otimes (\neg)^{\otimes \ell-k}$ . 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  $\mathbf{QC}_{\text{ancilla}} \vdash C_0 \otimes (\neg)^{\otimes \ell-k} = C_1$ . 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 25.** Let  $\mathbf{QC}_{\text{discard}}$  be the prop generated by  $\boxed{H} : 1 \rightarrow 1$ ,  $\boxed{P(\varphi)} : 1 \rightarrow 1$ ,  $\dashv : 2 \rightarrow 1$ ,  $\vdash : 0 \rightarrow 1$  and  $\dashv : 1 \rightarrow 0$  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:

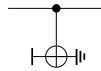
► **Definition 26 (Semantics).** For any quantum  $\mathbf{QC}_{\text{discard}}$ -circuit  $C : n \rightarrow m$ , let  $\langle C \rangle : \mathcal{M}_{2^n, 2^n}(\mathbb{C}) \rightarrow \mathcal{M}_{2^m, 2^m}(\mathbb{C})$  be the semantics of  $C$  inductively defined as the linear map  $\langle C_2 \circ C_1 \rangle = \langle C_2 \rangle \circ \langle C_1 \rangle$ ;  $\langle C_1 \otimes C_2 \rangle = \langle C_1 \rangle \otimes \langle C_2 \rangle$ ;  $\langle \dashv \rangle = \rho \mapsto \text{tr}(\rho)$  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  $\oplus$  is not part of the prop anymore. If it were, its interpretation would be  $\langle \oplus \rangle = \rho \mapsto \llbracket \oplus \rrbracket \rho \llbracket \oplus \rrbracket^\dagger = e^{i\varphi} \rho e^{-i\varphi} = \rho$ , which is the same as that of the empty circuit. Thus, for this model the X-rotation can simply be defined as  $\boxed{R_X(\theta)} := \boxed{H} \boxed{P(\theta)} \boxed{H}$  (the same definition as Figure 1 but without the global phase).

► **Proposition 27 (Universality).**  $\mathbf{QC}_{\text{discard}}$  is universal for CPTP maps.

**Proof.** According to the Stinespring dilation lemma [44], 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:

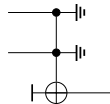


Indeed we recover the semantics of the standard basis measurement:

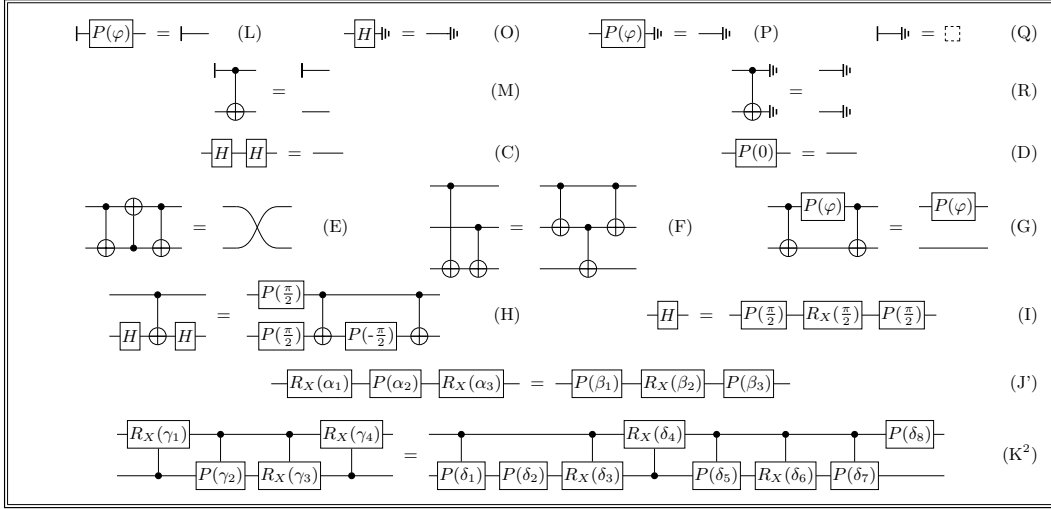
$$\left( \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \vdash \oplus \dashv \end{array} \right) = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

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.



■ **Figure 7** Equational theory  $\mathbf{QC}_{\text{discard}}$ . It contains all the equations of  $\mathbf{QC}_{\text{ancilla}}$  except Equations (A), (B), (N) and where Equation (J) has been replaced by its global-phase free-version Equation (J'), together with Equations (O), (P) (defined for any  $\varphi \in \mathbb{R}$ ), (Q) and (R), which are new equations governing the behaviour of the new generator  $\dashv$ .

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 [43] provides a way to get completeness for quantum circuits with measurements from a complete one for isometries, we instead use [8] 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  $\mathbf{QC}_{\text{discard}}$  defined in Figure 7, which is a global-phase-free version of  $\mathbf{QC}_{\text{ancilla}}$  where  $\dashv$  replaces  $\vdash$ , and with the addition of:

$$\begin{aligned} \boxed{H} \dashv &= \text{---} \quad (\text{O}) & \boxed{P(\varphi)} \dashv &= \text{---} \quad (\text{P}) & \vdash &= \boxed{\phantom{0}} \quad (\text{Q}) \\ \text{---} \dashv &= \text{---} & \text{---} \dashv &= \text{---} & & \\ \text{---} \dashv &= \text{---} & & & & \end{aligned} \quad (\text{R})$$

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

► **Theorem 28 (Completeness).** *The equational theory  $\mathbf{QC}_{\text{discard}}$ , defined in Figure 7, is complete for  $\mathbf{QC}_{\text{discard}}$ -circuits.*

**Proof.** We can use the *discard construction* [8] to build  $\mathbf{QC}_{\text{iso}}^{\dashv}$  from  $\mathbf{QC}_{\text{iso}}$ , by adding equation:

$$\dashv^{\otimes m} \circ U = \dashv^{\otimes n} \quad (13)$$

for any  $\mathbf{QC}_{\text{iso}}$ -circuit  $U : n \rightarrow m$ . The discard construction guarantees that  $\mathbf{QC}_{\text{iso}}^{\dashv}$  is complete for CPTP maps (Proposition 2 in [8]). It remains to prove that all equations in  $\mathbf{QC}_{\text{iso}}^{\dashv}$  derive from those of  $\mathbf{QC}_{\text{discard}}$ . All equations of the former except Equations (K\*) and (13) appear in  $\mathbf{QC}_{\text{discard}}$ . Those are trivially derivable. As mentioned above, it is possible to prove (K\*) from  $\mathbf{QC}_{\text{discard}}$  exactly as in the case of  $\mathbf{QC}_{\text{ancilla}}$  by replacing each occurrence of  $\vdash = \boxed{\phantom{0}}$

by  $\vdash = \Box$ . This means all the equations of  $\text{QC}_{\text{iso}}$  are derivable. Finally, all the equations  $\vdash^{\otimes m} \circ U = \vdash^{\otimes n}$  for different isometries  $U$  can be derived from Equations (O), (P), (Q), and (R).  $\blacktriangleleft$

## 6 Concluding remarks

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

This simplification of the equational theory is a step towards a minimal equational theory (i.e. an equational theory where each equation provably cannot be derived from the other ones), a question which remains open.

Getting rid of Equation (K\*) eases also the practical implementation of the rewriting rules as it avoids to consider a family of rules acting on an unbounded of qubits. Notice that regarding practical considerations, various equations presented in this paper have parameters, e.g.  $\boxed{R_X(\alpha_1)}\boxed{P(\alpha_2)}\boxed{R_X(\alpha_3)} = \boxed{P(\beta_1)}\boxed{R_X(\beta_2)}\boxed{P(\beta_3)}$  that should be read as follows: for any angle  $\alpha_i$  on the LHS, there exist  $\beta_j$  on the RHS so that the equation holds.  $\beta_j$  can be computed using fairly simple trigonometric operations. Notice that even if the equation looks non-symmetric, one can show conversely that for any  $\beta_j$  there exist  $\alpha_i$  angles such that the equation holds (see Equation (35)).

## 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 Atul Singh Arora, Andrea Coladangelo, Matthew Coudron, Alexandru Gheorghiu, Uttam Singh, and Hendrik Waldner. Quantum depth in the random oracle model. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1111–1124. ACM, 2023. URL: <https://doi.org/10.1145/3564246.3585153>, doi:10.1145/3564246.3585153.
- 3 Miriam Backens, Aleks Kissinger, Hector Miller-Bakewell, John van de Wetering, and Sal Wolffs. Completeness of the ZH-calculus. *Compositionality*, 5, July 2023. URL: <https://doi.org/10.32408/compositionality-5-5>, doi:10.32408/compositionality-5-5.
- 4 Miriam Backens, Hector Miller-Bakewell, Giovanni de Felice, Leo Lobski, and John van de Wetering. There and back again: A circuit extraction tale. *arXiv: Quantum Physics*, 2020. URL: <https://arxiv.org/abs/2003.01664>.
- 5 Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, November 1995. arXiv: quant-ph/9503016, doi:10.1103/physreva.52.3457.



- 6 Xiaoning Bian and Peter Selinger. Generators and relations for 2-qubit Clifford+T operators. *arXiv preprint arXiv:2204.02217*, 2022.
- 7 Robert I. Booth and Titouan Carette. Complete ZX-Calculi for the Stabiliser Fragment in Odd Prime Dimensions. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:15, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2022/16822>, doi:10.4230/LIPIcs.MFCS.2022.24.
- 8 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.
- 9 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. LO<sub>v</sub>-Calculus: A Graphical Language for Linear Optical Quantum Circuits. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 35:1–35:16, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2022/16833>, doi:10.4230/LIPIcs.MFCS.2022.35.
- 10 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. A complete equational theory for quantum circuits. In *Logic in Computer Science (LICS)*, 2023.
- 11 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.
- 12 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.
- 13 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.
- 14 Vincent Danos, Elham Kashefi, Prakash Panangaden, and Simon Perdrix. Extended measurement calculus. *Semantic techniques in quantum computation*, pages 235–310, 2009.
- 15 Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and Effective Techniques for T-Count Reduction via Spider Nest Identities. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:23, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2020/12070>, doi:10.4230/LIPIcs.TQC.2020.11.
- 16 D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 425(1868):73–90, 1989.
- 17 Amar Hadzihasanovic. *The algebra of entanglement and the geometry of composition*. PhD thesis, 2017.
- 18 Amar Hadzihasanovic, Kang Feng Ng, and Quanlong Wang. Two complete axiomatisations of pure-state qubit quantum computing. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '18*, pages 502–511, New York, NY, USA, 2018. ACM. URL: <http://doi.acm.org/10.1145/3209108.3209128>, doi:10.1145/3209108.3209128.
- 19 Atsuya Hasegawa and François Le Gall. An optimal oracle separation of classical and quantum hybrid schemes. In Sang Won Bae and Heejin Park, editors, *33rd International Symposium on Algorithms and Computation, ISAAC 2022, December 19-21, 2022, Seoul, Korea*, volume 248 of *LIPIcs*, pages 6:1–6:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. URL: <https://doi.org/10.4230/LIPIcs.ISAAC.2022.6>, doi:10.4230/LIPIcs.ISAAC.2022.6.

- 20 Mathieu Huot and Sam Staton. Universal properties in quantum theory. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 213–223, 2019. doi:10.4204/EPTCS.287.12.
- 21 Toshinari Itoko, Rudy Raymond, Takashi Imamichi, and Atsushi Matsuo. Optimization of quantum circuit mapping using gate transformation and commutation. *Integration*, 70:43–50, 2020.
- 22 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.
- 23 Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 559–568. ACM, 2018. URL: <https://doi.org/10.1145/3209108.3209131>, doi:10.1145/3209108.3209131.
- 24 Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 569–578. ACM, 2018. URL: <https://doi.org/10.1145/3209108.3209139>, doi:10.1145/3209108.3209139.
- 25 Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A generic normal form for ZX-diagrams and application to the rational angle completeness. In *34th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2019, Vancouver, BC, Canada, June 24-27, 2019*, pages 1–10. IEEE, 2019. URL: <https://doi.org/10.1109/LICS.2019.8785754>, doi:10.1109/LICS.2019.8785754.
- 26 Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Completeness of the ZX-Calculus. *Logical Methods in Computer Science*, Volume 16, Issue 2, June 2020. URL: <https://lmcs.episciences.org/6532>, doi:10.23638/LMCS-16(2:11)2020.
- 27 Aleks Kissinger and John van de Wetering. PyZX, 2018. URL: <https://github.com/Quantomatic/pyzx>.
- 28 Aleks Kissinger and John van de Wetering. Reducing the number of non-Clifford gates in quantum circuits. *Phys. Rev. A*, 102:022406, Aug 2020. URL: <https://link.aps.org/doi/10.1103/PhysRevA.102.022406>, doi:10.1103/PhysRevA.102.022406.
- 29 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>.
- 30 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.
- 31 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.
- 32 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.
- 33 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.
- 34 Cristopher Moore and Martin Nilsson. Parallel quantum computation and quantum codes. *SIAM journal on computing*, 31(3):799–815, 2001.
- 35 M. Möttönen and J.J. Vartiainen. *Decompositions of general quantum gates*. Nova Science Publishers Inc, United States, 2006.

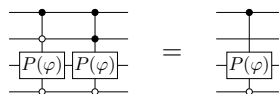
- 36 Yunseong Nam, Neil J Ross, Yuan Su, Andrew M Childs, and Dmitri Maslov. Automated optimization of large quantum circuits with continuous parameters. *npj Quantum Information*, 4(1):1–12, 2018.
- 37 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.
- 38 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).
- 39 Boldizsár Poór, Quanlong Wang, Razin A. Shaikh, Lia Yeh, Richie Yeung, and Bob Coecke. Completeness for arbitrary finite dimensions of ZXW-calculus, a unifying calculus. In *LICS*, pages 1–14, 2023. URL: <https://doi.org/10.1109/LICS56636.2023.10175672>, doi:10.1109/LICS56636.2023.10175672.
- 40 André Ranchin and Bob Coecke. Complete set of circuit equations for stabilizer quantum mechanics. *Physical Review A*, 90(1):012109, 2014.
- 41 Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical review letters*, 86(22):5188, 2001.
- 42 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).
- 43 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.
- 44 W Forrest Stinespring. Positive functions on  $c^*$ -algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.
- 45 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/10.1137/2F1.9780898719574>, doi:10.1137/1.9780898719574.
- 46 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.
- 47 Renaud Vilmart. A near-minimal axiomatisation of ZX-calculus for pure qubit quantum mechanics. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–10, 2019. doi:10.1109/LICS.2019.8785765.

## A 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*)  $\neg$  is a shortcut notation for  $\neg X \oplus X$ . For instance,

stands for the gate  $\neg P(\varphi)$  on the third qubit positively controlled by the first and fourth qubits and negatively controlled by the second qubit. According to [10] 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.

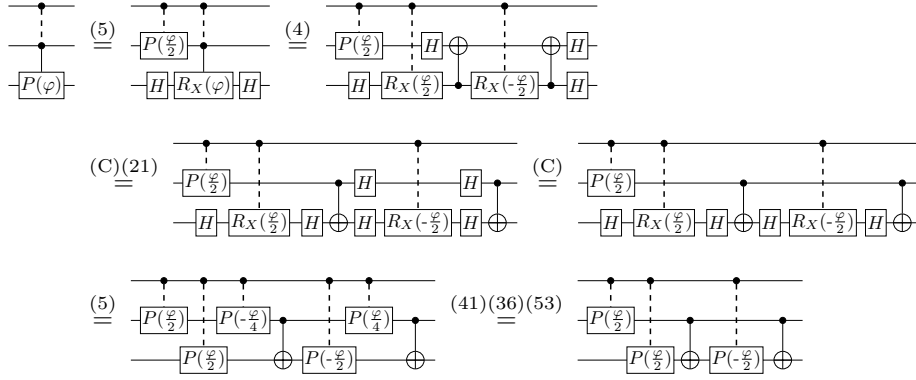


In the following, the use of such properties is denoted by  $(\diamond)$  and refers to Propositions 15, 16 and 17 (together with Propositions 10 and 11 in some cases) of [10].

## B Proofs of intermediate circuit equations

### B.1 Proof of the alternative definition of the multi-controlled phase gate

Proof of Equation (7).



### B.2 Proofs of usual circuit identities

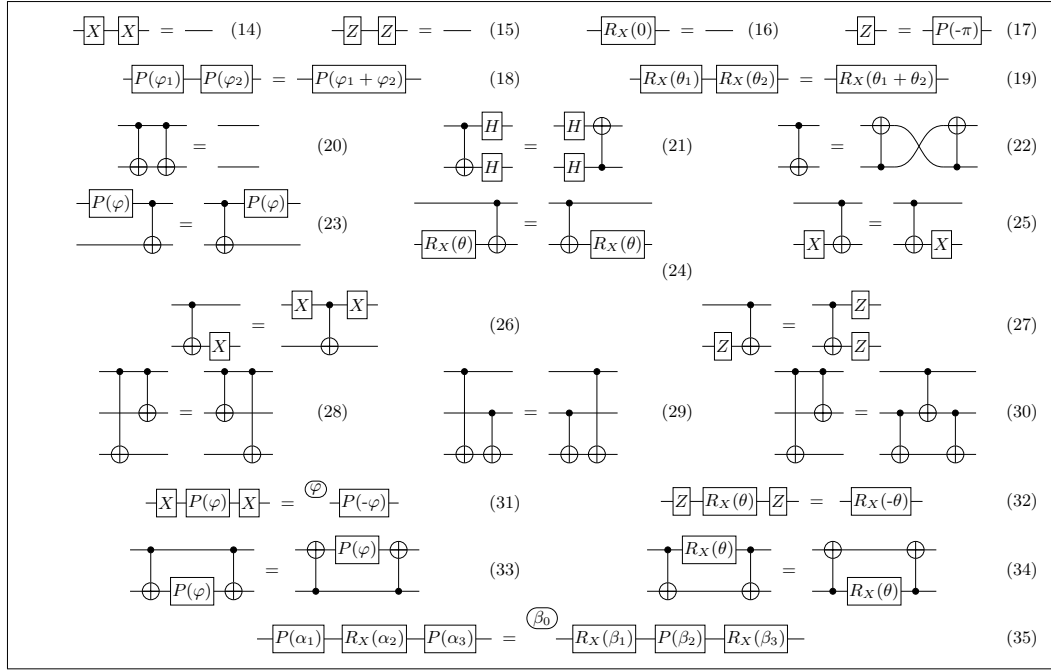
**Proof of Equation (18) and Equation (31).** Those two equations are consequences of Equation (J). See Proposition 20 of [10].

