Technical University of Munich
School of Computation, Information and Technology - Informatics

Master's Thesis in Informatics

Simplification of Complete Equational Theories for Quantum Circuits With and Without Ancillae

Noé Delorme

Technical University of Munich
School of Computation, Information and Technology - Informatics

Master's Thesis in Informatics

Simplification of Complete Equational Theories for Quantum Circuits With and Without Ancillae

Vereinfachung Vollständiger Gleichungstheorien für Quantenschaltungen Mit und Ohne Ancillae

Author: Noé Delorme
Supervisor: Prof. Dr. Christian Mendl
Advisor: Simon Perdrix

Submission date: 15/04/2023

I confirm that this master's thesis is my own work and I have documented all sources and material used.

Abstract

Quantum mechanics is based on linear algreba, however matrices and linear maps are not convenient to design quantum algorithms. Graphical languages such as quantum circuits allow one to reason purely graphically. It is of interest to provide equational theories for such graphical languages in order to perform graphical transformations that preserve the circuit's interpretation. Although quantum circuits have been ubiquitous for decades, the first complete equational theory for it has only recently been introduced [4]. Completeness guarantees that any true equation on quantum circuits can be derived from the equational theory. In order to reveal the full potential of this equational theory, one would want to simplify it as much as possible. In this master's thesis we show that several rules can actually be removed without altering the completeness. Especially, two out of the three most intricate rules can be derived from the others. Finally, we show that the last intricate rule can be drastically simplified within a more general model of quantum circuits in which one can use ancillae as temporary additional work space.

Acknowledgements

First and foremost I would like to thank my supervisor Christian Mendl for his continuous support and for allowing me to study quantum computation in my master's thesis. I am also extremely grateful to my advisor Simon perdrix for introducing me to this amazing subject and for his invaluable supervision. I would also like to thank Alexandre Clément and Renaud Vilmart, for having co-written with Simon Perdrix and myself the paper that contains the results of my master's thesis. Additionally, it has been a pleasure to work in the MOCQUA research team at the Loria laboratory and my gratitude extends to the Technical University of Munich and Télécom Paris for making my double degree possible. A special thanks to Nathan Claudet, with whom we discussed about our respective subjects on a daily basis.

Introduction

Quantum computation is the science that tries to take advantage from the non-expected behaviour of quantum mechanics. It provides a new computational model that may lead to an exponential advantage over classical computational models such as Turing machine, and therefore may violate the strong Church-Turing thesis which stipulates that every physically buildable computation device can be simulated by a Turing machine with at most a polynomial slowdown. Indeed, there is a polynomial-time quantum algorithm to factor integers (finding the prime factors of a given integer), whereas after thousands of years of research, no such algorithm is known for Turing machines. Moreover, society currently relies on the fact that there is no such efficient algorithm since many cryptographic schemes (such as RSA) are based of this problem. However, it is still an open question whether scalable quantum computers can be built. This is an active area of research, and we believe that theoretically there is no inherent obstacle. Thus, if there is no such algorithm for Turing machines and if quantum computers are indeed buildable, then the strong Church-Turing Thesis is wrong [17].

Quantum mechanics is based on linear algebra. It is of interest to have graphical languages for quantum computation to allow one to not work on linear maps and matrix directly. Quantum circuits are the most ubiquitous model for quantum computing. It has been introduced in the 80's by Deutch [9]. It allows one to reveal the interesting computational properties of usual quantum operations. Such graphical languages have to be built upon solid formal foundations, especially because when dealing with circuit-based graphical languages, one could deform the circuit without changing its interpretation by bending its wires. Categorical theory is a mathematical framework that allows one to define rigourously graphical languages using the PROP formalism [12, 18].

Circuit transformation, i.e. transforming a circuit without changing its interpretation, is an important task. For instance, circuit optimisation, fault-tolerant quantum computing, hardware constraint satisfaction, and verification [10, 14, 15, 16] involve circuit transformation. 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 equation can be derived, it is said to be complete, in other words, any two circuits representing the same unitary map can be transformed into one another using the rules of the equational theory.

Complete equational theories for quantum circuits were only known for non-universal fragments of quantum circuits, such as Clifford+T circuits acting on at most two qubits [2, 8], the stabiliser fragment [13, 19], the CNot-dihedral fragment [1], or fragments of reversible circuits [11, 7, 6]. Recently, the first complete equational theory for quantum circuit in the general case has been introduced [4]. This equational theory is derived from the completeness of a graphical language for optical quantum computation, namely the LOv-calculus [5]. It contains eighteen rules including three intricate ones which are mathematical residues coming from the translation between quantum circuits and optical circuits. The goal of the master's thesis is to simplify this complete equational theory. Simplifications could be either removing one rule because it can be derived from the other, either replacing one rule by some other more intuitive rules. It turns out that two out of the most intricate rules can be removed.

The vanilla model of quantum circuits can represent any unitary map. In practice one could use axiliary qubits, a.k.a. ancillae, to temporary create additional work space. This leads to an extension of the vanilla model. It turns out that, while it is difficult to simplify the last intricate rule of the complete equational theory, it becomes possible for quantum circuits with ancillae.

The master's thesis is structured as follows: In Chapter 1, the two models – vanilla quantum circuits and quantum circuits with ancillae – are defined, and we introduce category theory and provide the mathematical background that one would require to define graphical languages and equational theories formally. Note that it is not necessary to keep in mind the PROP formalism in the next chapters, one could then just think about circuits "up to deformation" after understanding the rigourous foundations. In Chapter 2 we introduce QC, the simplified equational theory for vanilla quantum circuits and prove its completeness. We also prove some useful properties on quantum circuits and show independently the completeness of QC on a very specific class of circuits, namely the circuits containing only one CNot gate. In Chapter 3 we introduce QC_{H}, the simplified equational theory for quantum circuits with ancillae and prove its completeness by simplying the third intricate rule. In Chapter 4 we discuss futur work and possible use of such simplified equational theories. Finally, all the derivations of the equations used in the proofs are given in the appendices.

The master's thesis took place in the MOCQUA (Classical and Quantum Computational Models) research team in the Loria laboratory (Nancy, France). All the results of the master's thesis have been included in a conjoint work with Alexandre Clément, Simon Perdrix and Renaud Vilmart [3]. Only the results for which I contributed actively are presented in this masters's thesis (some intermediate results are cited for better understanding).

Contents

Introduction **3**

1 Graphical languages for quantum computation **6**
1.1 Categorical theory . . . 6
1.2 PROPs for quantum circuits . . . 8
1.2.1 Vanilla quantum circuits . . . 9
1.2.2 Quantum circuits with ancillae . . . 10
1.3 Equational theories . . . 11

2 Vanilla quantum circuits **12**
2.1 Equational theory for vanilla quantum circuits . . . 12
2.2 Reasonning on quantum circuits . . . 14
2.3 2-qubit 1-CNot 0-Swap completeness . . . 15
2.4 Simplification of the equational theory . . . 19
2.5 Bullet-based graphical notation for multi-controlled gates . . . 20

3 Quantum circuits with ancillae **22**
3.1 Equational theory for quantum circtuits with ancillae . . . 22
3.2 Alternative definitions of multi-controlled gates . . . 23
3.3 Deriving Equation (K^*) from Equation (K^2) . . . 24

4 Discussion **25**

A Proofs of circuits identities **28**
A.1 Proofs of the equations of Figure 1.1 . . . 28
A.2 Proofs of the equations of Figure 2.3 . . . 28
A.3 Proofs of the equations of Figure 2.4 . . . 31
A.4 Proofs of the equations of Figure 3.2 . . . 31

B Proofs of Equations (15) and (16) **33**
B.1 Proof of Equation (15) . . . 33
B.2 Proof of Equation (16) . . . 34

C Proofs used for deriving (K^*) in QC_{H} **37**
C.1 Proof of alternative definitions of multi-controlled gates . . . 37
C.2 Proof of Equation (K^3) . . . 39
C.3 Induction step for proving Equation (K^*) . . . 48

Chapter 1

Graphical languages for quantum computation

1.1 Categorical theory

We use *category theory* to formalize the notion of graphical language. The materials used in this section are extracted from [18]. Firstly, we give the general definition of a *category*, a mathematical object that allows one to compose morphisms sequentially, which consitutes the primary feature of a graphical language such as quantum circuits. Secondly, we define *strict monoidal categories* which allow one the compose morphisms in parallel using a *tensor product* operator. Thirdly, we define *strict braided monoidal categories* which allow one to switch wires and *strict symmetric monoidal categories* which allow one to swap wires. Finally, we define *PROPs* which are a special kind of strict symmetric monoidal categories. This gives us a mathematical framework which allows one to represent graphically circuits "up to deformation".

Definition 1 (Category)**.** *A* category *consists of a collection*[1] *of* objects $\mathrm{Ob}(\mathcal{C})$ *and a collection of* morphisms $\mathrm{Mor}(\mathcal{C})$ *together with a binary operator* $\circ$ *between morphisms. The notations* $f : A \to B$ *or* $A \xrightarrow{f} B$ *denotes the morphism* $f \in \mathrm{Mor}(\mathcal{C})$ *where* A *and* B *are respectively called the* domain *and the* codomain *of* f*. We write* $\mathcal{C}(A, B)$ *for the collection of morphisms of* $\mathcal{C}$ *with domain* A *and codomain* B*. Moreover, to qualify for being a category,* $\mathcal{C}$ *has to satisfy*

- *for any pair of morphims* $f : A \to B, g : B \to C \in \mathrm{Mor}(\mathcal{C})$ *(where the codomain of* f *coincide with the domain of* g*), there exists a morphism* $g \circ f : A \to C \in \mathrm{Mor}(\mathcal{C})$ *called their* composite*,*
- *for any object* $A \in \mathrm{Ob}(\mathcal{C})$*, there exists a morphism* $id_A : A \to A \in \mathrm{Mor}(\mathcal{C})$ *called the* identity on A*, such that for any morphism* $f : A \to B \in \mathrm{Mor}(\mathcal{C})$ *we have* $f \circ id_A = f$ *and for any morphism* $g : B \to A \in \mathrm{Mor}(\mathcal{C})$ *we have* $id_A \circ g = g$*,*
- $\circ$ *is associative, i.e.* $(h \circ g) \circ f = h \circ (g \circ f)$ *for any morphisms* $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \in \mathrm{Mor}(\mathcal{C})$.

The classic example of a category is Set, the category with sets as objects and functions as morphisms, and the usual composition of functions as composition. In our case, we are interested in using the category theory to formalize the notion of circuit-based graphical languages. In this framework, objects are graphically represented as wires, morphisms are represented by gates, and composing morphisms allows one to build circuits.

The morphism $f : A \to B$ is graphically represented by $A - \boxed{f} - B$. This diagrammatic form improves our intuition about the way morphisms compose. For instance, the conditions of

[1] Mathematicians often use the term *collection* to denote a bunch of "things" without prejudice as to whether those things form a *set* or some other formal notions of collection.

Definition 1 can be graphically expressed as follows.

$$\left(B -\boxed{g}- C \right) \circ \left(A -\boxed{f}- B \right) = A -\boxed{f}-\boxed{g}- C$$
$$\left(A -\boxed{f}- B \right) \circ \left(A — A \right) = A ——\boxed{f}- B = A -\boxed{f}- B$$
$$\left(A — A \right) \circ \left(B -\boxed{g}- A \right) = B -\boxed{g}—— A = B -\boxed{g}- A$$
$$\left(B -\boxed{g}-\boxed{h}- D \right) \circ \left(A -\boxed{f}- B \right) = A -\boxed{f}-\boxed{g}-\boxed{h}- D = \left(C -\boxed{h}- D \right) \circ \left(A -\boxed{f}-\boxed{g}- C \right)$$

Definition 2 (Isomorphism). *An* isomorphism *is an invertible morphism, i.e. a morphism $f : A \to B \in \mathrm{Mor}(\mathcal{C})$ such that there exists another morphism $f^{-1} : B \to A \in \mathrm{Mor}(\mathcal{C})$ that satisfies $f^{-1} \circ f = id_A$ and $f \circ f^{-1} = id_B$.*

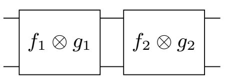
Definition 3 (Functor). *A* functor $F : \mathcal{C} \to \mathcal{D}$ *between two categories $\mathcal{C}$ and $\mathcal{D}$ is a map sending each object $A \in \mathrm{Ob}(\mathcal{C})$ to an object $F(A) \in \mathrm{Ob}(\mathcal{D})$ and each morphism $f : A \to B \in \mathrm{Mor}(\mathcal{C})$ to a morphism $F(f) : F(A) \to F(B) \in \mathrm{Mor}(\mathcal{D})$, such that*
- *F preserves composition, i.e. $F(g \circ f) = F(g) \circ F(f)$ whenever $g \circ f$ is defined in $\mathcal{C}$,*
- *F preserves identity morphisms, i.e. for each object $A \in \mathrm{Ob}(\mathcal{C})$, $F(id_A) = id_{F(A)}$.*

Intuitively, a functor is a map between two categories that preserves the structure. As a second step toward graphical languages, we introduce *strict monoidal categories*, which allow one to compose morphisms in parallel using the *tensor product.*

Definition 4 (Strict monoidal category). *A* strict monoidal category $\mathcal{C}$ *is a category equipped with a functor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ called* tensor product *and a particular object $1 \in \mathrm{Ob}(\mathcal{C})$ called the* unit object*, such that*
- *1 is neutral for $\otimes$, i.e. $A \otimes 1 = A = 1 \otimes A$,*
- *$\otimes$ is associative, i.e. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ and $(f \otimes g) \otimes h = f \otimes (g \otimes h)$,*
- *$(f_2 \otimes g_2) \circ (f_1 \otimes g_1) = (f_2 \circ f_1) \otimes (g_2 \circ g_1)$ whenever $f_2 \circ f_1$ and $g_2 \circ g_1$ are defined.*

Graphically, the tensor product of a monoidal category behave as expected: the tensor product of two morphisms is the parallel composition of those morphisms.

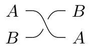
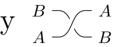
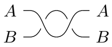
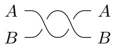
$$\left(A -\boxed{f}- B \right) \otimes \left(C -\boxed{g}- D \right) = \begin{array}{c} A -\boxed{f}- B \\ C -\boxed{g}- D \end{array}$$

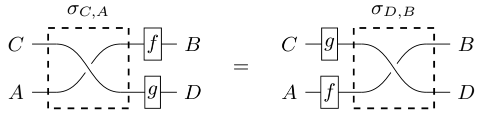


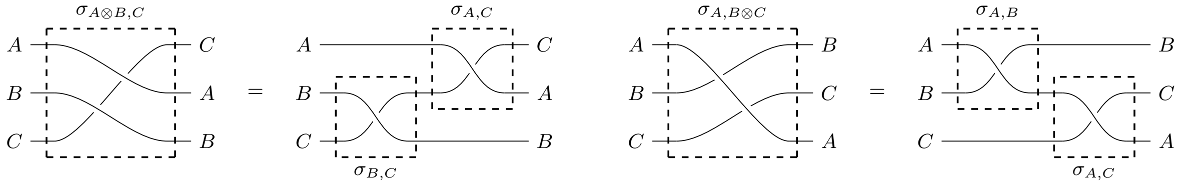
$$= \begin{array}{c} -\boxed{f_1}-\boxed{f_2}- \\ -\boxed{g_1}-\boxed{g_2}- \end{array}$$

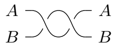
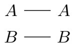
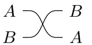
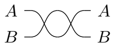
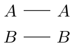
We want to define circuits of a graphical language "up to deformation", we make this notion formal by introducing *strict braided monoidal categories*, which are strict monoidal categories equipped with a special braiding morphism that allows one to basically "switch wires".

Definition 5 (Strict braided monoidal category). *A* strict braided monoidal category $\mathcal{C}$ *is a strict monoidal category such that for any objects $A, B \in \mathrm{Ob}(\mathcal{C})$, there exists an isomorphism $\sigma_{A,B} : A \otimes B \to B \otimes A \in \mathrm{Mor}(\mathcal{C})$ called* braiding*, such that*
- *for any $f : A \to B, g : C \to D \in \mathrm{Mor}(\mathcal{C})$ we have $(f \otimes g) \circ \sigma_{C,A} = \sigma_{D,B} \circ (g \otimes f)$,*
- *for any $A, B, C \in \mathrm{Ob}(\mathcal{C})$ we have $\sigma_{A \otimes B,C} = (\sigma_{A,C} \otimes id_B) \circ (id_A \otimes \sigma_{B,C})$,*
- *for any $A, B, C \in \mathrm{Ob}(\mathcal{C})$ we have $\sigma_{A,B \otimes C} = (id_B \otimes \sigma_{A,C}) \circ (\sigma_{A,B} \otimes id_C)$.*

The braiding $\sigma_{A,B}$ is represented by  and its inverse $\sigma_{A,B}^{-1}$ by . This notation is convenient as it refects graphically that $\sigma_{A,B} \circ \sigma_{A,B}^{-1} =$  $= \begin{smallmatrix} A — A \\ B — B \end{smallmatrix} = id_{A \otimes B}$. Notice however that $\sigma_{A,B} \circ \sigma_{B,A} =$  $\neq \begin{smallmatrix} A — A \\ B — B \end{smallmatrix}$ in general. The three conditions of Definition 5 are graphically traduced as follows.



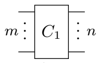
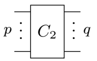


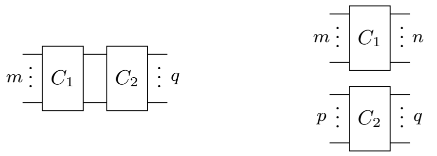
When  =  holds in general, the category is said to be *strict symmetric monoidal* and we can represente $\sigma_{A,B}$ by  without ambiguity so that  = . Intuitively, switching wires twice in the same direction has no effect.

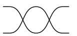
Definition 6 (Strict symmetric monoidal category)**.** *A* strict symmetric monoidal category *is a strict braided monoidal category such that $\sigma_{B,A} \circ \sigma_{A,B} = id_{A\otimes B}$ for any objects $A, B \in \mathrm{Ob}(\mathcal{C})$.*

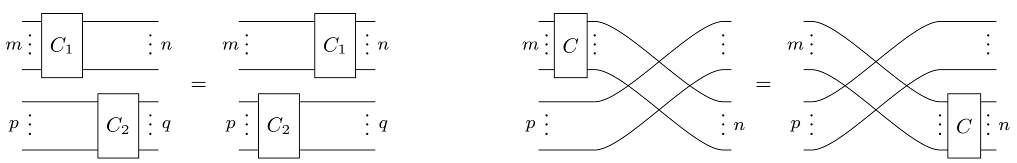
We are now ready to define the mathematical object used to formalize the notion of graphical languages. A *PROP* is a special kind of strict symmetric monoidal category.

Definition 7 (Products and permutations category)**.** *A* PROP *is a strict symmetric monoidal category whose objects are of the form $x^{\otimes n} = x \otimes \cdots \otimes x$ for a single object x and $n \geq 0$.*[2]

In the following we identify $x^{\otimes n}$ with n. The PROP formalism provides a formal and rigorous framework to describe circuits as elements of $\mathrm{Mor}(\mathcal{C})$. The domain and the codomain of a morphism respectively represente the number of inputs and outputs of the circuit. The circuits $C_1 : m \to n$ and $C_2 : p \to q$, depicted as  and  can be composed in two different ways: (1) "sequentially" $C_2 \circ C_1 : m \to q$ if $n = p$; (2) "in parallel" $C_1 \otimes C_2 : m + p \to n + q$. Graphically,



The neutral element for $\otimes$ over objects is 0, thus the neutral element for $\otimes$ over circuits is the empty circuit ⬚ : $0 \to 0$ which satisfies $C \otimes$ ⬚ $= C =$ ⬚ $\otimes\, C$ for any circuit C. The circuit $—^{\otimes n}$, inductively defined by $—^{\otimes n} := — \otimes —^{\otimes n-1}$ and $—^{\otimes 0} :=$ ⬚, is the identity circuit acting on n wires. Morevover, a PROP also has a particular circuit : $2 \to 2$ that graphically swap wires and satisfies  = . PROPs formalize the notion of "being able to deform the circuit by bending wires".[3] For instance, the following identities are valid transformations.



1.2 PROPs for quantum circuits

In this master's thesis, we consider two models of quantum circuits: vanilla quantum circuits, which can implement any unitary; and quantum circuits with ancillae, which use an additional work space to implement any isometries[4].

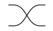
[2] A prop can be equivalentely defined as a strict symmetric monoidal category whose objects are all natural integers (by identifying $x^{\otimes n}$ with $n \in \mathbb{N}$).

[3] Note however that one can not bend the wires backward (this is not allowed by the PROP formalism).

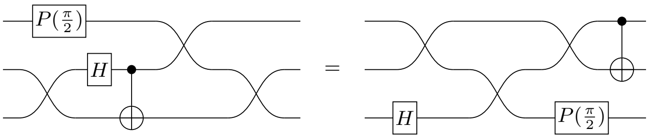
[4] An isometry is a linear map V such that $V^\dagger V$ is the identity.

1.2.1 Vanilla quantum circuits

Vanilla quantum circuits are circuits generated by the Hadamard gate, phase gates and CNot together with global phases. Quantum computer scientists usually concider quantum circuits up to global phase. However, we concider here the general case where different global phases lead to different quantum circuits.

