



**HAL**  
open science

## A Complete Equational Theory for Quantum Circuits

Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, Benoît Valiron

► **To cite this version:**

Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, Benoît Valiron. A Complete Equational Theory for Quantum Circuits. 2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), Jun 2023, Boston, United States. pp.1-13, 10.1109/LICS56636.2023.10175801 . hal-03926757

**HAL Id: hal-03926757**

**<https://hal.science/hal-03926757>**

Submitted on 8 Feb 2024

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

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

# A Complete Equational Theory for Quantum Circuits

Alexandre Clément\*  
alexandre.clement@loria.fr  
<https://orcid.org/0000-0002-7958-5712>  
<https://members.loria.fr/AClement>

Nicolas Heurtel<sup>†‡</sup>  
nicolas.heurtel@quandela.com  
<https://orcid.org/0000-0002-9380-8396>

Shane Mansfield<sup>†</sup>  
shane.mansfield@quandela.com

Simon Perdrix\*  
simon.perdrix@loria.fr  
<https://orcid.org/0000-0002-1808-2409>  
<https://members.loria.fr/SPerdrix>

Benoît Valiron<sup>‡</sup>  
benoit.valiron@universite-paris-saclay.fr  
<https://orcid.org/0000-0002-1008-5605>  
<https://www.monoidal.net>

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

<sup>†</sup>Quandela  
7 Rue Léonard de Vinci  
91300 Massy, France

<sup>‡</sup>Université Paris-Saclay, CentraleSupélec,  
Inria, CNRS, ENS Paris-Saclay,  
Laboratoire Méthodes Formelles  
91190, Gif-sur-Yvette, France

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

## I. INTRODUCTION

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

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

However, as ubiquitous to quantum computing as they are, the graphical language of quantum circuits has never been fully formalized. In particular, a *complete equational theory*

has been a longstanding open problem for 30 years [11]. It would make it possible to directly prove properties such as circuit equivalence without having to rely on ad-hoc sets of equations. So far, complete equational theories were only known for non-universal fragments, such as circuits acting on at most two qubits [12], [13], the stabilizer fragment [14], [15], the CNot-dihedral fragment [16], or fragments of reversible circuits [17]–[19].

Interestingly enough, other diagrammatic languages for quantum computation have been developed on sound foundations: it is reasonable to think that this could help in developing a complete equational theory for circuits. Arguably the strongest candidate has been the ZX-calculus [20], [21],<sup>1</sup> equipped with complete equational theories [24]–[28]. The ZX-calculus shares the same underlying mathematical representation for states: wires corresponds to Hilbert spaces and parallel composition to the tensor operation. Nonetheless, the completeness of the ZX-calculus does not lead *a priori* to a complete equational theory for quantum circuits. The reason lies in the expressiveness of the ZX-calculus and the *non-unitarity* of some of its generators. Any quantum circuit can be straightforwardly seen as a ZX-diagram. On the other hand, a ZX-diagram does not necessarily represent a unitary map, and even when it does, extracting a corresponding quantum circuit is known to be a hard task in general [4], [29].

Another example of a quantum language with a complete equational theory is the LOv-calculus, a language for linear optical quantum circuits for which a simple complete equational theory has recently been introduced [30]. While both linear optical and regular quantum circuits are universal for unitary transformations, they do not share the same structure.

<sup>1</sup>or its variants like ZH [22] and ZW [23], sharing several similar properties.

In particular, if the parallel composition of quantum circuits corresponds to the tensor product, for linear optical circuits it stands for the *direct sum*.

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

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

Due to the difference in its interpretation in both kinds of circuits, the parallel composition is not preserved by the encoding nor the decoding maps. The translations are actually based on a sequentialisation of circuits, since the translation of a local gate (acting on at most two wires) is translated as a piece of circuit acting potentially on all wires. Technically, it forces to work with a raw version of circuits, as a circuit may lead to a priori distinct translations depending on the choice of the sequentialisation. Moreover, a single linear optical gate like a phase shifter (which consists in applying a phase on a particular basis state) is decoded as a piece of circuits that can be interpreted as a multi-controlled gate acting on all qubits. As we choose to stick with the usual generators of quantum circuits acting on at most two qubits, multi-controlled gates are inductively defined and we introduce an equational theory powerful enough to prove the basic algebra of multi-controlled gates, necessary to finalise the proof of completeness.

The paper is structured as follows. We first introduce a set of structural relations for quantum circuits generated by the standard elementary gates: Hadamard, Phase-rotations, and CNot. We define multi-controlled gates using these elementary gates, and show that the basic algebra of multi-controlled gates can be derived from the structural relations. In addition to the structural equations, we introduce Euler-angle-based equations. We then proceed to the proof of completeness, based on a back-and-forth translation from quantum circuits to linear optical circuits.

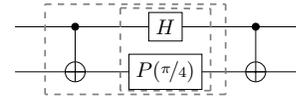
## II. QUANTUM CIRCUITS

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

(incoming the circuit from the left) and a set of output wires (exiting the circuit on the right).

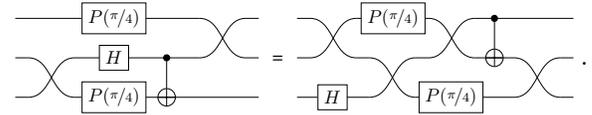
### A. Graphical languages

To provide a formal definition of circuits, we first use the notion of *raw circuits*.<sup>2</sup> Given a set of generators, one can generate a *raw circuit* by means of iterative sequential ( $\circ$ ) and parallel ( $\otimes$ ) compositions. For instance, given the elementary gates  $\boxed{H}$  and  $\boxed{P(\pi/4)}$  (with one input and one output) and  $\oplus$  (with two inputs and two outputs), one can construct the raw circuit  $\oplus \circ ((\boxed{H} \otimes \boxed{P(\pi/4)}) \circ \oplus)$ . Notice that a sequential composition  $C' \circ C$  requires that the number of outputs of  $C$  matches the number of inputs of  $C'$ . This raw circuit can be depicted by gluing the generators together and using boxes to witness how the generators have been composed:



To avoid the use of boxes and recover the intuitive notion of circuits, we formally define circuits as a prop [32], which consists in considering the raw circuits up to the rules given in Figure 1. More precisely, a prop generated by a set  $\mathcal{G}$  of elementary gates is the collection of raw circuits generated by  $\mathcal{G} \cup \{ \text{---}, \text{---}, \text{---} \}$ <sup>3</sup> quotiented by the equations of Figure 1.

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



### B. Quantum circuits: Syntax and semantics

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

**Definition 1.** Let  $\mathbf{QC}$  be the prop generated by  $\boxed{H}$ ,  $\oplus$ , and for any  $\varphi \in \mathbb{R}$ ,  $\boxed{P(\varphi)}$  and  $\odot$ .

The gates  $\boxed{H}$  and  $\boxed{P(\varphi)}$  have one input and one output, while  $\oplus$  has two and  $\odot$  zero. A quantum circuit  $C$  with  $n$  inputs and  $n$  outputs is called a  $n$ -qubit circuit. Given an  $n$ -qubit circuit  $C$ , the corresponding unitary map  $\llbracket C \rrbracket$  is acting on the Hilbert space  $\mathbb{C}^{\{0,1\}^n} = \text{span}(|x\rangle, x \in \{0,1\}^n)$ .<sup>4</sup>

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

$$\llbracket \boxed{H} \rrbracket = |x\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle),$$

<sup>2</sup>Raw terms are for instance similarly used [31] as an intermediate step in the definition of prop.

<sup>3</sup>--- denotes the identity,  $\text{---}$  the swap and  $\text{---}$  the empty circuit.

<sup>4</sup>We use the standard Dirac notations.

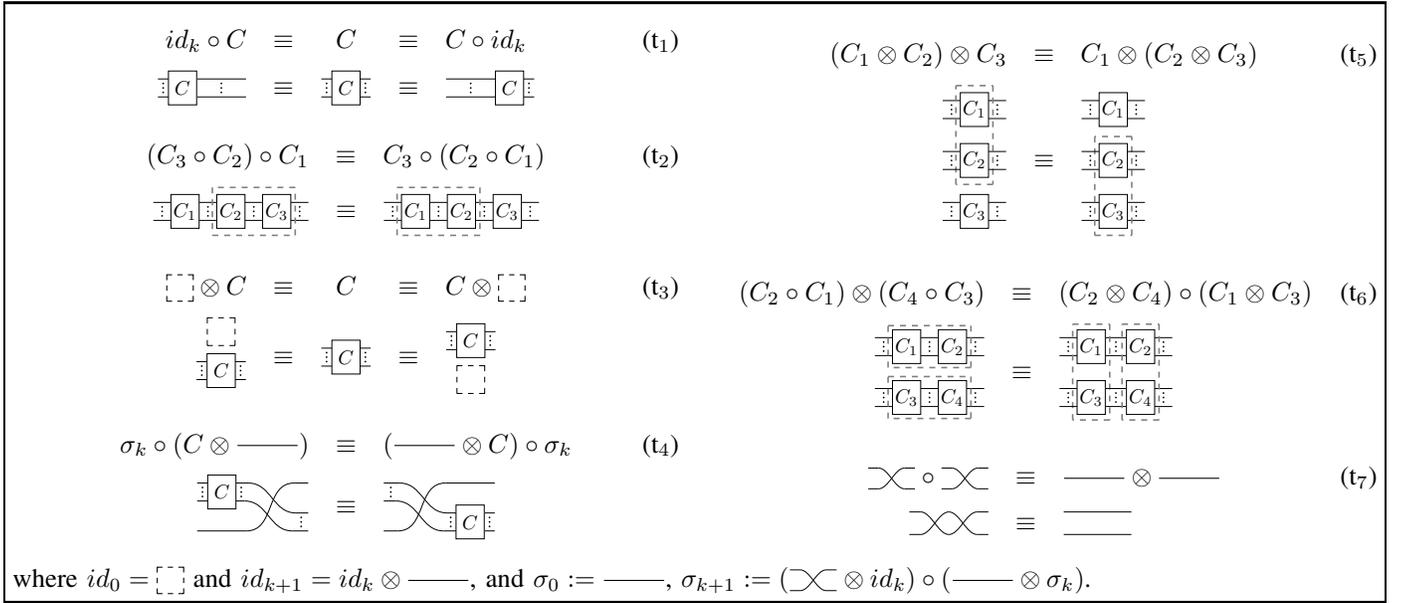


Fig. 1: Definition of  $\equiv$  for raw circuits (either raw quantum circuits or raw optical circuits).

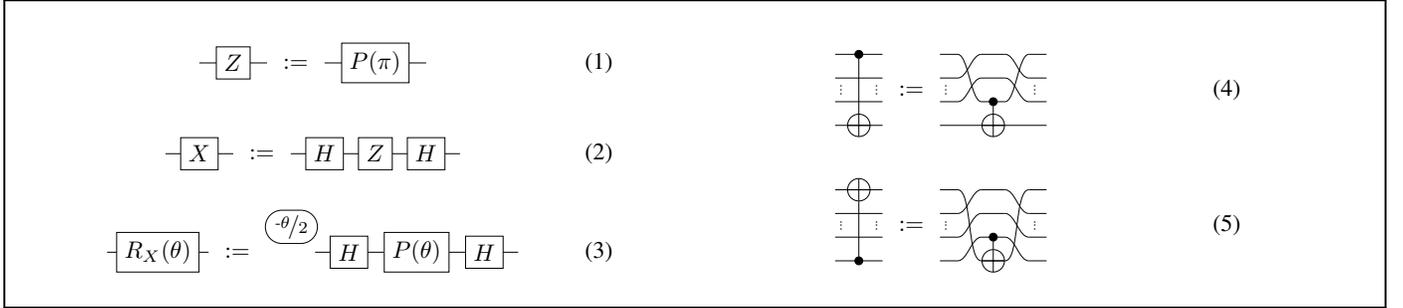


Fig. 2: Usual abbreviations of quantum circuits.

$$\begin{aligned}
[[P(\varphi)]] &= |x\rangle \mapsto e^{ix\varphi} |x\rangle, \\
[[\text{---}]] &= |x\rangle \mapsto |x\rangle, \\
[[\text{---} \oplus \text{---}]] &= |x, y\rangle \mapsto |x, x \oplus y\rangle, \\
[[\text{---} \times \text{---}]] &= |x, y\rangle \mapsto |y, x\rangle, \\
[[\text{---} \oplus \text{---}]] &= 1 \mapsto e^{i\varphi}, \\
[[[ ]]] &= 1 \mapsto 1.
\end{aligned}$$

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

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

We use standard shortcuts in the description of quantum circuits, given in Figure 2. In textual description, we sometimes use CNot,  $s(\varphi)$ ,  $X$ ,  $P(\varphi)$ , etc to denote respectively  $\text{---} \oplus \text{---}$ ,  $\text{---} \oplus$ ,  $[\text{---}]$ ,  $[\text{---}]$ , etc. Moreover, when the parameters (e.g.  $\varphi$ ) are not specific values they can take arbitrary ones. We write

$R_X(\theta)$  for the so-called  $X$ -rotation [34], whereas the standard phase gate  $P(\varphi)$  is a  $Z$ -rotation only up to a global phase. As a consequence, they have a slightly different behaviour:  $P$  is  $2\pi$ -periodic:  $[[P(2\pi)]] = I$ , whereas  $R_X$  is  $4\pi$ -periodic, and we instead have  $[[R_X(2\pi)]] = -I$ .

### C. Structural equations

We introduce a set  $\text{QC}_0$  of *structural equations* on quantum circuits in Figure 3. These equations are structural in the sense that the transformations on the parameters are only based on the fact that  $\mathbb{R}$  is an additive group. In particular, these equations are valid for any reasonable<sup>5</sup> restriction on the angles.

We write  $\text{QC}_0 \vdash C_1 = C_2$  when  $C_1$  can be transformed into  $C_2$  using the equations of Figure 3.<sup>6</sup>

**Proposition 5.** The structural equations of Figure 3 are sound, i.e. if  $\text{QC}_0 \vdash C_1 = C_2$  then  $[[C_1]] = [[C_2]]$ .

<sup>5</sup>I.e. which forms an additive group and contains  $\pi/2$ .

<sup>6</sup>More formally,  $\text{QC}_0 \vdash \cdot = \cdot$  is defined as the smallest congruence which satisfies equations of Figures 1 and 3.

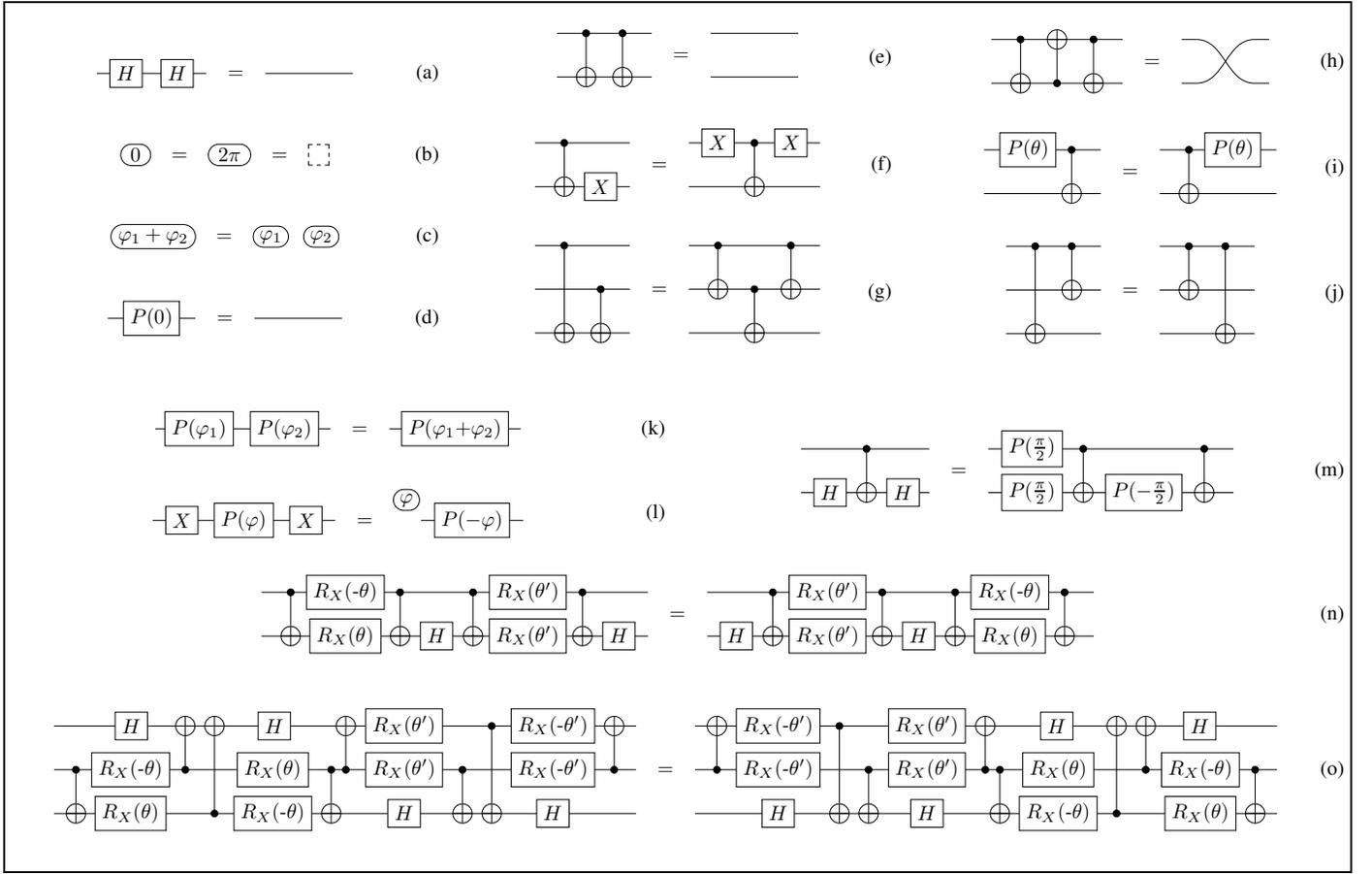


Fig. 3: **Axioms of  $QC_0$** : Structural equations on quantum circuits. The equations are defined for any  $\varphi, \varphi_1, \varphi_2, \theta, \theta' \in \mathbb{R}$ .

*Proof.* By inspection of the equations of Figure 3.  $\square$

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

The axioms of  $QC_0$ , i.e. the equations given in Figure 3, are sufficient to derive standard elementary circuit identities like those given in Figure 4.

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

$$QC_0 \vdash \begin{array}{c} \text{---} \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} = \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \quad (6)$$

$$QC_0 \vdash \begin{array}{c} \text{---} \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} = \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \quad (7)$$

The derivations are given in Appendix B-A. Combining Equation (6) and Equation (i), one can easily prove the following equation, used for instance in [8] in the context of circuit optimisation:

$$QC_0 \vdash \begin{array}{c} \text{---} \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} = \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array} \begin{array}{c} \oplus \\ | \\ \oplus \\ | \\ \oplus \\ \text{---} \end{array}$$

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

#### D. Controlled gates

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



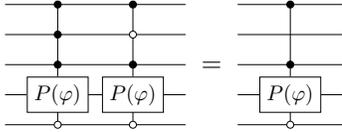


gates, use Equation (24) to put the multi-controlled gates with angles  $\theta/2$  and  $\theta'/2$  side by side, and merge them using the induction hypothesis. We use again Equation (24) to allow the combination of the multi-controlled gates with angle  $-\theta/2$  and  $-\theta'/2$ , closing the case.

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

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

Combining a control and anti-control on the same qubit makes the evolution independent of this qubit, as in the following example in which the evolution is independent of the second qubit:<sup>8</sup>



Such simplifications can be derived in  $\text{QC}_0$ .

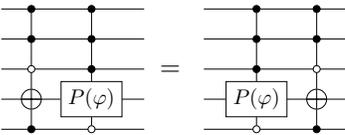
**Proposition 15.** For all bitstrings  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^\ell$ , and for all  $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$ ,

$$\text{QC}_0 \vdash \Lambda_y^{0x} G \circ \Lambda_y^{1x} G = \text{---} \otimes \Lambda_y^x G.$$

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

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

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



<sup>8</sup>Notice that in the above example we implicitly use Proposition 11 to swap the first two qubits and apply Proposition 15. As a consequence, the resulting multi-controlled gate acts on non-adjacent qubits. Similarly to the CNot case (see Equations (4) and (5)), we use some syntactic sugar to represent such multi-controlled gates acting on non-adjacent qubits.

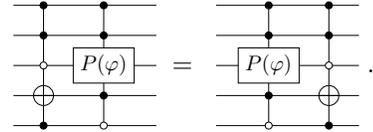
When the target qubit is the same, such a commutation property can be derived in  $\text{QC}_0$ , using in particular Equation (n).

**Proposition 16.** For any  $x, x' \in \{0, 1\}^k$ ,  $y, y' \in \{0, 1\}^\ell$ , and  $G, G' \in \{X, R_X(\theta), P(\varphi)\}$ , if  $xy \neq x'y'$ <sup>9</sup> then

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

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

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



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

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

$$\text{QC}_0 \vdash \Lambda_{yaz}^x G \circ \Lambda_{z'y'}^{x'} G' = \Lambda_{z'y'}^{x'} G' \circ \Lambda_{yaz}^x G$$

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

## F. Euler angles and Periodicity

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

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

**Proposition 18.**  $\text{QC} \vdash \boxed{H} = \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})}$

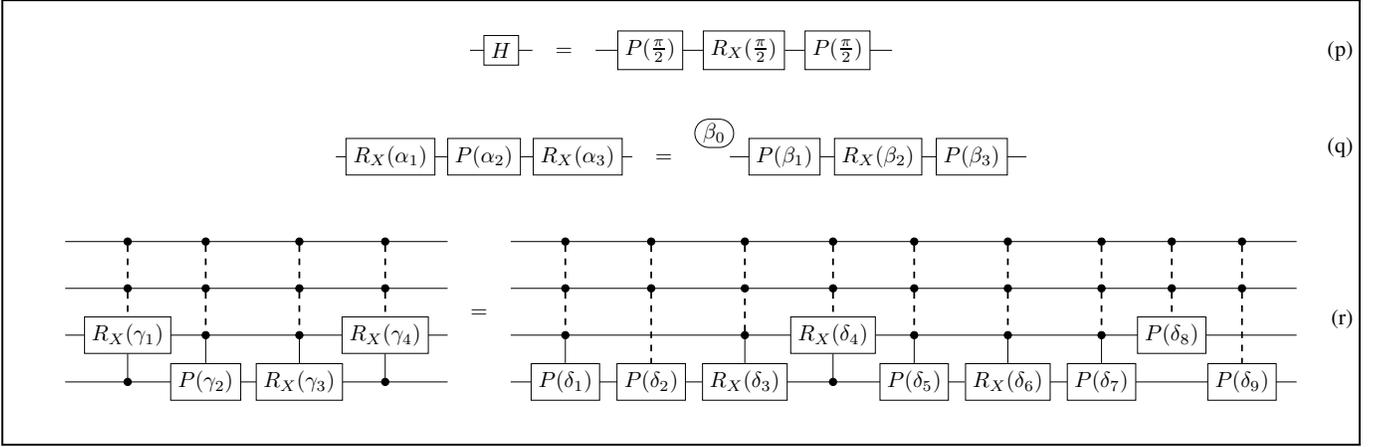
*Proof.* The proof is given in Appendix C-F.  $\square$

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

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

*Proof.* The soundness and uniqueness of Equation (q) are well-known properties. Regarding Equation (r), we first notice

<sup>9</sup> $xy \neq x'y'$  iff  $\exists i, x_i \neq x'_i \vee y_i \neq y'_i$ .



**Fig. 5: Non-structural equations.** In Equations (q) and (r) the LHS circuit has arbitrary parameters which uniquely determine the parameters of the RHS circuit. Equation (q) is nothing but the well-known Euler-decomposition rule which states that any unitary can be decomposed, up to a global phase, into basic  $X$ - and  $Z$ -rotations. Thus for any  $\alpha_i \in \mathbb{R}$ , there exist  $\beta_j \in [0, 2\pi)$  such that Equation (q) is sound. We make the angles  $\beta_j$  unique by assuming that  $\beta_1 \in [0, \pi)$ ,  $\beta_2 \in [0, 2\pi)$  and if  $\beta_2 \in \{0, \pi\}$  then  $\beta_1 = 0$ . Equation (p) is the particular Euler decomposition of  $H$ . Equation (r) 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 (r) can be seen as a generalisation of the Euler rule, using multi-controlled gates. Similarly to Equation (q), for any  $\gamma_i \in \mathbb{R}$ , there exist  $\delta_j \in [0, 2\pi)$  such that Equation (r) is sound. We can ensure that the angles  $\delta_j$  are uniquely determined by assuming that  $\delta_1, \delta_2, \delta_5, \in [0, \pi)$ ,  $\delta_3, \delta_4, \delta_6 \in [0, 2\pi)$ , 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  $\delta_5 = 0$ .

that the semantics of both circuits is of the form  $\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$  where  $U$  is a  $3 \times 3$  matrix. We then use the fact that this matrix can be decomposed into basic rotations that can be proved to be unique [30]. The details of the proof are given in Appendix C-G.  $\square$

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

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

$$\boxed{P(\varphi_1)} \boxed{P(\varphi_2)} = \boxed{P(\varphi_1 + \varphi_2)} \quad (k)$$

$$\boxed{X} \boxed{P(\varphi)} \boxed{X} = \overset{\varphi}{\circlearrowleft} \boxed{P(-\varphi)} \quad (l)$$

can be derived from the other axioms of QC.

*Proof.* The proofs are given in Appendix C-H.  $\square$

The introduction of the additional equations of Figure 5 allows us to prove some extra properties about multi-controlled gates, like periodicity (for those with a parameter) in Proposition 22 and the fact that a multi-controlled  $X$  gate is self-inverse.

**Proposition 21.** *For any  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^\ell$ ,*

$$\text{QC} \vdash \Lambda_y^x X \circ \Lambda_y^x X = id_{k+\ell+1}$$

*Proof.* The case  $x = y = \epsilon$  is a direct consequence of Equation (10). For the other cases, by Definitions 6 to 8,

Equations (10) and (a), and Proposition 13, it is equivalent to show that, for any  $x \in \{0, 1\}^k$ ,

$$\text{QC} \vdash \Lambda^x P(2\pi) = id_{k+1}.$$

Without loss of generality, we can consider  $x \in \{1\}^k$ . Then the result is a consequence of Proposition 13 and Equation (r). Indeed, by taking  $\gamma_1 = \gamma_3 = \gamma_4 = 0$  and  $\gamma_2 = 2\pi$  in the LHS of Equation (r), the unique angles on the right are all zeros:  $\delta_1 = \delta_2 = \delta_3 = \delta_4 = \delta_5 = \delta_6 = \delta_7 = \delta_8 = \delta_9 = 0$ . By Proposition 13, any multi-controlled gate with zero angle is the identity, which gives us the desired equality. Further details can be found in Appendix C-I.  $\square$

**Proposition 22.** *For any  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^\ell$ ,  $\theta \in \mathbb{R}$ ,*

$$\text{QC} \vdash \Lambda_y^x R_X(\theta + 4\pi) = \Lambda_y^x R_X(\theta)$$

$$\text{QC} \vdash \Lambda_y^x P(\theta + 2\pi) = \Lambda_y^x P(\theta)$$

$$\text{QC} \vdash \Lambda_y^x s(\theta + 2\pi) = \Lambda_y^x s(\theta)$$

*Proof.* Following the additivity of Proposition 13, it is sufficient to show that for any  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^\ell$ ,

$$\text{QC} \vdash \Lambda_y^x R_X(4\pi) = id_{k+\ell+1},$$

$$\text{QC} \vdash \Lambda_y^x P(2\pi) = id_{k+\ell+1},$$

$$\text{QC} \vdash \Lambda_y^x s(2\pi) = id_{k+\ell}.$$

Also, with Equations (10) and Definitions 7 and 8, it is sufficient to show that for any  $x \in \{1\}^k$ ,

$$\text{QC} \vdash \Lambda^x R_X(4\pi) = id_{k+1},$$

$$\text{QC} \vdash \Lambda^x P(2\pi) = id_{k+1},$$

$$\text{QC} \vdash \Lambda^x s(2\pi) = id_k.$$

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

### III. COMPLETENESS

In this section we prove the main result of the paper, namely the completeness of QC. To this end, a back and forth encoding of quantum circuits into linear optical quantum circuits is introduced. We use the graphical language for linear optical circuits introduced in [30].

#### A. Optical circuits

A *linear optical polarisation-preserving* (LOPP for short) circuit is an optical circuit made of beam splitters ( $\curvearrowright^\theta$ ) and phase shifters ( $\boxed{\varphi}$ ):

**Definition 23.** Let **LOPP** be the prop generated by  $\boxed{\varphi}$ ,  $\curvearrowright^\theta$  with  $\varphi, \theta \in \mathbb{R}$ .

Like quantum circuits, LOPP-circuits are defined as a prop: one can see them as raw circuits quotiented by the  $\equiv$ -equivalence given in Figure 1.

In the following, we consider the single photon case, hence each input mode (or wire) represents a possible input position for the photon. The photon moves from left to right in the circuit. The state of the photon is entirely defined by its position, and as a consequence the state space is of the form  $\mathbb{C}^n$  when there are  $n$  possible modes. We consider the standard orthonormal basis  $\{|p\rangle\}_{p \in [0, n]}$  of  $\mathbb{C}^n$ . The semantics is defined as follows.

**Definition 24** (Semantics). For any  $n$ -mode LOPP-circuit  $C$ , let  $\llbracket C \rrbracket : \mathbb{C}^n \rightarrow \mathbb{C}^n$  be a linear map inductively defined as follows:  $\llbracket C_2 \circ C_1 \rrbracket := \llbracket C_2 \rrbracket \circ \llbracket C_1 \rrbracket$ ,  $\llbracket C_1 \otimes C_3 \rrbracket := \llbracket C_1 \rrbracket \oplus \llbracket C_3 \rrbracket = \left( \begin{array}{c|c} \llbracket C_1 \rrbracket & 0 \\ \hline 0 & \llbracket C_3 \rrbracket \end{array} \right)$ ,

$$\llbracket \curvearrowright^\theta \rrbracket := |p\rangle \mapsto \cos(\theta) |p\rangle + i \sin(\theta) |1-p\rangle \\ = \begin{pmatrix} \cos(\theta) & i \sin(\theta) \\ i \sin(\theta) & \cos(\theta) \end{pmatrix}$$

$$\llbracket \curvearrowleft \rrbracket := |p\rangle \mapsto |1-p\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\llbracket \boxed{\varphi} \rrbracket := e^{i\varphi} \quad \llbracket \text{---} \rrbracket := 1 \quad \llbracket \text{---} \rrbracket := 0$$

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

We consider a simple equational theory for LOPP-circuits (Figure 6), which is derived from the rewriting system introduced in [30]. Contrary to the rewriting system of [30], the swap is part of LOPP-circuits. Moreover, the most elaborate

equation – Equation (G) – is slightly simplified in the present paper to have one parameter less.

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

**Theorem 26.** The equational theory given by Figure 6 is sound and complete: for any LOPP-circuits  $C_1, C_2$ ,  $\text{LOPP} \vdash C_1 = C_2$  iff  $\llbracket C_1 \rrbracket = \llbracket C_2 \rrbracket$ .

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

#### B. Forgetting the monoidal structure

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

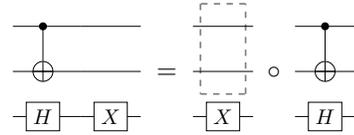
As a consequence there is a technical issue around defining the translation directly on circuits. We instead define the transformations on *raw* circuits (cf. Section II-A). The collection of raw quantum (resp. LOPP) circuits is denoted  $\text{QC}_{\text{raw}}$  (resp.  $\text{LOPP}_{\text{raw}}$ ).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

To avoid ambiguity in the graphical representation of raw

circuits one can use boxes like  $\boxed{X}$  for  $(\text{---} \otimes \text{---}) \otimes \text{---}$ .

We also use box-free graphical representation that we interpret as a layer-by-layer description of a raw circuit, more precisely we associate with any box-free graphical representation, a raw-circuit of the form  $C = (\dots ((L_1 \circ L_2) \circ L_3) \circ \dots) \circ L_k$  where  $L_i = (\dots ((g_{i,1} \otimes g_{i,2}) \otimes g_{i,3}) \otimes \dots) \otimes g_{i,\ell_i}$ .

For instance,  $((id_1 \otimes id_1) \otimes X) \circ (CNot \otimes H)$  is



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

Notice that there exists a derivation between two circuits if and only if there exists a derivation between two of

<sup>10</sup>In this context, the circuits depicted in Figures 3, 5 and 6 are interpreted as box-free graphical representations of raw circuits.