**Proof of Equation (19).**

$$\begin{aligned}
 [R_X(\theta_1)][R_X(\theta_2)] &\stackrel{(1)}{=} \left( \frac{-\theta_1 - \theta_2}{2} \right) [H][P(\theta_1)][H][H][P(\theta_2)][H] \stackrel{(C)}{=} \left( \frac{-\theta_1 - \theta_2}{2} \right) [H][P(\theta_1)][P(\theta_2)][H] \\
 &\stackrel{(18)}{=} \left( \frac{-\theta_1 + \theta_2}{2} \right) [H][P(\theta_1 + \theta_2)][H] \stackrel{(1)}{=} [R_X(\theta_1 + \theta_2)]
 \end{aligned}$$

**Proof of Equation (32).**

$$\begin{aligned}
 [Z][R_X(\theta)][Z] &\stackrel{(3)(1)}{=} \left( \frac{-\theta}{2} \right) [H][X][H][H][P(\theta)][H][H][X][H] \stackrel{(C)}{=} \left( \frac{-\theta}{2} \right) [H][X][P(\theta)][X][H] \\
 &\stackrel{(31)}{=} \left( \frac{\theta}{2} \right) [H][P(-\theta)][H] \stackrel{(1)}{=} \left( \frac{\theta}{2} \right) \left( \frac{-\theta}{2} \right) [R_X(-\theta)] \stackrel{(B)(A)}{=} [R_X(-\theta)]
 \end{aligned}$$



■ **Figure 8** Some usual identities provable in QC for any  $\varphi, \varphi_1, \varphi_2, \theta, \theta_1, \theta_2 \in \mathbb{R}$ . Equation (35) is the dual version of Equation (J) where the angles are computed in a similar way.

**Proof of Equation (14).**

$$\boxed{X} \boxed{X} \stackrel{(D)}{=} \boxed{X} \boxed{P(0)} \boxed{X} \stackrel{(31)}{=} \boxed{P(0)} \stackrel{(D)(A)}{=} \text{---}$$

**Proof of Equation (15).**

$$\boxed{Z} \boxed{Z} \stackrel{(3)}{=} \boxed{H} \boxed{X} \boxed{H} \boxed{H} \boxed{X} \boxed{H} \stackrel{(C)}{=} \boxed{H} \boxed{X} \boxed{X} \boxed{H} \stackrel{(14)}{=} \boxed{H} \boxed{H} \stackrel{(C)}{=} \text{---}$$

**Proof of Equation (16).**

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

**Proof of Equation (17).**

$$\boxed{Z} \stackrel{(D)}{=} \boxed{P(0)} \boxed{Z} \stackrel{(18)}{=} \boxed{P(-\pi)} \boxed{P(\pi)} \boxed{Z} \stackrel{(2)}{=} \boxed{P(-\pi)} \boxed{Z} \boxed{Z} \stackrel{(15)}{=} \boxed{P(-\pi)}$$

**Proof of Equation (20).**

$$\text{---} \stackrel{(D)}{=} \text{---} \boxed{P(0)} \text{---} \stackrel{(G)}{=} \boxed{P(0)} \stackrel{(D)}{=} \text{---}$$

### Proof of Equation (22).

### Proof of Equation (33).

$$\begin{array}{c}
 \text{(E)} \\
 \text{(G)}
 \end{array}
 \quad
 \begin{array}{c}
 \text{(20)} \\
 \text{(G)}
 \end{array}$$

### Proof of Equation (21).

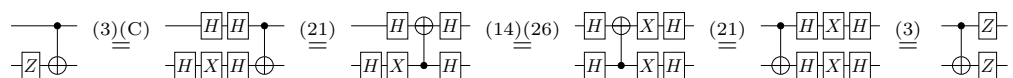
(C) (H)   
(33) (H) (C)

### Proof of Equation (34).

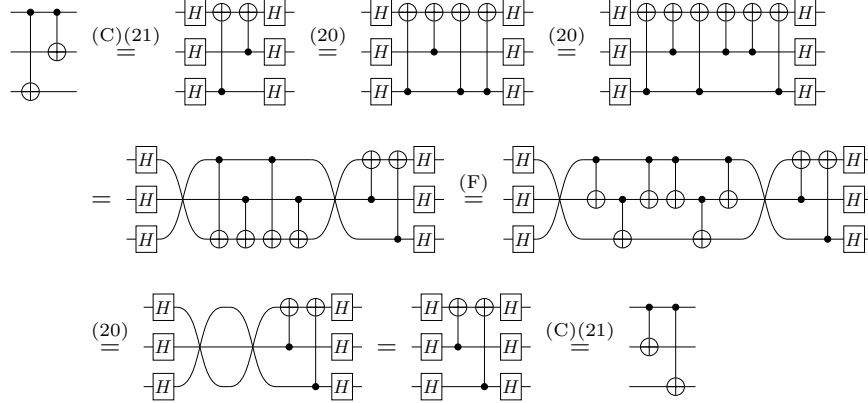
$(1)(C) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$ 
 $(21) \equiv$

### Proof of Equation (23).

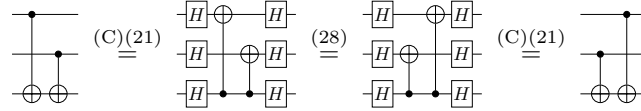
### Proof of Equation (24).



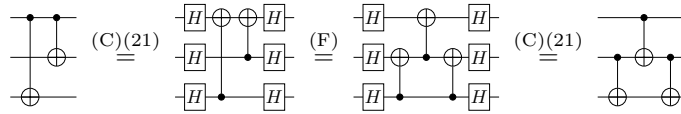
**Proof of Equation (28).**



**Proof of Equation (29).**



**Proof of Equation (30).**



**Proof of Equation (35).**

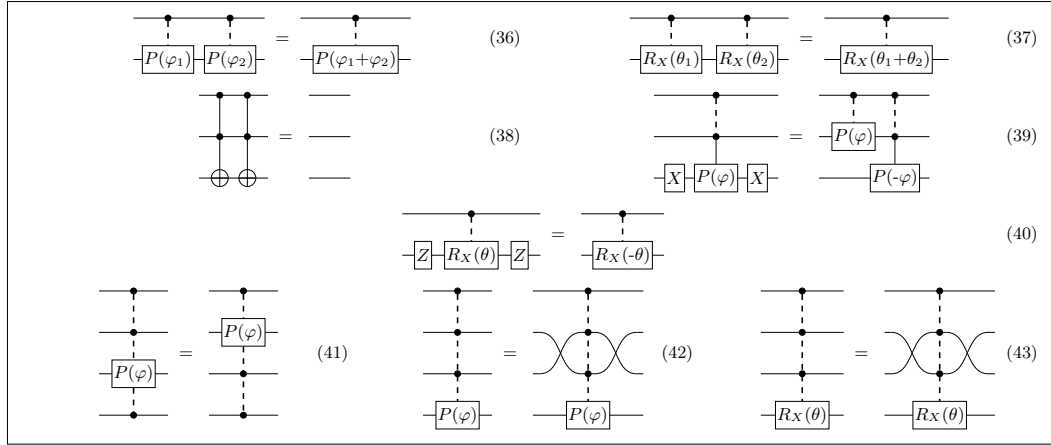
$$\begin{aligned}
 -[P(\alpha_1)]-[R_X(\alpha_2)]-[P(\alpha_3)]- & \stackrel{(1)}{=} \overset{(\alpha_0)}{[H-R_X(\alpha_1)-H-H-P(\alpha_2)-H-H-R_X(\alpha_3)-H]} \\
 & \stackrel{(C)}{=} \overset{(\alpha_0)}{[H-R_X(\alpha_1)-P(\alpha_2)-R_X(\alpha_3)-H]} \\
 & \stackrel{(J)}{=} \overset{(\alpha_0 + \beta'_0)}{[H-[P(\beta_1)]-[R_X(\beta_2)]-[P(\beta_3)]-H]}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

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 usual circuit identities over multi-controlled gates

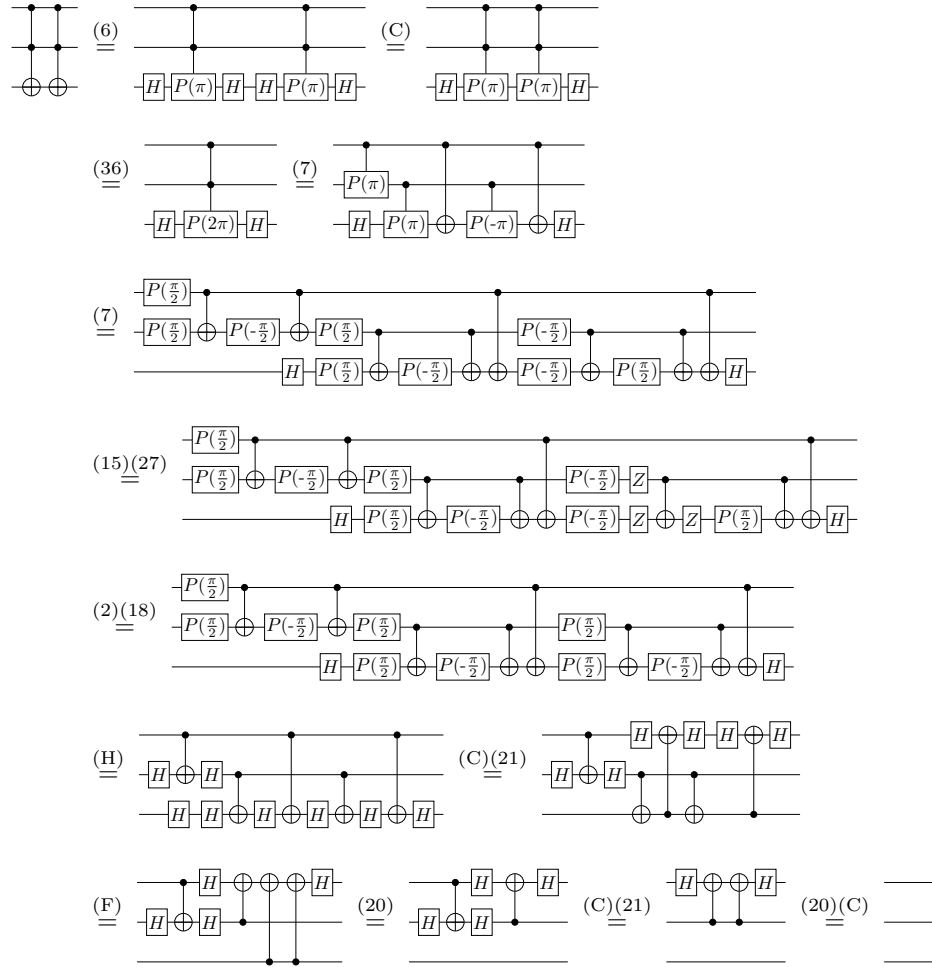
Equations (36) and (37) are proved in Proposition 13 of [10]. Equation (39) is proved in Lemma 53 of [10]. Equation (40) is proved in Lemma 47 of [10]. Equation (41) is proved in Proposition 12 of [10]. Equations (42) and (43) are proved in Proposition 11 of [10]. The proofs also hold for the equational theory QC because all the equations used are provable in QC.



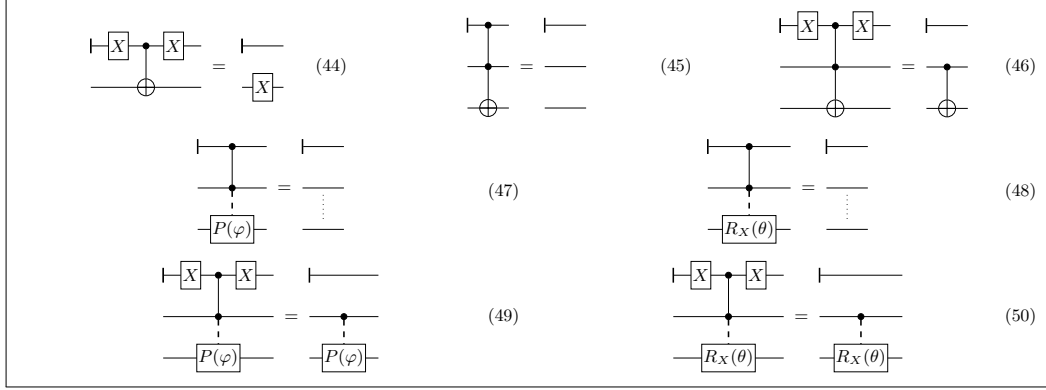


■ **Figure 9** Some usual identities over multi-controlled gates provable in QC for any  $\varphi, \varphi_1, \varphi_2, \theta, \theta_1, \theta_2 \in \mathbb{R}$ .

### Proof of Equation (38).



## B.4 Proofs of usual circuit identities using ancillae



■ **Figure 10** 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\*).

**Proof of Equation (44).**

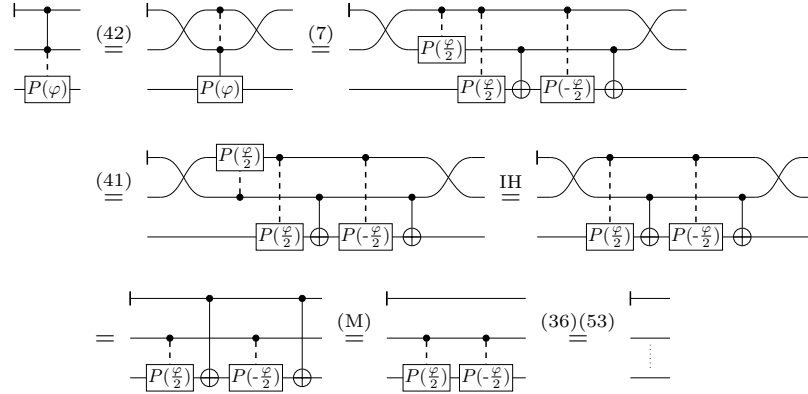
$$\begin{array}{c} \text{---} \boxed{X} \text{---} \bullet \text{---} \boxed{X} \text{---} \\ | \\ \text{---} \oplus \text{---} \end{array} \stackrel{(26)}{=} \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \oplus \text{---} \boxed{X} \text{---} \end{array} \stackrel{(M)}{=} \begin{array}{c} \text{---} \\ | \\ \text{---} \boxed{X} \text{---} \end{array}$$

**Proof of Equation (48).**

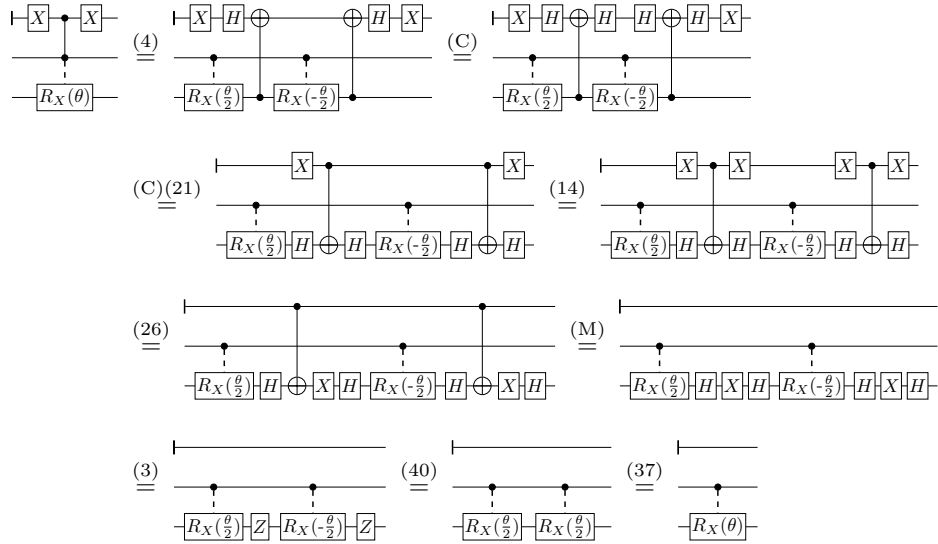
$$\begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \boxed{R_X(\theta)} \text{---} \end{array} \stackrel{(4)}{=} \begin{array}{c} \text{---} \boxed{H} \oplus \text{---} \oplus \text{---} \boxed{H} \text{---} \\ | \quad \quad \quad | \\ \text{---} \boxed{R_X(\frac{\theta}{2})} \bullet \text{---} \boxed{R_X(-\frac{\theta}{2})} \bullet \text{---} \end{array} \stackrel{(C)}{=} \begin{array}{c} \text{---} \boxed{H} \oplus \text{---} \boxed{H} \oplus \text{---} \boxed{H} \oplus \text{---} \boxed{H} \text{---} \\ | \quad \quad \quad | \quad \quad \quad | \\ \text{---} \boxed{R_X(\frac{\theta}{2})} \bullet \text{---} \boxed{R_X(-\frac{\theta}{2})} \bullet \text{---} \end{array} \\ \\ \stackrel{(C)(21)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad \quad \quad | \quad \quad \quad | \quad \quad \quad | \\ \text{---} \boxed{R_X(\frac{\theta}{2})} \text{---} \boxed{H} \oplus \text{---} \boxed{H} \text{---} \boxed{R_X(-\frac{\theta}{2})} \text{---} \boxed{H} \oplus \text{---} \boxed{H} \text{---} \end{array} \stackrel{(M)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad \quad \quad | \quad \quad \quad | \quad \quad \quad | \\ \text{---} \boxed{R_X(\frac{\theta}{2})} \text{---} \boxed{H} \text{---} \boxed{H} \text{---} \boxed{R_X(-\frac{\theta}{2})} \text{---} \boxed{H} \text{---} \boxed{H} \text{---} \end{array} \\ \\ \stackrel{(C)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad \quad \quad | \\ \text{---} \boxed{R_X(\frac{\theta}{2})} \text{---} \boxed{R_X(-\frac{\theta}{2})} \text{---} \end{array} \stackrel{(37)(53)}{=} \begin{array}{c} \text{---} \\ | \\ \text{---} \end{array}$$

**Proof of Equation (47).** By induction on the number of controls with base case  $n = 1$  control.

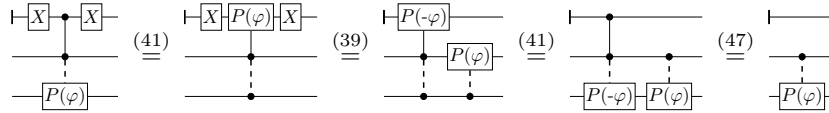
$$\begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \boxed{P(\varphi)} \text{---} \end{array} \stackrel{(7)}{=} \begin{array}{c} \text{---} \boxed{P(\frac{\varphi}{2})} \bullet \text{---} \bullet \text{---} \\ | \quad \quad \quad | \\ \text{---} \boxed{P(\frac{\varphi}{2})} \oplus \text{---} \boxed{P(-\frac{\varphi}{2})} \oplus \text{---} \end{array} \stackrel{(L)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad \quad \quad | \\ \text{---} \boxed{P(\frac{\varphi}{2})} \oplus \text{---} \boxed{P(-\frac{\varphi}{2})} \oplus \text{---} \end{array} \\ \\ \stackrel{(M)}{=} \text{---} \quad \quad \quad \stackrel{(18)(D)}{=} \text{---} \\ | \quad \quad \quad | \\ \text{---} \boxed{P(\frac{\varphi}{2})} \text{---} \boxed{P(-\frac{\varphi}{2})} \text{---} \quad \quad \quad \text{---}$$



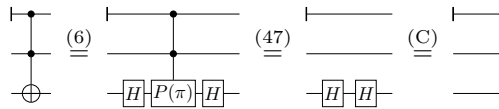
**Proof of Equation (50).**



**Proof of Equation (49).**



**Proof of Equation (45).**



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

◀

► **Lemma 33.** 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  $A = e^{i\alpha} X^k P(\varphi)$ ,  $B = e^{i\beta} Z^l R_X(\theta)$ ,  $C = e^{i\gamma} P(-\varphi) Z^l X^k$  and  $D = e^{i(-\alpha-\beta-\gamma)} R_X(-\theta) Z^l X^k$ .