Definition 8 (Vanilla quantum circuits)**.** *Let $\mathcal{QC}$ be the PROP generated by* $: 0 \to 0$, $-\boxed{H}-$ $: 1 \to 1$, $-\boxed{P(\varphi)}-$ $: 1 \to 1$, $: 2 \to 2$ *for any* $\varphi \in \mathbb{R}$. *The empty, identity and swap circuits are respectively denoted* $: 0 \to 0$, $— : 1 \to 1$ *and*  $: 2 \to 2$.

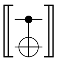
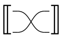
The PROP formalism ensure that quantum circuits are defined "up to deformation" without ambiguity. For instance:



Quantum circuits are a formal notion. In order to use them to describe quantum evolutions we associate to each circuit its standard interpretation (its *semantics*) as follows.

Definition 9 (Semantics)**.** *For any n-qubit vanilla quantum circuit $C \in \mathcal{QC}(n,n)$, let $[\![C]\!] : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ be the* semantics *of C inductively defined as the linear map $[\![C_2 \circ C_1]\!] = [\![C_2]\!] \circ [\![C_1]\!]$; $[\![C_1 \otimes C_2]\!] = [\![C_1]\!] \otimes [\![C_2]\!]$; and*

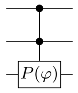
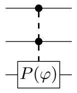
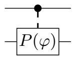
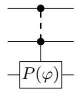
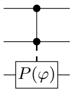
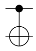
$[\![$ $]\!] = 1 \mapsto 1$ $[\![$ $]\!] = 1 \mapsto e^{i\varphi}$ $[\![-\boxed{H}-]\!] = |x\rangle \mapsto \dfrac{|0\rangle + (-1)^x\,|1\rangle}{\sqrt{2}}$ $[\![-\boxed{P(\varphi)}-]\!] = |x\rangle \mapsto e^{ix\varphi}\,|x\rangle$

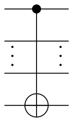
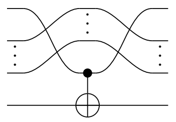
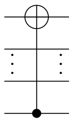
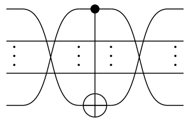
$[\![$  $]\!] = |x,y\rangle \mapsto |x, x \oplus y\rangle$ $[\![—]\!] = |x\rangle \mapsto |x\rangle$ $[\![$  $]\!] = |x,y\rangle \mapsto |y,x\rangle$

The choice of the generators ensure that every quantum evolutions can be represented by some circuit of $\mathcal{QC}$.

Proposition 1 (Universality [17])**.** *$\mathcal{QC}$ is universal, i.e. for any unitary $U : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ there exists a quantum circuit $C \in \mathcal{QC}(n,n)$ such that $[\![C]\!] = U$.*

Vanilla quantum circuits as defined in Definition 8 only have four different kinds of gates. While it is sufficient to describe any quantum algorithm, it is often convenient to use other gates that can be defined by combining the generators together. For instance, X-rotations, Pauli gates, Toffoli and multi-controlled gates are defined in Figure 1.1. Note that the phase gate $-\boxed{P(\varphi)}-$ is 2π-periodic while the X-rotation gate $-\boxed{R_X(\theta)}-$ is 4π-periodic.

We use the standard bullet-based notation for multi-controlled gates. For instance  denotes the application of a phase gate $-\boxed{P(\varphi)}-$ on the third qubit controlled by the first two qubits. With a slight abuse of notation, we use dashed lines for arbitrary number of control qubits, e.g.  $: n+1 \to n+1$ or simply  $: n+1 \to n+1$ have $n \geq 0$ control qubits (possibly zero), whereas  $: n+2 \to n+2$ and  $: 1+n+1 \to 1+n+1$ have at least one control qubit. Additionally, we use some specific shortcut notations for :

 $:=$   $:=$ 

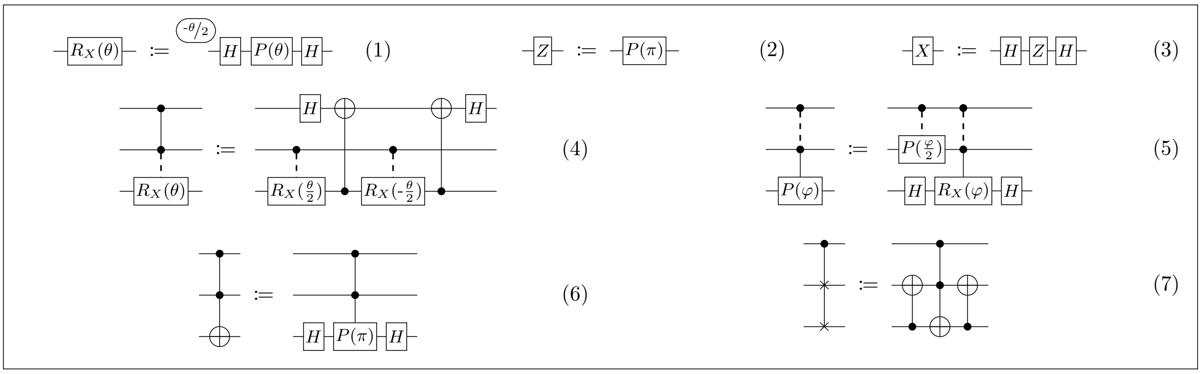
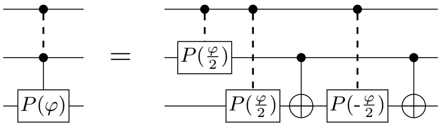


Figure 1.1: Shortcut notations for usual gates defined for any $\varphi, \theta \in \mathbb{R}$. Equation (1) defines X-rotations while Equations (2) and (3) define Pauli gates. Equations (4) and (5) are inductive definitions of multi-controlled gates. Equation (6) is the definition of the well known Toffoli gate. Equation (7) is the definition of the Fredkin gate (or controlled-swap gate).

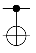
Notice that the multi-controlled phase gate (Equation (5)) is defined using the multi-controlled X-rotation gate (Equation (4)). One could alternatively define it inductively only using multi-controlled phase gate: Equation (8) is proved to be equivalent to Equation (5) in Appendix A.1.



(8)

1.2.2 Quantum circuits with ancillae

Quantum circuits with ancillae is an extension of vanilla quantum circuits where there is the possibility to create temporary additional work space. In some sence, the vanilla model is included in the model with ancillae: any vanilla quantum circuit can be seen as a quantum circuit without ancilla.

Definition 10. *Let $\mathcal{QC}^*_{\mathsf{H}}$ be the PROP generated by* $\textcircled{\scriptsize\varphi} : 0 \to 0$, $\boxed{H} : 1 \to 1$, $\boxed{P(\varphi)} : 1 \to 1$,  $: 2 \to 2$, $\vdash : 0 \to 1$, $\dashv : 1 \to 0$ *for any* $\varphi \in \mathbb{R}$*. The empty, identity and swap circuits are respectively denoted* ⬚ $: 0 \to 0$, — $: 1 \to 1$ *and* $\times$ $: 2 \to 2$.

Definition 11 (Semantics)**.** *We extend the semantics* $[\![\cdot]\!]$ *with* $[\![\vdash]\!] = |0\rangle$ *and* $[\![\dashv]\!] = \langle 0|$.

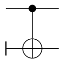
Notice that the semantics of a $\mathcal{QC}^*_{\mathsf{H}}$-circuit is not necessarily an isometry as $[\![\dashv]\!]$ is not isometric. As a consequence, we define the PROP of quantum circtuit with ancillae $\mathcal{QC}_{\mathsf{H}}$ as the subclass of $\mathcal{QC}^*_{\mathsf{H}}$-circuits with an isometric semantics.

Definition 12 (Quantum circuits with ancillae)**.** *Let $\mathcal{QC}_{\mathsf{H}}$ be the sub-PROP of circuits $C \in \mathcal{QC}^*_{\mathsf{H}}$ such that $[\![C]\!]$ is an isometry.*

Intuitively, the generator $\dashv$ can only be applied on an ancilla in the $|0\rangle$-state. Notice that $\mathcal{QC}_{\mathsf{H}}$ is indeed a sub-PROP (and thus a PROP) because it satisfies the composition conditions of Definition 1. The universality of $\mathcal{QC}_{\mathsf{H}}$ is straightforward:

Proposition 2 (Universality)**.** *$\mathcal{QC}_{\mathsf{H}}$ is universal, i.e. for any unitary $U : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ there exists a quantum circuit $C \in \mathcal{QC}_{\mathsf{H}}(n,n)$ such that $[\![C]\!] = U$.*

Proof. If $C \in \mathcal{QC}$ then $C \in \mathcal{QC}_{\mathsf{H}}$. Hence, as $\mathcal{QC}$ is universal (Proposition 1), so is $\mathcal{QC}_{\mathsf{H}}$. □

Ancillae add expresive power to the vanilla model. For instance, the so-called copy in the standard basis can be implemented as  .

1.3 Equational theories

An equational theory Γ is a set of equations that one could use to transform circuits. Γ can be seen as an axiomatization whose axioms are some equations over circuits. For instance the rule $-\boxed{H}-\boxed{H}- \;=\; -\!\!-$ could be one axiom of an equational theory for quantum circuits. We write $\Gamma \vdash C_1 = C_2$ when C_1 can be transformed into C_2 using only the equations of Γ. More formally, $\Gamma \vdash \cdot = \cdot$ is the smallest congrence which satisfies the equations of Γ together with the deformation rules that come with the PROP formalism.

When dealing with equational theories we often want two important properties: (1) the *soundness* of the equational theory which guarantees that any provable equation is semantically correct; and (2) the *completeness* of the equational theory which guarantees that any semantically correct equation is provable.

Definition 13 (Soundness)**.** *Let Γ be an equational theory for a graphical language $\mathcal{L}$ equipped with an interpretation $[\![\cdot]\!]$. Γ is* sound *if* $\Gamma \vdash C_1 = C_2 \implies [\![C_1]\!] = [\![C_2]\!]$ *for any* $C_1, C_2 \in \mathcal{L}$.

Definition 14 (Completeness)**.** *Let Γ be an equational theory for a graphical language $\mathcal{L}$ equipped with an interpretation $[\![\cdot]\!]$. Γ is* complete *if* $[\![C_1]\!] = [\![C_2]\!] \implies \Gamma \vdash C_1 = C_2$ *for any* $C_1, C_2 \in \mathcal{L}$.

Chapter 2

Vanilla quantum circuits

2.1 Equational theory for vanilla quantum circuits

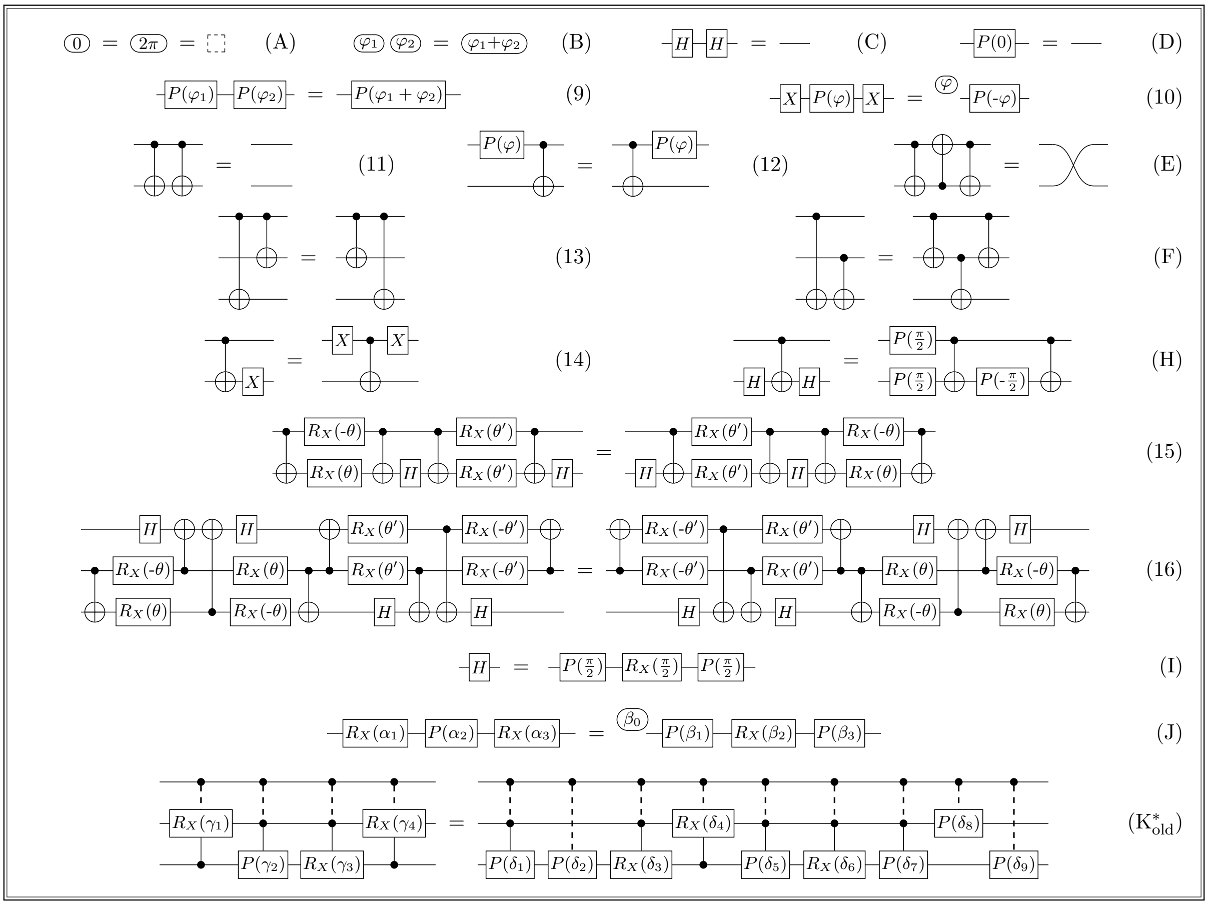


Figure 2.1: Equational theory $\widehat{\mathrm{QC}}$. Equations (B), (9), (10) and (12) are defined for any $\varphi, \varphi_1, \varphi_2 \in \mathbb{R}$. Equations (15) and (16) are some intricate rules defined for any $\theta, \theta' \in \mathbb{R}$ that are mathematical residues of the proof of completeness of $\widehat{\mathrm{QC}}$ in [4]. In Equations (J) and (K$^*_{\text{old}}$) 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. Equation (K$^*_{\text{old}}$) 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$^*_{\text{old}}$) can be seen as a generalization of the Euler rule, using multi-controlled gates.

The equational theory $\widehat{\mathrm{QC}}$ defined in Figure 2.1 is the equational theory introduced in [4] and has been shown to be sound and complete. Before that, complete equational theories were known for non-universal fragments such as Clifford+T acting on at most two qubits [2]. The completeness of $\widehat{\mathrm{QC}}$ has been proved using a back and forth translation from a complete equational theory for optical circuits [5].

$\widehat{\mathrm{QC}}$ contains some simple rules that are commonly used equations in the litterature. However it also contains three intricate rules, namely Equations (15), (16) and ($\mathrm{K}^*_{\mathrm{old}}$). Equations (15) and (16) are mathematical residues of the proof of completeness of $\widehat{\mathrm{QC}}$ (those equations are base cases of some commutation properties of multi-controlled operations). Equation ($\mathrm{K}^*_{\mathrm{old}}$) is the translation of the most intricate axiom of the complete equational theory for optical circuits.

Remark 1. *For any $\alpha_i \in \mathbb{R}$ in Equation* (J)*, there exist $\beta_j \in \mathbb{R}$ such that Equation* (J) *is sound. We make the angles β_j unique by assuming that $\beta_1 \in [0, \pi)$, $\beta_0, \beta_2, \beta_3 \in [0, 2\pi)$ and if $\beta_2 \in \{0, \pi\}$ then $\beta_1 = 0$. Similarly to Equation* (J)*, for any $\gamma_i \in \mathbb{R}$ in Equation* ($\mathrm{K}^*_{\mathrm{old}}$)*, there exist $\delta_j \in [0, 2\pi)$ such that Equation* ($\mathrm{K}^*_{\mathrm{old}}$) *is sound. We can ensure that the angles δ_j are uniquely determined by assuming that $\delta_1, \delta_2, \delta_5, \in [0, \pi)$, $\delta_3, \delta_4, \delta_6 \in [0, 2\pi)$, 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 $\delta_5 = 0$.*

In this master's thesis we simply $\widehat{\mathrm{QC}}$ into QC which is defined in Figure 2.2. While $\widehat{\mathrm{QC}}$ contains eighteen axioms, QC only contains eleven axioms. Moreover two out of the three most intricate rules of $\widehat{\mathrm{QC}}$ has been removed. This chapter aims to prove the completeness of QC.

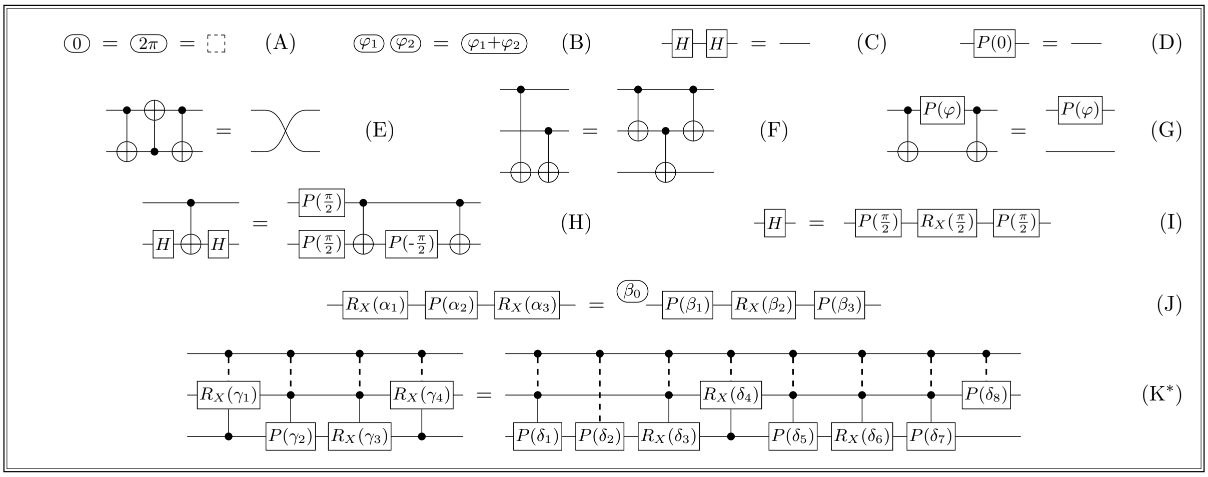


Figure 2.2: Equational theory QC. Equation (G) is a new axiom defined for any $\varphi \in \mathbb{R}$. Equation (K*) is a simplified version of Equation ($\mathrm{K}^*_{\mathrm{old}}$) (with one less parameter). The other equations are axioms of $\widehat{\mathrm{QC}}$.

Remark 2. *In Equation* (K*) *we ensure that the angles δ_j are uniquely determined by assuming that $\delta_1, \delta_2, \delta_5 \in [0, \pi)$, $\delta_3, \delta_6, \delta_7, \delta_8 \in [0, 2\pi)$, $\delta_4 \in [0, 4\pi)$, if $\delta_3 = 0$ and $\delta_6 \neq 0$ then $\delta_2 = 0$, if $\delta_3 = \pi$ then $\delta_1 = 0$, if $\delta_4 \in \{0, 2\pi\}$ then $\delta_1 = \delta_3 = 0$, if $\delta_4 \in \{\pi, 3\pi\}$ then $\delta_2 = 0$, if $\delta_4 \in \{\pi, 3\pi\}$ and $\delta_3 = 0$ then $\delta_1 = 0$, and if $\delta_6 \in \{0, \pi\}$ then $\delta_5 = 0$.*

One can derive many useful equations within QC.[1] In particular the equations of Figure 2.3 are proved in Appendix A.2 and the equations of Figure 2.4 are proved in Appendix A.3.

[1] In fact, any true equations can be derived within QC as QC will be shown to be complete in the following.

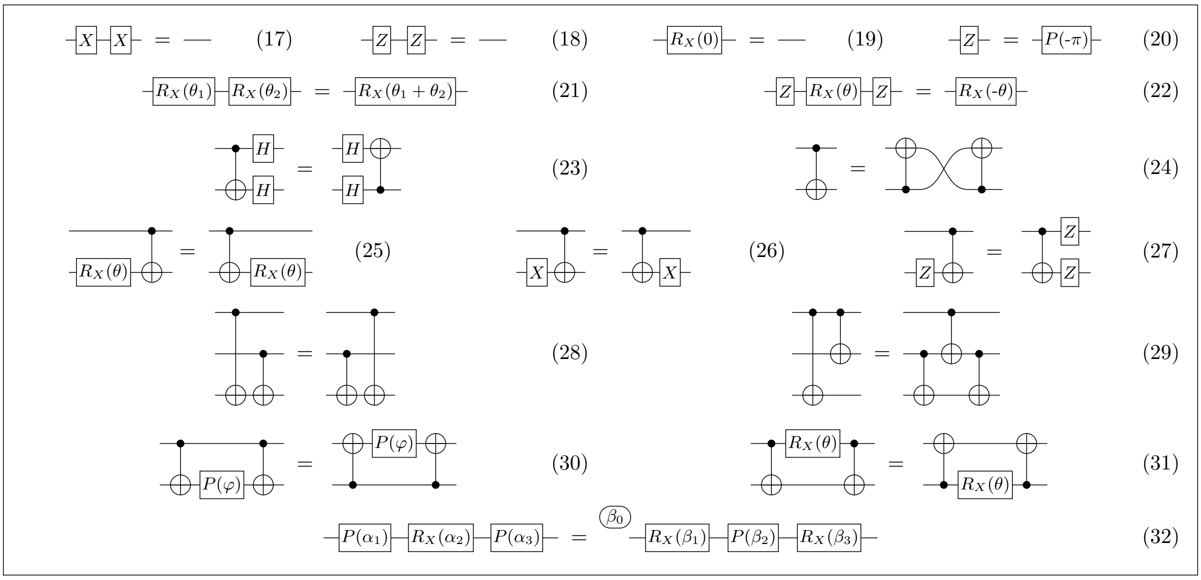


Figure 2.3: Some usual identities provable in QC for any $\varphi, \varphi_1, \varphi_2, \theta, \theta_1, \theta_2 \in \mathbb{R}$. Equation (32) is the dual version of Equation (J) where the angles are computed in a similar way. All the proofs are given in Appendix A.2.