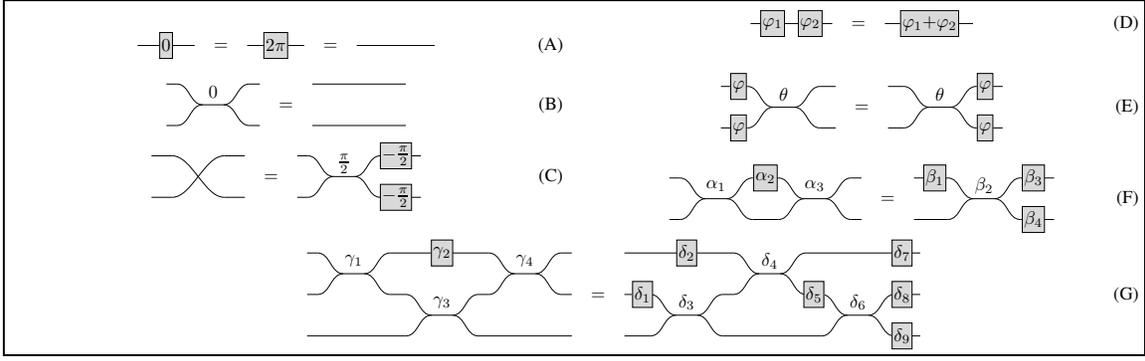


Fig. 6: Axioms of the LOPP-calculus. In Equation (F) and Equation (G), the LHS circuit has arbitrary parameters which uniquely determine the parameters of the RHS circuit. For any  $\alpha_i \in \mathbb{R}$ , there exist  $\beta_j \in [0, 2\pi)$  such that Equation (F) is sound, and for any  $\gamma_i \in \mathbb{R}$ , there exist  $\delta_j \in [0, 2\pi)$  such that Equation (G) is sound. We can ensure that the angles  $\beta_j$  are unique by assuming that  $\beta_1, \beta_2 \in [0, \pi)$  and if  $\beta_2 \in \{0, \frac{\pi}{2}\}$  then  $\beta_1 = 0$ , and we can ensure that the angles  $\delta_j$  are unique by assuming that  $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6 \in [0, \pi)$ . If  $\delta_3 \in \{0, \frac{\pi}{2}\}$  then  $\delta_1 = 0$ , if  $\delta_4 \in \{0, \frac{\pi}{2}\}$  then  $\delta_2 = 0$ , if  $\delta_4 = 0$  then  $\delta_3 = 0$ , and if  $\delta_6 \in \{0, \frac{\pi}{2}\}$  then  $\delta_5 = 0$ . The existence and uniqueness of such  $\beta_j$  and  $\delta_j$  are given by Lemmas 10 and 11 of [30].

their representative raw circuits. Indeed, intuitively the only difference is that the derivation on raw circuits is more fine-grained as the equivalence relation  $\equiv$  is made explicit.

### C. Encoding quantum circuits into optical ones

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

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

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

For instance  $G_3$  is defined as follows:

$$\begin{array}{ll} 0 \mapsto 000 & 4 \mapsto 110 \\ 1 \mapsto 001 & 5 \mapsto 111 \\ 2 \mapsto 011 & 6 \mapsto 101 \\ 3 \mapsto 010 & 7 \mapsto 100 \end{array}$$

In order to get around the fact that the encoding an  $n$ -qubit circuit into a  $2^n$ -mode optical circuit cannot preserve the parallel composition, we proceed by ‘sequentialising’ the circuit: roughly speaking, an  $n$ -qubit circuit is seen as a sequential composition of layers, each layer being an  $n$ -qubit circuit made of an elementary gate  $g$  acting on at most two qubits in parallel with the identity on all other qubits, e.g.  $id_k \otimes g \otimes id_l$ . The encoding of such a layer, denoted  $E_{k,l}(g)$ , is a  $2^n$ -mode optical circuit acting non-trivially on potentially all the modes.

For instance, consider a 3-qubit layer which consists in applying  $P(\varphi)$  on the second qubit. Its semantics is  $|x, y, z\rangle \mapsto e^{i\varphi y} |x, y, z\rangle$ . Such a circuit is encoded into an 8-mode optical circuit  $E_{1,1}(P(\varphi))$  made of 4 phase shifters acting on the modes  $p \in [2, 5]$  (those s.t.  $G_3(p) = x1z$ ). Indeed, the semantics of  $E_{1,1}(P(\varphi))$  is  $|p\rangle \mapsto \begin{cases} e^{i\varphi} |p\rangle & \text{if } p \in [2, 5] \\ |p\rangle & \text{otherwise} \end{cases}$ .

The encoding map is formally defined as follows:

**Definition 28** (Encoding). *Let  $E : \mathbf{QC}_{\text{raw}} \rightarrow \mathbf{LOPP}_{\text{raw}}$  be defined as follows: for any  $n$ -qubit circuit  $C$ ,  $E(C) = E_{0,0}(C)$  where  $E_{k,\ell}$  is inductively defined as:*

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

Let us define  $\sigma_{k,n,\ell}$  as a  $2^{k+n+\ell}$ -mode linear optical circuit made only of swaps (that is, without any  $\boxed{\varphi}$  or  $\curvearrowright^{\theta}$ ) such that  $\mathfrak{G}_n \circ \llbracket \sigma_{k,n,\ell} \rrbracket \circ \mathfrak{G}_n^{-1}(|x, y, z\rangle) = |x, z, y\rangle$  for any  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^n$  and  $z \in \{0, 1\}^\ell$ . We then define

$$\begin{aligned} E_{k,\ell}(\curvearrowright) &= \sigma_{k,\ell,2} \circ \sigma_{k+\ell,1,1} \circ \sigma_{k,2,\ell}, \\ E_{k,\ell}(\boxed{\varphi}) &= (\text{---})^{\otimes 2^{k+\ell}}, \\ E_{k,\ell}(\text{---}) &= (\text{---})^{\otimes 2^{k+\ell+1}}, \\ E_{k,\ell}(s(\varphi)) &= (\boxed{\varphi})^{\otimes 2^{k+\ell}}. \end{aligned}$$

where  $C^{\otimes n}$  means  $C$   $n$  times in parallel:  $C^{\otimes 0} = \boxed{\phantom{C}}$  and  $C^{\otimes n+1} = C \otimes C^{\otimes n}$ .

For the remaining generators, we have:

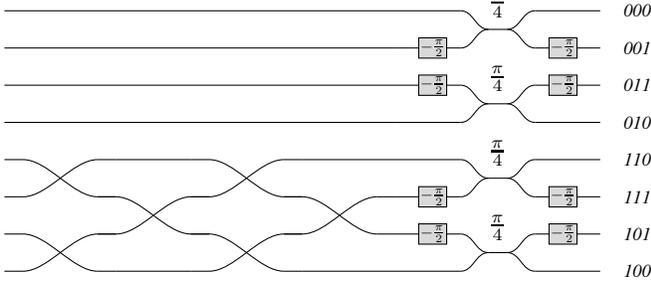
$$\begin{aligned} E_{0,0}(\boxed{-H}) &= \boxed{\frac{\pi}{2}} \curvearrowright \boxed{\frac{\pi}{2}}, \\ E_{0,0}(\boxed{-P(\varphi)}) &= \boxed{\varphi}, \\ E_{0,0}(\bigoplus) &= \text{---} \end{aligned}$$

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

$$\begin{aligned}
E_{k,\ell}(\boxed{-H-}) &= \sigma_{k,\ell,1} \circ \left( \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \begin{array}{c} \frac{\pi}{4} \\ \frac{\pi}{4} \\ \frac{\pi}{4} \\ \frac{\pi}{4} \end{array} \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \right) \otimes 2^{k+\ell-1} \circ \sigma_{k,1,\ell}, \\
E_{k,\ell}(\boxed{-P(\varphi)-}) &= \sigma_{k,\ell,1} \circ \left( \begin{array}{c} \text{---} \\ \text{---} \end{array} \begin{array}{c} \frac{\varphi}{2} \\ \frac{\varphi}{2} \end{array} \begin{array}{c} \text{---} \\ \text{---} \end{array} \right) \otimes 2^{k+\ell-1} \circ \sigma_{k,1,\ell}, \\
E_{k,\ell}(\bigoplus) &= \sigma_{k,\ell,2} \circ \left( \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \right) \otimes 2^{k+\ell-1} \circ \sigma_{k,2,\ell}.
\end{aligned}$$

**Remark 29.** Note that for any  $n$ -qubit circuit  $C$ ,  $E_{k,\ell}(C)$  is a  $2^{k+n+\ell}$ -mode optical circuit. Also note that  $\sigma_{k,n,\ell}$  is nothing but a permutation of wires. By Lemma 36 – which is independent from the definition of  $E$  – any actual circuit satisfying the above property ( $\mathfrak{G}_n \circ \llbracket \sigma_{k,n,\ell} \rrbracket \circ \mathfrak{G}_n^{-1}(|x, y, z\rangle) = |x, z, y\rangle$ ) is convenient for our purposes. A formal definition of  $\sigma_{k,n,\ell}$  is however given in Appendix D-G.

**Example 30.** Consider the simple circuit  $C_0 = \bigoplus \boxed{-H-}$ . The encoding is as shown in Figure 7. Using the topological rules (Figure 1), one can simplify  $E(C_0)$  into the circuit  $C_1$ :



The encoding of quantum circuits into linear optical circuits preserves the semantics, up to Gray codes.

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

$$\mathfrak{G}_n \circ \llbracket E(C) \rrbracket = \llbracket C \rrbracket \circ \mathfrak{G}_n$$

*Proof.* By induction.  $\square$

### D. Decoding

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

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

Its semantics is  $|p\rangle \mapsto \begin{cases} e^{i\varphi} |p\rangle & \text{if } p = 3 \\ |p\rangle & \text{otherwise} \end{cases}$ . Such a circuit is decoded into a 4-qubit circuit  $D_{3,4}(\boxed{-\varphi-})$  implementing

the multi-controlled phase  $\Lambda^{G_4(3)}s(\varphi)$ , whose semantics is  $|x, y, z, t\rangle \mapsto \begin{cases} e^{i\varphi} |x, y, z, t\rangle & \text{if } xyz = G_4(3) \\ |x, y, z, t\rangle & \text{otherwise} \end{cases}$ .

The decoding map is formally defined as follows:

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

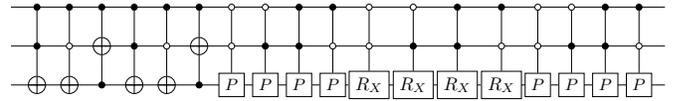
- $D_{k,n}(C_1 \otimes C_2) = D_{k+\ell_1,n}(C_2) \circ D_{k,n}(C_1)$ , where  $C_1$  is acting on  $\ell_1$  modes;
- $D_{k,n}(C_2 \circ C_1) = D_{k,n}(C_2) \circ D_{k,n}(C_1)$ ;
- $D_{k,n}(\text{---}) = id_n$ .

The remaining generators are treated as follows.

$$\begin{aligned}
D_{k,n}(\boxed{-\varphi-}) &= id_n, & D_{k,n}(\boxed{-\varphi-}) &= \Lambda^{G_n(k)}s(\varphi), \\
D_{k,n}(\text{---}) &= \Lambda^{x_{k,n}}X, & D_{k,n}(\text{---}) &= \Lambda^{x_{k,n}}R_X(-2\theta),
\end{aligned}$$

where  $x_{2k,n} := G_{n-1}(k)$ ,  $y_{2k,n} := \epsilon$ ,  $x_{2k+1,n} := w$  and  $y_{2k+1,n} := 1.0^q$ , where  $q \in \{0, \dots, n-2\}$  and  $w \in \{0, 1\}^{n-q-2}$  are such that  $G_n(2k+1) = wa1.0^q$  for some  $a \in \{0, 1\}$ .

**Example 33.** We consider the optical circuit  $C_1$  obtained in Example 30. With all of the gates  $P$  and  $R_X$  parametrized with  $\frac{\pi}{2}$ , we can show that  $D(C_1) \equiv$



Similarly to the encoding function, the decoding function preserves the semantics up to Gray codes.

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

$$\llbracket D(C) \rrbracket \circ \mathfrak{G}_n = \mathfrak{G}_n \circ \llbracket C \rrbracket.$$

*Proof.* The proof is by induction.  $\square$

### E. Quantum circuit completeness

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

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

$$\begin{aligned}
E(C_0) &= E_{0,0}(\text{CNOT} \otimes \text{H}) \\
&= E_{2,0}(\text{H}) \circ E_{0,1}(\text{CNOT}) \\
&= \sigma_{2,0,1} \circ \left( \text{CNOT} \otimes \text{CNOT} \right) \otimes^2 \circ \sigma_{2,1,0} \circ \sigma_{0,1,2} \circ \left( \text{CNOT} \otimes \text{CNOT} \right) \circ \sigma_{0,2,1} \\
&= id_8 \circ \left( \text{CNOT} \otimes \text{CNOT} \right) \otimes^2 \circ id_8 \circ \left( \text{CNOT} \otimes \text{CNOT} \right) \circ \left( \text{CNOT} \otimes \text{CNOT} \right) \circ \left( \text{CNOT} \otimes \text{CNOT} \right)
\end{aligned}$$

Fig. 7: Encoding of the circuit discussed in Example 30.

**Lemma 35.** For any  $n$ -qubit raw quantum circuit  $C$ ,

$$\text{QC} \vdash D(E(C)) = C.$$

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

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

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

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

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

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

Hence, it remains the basis cases which are proved as Lemma 64 in Appendix D-D.  $\square$

Note that in general, the decoding function does not preserve the topological equivalence. For instance, with the raw

circuits  $C_1 = \text{CNOT} \otimes \text{CNOT}$  and  $C_2 = \text{CNOT}$ , we have

$$C_1 \equiv C_2 \text{ but } D(C_1) = \text{CNOT} \otimes \text{CNOT} \text{ and } D(C_2) = \text{CNOT}.$$

Thus, the topological rules also have to be mimicked in QC:

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

*Proof.* The proof consists intuitively in verifying that the decoding of every equation of Figure 1 is provable in QC. The proof is given in Appendix D-E.  $\square$

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

*Proof.* The proof consists intuitively in verifying that the decoding of every equation of Figure 6 is provable in QC. The proof is given in Appendix D-F.  $\square$

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

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

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

#### IV. DISCUSSIONS

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

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

$$\begin{aligned}
&\text{CNOT} \otimes \text{CNOT} = \text{CNOT} \\
&\text{CNOT} \otimes \text{CNOT} = \text{CNOT} \otimes \text{CNOT} \otimes \text{CNOT} \otimes \text{CNOT} \otimes \dots \otimes \text{CNOT} \otimes \text{CNOT} \quad (\text{r}')
\end{aligned}$$

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

A natural application of the completeness result is to design procedures for quantum circuit optimisation based on this equational theory. One can take advantage of the terminating and confluent rewriting system for optical circuits [30] by mimicking the applications of the rewrite rules on quantum

circuits. However, the exponential blowup of the encoding map makes this approach probably inefficient as it is and requires some improvements.

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

#### Acknowledgements

The authors wish to thank Emmanuel Jeandel for his comments on an early version of this paper. This work is supported by the PEPR integrated project EPiQ ANR-22-PETQ-0007 part of Plan France 2030, the CIFRE 2022/0081, the French National Research Agency (ANR) under the research projects SoftQPro ANR-17-CE25-0009-02 and VanQuTe ANR-17-CE24-0035, BPI France under the Concours Innovation PIA3 projects DOS0148634/00 and DOS0148633/00, by the STIC-AmSud project Qapla' 21-STIC-10, and by the European projects NEASQC and HPCQS.

#### REFERENCES

- [1] D. Deutsch, “Quantum computational networks,” *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, vol. 425, no. 1868, pp. 73–90, 1989.
- [2] A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger, and B. Valiron, “Quipper: A scalable quantum programming language,” in *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI’13*, H.-J. Boehm and C. Flanagan, Eds. ACM, 2013, pp. 333–342.
- [3] M. Amy, D. Maslov, and M. Mosca, “Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 33, no. 10, pp. 1476–1489, 2014.
- [4] R. Duncan, A. Kissinger, S. Perdrix, and J. Van De Wetering, “Graph-theoretic simplification of quantum circuits with the ZX-calculus,” *Quantum*, vol. 4, p. 279, 2020.
- [5] A. Kissinger and J. van de Wetering, “Reducing the number of non-Clifford gates in quantum circuits,” *Phys. Rev. A*, vol. 102, p. 022406, Aug. 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.102.022406>
- [6] D. Maslov, C. Young, D. M. Miller, and G. W. Dueck, “Quantum circuit simplification using templates,” in *Design, Automation and Test in Europe*. IEEE, 2005, pp. 1208–1213.
- [7] D. Maslov, G. W. Dueck, D. M. Miller, and C. Negrevergne, “Quantum circuit simplification and level compaction,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 27, no. 3, pp. 436–444, 2008.
- [8] Y. Nam, N. J. Ross, Y. Su, A. M. Childs, and D. Maslov, “Automated optimization of large quantum circuits with continuous parameters,” *npj Quantum Information*, vol. 4, no. 1, pp. 1–12, 2018.
- [9] A. Kissinger and A. M.-v. de Griend, “CNOT circuit extraction for topologically-constrained quantum memories,” *arXiv preprint arXiv:1904.00633*, 2019.
- [10] B. Nash, V. Gheorghiu, and M. Mosca, “Quantum circuit optimizations for NISQ architectures,” *Quantum Science and Technology*, vol. 5, no. 2, p. 025010, 2020.
- [11] S. Aaronson, “Verifiable quantum advantage: What I hope will be done,” Set of slides, presented at *Quantum Advantage Workshop*, Chicago, IL, August 1, 2022. Slide 10. Online at <https://www.scottaaronson.com/talks/whatihope.ppt>.
- [12] X. Bian and P. Selinger, “Generators and relations for 2-qubit Clifford+T operators,” *arXiv preprint arXiv:2204.02217*, 2022.
- [13] B. Coecke and Q. Wang, “ZX-rules for 2-qubit Clifford+T quantum circuits,” in *International Conference on Reversible Computation*. Springer, 2018, pp. 144–161.
- [14] J. Makary, N. J. Ross, and P. Selinger, “Generators and relations for real stabilizer operators,” in *Proceedings of the 18th International Conference on Quantum Physics and Logic, QPL 2021*, ser. EPTCS, C. Heunen and M. Backens, Eds., vol. 343, 2021, pp. 14–36.
- [15] A. Ranchin and B. Coecke, “Complete set of circuit equations for stabilizer quantum mechanics,” *Physical Review A*, vol. 90, no. 1, p. 012109, 2014.
- [16] M. Amy, J. Chen, and N. J. Ross, “A finite presentation of CNOT-dihedral operators,” *Electronic Proceedings in Theoretical Computer Science*, vol. 266, pp. 84–97, Feb. 2018. [Online]. Available: <https://doi.org/10.4204%2Fepctcs.266.5>
- [17] K. Iwama, Y. Kambayashi, and S. Yamashita, “Transformation rules for designing CNOT-based quantum circuits,” in *Proceedings of the 39th annual Design Automation Conference*, 2002, pp. 419–424.
- [18] R. Cockett, C. Comfort, and P. Srinivasan, “The category CNOT,” in *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018*, ser. EPTCS, P. Selinger and G. Chiribella, Eds., vol. 287, 2019, pp. 258–293.
- [19] R. Cockett and C. Comfort, “The category TOF,” in *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018*, ser. EPTCS, P. Selinger and G. Chiribella, Eds., vol. 287, 2019, pp. 67–84.
- [20] B. Coecke and R. Duncan, “Interacting quantum observables,” in *International Colloquium on Automata, Languages, and Programming*. Springer, 2008, pp. 298–310.
- [21] —, “Interacting quantum observables: categorical algebra and diagrammatics,” *New Journal of Physics*, vol. 13, no. 4, p. 043016, 2011.
- [22] M. Backens and A. Kissinger, “ZH: A complete graphical calculus for quantum computations involving classical non-linearity,” *Electronic Proceedings in Theoretical Computer Science*, vol. 287, pp. 23–42, Jan. 2019. [Online]. Available: <https://doi.org/10.4204%2Fepctcs.287.2>
- [23] A. Hadzihasanovic, K. F. Ng, and Q. Wang, “Two complete axiomatisations of pure-state qubit quantum computing,” in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09–12, 2018*, A. Dawar and E. Grädel, Eds. ACM, 2018, pp. 502–511. [Online]. Available: <https://doi.org/10.1145/3209108.3209128>
- [24] E. Jeandel, S. Perdrix, and R. Vilmart, “A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics,” in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, 2018, pp. 559–568.
- [25] A. Hadzihasanovic, K. F. Ng, and Q. Wang, “Two complete axiomatisations of pure-state qubit quantum computing,” in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, 2018, pp. 502–511.
- [26] E. Jeandel, S. Perdrix, and R. Vilmart, “Diagrammatic reasoning beyond Clifford+T quantum mechanics,” in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, 2018, pp. 569–578.
- [27] —, “Completeness of the ZX-Calculus,” *Logical Methods in Computer Science*, vol. Volume 16, Issue 2, Jun. 2020. [Online]. Available: <https://lmcs.episciences.org/6532>
- [28] R. Vilmart, “A near-minimal axiomatisation of ZX-calculus for pure qubit quantum mechanics,” in *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, 2019, pp. 1–10.
- [29] N. de Beaudrap, A. Kissinger, and J. van de Wetering, “Circuit extraction for ZX-diagrams can be #P-hard,” *arXiv preprint arXiv:2202.09194*, 2022.
- [30] A. Clément, N. Heurtel, S. Mansfield, S. Perdrix, and B. Valiron, “LOV-calculus: A graphical language for linear optical quantum circuits,” 2022. [Online]. Available: <https://arxiv.org/abs/2204.11787>
- [31] J. Paixão and P. Sobociński, “Calculational proofs in relational graphical linear algebra,” in *Formal Methods: Foundations and Applications*, G. Carvalho and V. Stolz, Eds. Springer, 2020, pp. 83–100.
- [32] S. MacLane, “Categorical algebra,” *Bulletin of the American Mathematical Society*, vol. 71, no. 1, pp. 40 – 106, 1965.
- [33] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, “Elementary gates for quantum computation,” *Physical Review A*, vol. 52, no. 5, pp. 3457–3467, Nov. 1995. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevA.52.3457>
- [34] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2002.

- [35] N. Abdessaied, M. Soeken, and R. Drechsler, "Quantum circuit optimization by hadamard gate reduction," in *International Conference on Reversible Computation*. Springer, 2014, pp. 149–162.
- [36] A. Cowtan, S. Dilkes, R. Duncan, W. Simmons, and S. Sivarajah, "Phase gadget synthesis for shallow circuits," *Electronic Proceedings in Theoretical Computer Science*, vol. 318, pp. 213–228, May 2020. [Online]. Available: <https://doi.org/10.4204%2Feptcs.318.13>

APPENDIX A  
CONTENTS

All the equations from Equation (6) to Equation (19) are proven either directly from the axioms of  $QC_0$ , given in Figure 3, or from the equations already proven. Those proofs are in Appendix B-A.

Proposition 10 is proven in Appendix B-B.

In Appendix B-C, we highlight the inductive properties of multicontrolled gates which will be used in the inductive proofs of the following appendices, in the form of Lemmas 39 to 44.

Lemmas 45 to 47 are introduced and proven by induction in Appendix B-D. Alongside with Equation (24) proven in Appendix B-E, those properties are used to prove Propositions 11 and 12 in Appendix B-F.

To prove Proposition 13, we introduce Lemma 48. We do a proof by induction with both hypotheses, to prove at the same time Proposition 13 and Lemma 48, as detailed in Appendix B-G.

Appendices B-H, C-B and C-D introduce and prove Equations (28) and (29) and Lemmas 50 to 54. Those properties on multi-controlled gates are to be used in other later proofs.

Propositions 15, 16, 17, 18, 19, 20, 21 and 22 are respectively proven in Appendix C-A, C-C, C-E, C-F, C-G, C-H, C-I and C-J.

Theorem 26 is proven in Appendix D-A.

Appendices D-B and D-C introduce convenient notations and Lemmas 57 to 61, useful for proving the main result.

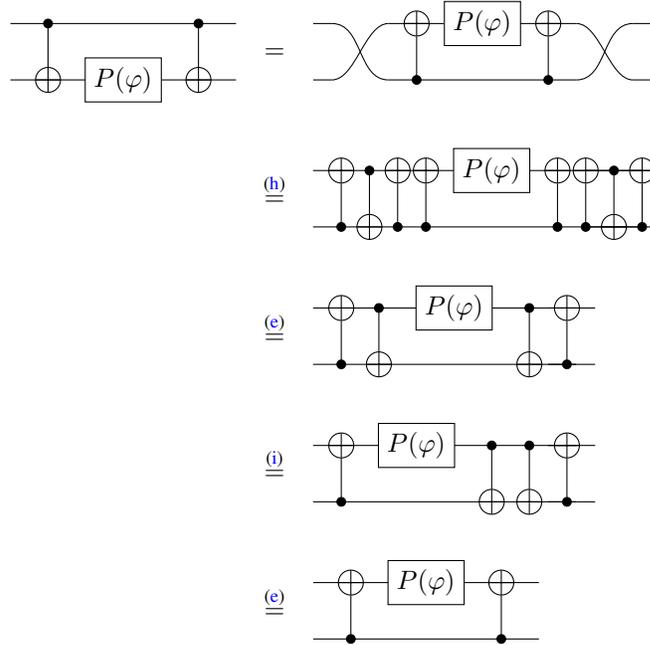
Finally, Lemmas 35, 36 and 37 are proven in Appendices D-D, D-E and D-F.

The  $\sigma_{k,n,\ell}$  are defined in Appendix D-G.

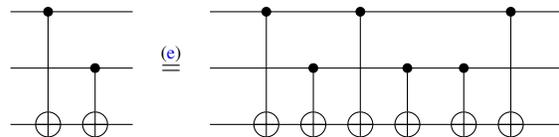
APPENDIX B  
USEFUL QUANTUM CIRCUITS EQUATIONS

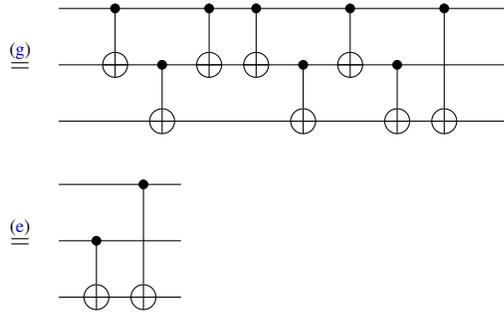
A. Proofs of Equations (6) to (19)

Proof of Equation (6):

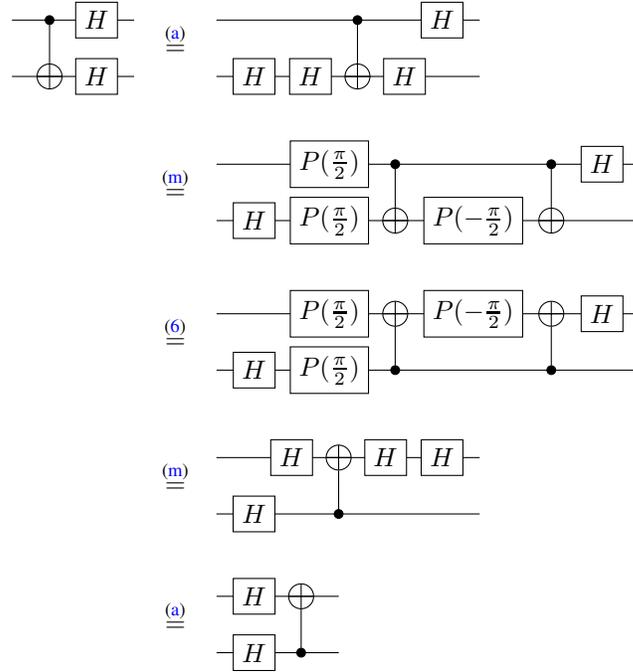


Proof of Equation (8):



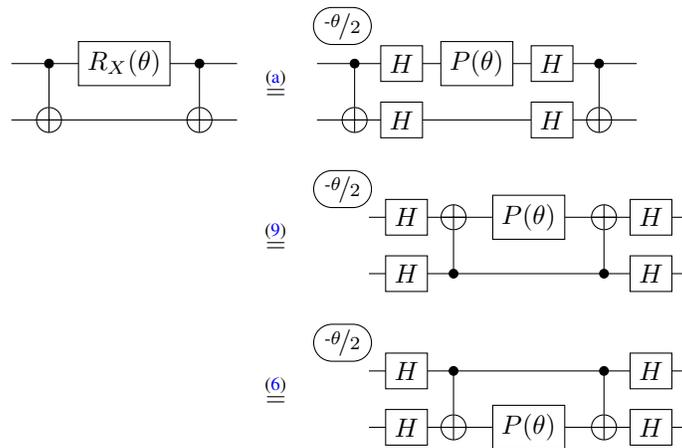


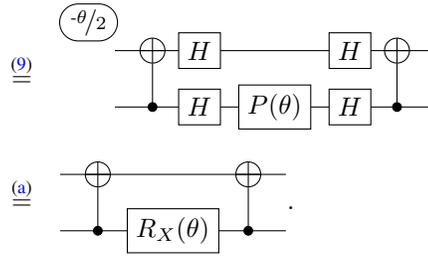
Proof of Equation (9):



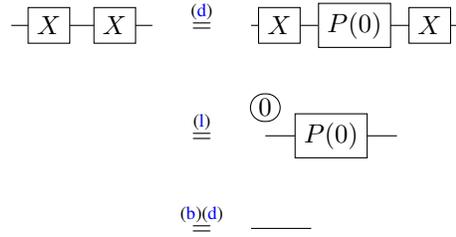
Note that the second use of Equation (m) relies on the fact that  $\text{CNOT} \equiv \text{CNOT} \circ \text{CNOT}$ , and uses a few topological rules.