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

**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  $k, l \in \{0, 1\}$ .

$$\begin{aligned} (C \otimes D) \circ \text{CNOT} \circ (A \otimes B) &= \text{CNOT} \\ \Rightarrow \begin{cases} (C \otimes D) \circ \text{CNOT} \circ (I \otimes B) &= \text{CNOT} \circ (A^\dagger \otimes I) \\ (C \otimes D) \circ \text{CNOT} \circ (A \otimes I) &= \text{CNOT} \circ (I \otimes B^\dagger) \end{cases} \\ \Rightarrow \begin{cases} \langle 0|_1 (C \otimes D) \circ \text{CNOT} \circ (I \otimes B) |0\rangle_1 &= \langle 0|_1 \text{CNOT} \circ (A^\dagger \otimes I) |0\rangle_1 \\ \langle 1|_1 (C \otimes D) \circ \text{CNOT} \circ (I \otimes B) |1\rangle_1 &= \langle 1|_1 \text{CNOT} \circ (A^\dagger \otimes I) |1\rangle_1 \\ \langle +|_2 (C \otimes D) \circ \text{CNOT} \circ (A \otimes I) |+\rangle_2 &= \langle +|_2 \text{CNOT} \circ (I \otimes B^\dagger) |+\rangle_2 \\ \langle -|_2 (C \otimes D) \circ \text{CNOT} \circ (A \otimes I) |-\rangle_2 &= \langle -|_2 \text{CNOT} \circ (I \otimes B^\dagger) |-\rangle_2 \end{cases} \\ \xRightarrow{\text{Claim 30}} \begin{cases} \langle 0|_1 (C \otimes D) \circ (I \otimes I) \circ (I \otimes B) |0\rangle_1 &= \langle 0|_1 (I \otimes I) \circ (A^\dagger \otimes I) |0\rangle_1 \\ \langle 1|_1 (C \otimes D) \circ (I \otimes X) \circ (I \otimes B) |1\rangle_1 &= \langle 1|_1 (I \otimes X) \circ (A^\dagger \otimes I) |1\rangle_1 \\ \langle +|_2 (C \otimes D) \circ (I \otimes I) \circ (A \otimes I) |+\rangle_2 &= \langle +|_2 (I \otimes I) \circ (I \otimes B^\dagger) |+\rangle_2 \\ \langle -|_2 (C \otimes D) \circ (Z \otimes I) \circ (A \otimes I) |-\rangle_2 &= \langle -|_2 (Z \otimes I) \circ (I \otimes B^\dagger) |-\rangle_2 \end{cases} \\ \Rightarrow \begin{cases} \langle 0| C |0\rangle DB &= \langle 0| A^\dagger |0\rangle I \\ \langle 1| C |1\rangle DXB &= \langle 1| A^\dagger |1\rangle X \\ \langle +| D |+\rangle CA &= \langle +| B^\dagger |+\rangle I \\ \langle -| D |-\rangle CZA &= \langle -| B^\dagger |-\rangle Z \end{cases} \end{aligned}$$

**Case  $\langle 0| A^\dagger |0\rangle \neq 0$  and  $\langle +| B^\dagger |+\rangle \neq 0$ .** It must also be the case that  $\langle 0| C |0\rangle \neq 0$  and  $\langle +| D |+\rangle \neq 0$ . Moreover, by unitarity of  $A^\dagger$  and  $B^\dagger$ , we also have  $\langle 1| A^\dagger |1\rangle \neq 0$  and  $\langle -| B^\dagger |-\rangle \neq 0$ . The first equation implies  $D = e^{i\delta} B^\dagger$  for some  $\delta \in \mathbb{R}$ , which implies that  $\langle +| D |+\rangle = e^{i\delta} \langle +| B^\dagger |+\rangle$  and  $\langle -| D |-\rangle = e^{i\delta} \langle -| B^\dagger |-\rangle$ . Then the third equation implies  $C = e^{-i\delta} A^\dagger$ , which implies  $\langle 1| C |1\rangle = e^{-i\delta} \langle 1| A^\dagger |1\rangle$ . Hence the system becomes:

$$\begin{cases} DB = e^{i\delta} I \\ DXB = e^{i\delta} X \\ CA = e^{-i\delta} I \\ CZA = e^{-i\delta} Z \end{cases} \Rightarrow \begin{cases} CA = CZA \\ DB = DXBX \end{cases}$$

The first equation implies that there exist  $\varphi, \alpha \in \mathbb{R}$  such that  $A = e^{i\alpha} P(\varphi)$  (because  $A = ZAZ$ ), which implies that  $C = e^{i(-\delta-\alpha)} P(-\varphi)$ . Similarly, the second equation implies that there exist  $\theta, \beta \in \mathbb{R}$  such that  $B = e^{i\beta} R_X(\theta)$  (because  $B = XBX$ ), which implies that  $D = e^{i(\delta-\beta)} R_X(-\theta)$ . And we are done by taking  $k = l = 0$  and  $\gamma := -\delta - \alpha$  which leads to  $\delta - \beta = -\alpha - \beta - \gamma$ .

**Case  $\langle 0| A^\dagger |0\rangle = 0$  and  $\langle +| B^\dagger |+\rangle \neq 0$ .** It must also be the case that  $\langle 0| C |0\rangle = 0$  and  $\langle +| D |+\rangle \neq 0$ . Lemma 31 implies that there exist  $\varphi, \varphi', \alpha, \gamma \in \mathbb{R}$  such that  $A = e^{i\alpha} XP(\varphi)$

and  $C = e^{i\gamma}P(\varphi')X$ . Moreover, the third equation implies  $CA = e^{i\delta}I$  for some  $\delta \in \mathbb{R}$ , thus  $e^{i(\alpha+\gamma)}P(\varphi')XXP(\varphi) = e^{i\delta}I$ , which implies that  $\varphi' = -\varphi \pmod{2\pi}$  (Lemma 32). Then we can use the following derivation to get a new condition satisfied by  $B$  and  $D$ .

$$\left[ \begin{array}{c} \text{---} \boxed{P(\varphi)} \text{---} \boxed{X} \text{---} \bullet \text{---} \boxed{X} \text{---} \boxed{P(-\varphi)} \text{---} \\ \text{---} \boxed{B} \oplus \boxed{D} \text{---} \end{array} \right] \stackrel{(26)}{=} \left[ \begin{array}{c} \text{---} \boxed{P(\varphi)} \text{---} \bullet \text{---} \boxed{P(-\varphi)} \text{---} \\ \text{---} \boxed{B} \oplus \boxed{X} \oplus \boxed{D} \text{---} \end{array} \right] \stackrel{(23)(18)(D)}{=} \left[ \begin{array}{c} \text{---} \bullet \text{---} \\ \text{---} \boxed{B} \oplus \boxed{X} \oplus \boxed{D} \text{---} \end{array} \right]$$

We get  $e^{i(\alpha+\gamma)}(I \otimes DX) \circ \text{CNOT} \circ (I \otimes B) = \text{CNOT}$  from which we obtain two new equations:

$$\begin{aligned} & e^{i(\alpha+\gamma)}(I \otimes DX) \circ \text{CNOT} \circ (I \otimes B) = \text{CNOT} \\ \Rightarrow & \begin{cases} e^{i(\alpha+\gamma)} \langle 0|_1 (I \otimes DX) \circ \text{CNOT} \circ (I \otimes B) |0\rangle_1 = \langle 0|_1 \text{CNOT} |0\rangle_1 \\ e^{i(\alpha+\gamma)} \langle 1|_1 (I \otimes DX) \circ \text{CNOT} \circ (I \otimes B) |1\rangle_1 = \langle 1|_1 \text{CNOT} |1\rangle_1 \end{cases} \\ \stackrel{\text{Claim } 30}{\Rightarrow} & \begin{cases} e^{i(\alpha+\gamma)} \langle 0|_1 (I \otimes DX) \circ (I \otimes I) \circ (I \otimes B) |0\rangle_1 = \langle 0|_1 (I \otimes I) |0\rangle_1 \\ e^{i(\alpha+\gamma)} \langle 1|_1 (I \otimes DX) \circ (I \otimes X) \circ (I \otimes B) |1\rangle_1 = \langle 1|_1 (I \otimes X) |1\rangle_1 \end{cases} \\ \Rightarrow & \begin{cases} e^{i(\alpha+\gamma)} DXB = I \\ e^{i(\alpha+\gamma)} DXXB = X \end{cases} \end{aligned}$$

This implies that  $DXB = DBX$ , thus there exist  $\theta, \beta \in \mathbb{R}$  such that  $B = e^{i\beta}R_X(\theta)$  (because  $B = XBX$ ). The first equation implies  $D = e^{i(-\alpha-\beta-\gamma)}R_X(-\theta)X$ , and we are done by taking  $k = 1$  and  $l = 0$ .

**Case  $\langle 0|A^\dagger|0\rangle \neq 0$  and  $\langle +|B^\dagger|+\rangle = 0$ .** It must also be the case that  $\langle 0|C|0\rangle \neq 0$  and  $\langle +|D|+\rangle = 0$ . Lemma 31 implies that there exist  $\theta, \theta', \beta, \sigma \in \mathbb{R}$  such that  $B = e^{i\beta}ZR_X(\theta)$  and  $D = e^{i\sigma}R_X(\theta')Z$ . Moreover, the first equation implies  $DB = e^{i\delta}I$  for some  $\delta \in \mathbb{R}$ , thus  $e^{i(\beta+\sigma)}R_X(\theta')ZZR_X(\theta) = e^{i\delta}I$ , which implies that  $\theta' = -\theta \pmod{2\pi}$  (Lemma 32). Then we can use the following derivation to get a new condition satisfied by  $A$  and  $C$ .

$$\left[ \begin{array}{c} \text{---} \boxed{A} \text{---} \bullet \text{---} \boxed{C} \text{---} \\ \text{---} \boxed{R_X(\theta)} \text{---} \boxed{Z} \oplus \boxed{Z} \text{---} \boxed{R_X(-\theta)} \text{---} \end{array} \right] \stackrel{(27)}{=} \left[ \begin{array}{c} \text{---} \boxed{A} \text{---} \bullet \text{---} \boxed{Z} \text{---} \boxed{C} \text{---} \\ \text{---} \boxed{R_X(\theta)} \oplus \boxed{R_X(-\theta)} \text{---} \end{array} \right] \stackrel{(24)(19)(16)}{=} \left[ \begin{array}{c} \text{---} \boxed{A} \text{---} \bullet \text{---} \boxed{Z} \text{---} \boxed{C} \text{---} \\ \text{---} \oplus \text{---} \end{array} \right]$$

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

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

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 taking  $k = 0$ ,  $l = 1$  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 31 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  $\varphi, \varphi', \theta, \theta'$ .

$$\left[ \begin{array}{c} \text{---} \boxed{P(\varphi)} \text{---} \boxed{X} \text{---} \bullet \text{---} \boxed{X} \text{---} \boxed{P(\varphi')} \text{---} \\ \text{---} \boxed{R_X(\theta)} \text{---} \boxed{Z} \oplus \boxed{Z} \text{---} \boxed{R_X(\theta')} \text{---} \end{array} \right] \stackrel{(26)(27)}{=} \left[ \begin{array}{c} \text{---} \boxed{P(\varphi)} \text{---} \bullet \text{---} \boxed{Z} \text{---} \boxed{P(\varphi')} \text{---} \\ \text{---} \boxed{R_X(\theta)} \oplus \boxed{X} \text{---} \boxed{R_X(\theta')} \text{---} \end{array} \right]$$

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

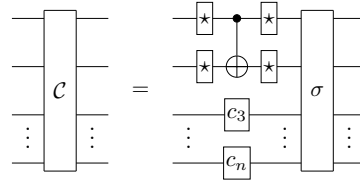
$$\begin{aligned}
& e^{i(\alpha+\beta+\gamma+\delta)}(P(\varphi')Z \otimes R_X(\theta')X) \circ \text{CNOT} \circ (P(\varphi) \otimes R_X(\theta)) = \text{CNOT} \\
\Rightarrow & \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} \langle 0|_1 (P(\varphi')Z \otimes R_X(\theta')X) \text{CNOT}(P(\varphi) \otimes R_X(\theta)) |0\rangle_1 = \langle 0|_1 \text{CNOT} |0\rangle_1 \\ e^{i(\alpha+\beta+\gamma+\delta)} \langle +|_2 (P(\varphi')Z \otimes R_X(\theta')X) \text{CNOT}(P(\varphi) \otimes R_X(\theta)) |+\rangle_2 = \langle +|_2 \text{CNOT} |+\rangle_2 \end{cases} \\
\Rightarrow & \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} \langle 0|_1 (P(\varphi')Z \otimes R_X(\theta')X)(I \otimes I)(P(\varphi) \otimes R_X(\theta)) |0\rangle_1 = \langle 0|_1 (I \otimes I) |0\rangle_1 \\ e^{i(\alpha+\beta+\gamma+\delta)} \langle +|_2 (P(\varphi')Z \otimes R_X(\theta')X)(I \otimes I)(P(\varphi) \otimes R_X(\theta)) |+\rangle_2 = \langle +|_2 (I \otimes I) |+\rangle_2 \end{cases} \\
\Rightarrow & \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} R_X(\theta')X R_X(\theta) = I \\ e^{i(\alpha+\beta+\gamma+\delta)} e^{-i(\theta+\theta')/2} P(\varphi')Z P(\varphi) = I \end{cases} \\
\Rightarrow & \begin{cases} R_X(\theta') = e^{-i(\alpha+\beta+\gamma+\delta)} R_X(-\theta)X \\ P(\varphi') = e^{-i(\alpha+\beta+\gamma+\delta)} e^{i(\theta+\theta')/2} P(-\varphi)Z \end{cases} \\
\Rightarrow & \begin{cases} R_X(\theta') = e^{-i(\alpha+\beta+\gamma+\delta)} e^{i\pi/2} R_X(\pi - \theta) \\ P(\varphi') = e^{-i(\alpha+\beta+\gamma+\delta)} e^{i(\theta+\theta')/2} P(\pi - \varphi) \end{cases} \\
\stackrel{\text{Lemma 32}}{\Rightarrow} & \begin{cases} \theta' = \pi - \theta \pmod{2\pi} \\ \varphi' = \pi - \varphi \pmod{2\pi} \end{cases}
\end{aligned}$$

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

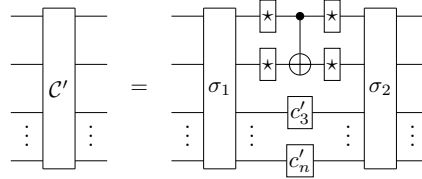
**Proof of Lemma 7 (1-CNot completeness).** Let  $\mathcal{C}, \mathcal{C}'$  be two 1-CNot **QC**-circuits, i.e. circuits containing at most one  $\bigoplus$  gate each, such that  $\llbracket \mathcal{C} \rrbracket = \llbracket \mathcal{C}' \rrbracket$ .

First notice that if both  $\mathcal{C}, \mathcal{C}'$  contains no CNot, then, according to Lemma 29 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:

$$\left[ \begin{array}{c} \bullet \\ \oplus \\ \vdots \end{array} \right] = \left[ \begin{array}{c} \sigma_1 \quad \star \quad \bullet \quad \star \quad \sigma_3 \\ \vdots \quad \vdots \quad c''_3 \quad \vdots \quad \vdots \\ \vdots \quad \vdots \quad c''_n \quad \vdots \quad \vdots \end{array} \right]$$

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  $\llbracket c''_i \rrbracket = \llbracket - \rrbracket$ . We then have:

$$\left[ \begin{array}{c} \bullet \\ \oplus \\ \vdots \end{array} \right] = \left[ \begin{array}{c} \sigma'_1 \quad \star \quad \bullet \quad \star \quad \sigma'_3 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \end{array} \right]$$

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  $\mathcal{C} = \bowtie \circ \bar{\mathcal{C}}'$ . Thus  $\llbracket \mathcal{C} \rrbracket = \llbracket \mathcal{C}' \rrbracket$  is then equivalent to  $\llbracket \bowtie \rrbracket = \llbracket \mathcal{C}' \circ \bar{\mathcal{C}}'^\dagger \rrbracket$ . We hence have a circuit  $\mathcal{C}' \circ \bar{\mathcal{C}}'^\dagger$  that implements  $\bowtie$ , using at most two CNOTs. This contradicts Theorem 6 of [46] 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 equivalent (Proposition 6) 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 (21) we can assume:

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

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

First, by the simplification principle (Proposition 6), we reduce it to showing the following equation for any semantically correct 1-qubit circuits  $\boxed{A}$ ,  $\boxed{B}$ ,  $\boxed{C}$ ,  $\boxed{D}$ .