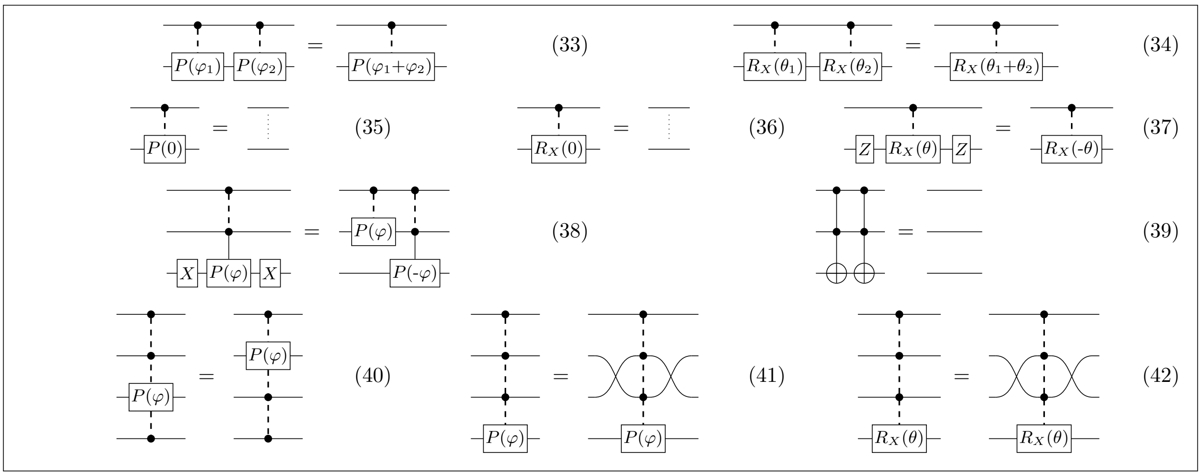


Figure 2.4: Some usual identities over multi-controlled gates provable in QC for any $\varphi, \varphi_1, \varphi_2, \theta, \theta_1, \theta_2 \in \mathbb{R}$. All the proofs are given in Appendix A.3.

2.2 Reasonning on quantum circuits

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

Definition 15. *For any vanilla quantum circuit $C \in \mathcal{QC}$, let $C^\dagger$ be the* adjoint *of C inductively defined as $(C_2 \circ C_1)^\dagger := C_1^\dagger \circ C_2^\dagger$; $(C_1 \otimes C_2)^\dagger := C_1^\dagger \otimes C_2^\dagger$; and for any $\varphi \in \mathbb{R}$, $(\textcircled{\varphi})^\dagger := \textcircled{-\varphi}$, $(\boxed{P(\varphi)})^\dagger := \boxed{P(\text{-}\varphi)}$, and $g^\dagger := g$ for any other generator g.*

Proposition 3. $[\![C^\dagger]\!] = [\![C]\!]^\dagger$ *for any vanilla quantum circuit $C \in \mathcal{QC}$, where $[\![C]\!]^\dagger$ is the usual linear algebra adjoint of $[\![C]\!]$.*

Proof. By induction on C. The statement holds for the generators (see Definition 9). Moreover $[\![C_2 \circ C_1]\!]^\dagger = ([\![C_2]\!] \circ [\![C_1]\!])^\dagger = [\![C_1]\!]^\dagger \circ [\![C_2]\!]^\dagger = \left[\!\!\left[C_1^\dagger\right]\!\!\right] \circ \left[\!\!\left[C_2^\dagger\right]\!\!\right] = \left[\!\!\left[C_1^\dagger \circ C_2^\dagger\right]\!\!\right] = \left[\!\!\left[(C_2 \circ C_1)^\dagger\right]\!\!\right]$ and $[\![C_1 \otimes C_2]\!]^\dagger = ([\![C_1]\!] \otimes [\![C_2]\!])^\dagger = [\![C_1]\!]^\dagger \otimes [\![C_2]\!]^\dagger = \left[\!\!\left[C_1^\dagger\right]\!\!\right] \otimes \left[\!\!\left[C_2^\dagger\right]\!\!\right] = \left[\!\!\left[C_1^\dagger \otimes C_2^\dagger\right]\!\!\right] = \left[\!\!\left[(C_1 \otimes C_2)^\dagger\right]\!\!\right]$. □

Proposition 4. $\mathrm{QC} \vdash C \circ C^\dagger = —^{\otimes n}$ *and* $\mathrm{QC} \vdash C^\dagger \circ C = —^{\otimes n}$ *for any n-qubit vanilla quantum circuit $C \in \mathcal{QC}(n,n)$.*

Proof. By induction on C using $\mathrm{QC} \vdash (C_2 \circ C_1) \circ (C_2 \circ C_1)^\dagger = C_2 \circ C_1 \circ C_1^\dagger \circ C_2^\dagger = —^{\otimes n}$ and $\mathrm{QC} \vdash (C_1 \otimes C_2) \circ (C_1 \otimes C_2)^\dagger = (C_1 \otimes C_2) \circ (C_1^\dagger \otimes C_2^\dagger) = (C_1 \circ C_1^\dagger) \otimes (C_2 \circ C_2^\dagger) = —^{\otimes n}$. The proof of the second statement is symmetric. □

Formally, we say that an equation $C_1 = C_2$ is QC-equivalent to another equation $C_3 = C_4$, denoted $(C_1 = C_2) \sim_{\mathrm{QC}} (C_3 = C_4)$, if $\mathrm{QC} \vdash C_1 = C_2 \iff \mathrm{QC} \vdash C_3 = C_4$, i.e. proving one in QC implies that the other is also provable in QC. Proposition 5 allows us to move gates from one side of the equation to the other. In the following, we refer to this as the *crossing gate property.*

Proposition 5 (Crossing gate property)**.** $(C_2 \circ C \circ C_1 = C') \sim_{\mathrm{QC}} (C = C_2^\dagger \circ C' \circ C_1^\dagger)$ *for any n-qubit vanilla quantum circuits $C, C', C_1, C_2 \in \mathcal{QC}(n,n)$.*

Proof. $\boxed{\Longrightarrow}$ Suppose $\mathrm{QC} \vdash C_2 \circ C \circ C_1 = C'$, then thanks to Proposition 4, we have $\mathrm{QC} \vdash C = C_2^\dagger \circ C_2 \circ C \circ C_1 \circ C_1^\dagger = C_2^\dagger \circ C' \circ C_1^\dagger$. $\boxed{\Longleftarrow}$ Suppose $\mathrm{QC} \vdash C = C_2^\dagger \circ C' \circ C_1^\dagger$, then thanks to Proposition 4, we have $\mathrm{QC} \vdash C' = C_2 \circ C_2^\dagger \circ C' \circ C_1^\dagger \circ C_1 = C_2 \circ C \circ C_1$. □

2.3 2-qubit 1-CNot 0-Swap completeness

In this section, we prove the completeness of QC for a very specific class of circuits, namely the 2-qubit circuits containing one and only one CNot and no Swap. This result will be useful in the following to prove Equation (15) and thus for the completeness of QC. To do so, we conduct a semantic analysis to show that QC contains enough equations to derive any semantically correct equation over 2-qubit 1-CNot 0-Swap circuits. In the following I, X, Z, CNOT, $P(\varphi)$ and $R_X(\theta)$ refers to the unitaries associated with the quantum gates —, $-\boxed{X}-$, $-\boxed{Z}-$, $\begin{smallmatrix}\bullet\\ \oplus\end{smallmatrix}$, $-\boxed{P(\varphi)}-$ and $-\boxed{R_X(\theta)}-$ respectively. First, we prove the following lemmata.

Lemma 1 (1-qubit completeness)**.** QC *is complete for 1-qubit quantum circuits, i.e. for any 1-qubit quantum circuits $C_1, C_2 \in \mathcal{QC}(1,1)$, if $[\![C_1]\!] = [\![C_2]\!]$ then* $\mathrm{QC} \vdash C_1 = C_2$.

Proof. QC contains all the equations of the complete equational theory from [4] acting on at most one qubit. □

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

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

Lemma 2. *Let $U \in \mathcal{U}_2$ be a 1-qubit unitary. If $\langle 0|\,U\,|0\rangle = 0 \vee \langle 1|\,U\,|1\rangle = 0$ then there exist $\varphi, \delta \in \mathbb{R}$ such that $U = e^{i\delta} X P(\varphi)$. Similarly, if $\langle +|\,U\,|+\rangle = 0 \vee \langle -|\,U\,|-\rangle = 0$ then there exist $\theta, \delta \in \mathbb{R}$ such that $U = e^{i\delta} Z R_X(\theta)$.*

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

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

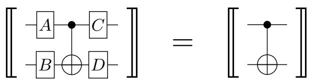
Lemma 3. *For any $\varphi, \varphi', \delta \in \mathbb{R}$, if $P(\varphi)P(\varphi') = e^{i\delta}I$ then $\varphi' = -\varphi \pmod{2\pi}$. Similarly, for any $\theta, \theta', \delta \in \mathbb{R}$, if $R_X(\theta)R_X(\theta') = e^{i\delta}I$ then $\theta' = -\theta \pmod{2\pi}$.*

Proof. For the first statement $P(\varphi)P(\varphi') = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i(\varphi+\varphi')} \end{smallmatrix}\right) = \left(\begin{smallmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{smallmatrix}\right) = e^{i\delta}I$ directly implies that $\varphi' = -\varphi \pmod{2\pi}$. The second statement is reduced to the first one as follows:

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

□

Lemma 4. *Let $A, B, C, D \in \mathcal{U}_2$ be 1-qubit unitaries, if $(C \otimes D) \circ \mathrm{CNOT} \circ (A \otimes B) = \mathrm{CNOT}$ (see the following circuit representation) then there exist $\varphi, \theta, \alpha, \beta, \gamma \in \mathbb{R}$ and $k, l \in \{0, 1\}$ such that $A = e^{i\alpha}X^kP(\varphi)$, $B = e^{i\beta}Z^lR_X(\theta)$, $C = e^{i\gamma}P(-\varphi)Z^lX^k$ and $D = e^{i(-\alpha-\beta-\gamma)}R_X(-\theta)Z^lX^k$.*



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 assignements of $k, l \in \{0, 1\}$.

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

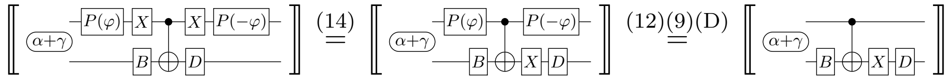
Case $\langle 0|\, A^\dagger\, |0\rangle \neq 0$ and $\langle +|\, B^\dagger\, |+\rangle \neq 0$. It must also be the case that $\langle 0|\, C\, |0\rangle \neq 0$ and $\langle +|\, D\, |+\rangle \neq 0$. Moreover, by unitarity of $A^\dagger$ and $B^\dagger$, we also have $\langle 1|\, A^\dagger\, |1\rangle \neq 0$ 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:

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

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 tacking $k = l = 0$ 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 2 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 3). Then we can use the following derivation to get a new condition satisfied by B and D.



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:

$$e^{i(\alpha+\gamma)}(I \otimes DX) \circ \text{CNOT} \circ (I \otimes B) = \text{CNOT}$$

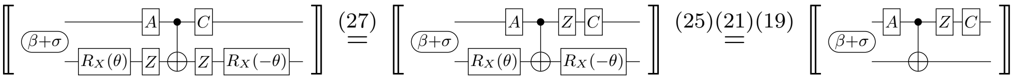
$$\implies \begin{cases} e^{i(\alpha+\gamma)} \langle 0|_1 (I \otimes DX) \circ \text{CNOT} \circ (I \otimes B) |0\rangle_1 = \langle 0|_1 \text{CNOT} |0\rangle_1 \\ e^{i(\alpha+\gamma)} \langle 1|_1 (I \otimes DX) \circ \text{CNOT} \circ (I \otimes B) |1\rangle_1 = \langle 1|_1 \text{CNOT} |1\rangle_1 \end{cases}$$

$$\overset{\text{Claim 1}}{\implies} \begin{cases} e^{i(\alpha+\gamma)} \langle 0|_1 (I \otimes DX) \circ (I \otimes I) \circ (I \otimes B) |0\rangle_1 = \langle 0|_1 (I \otimes I) |0\rangle_1 \\ e^{i(\alpha+\gamma)} \langle 1|_1 (I \otimes DX) \circ (I \otimes X) \circ (I \otimes B) |1\rangle_1 = \langle 1|_1 (I \otimes X) |1\rangle_1 \end{cases}$$

$$\implies \begin{cases} e^{i(\alpha+\gamma)} DXB = I \\ e^{i(\alpha+\gamma)} DXXB = X \end{cases}$$

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 tacking $k = 1$ 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 2 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 3). Then we can use the following derivation to get a new condition satisfied by A and C.



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:

$$e^{i(\beta+\sigma)}(CZ \otimes I) \circ \text{CNOT} \circ (A \otimes I) = \text{CNOT}$$

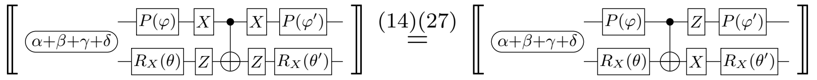
$$\implies \begin{cases} e^{i(\beta+\sigma)} \langle +|_2 (CZ \otimes I) \circ \text{CNOT} \circ (A \otimes I) |+\rangle_2 = \langle +|_2 \text{CNOT} |+\rangle_2 \\ e^{i(\beta+\sigma)} \langle -|_2 (CZ \otimes I) \circ \text{CNOT} \circ (A \otimes I) |-\rangle_2 = \langle -|_2 \text{CNOT} |-\rangle_2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

$$\implies \begin{cases} e^{i(\beta+\sigma)} \langle +|_2 (CZ \otimes I) \circ (I \otimes I) \circ (A \otimes I) |+\rangle_2 = \langle +|_2 (I \otimes I) |+\rangle_2 \\ e^{i(\beta+\sigma)} \langle -|_2 (CZ \otimes I) \circ (Z \otimes I) \circ (A \otimes I) |-\rangle_2 = \langle -|_2 (Z \otimes I) |-\rangle_2 \end{cases}$$

$$\implies \begin{cases} e^{i(\beta+\sigma)} CZA = I \\ e^{i(\beta+\sigma)} CZZA = Z \end{cases}$$

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

Case $\langle 0| \boldsymbol{A}^\dagger |0\rangle = 0$ and $\langle +| \boldsymbol{B}^\dagger |+\rangle = 0$. It must also be the case that $\langle 0| C |0\rangle = 0$ and $\langle +| D |+\rangle = 0$. Lemma 2 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 $\varphi, \varphi', \theta, \theta'$.



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

$$e^{i(\alpha+\beta+\gamma+\delta)}(P(\varphi')Z \otimes R_X(\theta' X) \circ \mathrm{CNOT} \circ (P(\varphi) \otimes R_X(\theta)) = \mathrm{CNOT}$$

$$\implies \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} \langle 0|_1 (P(\varphi')Z \otimes R_X(\theta')X) \circ \mathrm{CNOT} \circ (P(\varphi) \otimes R_X(\theta)) |0\rangle_1 = \langle 0|_1 \mathrm{CNOT} |0\rangle_1 \\ e^{i(\alpha+\beta+\gamma+\delta)} \langle +|_2 (P(\varphi')Z \otimes R_X(\theta')X) \circ \mathrm{CNOT} \circ (P(\varphi)) \otimes R_X(\theta) |+\rangle_2 = \langle +|_2 \mathrm{CNOT} |+\rangle_2 \end{cases}$$

$$\implies \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} \langle 0|_1 (P(\varphi')Z \otimes R_X(\theta')X) \circ (I \otimes I) \circ (P(\varphi) \otimes R_X(\theta)) |0\rangle_1 = \langle 0|_1 (I \otimes I) |0\rangle_1 \\ e^{i(\alpha+\beta+\gamma+\delta)} \langle +|_2 (P(\varphi')Z \otimes R_X(\theta')X) \circ (I \otimes I) \circ (P(\varphi) \otimes R_X(\theta)) |+\rangle_2 = \langle +|_2 (I \otimes I) |+\rangle_2 \end{cases}$$

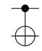
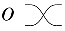
$$\implies \begin{cases} e^{i(\alpha+\beta+\gamma+\delta)} R_X(\theta') X R_X(\theta) = I \\ e^{i(\alpha+\beta+\gamma+\delta)} e^{-i(\theta+\theta')/2} P(\varphi') Z P(\varphi) = I \end{cases}$$

$$\implies \begin{cases} R_X(\theta') = e^{-i(\alpha+\beta+\gamma+\delta)} R_X(-\theta) X \\ P(\varphi') = e^{-i(\alpha+\beta+\gamma+\delta)} e^{i(\theta+\theta')/2} P(-\varphi) Z \end{cases}$$

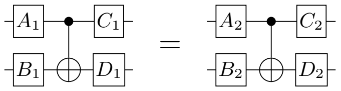
$$\implies \begin{cases} R_X(\theta') = e^{-i(\alpha+\beta+\gamma+\delta)} e^{i\pi/2} R_X(\pi-\theta) \\ P(\varphi') = e^{-i(\alpha+\beta+\gamma+\delta)} e^{i(\theta+\theta')/2} P(\pi-\varphi) \end{cases}$$

$$\overset{\text{Lemma 3}}{\implies} \begin{cases} \theta' = \pi - \theta \pmod{2\pi} \\ \varphi' = \pi - \varphi \pmod{2\pi} \end{cases}$$

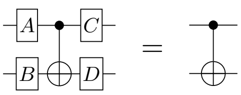
Hence, we get $A = e^{i\alpha}XP(\varphi)$, $B = e^{i\beta}ZR_X(\theta)$, $C = e^{i\gamma}P(\pi-\varphi)X = e^{i\gamma}P(-\varphi)ZX$ and $D = e^{i(-\alpha-\beta-\gamma+\pi/2)}R_X(\pi-\theta)Z = e^{i(-\alpha-\beta-\gamma)}R_X(-\theta)ZX$. Thus we are done by taking $k = l = 1$. □

Theorem 1 (2-qubit 1-CNot 0-Swap completeness)**.** *The equational theory* QC *is complete for 2-qubit 1-CNot 0-Swap circuits, i.e. for any 2-qubit vanilla quantum circuits $C_1, C_2 \in \mathcal{QC}(2,2)$ containing one and only one*  *and no* *, if $[\![C_1]\!] = [\![C_2]\!]$ then* QC $\vdash C_1 = C_2$.

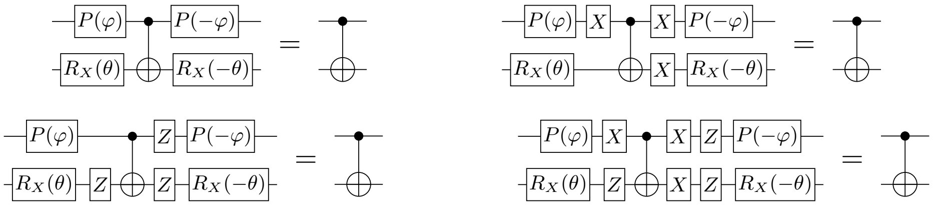
Proof. Thanks to Equations (A), (B) and (23), it is sufficient to show that



is derivable in QC for some 1-qubit circuits A_i , B_i , C_i , D_i whenever the equation is semantically correct. The crossing gate property (Proposition 5) implies that this equation is QC-equivalent to



for any 1-qubit circuits A , B , C , D . Lemma 4 and Lemma 1 together with Equations (A) and (B) implies that this is always the case that this new equation is QC-equivalent to one of the following equations:



We conclude the proof by observing that we can derive all those equations for any $\varphi, \theta \in \mathbb{R}$ using Equations (27),(14),(12),(25),(9),(21),(D), and (19). □

Remark 3. *This result can be generalized to circuit containing at most one CNot and acting on an arbitrary number of qubits. The generalization is tedious as circuits can contain swap gates. The details are given in [3].*

2.4 Simplification of the equational theory

Simplifying $\widehat{\mathrm{QC}}$ into QC amounts to proving the completeness of QC. To to so, we prove in the following propositions that every axioms of $\widehat{\mathrm{QC}}$ that are not in QC are derivable in QC.

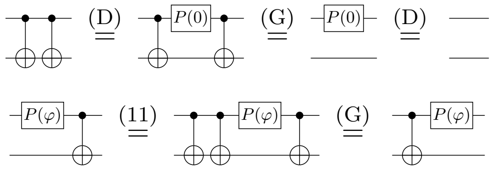
Proposition 6 ([4])**.** *Equations* (9) *and* (10) *of the equational theory* $\widehat{\mathrm{QC}}$ *can be derived in* QC.

Proof. Equations (9) and (10) are consequences of Equation (J). The details are given in [4]. □

It turns out that we can merge Equation (11) and Equation (12) to form Equation (G). In practice one would mostly use Equation (11) and Equation (12) and not Equation (G) to perform circuit transformation, however this simplification is interesting in its own right and leads to a equational theory with one less axiom.