Proof of Equation (7):

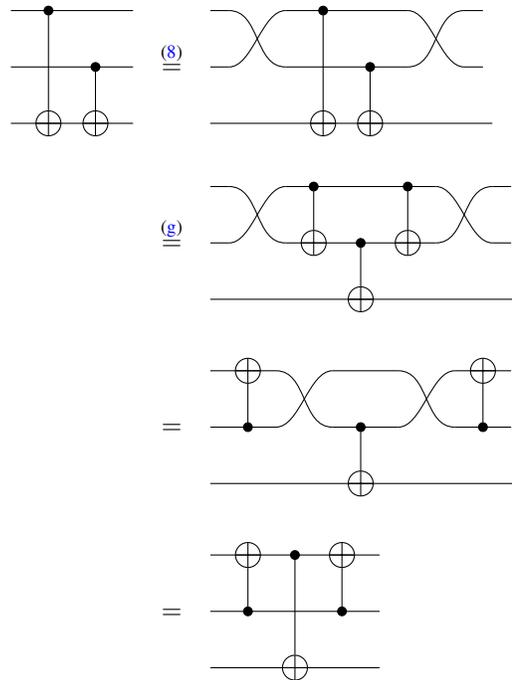




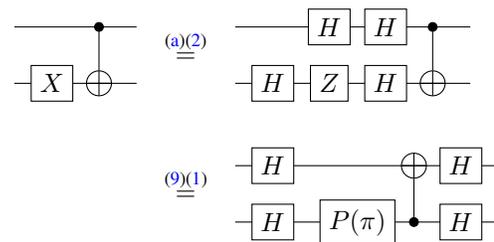
Proof of Equation (10):



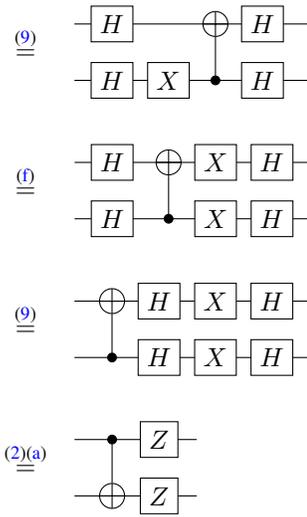
Proof of Equation (11):



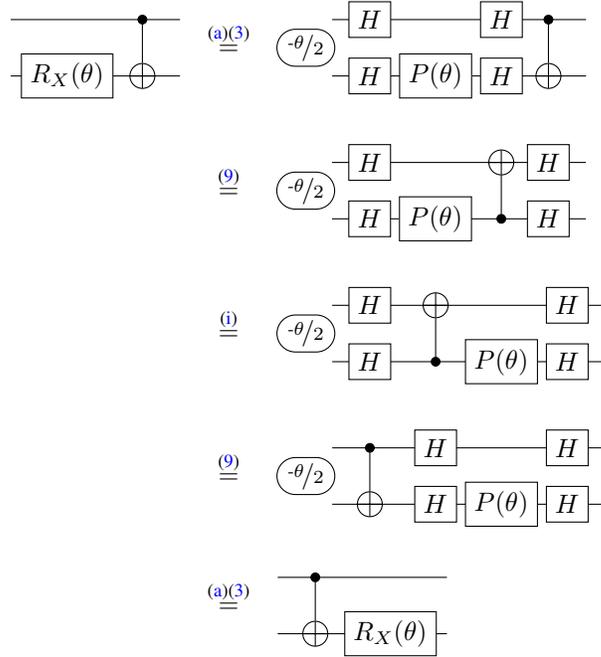
Proof of Equation (12):



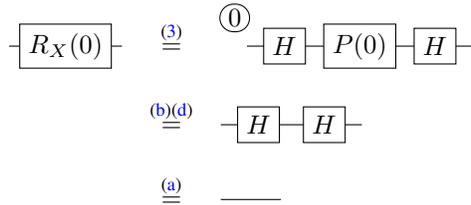




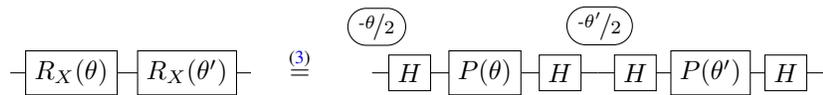
Proof of Equation (16):



Proof of Equation (17):

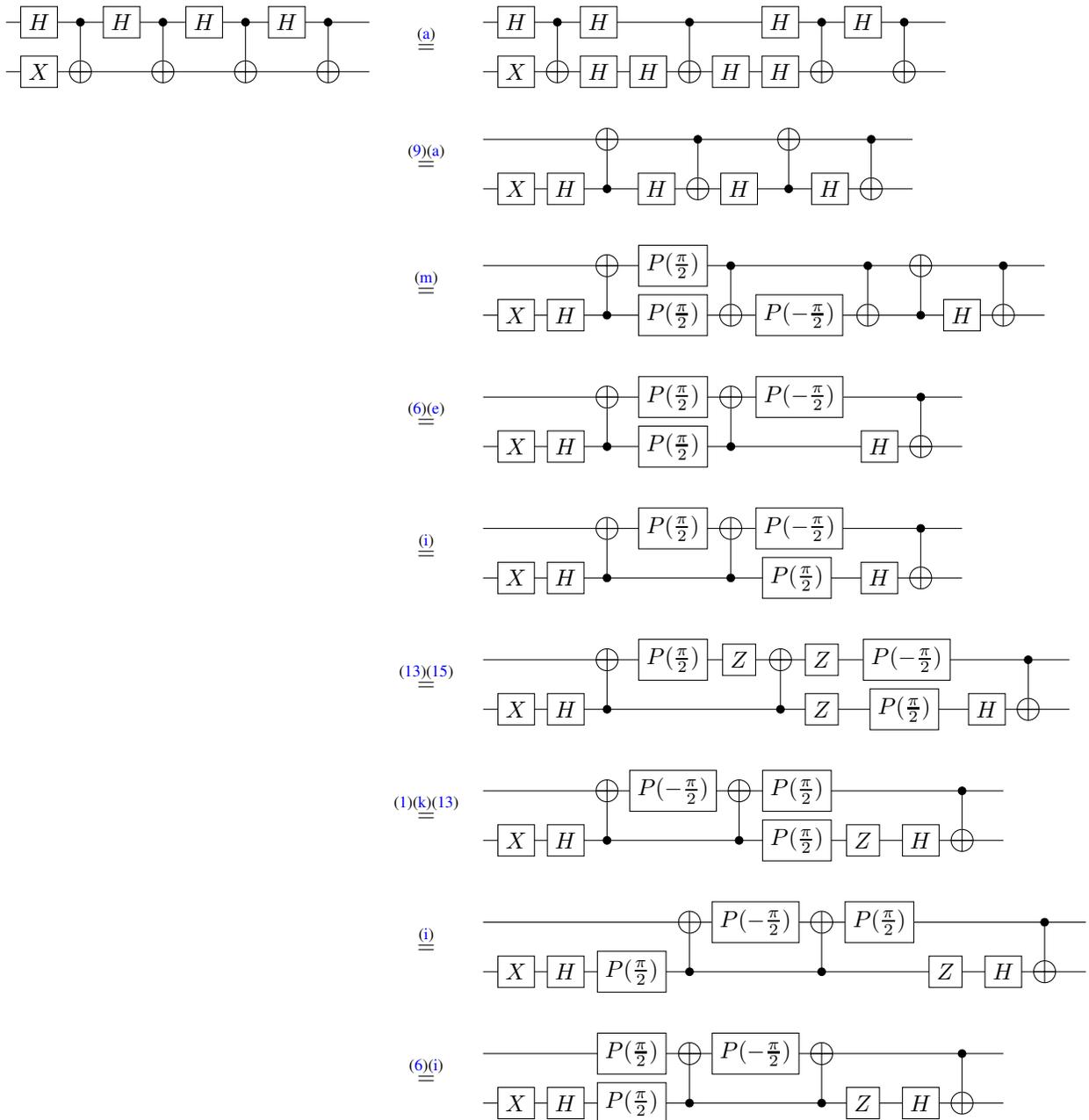


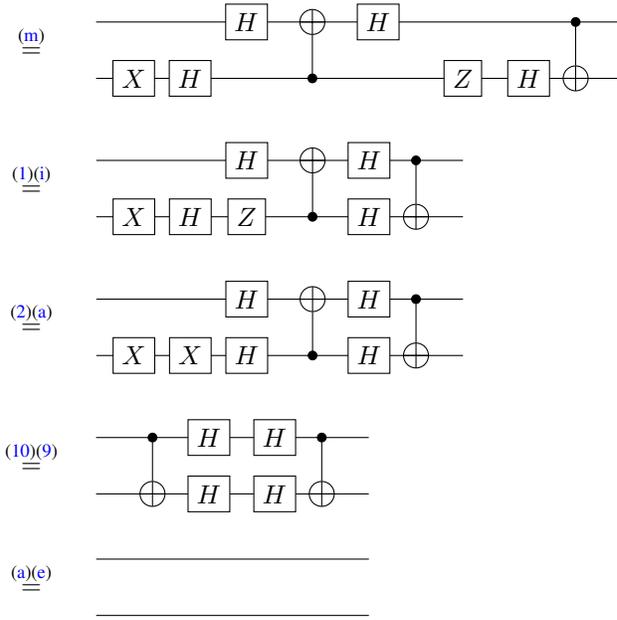
Proof of Equation (18):



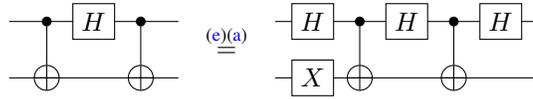
$$\begin{aligned}
&\stackrel{(a)}{=} \begin{array}{c} \textcircled{-\theta/2} \qquad \textcircled{-\theta'/2} \\ \text{---} [H] \text{---} [P(\theta)] \text{---} [P(\theta')] \text{---} [H] \text{---} \end{array} \\
&\stackrel{(c)(k)}{=} \begin{array}{c} \textcircled{-\frac{\theta+\theta'}{2}} \\ \text{---} [H] \text{---} [P(\theta+\theta')] \text{---} [H] \text{---} \end{array} \\
&\stackrel{(3)}{=} \text{---} [R_X(\theta+\theta')] \text{---}
\end{aligned}$$

Proof of Equation (19):



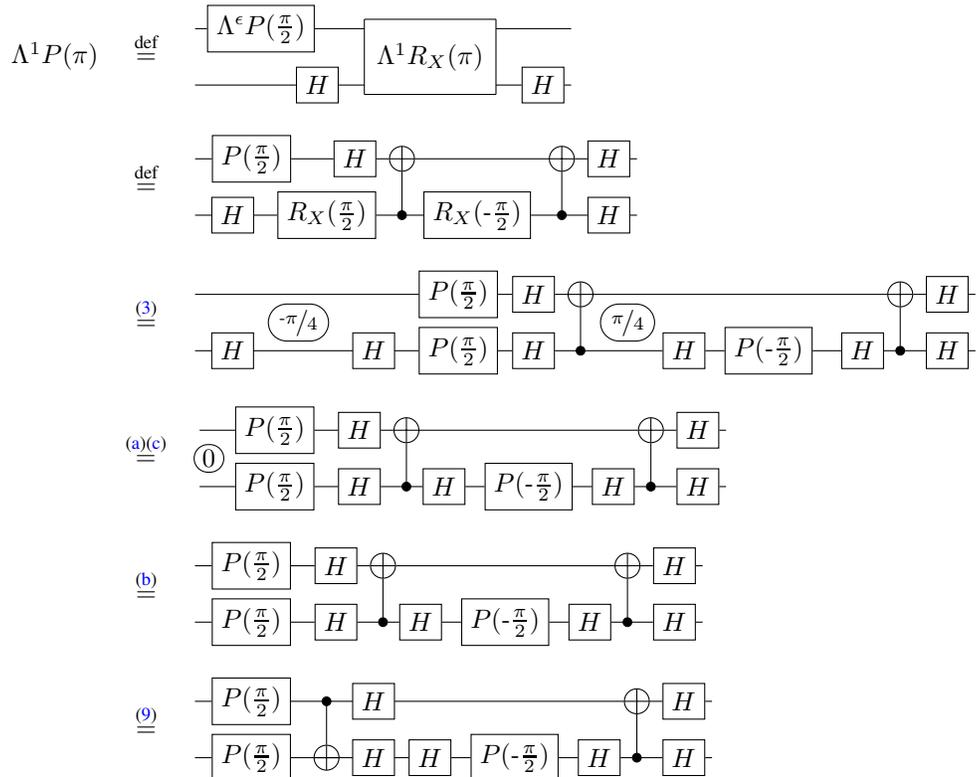


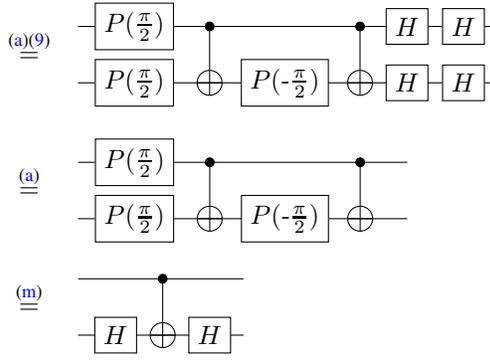
It follows that



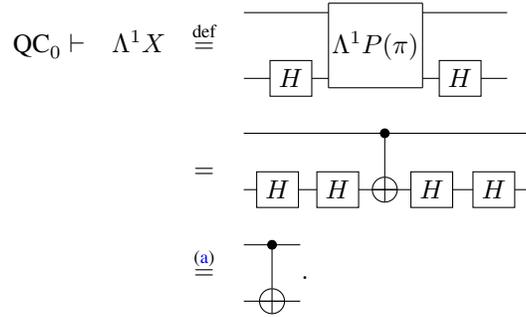
### B. Proof of Proposition 10

First, we can notice that





It follows that



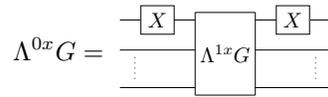
### C. Inductive properties for multi-controls: Lemmas 39 to 44

The following technical lemmas highlight the inductive properties of the circuits  $\Lambda^x G$ . They are at the heart of the proof of the completeness result.

**Lemma 39** (Base case for the inductive properties). *For all  $G \in \{s(\psi), X, R_X(\theta), P(\varphi)\}$ , if  $\epsilon$  is the empty list,  $\Lambda^\epsilon G = G$ .*

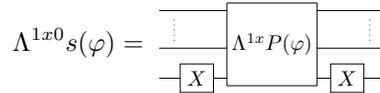
*Proof.* In the case of an empty list, in Definition 7 there are no gates  $X^{\bar{x}_i}$ , and  $\Lambda^\epsilon G = \lambda^0 G$ . We can then check in Definition 6 that each  $\lambda^0 G$  is  $G$ : by definition this is true for  $R_X(\theta)$ ,  $s(\psi)$  and  $P(\theta)$ . For  $X$  we fall back on the definition of  $X$  as  $HP(\pi)H = HZH$ .  $\square$

**Lemma 40** (Inductive properties for  $\Lambda^x G$ ). *For all  $x \in \{0, 1\}^k$ , and  $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$ ,*



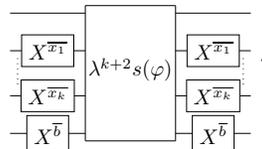
*Proof.* This is directly derived from the definition of  $\Lambda^x G$ : the  $X^{\bar{x}_i}$ 's on the top wire are  $X$  for  $\Lambda^{0x} G$  and the identity for  $\Lambda^{1x} G$ , while the  $X^{\bar{x}_i}$ 's on the lower wires are the same.  $\square$

**Lemma 41** (Inductive properties for  $\Lambda^x s(\varphi)$ ). *Suppose that  $x$  is a  $k$ -length list of booleans. We then have  $\Lambda^1 s(\varphi) = P(\varphi)$ ,  $\Lambda^{1x1} s(\varphi) = \Lambda^{1x} P(\varphi)$ , and*

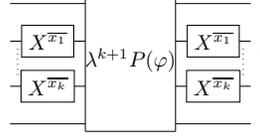


*Proof.* By definition,  $\Lambda^1 s(\varphi)$  is  $\lambda^1 s(\varphi)$ : there are no  $X^{\bar{x}_i}$  since the list only contains a single 1. By definition,  $\lambda^1 s(\varphi)$  is  $\lambda^0 P(\varphi)$ , which is  $P(\varphi)$ .

Suppose now that  $x$  is a  $k$ -length list of booleans, and  $b$  is a single boolean. Consider  $\Lambda^{1xb} s(\varphi)$ : by definition it is

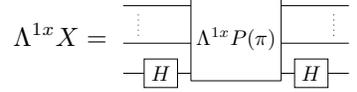


By definition,  $\lambda^{k+2}s(\varphi) = \lambda^{k+1}P(\varphi)$ . Now,  $\Lambda^{1x}P(\varphi)$  is

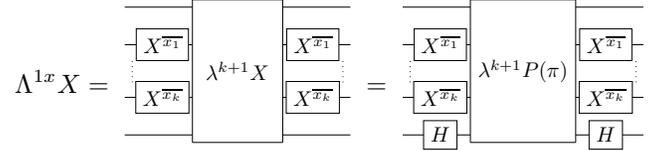


We directly recover  $\Lambda^{1x^1}s(\varphi)$ , i.e. when  $b = 1$ , and the case  $b = 0$  since this just amounts to add the two gates  $X^{\bar{0}} = X^1 = X$  on the bottom wire.  $\square$

**Lemma 42** (Inductive properties of  $\Lambda^x X$ ). *Suppose that  $x$  is a  $k$ -length list of boolean. Then*

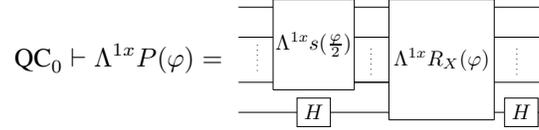


*Proof.* By definition,

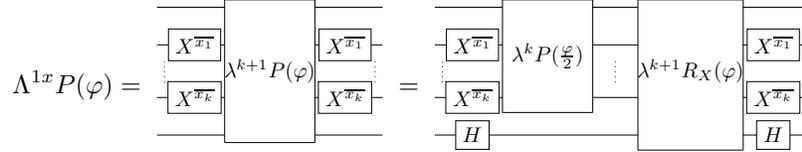


which is exactly the right-hand-side of the desired equation.  $\square$

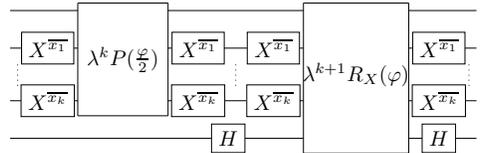
**Lemma 43** (Inductive properties of  $\Lambda^x P(\varphi)$ ). *Suppose that  $x$  is a  $k$ -length list of boolean. Then*



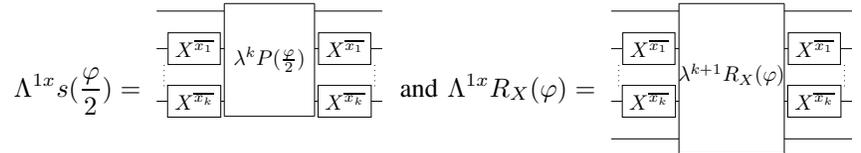
*Proof.* By definition,



Since  $XX$  is the identity according to Equation (10), this is equal to

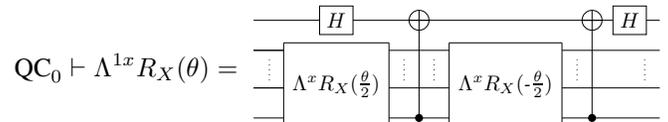


We can conclude by noting that

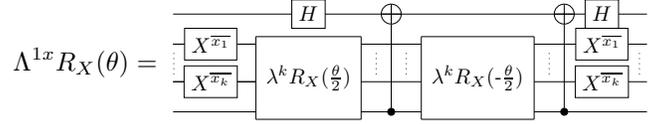


$\square$

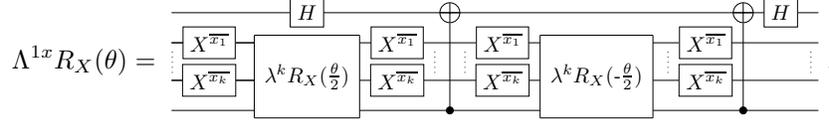
**Lemma 44** (Inductive properties of  $\Lambda^x R_X(\varphi)$ ). *Suppose that  $x$  is a  $k$ -length list of boolean. Then*



*Proof.* By definition of  $\Lambda^{1^x} R_X(\theta)$  and  $\lambda^{k+1} R_X(\theta)$ , we have:



Using Equation (10), we infer that

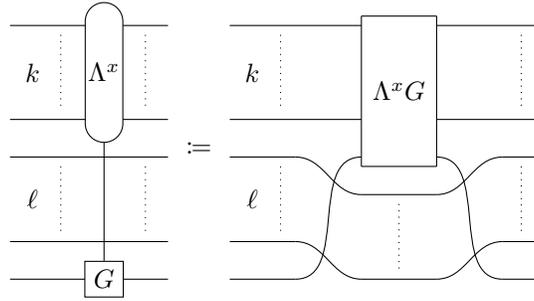


We can then conclude by using the definition of  $\Lambda^x R_X(\frac{\theta}{2})$  and  $\Lambda^x R_X(-\frac{\theta}{2})$  (and the deformation of circuits coming from the prop structure).  $\square$

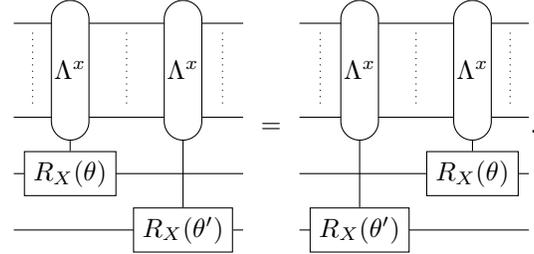
Since these lemmas are essentially consequences of the definitions (except for the use of Equation (10) in Lemmas 43 and 44), in the following we will mostly keep their uses implicit.

#### D. Ancillary lemmas: Lemmas 45 to 47

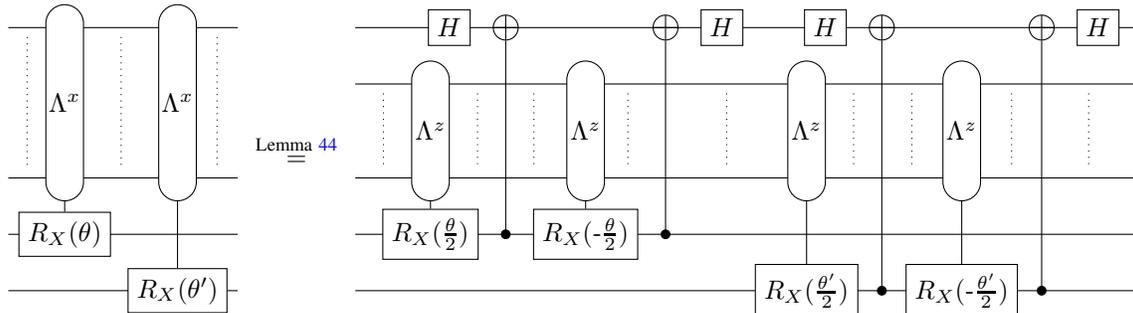
For the following lemmas, it is convenient to introduce a graphical notation of multi-controlled gate which allows for more flexibility in the position of the target qubit, relatively to the control qubits:



**Lemma 45.** For any  $x \in \{0, 1\}^k$ ,

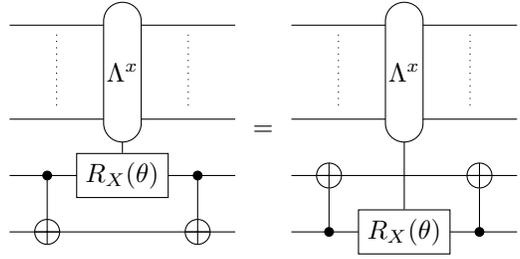


*Proof.* We proceed by induction on  $k$ . If  $k = 0$ , then the equality is a consequence of the topological rules. If  $k \geq 1$ , by Equation (10) we can assume without loss of generality that  $x = 1z$  with  $z \in \{0, 1\}^{k-1}$ . One has

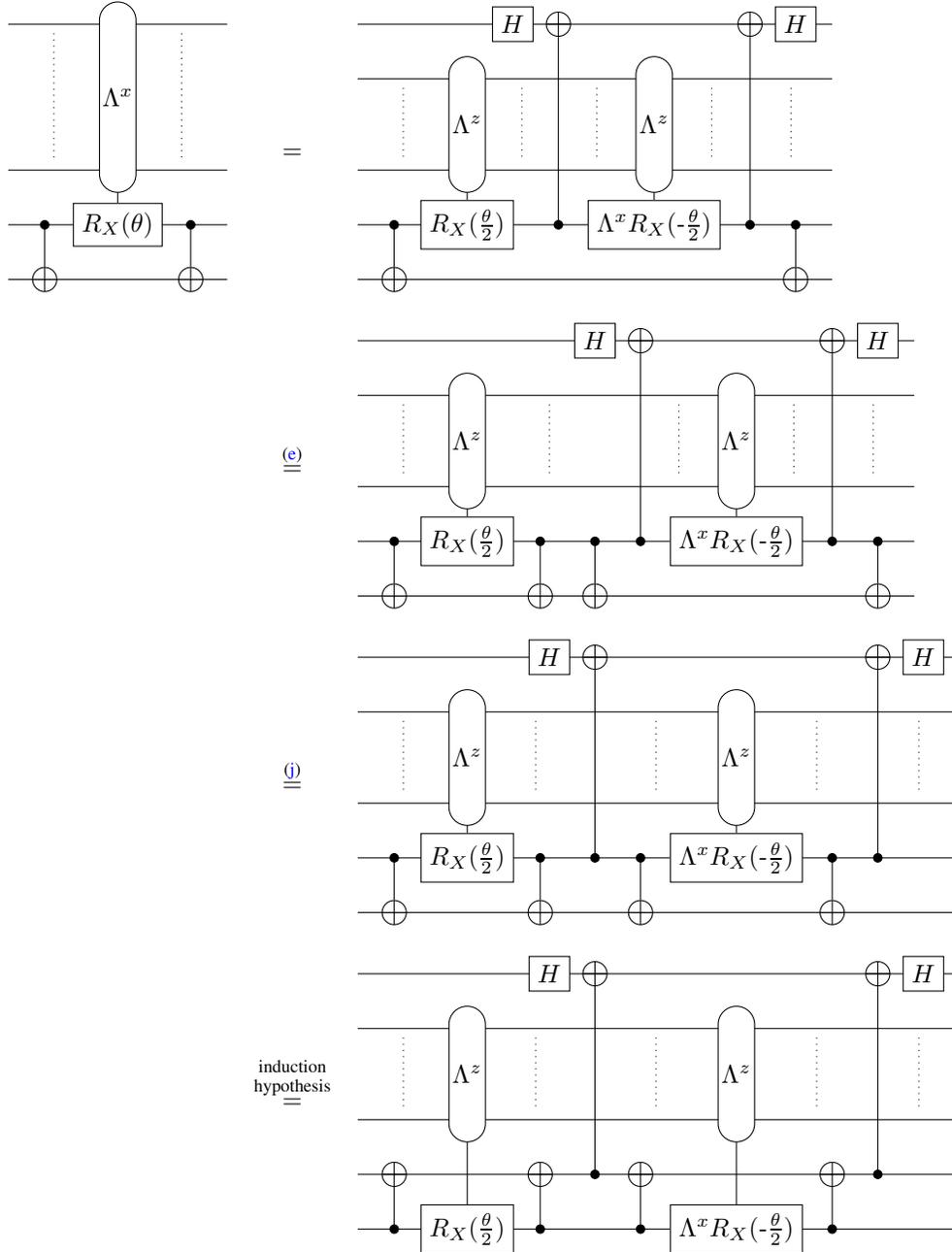


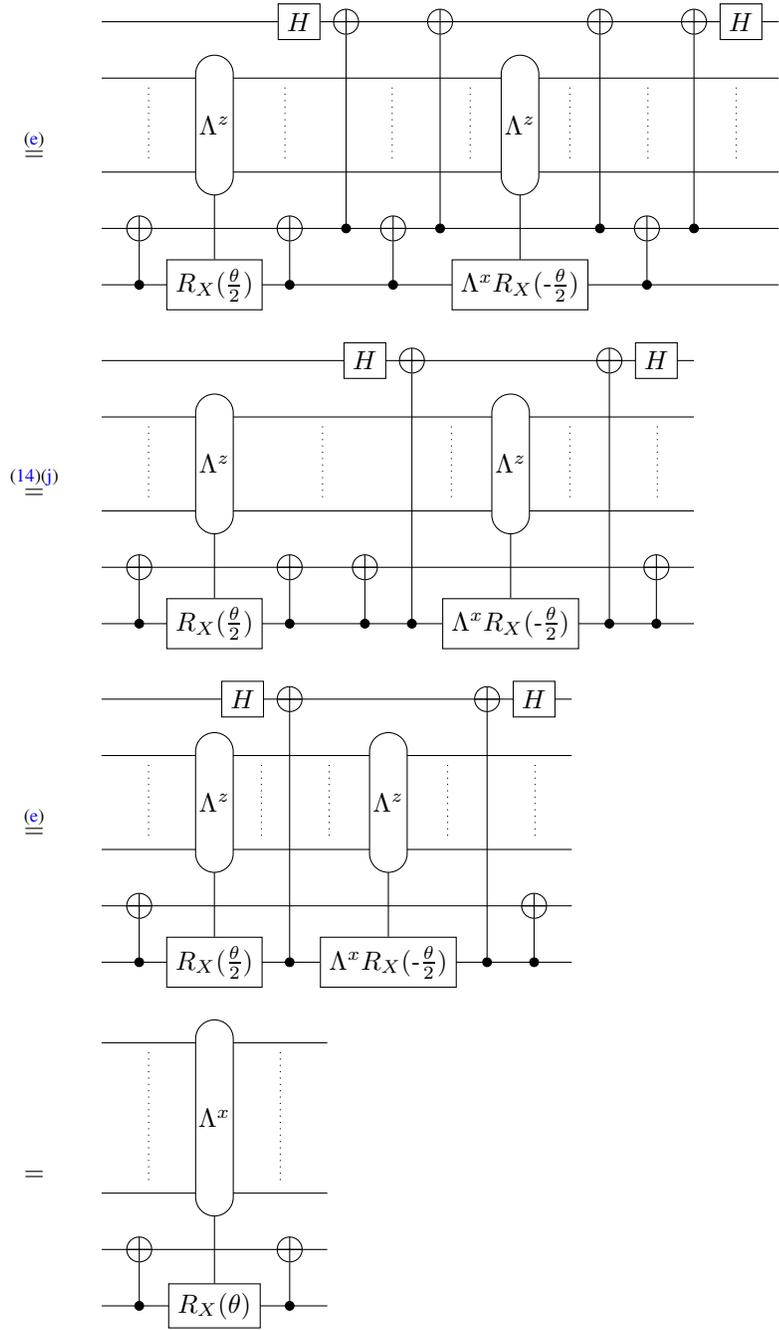
then it is easy to see that the two parts commute by induction hypothesis and Equations (8) and (a), together with topological rules.  $\square$

**Lemma 46.** For any  $x \in \{0, 1\}^k$ ,



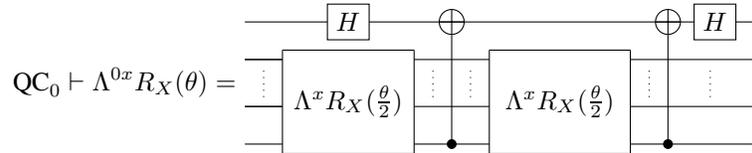
*Proof.* We proceed by induction on  $k$ . If  $k = 0$ , then the result is just Equation (7). If  $k \geq 1$ , then we can assume without loss of generality that  $x = 1z$  with  $z \in \{0, 1\}^{k-1}$ . One has





□

**Lemma 47.** For any  $x \in \{0, 1\}^k$ ,



*Proof.* The proof relies on the following property:

$$\text{QC}_0 \vdash \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \Lambda^x R_X(\theta) \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} = \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \Lambda^x R_X(-\theta) \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \quad (25)$$

that we prove by induction on the length of  $x$  as follows:

If  $x = \epsilon$ , then

$$\begin{aligned}
 \boxed{Z} \boxed{R_X(\theta)} &\stackrel{(3)}{=} \boxed{Z} \overset{\ominus \theta/2}{\text{---}} \boxed{H} \boxed{P(\theta)} \boxed{H} \\
 &\stackrel{(a)(2)}{=} \boxed{H} \overset{\ominus \theta/2}{\text{---}} \boxed{X} \boxed{P(\theta)} \boxed{H} \\
 &\stackrel{(10)(1)(c)}{=} \boxed{H} \overset{\oplus \theta/2}{\text{---}} \boxed{P(-\theta)} \boxed{X} \boxed{H} \\
 &\stackrel{(2)(3)(a)}{=} \boxed{R_X(-\theta)} \boxed{Z}
 \end{aligned}$$

If  $x \neq \epsilon$ , then the commutation is a direct consequence of the induction hypothesis and Equation (i).