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

Lemma 33 and Lemma 29 together with Equations (A) and (B) implies that this is always the case that this equation is equivalent (Proposition 6) to one of the following equations:

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

We conclude the proof by observing that we can derive all those equations for any  $\varphi, \theta \in \mathbb{R}$  using Equations (27),(26),(23),(24),(18),(19),(D), and (16).  $\blacktriangleleft$



## C.2 Proof of Equation (8)

► **Lemma 34.** Equation (51) can be derived in QC.

$$\boxed{H} = \left(\frac{\pi}{4}\right) \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \quad (51)$$

**Proof.**

$$\begin{aligned} \boxed{H} &\stackrel{(D)(18)(16)(19)}{=} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{H} \\ &\stackrel{(I)}{=} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{H} \boxed{H} \\ &\stackrel{(C)}{=} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \\ &\stackrel{(1)}{=} \left(\frac{\pi}{4}\right) \boxed{P(-\frac{\pi}{2})} \boxed{H} \boxed{P(-\frac{\pi}{2})} \boxed{H} \boxed{P(-\frac{\pi}{2})} \\ &\stackrel{(I)}{=} \left(\frac{\pi}{4}\right) \boxed{P(-\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \\ &\stackrel{(18)(D)}{=} \left(\frac{\pi}{4}\right) \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \end{aligned}$$

◀

► **Lemma 35.** For any 1-qubit QC-circuit  $\boxed{C}$ , there exists  $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \beta_0, \beta_1, \beta_2, \beta_3 \in \mathbb{R}$  such that  $\text{QC} \vdash \boxed{C} = \left(\alpha_0\right) \boxed{R_X(\alpha_1)} \boxed{P(\alpha_2)} \boxed{R_X(\alpha_3)}$  and  $\text{QC} \vdash \boxed{C} = \left(\beta_0\right) \boxed{P(\beta_1)} \boxed{R_X(\beta_2)} \boxed{P(\beta_3)}$ .

**Proof.** Whatever  $\boxed{C}$  is, we can always apply Equations (I), (J), (35), (A) and (B). ◀

**Proof of Equation (8).** First, we do some steps on the LHS and RHS circuits.

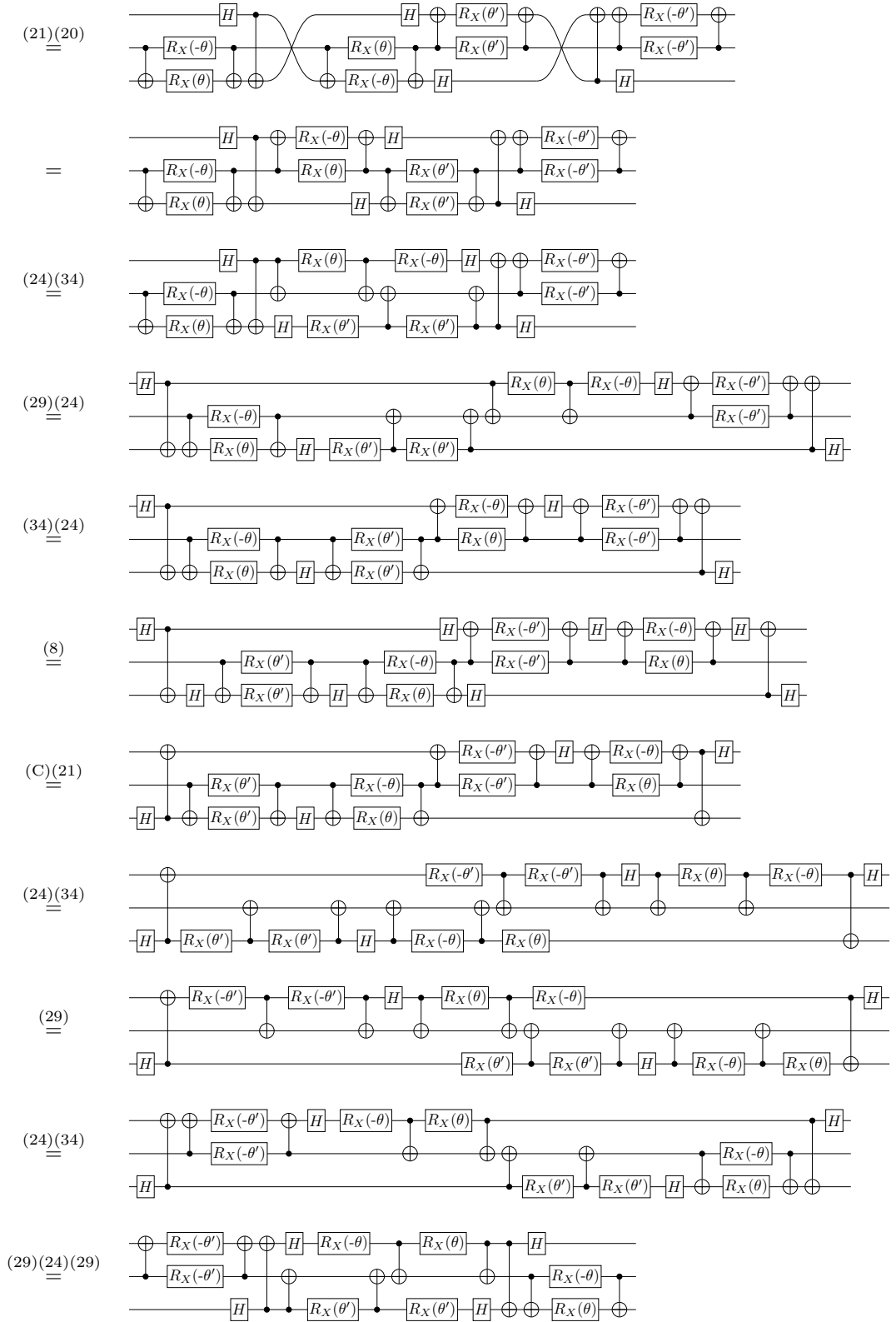
$$\begin{aligned} &\begin{array}{c} \text{---} \boxed{R_X(-\theta)} \text{---} \text{---} \boxed{R_X(\theta')} \text{---} \\ \oplus \boxed{R_X(\theta)} \oplus \boxed{H} \oplus \boxed{R_X(\theta')} \oplus \boxed{H} \end{array} \stackrel{(51)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \boxed{R_X(-\theta)} \text{---} \text{---} \boxed{R_X(\theta')} \text{---} \\ \oplus \boxed{R_X(\theta)} \oplus \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \oplus \boxed{R_X(\theta')} \oplus \boxed{H} \end{array} \\ &\stackrel{(24)(19)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \boxed{R_X(-\theta)} \text{---} \text{---} \boxed{R_X(\theta')} \text{---} \\ \oplus \boxed{R_X(\theta + \frac{\pi}{2})} \oplus \boxed{P(\frac{\pi}{2})} \oplus \boxed{R_X(\theta' + \frac{\pi}{2})} \oplus \boxed{H} \end{array} \\ &\stackrel{(34)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \oplus \text{---} \oplus \text{---} \oplus \text{---} \oplus \text{---} \\ \oplus \boxed{R_X(\theta + \frac{\pi}{2})} \oplus \boxed{R_X(-\theta)} \oplus \boxed{P(\frac{\pi}{2})} \oplus \boxed{R_X(\theta')} \oplus \boxed{R_X(\theta' + \frac{\pi}{2})} \oplus \boxed{H} \end{array} \\ &\stackrel{(G)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \oplus \text{---} \oplus \text{---} \\ \oplus \boxed{R_X(\theta + \frac{\pi}{2})} \oplus \boxed{R_X(-\theta)} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\theta')} \oplus \boxed{R_X(\theta' + \frac{\pi}{2})} \oplus \boxed{H} \end{array} \\ &\begin{array}{c} \text{---} \boxed{R_X(\theta')} \text{---} \text{---} \boxed{R_X(-\theta)} \text{---} \\ \boxed{H} \oplus \boxed{R_X(\theta')} \oplus \boxed{H} \oplus \boxed{R_X(\theta)} \oplus \end{array} \stackrel{(51)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \boxed{R_X(\theta')} \text{---} \text{---} \boxed{R_X(-\theta)} \text{---} \\ \oplus \boxed{H} \oplus \boxed{R_X(\theta')} \oplus \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \oplus \boxed{R_X(\theta)} \oplus \end{array} \\ &\stackrel{(24)(19)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \boxed{R_X(\theta')} \text{---} \text{---} \boxed{R_X(-\theta)} \text{---} \\ \oplus \boxed{H} \oplus \boxed{R_X(\theta' + \frac{\pi}{2})} \oplus \boxed{P(\frac{\pi}{2})} \oplus \boxed{R_X(\theta + \frac{\pi}{2})} \end{array} \\ &\stackrel{(34)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \oplus \text{---} \oplus \text{---} \oplus \text{---} \\ \oplus \boxed{H} \oplus \boxed{R_X(\theta' + \frac{\pi}{2})} \oplus \boxed{R_X(\theta')} \oplus \boxed{P(\frac{\pi}{2})} \oplus \boxed{R_X(-\theta)} \oplus \boxed{R_X(\theta + \frac{\pi}{2})} \end{array} \\ &\stackrel{(G)}{=} \begin{array}{c} \left(\frac{\pi}{4}\right) \text{---} \oplus \text{---} \oplus \text{---} \\ \oplus \boxed{H} \oplus \boxed{R_X(\theta' + \frac{\pi}{2})} \oplus \boxed{R_X(\theta')} \boxed{P(\frac{\pi}{2})} \boxed{R_X(-\theta)} \oplus \boxed{R_X(\theta + \frac{\pi}{2})} \end{array} \end{aligned}$$

Then we can use the simplification principle (Proposition 6) to turn Equation (8) into the following equivalent equations for some  $\alpha_i, \beta_i, \gamma_i, \delta_i, \nu_i \in \mathbb{R}$ . The last equation is over 1-CNot circuits, which together with Lemma 7 conclude the proof.

$$\begin{aligned}
& \begin{array}{c} \oplus \quad \oplus \\ \hline \boxed{R_X(\alpha_1)} \bullet \boxed{R_X(\alpha_2)} \boxed{P(\alpha_3)} \boxed{R_X(\alpha_4)} \bullet \boxed{R_X(\alpha_5)} \boxed{H} \end{array} = \begin{array}{c} \oplus \quad \oplus \\ \hline \boxed{H} \boxed{R_X(\beta_1)} \bullet \boxed{R_X(\beta_2)} \boxed{P(\beta_3)} \boxed{R_X(\beta_4)} \bullet \boxed{R_X(\beta_5)} \end{array} \\
& \stackrel{(J)}{\iff} \begin{array}{c} \oplus \quad \oplus \\ \hline \gamma_0 \boxed{R_X(\alpha_1)} \bullet \boxed{P(\gamma_1)} \boxed{R_X(\gamma_2)} \boxed{P(\gamma_3)} \bullet \boxed{R_X(\alpha_5)} \boxed{H} \end{array} = \begin{array}{c} \oplus \quad \oplus \\ \hline \delta_0 \boxed{H} \boxed{R_X(\beta_1)} \bullet \boxed{P(\delta_1)} \boxed{R_X(\delta_2)} \boxed{P(\delta_3)} \bullet \boxed{R_X(\beta_5)} \end{array} \\
& \stackrel{(23)}{\iff} \begin{array}{c} \oplus \quad \oplus \\ \hline \gamma_0 \boxed{R_X(\alpha_1)} \boxed{P(\gamma_1)} \bullet \boxed{R_X(\gamma_2)} \bullet \boxed{P(\gamma_3)} \boxed{R_X(\alpha_5)} \boxed{H} \end{array} = \begin{array}{c} \oplus \quad \oplus \\ \hline \delta_0 \boxed{H} \boxed{R_X(\beta_1)} \boxed{P(\delta_1)} \bullet \boxed{R_X(\delta_2)} \bullet \boxed{P(\delta_3)} \boxed{R_X(\beta_5)} \end{array} \\
& \iff \begin{array}{c} \oplus \quad \oplus \\ \hline \gamma_0 \boxed{R_X(\alpha_1)} \boxed{P(\gamma_1)} \bullet \boxed{R_X(\gamma_2)} \bullet \boxed{P(\gamma_3)} \boxed{R_X(\alpha_5)} \boxed{H} \boxed{R_X(-\beta_5)} \boxed{P(-\delta_3)} \end{array} = \begin{array}{c} \oplus \quad \oplus \\ \hline \delta_0 \boxed{H} \boxed{R_X(\beta_1)} \boxed{P(\delta_1)} \bullet \boxed{R_X(\delta_2)} \bullet \end{array} \\
& \stackrel{\text{Lemma 35}}{\iff} \begin{array}{c} \oplus \quad \oplus \\ \hline \gamma_0 + \nu_0 \boxed{R_X(\alpha_1)} \boxed{P(\gamma_1)} \bullet \boxed{R_X(\gamma_2)} \bullet \boxed{R_X(\nu_1)} \boxed{P(\nu_2)} \boxed{R_X(\nu_3)} \end{array} = \begin{array}{c} \oplus \quad \oplus \\ \hline \delta_0 \boxed{H} \boxed{R_X(\beta_1)} \boxed{P(\delta_1)} \bullet \boxed{R_X(\delta_2)} \bullet \end{array} \\
& \stackrel{(34)(24)}{\iff} \begin{array}{c} \oplus \quad \oplus \\ \hline \gamma_0 + \nu_0 \boxed{R_X(\alpha_1)} \boxed{P(\gamma_1)} \boxed{R_X(\nu_1)} \bullet \boxed{R_X(\gamma_2)} \bullet \boxed{P(\nu_2)} \end{array} = \begin{array}{c} \oplus \quad \oplus \\ \hline \delta_0 \boxed{H} \boxed{R_X(\beta_1)} \boxed{P(\delta_1)} \boxed{R_X(-\nu_3)} \bullet \boxed{R_X(\delta_2)} \bullet \end{array} \\
& \iff \begin{array}{c} \oplus \quad \oplus \quad \oplus \\ \hline \gamma_0 + \nu_0 \boxed{R_X(\alpha_1)} \boxed{P(\gamma_1)} \boxed{R_X(\nu_1)} \bullet \boxed{R_X(\gamma_2)} \bullet \boxed{P(\nu_2)} \bullet \end{array} = \begin{array}{c} \oplus \\ \hline \delta_0 \boxed{H} \boxed{R_X(\beta_1)} \boxed{P(\delta_1)} \boxed{R_X(-\nu_3)} \bullet \boxed{R_X(\delta_2)} \bullet \end{array} \\
& \stackrel{(G)}{\iff} \begin{array}{c} \oplus \\ \hline \gamma_0 + \nu_0 \boxed{R_X(\alpha_1)} \boxed{P(\gamma_1)} \boxed{R_X(\nu_1)} \bullet \boxed{R_X(\gamma_2)} \boxed{P(\nu_2)} \end{array} = \begin{array}{c} \oplus \\ \hline \delta_0 \boxed{H} \boxed{R_X(\beta_1)} \boxed{P(\delta_1)} \boxed{R_X(-\nu_3)} \bullet \boxed{R_X(\delta_2)} \bullet \end{array}
\end{aligned}$$

### C.3 Proof of Equation (9)

$$\begin{aligned}
& \begin{array}{c} \boxed{H} \oplus \oplus \boxed{H} \oplus \oplus \boxed{R_X(\theta')} \bullet \boxed{R_X(-\theta')} \oplus \\ \bullet \boxed{R_X(-\theta)} \bullet \boxed{R_X(\theta)} \bullet \boxed{R_X(\theta')} \bullet \boxed{R_X(-\theta')} \bullet \\ \oplus \boxed{R_X(\theta)} \bullet \boxed{R_X(-\theta)} \oplus \oplus \boxed{H} \oplus \oplus \boxed{H} \end{array} \\
& \stackrel{(F)}{=} \begin{array}{c} \boxed{H} \oplus \oplus \boxed{H} \oplus \oplus \boxed{R_X(\theta')} \oplus \oplus \boxed{R_X(-\theta')} \oplus \\ \bullet \boxed{R_X(-\theta)} \bullet \bullet \boxed{R_X(\theta)} \bullet \bullet \boxed{R_X(\theta')} \bullet \bullet \boxed{R_X(-\theta')} \bullet \\ \oplus \boxed{R_X(\theta)} \oplus \oplus \oplus \boxed{R_X(-\theta)} \oplus \oplus \boxed{H} \oplus \oplus \boxed{H} \end{array} \\
& \stackrel{(22)}{=} \begin{array}{c} \boxed{H} \bullet \oplus \oplus \boxed{H} \oplus \oplus \boxed{R_X(\theta')} \oplus \oplus \boxed{R_X(-\theta')} \oplus \\ \bullet \boxed{R_X(-\theta)} \bullet \bullet \boxed{R_X(\theta)} \bullet \bullet \boxed{R_X(\theta')} \bullet \bullet \boxed{R_X(-\theta')} \bullet \\ \oplus \boxed{R_X(\theta)} \oplus \oplus \oplus \boxed{R_X(-\theta)} \oplus \oplus \boxed{H} \bullet \oplus \oplus \boxed{H} \end{array} \\
& \stackrel{(29)(24)}{=} \begin{array}{c} \boxed{H} \bullet \oplus \oplus \boxed{H} \oplus \oplus \boxed{R_X(\theta')} \oplus \oplus \boxed{R_X(-\theta')} \oplus \\ \bullet \boxed{R_X(-\theta)} \bullet \bullet \boxed{R_X(\theta)} \bullet \bullet \boxed{R_X(\theta')} \bullet \bullet \boxed{R_X(-\theta')} \bullet \\ \oplus \boxed{R_X(\theta)} \oplus \oplus \oplus \boxed{R_X(-\theta)} \oplus \oplus \boxed{H} \bullet \oplus \oplus \boxed{H} \end{array}
\end{aligned}$$



$$\begin{aligned}
& \stackrel{(24)(34)}{=} \text{Diagram 1} \\
& = \text{Diagram 2} \\
& \stackrel{(20)(21)}{=} \text{Diagram 3} \\
& \stackrel{(29)(24)}{=} \text{Diagram 4} \\
& \stackrel{(22)}{=} \text{Diagram 5} \\
& \stackrel{(F)}{=} \text{Diagram 6}
\end{aligned}$$

#### 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 36.** *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,

$$\begin{array}{c}
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\circ \quad \circ \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet
\end{array}
=
\begin{array}{c}
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\circ \quad \circ \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet
\end{array}$$

**Proof of Lemma 36.** This is a direct consequence of the results of [10], namely of Lemma 54 together with Propositions 11, 12 and 15. ◀

► **Lemma 37.** *The following equations are consequences of the equations of QC without Equation  $(K^*)$ :*

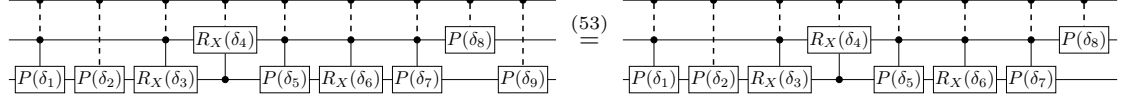
$$\begin{array}{c}
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet
\end{array}
=
\begin{array}{c}
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet
\end{array}
\quad (52)$$

$$\begin{array}{c}
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet
\end{array}
=
\begin{array}{c}
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet
\end{array}
=
\begin{array}{c}
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet \\
\vdots \quad \vdots \\
\bullet \quad \bullet
\end{array}
\quad (53)$$

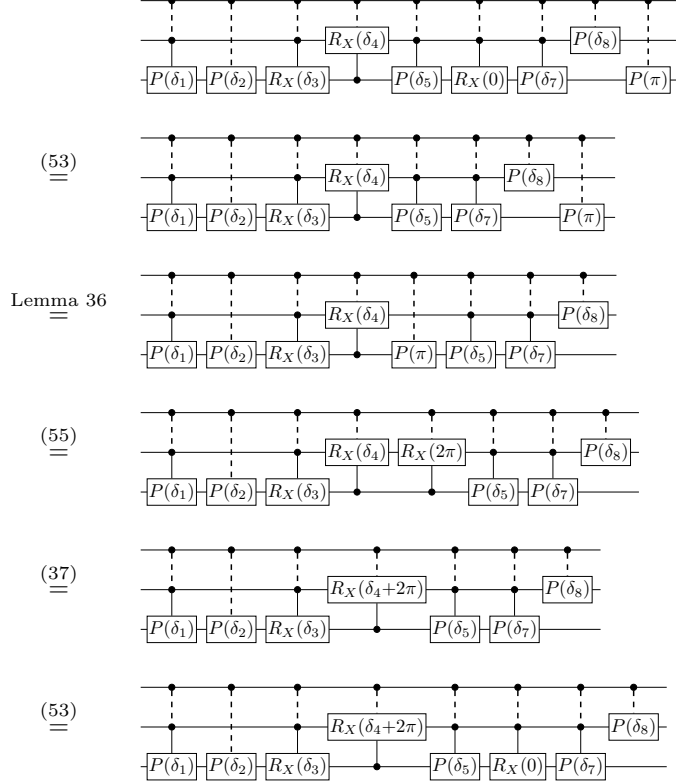


- If  $\sin(\frac{\delta_3}{2})\sin(\frac{\delta_4}{2}) \neq 0$ , this implies that  $e^{i\delta_9}$  is a real number, which, since  $\delta_9 \in [0, 2\pi)$ , implies that  $\delta_9 \in \{0, \pi\}$ .