Proposition 7. *Equations* (11) *and* (12) *of the equational theory* $\widehat{\mathrm{QC}}$ *can be derived in* QC.

Proof.

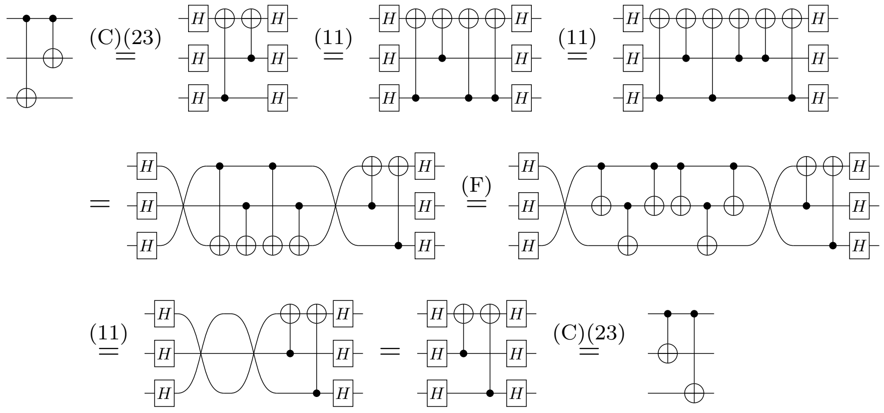


□

Equations (13) and (14) can actually be derived in QC from the other axioms, and thus are not necessary in the equational theory.

Proposition 8. *Equation* (13) *of the equational theory* $\widehat{\mathrm{QC}}$ *can be derived in* QC.

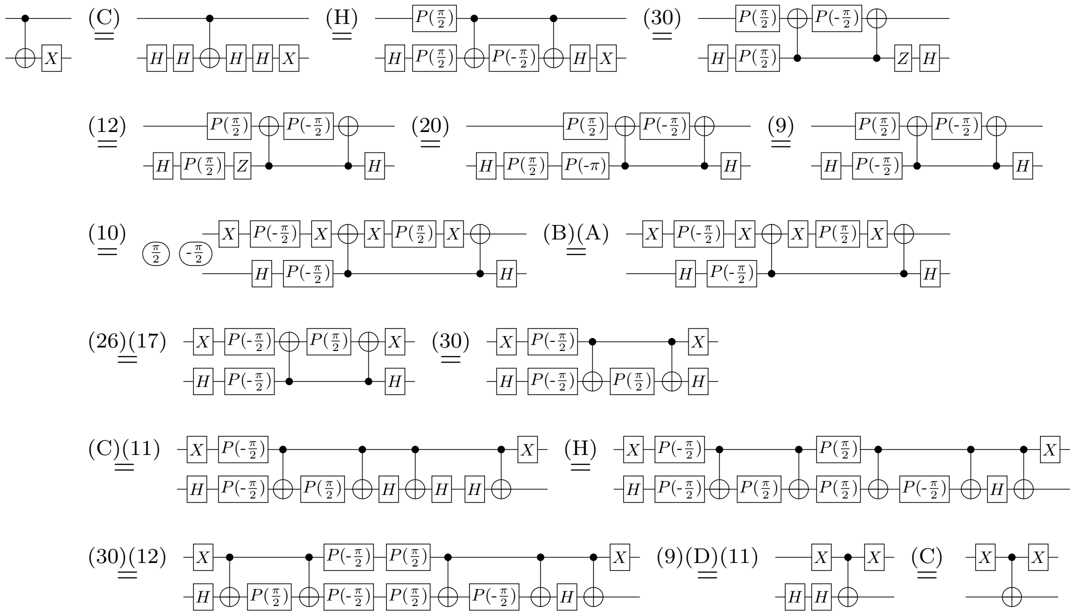
Proof.



□

Proposition 9. *Equation* (14) *of the equational theory* $\widehat{\mathrm{QC}}$ *can be derived in* QC.

Proof.



□

Proposition 10. *Equation* (15) *of the equational theory* $\widehat{\mathrm{QC}}$ *can be derived in* QC.

Proof. Equation (15) is QC-equivalent to an equation whose circuits contain only one CNot. The derivation is given in Appendix B.1. We conclude the proof using the completeness of QC for 2-qubit 1-CNot 0-Swap circuits (Theorem 1). □

Proposition 11. *Equation* (16) *of the equational theory* $\widehat{\mathrm{QC}}$ *can be derived in* QC.

Proof. It turns out that we can use Equation (15) to derive Equation (16) in QC. The derivation is given in Appendix B.2. □

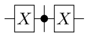
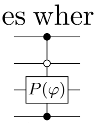
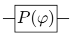
We proved that Equation ($\mathrm{K}^*_{\mathrm{old}}$) can be simplified into Equation (K^*) (where the parameter δ_9 has been removed) in [3]. This observation comes from the optical circuit version of Equation ($\mathrm{K}^*_{\mathrm{old}}$). The proof is very tedious as one have to conduct a huge semantic analysis and distinguish many cases.

Proposition 12 ([3])**.** *Equation* ($\mathrm{K}^*_{\mathrm{old}}$) *of the equational theory* $\widehat{\mathrm{QC}}$ *can be derived in* QC.

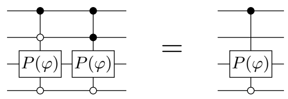
Theorem 2. *The equational theory* QC *is complete for vanilla quantum circuits.*

Proof. Propositions 6, 7, 8, 9, 10, 11 and 12 prove that every axioms of the complete equational theory $\widehat{\mathrm{QC}}$ that are not in QC are provable in QC. □

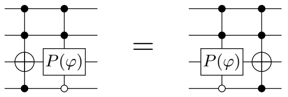
2.5 Bullet-based graphical notation for multi-controlled gates

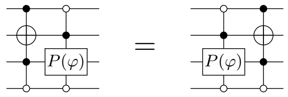
We use the standard bullet-based graphical notation for multi-controlled gates where the *negative control* (or *anti-control*) is a shortcut notation for  . For instance,  stands for the gate  on the third qubit positively controlled by the first and fourth qubits and negatively controlled by the second qubit. According to [4] 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 ($\circ$) and refers to Propositions 15, 16 and 17 (together with Propositions 10 and 11 in some cases) of [4].

Chapter 3

Quantum circuits with ancillae

The model $\mathcal{QC}_{\mathsf{H}}$ of quantum circuits with ancillae is more general than the model $\mathcal{QC}$ of vanilla quantum circuits. One could try to take advantage of the possibility to add temporary additional work space. Intuitively, ancillae allow us to put information on temporary wires. Thus, expressing quantum evolutions with this model could leads to simpler and maybe more intuitive circuits. In this chapter we construct a complete equational theory for quantum circuits with ancillae where the last intricate axiom is drastically simplified.

3.1 Equational theory for quantum circtuits with ancillae

We use QC_{H} (defined in Figure 3.1) as an equational theory for $\mathcal{QC}_{\mathsf{H}}$ (see Definition 12). QC_{H} is sound as every axiom is semantically correct. This chapter is dedicated to showing its completeness. The main difference with the equational theory QC for vanilla quantum circuits is the addition of Equations (L), (M) and (N), which are new equations explaining the behaviour of the new generators $\vdash$ and $\dashv$. The second difference is that Equation (K*) has been replaced by its 2-qubit version, namely Equation (K^2).

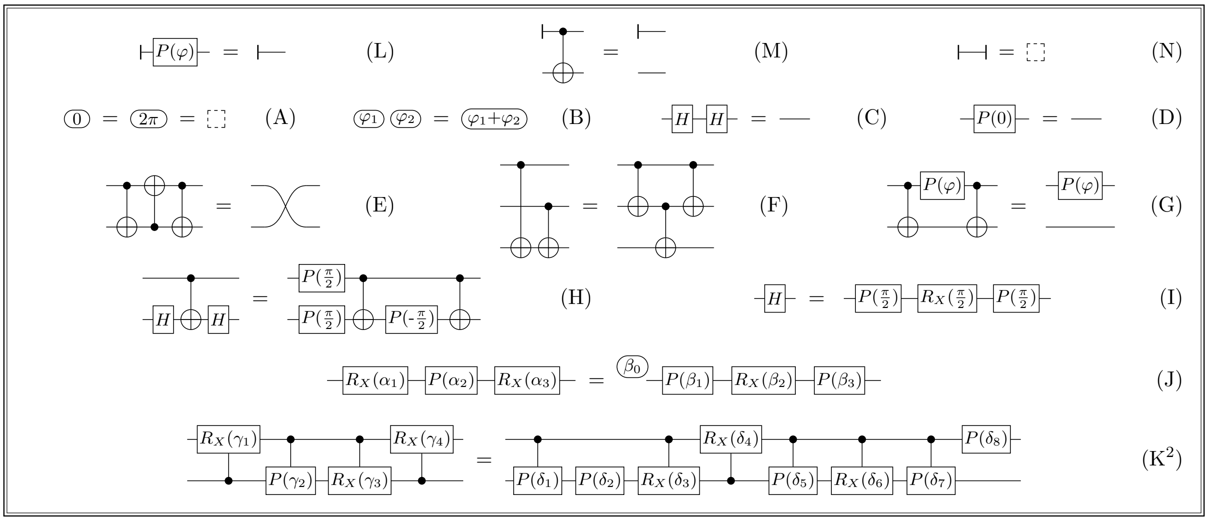


Figure 3.1: Equational theory QC_{H}. It contains all the equations of QC where Equation (K*) has been replaced by Equation (K^2), together with Equation (L) (defined for any $\varphi \in \mathbb{R}$), Equation (M) and Equation (N), which are a new equations associated with the new generators.

We can prove some new identities illustrating the expected behaviour of ancillae with controlled gates (see Figure 3.2).

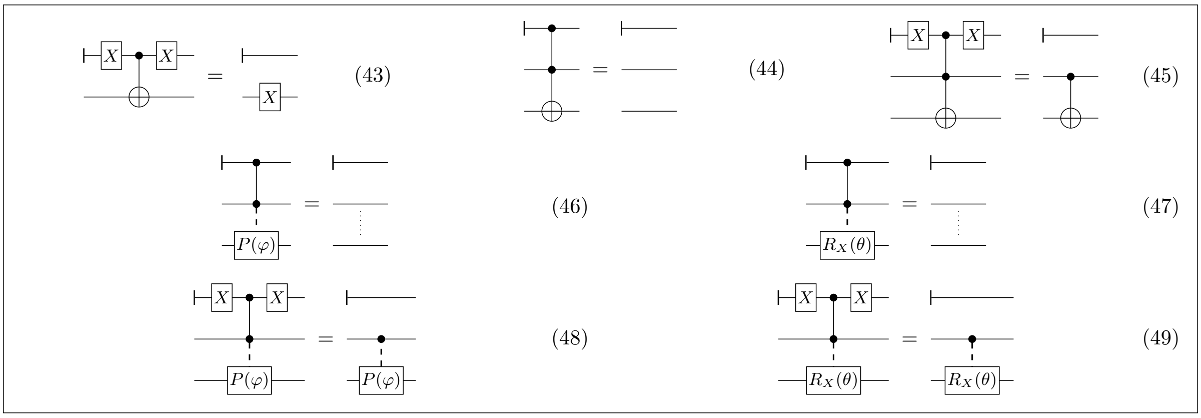


Figure 3.2: Some identities provable in QC_{H} defined for any $\varphi, \theta \in \mathbb{R}$. All the proofs are given in Appendix A.4. Note that the proofs do not use Equation (K^2).

As a step toward the completeness of QC_{H}, we first use a result from [3] that prove the completeness of $\widehat{\mathrm{QC}}_{\mathsf{H}}$, the equational theory QC augmented with the new equations associated to the new generators (Equations (L), (M) and (N)).

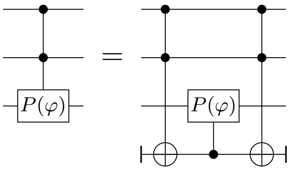
Theorem 3 ([3])**.** *The equational theory* $\widehat{\mathrm{QC}}_{\mathsf{H}}$ *composed of the axioms of* QC *together with Equations* (L)*,* (M) *and* (N) *is complete for quantum circuits with ancillae.*

Proof. We proved this result in [3]. The proof goes in two steps: (1) First we defined an intermediate model of quantum circuits that allows qubit intitialization. The model is defined by adding the generator $\vdash$ to $\mathcal{QC}$. Then, by conducting a matrix analysis, one can show that adding Equation (L) and Equation (M) to a complete equational theory for $\mathcal{QC}$ gives a complete equational theory for the intermediate model. (2) Adding the generator $\dashv$ to the intermediate model leads exactly to $\mathcal{QC}^*_{\mathsf{H}}$ and one can show that adding Equation (N) to a complete equational theory for the intermetiate model gives a complete equational theory for $\mathcal{QC}_{\mathsf{H}}$. The detailed proof is given in [3]. □

All the axioms of QC are also in QC_{H} except Equation (K^*), which as been replaced by Equation (K^2). In order to show that QC_{H} is complete, using Theorem 3, we then need to prove that Equation (K^*) is derivable within QC_{H}. To do so, we introduce (in the next section) new definitions for multi-controlled gates that use ancillae.

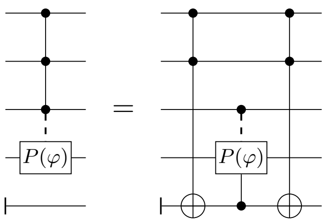
3.2 Alternative definitions of multi-controlled gates

The definition of the n+1-controlled phase gate (Equation (8)) with angle $\varphi \in \mathbb{R}$ uses the n-controlled phase gate with angle $\frac{\varphi}{2}$. The same is true for the n+1-controlled X-rotation gate (Equation (4)). More generally, one step in the inductive definitions of multi-controlled gates divides the angles by 2. This is not a desirable property because, intuitively, it prevents us to conduct inductions on multi-controlled gates. Fortunately, using ancillae we can alternatively define multi-controlled gates without dividing the angles. Indeed, we can use the Toffoli gate to push the value of control qubits into fresh ancillae. For instance, one can define the 2-controlled phase gate as follows.

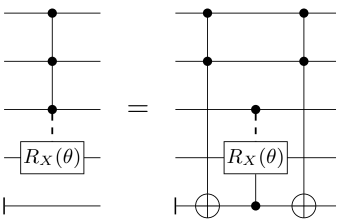


More generally,

Proposition 13 (Toffoli-based multi-controlled gates definitions)**.** *Equation* (50) *and Equation* (51) *can be derived in* QC_{H}*.*



(50)



(51)

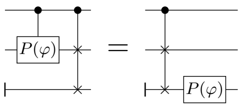
Proof. By induction on the number of qubits. The proof is given in Appendix C. □

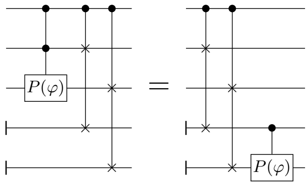
3.3 Deriving Equation (K*) from Equation (K^2)

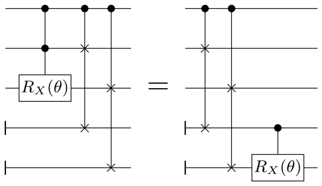
Let (K^n) be Equation (K*) acting on n qubits for any $n \geq 2$. To prove Equation (K*) within QC_{H} we proceed by induction (see Proposition 15) whose base case, Equation (K^3), is proved independently in Proposition 14.

Proposition 14. *Equation* (K^3) *is derivable in* QC_{H}*.*

Proof. We show that (K^3) can be derived from (K^2) by using 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). To do so, we use the following equations:







The detailed proof is given in C.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). □

Proposition 15. *Equation* (K*) *is derivable in* QC_{H}*.*

Proof. Equation (K^2) is trivially provable in QC_{H} as it is an axiom. We prove that (K^n) is derivable in QC_{H} for any $n \geq 3$ by induction on n (with base case proved in Proposition 14) using the alternative definitions of multi-controlled gates (Proposition 13), which allows us to construct an instance of the LHS circuit of (K^n) from the LHS circuit of (K^{n+1}). The detailed proof is given in C.3. □

Theorem 4. *The equational theory* QC_{H} *is complete for quantum circuits with ancillae.*

Proof. According to Theorem 3 $\widehat{\mathrm{QC}}_{\mathsf{H}}$ is complete for quantum circuits with ancillae. Equation (K*) is the only rule of $\widehat{\mathrm{QC}}_{\mathsf{H}}$ that is not in QC_{H} and is provable in QC_{H}. □

Chapter 4

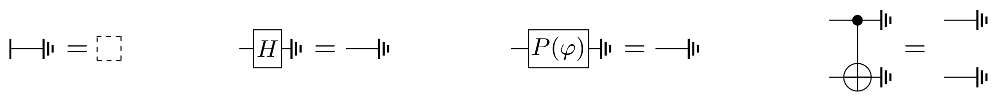
Discussion

The original complete equational theory introduced in [4] is composed of eighteen axioms. In this master's thesis and in [3] we simplied it into an equational theory composed of eleven axioms where two out of the three most intricate rules has been removed. The question of minimality is legitimate and could be a part of the futur work: Can we simplify QC even more? How many equations should contain a complete equational theory? Can we find a better set of equations that form a complete equational theory? Moreover, we can wonder if the most intricate rule, namely Equation (K*), can be simplied in the vanilla model. Or maybe we can replace it by some more intuitive rules. Many ideas has been studied in this regard (especially using an universal 2-qubit circuit form [20] to simplify the composition of multi-controlled gates) but none of them has been successful yet.

About the use of such equational theories, one could try to perform some circuit simplification, by turning a complete equational theory into a rewritting system (possibly confluent and terminating). We can also wonder what are the complexity limitations of such equational theories: How many steps do we have to do to transform a circuit into another semantically equivalent circuit?

The models introduced in this work are universal models where the angles have arbitrary real values. In practice, some fragments such as Clifford+T are of interest. In particular, finding a complete equational theory for this fragment could be a significant result. It seems like the only axioms that are not well defined for the Clifford+T fragment are Equation (J) and Equation (K*) (or Equation (K^2) for QC_{H}). How to construct a complete equational theory for Clifford+T?

One could also extend the simplifications done in the master's thesis to other quantum circuits models. For instance, we can define a new model for quantum circuits, namely quantum circuits with discard for completely positive map, denoted $\mathcal{QC}_{\dashv\Vert}$ [3]. This model is $\mathcal{QC}_{\mathsf{H}}$ where the generator $\dashv : 1 \to 0$ is replaced by $\dashv\Vert : 1 \to 0$. Contrary to quantum circuits with ancillae where the destruction generator $\dashv$ can only be applied on ancilla qubits in the $|0\rangle$-state, in $\mathcal{QC}_{\dashv\Vert}$ any qubit can be discarded whatever its state is. This implies that the evolution represented by a $\mathcal{QC}_{\dashv\Vert}$-circuit is not pure anymore. As a consequence the semantics is a completely positive trace-preserving (CPTP) map acting on density matrices. This model is interesting because it allows one to model measurements and classical feedback. Moreover, adding the equations



together with Equations (L) and (M) to a complete equational theory for vanilla quantum circuit gives a complete equational theory $\mathrm{QC}_{\dashv\Vert}$ for $\mathcal{QC}_{\dashv\Vert}$. The details are given in [3]. The important observation is that the simplification of (K*) done for QC_{H} also holds for $\mathrm{QC}_{\dashv\Vert}$.

Bibliography

[1] Matthew Amy, Jianxin Chen, and Neil J. Ross. “A Finite Presentation of CNOT-Dihedral Operators”. In: *Electronic Proceedings in Theoretical Computer Science* 266 (Feb. 2018), pp. 84–97. DOI: 10.4204/eptcs.266.5. URL: https://doi.org/10.4204%2Feptcs.266.5.

[2] Xiaoning Bian and Peter Selinger. “Generators and relations for 2-qubit Clifford+T operators”. In: *arXiv preprint arXiv:2204.02217* (2022).

[3] Alexandre Clément, Noé Delorme, Simon Perdrix, and Renaud Vilmart. *Simple Complete Equational Theories for Quantum Circuits with Ancillae or Partial Trace.* 2023. URL: https://arxiv.org/abs/2303.03117.

[4] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. *A Complete Equational Theory for Quantum Circuits.* 2022. URL: https://arxiv.org/abs/2206.10577.

[5] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. *LOv-Calculus: A Graphical Language for Linear Optical Quantum Circuits.* 2022. URL: https://arxiv.org/abs/2204.11787.

[6] Robin Cockett and Cole Comfort. “The Category TOF”. In: *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018* (Halifax, Canada, June 3–7, 2018). Ed. by Peter Selinger and Giulio Chiribella. Vol. 287. EPTCS. 2019, pp. 67–84.

[7] Robin Cockett, Cole Comfort, and Priyaa Srinivasan. “The Category CNOT”. In: *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018* (Halifax, Canada, June 3–7, 2018). Ed. by Peter Selinger and Giulio Chiribella. Vol. 287. EPTCS. 2019, pp. 258–293. DOI: 10.4204/EPTCS.266.18.

[8] Bob Coecke and Quanlong Wang. “ZX-rules for 2-qubit Clifford+T quantum circuits”. In: *International Conference on Reversible Computation.* Springer. 2018, pp. 144–161.

[9] D. Deutsch. “Quantum Computational Networks”. In: *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* 425.1868 (1989), pp. 73–90. (Visited on 01/20/2023).

[10] Toshinari Itoko, Rudy Raymond, Takashi Imamichi, and Atsushi Matsuo. “Optimization of quantum circuit mapping using gate transformation and commutation”. In: *Integration* 70 (2020), pp. 43–50.