Given this property, the result can be deduced as follows:

$$\begin{aligned}
 \Lambda^{0x} R_X(\theta) &= \begin{array}{c} \boxed{X} \boxed{H} \oplus \oplus \boxed{H} \boxed{X} \\ \vdots \\ \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \quad \Lambda^x R_X(-\frac{\theta}{2}) \quad \vdots \\ \vdots \end{array} \\
 &\stackrel{(2)(a)}{=} \begin{array}{c} \boxed{H} \boxed{Z} \oplus \oplus \boxed{H} \boxed{X} \\ \vdots \\ \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \quad \Lambda^x R_X(-\frac{\theta}{2}) \quad \vdots \\ \vdots \end{array} \\
 &\stackrel{(15)}{=} \begin{array}{c} \boxed{H} \oplus \boxed{Z} \oplus \oplus \boxed{H} \boxed{X} \\ \vdots \\ \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \quad \Lambda^x R_X(-\frac{\theta}{2}) \quad \vdots \\ \vdots \end{array} \\
 &\stackrel{(25)}{=} \begin{array}{c} \boxed{H} \oplus \oplus \boxed{Z} \oplus \oplus \boxed{H} \boxed{X} \\ \vdots \\ \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \quad \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \\ \vdots \end{array} \\
 &\stackrel{(15)(1)(i)(13)}{=} \begin{array}{c} \boxed{H} \oplus \oplus \boxed{Z} \boxed{H} \boxed{X} \\ \vdots \\ \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \quad \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \\ \vdots \end{array} \\
 &\stackrel{(2)(a)(13)}{=} \begin{array}{c} \boxed{H} \oplus \oplus \boxed{H} \\ \vdots \\ \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \quad \Lambda^x R_X(\frac{\theta}{2}) \quad \vdots \\ \vdots \end{array}
 \end{aligned}$$

□

E. Proof of Equation (24)

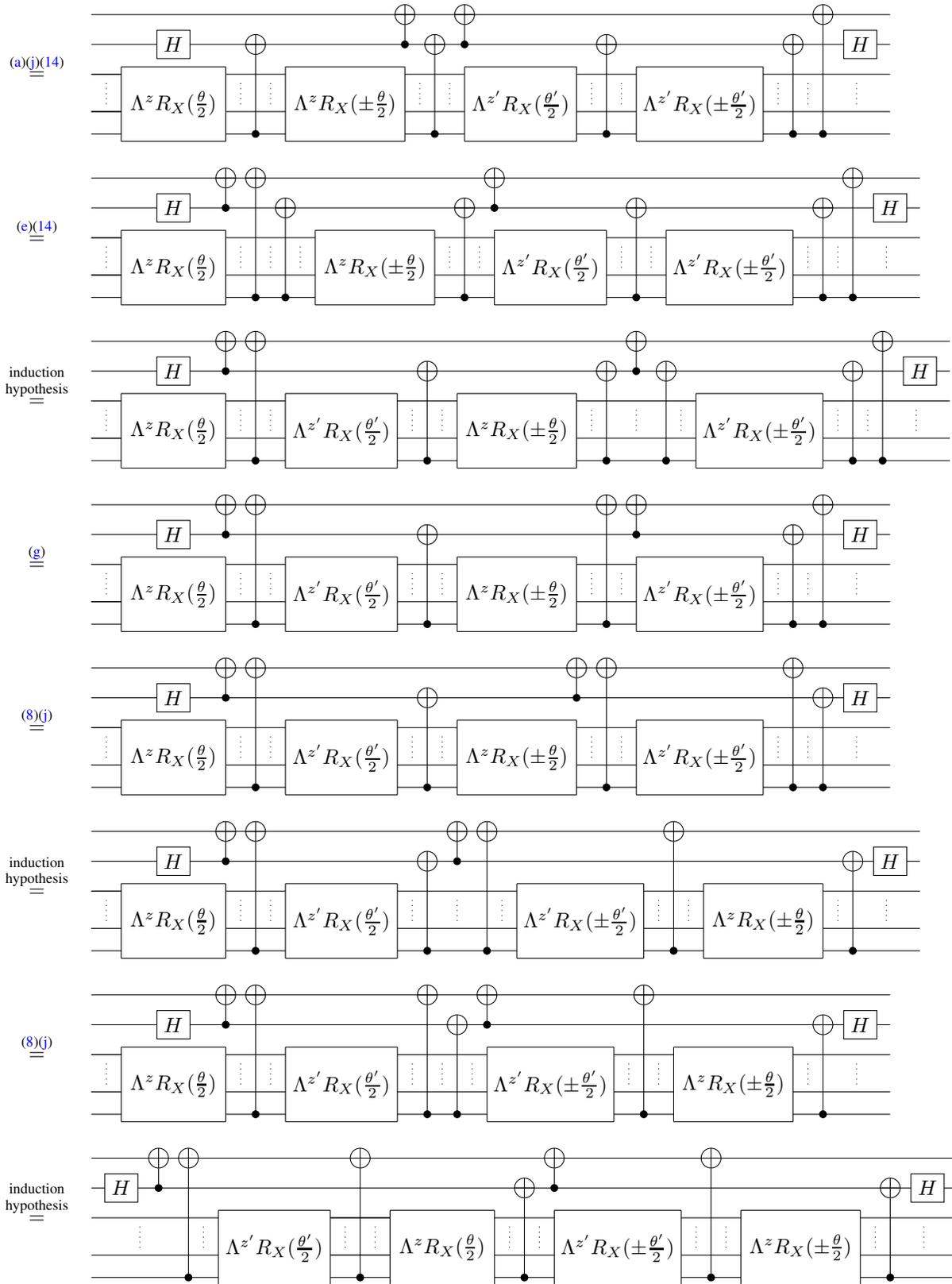
We actually prove a slightly more general result: for any  $x, x' \in \{0, 1\}^k$ ,

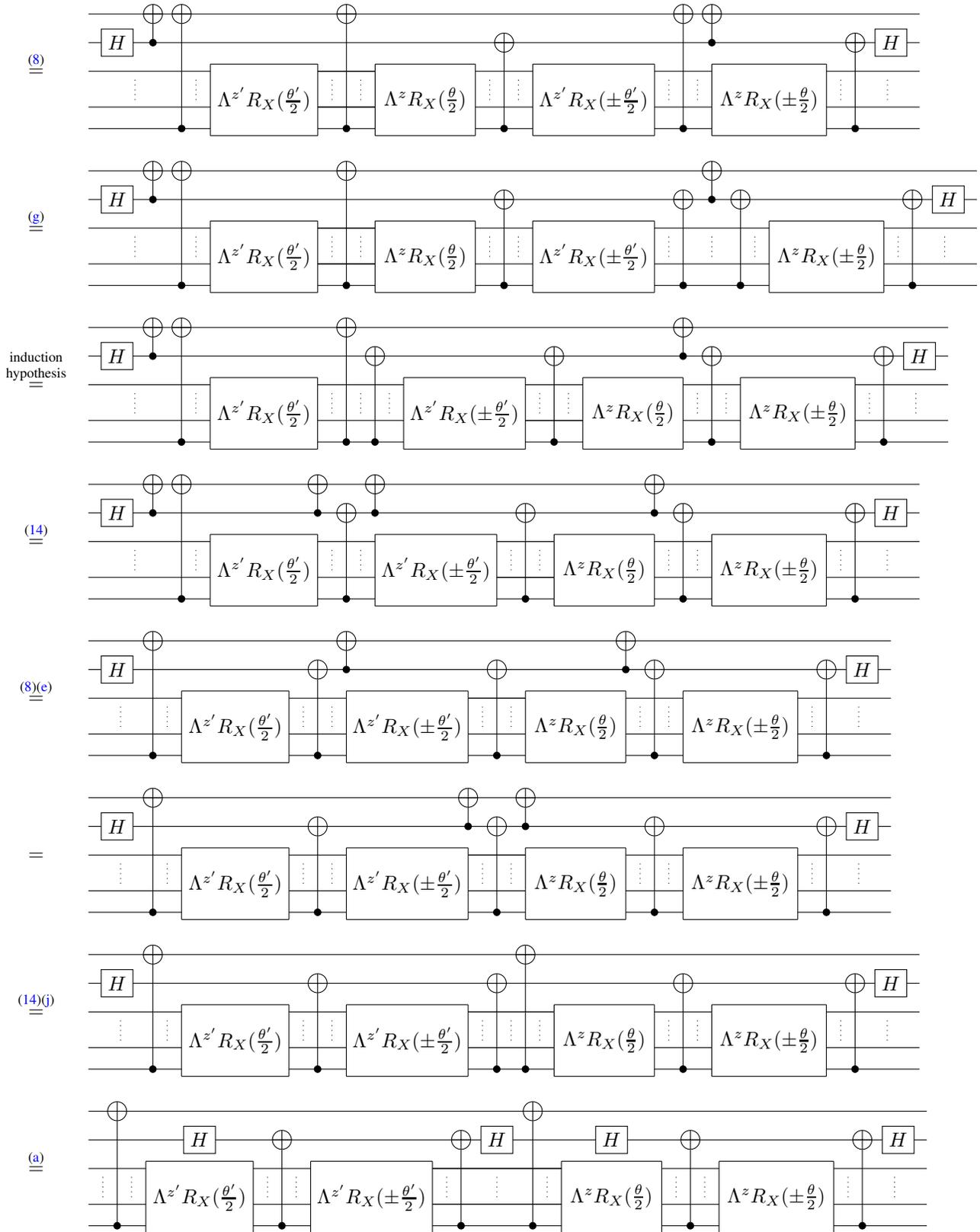
Equation (24) corresponds to the case where  $x = x'$ .

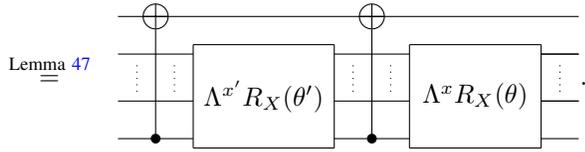
*Proof of Equation (26).* The proof is by induction on  $x$ .

If  $x = \epsilon$  (i.e.  $k = 0$ ),

If  $k \geq 1$ , then we can write  $x = az$  and  $x' = a'z'$  with  $a, a' \in \{0, 1\}$ . One has (where the  $\pm$  signs correspond respectively to  $(-1)^a$  and  $(-1)^{a'}$ ):







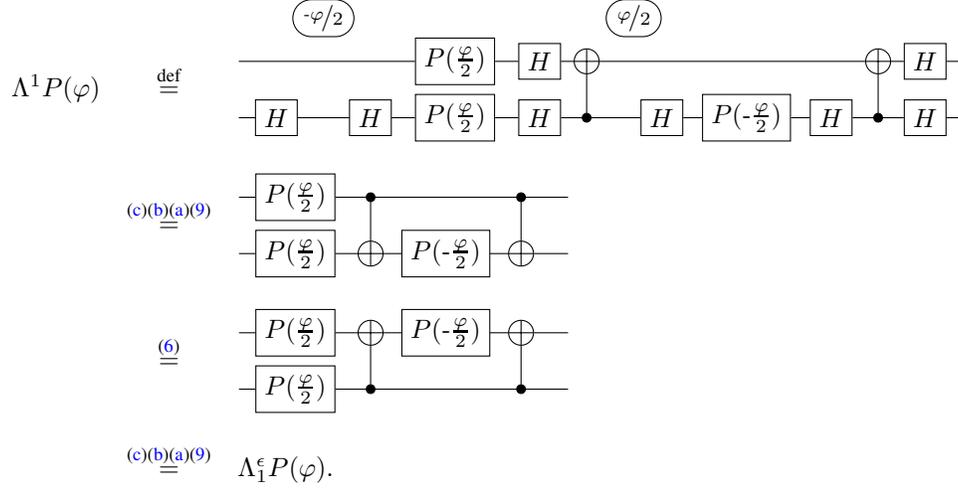
□

### F. Proof of Propositions 11 and 12

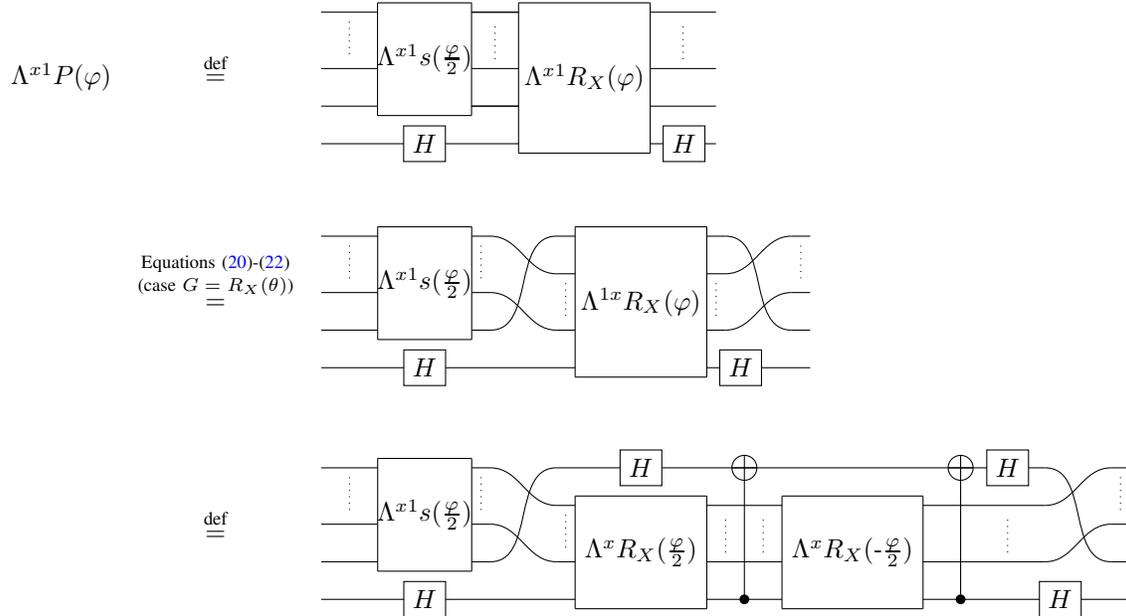
First, we consider the case  $G = R_X(\theta)$  of Equations (20)-(22), for which the proof is a direct induction based on Equation (24) that is proven in Appendix B-E.

Next, we prove Equation (23) in the case  $y = \epsilon$ .

We can assume without loss of generality that  $x = 1^k$ . We proceed by induction on  $k$ . If  $k = 0$ , then



If  $k \geq 1$ , then one has



$$\begin{aligned}
&= \text{Diagram 1} \\
&\stackrel{\text{def}}{=} \text{Diagram 2} \\
&\stackrel{\text{Lemmas 45 and 46}}{=} \text{Diagram 3} \\
&= \text{Diagram 4} \\
&= \text{Diagram 5} \\
&= \Lambda_1^x P(\varphi).
\end{aligned}$$

Now, we can prove Equations (20)-(22) in the case  $G = s(\psi)$  (the cases  $G = P(\varphi)$  and  $G = X$  are direct consequences of this case). Without loss of generality we can assume  $y = \epsilon$  and consider only Equation (20).

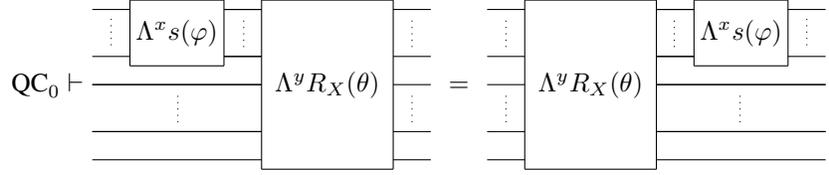
The proof is by induction on the number  $r$  of input qubits of  $\Lambda^{xaby}G$ . If  $z = \epsilon$ , which is necessarily the case in the base case  $r = 2$ , then the result is a direct consequence of the case  $y = \epsilon$  of Equation (23). If  $z \neq \epsilon$ , then using Definitions 6 and 7 (in particular in the case of  $\Lambda^{1x}P(\varphi)$ ), the result is a direct consequence of the induction hypothesis and the case  $G = R_X(\theta)$  of Equations (20)-(22).

Finally, using the definition of  $\Lambda_{y1}^x P(\varphi)$  in terms of  $\Lambda^{xy1}P(\varphi)$ , the general case of Equation (23) follows directly from the case  $y = \epsilon$  and Equations (20)-(22).

### G. Proof of Proposition 13

It remains to treat the  $\Lambda^x P$  and  $\Lambda^x s$  cases of Proposition 13. Those cases are a direct consequence of the following lemma:

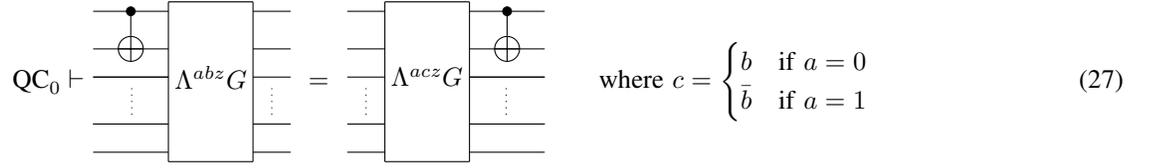
**Lemma 48.** For any  $x \in \{0, 1\}^k$  and  $y \in \{0, 1\}^\ell$  with  $\ell \geq k$ ,



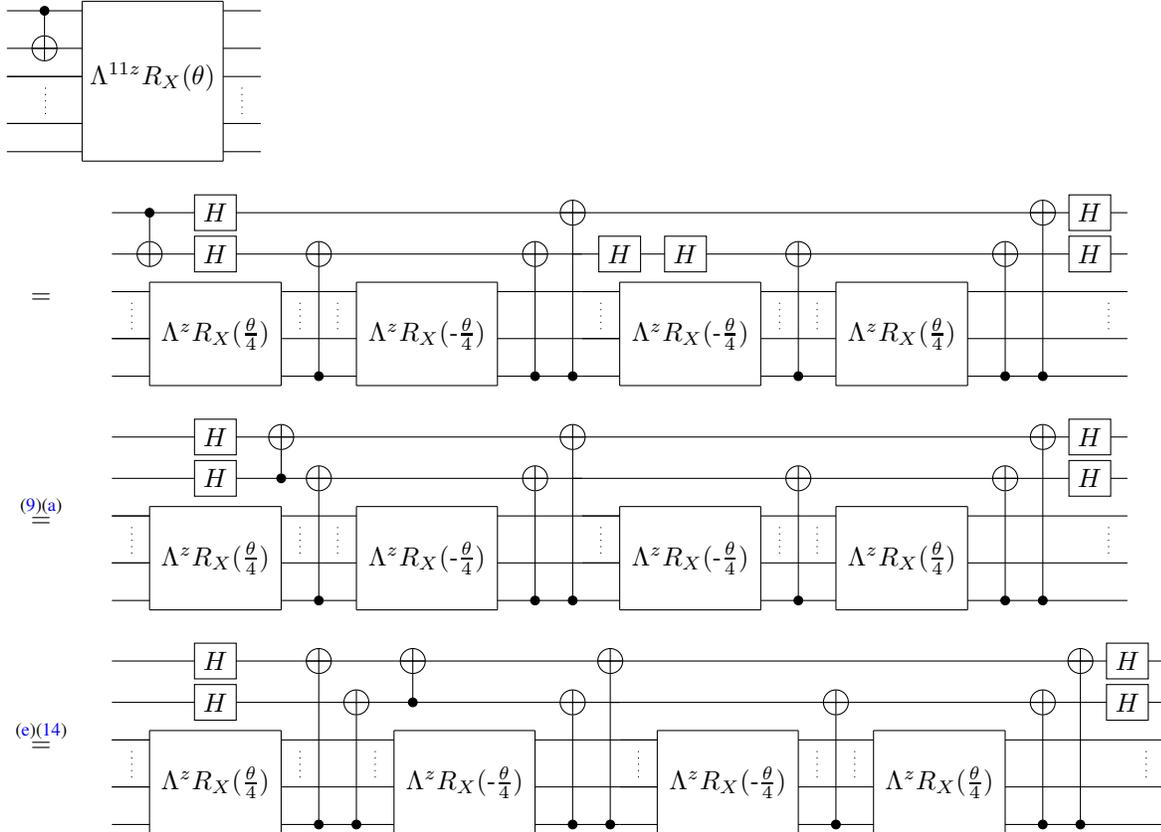
To prove the previous lemma, we do a proof by induction on  $k$ . However, to prove the induction step for  $k \geq 2$ , we use  $\text{QC}_0 \vdash \Lambda^{1^{k-2}} s(\varphi) \circ \Lambda^{1^{k-2}} s(\varphi') = \Lambda^{1^{k-2}} s(\varphi + \varphi')$  and  $\text{QC}_0 \vdash \Lambda^{1^{k-2}} s(0) = id_{k-1}$ , which are the statements of Proposition 13.

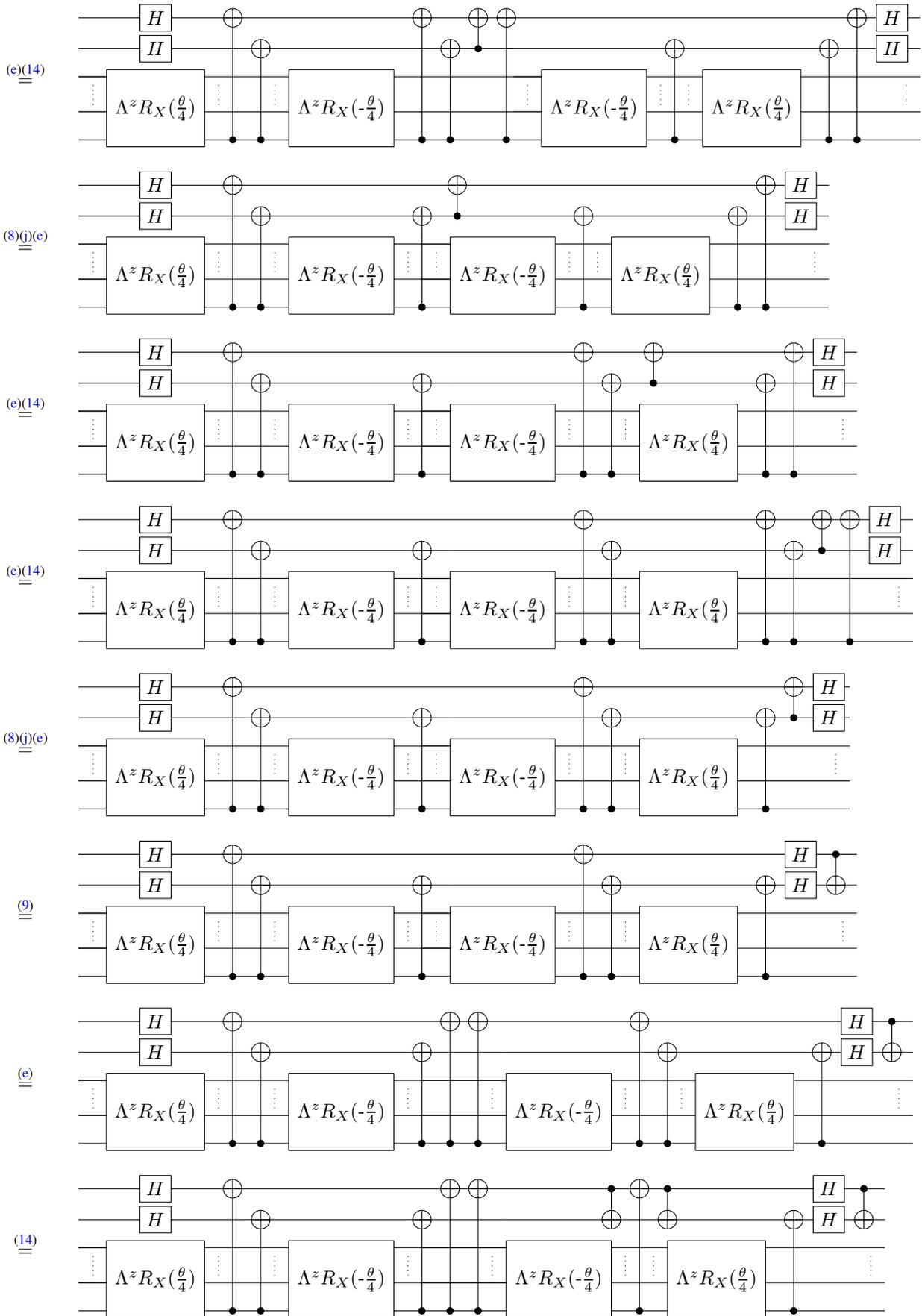
Therefore, we will do a common induction proof for both the other cases of Proposition 13 and for Lemma 48. The plan of the proof is the following. First we prove an ancillary equation (Equation (27)) which is derived from previous lemmas. Then we proceed with the induction proof: for  $k \geq 2$ , Lemma 48 is proved with Proposition 13 for  $k - 2$ , while the induction step of Proposition 13 is directly a consequence of Lemma 48 and Proposition 13 for  $k - 1$ , and the  $\Lambda^x R_X$  case which is already proven.

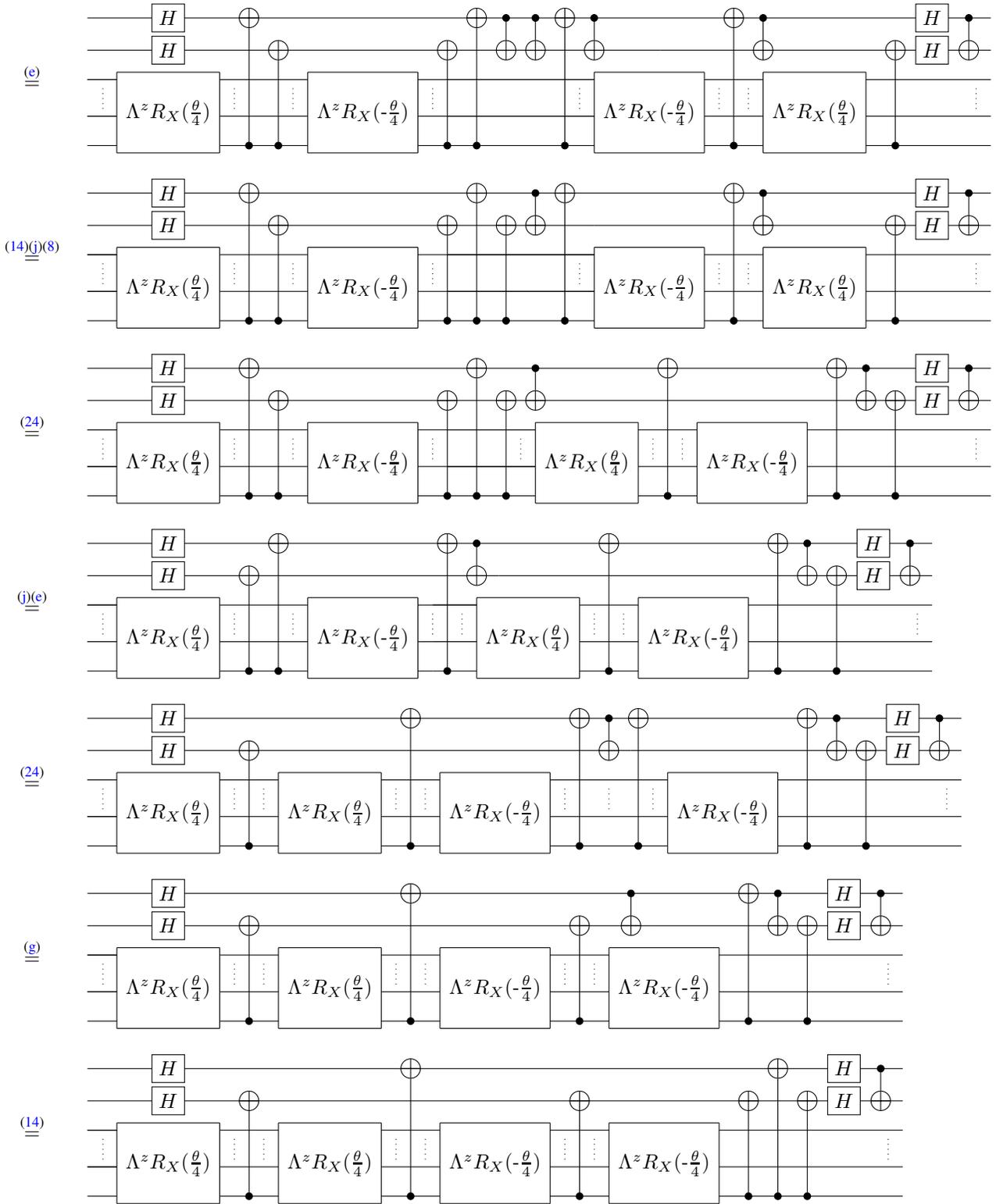
*Proof.* First we prove the following property, which is true for any  $a, b \in \{0, 1\}$ ,  $z \in \{0, 1\}^m$  and  $G \in \{s(\varphi), P(\varphi), R_X(\theta), X\}$ :

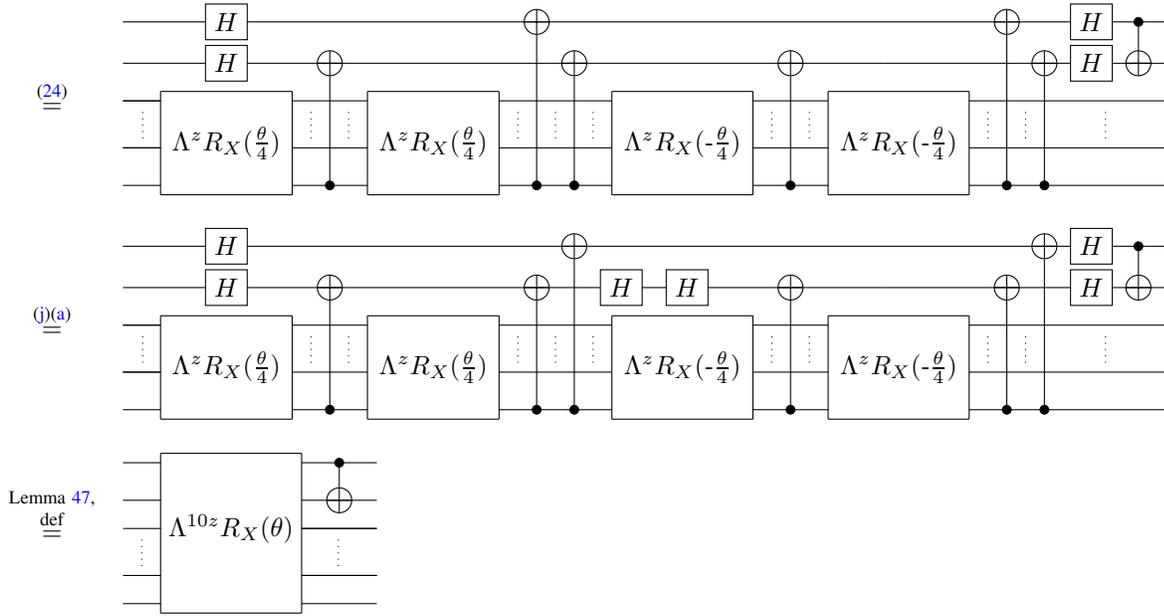


To prove Equation (27), by Equations (10), (12) and (f) we can assume without loss of generality that  $a = b = 1$ . If  $G = R_X(\theta)$ , then

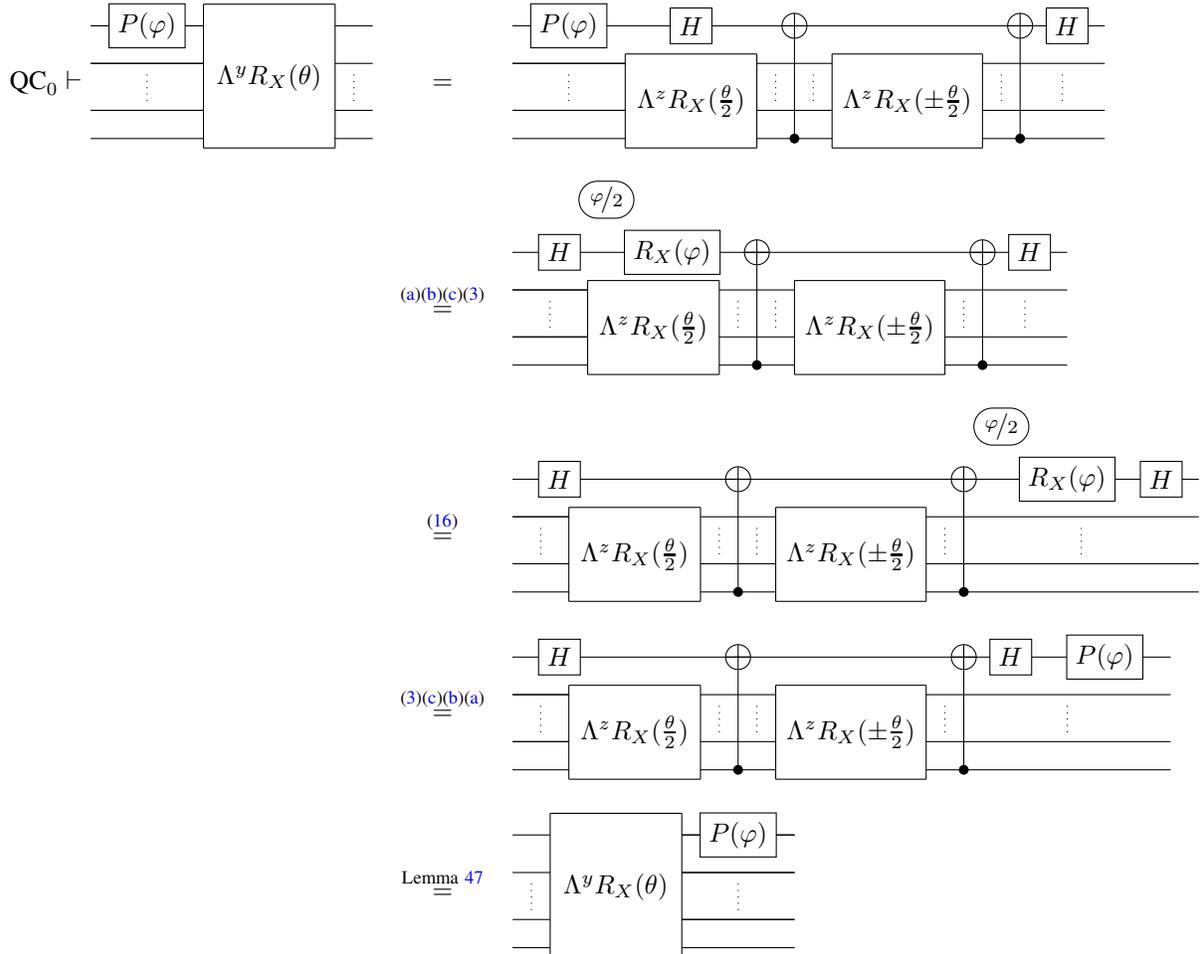








Now, to prove Proposition 13 and Lemma 48, by Equation (10) we can assume without loss of generality that  $x = 1^k$ . We proceed by induction on  $k$ . If  $k = 0$ , then Proposition 13 is a consequence of Equations (b), (c), (d) and (k), and Lemma 48 is a consequence of the topological rules. If  $k = 1$ , then  $\Lambda^x s(\varphi) = P(\varphi)$ . Let  $y = az$  with  $a \in \{0, 1\}$ . By Lemma 47, one has



where the  $\pm$  sign is  $(-1)^a$ . The case of  $k = 1$  for Proposition 13 is then a direct consequence of the previous result, the case with  $R_X$ , Definition 6 (case  $\lambda^n P(\varphi)$ ) and Equations (a), (d) and (k).  
 If  $k \geq 2$ , let  $z = 1^{k-1}$  and  $t = 1^{k-2}$ . To prove Lemma 48, one has

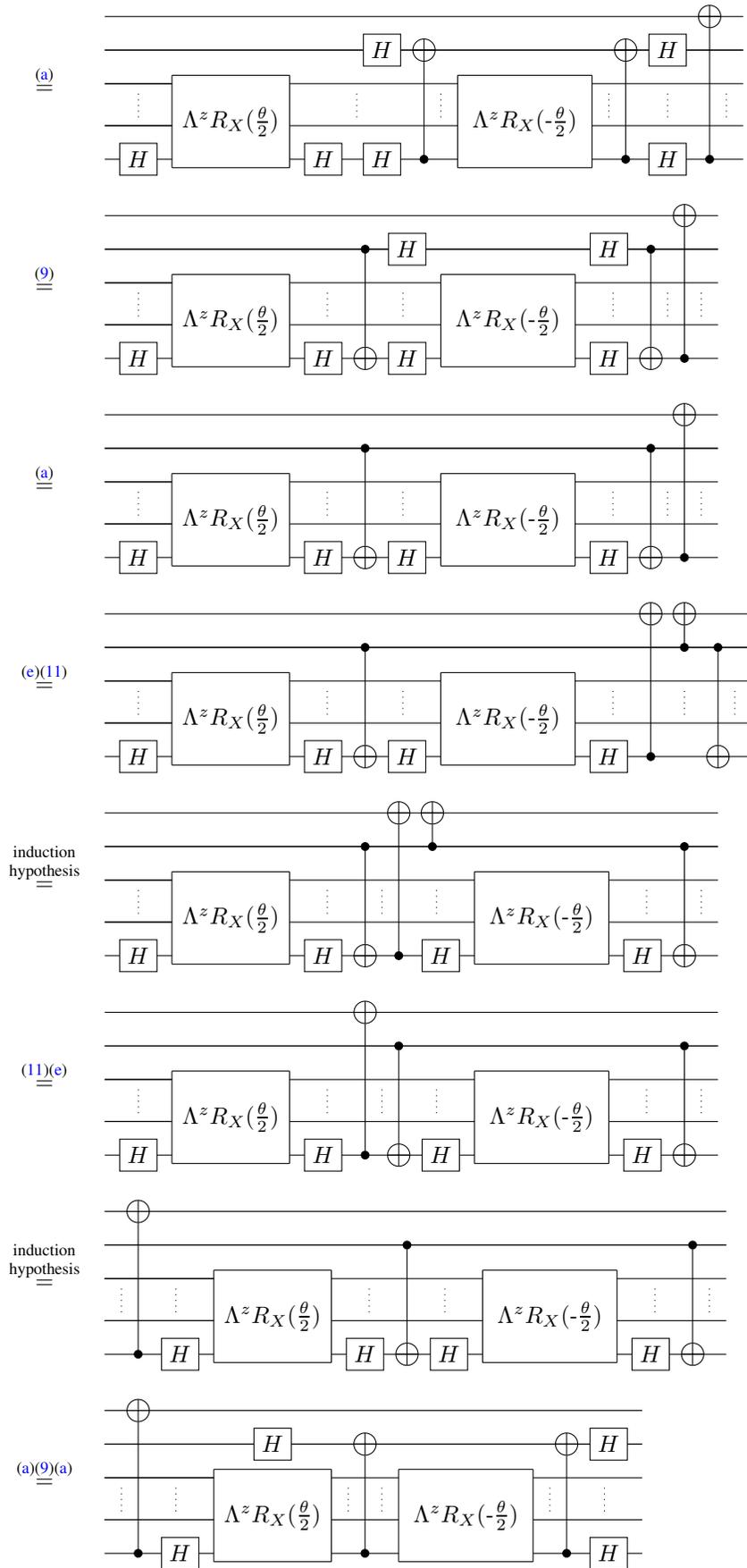
$$\begin{aligned}
 \Lambda^x s(\varphi) &= \text{Diagram 1} \\
 &\stackrel{\text{induction hypothesis of Proposition 13}}{=} \text{Diagram 2} \\
 &\stackrel{\text{induction hypothesis of Lemma 48}}{=} \text{Diagram 3} \\
 &\stackrel{\text{(a), def}}{=} \text{Diagram 4} \\
 &\stackrel{\text{(9)(a)}}{=} \text{Diagram 5} \\
 &\stackrel{\text{def}}{=} \text{Diagram 6}
 \end{aligned}$$