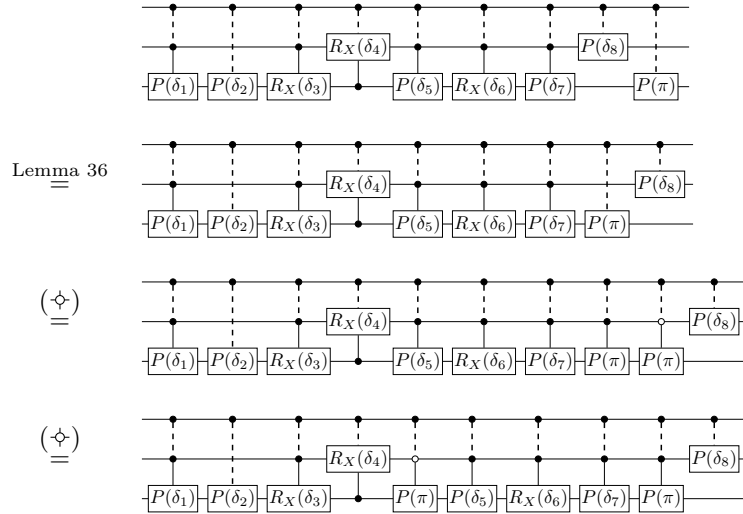
- If  $\delta_9 = 0$ , then

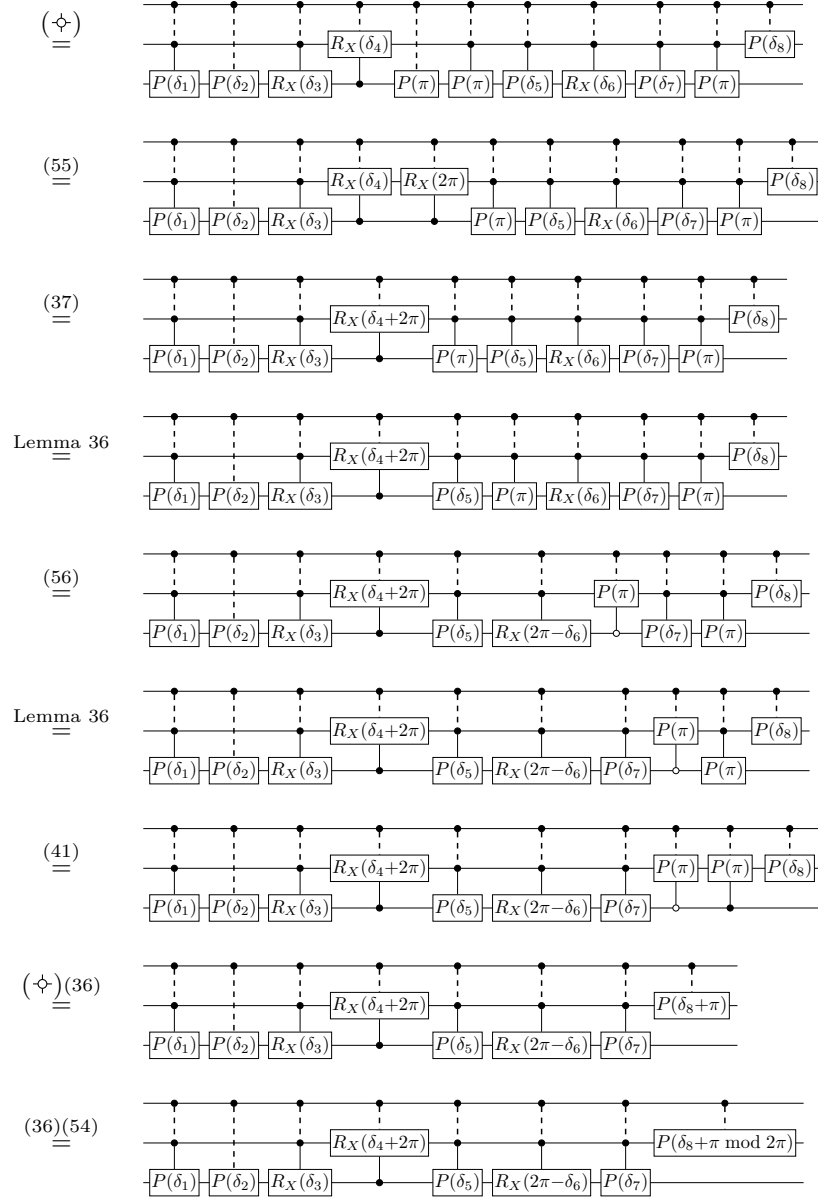


- If  $\delta_9 = \pi$  and  $\delta_6 = 0$ , then



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





- If  $\sin(\frac{\delta_3}{2}) \sin(\frac{\delta_4}{2}) = 0$ , then since  $\delta_3, \delta_4 \in [0, 2\pi)$  and  $\delta_4 = 0 \Rightarrow \delta_3 = 0$ , one necessarily has  $\delta_3 = 0$ . In turn, the conditions of Figure 4 also imply that  $\delta_2 = 0$ . Additionally, this implies that  $\sin(\frac{\gamma_3}{2}) \sin(\frac{\gamma_4}{2}) = 0$  too, that is,  $\sin(\frac{\gamma_3}{2}) = 0$  or  $\sin(\frac{\gamma_4}{2}) = 0$ .
- If  $\sin(\frac{\gamma_3}{2}) = 0$ , then  $\cos(\frac{\gamma_3}{2}) \in \{-1, 1\}$ , and one can remark that

$$\langle 1\dots 110 | \left[ \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \\ \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \\ \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \end{array} \right] | 1\dots 110 \rangle = \cos(\frac{\gamma_3}{2})$$

while, since  $\delta_3 = 0$ ,

$$\langle 1\dots 110 | \left[ \begin{array}{c} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \\ \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \\ \text{---} \text{---} \text{---} \text{---} \text{---} \text{---} \end{array} \right] | 1\dots 110 \rangle = e^{i\delta_8} \cos(\frac{\delta_6}{2}).$$

Hence,  $\cos(\frac{\delta_6}{2})$  has absolute value 1, which, since  $\delta_6 \in [0, 2\pi)$ , implies that  $\delta_6 = 0$ .<sup>10</sup> In turn, the conditions of Figure 4 also imply that  $\delta_5 = 0$ . Thus,

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{(53)}{=} \begin{array}{c} \text{Diagram 2} \end{array}$$

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

$$\begin{array}{c} \text{Diagram 3} \\ \text{Lemma 36,} \\ (52) \\ \text{Diagram 4} \\ (53) \\ \text{Diagram 5} \end{array}$$

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

$$\begin{array}{c} \text{Diagram 6} \\ (36) \\ \text{Diagram 7} \\ \text{Lemma 36,} \\ (52) \\ \text{Diagram 8} \\ (55) \\ \text{Diagram 9} \\ (37) \\ \text{Diagram 10} \\ (53) \\ \text{Diagram 11} \end{array}$$

<sup>10</sup> Moreover,  $e^{i\delta_8}$  is a real number, which, since  $\delta_8 \in [0, 2\pi)$ , implies that  $\delta_8 \in \{0, \pi\}$ . Note however that we do not use this property.



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

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

while, since  $\delta_2 = 0$ ,

- \* 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  $\sin(\frac{\delta_3}{2})\sin(\frac{\delta_4}{2}) \neq 0$ ).
- \* If  $\cos(\frac{\delta_4}{2}) = 0$ , then on the one hand, since  $\delta_4 \in [0, 2\pi)$ , one has  $\delta_4 = \pi$ . In turn, since  $\delta_3 = 0$ , the conditions of Figure 4 imply that  $\delta_1 = 0$ . On the other hand,  $\cos(\frac{\gamma_1}{2}) = 0$  too, so that  $\sin(\frac{\gamma_1}{2}) \in \{-1, 1\}$  and

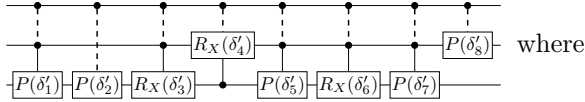
$$\langle 1...101 | \left[ \begin{array}{c} \bullet \quad \bullet \quad \bullet \quad \bullet \\ | \\ \text{---} R_X(\gamma_1) \text{---} \bullet \text{---} R_X(\gamma_4) \text{---} \\ | \\ \bullet \quad \bullet \quad \bullet \quad \bullet \\ | \\ \text{---} P(\gamma_2) \text{---} R_X(\gamma_3) \text{---} \\ | \\ \bullet \quad \bullet \quad \bullet \quad \bullet \end{array} \right] | 1...111 \rangle = \pm i$$

while, since  $\delta_2 = 0$ ,

$$\langle 1 \dots 101 | \left[ \begin{array}{c} \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\ \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \\ \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \\ \boxed{P(\delta_1)} \quad \boxed{P(\delta_2)} \quad \boxed{R_X(\delta_3)} \quad \bullet \quad \boxed{P(\delta_5)} \quad \boxed{R_X(\delta_6)} \quad \boxed{P(\delta_7)} \quad \boxed{P(\delta_9)} \end{array} \right] | 1 \dots 111 \rangle = \pm i e^{i\delta_9}.$$

Hence,  $\delta_9 \in \{0, \pi\}$  and we can also proceed as in the first case.

Thus, given any instance of Equation (K<sub>old</sub><sup>\*</sup>), its right-hand side can be transformed into



- $$\begin{aligned} \blacksquare \quad \delta'_1 &= \delta_1 \\ \blacksquare \quad \delta'_3 &= \delta_3 \\ \blacksquare \quad \delta'_5 &= \delta_5 \\ \blacksquare \quad \delta'_7 &= \delta_7 \\ \blacksquare \quad \delta'_2 &= \begin{cases} \delta_2 & \text{if } \delta_9 \in \{0, \pi\} \\ \delta_9 & \text{if } \delta_9 \in (0, \pi) \\ \delta_9 - \pi & \text{if } \delta_9 \in (\pi, 2\pi) \end{cases} \\ \blacksquare \quad \delta'_4 &= \begin{cases} \delta_4 & \text{if } \delta_9 \in [0, \pi) \\ \delta_4 + 2\pi & \text{if } \delta_9 \in [\pi, 2\pi) \end{cases} \\ \blacksquare \quad \delta'_6 &= \begin{cases} 2\pi - \delta_6 & \text{if } \delta_9 = \pi \text{ and } \delta_6 \neq 0 \\ \delta_6 & \text{else} \end{cases} \\ \blacksquare \quad \delta'_8 &= \begin{cases} \delta_8 + \pi \bmod 2\pi & \text{if } \delta_9 = \pi \text{ and } \delta_6 \neq 0 \\ \delta_8 & \text{else} \end{cases} \end{aligned}$$

These angles satisfy the conditions of Figure 2. Indeed, the only case where we can obtain  $\delta'_3 = 0$  and  $\delta'_2 \neq 0$  in the case distinction above, is the case where  $\sin(\frac{\gamma_3}{2}) = 0$ , in which  $\delta'_6 = \delta_6 = 0$ . For the other conditions of Figure 2, the fact that they are satisfied by the  $\delta'_k$  follows directly from the fact that the  $\delta_j$  satisfy the conditions of Figure 4.

The transformation only uses:

- Equations (36), (37), and (41), which are proved in [10] without using Equation  $(K_{\text{old}}^*)$  and therefore are provable in QC without Equation  $(K^*)$ ,
- Lemma 36 and Equations (52) and (53), which only rely on QC without Equation  $(K^*)$ ,
- Equation (54), which can be proved using Equation  $(K_{\text{old}}^*)$  instead of Equation  $(K^*)$
- and Equations (55) and (56), which are consequences of the equations of QC without Equation  $(K^*)$  together with Equation (54).

Since Equation  $(K_{\text{old}}^*)$  has been proved to be sound in [10] (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 4 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  $\delta'_k$ :

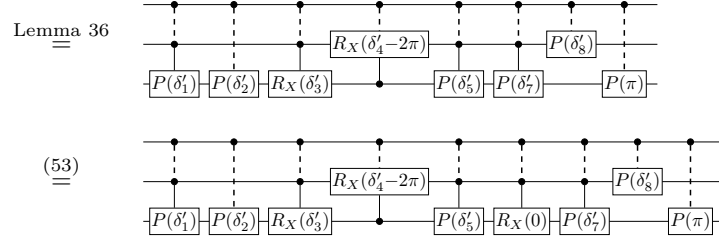
$$\begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \\ \boxed{R_X(\gamma_1)} \quad \quad \quad \boxed{R_X(\gamma_4)} \\ | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \\ \boxed{P(\gamma_2)} \quad \boxed{R_X(\gamma_3)} \end{array} = \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{R_X(\delta'_4)} \quad \quad \quad \boxed{P(\delta'_8)} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \boxed{P(\delta'_5)} \quad \boxed{R_X(\delta'_6)} \quad \boxed{P(\delta'_7)} \end{array} \quad (K^*)$$

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

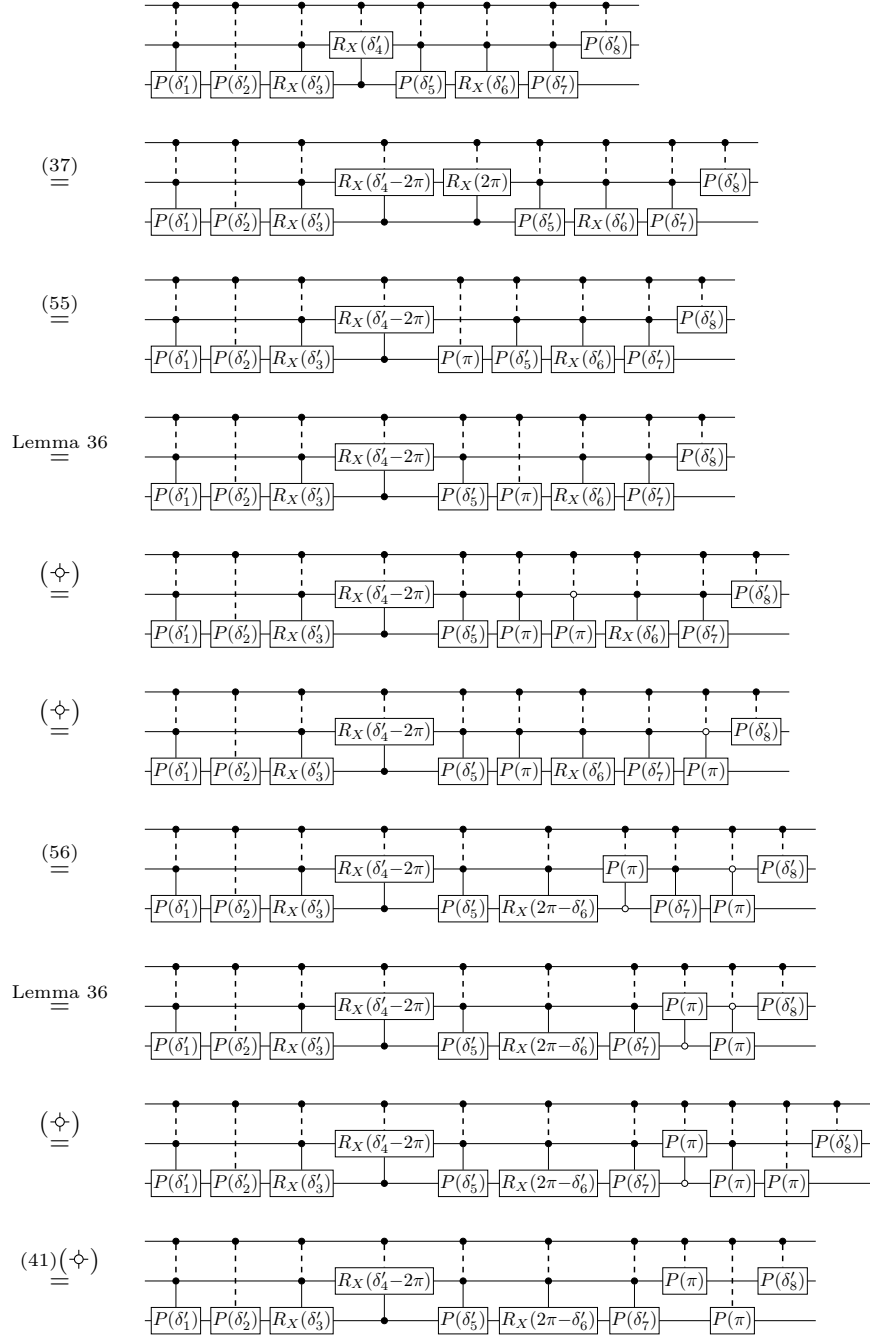
$$\begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{R_X(\delta'_4)} \quad \quad \quad \boxed{P(\delta'_8)} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \boxed{P(\delta'_5)} \quad \boxed{R_X(\delta'_6)} \quad \boxed{P(\delta'_7)} \end{array} \stackrel{(53)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{R_X(\delta'_4)} \quad \quad \quad \boxed{P(\delta'_8)} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \boxed{P(\delta'_5)} \quad \boxed{R_X(\delta'_6)} \quad \boxed{P(\delta'_7)} \quad \boxed{P(0)} \end{array}$$