[11] Kazuo Iwama, Yahiko Kambayashi, and Shigeru Yamashita. “Transformation rules for designing CNOT-based quantum circuits”. In: *Proceedings of the 39th annual Design Automation Conference.* 2002, pp. 419–424.

[12] Stephen Lack. “Composing PROPs”. In: *Theory and Applications of Categories.* Vol. 13. 9. 2004, pp. 147–163. URL: http://www.tac.mta.ca/tac/volumes/13/9/13-09abs.html.

[13] Justin Makary, Neil J. Ross, and Peter Selinger. “Generators and Relations for Real Stabilizer Operators”. In: *Proceedings of the 18th International Conference on Quantum Physics and Logic, QPL 2021* (Gdansk, Poland, and online, June 7–11, 2021). Ed. by Chris Heunen and Miriam Backens. Vol. 343. EPTCS. 2021, pp. 14–36. DOI: `10.4204/EPTCS.343.2`.

[14] Dmitri Maslov, Christina Young, D Michael Miller, and Gerhard W Dueck. “Quantum circuit simplification using templates”. In: *Design, Automation and Test in Europe*. IEEE. 2005, pp. 1208–1213.

[15] 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*. 2003, pp. 318–323.

[16] Yunseong Nam, Neil J Ross, Yuan Su, Andrew M Childs, and Dmitri Maslov. “Automated optimization of large quantum circuits with continuous parameters”. In: *npj Quantum Information* 4.1 (2018), pp. 1–12.

[17] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2002. ISBN: 0-521-63503-9.

[18] nLab authors. *PROP*. `https://ncatlab.org/nlab/show/PROP`. Revision 28. Mar. 2023.

[19] André Ranchin and Bob Coecke. “Complete set of circuit equations for stabilizer quantum mechanics”. In: *Physical Review A* 90.1 (2014), p. 012109.

[20] Vivek V. Shende, Igor L. Markov, and Stephen S. Bullock. “Minimal universal two-qubit controlled-NOT-based circuits”. In: *Physical Review A* (June 2004). URL: `https://doi.org/10.1103%2Fphysreva.69.062321`.

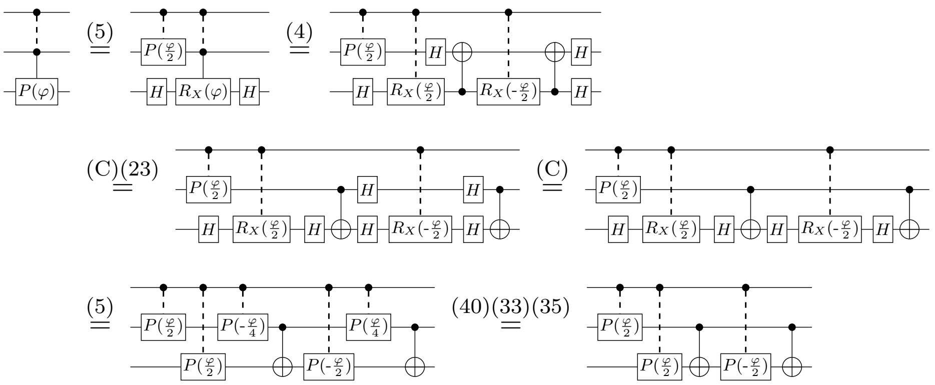
Appendix A

Proofs of circuits identities

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

A.1 Proofs of the equations of Figure 1.1

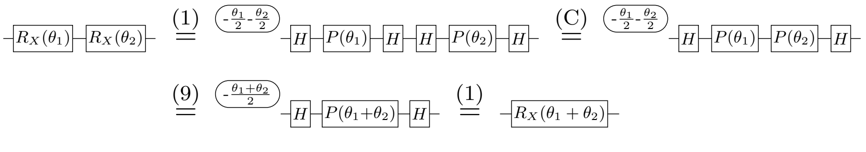
Proof of Equation (8).



□

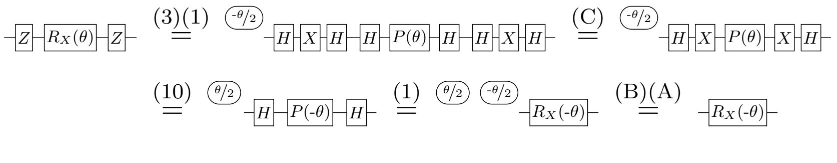
A.2 Proofs of the equations of Figure 2.3

Proof of Equation (21).



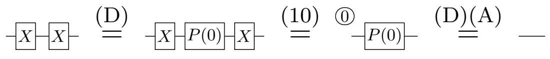
□

Proof of Equation (22).



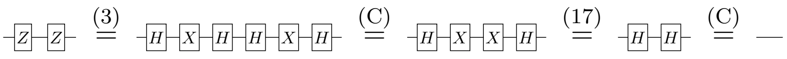
□

Proof of Equation (17).



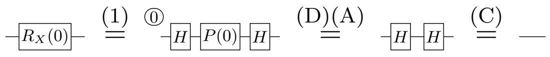
□

Proof of Equation (18).



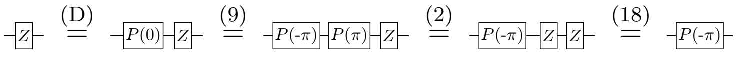
□

Proof of Equation (19).



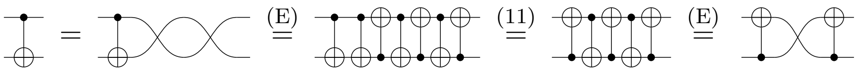
□

Proof of Equation (20).



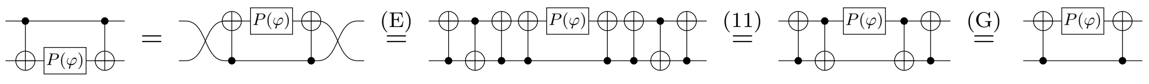
□

Proof of Equation (24).



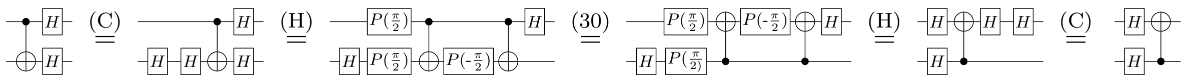
□

Proof of Equation (30).



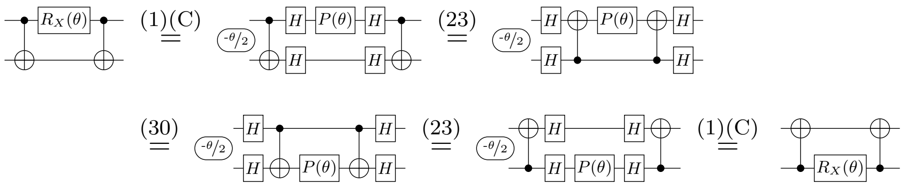
□

Proof of Equation (23).



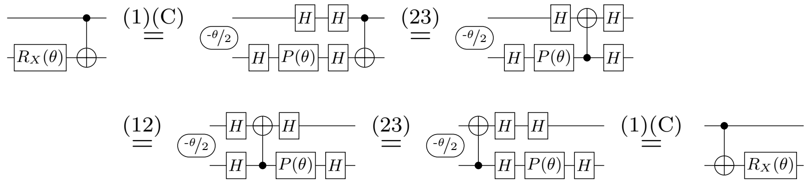
□

Proof of Equation (31).



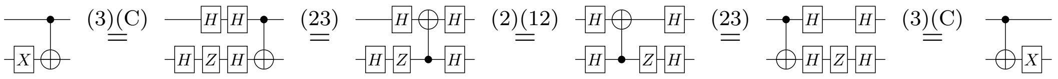
□

Proof of Equation (25).



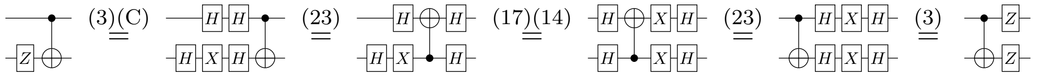
□

Proof of Equation (26).



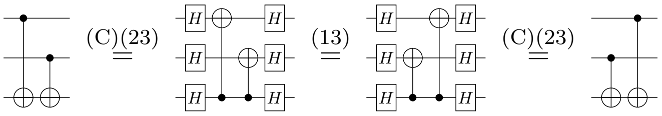
□

Proof of Equation (27).



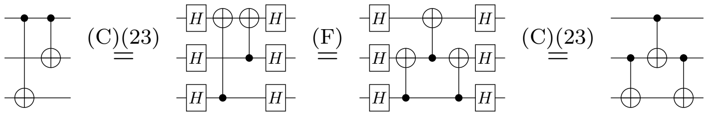
□

Proof of Equation (28).



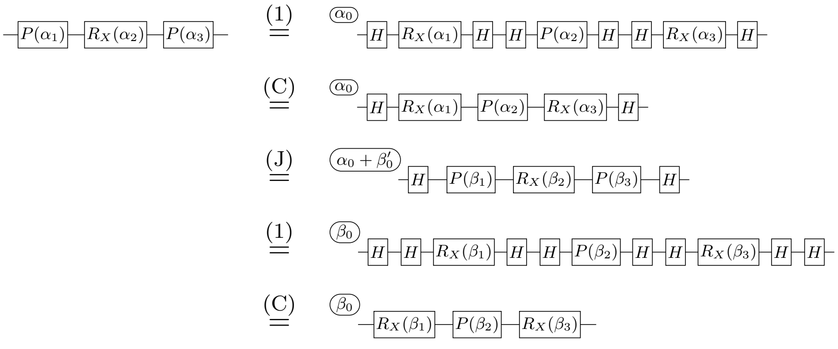
□

Proof of Equation (29).



□

Proof of Equation (32).

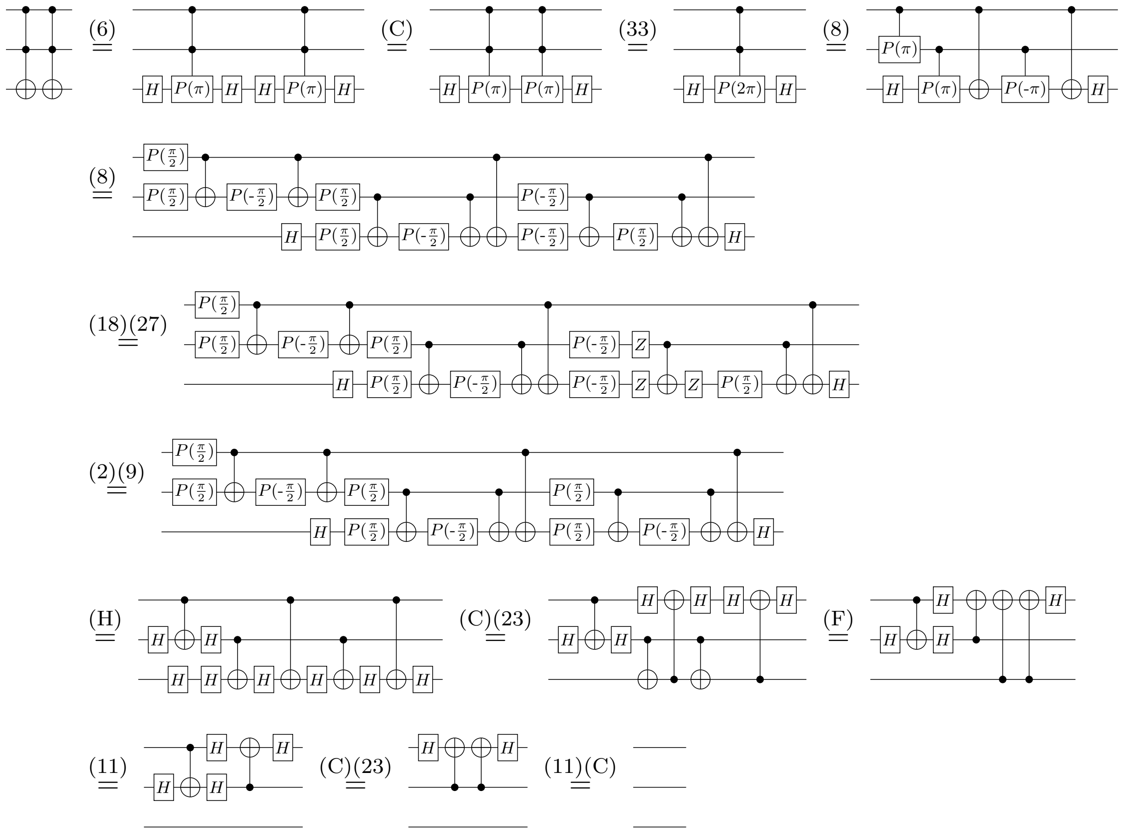

$P(\alpha_1)$ $R_X(\alpha_2)$ $P(\alpha_3)$
(1) =
α_0
H $R_X(\alpha_1)$ H H $P(\alpha_2)$ H H $R_X(\alpha_3)$ H
(C) =
α_0
H $R_X(\alpha_1)$ $P(\alpha_2)$ $R_X(\alpha_3)$ H
(J) =
$\alpha_0 + \beta_0'$
H $P(\beta_1)$ $R_X(\beta_2)$ $P(\beta_3)$ H
(1) =
β_0
H H $R_X(\beta_1)$ H H $P(\beta_2)$ H H $R_X(\beta_3)$ H H
(C) =
β_0
$R_X(\beta_1)$ $P(\beta_2)$ $R_X(\beta_3)$

With $\alpha_0 \coloneqq \frac{\alpha_1-\alpha_2+\alpha_3}{2}$ and $\beta_0 \coloneqq \alpha_0 + \beta_0' + \frac{\beta_1-\beta_2+\beta_3}{2}$. □

A.3 Proofs of the equations of Figure 2.4

Equations (33), (34), (35) and (36) are proved in Proposition 13 of [4]. Equation (37) is proved in Lemma 47 of [4]. Equation (38) is proved in Lemma 53 of [4]. Equation (40) is proved in Proposition 12 of [4]. Equations (41) and (42) are proved in Proposition 11 of [4]. The proofs also hold for the equational theory QC because all the equations used are provable in QC.

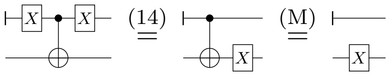
Proof of Equation (39).



□

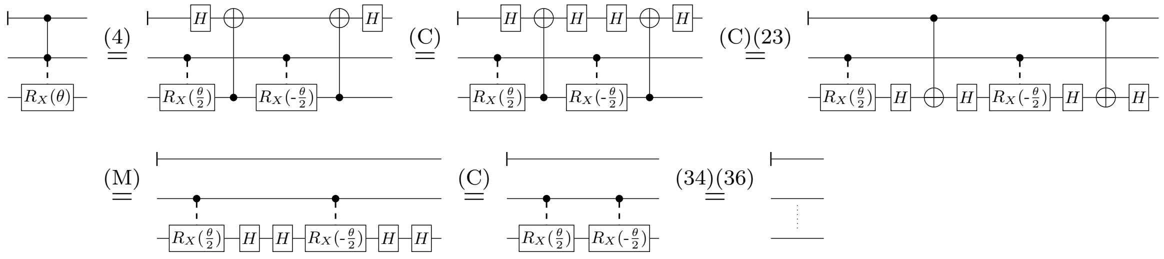
A.4 Proofs of the equations of Figure 3.2

Proof of Equation (43).



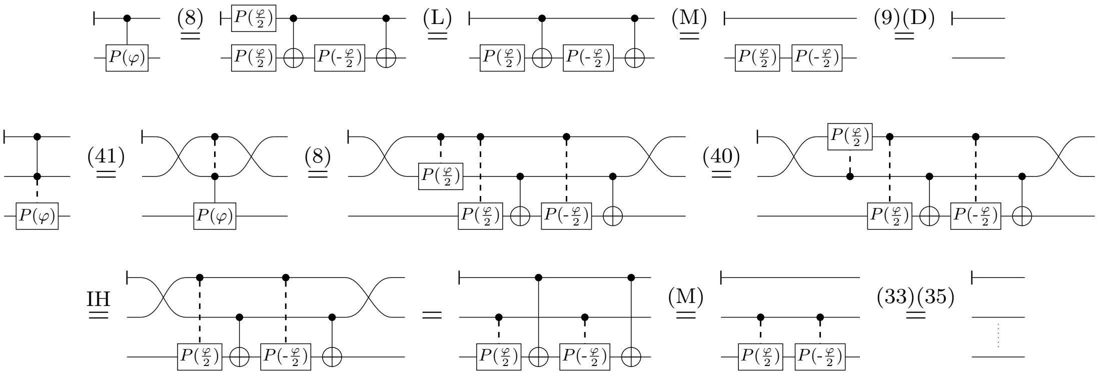
□

Proof of Equation (47).



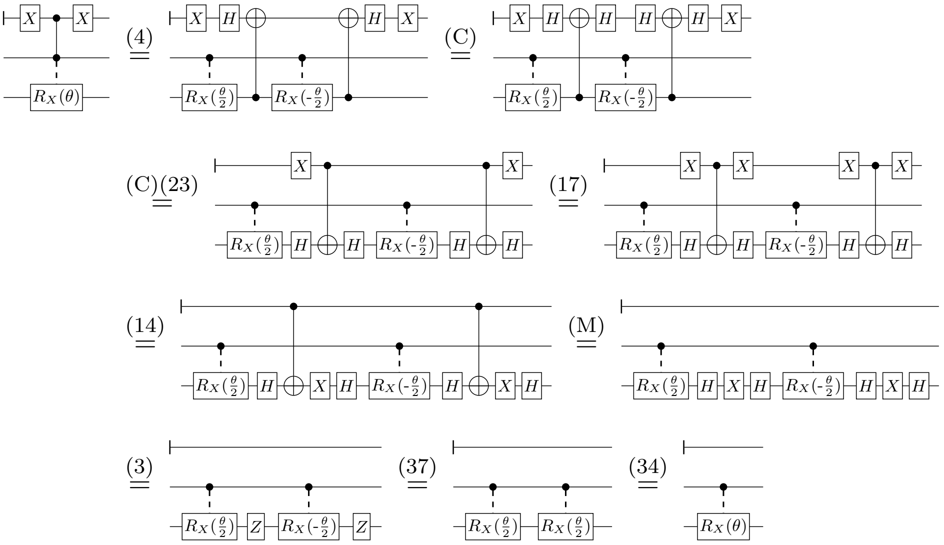
□

Proof of Equation (46). By induction on the number of controls with base case $n = 1$ control.



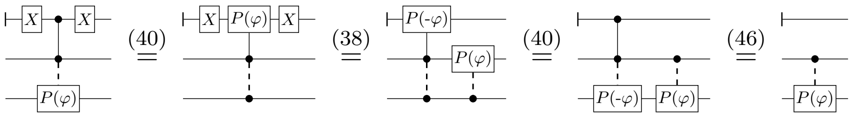
□

Proof of Equation (49).



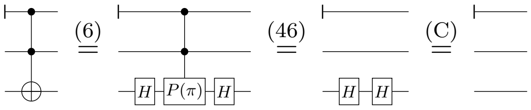
□

Proof of Equation (48).



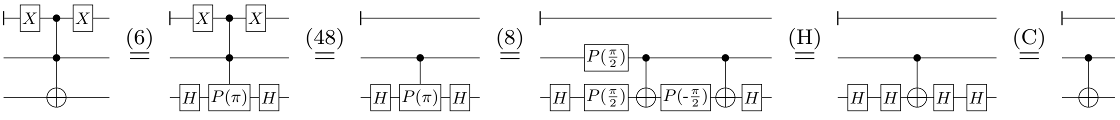
□

Proof of Equation (44).



□

Proof of Equation (45).



□

Appendix B

Proofs of Equations (15) and (16)

B.1 Proof of Equation (15)

Lemma 5. *Equation* (52) *can be derived in* QC.

$$-\boxed{H}- \;=\; \textcircled{$\frac{\pi}{4}$}-\boxed{R_X(\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{R_X(\tfrac{\pi}{2})}- \tag{52}$$

Proof.