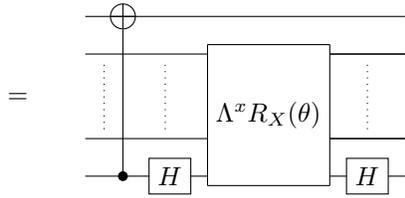
Hence, the commutation with  $\Lambda^y R_X(\theta)$  follows by induction hypothesis and Equation (27), together with Proposition 11.  
 Then to prove the  $\Lambda^x P$  case of Proposition 13, one has

$$\begin{aligned}
 \Lambda^x P(\varphi') \circ \Lambda^x P(\varphi) &= \text{Diagram 1} \\
 &\stackrel{\text{(a)}}{=} \text{Diagram 2} \\
 &\stackrel{\text{induction hypothesis of Lemma 48}}{=} \text{Diagram 3}
 \end{aligned}$$



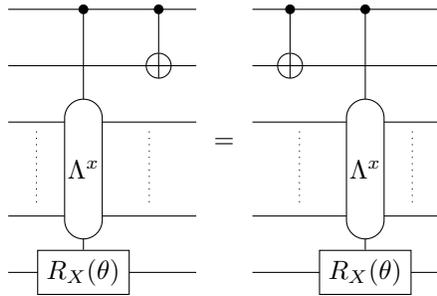




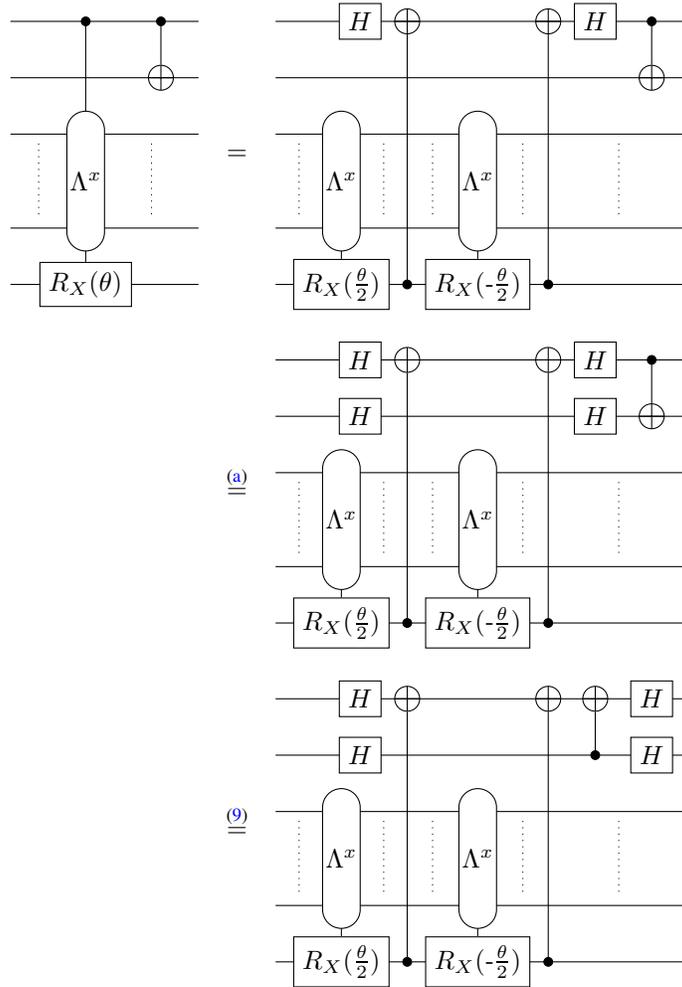


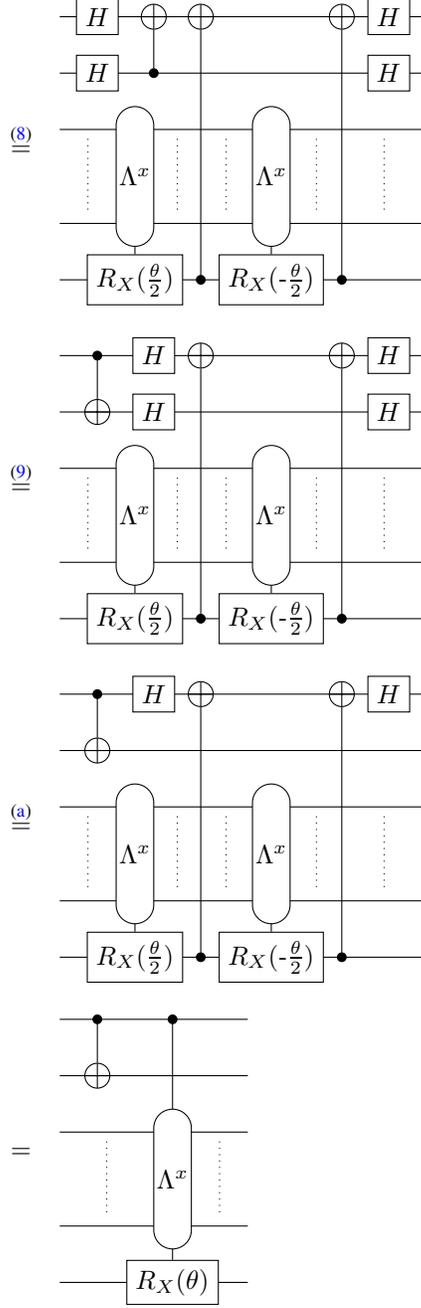
□

**Lemma 51.** For any  $x \in \{0, 1\}^k$ ,



*Proof.*





### C. Proof of Proposition 16

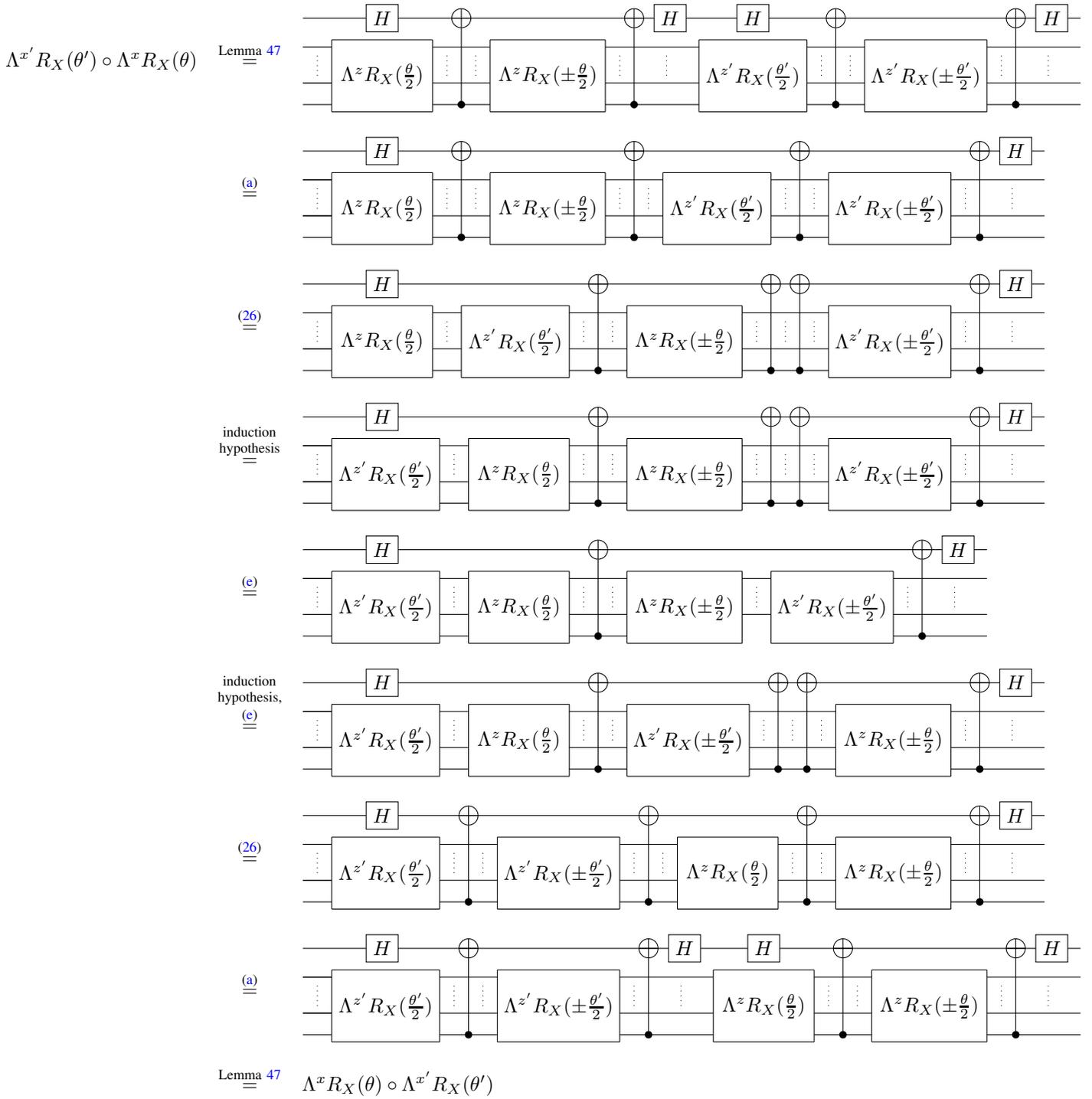
We assume without loss of generality that  $y = y' = \epsilon$ .

First, for the case where  $G = R_X(\theta)$  and  $G' = R_X(\theta')$ , we prove by induction on  $k$  that for any  $x, x' \in \{0, 1\}^k$ ,

$$\text{QC}_0 \vdash \Lambda^x R_X(\theta) \circ \Lambda^{x'} R_X(\theta') = \Lambda^{x'} R_X(\theta') \circ \Lambda^x R_X(\theta). \quad (30)$$

The desired result corresponds to Equation (30) with  $x \neq x'$ . Note that when  $x = x'$ , Equation (30) is a consequence of Proposition 13.

If  $k = 0$ , then Equation (30) is a direct consequence of Equation (18). If  $k \geq 1$ , then we can write  $x = az$  and  $x' = a'z'$  with  $a, a' \in \{0, 1\}$ . One has (where the  $\pm$  signs correspond respectively to  $(-1)^a$  and  $(-1)^{a'}$ ):



If  $G = P(\theta)$  and  $G' = P(\theta')$ , we prove by induction on  $k$  that for any  $z, z' \in \{0, 1\}^k$ ,

$$\Lambda^z s(\varphi) \circ \Lambda^{z'} s(\varphi') = \Lambda^{z'} s(\varphi') \circ \Lambda^z s(\varphi). \quad (31)$$

The result corresponds to the case where  $z = x1$  and  $z' = x'1$  with  $x \neq x'$ . Note that the case where  $x = x'$  is a consequence of Proposition 13.

If  $k = 0$ , then Equation (31) is a consequence of the topological rules.

If  $k = 1$ , then it is a consequence of Equations (k) and (l).

If  $k \geq 2$ , note first that by Equations (2), (a), (25), and (13) (or (1), (a) and (3) if  $m = 0$ ), for any  $x \in \{0, 1\}^m$ ,

$$\text{QC}_0 \vdash \Lambda^{x0}s(\varphi) = \begin{array}{c} \vdots \\ \Lambda^x s(\frac{\varphi}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x R_X(-\varphi) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array}. \quad (32)$$

Let  $z = xa$  and  $z' = x'a'$  with  $a, a' \in \{0, 1\}$  and  $x, x' \in \{0, 1\}^{k-1}$ . One has (with the  $\pm$  signs being  $(-1)^{1-a}$  and  $(-1)^{1-a'}$  respectively):

$$\begin{array}{l} \Lambda^{z'}s(\varphi') \circ \Lambda^z s(\varphi) \\ \text{---} \\ \text{---} \end{array} \stackrel{(10)(a)(32)}{=} \begin{array}{c} \vdots \\ \Lambda^x s(\frac{\varphi}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x R_X(\pm\varphi) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} s(\frac{\varphi'}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} R_X(\pm\varphi') \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \\ \text{---} \\ \text{---} \\ \stackrel{\text{Lemma 48}}{=} \begin{array}{c} \vdots \\ \Lambda^x s(\frac{\varphi}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} s(\frac{\varphi'}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x R_X(\pm\varphi) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} R_X(\pm\varphi') \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \\ \text{---} \\ \text{---} \\ \stackrel{\text{induction hypothesis}}{=} \begin{array}{c} \vdots \\ \Lambda^{x'} s(\frac{\varphi'}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x s(\frac{\varphi}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x R_X(\pm\varphi) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} R_X(\pm\varphi') \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \\ \text{---} \\ \text{---} \\ \stackrel{(30)}{=} \begin{array}{c} \vdots \\ \Lambda^{x'} s(\frac{\varphi'}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x s(\frac{\varphi}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} R_X(\pm\varphi') \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x R_X(\pm\varphi) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \\ \text{---} \\ \text{---} \\ \stackrel{\text{Lemma 48}}{=} \begin{array}{c} \vdots \\ \Lambda^{x'} s(\frac{\varphi'}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} R_X(\pm\varphi') \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x s(\frac{\varphi}{2}) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x R_X(\pm\varphi) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \\ \text{---} \\ \text{---} \\ \stackrel{(10)(a)(32)}{=} \Lambda^z s(\varphi) \circ \Lambda^{z'} s(\varphi'). \end{array}$$

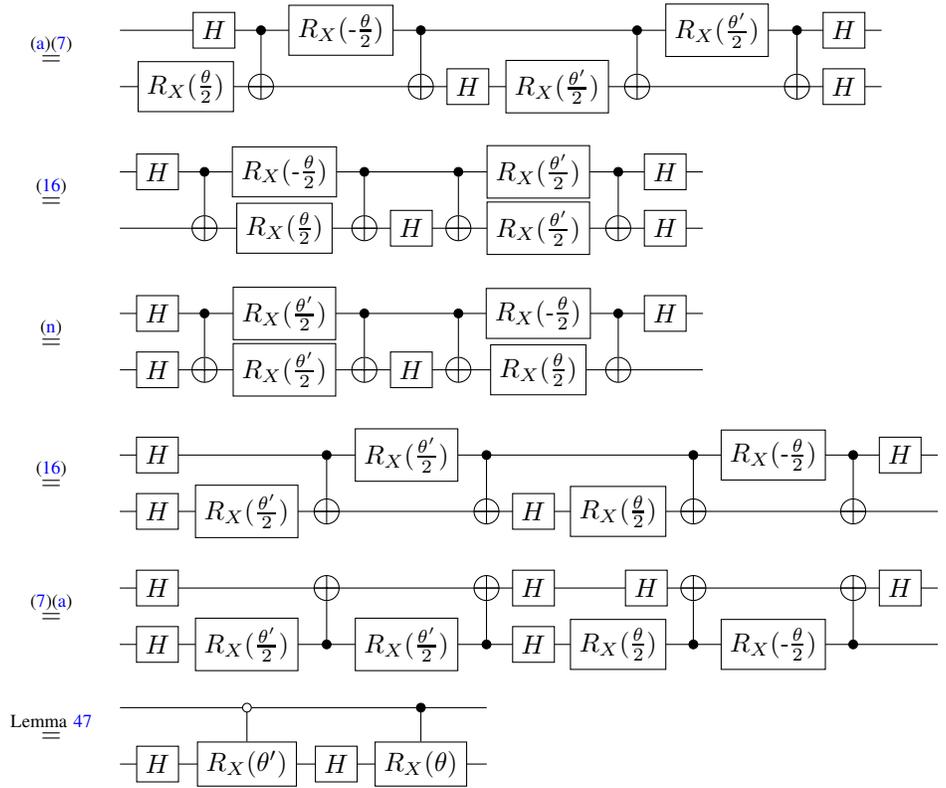
For the case where  $G = R_X(\theta)$  and  $G' = P(\theta')$ , we prove by induction on  $k \geq 1$  that for any  $x, x' \in \{0, 1\}^k$  with  $x \neq x'$ ,

$$\text{QC}_0 \vdash \begin{array}{c} \vdots \\ \Lambda^x R_X(\theta) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^{x'} R_X(\theta') \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} = \begin{array}{c} \vdots \\ \Lambda^{x'} R_X(\theta') \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \begin{array}{c} \vdots \\ \Lambda^x R_X(\theta) \\ \vdots \\ \text{---} \\ H \\ \text{---} \end{array} \quad (33)$$

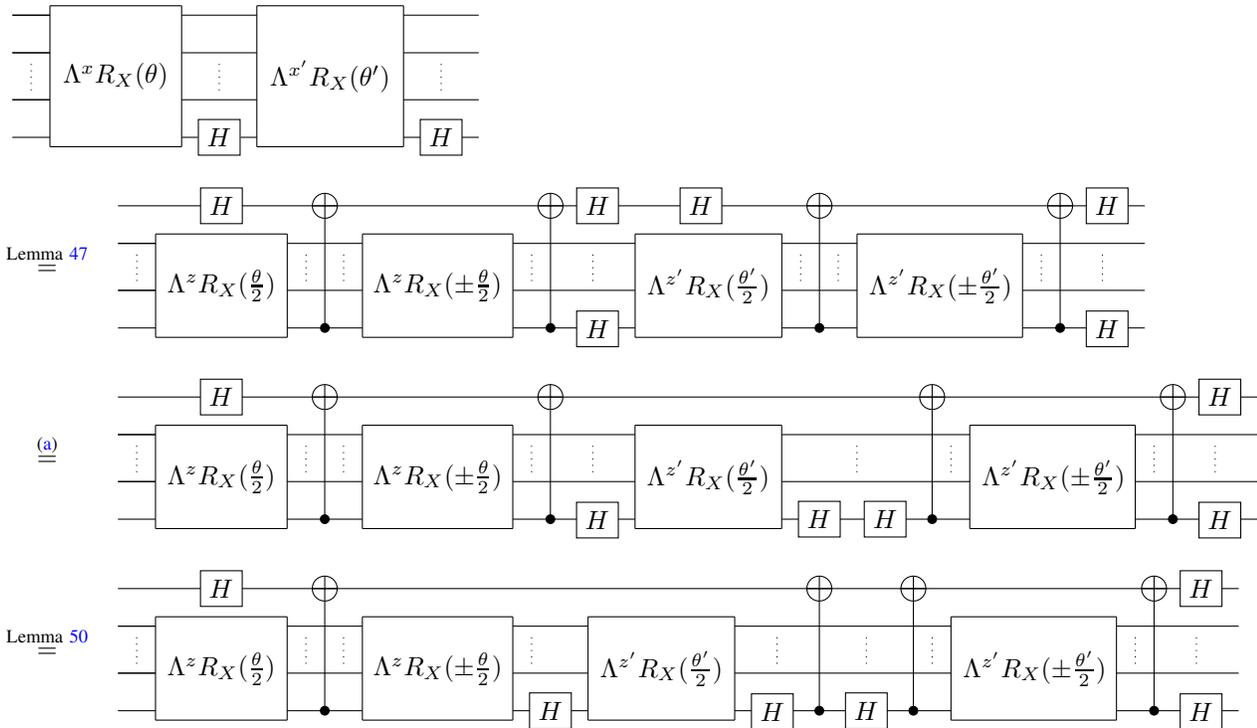
Note that by Lemma 48 and the preceding case, Equation (33) is equivalent to the desired result.

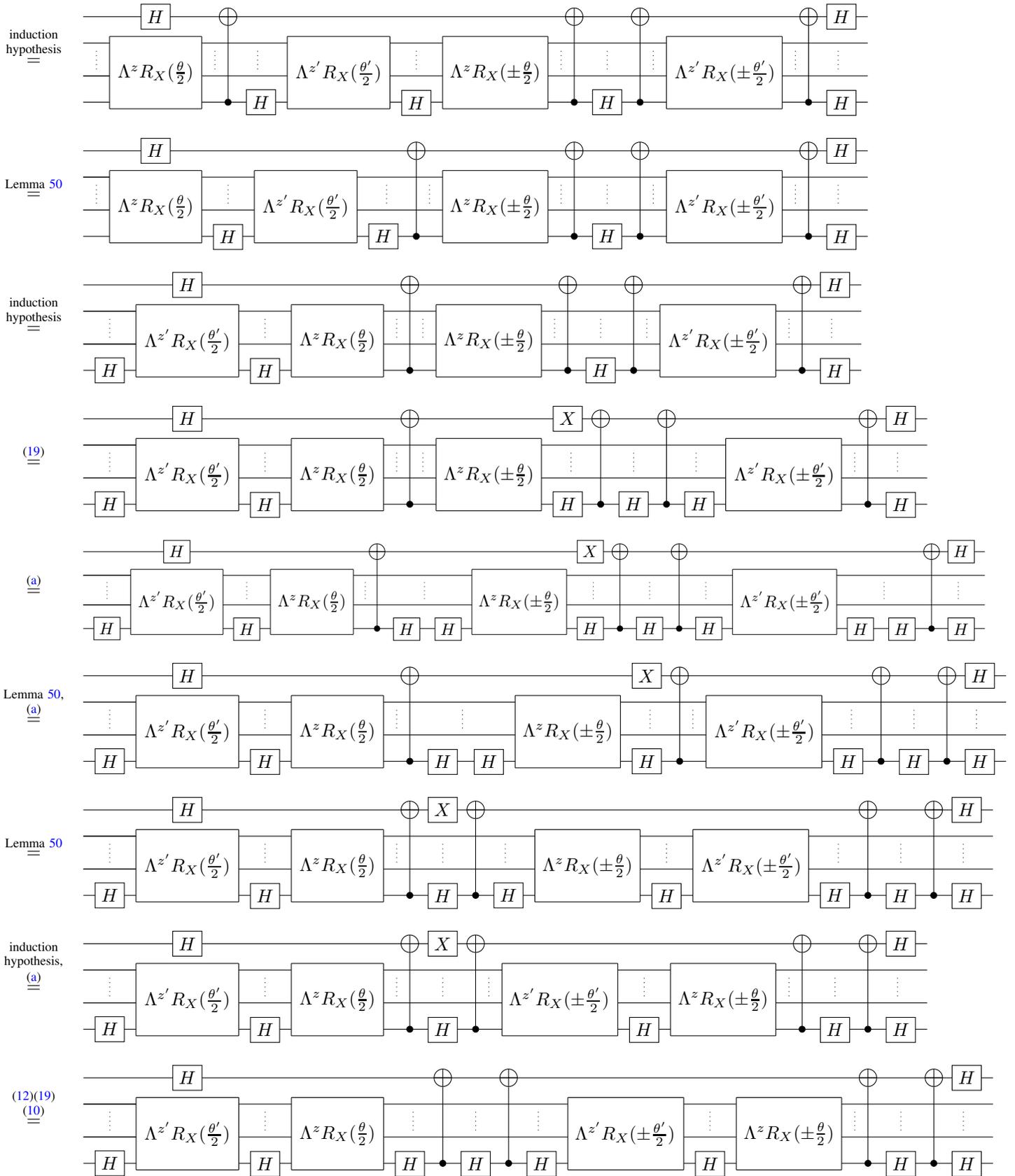
If  $k = 1$ , then without loss of generality we can assume that  $x = 1$  and  $x' = 0$ . One has

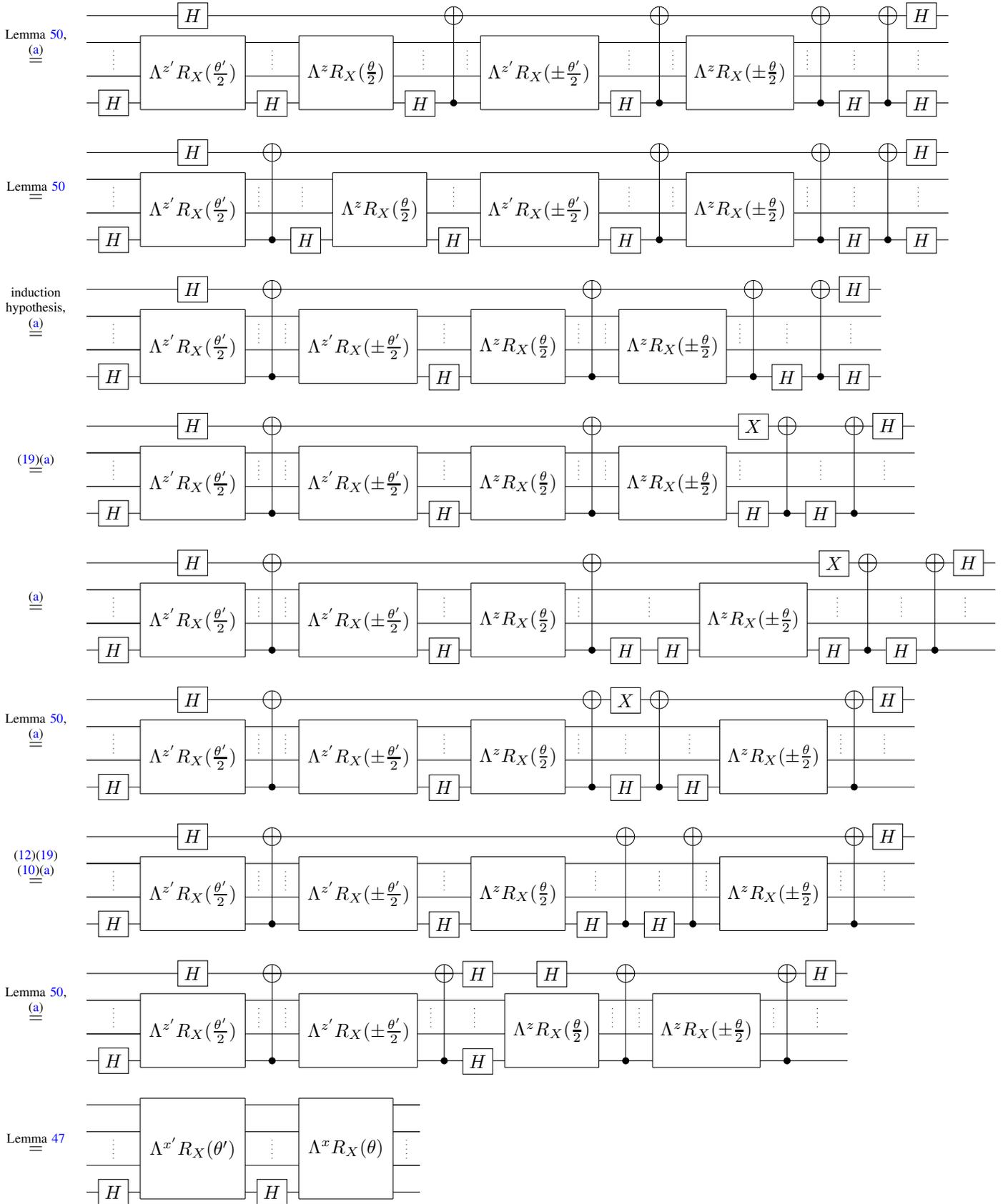
$$\begin{array}{c} \bullet \\ \text{---} \\ R_X(\theta) \\ \text{---} \\ \text{---} \\ \circ \\ \text{---} \\ R_X(\theta') \\ \text{---} \\ \text{---} \end{array} \stackrel{\text{Lemma 47}}{=} \begin{array}{c} \text{---} \\ H \\ \text{---} \\ \oplus \\ \text{---} \\ R_X(\frac{\theta}{2}) \\ \text{---} \\ \bullet \\ \text{---} \\ R_X(-\frac{\theta}{2}) \\ \text{---} \\ \bullet \\ \text{---} \\ H \\ \text{---} \\ \oplus \\ \text{---} \\ R_X(\frac{\theta'}{2}) \\ \text{---} \\ \bullet \\ \text{---} \\ R_X(\frac{\theta'}{2}) \\ \text{---} \\ \bullet \\ \text{---} \\ H \\ \text{---} \\ \oplus \\ \text{---} \\ H \\ \text{---} \end{array}$$



If  $k \geq 2$ , then by Proposition 11, we can assume without loss of generality that we can write  $x = az$  and  $x' = az'$  with  $a, a' \in \{0, 1\}$  and  $z \neq z'$ . One has (where the  $\pm$  signs correspond respectively to  $(-1)^a$  and  $(-1)^{a'}$ ):







If  $G = X$  or  $G' = X$ , then by Equation (28), the result follows from the preceding cases together with Lemma 48 and Equation (31).

D. Ancillary lemmas: Lemmas 52 to 54

**Lemma 52.** For any  $x \in \{0, 1\}^k$  and  $y \in \{0, 1\}^\ell$ ,

$$\text{QC}_0 \vdash (id_k \otimes X \otimes id_\ell) \circ \Lambda_y^x X = \Lambda_y^x X \circ (id_k \otimes X \otimes id_\ell)$$

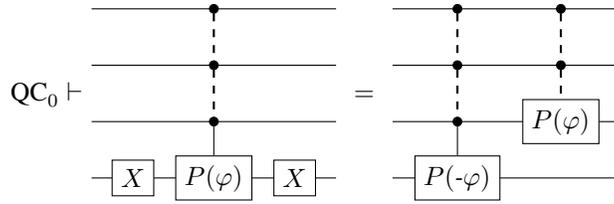
and

$$\text{QC}_0 \vdash (id_k \otimes X \otimes id_\ell) \circ \Lambda_y^x R_X(\theta) = \Lambda_y^x R_X(\theta) \circ (id_k \otimes X \otimes id_\ell)$$

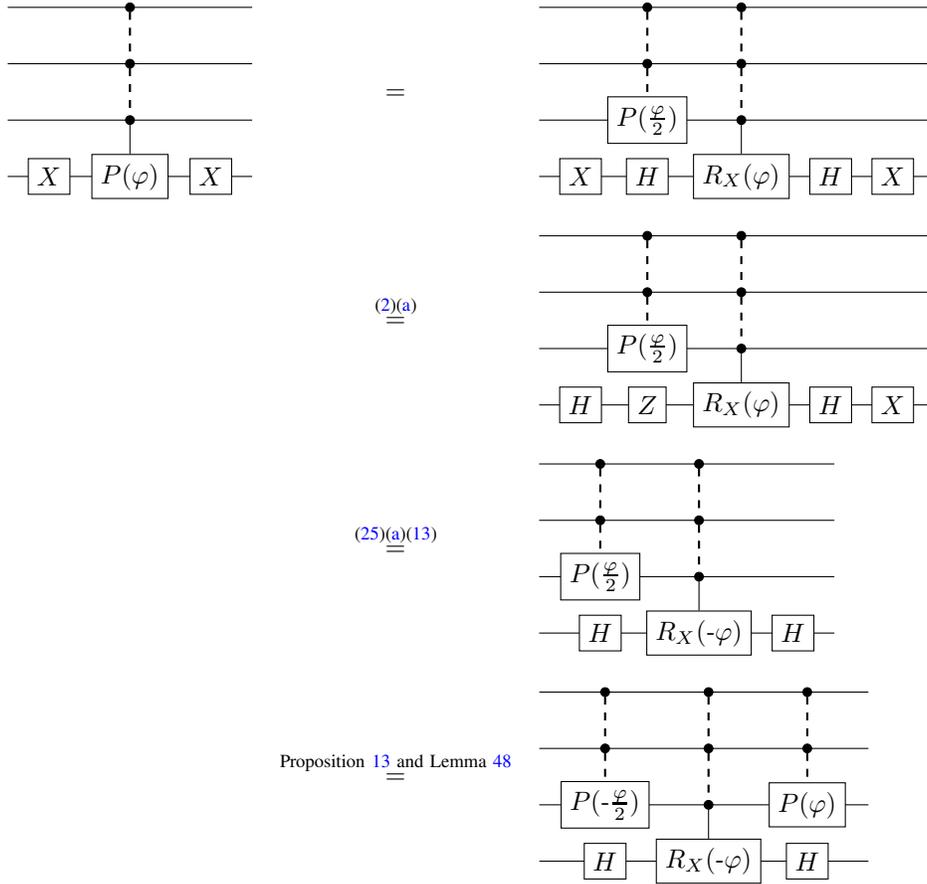
*Proof.* The case of  $\Lambda_y^x X$  is a direct consequence of Propositions 15 and 16. Indeed, using Proposition 15,  $(id_k \otimes X \otimes id_\ell)$  can be decomposed into a product of multi-controlled gates of the form  $\Lambda_{y'}^{x'} X$  with  $x' \in \{0, 1\}^k$  and  $y' \in \{0, 1\}^\ell$ . Then these multi-controlled gates commute with  $\Lambda_y^x X$ , trivially in the case where  $x'y' = xy$ , and by Proposition 16 in the other cases.