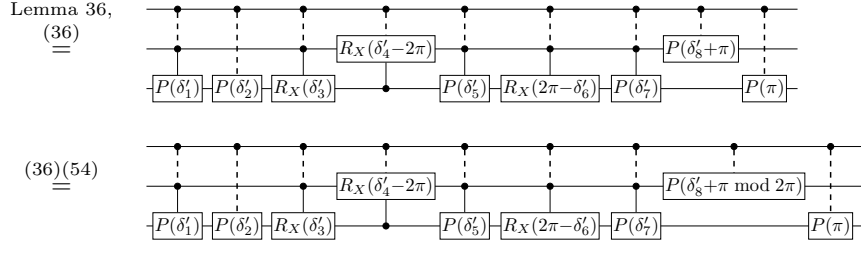
- If  $\delta'_4 \in [2\pi, 4\pi)$ , either  $\delta'_3 \neq 0$  or  $\delta'_2 = 0$ , and  $\delta'_6 = 0$ , then

$$\begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{R_X(\delta'_4)} \quad \quad \quad \boxed{P(\delta'_8)} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \boxed{P(\delta'_5)} \quad \boxed{R_X(0)} \quad \boxed{P(\delta'_7)} \end{array} \stackrel{(53)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{R_X(\delta'_4)} \quad \quad \quad \boxed{P(\delta'_8)} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \boxed{P(\delta'_5)} \quad \boxed{P(\delta'_7)} \end{array} \stackrel{(37)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{R_X(\delta'_4 - 2\pi)} \quad \boxed{R_X(2\pi)} \quad \quad \quad \boxed{P(\delta'_8)} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \quad \quad \boxed{P(\delta'_5)} \quad \boxed{P(\delta'_7)} \end{array} \stackrel{(55)}{=} \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{R_X(\delta'_4 - 2\pi)} \quad \quad \quad \quad \quad \quad \boxed{P(\delta'_8)} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ \boxed{P(\delta'_1)} \quad \boxed{P(\delta'_2)} \quad \boxed{R_X(\delta'_3)} \quad \quad \quad \boxed{P(\pi)} \quad \boxed{P(\delta'_5)} \quad \boxed{P(\delta'_7)} \end{array}$$

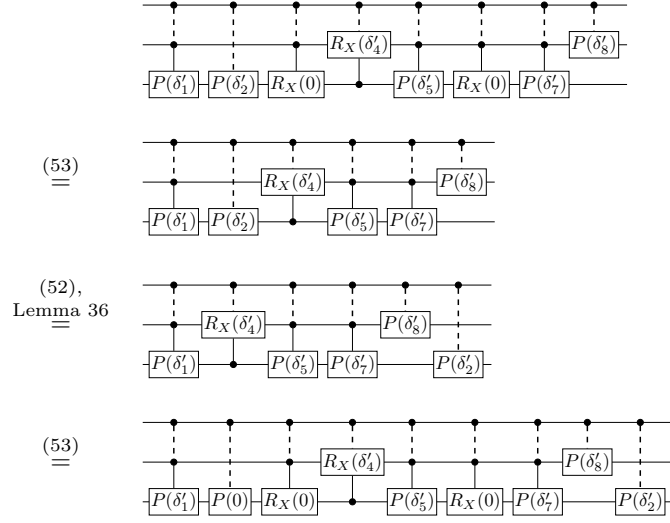


■ If  $\delta'_4 \in [2\pi, 4\pi)$ , either  $\delta'_3 \neq 0$  or  $\delta'_2 = 0$ , and  $\delta'_6 \neq 0$ , then

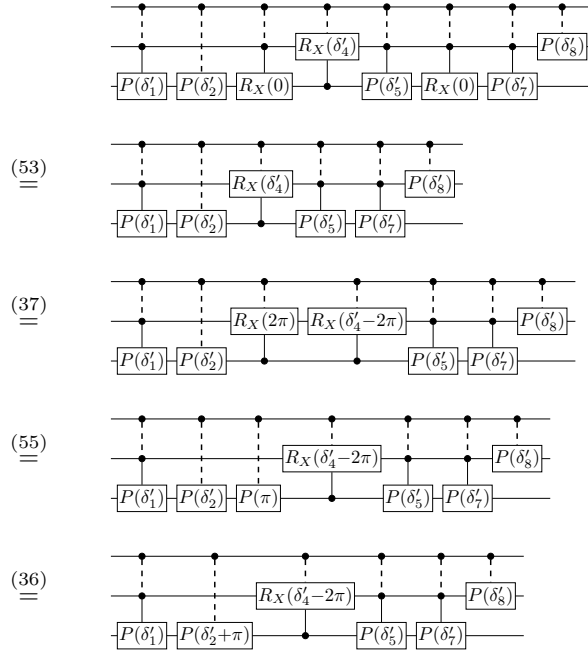


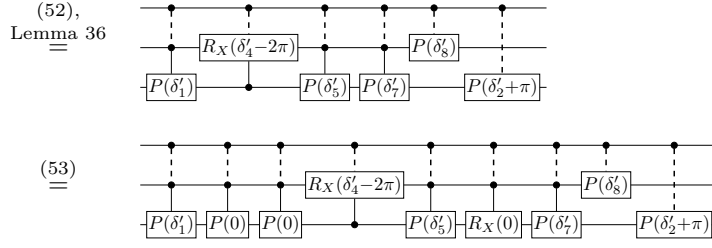


- If  $\delta'_4 \in [0, 2\pi)$  but  $\delta'_3 = 0$  and  $\delta'_2 \neq 0$ , then the conditions of Figure 2 imply that  $\delta'_6 = 0$ , so that

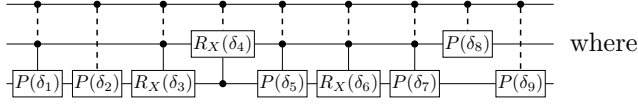


- If  $\delta'_4 \in [2\pi, 4\pi)$ ,  $\delta'_3 = 0$  and  $\delta'_2 \neq 0$ , then the conditions of Figure 2 still imply that  $\delta'_6 = 0$ , so that





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



- $\delta_1 = \delta'_1$
- $\delta_3 = \delta'_3$
- $\delta_5 = \delta'_5$
- $\delta_7 = \delta'_7$
- $\delta_2 = \begin{cases} 0 & \text{if } \delta'_3 = 0 \text{ and } \delta'_2 \neq 0 \\ \delta'_2 & \text{else} \end{cases}$
- $\delta_4 = \begin{cases} \delta'_4 & \text{if } \delta'_4 \in [0, 2\pi) \\ \delta'_4 - 2\pi & \text{if } \delta'_4 \in [2\pi, 4\pi) \end{cases}$
- $\delta_6 = \begin{cases} 2\pi - \delta'_6 & \text{if } \delta'_6 \neq 0 \text{ and } \delta'_4 \in [2\pi, 4\pi) \\ \delta'_6 & \text{else} \end{cases}$
- $\delta_8 = \begin{cases} \delta'_8 + \pi \bmod 2\pi & \text{if } \delta'_6 \neq 0 \text{ and } \delta'_4 \in [2\pi, 4\pi) \\ \delta'_8 & \text{else} \end{cases}$
- $\delta_9 = \begin{cases} \delta'_2 & \text{if } \delta'_3 = 0, \delta'_2 \neq 0 \text{ and } \delta'_4 \in [0, 2\pi) \\ \delta'_2 + \pi & \text{if } \delta'_3 = 0, \delta'_2 \neq 0 \text{ and } \delta'_4 \in [2\pi, 4\pi) \\ 0 & \text{if } (\delta'_3 \neq 0 \text{ or } \delta'_2 = 0) \text{ and } \delta'_4 \in [0, 2\pi) \\ \pi & \text{if } (\delta'_3 \neq 0 \text{ or } \delta'_2 = 0) \text{ and } \delta'_4 \in [2\pi, 4\pi) \end{cases}.$

It is easy to check that these angles  $\delta_j$  satisfy the conditions of Figure 4 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 [10] 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 15.** 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

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

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  $\boxed{H} \rightarrow \boxed{P(\frac{\pi}{2})}\boxed{Rx(\frac{\pi}{2})}\boxed{P(\frac{\pi}{2})}$  and  $\text{CNOT} \rightarrow \begin{array}{cc} \bullet & \oplus \\ | & | \\ \oplus & \bullet \end{array}$ , 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  $\mathbf{QC}_{\text{iso}} \vdash \begin{array}{c} \vdash \\ \vdots \\ \boxed{C} \\ \vdots \end{array} = \begin{array}{c} \vdash \\ \vdots \\ \boxed{\Lambda\tilde{C}_{U'}} \\ \vdots \end{array}$ .

Thus, one can push the initialisation of  $\begin{array}{c} \vdash \\ \vdots \\ \boxed{\Lambda\tilde{C}_{U'}} \\ \vdots \end{array}$  through all the (controlled) gates using

Equations 47, 48 and 45, leading to  $\begin{array}{c} \vdash \\ \vdots \\ \vdots \end{array}$ . ◀

To show Lemma 16, we first introduce useful known decompositions, and recall as well the usual (balanced) CSD for reference:

► **Lemma 40** (Matrix Decompositions [45]).

- **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 16.** This is a small variation on the usual CSD. Let us start with  $U =$

$$\left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & U_{00} & U_{01} \\ \hline 0 & U_{10} & U_{11} \end{array} \right). \text{ Let:}$$

- $A_0 C_0 B_0$  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 then from largest to smallest. We then denote  $C$  the submatrix of  $C_0$  which has only  $< 1$  components. We

$$\text{then have: } U = \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & A_0 & 0 \\ \hline 0 & 0 & A_1 \end{array} \right) \left( \begin{array}{c|c|c} I & 0 & \\ \hline 0 & C & R \\ \hline L & & A_1^\dagger U_{11} B_1^{\dagger\dagger} \end{array} \right) \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & B_0 & 0 \\ \hline 0 & 0 & B'_1 \end{array} \right). \text{ Notice}$$

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

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

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

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

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  $B_1 := \left( \begin{array}{c|c} X_0 & 0 \\ \hline 0 & -I \end{array} \right) B'_1$ .  $\blacktriangleleft$

**Proof of Theorem 17.** 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 15, there exist two  $\mathbf{QC}$ -circuits

$C_{u_1}$  and  $C_{u_2}$  such that  $C_i = \begin{array}{c} \vdots \\ n: \\ \vdots \\ \vdots \\ k: \\ \vdots \end{array} \begin{array}{c} \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array} C_{u_i} \begin{array}{c} \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array}$ . By completeness of  $\mathbf{QC}$ , showing that  $C_1 = C_2$  is

equivalent to showing that  $\begin{array}{c} \vdots \\ n: \\ \vdots \\ \vdots \\ k: \\ \vdots \end{array} \begin{array}{c} \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array} C_U \begin{array}{c} \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array} = \begin{array}{c} \vdots \\ n: \\ \vdots \\ \vdots \\ k: \\ \vdots \end{array} \begin{array}{c} \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \end{array}$  for  $C_U = C_{u_1} C_{u_2}^\dagger$  (Proposition 6).

Let us denote  $U = \llbracket C_U \rrbracket$ . Notice that  $U$  has to be such that  $U \begin{pmatrix} I \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} I \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ , which,

by unitarity, means  $U = \left( \begin{array}{c|c} I & 0 \\ \hline 0 & \star \end{array} \right)$ . Let us now prove that  $\mathbf{QC}_{\text{iso}}$  proves the equality, by reasoning inductively on the number  $n$  of initialised qubits.

Case  $n = 0$ : In that case, there is no initialised qubit, and since  $\llbracket U \rrbracket = I$ , by completeness of  $\mathbf{QC}$ ,  $\mathbf{QC} \vdash U = Id$ .

Case  $n = 1$ : There, we have  $U = \left( \begin{array}{c|c} I & 0 \\ \hline 0 & U' \end{array} \right)$ . Then Lemma 15 gives directly the expected equality.

Case  $n + 1$ :  $U$  is of the form  $U = \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & U_{00} & U_{01} \\ \hline 0 & U_{10} & U_{11} \end{array} \right)$  (with  $U_{00}$  and  $U_{11}$  square). Notice that  $U$

has dimension  $2^{k+n+1}$ . We can hence use the modified CSD to get:

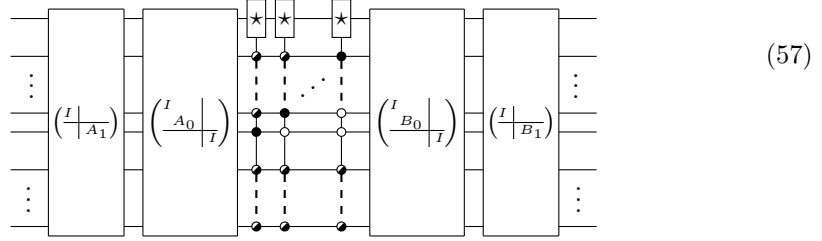
$$U = \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & A_0 & 0 \\ \hline 0 & 0 & A_1 \end{array} \right) \left( \begin{array}{c|c|c|c} I & 0 & 0 & 0 \\ \hline 0 & C & 0 & -S \\ \hline 0 & 0 & I & 0 \\ \hline 0 & S & 0 & C \end{array} \right) \left( \begin{array}{c|c|c} I & 0 & 0 \\ \hline 0 & B_0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

The middle matrix can be seen as a product of:

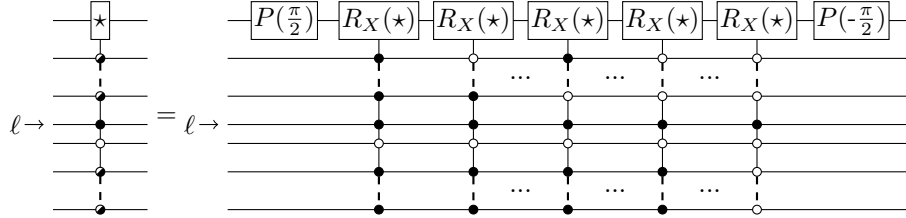
$$R_j := c_j |j\rangle\langle j| + s_j |j + 10\dots 0\rangle\langle j| - s_j |j\rangle\langle j + 10\dots 0| + c_j |j + 10\dots 0\rangle\langle j + 10\dots 0| \\ + \sum_{x \notin \{j, j+10\dots 0\}} |x\rangle\langle x|$$



for  $\overbrace{0\dots 0}^{n+1}\overbrace{1\dots 1}^k < j < \overbrace{10\dots 0}^{n+k}$  in binary. Notice that the first  $R_j$ s might be the identity, if  $A_0$  and  $C$  do not have the same dimensions. Notice also that  $j$  has at least one 1 in its first  $n+1$  bits.  $R_j$  is hence a rotation  $\begin{pmatrix} c_j & -s_j \\ s_j & c_j \end{pmatrix} = P(\frac{\pi}{2})R_X(\theta_j)P(-\frac{\pi}{2})$  on the first qubit, controlled by all the other qubits. Matrix  $U$  can hence be implemented by the following circuit:



where, similarly to [35], 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 (36) 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  $\forall |\varphi\rangle \in \mathbb{C}^{2^n}$ ,  $\left(I \begin{smallmatrix} | \\ A_1 \end{smallmatrix} \right) (|0\rangle \otimes |\varphi\rangle) = |0\rangle \otimes |\varphi\rangle$ , hence using Lemma 15, 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.