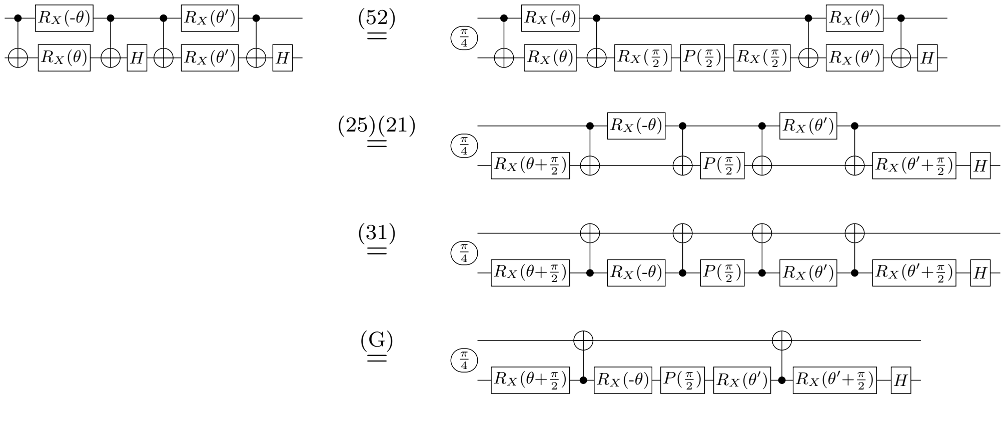
$$\begin{aligned}
-\boxed{H}- &\overset{(\mathrm{D})(9)(19)(21)}{=} -\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{R_X(\text{-}\tfrac{\pi}{2})}-\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{R_X(\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{H}- \\
&\overset{(\mathrm{I})}{=} -\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{R_X(\text{-}\tfrac{\pi}{2})}-\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{H}-\boxed{H}- \\
&\overset{(\mathrm{C})}{=} -\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{R_X(\text{-}\tfrac{\pi}{2})}-\boxed{P(\text{-}\tfrac{\pi}{2})}- \\
&\overset{(1)}{=} \textcircled{$\frac{\pi}{4}$}-\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{H}-\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{H}-\boxed{P(\text{-}\tfrac{\pi}{2})}- \\
&\overset{(\mathrm{I})}{=} \textcircled{$\frac{\pi}{4}$}-\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{R_X(\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{P(\text{-}\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{R_X(\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{P(\text{-}\tfrac{\pi}{2})}- \\
&\overset{(9)(\mathrm{D})}{=} \textcircled{$\frac{\pi}{4}$}-\boxed{R_X(\tfrac{\pi}{2})}-\boxed{P(\tfrac{\pi}{2})}-\boxed{R_X(\tfrac{\pi}{2})}-
\end{aligned}$$

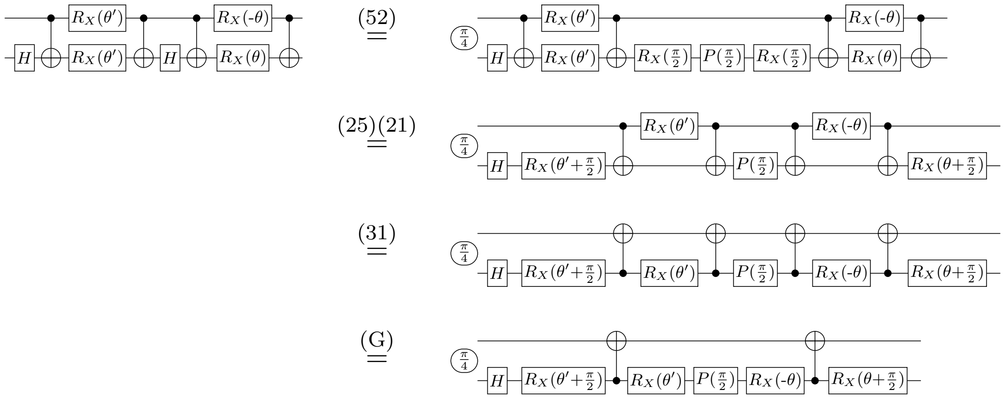
□

Lemma 6. *For any 1-qubit circuit* $-\boxed{C}-$ $\in \mathcal{QC}$, *there exists* $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \beta_0, \beta_1, \beta_2, \beta_3 \in \mathbb{R}$ *such that* $\mathrm{QC} \vdash -\boxed{C}- = \textcircled{α_0}-\boxed{R_X(\alpha_1)}-\boxed{P(\alpha_2)}-\boxed{R_X(\alpha_3)}-$ *and* $\mathrm{QC} \vdash -\boxed{C}- = \textcircled{β_0}-\boxed{P(\beta_1)}-\boxed{R_X(\beta_2)}-\boxed{P(\beta_3)}-$.

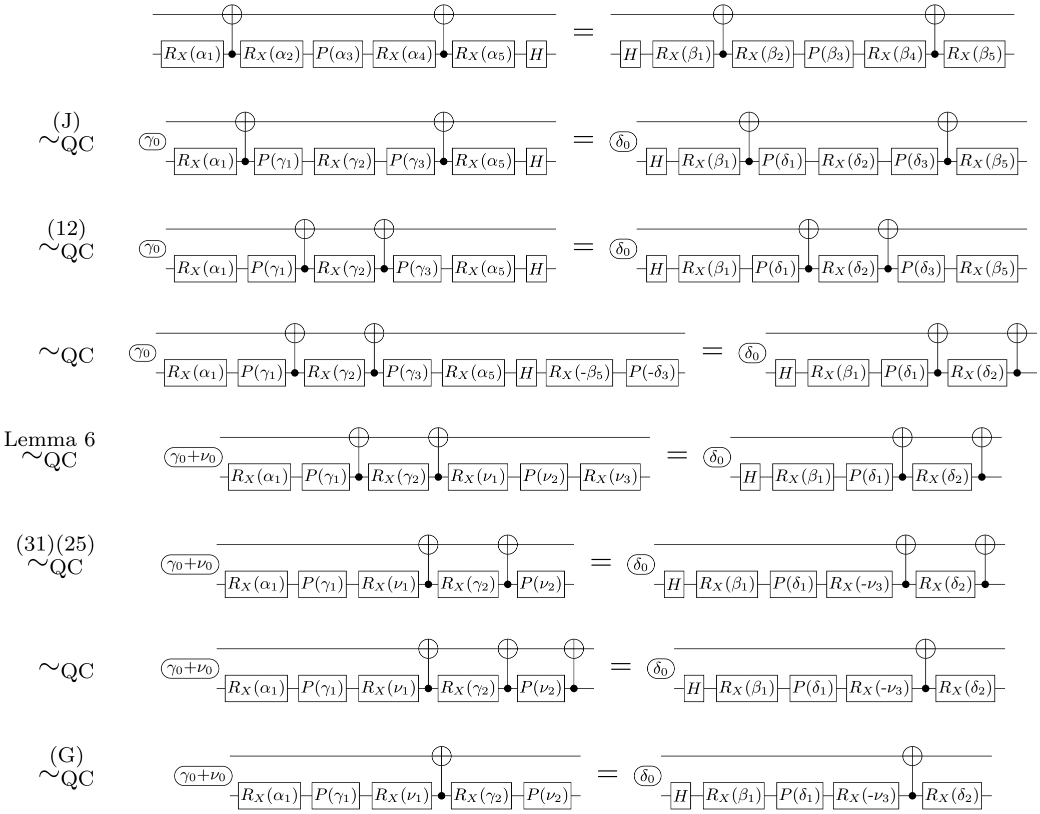
Proof. Whatever $-\boxed{C}-$ is, we can always apply Equations (I), (J), (32), (A) and (B). □

Proof of Equation (15). First, we do some steps on the LHS and RHS circuits.



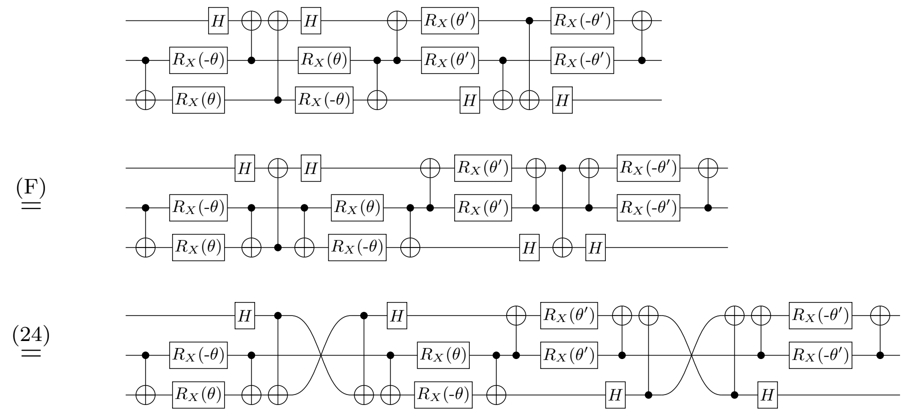


Equation (15) is QC-equivalent to the following equations for some $\alpha_i, \beta_i, \gamma_i, \delta_i, \nu_i \in \mathbb{R}$. The last equation is over 1-CNot circuits, which together with Theorem 1 conclude the proof.

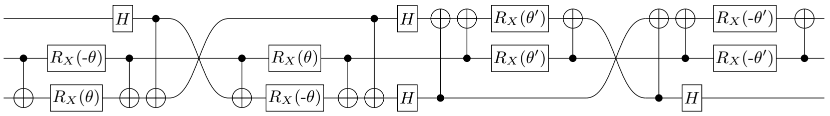


□

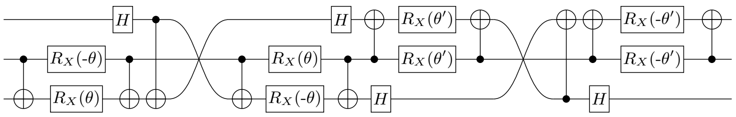
B.2 Proof of Equation (16)



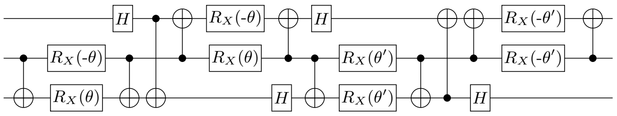
$\overset{(28)(25)}{=}$



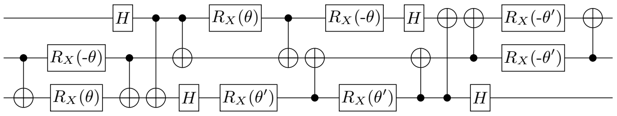
$\overset{(23)(11)}{=}$



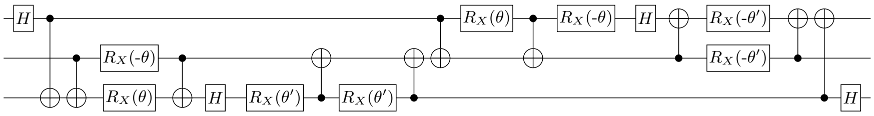
$=$



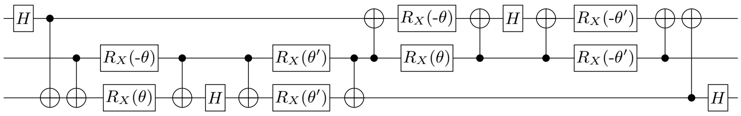
$\overset{(25)(31)}{=}$



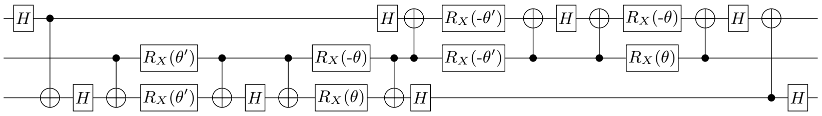
$\overset{(28)(25)}{=}$



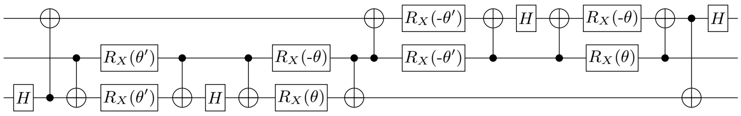
$\overset{(31)(25)}{=}$



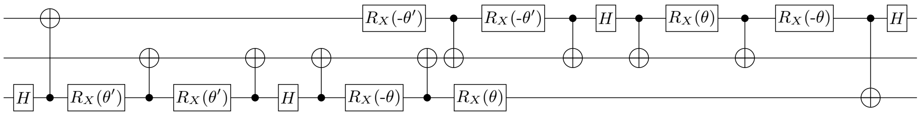
$\overset{(15)}{=}$



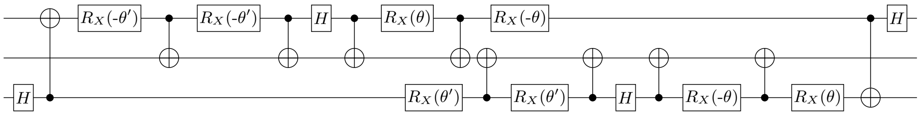
$\overset{(C)(23)}{=}$



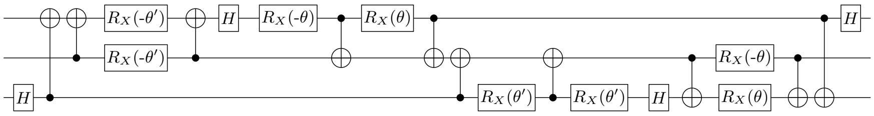
$\overset{(25)(31)}{=}$



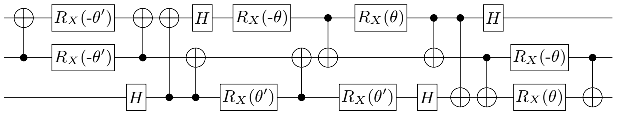
$\overset{(28)}{=}$



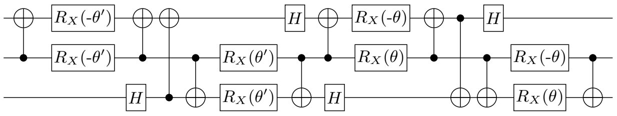
$\overset{(25)(31)}{=}$



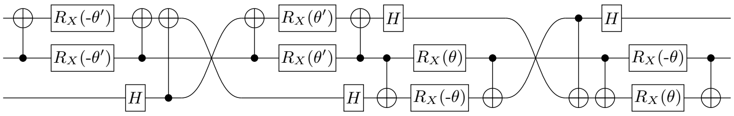
$\overset{(28)(25)(28)}{=}$



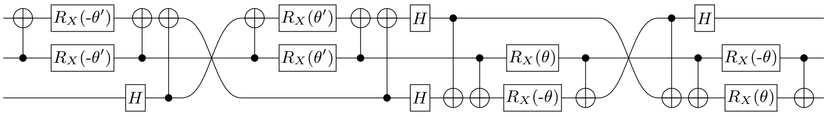
$\overset{(25)(31)}{=}$



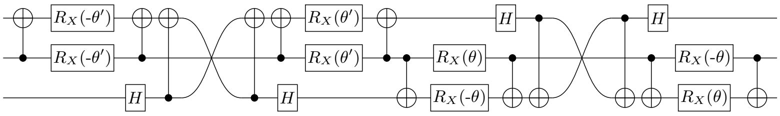
$=$



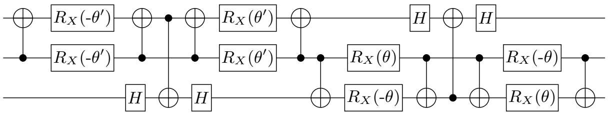
$\overset{(11)(23)}{=}$



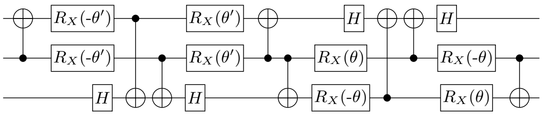
$\overset{(28)(25)}{=}$



$\overset{(24)}{=}$



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

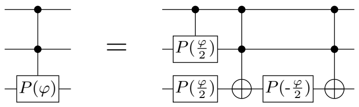


Appendix C

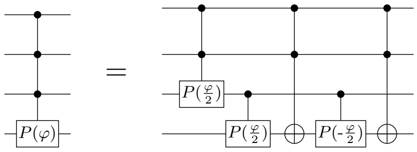
Proofs used for deriving (K*) in $\mathsf{QC_H}$

C.1 Proof of alternative definitions of multi-controlled gates

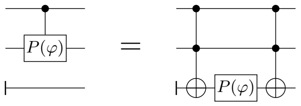
First, we derive the following equations. Equations (53) and (54) are alternative definitions of 2-controlled and 3-controlled phase gates. Equation (55) tells us how we can express a simply controlled phase gate with Toffoli gates and one 1-qubit phase gate using one ancilla.



(53)

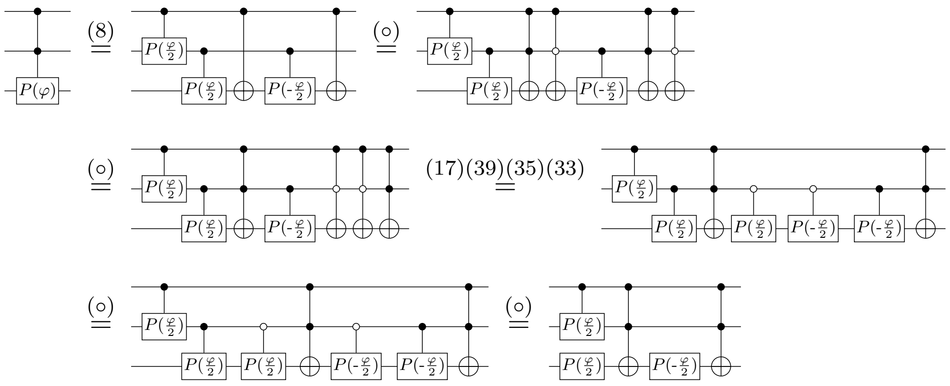


(54)



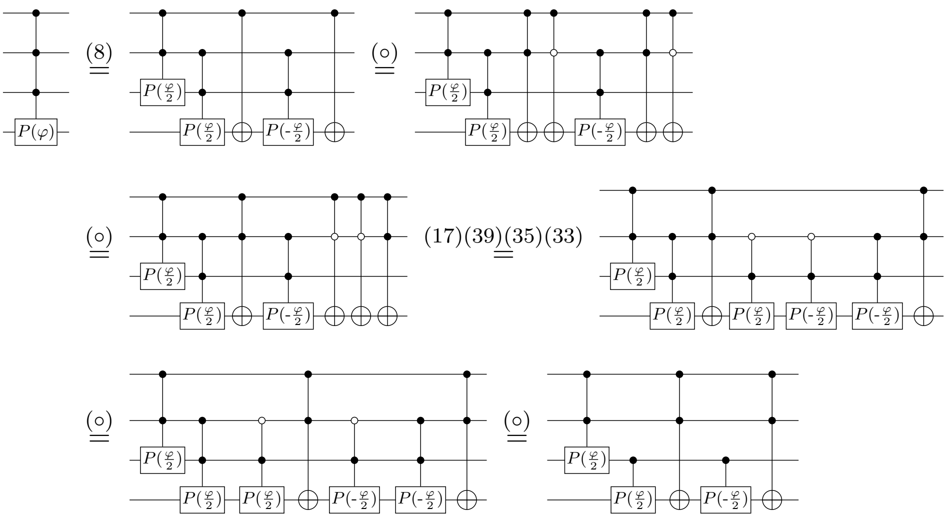
(55)

Proof of Equation (53).



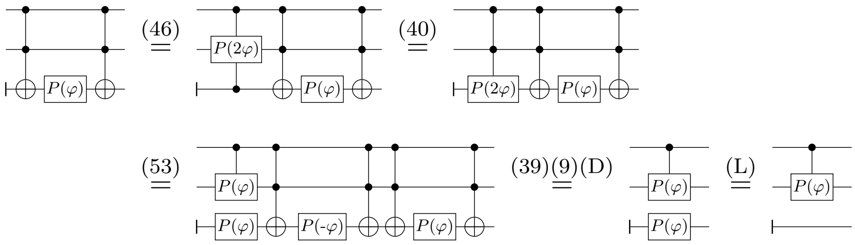
□

Proof of Equation (54).



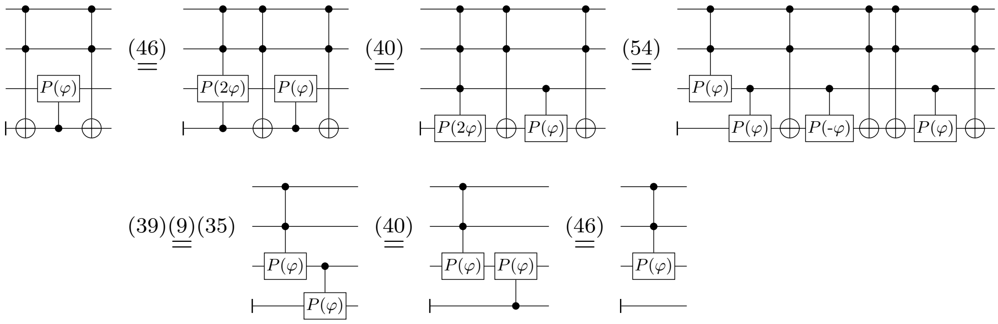
□

Proof of Equation (55).

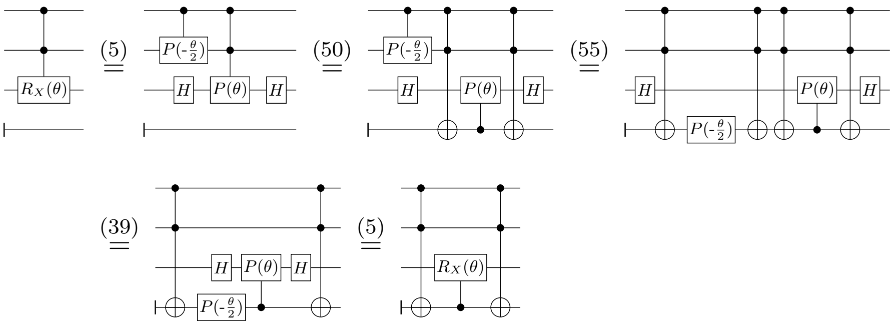


□

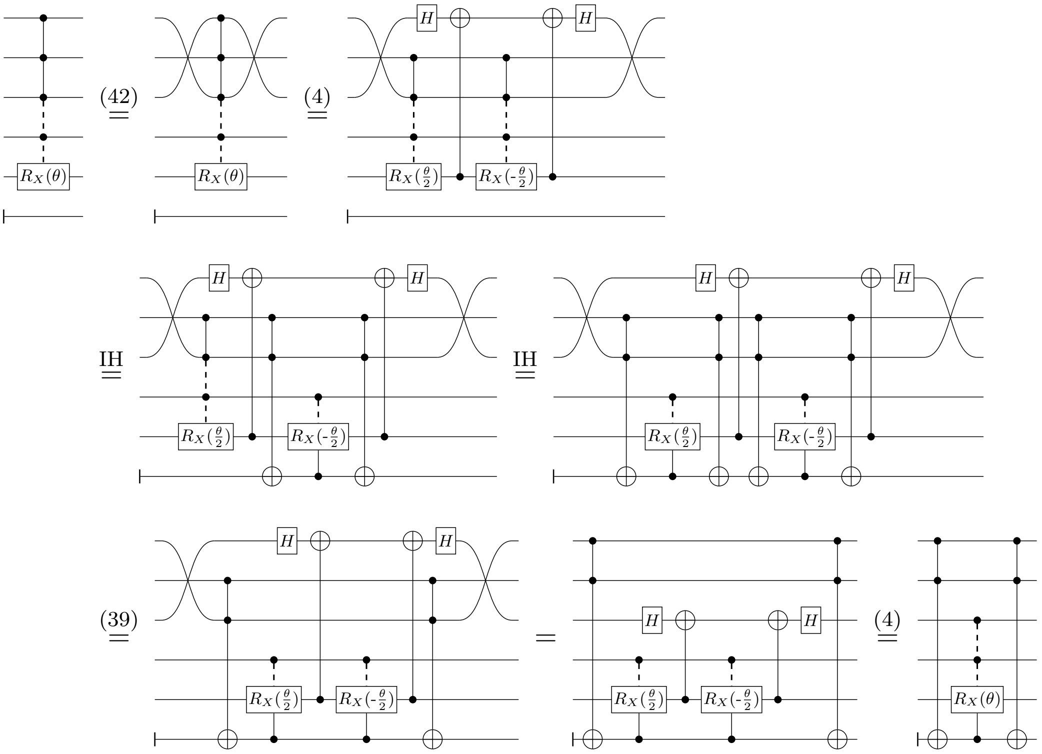
Proof of Equation (50) *and Equation* (51). We prove Equations (50) and (51) by induction on the number of qubits, whose base cases contains $n = 4$ qubits. The base case for Equations (50) can be derived as follows.