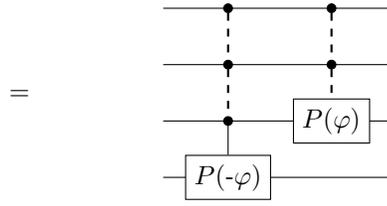
For the case of  $\Lambda_y^x R_X(\theta)$ , note that (b), (c)  $\vdash \boxed{X} = \overset{(\pi/2)}{\boxed{R_X(\pi)}}$ . Then  $s(\frac{\pi}{2})$  commutes by the topological rules, while the commutation of  $(id_k \otimes R_X(\pi) \otimes id_\ell)$  is a direct consequence of Propositions 15, 16 and 13: using Proposition 15, it can be decomposed into a product of multi-controlled gates of the form  $\Lambda_{y'}^{x'} R_X(\pi)$  with  $x' \in \{0, 1\}^k$  and  $y' \in \{0, 1\}^\ell$ . Then these multi-controlled gates commute with  $\Lambda_y^x R_X(\theta)$ , by Proposition 16 in the cases where  $x'y' \neq xy$ , and by Proposition 13 in the case where  $x'y' = xy$ .  $\square$

**Lemma 53.**



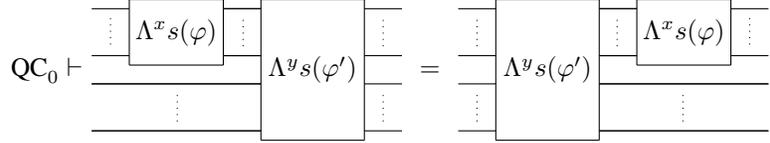
*Proof.*



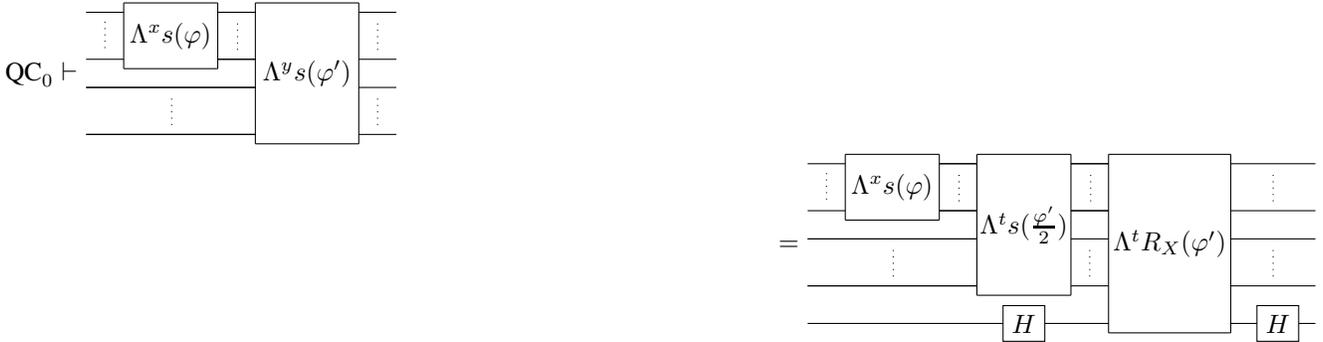


□

**Lemma 54.** For any  $x \in \{0, 1\}^k$  and  $y \in \{0, 1\}^\ell$  with  $\ell \geq k$ ,



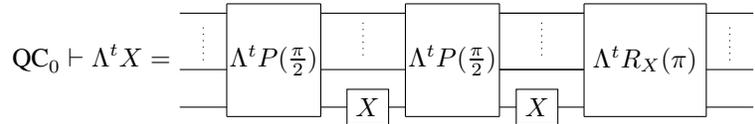
*Proof.* We proceed by induction on  $\ell - k$ . If  $\ell = k$  then the result is a consequence of Proposition 13 or 16 (or just of the topological rules if  $k = \ell = 0$ ). If  $\ell \geq k + 1$ , then without loss of generality, we can assume that  $y = t1$  for some  $t \in \{0, 1\}^{\ell-1}$ . Then by Lemma 43 (together with Lemma 40 and Equation (10)),



so that the commutation follows by induction hypothesis and Lemma 48. □

#### E. Proof of Proposition 17

First, the cases where  $G$  or  $G' = X$  follow from the other cases. Indeed, using Equation (28) and Proposition 15 (together with Proposition 11), and then Proposition 12, one gets that for any  $t \in \{0, 1\}^p$ ,



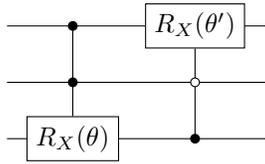
Then, if  $G$  or  $G' = X$ , one can use this decomposition and make the multi-controlled parts commute using the other cases. The non-controlled  $X$  gates commute with the control dots by changing their colour, with the help of Equation (10). This does not alter the fact that the multi-controlled gates commute, since the  $X$  gates are not on the same wire than the control dots of different colours. And since the decomposition produces each time two  $X$  gates on the same wire, any control dot gets changed twice, so that it is the same at the end as at the beginning.

Thus, it suffices to treat the cases where  $G, G' \in \{R_X(\theta), P(\varphi)\}$ .

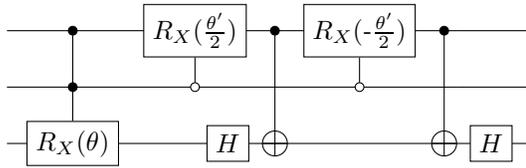
If  $G = R_X(\theta)$  and  $G' = P(\varphi)$  (or conversely), then by Proposition 12, the result is a consequence of Lemma 52 and Proposition 16.

If  $G = P(\varphi)$  and  $G' = P(\varphi')$ , then by Proposition 12, the result is a consequence of Lemmas 53 and 54 (together with Equation (10)) and Proposition 16.

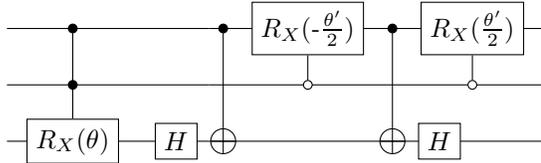
It remains to treat the case where  $G = R_X(\theta)$  and  $G' = R_X(\theta')$ . By Lemma 52, we can assume without loss of generality that  $a = b = 1$ . By definition of  $\Lambda_u^t$ , we can also assume without loss of generality that  $k = m = 0$ . Then the hypothesis  $xyz \neq x'y'z'$  becomes  $y \neq y'$ . We proceed by induction on  $\ell$ . If  $\ell = 1$ , then without loss of generality we can assume that  $x = 1$  and  $x' = 0$ . One has



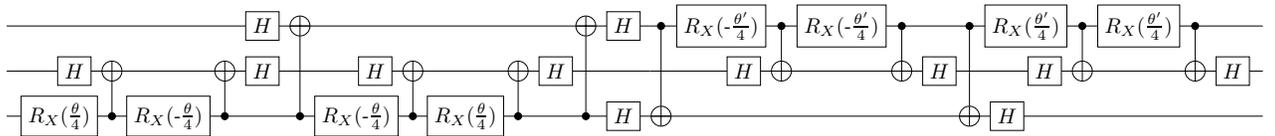
Proposition 11,  
def



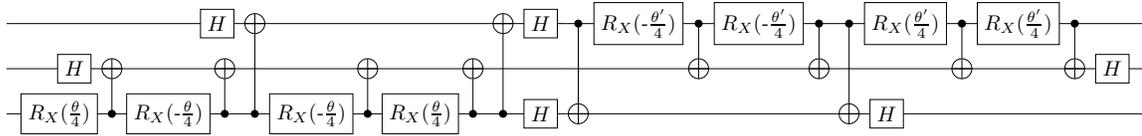
(24)



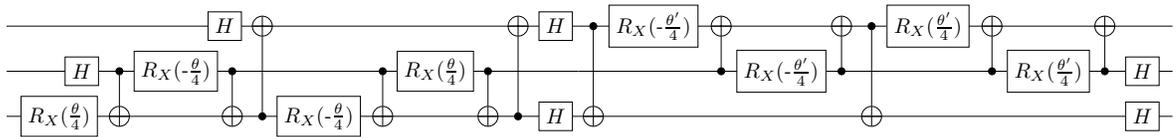
Lemma 47,  
def



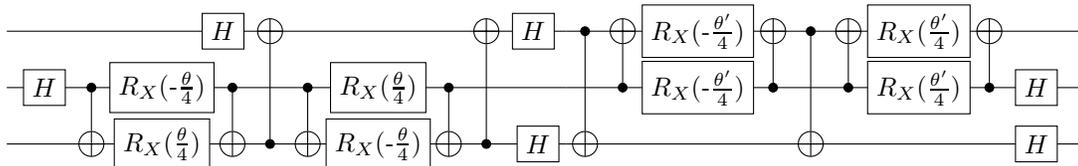
(a)



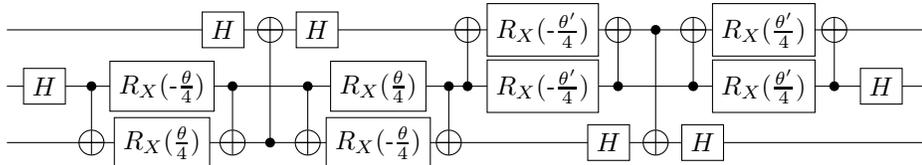
(7)



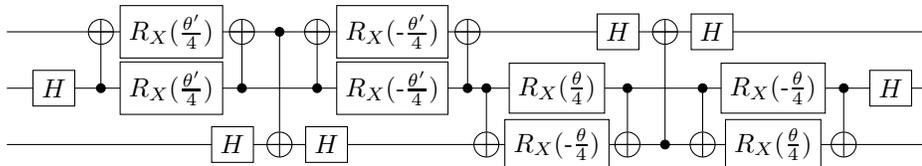
(16)

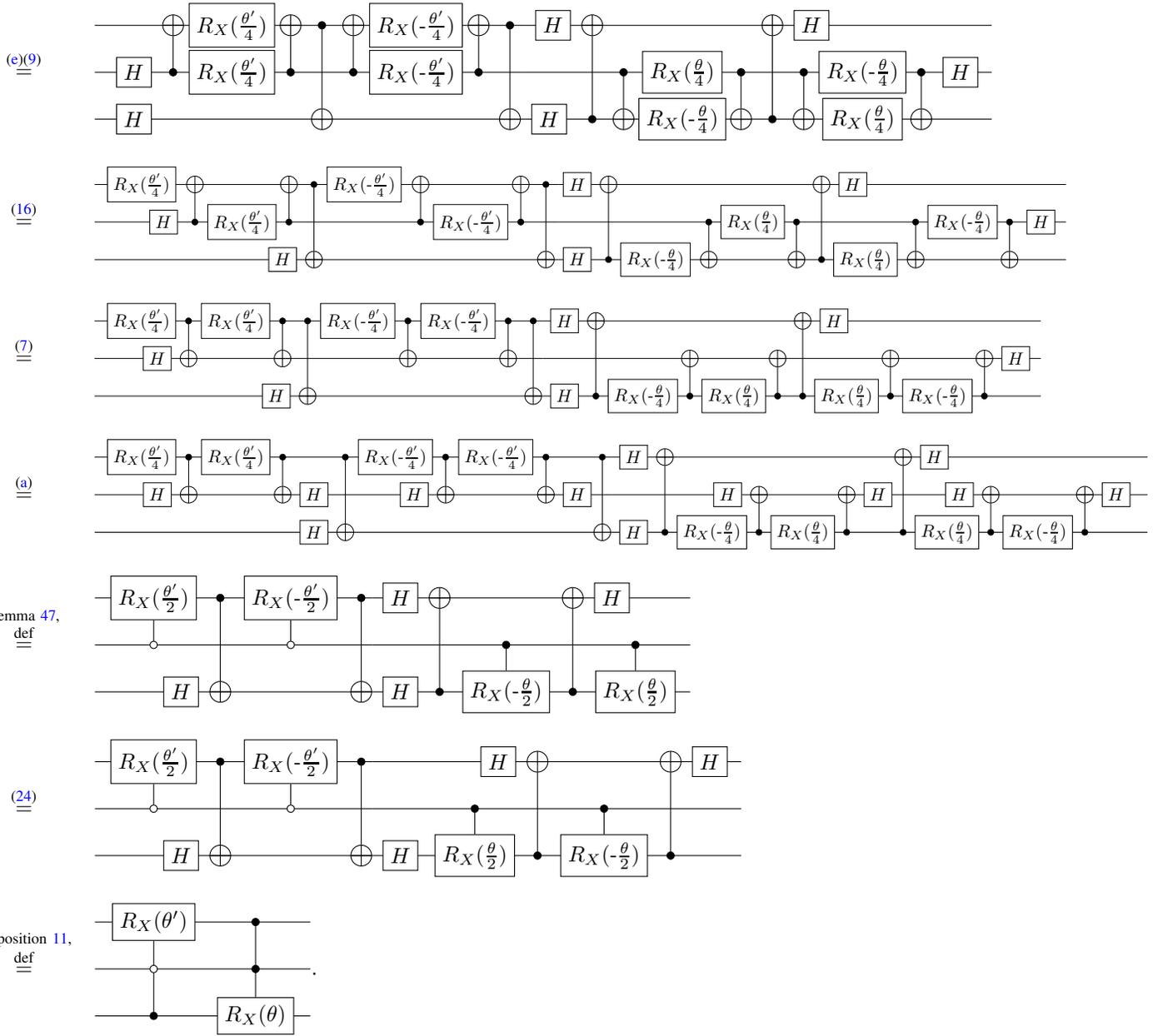


(9)(e)

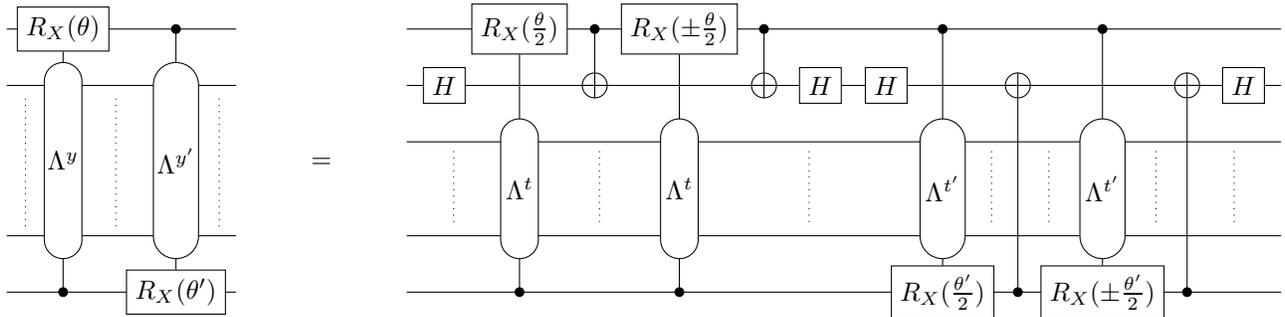


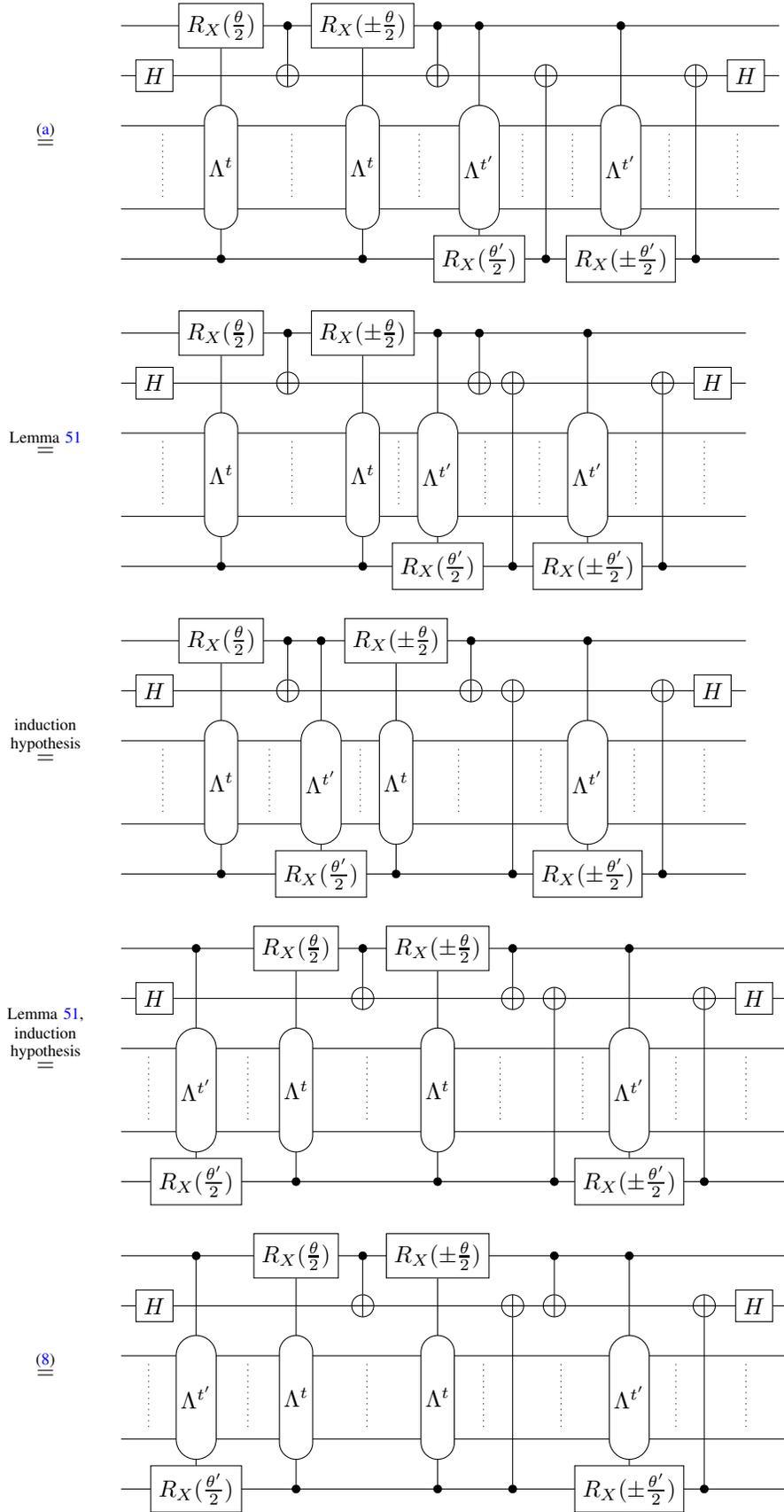
(o)

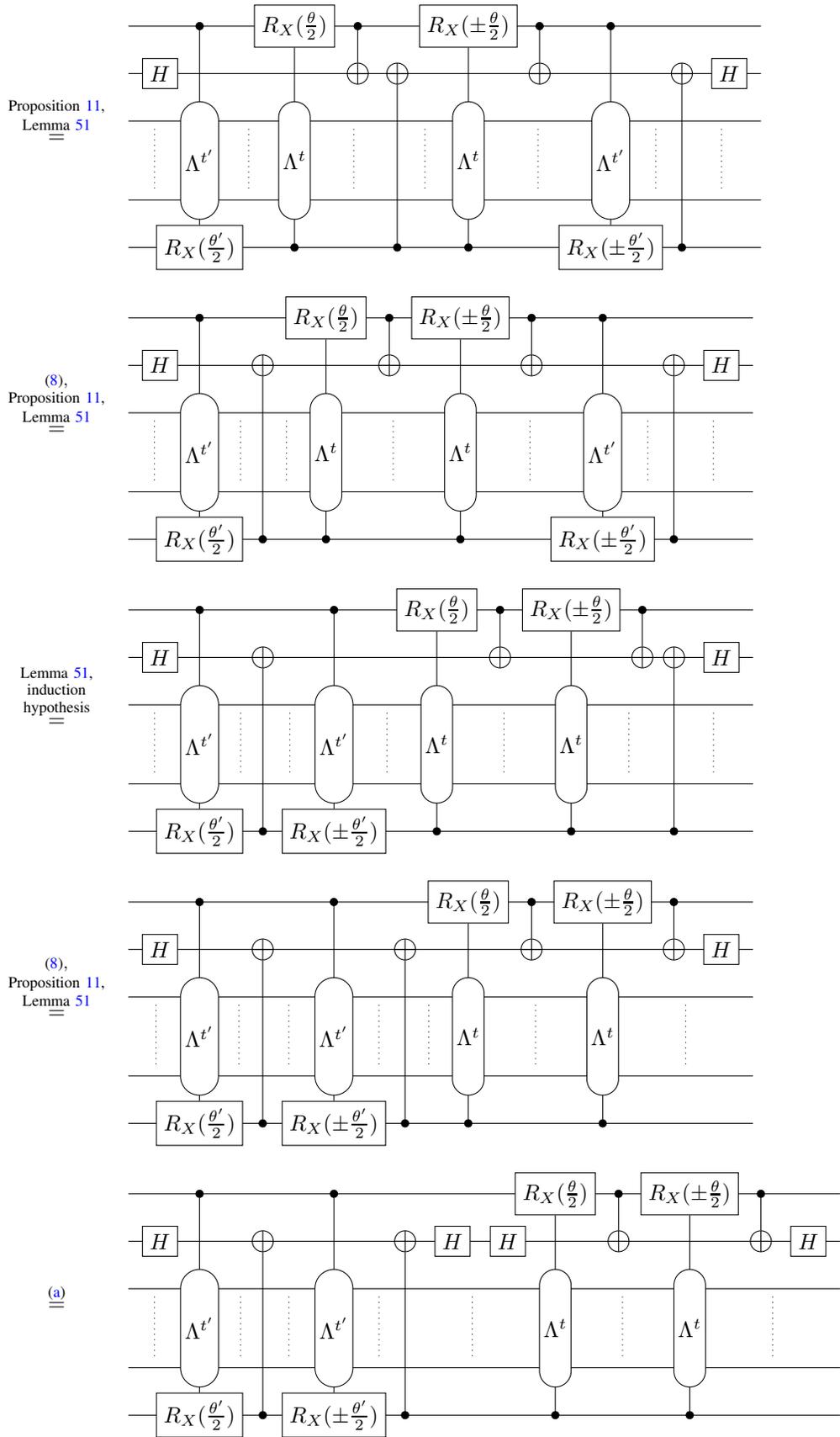


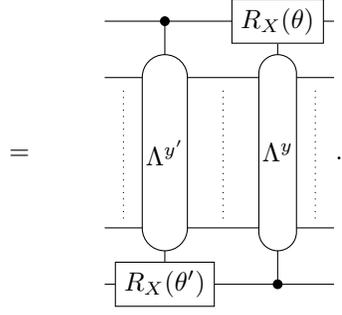


If  $k \geq 2$ , by Proposition 11 we can assume without loss of generality that  $y = at$  and  $y' = a't'$  with  $a, a' \in \{0, 1\}$  and  $t \neq t'$ . One has (with the  $\pm$  signs being  $(-1)^a$  and  $(-1)^{a'}$  respectively):









F. Proof of Proposition 18

$$\begin{aligned}
\text{---} \boxed{H} \text{---} &\stackrel{\text{(d)(k)(17)(18)}}{=} \text{---} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \boxed{R_X(\frac{\pi}{2})} \boxed{P(\frac{\pi}{2})} \text{---} \boxed{H} \text{---} \\
&\stackrel{\text{(p)}}{=} \text{---} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \boxed{H} \boxed{H} \text{---} \\
&\stackrel{\text{(a)}}{=} \text{---} \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \text{---}
\end{aligned}$$

G. Proof of Proposition 19

The proof is inspired by the proofs of Lemmas 10 and 11 of [30]. Given any  $n$ -qubit quantum circuit  $C$ , let  $\llbracket C \rrbracket_g := \mathfrak{G}_n^{-1} \circ \llbracket C \rrbracket \circ \mathfrak{G}_n$ .

1) *Soundness of Equation (q)*: Given any  $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ , let  $U := \llbracket \text{---} \boxed{R_X(\alpha_1)} \text{---} \boxed{P(\alpha_2)} \text{---} \boxed{R_X(\alpha_3)} \text{---} \rrbracket_g$ . We have to prove that there exist unique  $\beta_0, \beta_1, \beta_2, \beta_3$  satisfying the conditions of Figure 5 such that  $\llbracket \text{---} \boxed{P(\beta_1)} \text{---} \boxed{R_X(\beta_2)} \text{---} \boxed{P(\beta_3)} \text{---} \rrbracket_g = U$ . We are going to first prove that assuming that such  $\beta_j$  exist, their values are uniquely determined by  $U$ . Since we are going to do so by giving explicit expressions of the unique possible value of each  $\beta_j$  in terms of the entries of  $U$ , it will then be easy to check that these expressions indeed define angles with the desired properties.

One has

$$U = \llbracket \text{---} \boxed{P(\beta_1)} \text{---} \boxed{R_X(\beta_2)} \text{---} \boxed{P(\beta_3)} \text{---} \rrbracket_g = e^{i\beta_0} \begin{pmatrix} \cos(\frac{\beta_2}{2}) & -ie^{i\beta_1} \sin(\frac{\beta_2}{2}) \\ -ie^{i\beta_3} \sin(\frac{\beta_2}{2}) & e^{i(\beta_1+\beta_3)} \cos(\frac{\beta_2}{2}) \end{pmatrix}$$

If  $U$  has a null entry, then since it is unitary, it is either diagonal or anti-diagonal. If it is diagonal, then  $\sin(\frac{\beta_2}{2}) = 0$ , which, since  $\beta_2 \in [0, 2\pi)$ , implies that  $\beta_2 = 0$ , which by the constraint on  $\beta_1$  and  $\beta_2$ , implies that  $\beta_1 = 0$ . Consequently,  $\beta_0 = \arg(U_{0,0})$  and  $\beta_3 = \arg(\frac{U_{1,1}}{U_{0,0}})$ . If  $U$  is anti-diagonal, then  $\cos(\frac{\beta_2}{2}) = 0$ , which, since  $\beta_2 \in [0, 2\pi)$ , implies that  $\beta_2 = \pi$ , which by the constraint on  $\beta_1$  and  $\beta_2$ , implies that  $\beta_1 = 0$ . Consequently,  $\beta_0 = \arg(\frac{U_{0,1}}{-i})$  and  $\beta_3 = \arg(\frac{U_{1,0}}{U_{0,1}})$ .

If  $U$  has no null entry, then one has  $\beta_2 \neq \pi$  and  $\frac{ie^{-i\beta_1}U_{0,1}}{U_{0,0}} = \tan(\frac{\beta_2}{2})$ . Hence,  $\beta_1$  is the unique angle in  $[0, \pi)$  such that  $\frac{ie^{-i\beta_1}U_{0,1}}{U_{0,0}} \in \mathbb{R}$ , namely  $\arg(\frac{iU_{0,1}}{U_{0,0}}) \bmod \pi$ . In turn,  $\beta_2$  is the unique angle in  $[0, 2\pi) \setminus \{\pi\}$  such that  $\tan(\frac{\beta_2}{2}) = \frac{ie^{-i\beta_1}U_{0,1}}{U_{0,0}}$ . Finally, one has  $e^{i\beta_3} = \frac{\cos(\frac{\beta_2}{2})U_{1,0}}{-i \sin(\frac{\beta_2}{2})U_{0,0}}$ , so that  $\beta_3 = \arg(\frac{\cos(\frac{\beta_2}{2})U_{1,0}}{-i \sin(\frac{\beta_2}{2})U_{0,0}})$ , and  $e^{i\beta_0} = \frac{U_{0,0}}{\cos(\frac{\beta_2}{2})}$ , so that  $\beta_0 = \arg(\frac{U_{0,0}}{\cos(\frac{\beta_2}{2})})$ .

2) *Soundness of Equation (r)*: Given any  $n$ -qubit quantum circuit  $C$  such that  $\llbracket C \rrbracket_g$  is of the form  $\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$  with  $U \in \mathbb{C}^{3 \times 3}$ , let  $\llbracket C \rrbracket_{g3} := U$ .

Given any  $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \mathbb{R}$ , let  $U := \llbracket \text{---} \boxed{R_X(\gamma_1)} \text{---} \boxed{P(\gamma_2)} \text{---} \boxed{R_X(\gamma_3)} \text{---} \boxed{R_X(\gamma_4)} \text{---} \rrbracket_{g3}$ . We have to prove that there exist unique

$\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9$  satisfying the conditions of Figure 5 such that

or equivalently,

We are going to first prove that assuming that such  $\delta_j$  exist, their values are uniquely determined by  $U$ . Since we are going to do so by giving explicit expressions of the unique possible value of each  $\delta_j$  in terms of the entries of  $U$ , it will then be easy to check that these expressions indeed define angles with the desired properties.

Let  $U_{123} := \left[ \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \\ \text{---} P(\delta_1) \text{---} P(\delta_2) \text{---} R_X(\delta_3) \text{---} \\ | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \end{array} \right]_{g_3} = \begin{pmatrix} e^{i\delta_2} & 0 & 0 \\ 0 & e^{i(\delta_1+\delta_2)} \cos(\frac{\delta_3}{2}) & -i \sin(\frac{\delta_3}{2}) \\ 0 & -ie^{i(\delta_1+\delta_2)} \sin(\frac{\delta_3}{2}) & \cos(\frac{\delta_3}{2}) \end{pmatrix}$ ,  $U_4 := \left[ \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} R_X(\delta_4) \text{---} \\ | \\ \text{---} \bullet \text{---} \end{array} \right]_{g_3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\delta_5} \cos(\frac{\delta_6}{2}) & -i \sin(\frac{\delta_6}{2}) \\ 0 & -ie^{i\delta_5} \sin(\frac{\delta_6}{2}) & \cos(\frac{\delta_6}{2}) \end{pmatrix}$ . Let also  $U_I := \begin{pmatrix} \cos(\frac{\delta_4}{2}) & -i \sin(\frac{\delta_4}{2}) & 0 \\ -i \sin(\frac{\delta_4}{2}) & \cos(\frac{\delta_4}{2}) & 0 \\ 0 & 0 & 1 \end{pmatrix}$  and  $U_{56} := \left[ \begin{array}{c} \text{---} \bullet \text{---} \bullet \text{---} \\ | \quad | \\ \text{---} P(\delta_5) \text{---} R_X(\delta_6) \text{---} \\ | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \end{array} \right]_{g_3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\delta_5} \cos(\frac{\delta_6}{2}) & -i \sin(\frac{\delta_6}{2}) \\ 0 & -ie^{i\delta_5} \sin(\frac{\delta_6}{2}) & \cos(\frac{\delta_6}{2}) \end{pmatrix}$ . Let also  $U_I := U_{123} \circ U^\dagger$ ,  $U_{II} := U_4 \circ U_I$  and  $U_{III} := U_{56} \circ U_{II}$ .