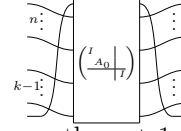
For the second block, notice that:

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

which implies

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

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 15. Finally, it is provable that:

$$\left[ \begin{array}{c} \vdots \\ n+1 \\ \vdots \end{array} \right] \left( \begin{array}{c|c} I & A_1 \end{array} \right) \left( \begin{array}{c|c|c} I & A_0 & I \end{array} \right) \left[ \begin{array}{c} \vdots \\ n+1 \\ \vdots \end{array} \right] \left( \begin{array}{c|c|c} I & B_0 & I \end{array} \right) \left( \begin{array}{c|c} I & B_1 \end{array} \right) \left[ \begin{array}{c} \vdots \\ n+1 \\ \vdots \end{array} \right] = \left[ \begin{array}{c} \vdots \\ n+1 \\ \vdots \end{array} \right]$$

◀

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

### E.1 Proof of Proposition 21

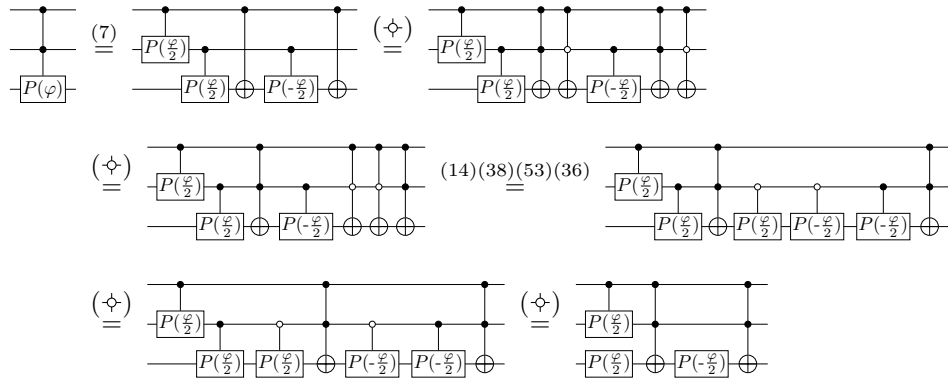
First, we derive the following equations. Equations (58) and (59) are alternative definitions of 2-controlled and 3-controlled phase gates. Equation (60) tells us how we can express a simply controlled gate with Toffoli gates and one 1-qubit gate using one ancilla.

$$\left[ \begin{array}{c} \bullet \\ \bullet \\ \hline P(\varphi) \end{array} \right] = \left[ \begin{array}{c} \bullet \\ \bullet \\ \hline P(\frac{\pi}{2}) \oplus P(-\frac{\pi}{2}) \end{array} \right] \quad (58)$$

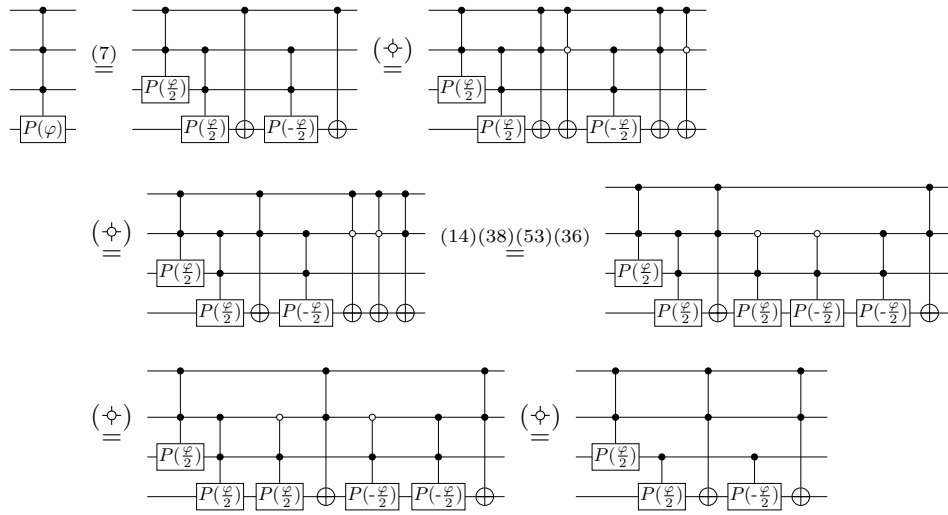
$$\left[ \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \hline P(\varphi) \end{array} \right] = \left[ \begin{array}{c} \bullet \\ \bullet \\ \bullet \\ \hline P(\frac{\pi}{2}) \oplus P(\frac{\pi}{2}) \oplus P(-\frac{\pi}{2}) \end{array} \right] \quad (59)$$

$$\left[ \begin{array}{c} \bullet \\ \hline P(\varphi) \end{array} \right] = \left[ \begin{array}{c} \bullet \\ \hline \oplus P(\varphi) \oplus \end{array} \right] \quad (60)$$

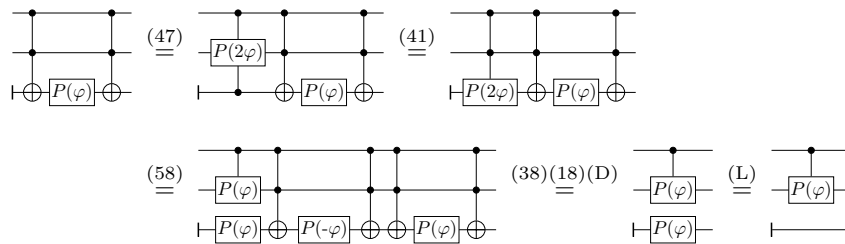
Proof of Equation (58).



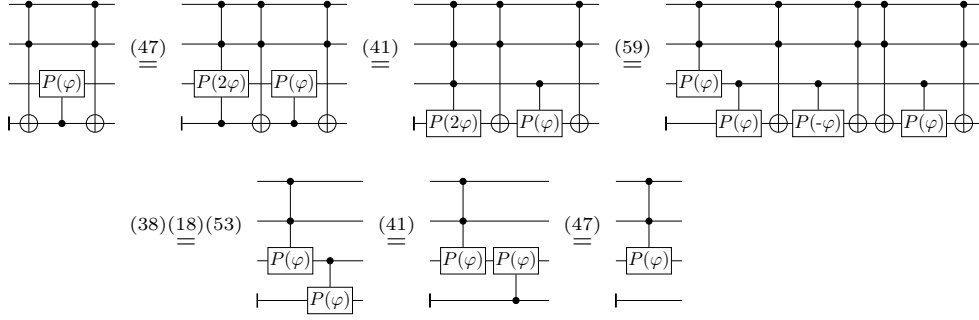
Proof of Equation (59).



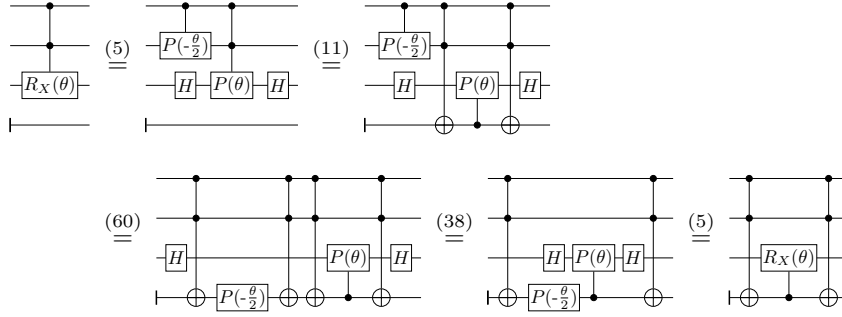
Proof of Equation (60).



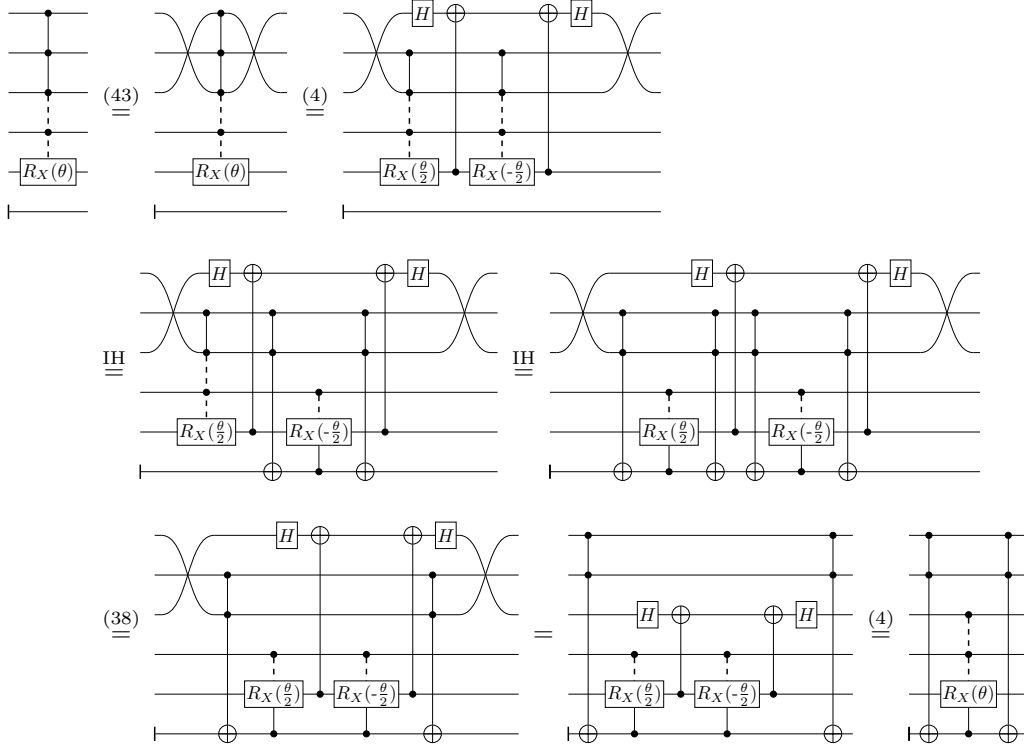
We first prove Equations (11) and (12) by induction on the number of qubits, whose base cases contains  $n = 4$  qubits. The base case for Equations (11) can be derived as follows.



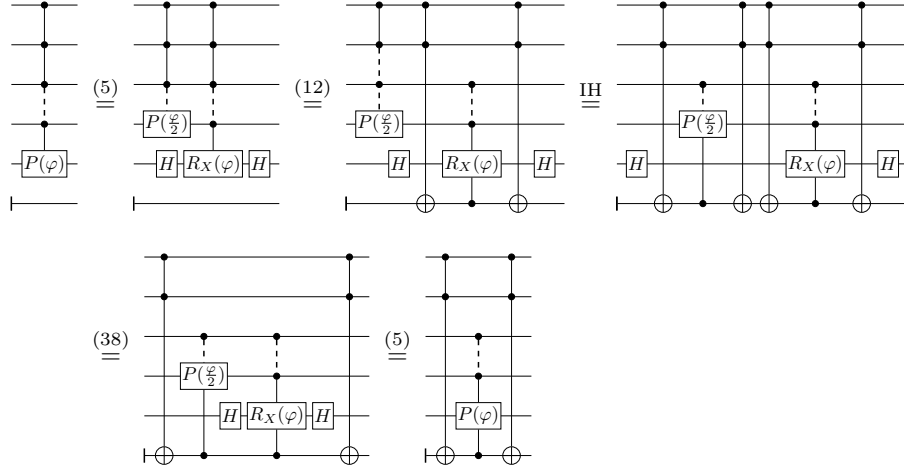
The base case for Equations (11) can be derived as follows.



The induction step for Equation (12) can be derived as follows.



The induction step for Equation (11) can be derived as follows.



## E.2 Proof of Equation ( $K^3$ )

The main idea of the proof of Equation ( $K^3$ ) is to use the *Fredkin gate* (or *controlled-swap gate*), defined by Equation (61).

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \times \\ \times \\ \times \\ \times \end{array} := \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (61)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} R_X(\gamma_1) \\ R_X(\gamma_4) \\ P(\gamma_2) \\ R_X(\gamma_3) \end{array} = \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} R_X(\delta_4) \\ P(\delta_1) \\ P(\delta_2) \\ R_X(\delta_3) \\ P(\delta_5) \\ R_X(\delta_6) \\ P(\delta_7) \\ P(\delta_8) \end{array} \quad (K^3)$$

First, we derive some useful equations.

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} H \\ H \\ H \\ H \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (62)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} H \\ H \\ H \\ H \end{array} = \begin{array}{c} \times \\ \times \\ \times \\ \times \end{array} \quad (63)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (64)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (65)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (66)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (67)$$

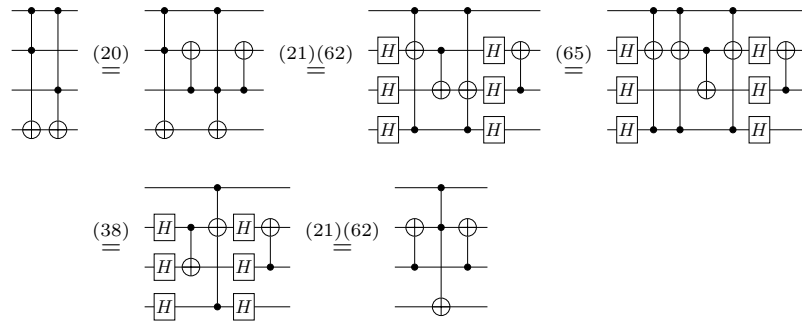
$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (68)$$

$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (69)$$

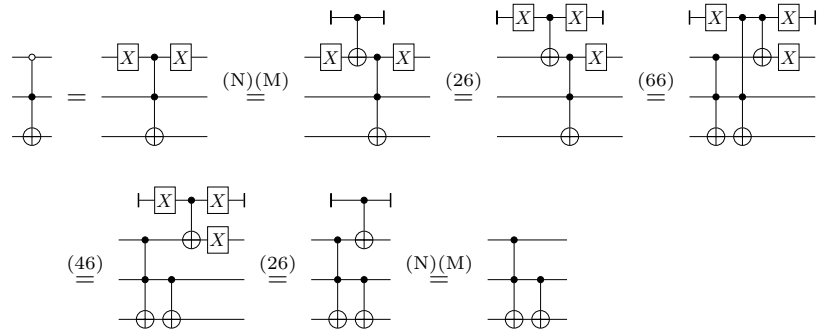
$$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} = \begin{array}{c} \oplus \\ \oplus \\ \oplus \\ \oplus \end{array} \quad (70)$$



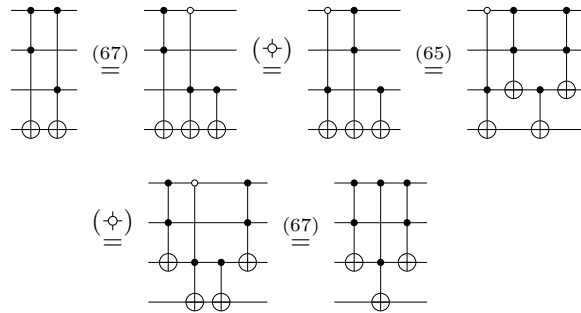
Proof of Equation (66).



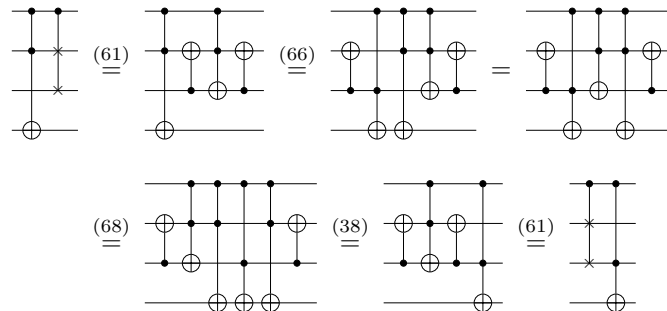
Proof of Equation (67).



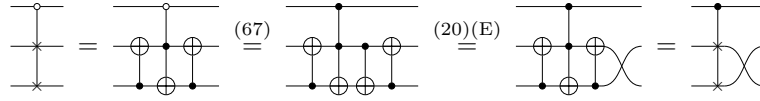
Proof of Equation (68).



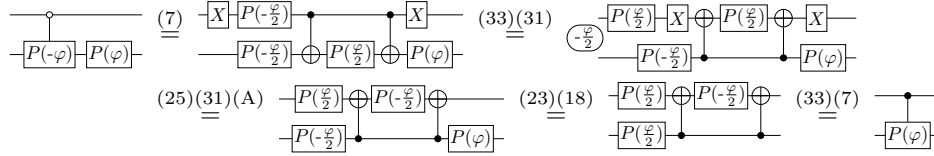
Proof of Equation (69).



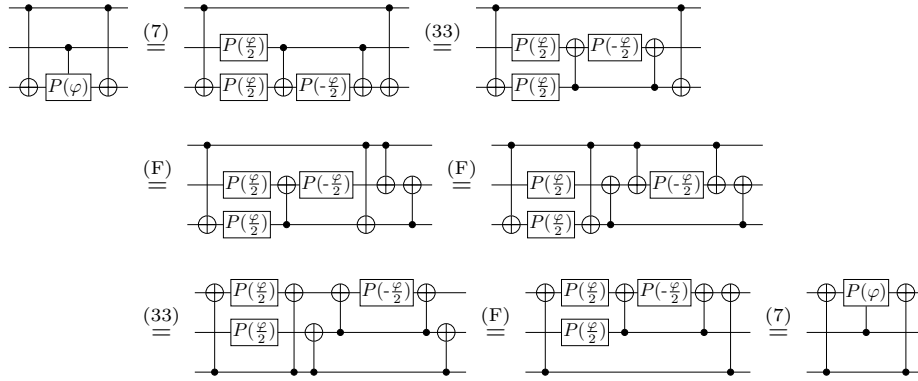
Proof of Equation (70).



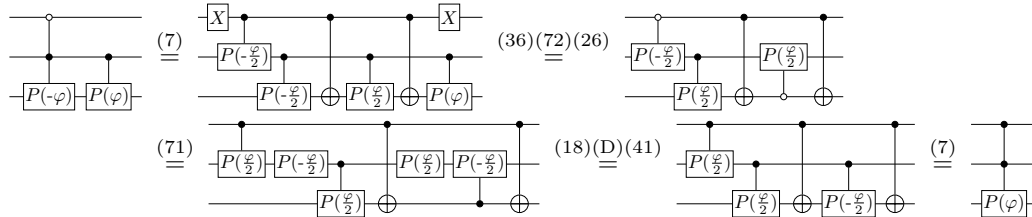
Proof of Equation (71).



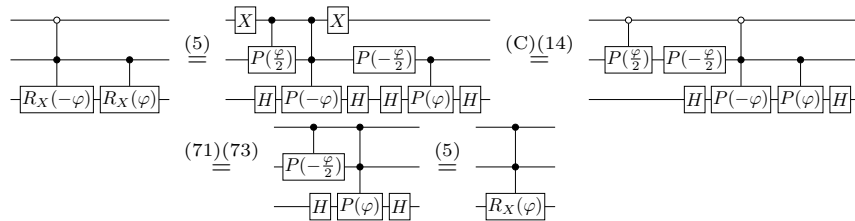
Proof of Equation (72).



Proof of Equation (73).

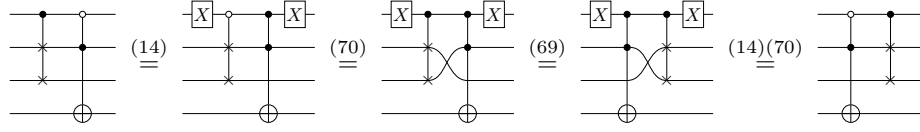


Proof of Equation (74).





**Proof of Equation (75).**

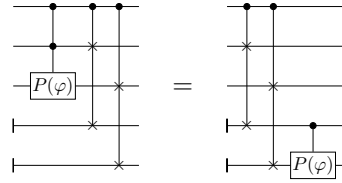


◀

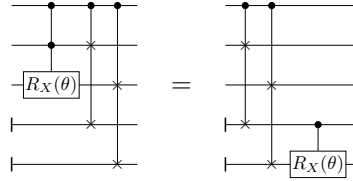
The idea of the proof of Equation  $(K^3)$  is to start from the LHS circuit of  $(K^3)$ , use Equations (76), (77) and (78) to build an instance of the LHS circuit of  $(K^2)$  on two ancillae, apply  $(K^2)$  and then rebuild the RHS circuit of  $(K^3)$  using the same equations.