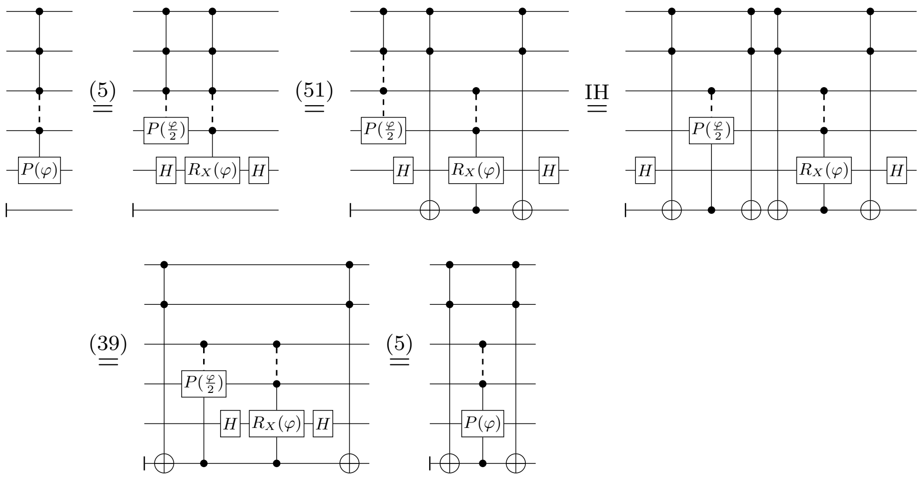
The base case for Equations (51) can be derived as follows.



The induction step for Equation (51) can be derived as follows.

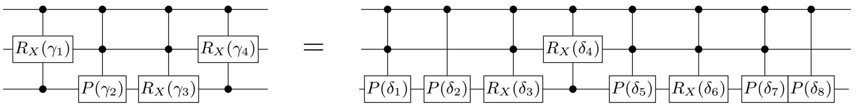


The induction step for Equation (50) can be derived as follows.



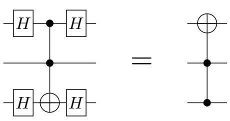
□

C.2 Proof of Equation (K^3)

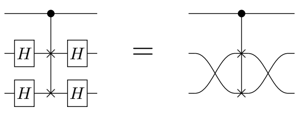


(K^3)

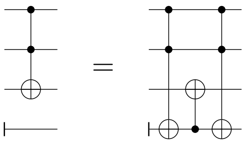
The main idea of the proof of Equation (K^3) is to use the *Fredkin gate* (or *controlled-swap gate*), defined by Equation (7). First, we derive some useful equations.

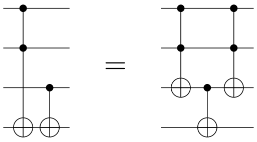


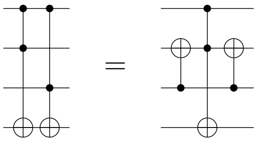
(56)

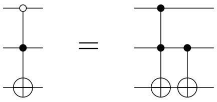


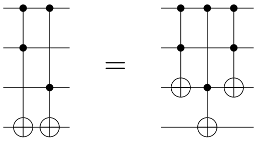
(57)

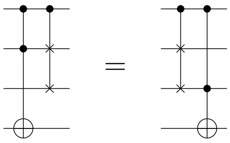

(58)

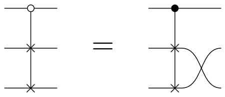

(59)

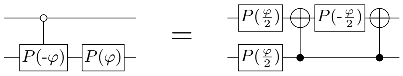

(60)


(61)

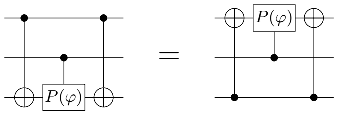

(62)


(63)

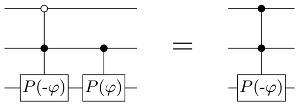

(64)



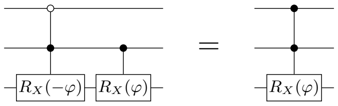
(65)



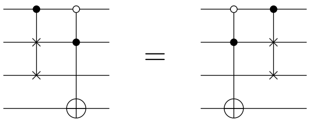
(66)



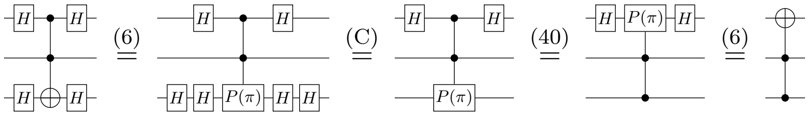
(67)



(68)

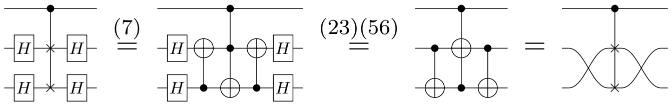

(69)

Proof of Equation (56).



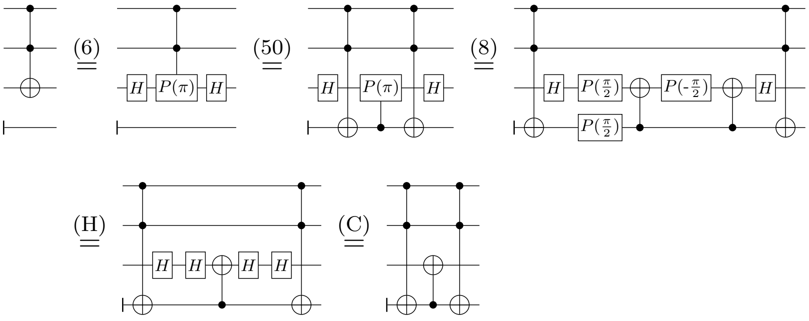
□

Proof of Equation (57).



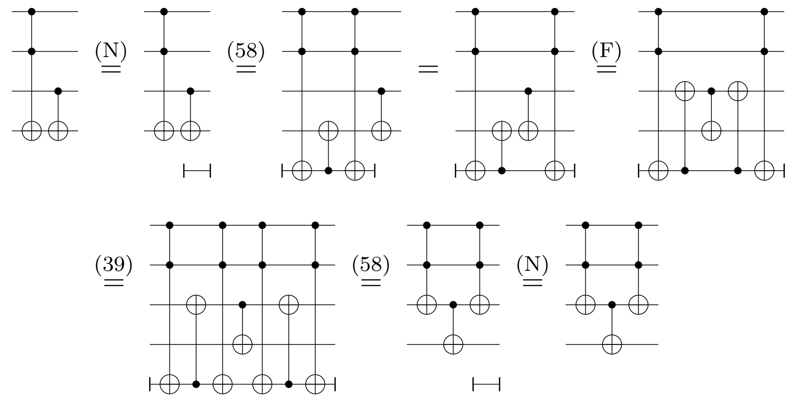
□

Proof of Equation (58).



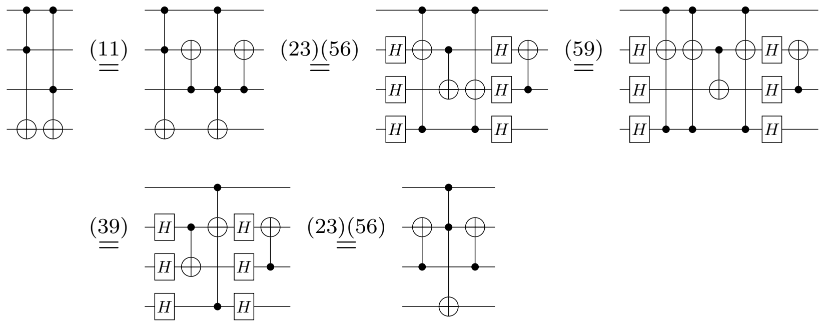
□

Proof of Equation (59).



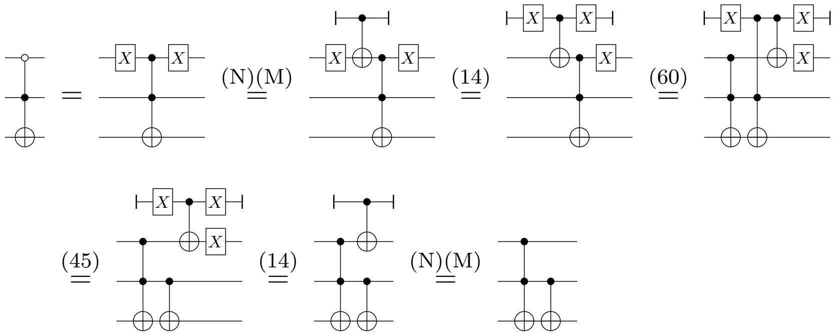
□

Proof of Equation (60).



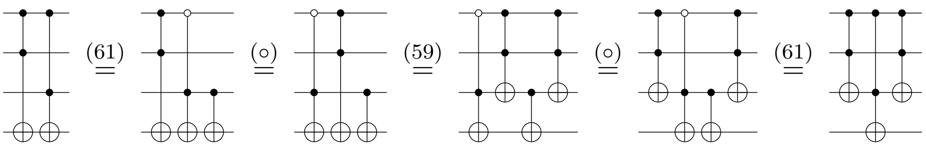
□

Proof of Equation (61).



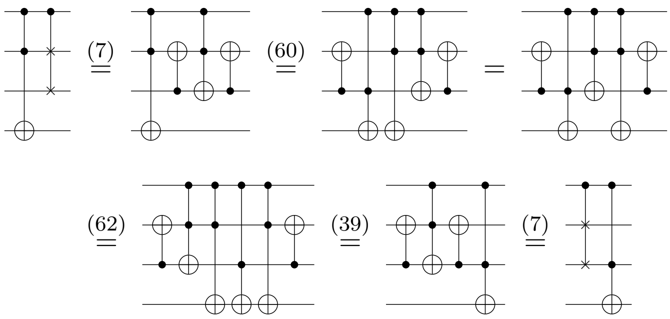
□

Proof of Equation (62).



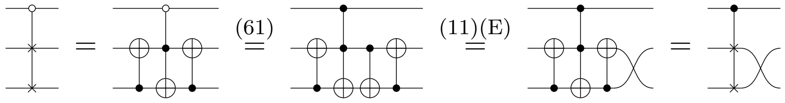
□

Proof of Equation (63).



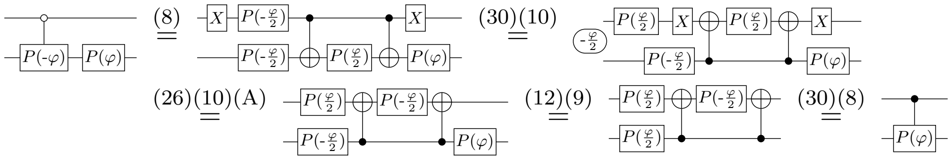
□

Proof of Equation (64).



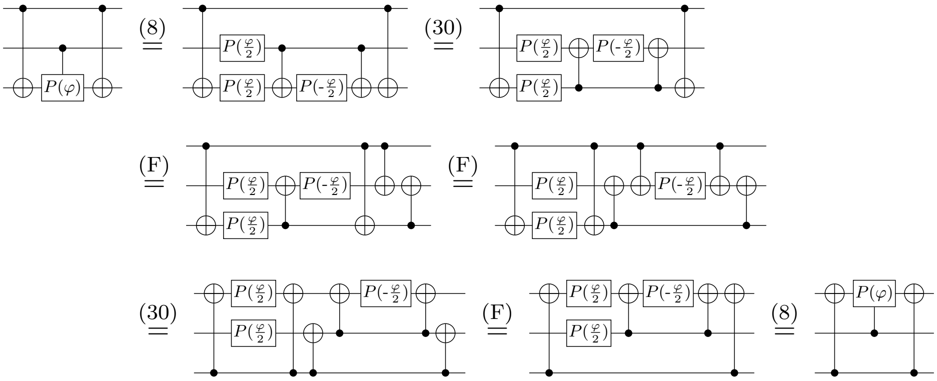
□

Proof of Equation (65).



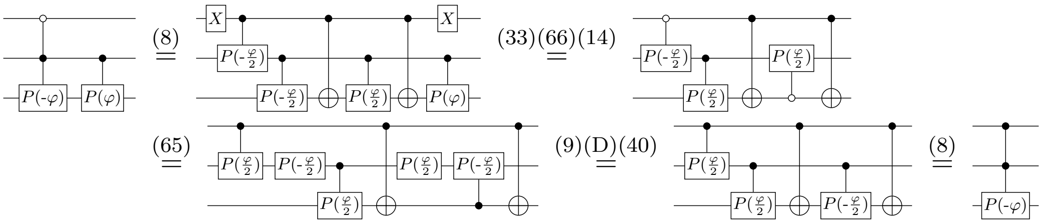
□

Proof of Equation (66).



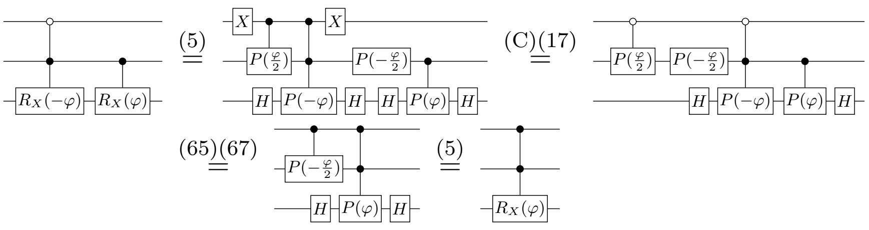
□

Proof of Equation (67).



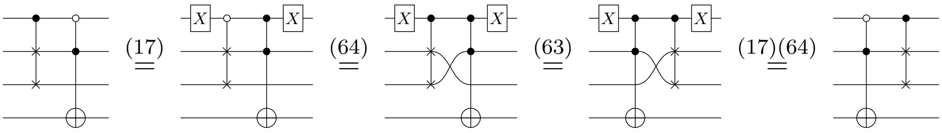
□

Proof of Equation (68).



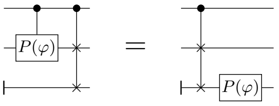
□

Proof of Equation (69).

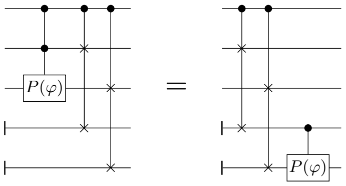


□

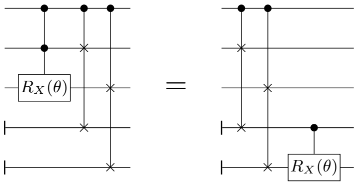
The idea of the proof of Equation (K^3) is to start from the LHS circuit of (K^3), use Equations (70),(71) and (72) to build an instance of the LHS circuit of (K^2) on two ancillae, apply (K^2) and then rebuild the RHS circuit of (K^3) using the same equations.



(70)

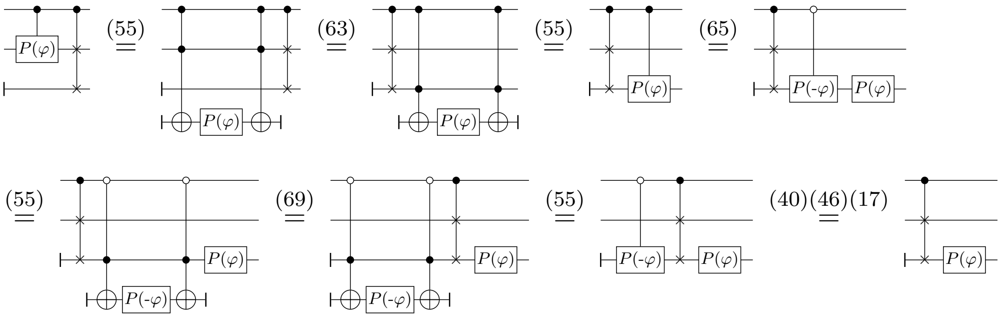


(71)



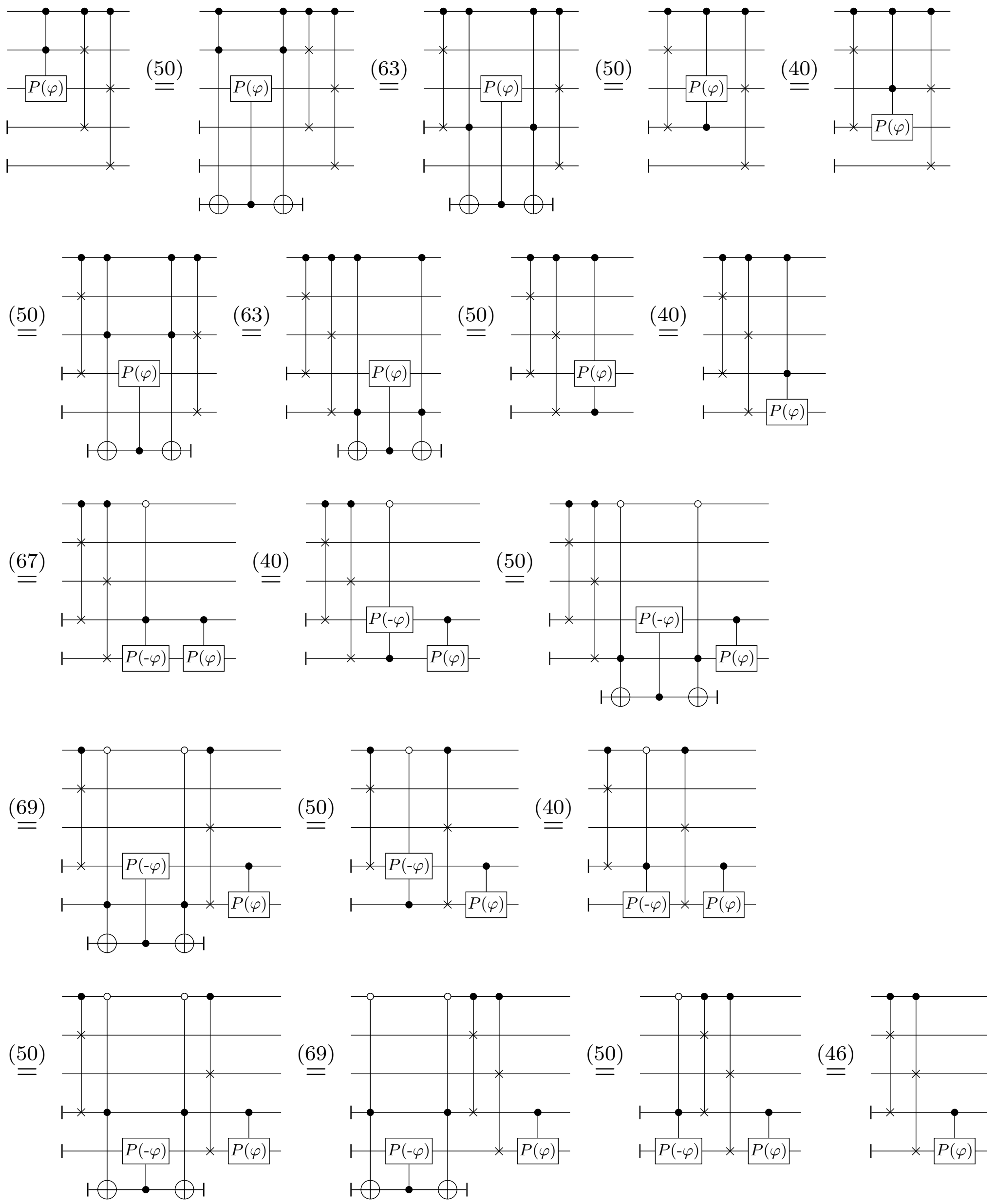
(72)

Proof of Equation (70).