By construction,

$$U_{III} = \left[ \begin{array}{c} \text{---} \bullet \text{---} P(\delta_8) \text{---} \\ | \quad | \\ \text{---} P(\delta_7) \text{---} P(\delta_9) \text{---} \\ | \quad | \\ \text{---} \bullet \text{---} \bullet \text{---} \end{array} \right]_{g_3}^\dagger = \begin{pmatrix} e^{-i\delta_9} & 0 & 0 \\ 0 & e^{-i(\delta_7+\delta_8+\delta_9)} & 0 \\ 0 & 0 & e^{-i\delta_8} \end{pmatrix} \quad (\text{E1})$$

so that

$$U_{II} = U_{56}^\dagger \circ U_{III} = \begin{pmatrix} e^{-i\delta_9} & 0 & 0 \\ 0 & e^{-i(\delta_5+\delta_7+\delta_8+\delta_9)} \cos(\frac{\delta_6}{2}) & ie^{-i(\delta_5+\delta_8)} \sin(\frac{\delta_6}{2}) \\ 0 & ie^{-i(\delta_7+\delta_8+\delta_9)} \sin(\frac{\delta_6}{2}) & e^{-i\delta_8} \cos(\frac{\delta_6}{2}) \end{pmatrix} \quad (\text{E2})$$

and  $U_I = U_4^\dagger \circ U_{II}$ . Since  $U_4$  acts as the identity on the last entry, this implies that  $(U_I)_{2,0} = 0$ .<sup>11</sup> That is, by definition of  $U_I$ ,

$$-ie^{i(\delta_1+\delta_2)} \sin(\frac{\delta_3}{2}) U_{0,1}^\dagger + \cos(\frac{\delta_3}{2}) U_{0,2}^\dagger = 0. \quad (\text{E3})$$

By direct calculation using the definitions of  $U_I$  and  $U_{II}$ , one gets  $(U_I)_{0,0} = e^{i\delta_2} U_{0,0}^\dagger$  and  $(U_I)_{1,0} = e^{i(\delta_1+\delta_2)} \cos(\frac{\delta_3}{2}) U_{0,1}^\dagger - i \sin(\frac{\delta_3}{2}) U_{0,2}^\dagger$ , so that  $(U_{II})_{1,0} = -i \sin(\frac{\delta_4}{2}) (U_I)_{0,0} + \cos(\frac{\delta_4}{2}) (U_I)_{1,0} = -i \sin(\frac{\delta_4}{2}) e^{i\delta_2} U_{0,0}^\dagger + \cos(\frac{\delta_4}{2}) (e^{i(\delta_1+\delta_2)} \cos(\frac{\delta_3}{2}) U_{0,1}^\dagger - i \sin(\frac{\delta_3}{2}) U_{0,2}^\dagger)$ . That is, since by (E2),  $(U_{II})_{1,0} = 0$ :

$$-i \sin(\frac{\delta_4}{2}) e^{i\delta_2} U_{0,0}^\dagger + \cos(\frac{\delta_4}{2}) \left( e^{i(\delta_1+\delta_2)} \cos(\frac{\delta_3}{2}) U_{0,1}^\dagger - i \sin(\frac{\delta_3}{2}) U_{0,2}^\dagger \right) = 0 \quad (\text{E4})$$

- If  $U_{0,1} = U_{0,2} = 0$ , then since  $U$  is unitary,  $U_{0,0} \neq 0$  and (E4) becomes  $-i \sin(\frac{\delta_4}{2}) e^{i\delta_2} U_{0,0}^\dagger = 0$ , that is  $\sin(\frac{\delta_4}{2}) = 0$ . Since  $\delta_4 \in [0, 2\pi)$ , this implies that  $\delta_4 = 0$ , which by the conditions of Figure 5, implies that  $\delta_1 = \delta_2 = \delta_3 = 0$ .
- If  $(U_{0,1}, U_{0,2}) \neq (0, 0)$ , then  $e^{i(\delta_1+\delta_2)} \cos(\frac{\delta_3}{2}) U_{0,1}^\dagger - i \sin(\frac{\delta_3}{2}) U_{0,2}^\dagger \neq 0$ . Indeed, if this expression was equal to 0, by (E3)

this would mean that the non-zero vector  $\begin{pmatrix} e^{i(\delta_1+\delta_2)} U_{0,1}^\dagger \\ U_{0,2}^\dagger \end{pmatrix}$  is in the kernel of the matrix  $\begin{pmatrix} \cos(\frac{\delta_3}{2}) & -i \sin(\frac{\delta_3}{2}) \\ -i \sin(\frac{\delta_3}{2}) & \cos(\frac{\delta_3}{2}) \end{pmatrix}$ ,

whereas this matrix is invertible. Then:

– If  $U_{0,0} = 0$ , then (E4) implies that  $\cos(\frac{\delta_4}{2}) = 0$ , which, since  $\delta_4 \in [0, 2\pi)$ , implies that  $\delta_4 = \pi$ . By the conditions of Figure 5, this implies that  $\delta_2 = 0$ . Then:

- \* If  $U_{0,2} = 0$ , then  $U_{0,1} \neq 0$ , and (E3) implies that  $\sin(\frac{\delta_3}{2}) = 0$ , that is, since  $\delta_3 \in [0, 2\pi)$ , that  $\delta_3 = 0$ . By the conditions of Figure 5, together with the fact that  $\delta_4 = \pi$ , this implies that  $\delta_1 = 0$ .
- \* If  $U_{0,1} = 0$ , then  $U_{0,2} \neq 0$ , and (E3) implies that  $\cos(\frac{\delta_3}{2}) = 0$ , that is, since  $\delta_3 \in [0, 2\pi)$ , that  $\delta_3 = \pi$ . By the conditions of Figure 5, this implies that  $\delta_1 = 0$ .
- \* If  $U_{0,1}, U_{0,2} \neq 0$ , then (E3), on the one hand, implies that  $\delta_3 \neq \pi$ , and on the other hand, is equivalent to

$$\tan(\frac{\delta_3}{2}) = \frac{e^{-i\delta_1} U_{0,2}^\dagger}{i U_{0,1}^\dagger}.$$

<sup>11</sup>Where we denote by  $M_{i,j}$  the entry of indices  $(i, j)$  of any matrix  $M$ , the index of the first row and column being 0.

Hence,  $\delta_1$  is the unique angle in  $[0, \pi)$  such that  $\frac{e^{-i\delta_1}U_{0,2}^\dagger}{iU_{0,1}^\dagger} \in \mathbb{R}$ . In turn,  $\delta_3$  is the unique angle in  $[0, 2\pi)$  such that  $\tan\left(\frac{\delta_3}{2}\right) = \frac{e^{-i\delta_1}U_{0,2}^\dagger}{iU_{0,1}^\dagger}$ .

– If  $U_{0,0} \neq 0$ , then (E<sub>4</sub>) can be simplified into

$$-i \tan\left(\frac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + e^{i(\delta_1+\delta_2)} \cos\left(\frac{\delta_3}{2}\right)U_{0,1}^\dagger - i \sin\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger = 0. \quad (\text{E}_5)$$

\* If  $U_{0,2} = 0$ , then  $U_{0,1} \neq 0$ , and (E<sub>3</sub>) implies that  $\sin\left(\frac{\delta_3}{2}\right) = 0$ , that is, since  $\delta_3 \in [0, 2\pi)$ , that  $\delta_3 = 0$ . By the conditions of Figure 5, this implies that  $\delta_2 = 0$ . Then (E<sub>5</sub>) becomes

$$-i \tan\left(\frac{\delta_4}{2}\right)U_{0,0}^\dagger + e^{i\delta_1}U_{0,1}^\dagger = 0$$

that is,

$$\tan\left(\frac{\delta_4}{2}\right) = \frac{e^{i\delta_1}U_{0,1}^\dagger}{iU_{0,0}^\dagger}.$$

Hence,  $\delta_1$  is the unique angle in  $[0, \pi)$  such that  $\frac{e^{i\delta_1}U_{0,1}^\dagger}{iU_{0,0}^\dagger} \in \mathbb{R}$ . In turn,  $\delta_4$  is the unique angle in  $[0, 2\pi)$  such that  $\tan\left(\frac{\delta_4}{2}\right) = \frac{e^{i\delta_1}U_{0,1}^\dagger}{iU_{0,0}^\dagger}$ .

\* If  $U_{0,1} = 0$ , then  $U_{0,2} \neq 0$ , and (E<sub>3</sub>) implies that  $\cos\left(\frac{\delta_3}{2}\right) = 0$ , that is, since  $\delta_3 \in [0, 2\pi)$ , that  $\delta_3 = \pi$ . By the conditions of Figure 5, this implies that  $\delta_1 = 0$ . Then (E<sub>5</sub>) becomes

$$-i \tan\left(\frac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger - iU_{0,2}^\dagger = 0$$

that is,

$$\tan\left(\frac{\delta_4}{2}\right) = -\frac{e^{-i\delta_2}U_{0,2}^\dagger}{U_{0,0}^\dagger}.$$

Hence,  $\delta_2$  is the unique angle in  $[0, \pi)$  such that  $\frac{e^{-i\delta_2}U_{0,2}^\dagger}{U_{0,0}^\dagger} \in \mathbb{R}$ . In turn,  $\delta_4$  is the unique angle in  $[0, 2\pi)$  such that  $\tan\left(\frac{\delta_4}{2}\right) = -\frac{e^{-i\delta_2}U_{0,2}^\dagger}{U_{0,0}^\dagger}$ .

\* If  $U_{0,1}, U_{0,2} \neq 0$ , then (E<sub>3</sub>), on the one hand, implies that  $\delta_3 \notin \{0, \pi\}$ , and on the other hand, is equivalent to

$$e^{i(\delta_1+\delta_2)} = \frac{\cos\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger}{i \sin\left(\frac{\delta_3}{2}\right)U_{0,1}^\dagger}. \quad (\text{E}_6)$$

Then by substituting in (E<sub>5</sub>), we get

$$-i \tan\left(\frac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + \frac{\cos^2\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger}{i \sin\left(\frac{\delta_3}{2}\right)} - i \sin\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger = 0$$

which can be simplified into

$$-i \tan\left(\frac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + \frac{U_{0,2}^\dagger}{i \sin\left(\frac{\delta_3}{2}\right)} = 0$$

which is equivalent to

$$\tan\left(\frac{\delta_4}{2}\right) = -\frac{e^{-i\delta_2}U_{0,2}^\dagger}{\sin\left(\frac{\delta_3}{2}\right)U_{0,0}^\dagger}. \quad (\text{E}_7)$$

Hence,  $\delta_2$  is the unique angle in  $[0, \pi)$  such that  $\frac{e^{-i\delta_2}U_{0,2}^\dagger}{U_{0,0}^\dagger} \in \mathbb{R}$ . Then (E<sub>6</sub>) can be rephrased into

$$\tan\left(\frac{\delta_3}{2}\right) = \frac{e^{-i(\delta_1+\delta_2)}U_{0,2}^\dagger}{iU_{0,1}^\dagger}.$$

Hence,  $\delta_1$  is the unique angle in  $[0, \pi)$  such that  $\frac{e^{-i(\delta_1+\delta_2)}U_{0,2}^\dagger}{iU_{0,1}^\dagger} \in \mathbb{R}$ . In turn,  $\delta_3$  is the unique angle in  $[0, 2\pi)$  such that  $\tan\left(\frac{\delta_3}{2}\right) = \frac{e^{-i(\delta_1+\delta_2)}U_{0,2}^\dagger}{iU_{0,1}^\dagger}$ . Finally,  $\delta_4$  is the unique angle in  $[0, 2\pi)$  satisfying (E<sub>7</sub>).

Thus, assuming that the  $\delta_j$  exist, since  $U_I$  and  $U_{II}$  only depend on  $\delta_1, \delta_2, \delta_3, \delta_4$  and  $U$ , they are uniquely determined by  $U$ . Then (E<sub>2</sub>) implies that

- If  $(U_{II})_{1,2} = 0$ , then  $\sin(\frac{\delta_6}{2}) = 0$ , which means, since  $\delta_6 \in [0, 2\pi)$ , that  $\delta_6 = 0$ . By the conditions of Figure 5, this implies that  $\delta_5 = 0$ .
- If  $(U_{II})_{2,2} = 0$ , then  $\cos(\frac{\delta_6}{2}) = 0$ , which means, since  $\delta_6 \in [0, 2\pi)$ , that  $\delta_6 = \pi$ . By the conditions of Figure 5, this implies that  $\delta_5 = 0$ .
- If  $(U_{II})_{1,2} = 0, (U_{II})_{2,2} \neq 0$ , then

$$\tan\left(\frac{\delta_6}{2}\right) = \frac{e^{i\delta_5}(U_{II})_{1,2}}{i(U_{II})_{2,2}}.$$

Hence,  $\delta_5$  is the unique angle in  $[0, \pi)$  such that  $\frac{e^{i\delta_5}(U_{II})_{1,2}}{i(U_{II})_{2,2}} \in \mathbb{R}$ . In turn,  $\delta_6$  is the unique angle in  $[0, 2\pi)$  such that  $\tan\left(\frac{\delta_6}{2}\right) = \frac{e^{i\delta_5}(U_{II})_{1,2}}{i(U_{II})_{2,2}}$ .

Thus, assuming that the  $\delta_j$  exist, since  $U_{III}$  only depends on  $\delta_5, \delta_6$  and  $U_{II}$ , it is uniquely determined by  $U$ . Then by (E<sub>1</sub>),  $\delta_8 = \arg((U_{III})_{2,2}^\dagger)$ ,  $\delta_9 = \arg((U_{III})_{0,0}^\dagger)$  and  $\delta_7 = \arg\left(\frac{(U_{III})_{0,0}(U_{III})_{2,2}}{(U_{III})_{1,1}}\right)$ .

#### H. Proof of Proposition 20

Proof of Equation (k):

$$\begin{aligned}
\boxed{P(\varphi_1)} \boxed{P(\varphi_2)} &\stackrel{(a)}{=} \boxed{H} \boxed{H} \boxed{P(\varphi_1)} \boxed{H} \boxed{H} \boxed{P(\varphi_2)} \boxed{H} \boxed{H} \\
&\stackrel{(b)(c)(3)}{=} \boxed{H} \boxed{R_X(\varphi_1)} \boxed{R_X(\varphi_2)} \boxed{H} \\
&\stackrel{(d)}{=} \boxed{H} \boxed{R_X(\varphi_1)} \boxed{P(0)} \boxed{R_X(\varphi_2)} \boxed{H} \\
&\stackrel{(q)}{=} \boxed{H} \boxed{P(\beta_1)} \boxed{R_X(\beta_2)} \boxed{P(\beta_3)} \boxed{H} \\
&\stackrel{(q)}{=} \boxed{H} \boxed{R_X(\varphi_1 + \varphi_2)} \boxed{P(0)} \boxed{R_X(0)} \boxed{H} \\
&\stackrel{(d)(17)}{=} \boxed{H} \boxed{R_X(\varphi_1 + \varphi_2)} \boxed{H} \\
&\stackrel{(3)(a)(c)(b)}{=} \boxed{P(\varphi_1 + \varphi_2)}
\end{aligned}$$

The first use of Equation (q) is valid since Equation (q) is applied from the left to the right. The second use of Equation (q) is valid since it preserves the semantics. Note that one can show that  $\beta_1 = \beta_3 = 0$ ,  $\beta_2 = \varphi_1 + \varphi_2 \bmod 2\pi$  and  $\beta_0 = \begin{cases} 0 & \text{if } (\varphi_1 + \varphi_2 \bmod 4\pi) \in [0, 2\pi) \\ \pi & \text{if } (\varphi_1 + \varphi_2 \bmod 4\pi) \in [2\pi, 4\pi) \end{cases}$ .

Proof of Equation (l):

$$\begin{aligned}
\boxed{X} \boxed{P(\varphi)} \boxed{X} &\stackrel{(2)(1)}{=} \boxed{H} \boxed{P(\pi)} \boxed{H} \boxed{P(\varphi)} \boxed{H} \boxed{P(\pi)} \boxed{H} \\
&\stackrel{(b)(c)(3)}{=} \boxed{R_X(\pi)} \boxed{P(\varphi)} \boxed{R_X(\pi)}
\end{aligned}$$

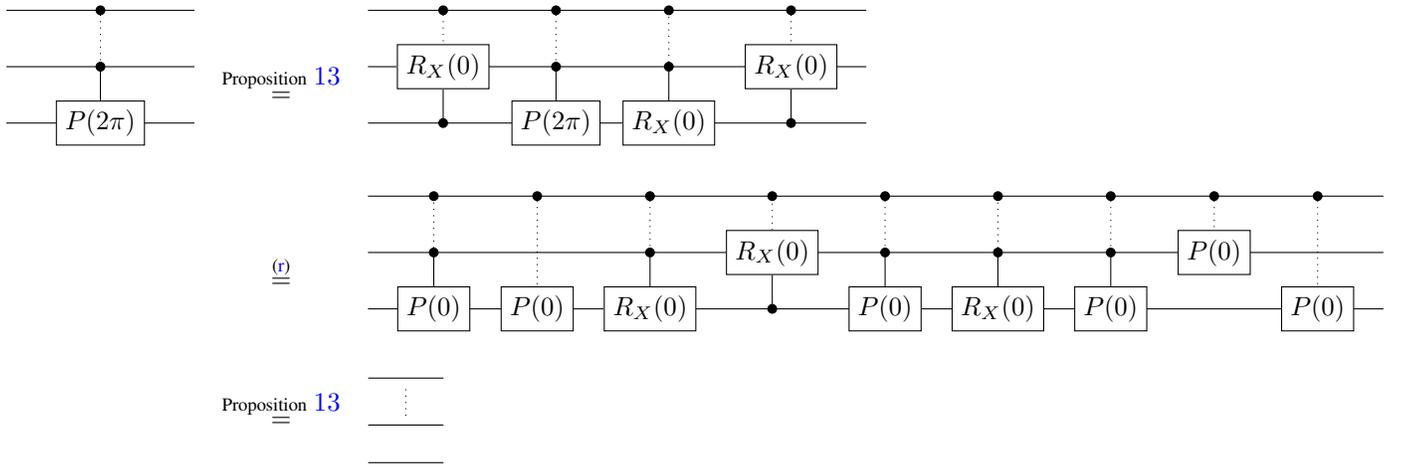
$$\stackrel{(q)(c)}{=} \overline{\begin{array}{c} \beta_0 + \pi \\ P(\beta_1) \quad R_X(\beta_2) \quad P(\beta_3) \end{array}}$$

One has  $\beta_1 = \beta_2 = 0$ ,  $\beta_3 = -\varphi \bmod 2\pi$  and  $\beta_0 = \varphi - \pi \bmod 2\pi$ . Indeed, this choice of angles satisfies the conditions of Equation (q) and is sound with respect to the semantics, and Proposition 19 guarantees that this is the only possible choice.

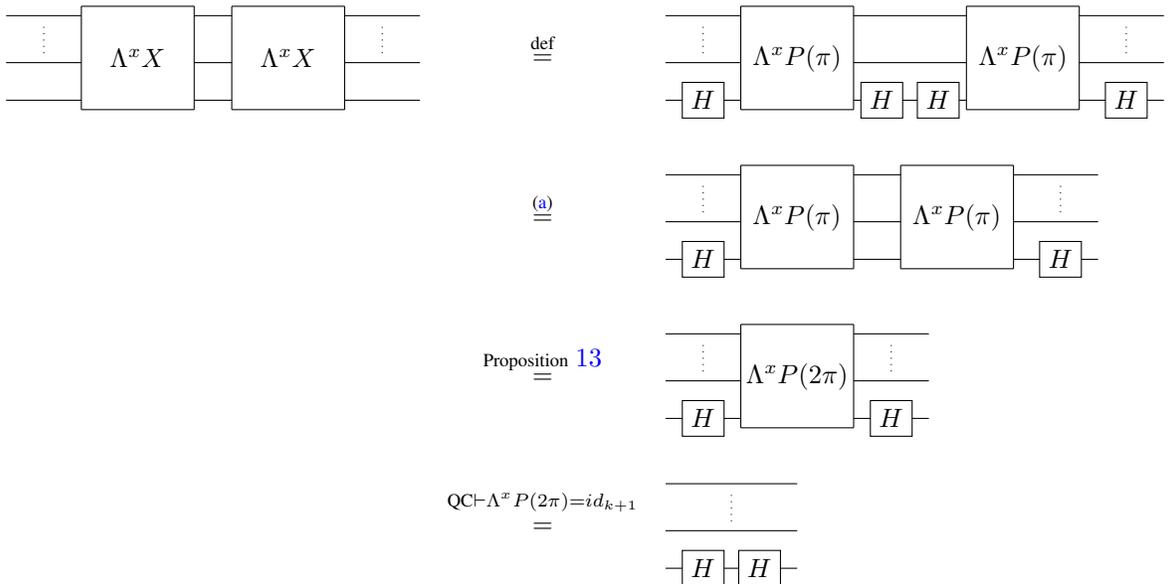
Thus, by Equations (d) and (17), this implies that one can transform  $\overline{X} \overline{P(\varphi)} \overline{X}$  into  $\overline{\overline{P(-\varphi \bmod 2\pi)}}$   $\stackrel{(b)(c)}{=}$   $\overline{P(-\varphi \bmod 2\pi)}$ . Finally,  $\overline{P(-\varphi)}$   $\stackrel{(17)}{=} \overline{R_X(0) \overline{P(-\varphi)} R_X(0)}$   $\stackrel{(q)(b)}{=} \overline{P(0) R_X(0) \overline{P(-\varphi \bmod 2\pi)}}$   $\stackrel{(d)(17)}{=} \overline{P(-\varphi \bmod 2\pi)}$ , which terminates the proof.

### I. Proof of Proposition 21

First, we can show that  $\text{QC} \vdash \Lambda^x P(2\pi) = id_{k+1}$  as follows:



It follows that, for  $x \in \{1\}^k$ :



$$\underline{\underline{(a)}} \quad \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \\ \text{---} \end{array}$$

*J. Proof of Proposition 22*

First, we prove the case for  $x = \epsilon$  :

$$\text{QC}_0 \vdash R_X(4\pi) = id_1 \quad \text{QC}_0 \vdash P(2\pi) = id_1 \quad \text{QC}_0 \vdash s(2\pi) = id_0$$

$$\begin{array}{c} \boxed{P(2\pi)} \quad \stackrel{(1)(k)}{=} \quad \boxed{Z} \text{---} \boxed{Z} \text{---} \\ \underline{\underline{(13)}} \quad \text{---} \end{array}$$

$$\textcircled{2\pi} \stackrel{(b)}{=} \boxed{\phantom{00}}$$

It follows that:

$$\begin{array}{c} \boxed{R_X(4\pi)} \quad \stackrel{(3)}{=} \quad \stackrel{\textcircled{-2\pi}}{\boxed{H}} \text{---} \boxed{P(4\pi)} \text{---} \boxed{H} \text{---} \\ = \quad \boxed{H} \text{---} \boxed{H} \text{---} \\ \underline{\underline{(a)}} \quad \text{---} \end{array}$$

We can now prove the general case, first by noticing that  $\text{QC} \vdash \Lambda^x P(2\pi) = id_{k+1}$ , as proven in Appendix C-I.

As  $\Lambda^{x_1} s(2\pi) = \Lambda^x P(2\pi)$ , we have for any  $x \in \{1\}^k$ ,  $\text{QC} \vdash \Lambda^x s(2\pi) = id_k$ .

Finally:

$$\begin{array}{c} \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \boxed{\Lambda^{1x} R_X(4\pi)} \begin{array}{c} \vdots \\ \text{---} \end{array} \\ = \quad \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \boxed{\Lambda^{1x} s(-2\pi)} \begin{array}{c} \vdots \\ \text{---} \end{array} \boxed{\Lambda^{1x} P(4\pi)} \begin{array}{c} \vdots \\ \text{---} \end{array} \\ \quad \quad \quad \boxed{H} \quad \quad \quad \boxed{H} \\ \text{QC} \vdash id_{k+1} = \Lambda^{1x} s(2\pi) \\ = \quad \begin{array}{c} \text{---} \\ \vdots \\ \text{---} \end{array} \boxed{\Lambda^{1x} s(2\pi)} \begin{array}{c} \vdots \\ \text{---} \end{array} \boxed{\Lambda^{1x} s(-2\pi)} \begin{array}{c} \vdots \\ \text{---} \end{array} \boxed{\Lambda^{1x} s(2\pi)} \begin{array}{c} \vdots \\ \text{---} \end{array} \boxed{\Lambda^{1x} P(4\pi)} \begin{array}{c} \vdots \\ \text{---} \end{array} \\ \quad \quad \quad \boxed{H} \quad \quad \quad \boxed{H} \end{array}$$

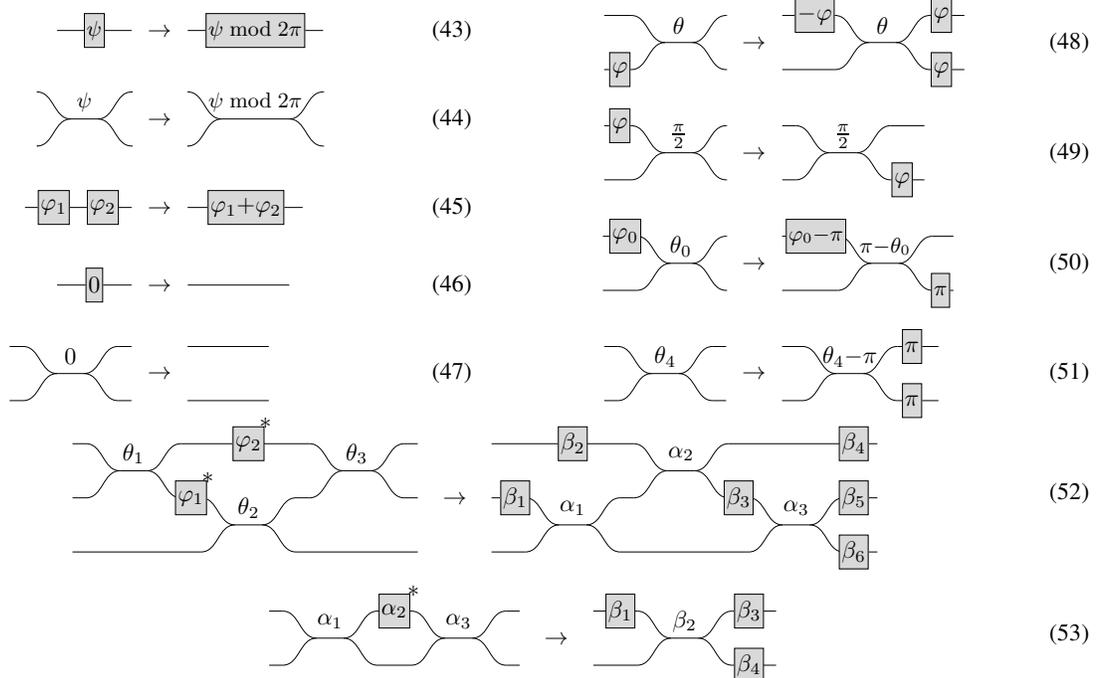
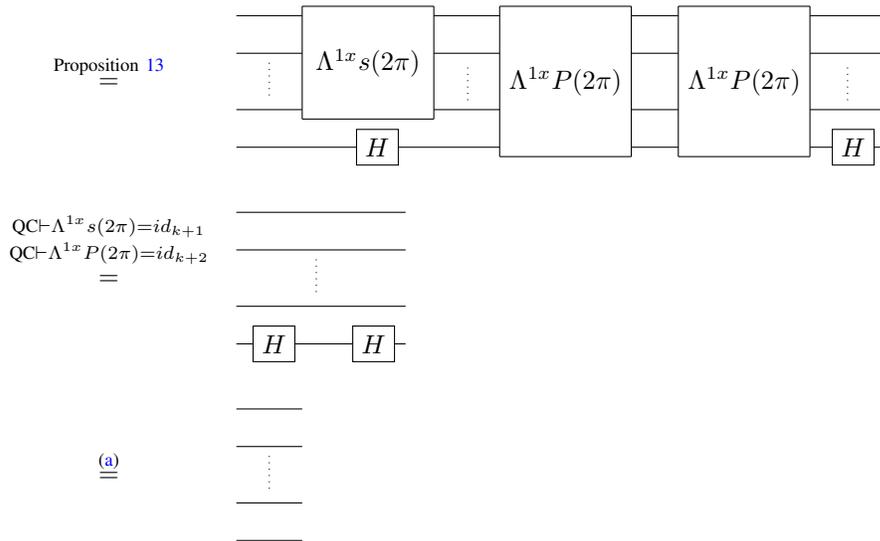


Fig. 8: Rewriting rules of PPRS.  $\boxed{\varphi}^*$  denotes either  $\boxed{\varphi}$  or  $\text{---}$ . The conditions on the angles are given in [30], note that for Equations (52) and (53) they are the same as in Figure 6 (with  $\varphi_1$ ,  $\varphi_2$  and  $\alpha_2$  taken as being 0 if missing).



## APPENDIX D PROOFS OF SECTION III

### A. Proof of Theorem 26

One can easily show that every equation of Figure 6 is sound with respect to the semantics. Regarding the completeness proof, we use the rewriting system of Figure 8 that has been introduced in [30]. This rewriting system has been proved to be strongly normalising, moreover it has been proved that any two swap-free circuits having the same semantics are reduced to the same normal form [30].

Using Equation (C) one can transform any circuit into a swap-free circuit. As a consequence, to prove the completeness it only remains to show that every rule of Figure 8 can be derived using the equations of Figure 6.

First we can notice that Rule (53) is exactly the same as Equation (F) (up to Equation (A)).

Rule (43) is derived from Equation (A) and Equation (D).

Rule (44) is derived from Equation (F) with  $\alpha_1 = \alpha_2 = 0$  and  $\alpha_3 = \psi + 2k\pi$ .

Rule (45) is derived from Equation (D).

Rule (46) is derived from Equation (A).

Rule (47) is derived from Equation (B).

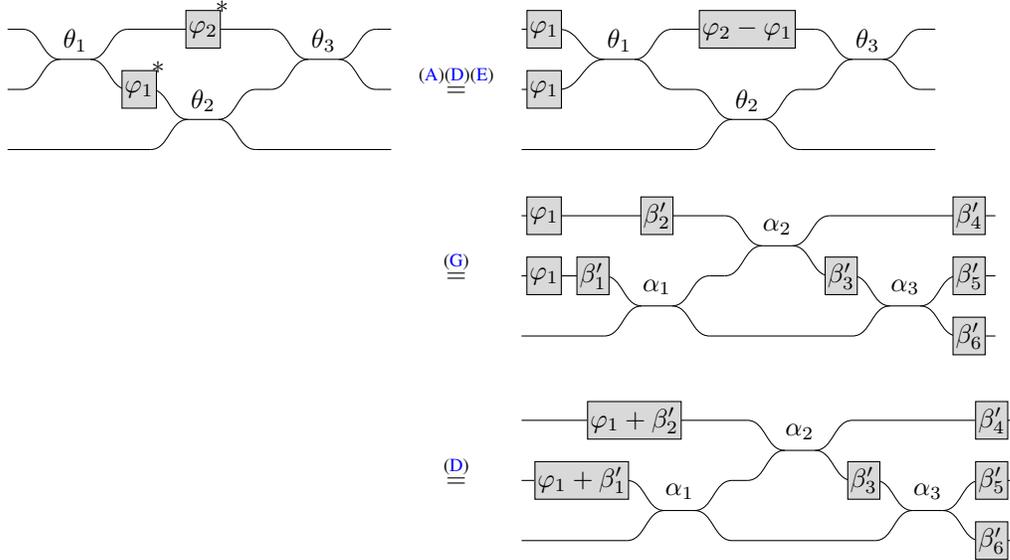
Rule (48) is derived from Equation (D), Equation (A) and Equation (E).

Rule (49) is derived from Equation (C) and Equation (D).

Rule (50) is derived from Equation (F) with  $\alpha_1 = 0$ ,  $\alpha_2 = \varphi_0$  and  $\alpha_3 = \theta_0$ .

Rule (51) is derived from Equation (F) with  $\alpha_1 = \alpha_2 = 0$  and  $\alpha_3 = \theta_4$ .

Regarding Rule (52), its LHS can be transformed as follows:



Note that the angles in the resulting circuit are not necessarily those of the RHS of Rule (52).

However, one can show that it can be put in normal form using the rules of Figure 8 except

Rule (52). As we have seen above that each of these rules can be derived using equations of Figure 6, this shows that Rule (52) can also be derived using the equations of Figure 6.

### B. Useful Definitions

**Definition 55.** Given  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^\ell$  and  $G \in \{s(\psi), X, R_X(\theta), P(\varphi)\}$ , we define

$$\bar{\Lambda}_y^x G := \prod_{\substack{x' \in \{0, 1\}^k \\ y' \in \{0, 1\}^\ell \\ x'y' \neq xy}} \Lambda_{y'}^{x'} G$$

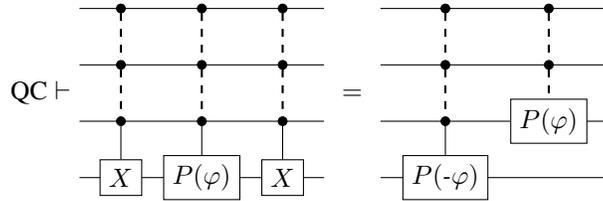
where the product denotes a sequential composition taken in an arbitrary order.