(76)

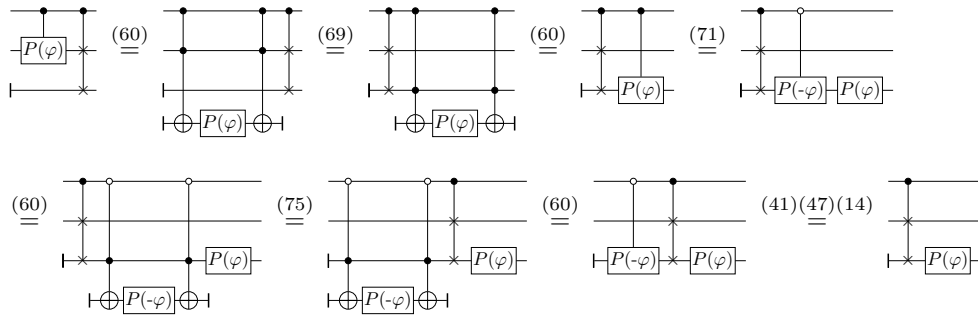


(77)



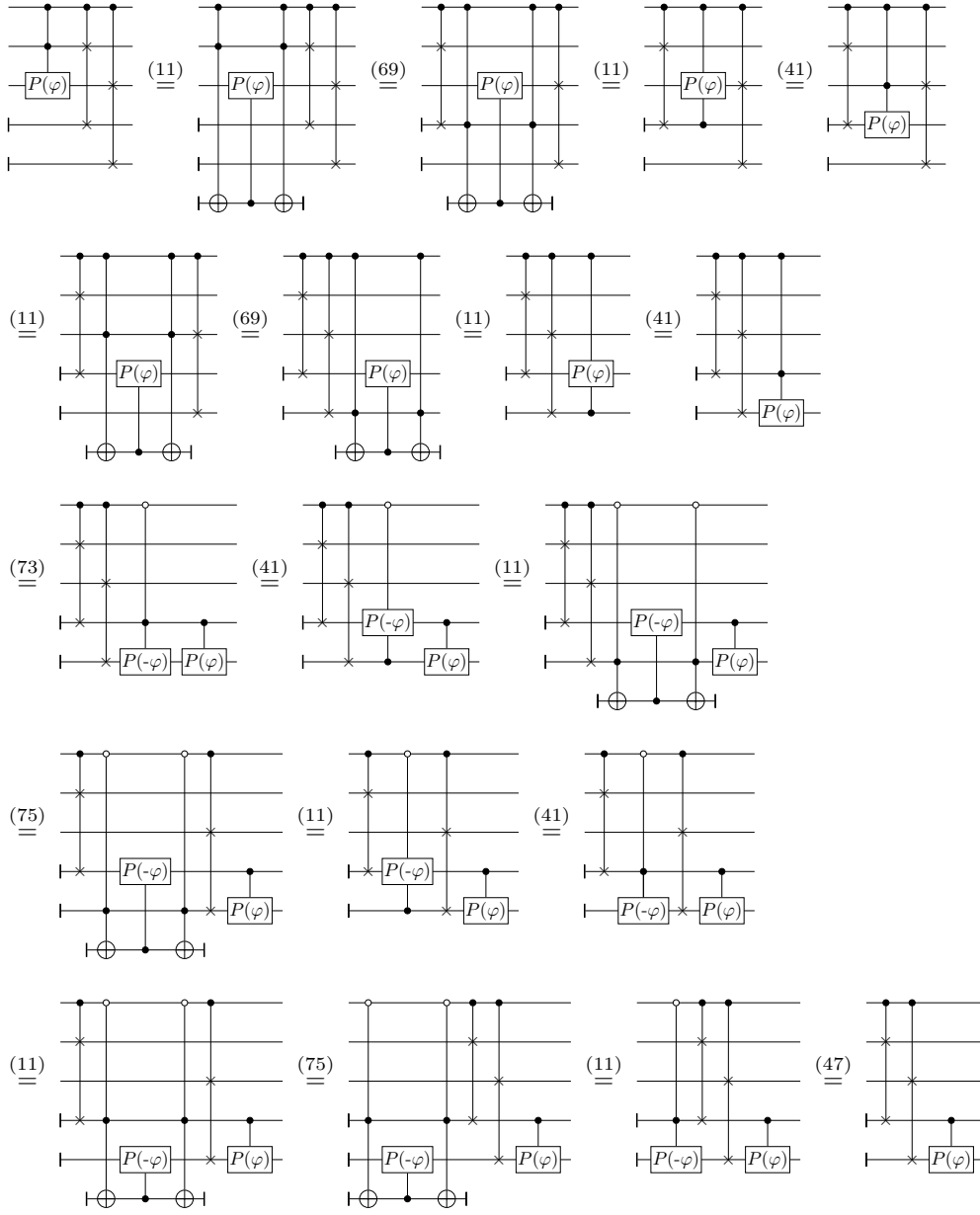
(78)

**Proof of Equation (76).**

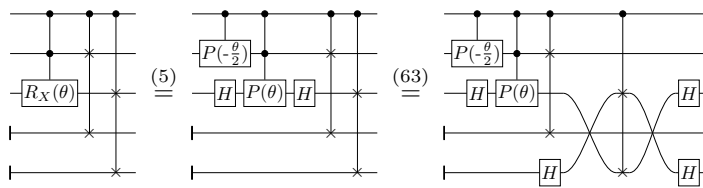


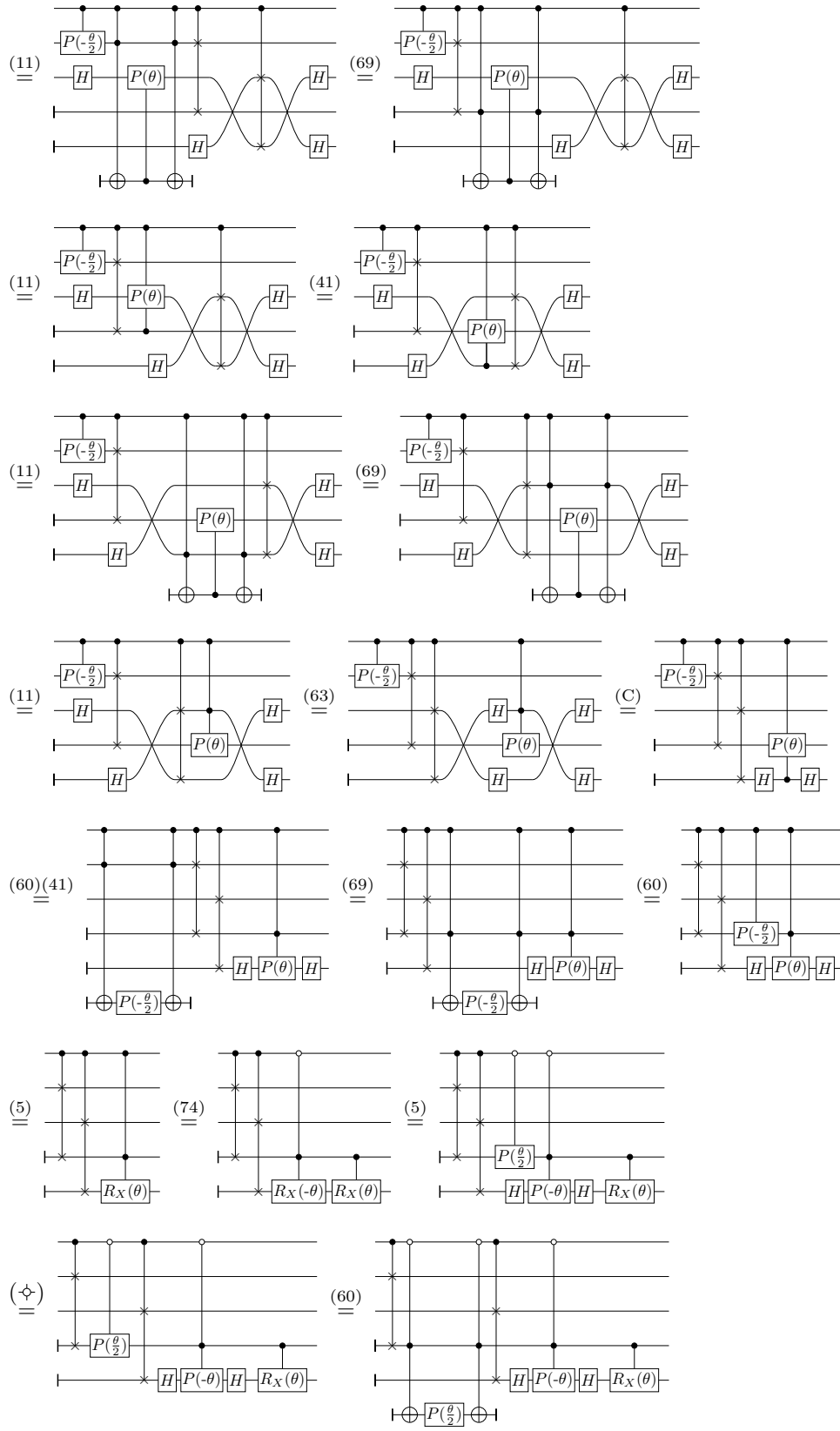
◀

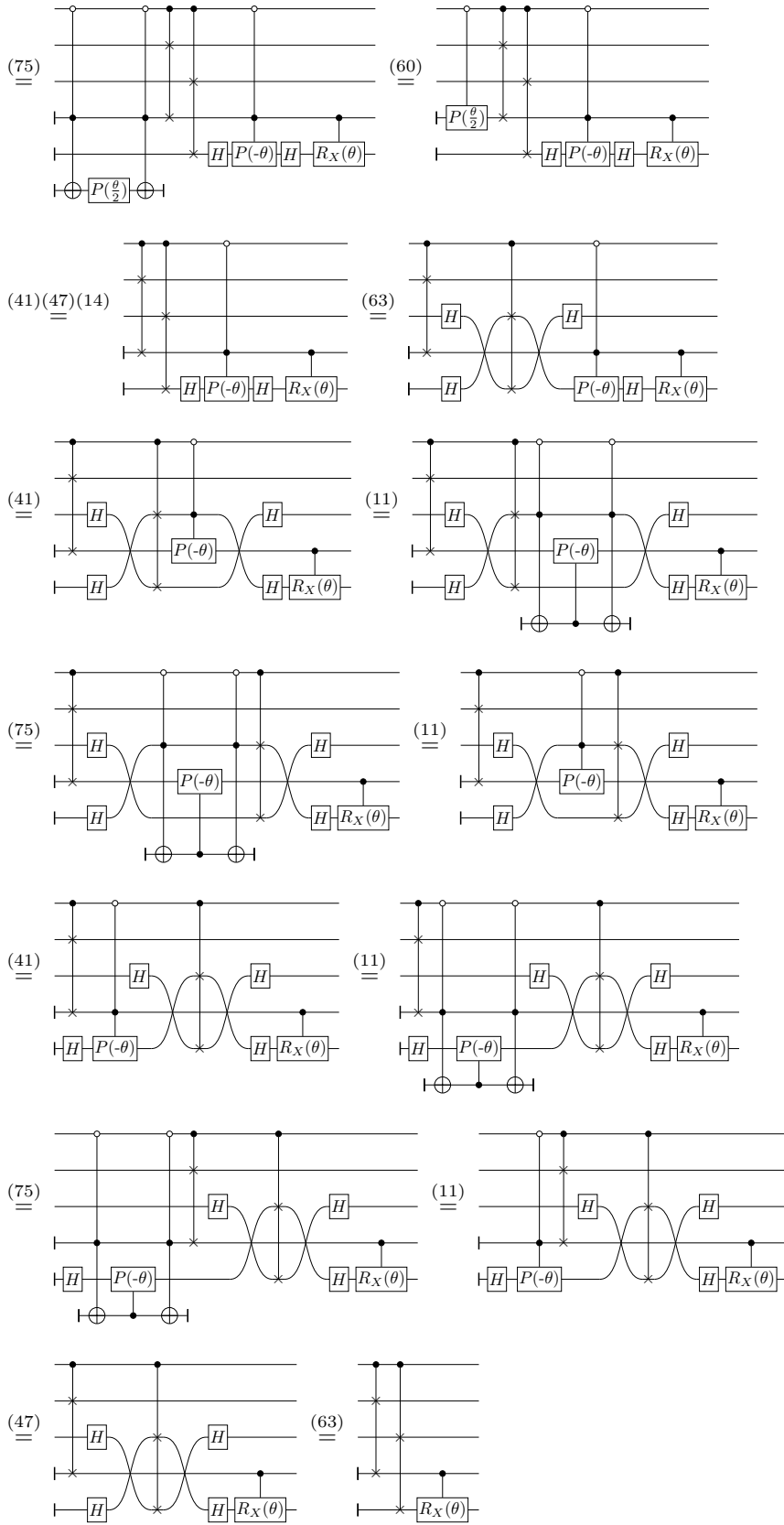
Proof of Equation (77).



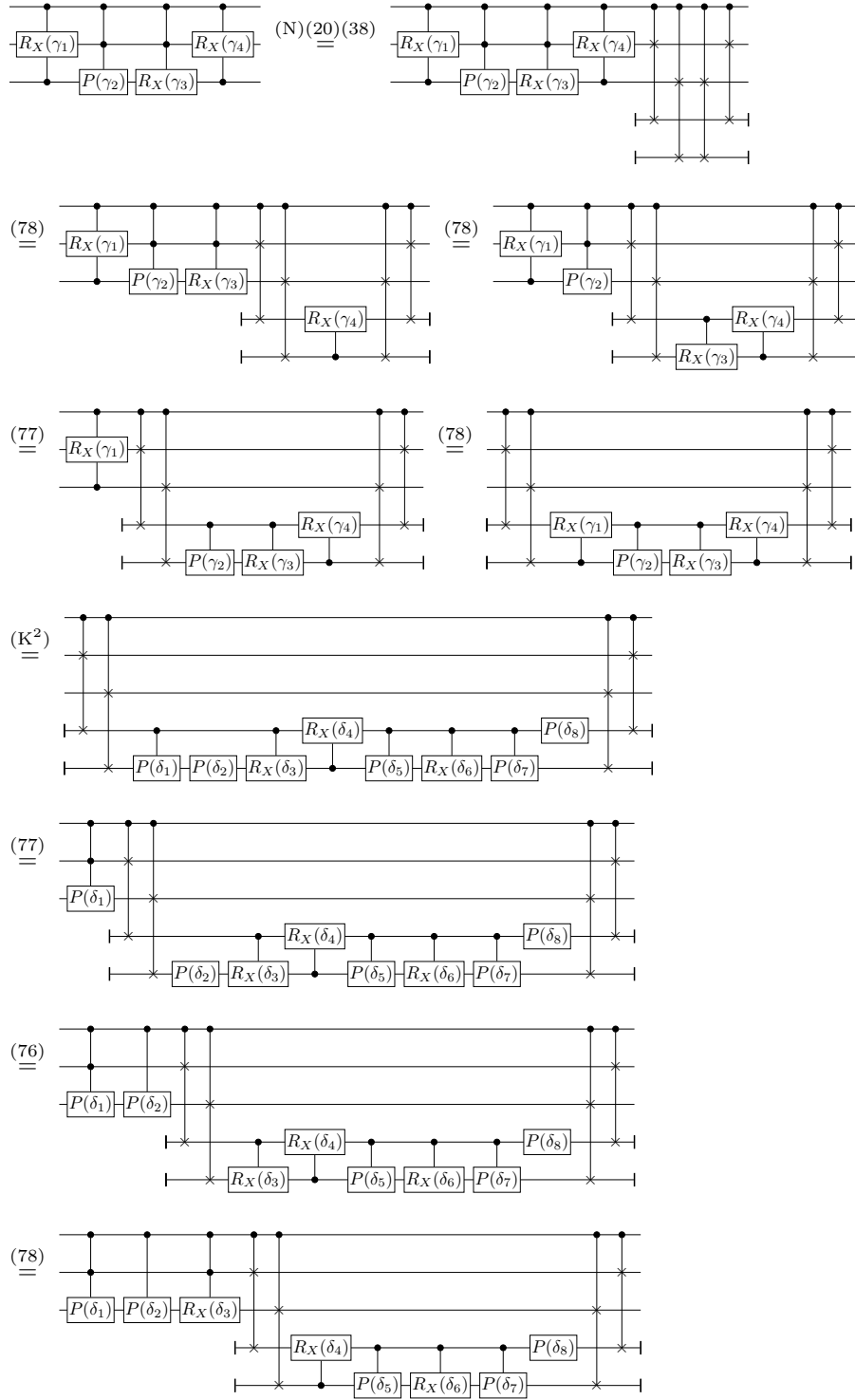
Proof of Equation (78).

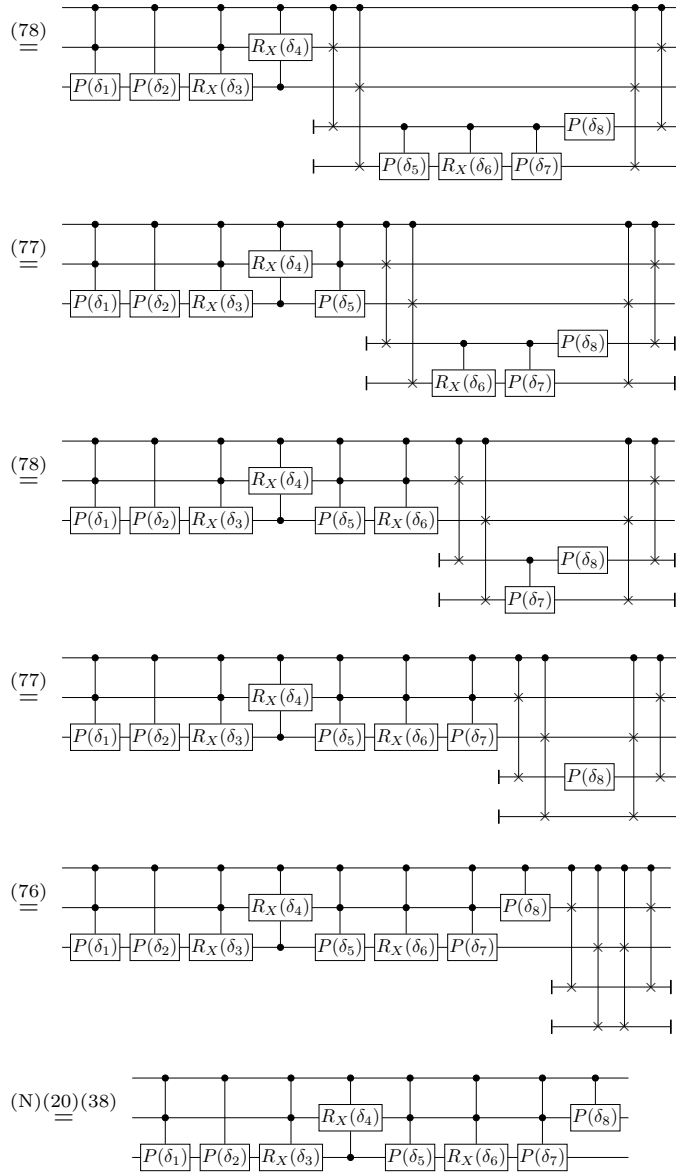






Proof of Equation ( $K^3$ ).





### E.3 Induction step for the proof of Equation (K\*)