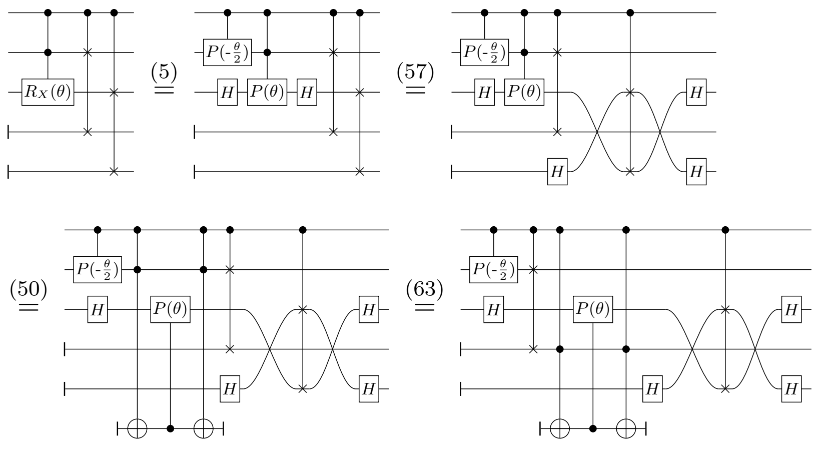
□

Proof of Equation (71).

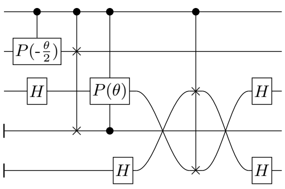


□

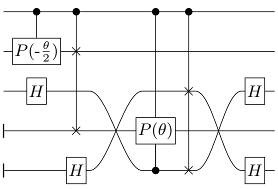
Proof of Equation (72).



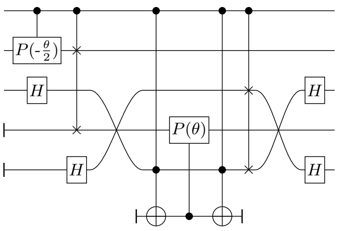
$\overset{(50)}{=}$



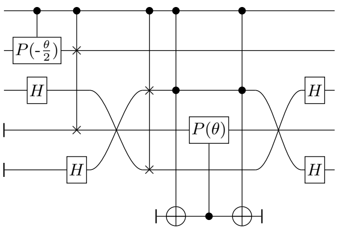
$\overset{(40)}{=}$



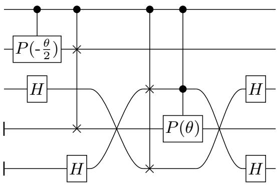
$\overset{(50)}{=}$



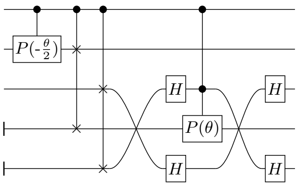
$\overset{(63)}{=}$



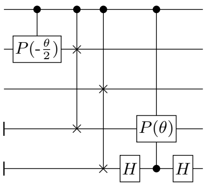
$\overset{(50)}{=}$



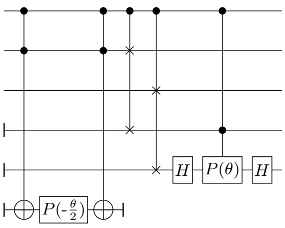
$\overset{(57)}{=}$



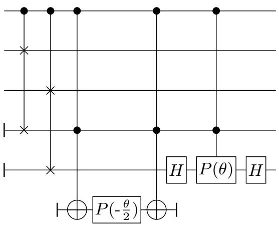
$\overset{(C)}{=}$



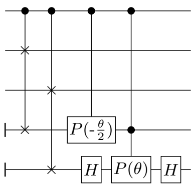
$\overset{(55)(40)}{=}$



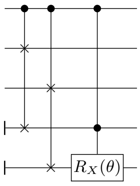
$\overset{(63)}{=}$



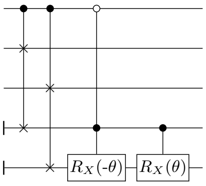
$\overset{(55)}{=}$



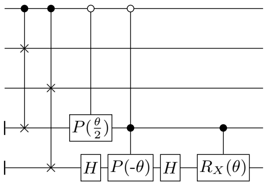
$\overset{(5)}{=}$



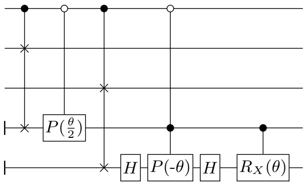
$\overset{(68)}{=}$



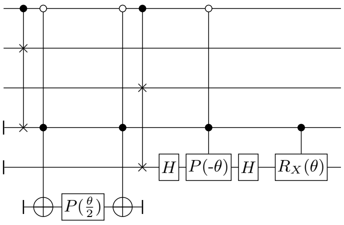
$\overset{(5)}{=}$



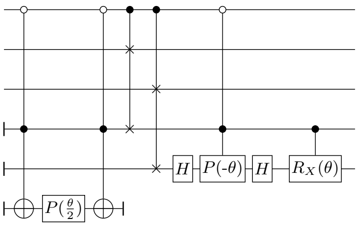
$\overset{(\circ)}{=}$



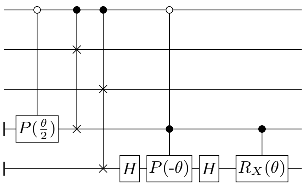
$\overset{(55)}{=}$



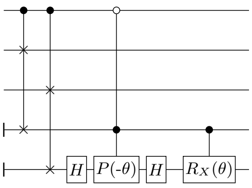
$\overset{(69)}{=}$



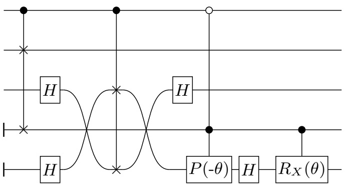
$\overset{(55)}{=}$



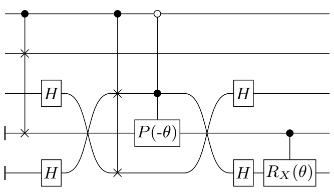
$\overset{(40)(46)(17)}{=}$



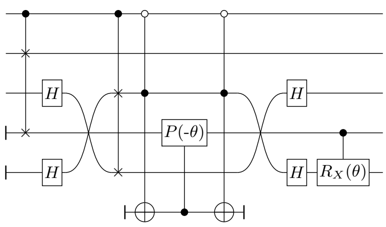
$\overset{(57)}{=}$



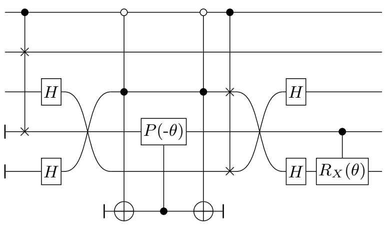
$\overset{(40)}{=}$



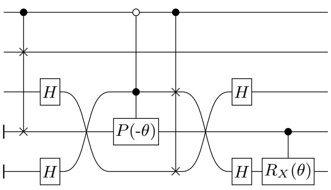
$\overset{(50)}{=}$



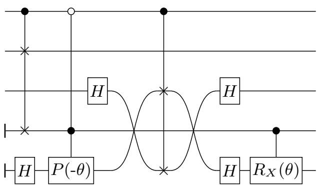
$\overset{(69)}{=}$



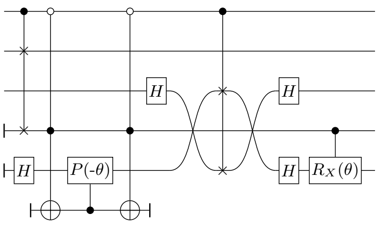
$\overset{(50)}{=}$



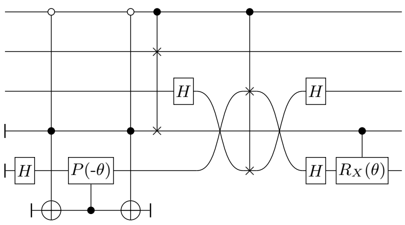
$\overset{(40)}{=}$



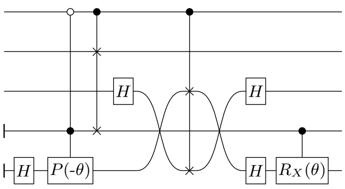
$\overset{(50)}{=}$



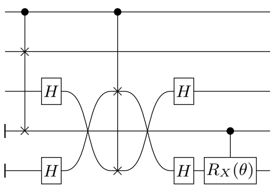
$\overset{(69)}{=}$



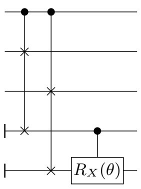
$\overset{(50)}{=}$



$\overset{(46)}{=}$

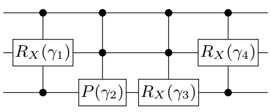


$\overset{(57)}{=}$

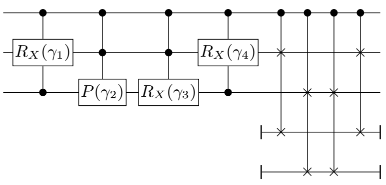


□

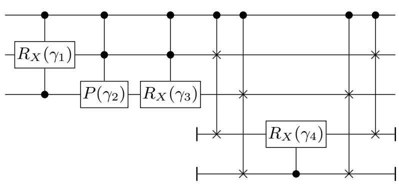
Proof of Equation (K^3).



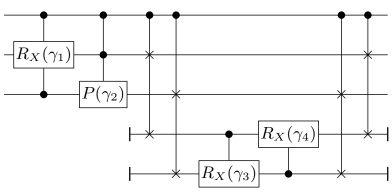
$\overset{(11)}{(\mathrm{N})\,=\,(39)}$



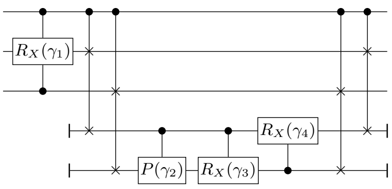
$\overset{(72)}{=}$



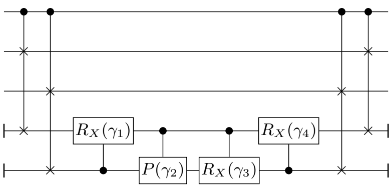
$\overset{(72)}{=}$



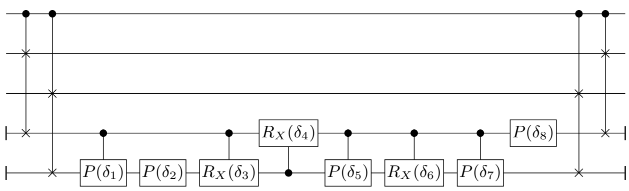
$\overset{(71)}{=}$



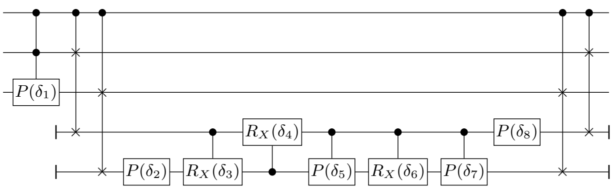
$\overset{(72)}{=}$



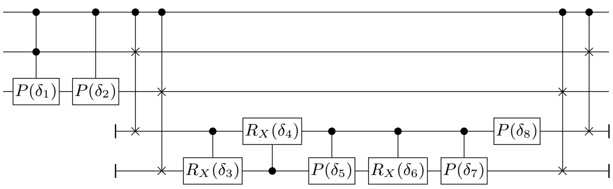
$\overset{(\mathrm{K}^2)}{=}$



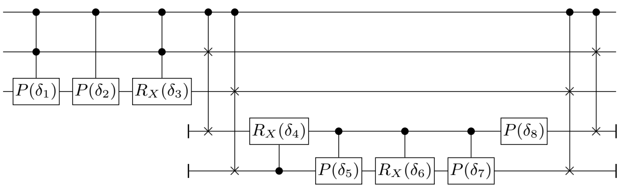
$\overset{(71)}{=}$



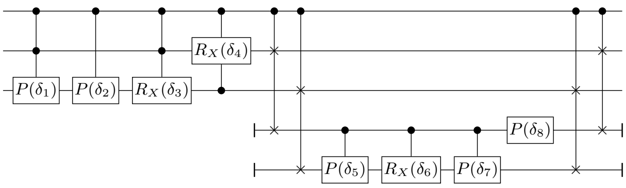
$\overset{(70)}{=}$



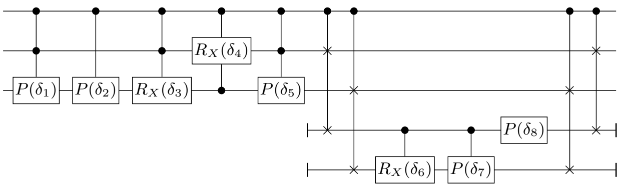
$\overset{(72)}{=}$



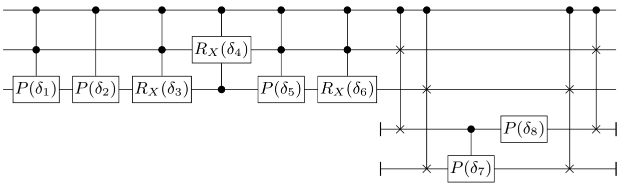
$\overset{(72)}{=}$



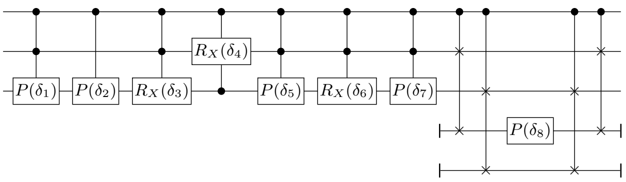
$\overset{(71)}{=}$



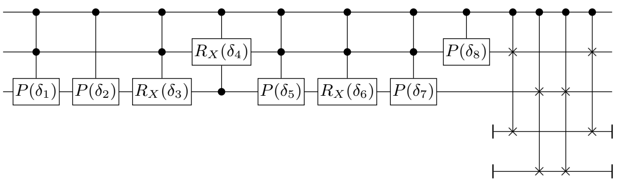
$\overset{(72)}{=}$



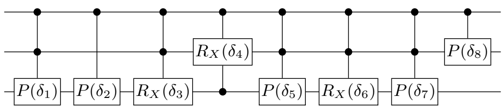
$\overset{(71)}{=}$



$\overset{(70)}{=}$

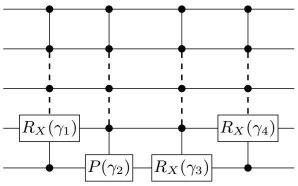


$(\mathrm{N})\overset{(11)}{=}(39)$

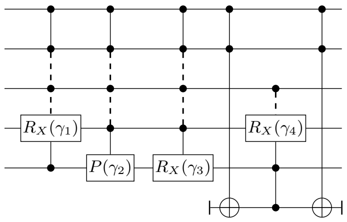


□

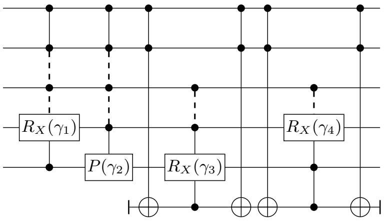
C.3 Induction step for proving Equation (K*)



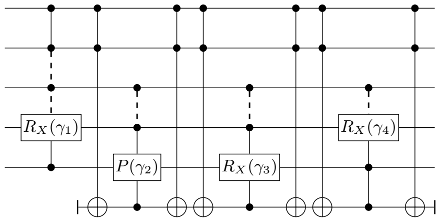
$(\mathrm{N})\overset{(51)}{=}$



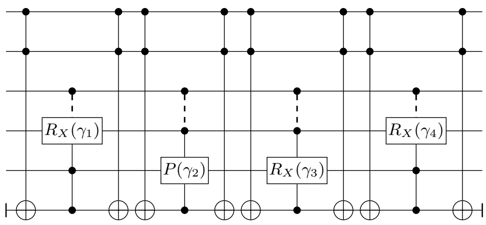
$\overset{(51)}{=}$



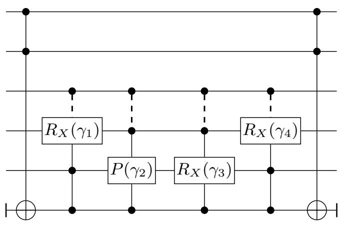
$\overset{(50)}{=}$



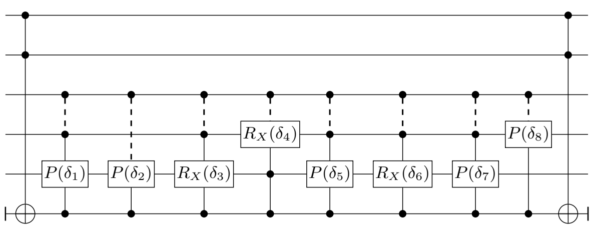
$\overset{(51)}{=}$



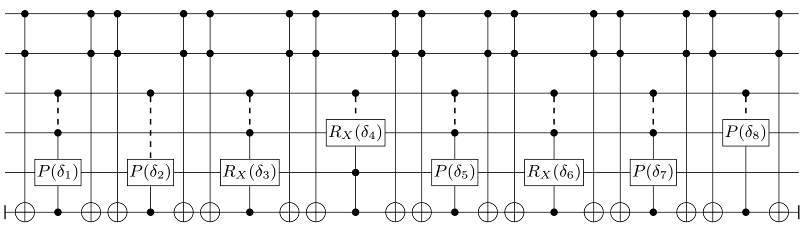
$\overset{(39)}{=}$



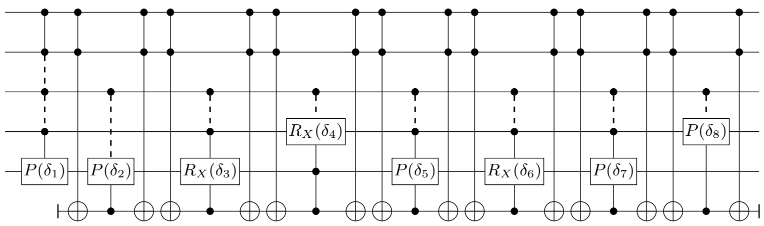
$\overset{\mathrm{IH}}{=}$



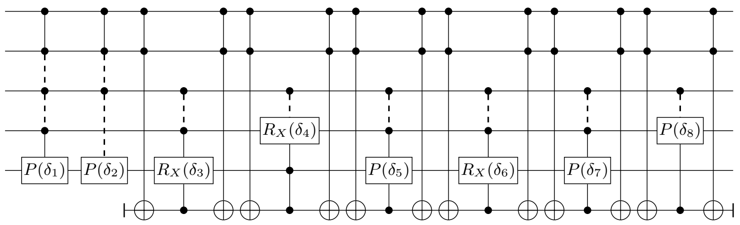
$\overset{(39)}{=}$



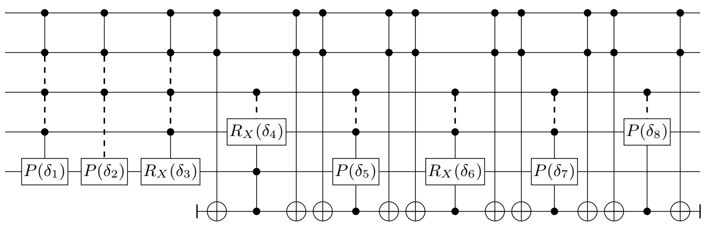
$\overset{(50)}{=}$



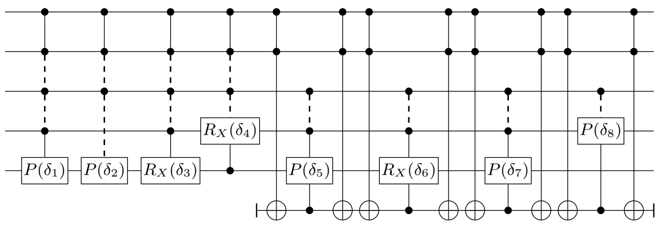
$\overset{(50)}{=}$



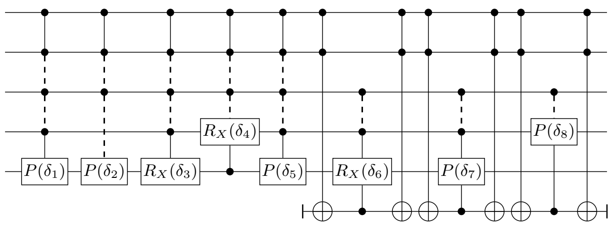
$\overset{(51)}{=}$



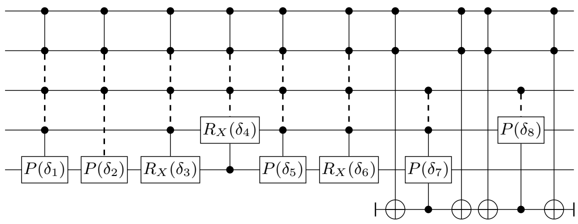
$\overset{(51)}{=}$



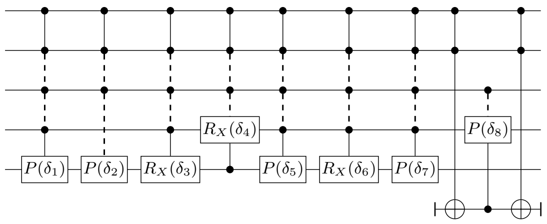
$\overset{(50)}{=}$



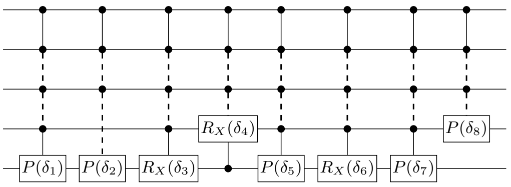
$\overset{(51)}{=}$



$\overset{(50)}{=}$



$\overset{(N)(50)}{=}$



Simplification of Complete Equational Theories for Quantum Circuits With and Without Ancillae

Noé Delorme