**Definition 56.** Given  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^\ell$  and  $z \in \{0, 1\}^m$ , we define

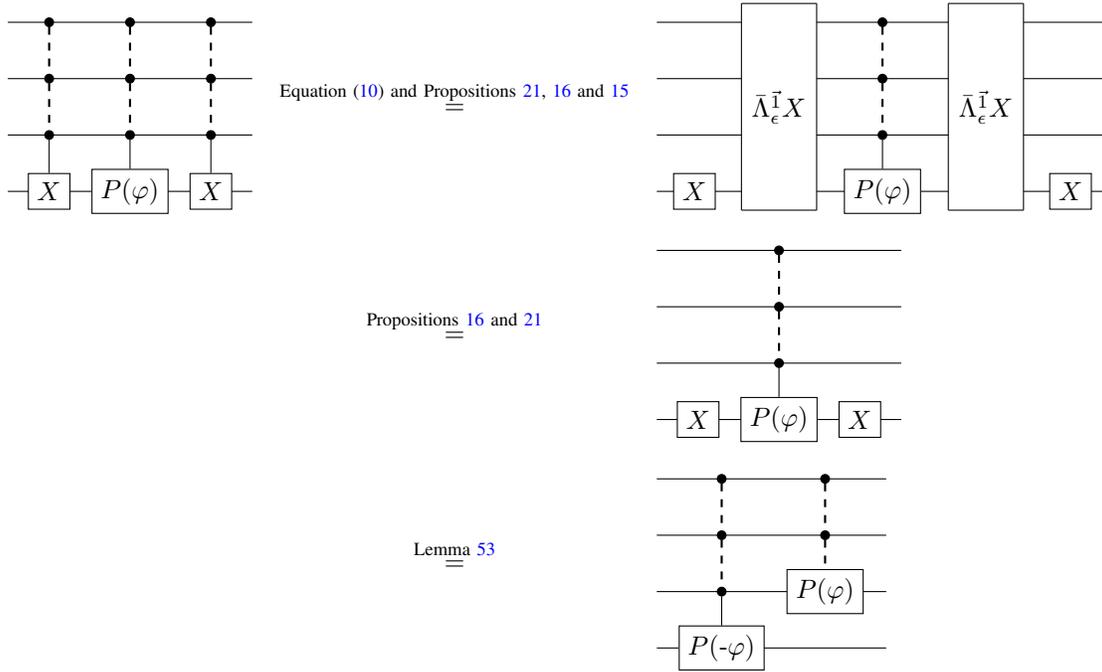
$$\Lambda_z^x \uparrow := \Lambda_z^{x1y} X, \quad \Lambda_z^x \oplus := \Lambda_{y1z}^x X, \quad \bar{\Lambda}_z^x \uparrow := \prod_{\substack{x' \in \{0, 1\}^k \\ y' \in \{0, 1\}^\ell \\ z' \in \{0, 1\}^m \\ x'y'z' \neq xyz}} \Lambda_{z'}^{x'1y'} X \quad \text{and} \quad \bar{\Lambda}_z^x \oplus := \prod_{\substack{x' \in \{0, 1\}^k \\ y' \in \{0, 1\}^\ell \\ z' \in \{0, 1\}^m \\ x'y'z' \neq xyz}} \Lambda_{y'1z'}^{x'} X.$$

C. Ancillary lemmas: Lemmas 57 to 61

**Lemma 57.**

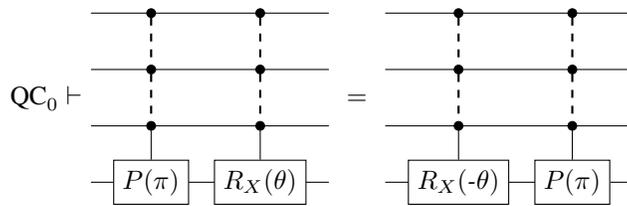


*Proof.*

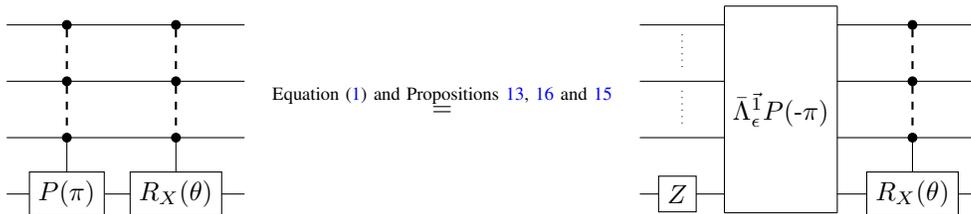


where  $\vec{1}$  denotes a list of appropriate length whose elements are all equal to 1. □

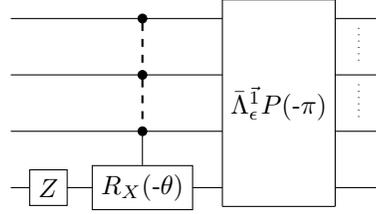
**Lemma 58.**



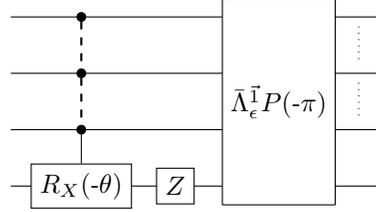
*Proof.*



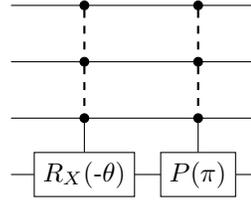
Proposition 16  
=



(25)  
=



Propositions 15, 16 and 13 and Equation (1)  
=



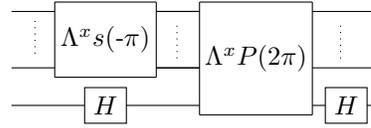
□

**Lemma 59.** For any  $x \in \{0, 1\}^k$ ,

$$\text{QC} \vdash \Lambda^x R_X(2\pi) = \Lambda^x s(\pi) \otimes \text{---}$$

*Proof.*

$$\Lambda^x R_X(2\pi) \stackrel{(10), (a), \text{Proposition 13 and Lemma 43}}{=} \text{---}$$

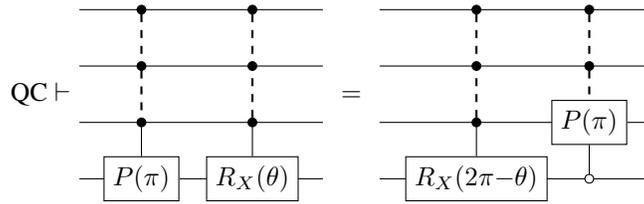


Propositions 22 and 13 and Equation (a)  
=

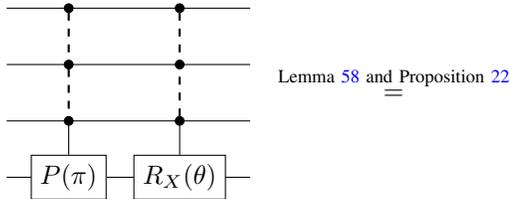
$$\Lambda^x s(\pi) \otimes \text{---}$$

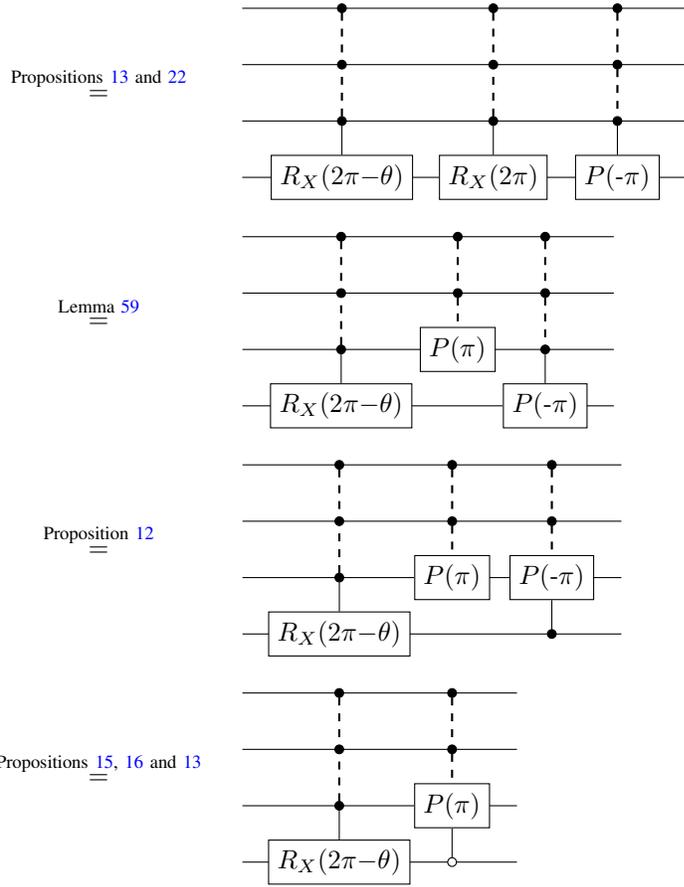
□

**Lemma 60.**



*Proof.*





□

**Lemma 61.** For any raw optical circuits  $C_1 : \ell_1 \rightarrow \ell_1$  and  $C_2 : \ell_2 \rightarrow \ell_2$ , and any  $k, \ell, n$  with  $\ell \geq \ell_1$  and  $k + \ell \leq 2^n$ ,

$$\text{QC}_0 \vdash D_{k+\ell, n}(C_2) \circ D_{k, n}(C_1) = D_{k, n}(C_1) \circ D_{k+\ell, n}(C_2).$$

*Proof.* We proceed by structural induction on  $C_1$  and  $C_2$ .

- If  $C_1 = C_1'' \circ C_1'$ , then

$$D_{k+\ell, n}(C_2) \circ D_{k, n}(C_1) = D_{k+\ell, n}(C_2) \circ (D_{k, n}(C_1'') \circ D_{k, n}(C_1'))$$

while

$$D_{k, n}(C_1) \circ D_{k+\ell, n}(C_2) = (D_{k, n}(C_1'') \circ D_{k, n}(C_1')) \circ D_{k+\ell, n}(C_2)$$

so the result follows by Equation (t<sub>2</sub>) of quantum circuits and the induction hypothesis.

- The case  $C_2 = C_2'' \circ C_2'$  is similar to the previous one.
- If  $C_1 = C_1' \otimes C_1''$  with  $C_1' : \ell_1' \rightarrow \ell_1'$ , then

$$D_{k+\ell, n}(C_2) \circ D_{k, n}(C_1) = D_{k+\ell, n}(C_2) \circ (D_{k+\ell_1', n}(C_1'') \circ D_{k, n}(C_1'))$$

while

$$D_{k, n}(C_1) \circ D_{k+\ell, n}(C_2) = (D_{k+\ell_1', n}(C_1'') \circ D_{k, n}(C_1')) \circ D_{k+\ell, n}(C_2)$$

so the result follows by Equation (t<sub>2</sub>) of quantum circuits and the induction hypothesis.

- The case  $C_2 = C_2' \otimes C_2''$  is similar to the previous one.
- If  $C_1$  or  $C_2$  is  $\begin{bmatrix} \square \\ \square \end{bmatrix}$  or  $\text{---}$ , then the results follows from Equation (t<sub>1</sub>) of quantum circuits.
- If  $C_1, C_2 \in \{\begin{bmatrix} \square \\ \square \end{bmatrix}, \begin{bmatrix} \square \\ \square \end{bmatrix}^\theta, \begin{bmatrix} \square \\ \square \end{bmatrix}^\times\}$ , then  $D_{k, n}(C_1) = \Lambda^{G_n(k)} s(\varphi)$ ,  $\Lambda_{y_{k, n}}^{x_{k, n}} R_X(-2\theta)$  or  $\Lambda_{y_{k, n}}^{x_{k, n}} X$  and  $D_{k+\ell, n}(C_2) = \Lambda^{G_n(k+\ell)} s(\varphi)$ ,  $\Lambda_{y_{k+\ell, n}}^{x_{k+\ell, n}} R_X(-2\theta)$  or  $\Lambda_{y_{k+\ell, n}}^{x_{k+\ell, n}} X$ . Using the definitions of  $G_n(k)$ ,  $x_{k, n}$  and  $y_{k, n}$ , it is easy to check that in any case,  $D_{k, n}(C_1)$  and  $D_{k+\ell, n}(C_2)$  satisfy the premises of either Proposition 16 or 17 and therefore commute.

□

#### D. Proof of Lemma 35

For the sake of clarity, the proofs are given separately in Appendices D-D1 to D-D3.

**Lemma 62.** For any  $N \geq 1$ ,  $i \in \{0, \dots, N-1\}$ ,  $b \in \{0, \dots, 2^i - 1\}$  and  $a \in \{0, \dots, 2^{N-i-1} - 1\}$ ,

$$\text{QC} \vdash D(v_{N,i,b,a}) = \Lambda_{G_{N-i-1}(2^{N-i-1}-a-1)}^{G_i(b)} X$$

where  $v_{N,i,b,a}$  is defined in Appendix D-G, and given  $n \in \mathbb{N}$  and  $k \in \{0, \dots, 2^n - 1\}$ ,  $G_n(k) \in \{0, 1\}^n$  is the  $n$ -bit Gray code of  $k$ , defined in Definition 27. Note that  $G_{N-i-1}(2^{N-i-1} - a - 1)$  differs from  $G_{N-i-1}(a)$  by only the first bit.

**Lemma 63.** For any  $k, \ell, n \in \mathbb{N}$ ,

$$\text{QC} \vdash D(\sigma_{k,n,\ell}) = id_k \otimes \sigma_{n,\ell}.$$

where  $\sigma_{0,0} := \square$  and  $\sigma_{n,\ell} := \sigma_{n+\ell-1}^\ell$ , where  $\sigma_{n+\ell-1}$  is defined in Figure 1.

**Lemma 64.** For any  $g \in \{\square, \text{---}, s(\varphi), \text{---} \square, \text{---} \square \text{---}, \text{---} \square \text{---}, \text{---} \square \text{---}, \text{---} \square \text{---}, \text{---} \square \text{---}\}$ ,

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

1) *Proof of Lemma 62:* We proceed by induction on  $a$ .

It follows from the definition of  $D$  that

$$D(v_{N,i,b,0}) \stackrel{\text{def}}{=} D \left( \begin{array}{c} (2b+1)2^{N-i-1}-1 \{ \text{---} \} \\ \text{---} \\ \text{---} \\ 2^N-(2b+1)2^{N-i-1}-1 \{ \text{---} \} \end{array} \right) = \Lambda_{G_{N-i-1}(2^{N-i-1}-1)}^{G_i(b)} X.$$

Assuming for some  $a \in \{1, \dots, 2^{N-i-1} - 1\}$  that  $\text{QC}_0 \vdash D(v_{N,i,b,a-1}) = \Lambda_{G_{N-i-1}(2^{N-i-1}-a)}^{G_i(b)} X$ , by definition of  $v_{N,i,b,a}$ , one has<sup>12</sup>

$$\text{QC}_0 \vdash D(v_{N,i,b,a}) = D(s_{-a}) \circ D(s_{+a}) \circ \left( \Lambda_{G_{N-i-1}(2^{N-i-1}-a)}^{G_i(b)} X \right) \circ D(s_{+a}) \circ D(s_{-a})$$

$$\text{where } s_{+a} = \begin{array}{c} (2b+1)2^{N-i-1}+a-1 \{ \text{---} \} \\ \text{---} \\ \text{---} \\ 2^N-(2b+1)2^{N-i-1}-a-1 \{ \text{---} \} \end{array} \text{ and } s_{-a} = \begin{array}{c} (2b+1)2^{N-i-1}-a-1 \{ \text{---} \} \\ \text{---} \\ \text{---} \\ 2^N-(2b+1)2^{N-i-1}+a-1 \{ \text{---} \} \end{array}.$$

Due to the properties of Gray codes,  $G_{N-i-1}(2^{N-i-1} - a - 1)$  differs from  $G_{N-i-1}(2^{N-i-1} - a)$  by only one bit. That is, there exist  $k, \ell \geq 0$  with  $k + \ell = N - i - 2$ ,  $x \in \{0, 1\}^k$ ,  $y \in \{0, 1\}^\ell$  and  $\alpha \in \{0, 1\}$ , such that

$$G_{N-i-1}(2^{N-i-1} - a - 1) = x\alpha y \quad \text{and} \quad G_{N-i-1}(2^{N-i-1} - a) = x\bar{\alpha}y$$

where  $\bar{\alpha} := 1 - \alpha$ .

Additionally,  $G_{N-i}(2^{N-i-1} - a - 1)$  differs from  $G_{N-i}(2^{N-i-1} + a)$  by only the first bit, and  $G_{N-i}(2^{N-i-1} - a)$  also differs from  $G_{N-i}(2^{N-i-1} + a - 1)$  by only the first bit. Therefore, there exists  $\beta \in \{0, 1\}$  such that

$$G_{N-i}(2^{N-i-1} - a - 1) = \beta x \alpha y, \quad G_{N-i}(2^{N-i-1} + a) = \bar{\beta} x \alpha y,$$

$$G_{N-i}(2^{N-i-1} - a) = \beta x \bar{\alpha} y \quad \text{and} \quad G_{N-i}(2^{N-i-1} + a - 1) = \bar{\beta} x \bar{\alpha} y.$$

It follows from the definition of  $D$  that  $D(s_{-a}) = \Lambda_y^{G_i(b) \cdot \beta x} X$  and  $D(s_{+a}) = \Lambda_y^{G_i(b) \cdot \bar{\beta} x} X$ . Hence, by Propositions 11, 15

$$\text{and 16, } \text{QC}_0 \vdash D(s_{-a}) \circ D(s_{+a}) = D(s_{+a}) \circ D(s_{-a}) = \begin{array}{c} \Lambda_{G_i(b)} \\ \text{---} \\ \text{---} \\ \Lambda^x \\ \text{---} \\ \text{---} \\ X \\ \text{---} \\ \text{---} \\ \Lambda^y \end{array} = (\sigma_{1,i} \otimes id_{N-i-1}) \circ \left( \text{---} \otimes \Lambda_y^{G_i(b)x} X \right) \circ (\sigma_{i,1} \otimes id_{N-i-1}),$$

so that

$$\text{QC} \vdash D(v_{N,i,b,a}) = (\sigma_{1,i} \otimes id_{N-i-1}) \circ \left( \text{---} \otimes \Lambda_y^{G_i(b)x} X \right) \circ \left( \Lambda_{G_i(b)x\bar{\alpha}y}^\epsilon X \right) \circ \left( \text{---} \otimes \Lambda_y^{G_i(b)x} X \right) \circ (\sigma_{i,1} \otimes id_{N-i-1})$$

with

<sup>12</sup>Note that this product of five raw circuits should be written with more parentheses since the composition is not associative. We have omitted these parentheses by abuse of language in order to lighten the notations. In the following, we will similarly omit the associativity parentheses whenever this does not create ambiguity.

$$\begin{aligned}
& \text{QC} \vdash \left( \text{---} \otimes \Lambda_y^{G_i(b)x} X \right) \circ \left( \Lambda_{G_i(b)x\bar{\alpha}y}^\epsilon X \right) \circ \left( \text{---} \otimes \Lambda_y^{G_i(b)x} X \right) \\
& \stackrel{\text{Propositions 21, 16 and 15}}{=} (id_{N-1} \otimes X) \circ \left( \text{---} \otimes \bar{\Lambda}_y^{G_i(b)x} X \right) \circ \left( \Lambda_{G_i(b)x\bar{\alpha}y}^\epsilon X \right) \circ \left( \text{---} \otimes \bar{\Lambda}_y^{G_i(b)x} X \right) \circ (id_{N-1} \otimes X) \\
& \stackrel{\text{Propositions 15 and 16}}{=} (id_{N-1} \otimes X) \circ \left( \text{---} \otimes \bar{\Lambda}_y^{G_i(b)x} X \right) \circ \left( \text{---} \otimes \bar{\Lambda}_y^{G_i(b)x} X \right) \circ \left( \Lambda_{G_i(b)x\bar{\alpha}y}^\epsilon X \right) \circ (id_{N-1} \otimes X) \\
& \stackrel{\text{Propositions 16 and 21}}{=} (id_{N-1} \otimes X) \circ \left( \Lambda_{G_i(b)x\bar{\alpha}y}^\epsilon X \right) \circ (id_{N-1} \otimes X)
\end{aligned}$$

In other words,

$$\text{QC} \vdash D(v_{N,i,b,a}) = (id_{i+k+1} \otimes X \otimes id_\ell) \circ \left( \Lambda_{x\bar{\alpha}y}^{G_i(b)} X \right) \circ (id_{i+k+1} \otimes X \otimes id_\ell).$$

By definition of  $\Lambda_{x\bar{\alpha}y}^{G_i(b)} X$  and Equation (10), this implies that

$$\text{QC} \vdash D(v_{N,i,b,a}) = \Lambda_{x\alpha y}^{G_i(b)} X$$

which, since  $x\alpha y = G_{N-i-1}(2^{N-i-1} - a - 1)$ , is the desired property.

**Remark 65.** By defining  $v_{N,i,b,a}$  in a less natural way using not only  $\text{---}$  and  $\bowtie$  but also  $\boxminus$  and  $\succ\curvearrowright$ , one could avoid using Proposition 21 and get the stronger result that  $\text{QC}_0 \vdash D(v_{N,i,b,a}) = \Lambda_{G_{N-i-1}(2^{N-i-1}-a-1)}^{G_i(b)} X$ , which would in turn imply that the equalities of Lemmas 63 and 64 can also be taken modulo  $\text{QC}_0$  instead of  $\text{QC}$ .

2) *Proof of Lemma 63:* First, if  $n = 1$ , by definition (see Definition 32 and Appendix D-G), one has

$$D(\sigma_{k,1,\ell}) = \prod_{j=k+1}^{k+\ell} P_j Q_j P_j$$

$$\text{where } M := k + \ell + 1, P_j := \prod_{\substack{b=0 \\ b \bmod 4 \in \{1,2\}}}^{2^j-1} \prod_{a=0}^{2^{M-j-1}-1} D(v_{M,j,b,a}) \text{ and } Q_j := \prod_{b=0}^{2^{j-1}-1} \prod_{a=0}^{2^{M-j-3}-1} D(v_{M,j-1,b,a}).$$

By Lemma 62, for all  $j$ ,

$$\text{QC} \vdash P_j = \prod_{\substack{b=0 \\ b \bmod 4 \in \{1,2\}}}^{2^j-1} \prod_{a=0}^{2^{M-j-1}-1} \Lambda_{G_{M-j-1}(2^{M-j-1}-a-1)}^{G_j(b)} X$$

It is easy to check that when  $a$  goes from 0 to  $2^{M-j-1} - 1$ ,  $G_{M-j-1}(2^{M-j-1} - a - 1)$  takes all possible values in  $\{0, 1\}^{M-j-1}$ , once each, and that when  $b$  takes all possible values between 0 and  $2^j - 1$  that are congruent to 1 or 2 modulo 4,  $G_j(b)$  takes, once each, all values in  $\{0, 1\}^j$  in which the last bit has value 1. Hence, it follows from Propositions 15, 16 and 10 that

$$\text{QC} \vdash P_j = id_{j-1} \otimes \begin{array}{c} \uparrow \\ \oplus \\ \uparrow \end{array} \otimes id_{M-j-1}.$$

Again by Lemma 62, for all  $j$ ,

$$\text{QC} \vdash Q_j = \prod_{b=0}^{2^{j-1}-1} \prod_{a=0}^{2^{M-j-3}-1} \Lambda_{G_{M-j}(2^{M-j}-a-1)}^{G_{j-1}(b)} X$$

Similarly, it is easy to check that when  $b$  goes from 0 to  $2^{j-1} - 1$ ,  $G_{j-1}(b)$  takes all values in  $\{0, 1\}^{j-1}$ , once each, and that when  $a$  goes from 0 to  $2^{M-j-3}$ ,  $G_{M-j}(2^{M-j} - a - 1)$  takes, once each, all values in  $\{0, 1\}^{M-j}$  in which the first bit has value 1. Hence, it follows from Propositions 15, 16 and 10 that

$$\text{QC} \vdash Q_j = id_{j-1} \otimes \begin{array}{c} \oplus \\ \uparrow \\ \oplus \end{array} \otimes id_{M-j-1}.$$

Thus,

$$\text{QC} \vdash D(\sigma_{k,1,\ell}) = \prod_{j=k+1}^{k+\ell} id_{j-1} \otimes \begin{array}{c} \oplus \\ \uparrow \oplus \\ \oplus \end{array} \otimes id_{M-j-1}.$$

By Equation (h), this implies that

$$\text{QC} \vdash D(\sigma_{k,1,\ell}) = \prod_{j=k+1}^{k+\ell} id_{j-1} \otimes \text{X} \otimes id_{M-j-1} \equiv id_k \otimes \sigma_{1,\ell}. \quad (54)$$

Finally, if  $n > 1$ , then

$$\begin{aligned} D(\sigma_{k,n,\ell}) &\stackrel{\text{def}}{=} D(\sigma_{k,1,\ell+n-1}^n) \\ &\stackrel{\text{def}}{=} D(\sigma_{k,1,\ell+n-1})^n \\ &\stackrel{(54)}{=} (id_k \otimes \sigma_{1,\ell+n-1})^n \\ &\equiv id_k \otimes \sigma_{n,\ell}. \end{aligned}$$

3) *Proof of Lemma 64:* If  $g = \boxed{\text{---}}$  or  $\text{---}$  then the result follows directly from the definitions. If  $g = s(\varphi)$ , then it follows from the definitions of  $E_{k,\ell}$  and  $D$  that

$$D(E_{k,\ell}(s(\varphi))) = \prod_{x \in \{0,1\}^{k+\ell}} \Lambda^x s(\varphi)$$

where we use the notation  $\prod_{x \in \{0,1\}^{k+\ell}}$  to denote the product without specifying the order of the factors. By Propositions 15 and 16, this implies that

$$\text{QC} \vdash D(E_{k,\ell}(s(\varphi))) = id_{k+\ell} \otimes s(\varphi)$$

which is equal to  $id_k \otimes s(\varphi) \otimes id_\ell$  by the topological rules of quantum circuits.

If  $g = \boxed{P(\varphi)}$ , then it follows from the definitions that if  $k = \ell = 0$ ,

$$D(E_{0,0}(\boxed{P(\varphi)})) = D(\boxed{P(\varphi)}) \equiv \Lambda^1 s(\varphi) = P(\varphi).$$

and if  $(k, \ell) \neq (0, 0)$ ,

$$D(E_{k,\ell}(P(\varphi))) = D(\sigma_{k,\ell,1}) \circ D \left( \left( \boxed{P(\varphi)} \right)^{\otimes 2^{k+\ell-1}} \right) \circ D(\sigma_{k,1,\ell})$$

with

$$D \left( \left( \boxed{P(\varphi)} \right)^{\otimes 2^{k+\ell-1}} \right) = \prod_{x \in \{0,1\}^{k+\ell}} \Lambda^{x^1} s(\varphi) = \prod_{x \in \{0,1\}^{k+\ell}} \Lambda^x P(\varphi).$$

By Propositions 15 and 16, this product is equal modulo  $\text{QC}_0$  to  $id_{k+\ell} \otimes P(\varphi)$ . Then, Lemma 63 together with topological rules of quantum circuits gives us the result.

If  $g = \boxed{H}$ , then it follows from the definitions that if  $k = \ell = 0$ ,

$$\begin{aligned} D(E_{0,0}(\boxed{H})) &= D(\boxed{H}) \stackrel{\frac{\pi}{4}}{\equiv} \Lambda^1 s(-\frac{\pi}{2}) \circ \Lambda_\epsilon^c R_X(-\frac{\pi}{2}) \circ \Lambda^1 s(-\frac{\pi}{2}) \\ &= \boxed{P(-\frac{\pi}{2})} \boxed{R_X(-\frac{\pi}{2})} \boxed{P(-\frac{\pi}{2})} \\ &\stackrel{(18)}{\equiv} \boxed{H} \end{aligned}$$

and if  $(k, \ell) \neq (0, 0)$ ,

$$D(E_{k,\ell}(\boxed{H})) = D(\sigma_{k,\ell,1}) \circ D \left( \left( \left( \boxed{H} \right)^{\otimes 2^{k+\ell-1}} \right) \right) \circ D(\sigma_{k,1,\ell})$$

with

$$D \left( \left( \left( \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \right) \otimes^{2^{k+\ell-1}} \right) \right) \equiv \prod_{x \in \{0,1\}^{k+\ell}} \left( \left( \prod_{a \in \{0,1\}} \Lambda^{xa1} S(-\frac{\pi}{2}) \right) \circ \left( \prod_{a \in \{0,1\}} \Lambda^{xa} R_X(-\frac{\pi}{2}) \right) \circ \left( \prod_{a \in \{0,1\}} \Lambda^{xa1} S(-\frac{\pi}{2}) \right) \right).$$

By Propositions 15 and 16, this product is equal modulo  $\text{QC}_0$  to  $id_{k+\ell} \otimes \text{---} \text{---} \text{---} \text{---}$ , which by Proposition 18 is equal modulo  $\text{QC}_0$  to  $\text{---} \text{---}$ . Then, Lemma 63 together with topological rules of quantum circuits gives us the result.

If  $g = \text{---}$ , then it follows from the definitions that if  $k = \ell = 0$ ,

$$D(E_{0,0}(\text{---})) = D(\text{---}) \equiv \Lambda_\epsilon^1 X$$

which is equal to  $\text{---}$  modulo  $\text{QC}_0$  by Proposition 10;  
and if  $(k, \ell) \neq (0, 0)$ ,

$$D(E_{k,\ell}(\text{---})) = D(\sigma_{k,\ell,2}) \circ D \left( \left( \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \right) \otimes^{2^{k+\ell-1}} \right) \circ D(\sigma_{k,2,\ell})$$

with

$$D \left( \left( \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \right) \otimes^{2^{k+\ell-1}} \right) \equiv \prod_{x \in \{0,1\}^{k+\ell}} \Lambda^{x1} X.$$

By Propositions 15 and 16, this product is equal modulo  $\text{QC}_0$  to  $id_{k+\ell} \otimes \Lambda^1 X$ , which by Proposition 10 is equal modulo  $\text{QC}_0$  to  $id_{k+\ell} \otimes \text{---}$ . Then, Lemma 63 together with topological rules of quantum circuits gives us the result.

If  $g = \text{---}$ , then it follows from the definitions that

$$D(E_{k,2,\ell}(\text{---})) = D(\sigma_{k,\ell,2}) \circ D(\sigma_{k+\ell,1,1}) \circ D(\sigma_{k,2,\ell})$$

By Lemma 63, this is equal modulo  $\text{QC}$  to  $(id_k \otimes \sigma_{\ell,2}) \circ (id_{k+\ell} \otimes \text{---}) \otimes (id_k \otimes \sigma_{\ell,2})$ , which by the topological rules of quantum circuits, is equal to  $id_k \otimes \text{---} \otimes id_\ell$ .

### E. Proof of Lemma 36

**Definition 66** (Context). A  $N$ -mode raw context  $\mathcal{C}[\cdot]_i$  with  $i \in \mathbb{N}$  is inductively defined as follows:

- $[\cdot]_i$  is a  $i$ -mode raw context
- if  $\mathcal{C}[\cdot]_i$  is a  $N$ -mode raw context and  $C$  is a  $M$ -mode raw optical circuit then  $\mathcal{C}[\cdot]_i \otimes C$  and  $C \otimes \mathcal{C}[\cdot]_i$  are  $N+M$ -mode raw contexts
- if  $\mathcal{C}[\cdot]_i$  is a  $N$ -mode raw context and  $C$  is a  $N$ -mode raw optical circuit then  $\mathcal{C}[\cdot]_i \circ C$  and  $C \circ \mathcal{C}[\cdot]_i$  are  $N$ -mode raw contexts.

**Definition 67** (Substitution). Given a  $N$ -mode raw context  $\mathcal{C}[\cdot]_i$  and a  $i$ -mode raw circuit  $C$ , we define the substituted circuit  $\mathcal{C}[C]$  as the  $N$ -mode raw circuit obtained by replacing the hole  $[\cdot]_i$  by  $C$  in  $\mathcal{C}[\cdot]_i$ .

To prove Lemma 36, it suffices to prove that for each rule of Figure 1, of the form  $C_1 = C_2$  with  $C_1, C_2 \in \mathbf{LOPP}_{\text{raw}}(i, i)$ , and any  $2^n$ -mode raw context  $\mathcal{C}[\cdot]_i$ , one has  $\text{QC} \vdash D(\mathcal{C}[C_1]) = D(\mathcal{C}[C_2])$ . For this purpose, we prove a slightly more general result, namely that for any  $k, n$  and any  $\ell$ -mode raw context  $\mathcal{C}[\cdot]_i$  with  $k + \ell \leq 2^n$ , one has  $\text{QC} \vdash D_{k,n}(\mathcal{C}[C_1]) = D(\mathcal{C}[C_2])$ . We proceed by induction on  $\mathcal{C}[\cdot]_i$ :

- If  $\mathcal{C}[\cdot]_i = C \circ \mathcal{C}'[\cdot]_i$ , then  $D_{k,n}(\mathcal{C}[C_1]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_1])$  and  $D_{k,n}(\mathcal{C}[C_2]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_2])$ , so the result follows by induction hypothesis. The case  $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \circ C$  is similar.
- If  $\mathcal{C}[\cdot]_i = C \otimes \mathcal{C}'[\cdot]_i$  with  $C : \ell_1 \rightarrow \ell_2$ , then  $D_{k,n}(\mathcal{C}[C_1]) = D_{k+\ell_1,n}(\mathcal{C}'[C_1]) \circ D_{k,n}(C)$  and  $D_{k,n}(\mathcal{C}[C_2]) = D_{k+\ell_1,n}(\mathcal{C}'[C_2]) \circ D_{k,n}(C)$ , so the result follows by induction hypothesis. The case  $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \otimes C$  is similar.

It remains to prove for each rule of Figure 1, of the form  $C_1 = C_2$  with  $C_1, C_2 \in \mathbf{LOPP}_{\text{raw}}(i, i)$ , that for any  $k, n$  with  $k + i \leq 2^n$ , one has  $\text{QC} \vdash D_{k,n}(C_1) = D_{k,n}(C_2)$ .

For Equation (t<sub>2</sub>), for any  $C_1, C_2, C_3 : \ell \rightarrow \ell$ ,

$$D_{k,n}((C_3 \circ C_2) \circ C_1) = (D_{k,n}(C_3) \circ D_{k,n}(C_2)) \circ D_{k,n}(C_1)$$

and

$$D_{k,n}(C_3 \circ (C_2 \circ C_1)) = D_{k,n}(C_3) \circ (D_{k,n}(C_2) \circ D_{k,n}(C_1)).$$

Both are equal according to Equation (t<sub>2</sub>) of quantum circuits.

For Equation (t<sub>5</sub>), for any optical circuits  $C_1 : \ell_1 \rightarrow \ell_1$ ,  $C_2 : \ell_2 \rightarrow \ell_2$  and  $C_3 : \ell_3 \rightarrow \ell_3$ ,

$$D_{k,n}((C_1 \otimes C_2) \otimes C_3) = D_{k+\ell_1+\ell_2,n}(C_3) \circ (D_{k+\ell_1,n}(C_2) \circ D_{k,n}(C_1))$$

and

$$D_{k,n}(C_1 \otimes (C_2 \otimes C_3)) = (D_{k+\ell_1+\ell_2,n}(C_3) \circ D_{k+\ell_1,n}(C_2)) \circ D_{k,n}(C_1).$$

Again, both are equal according to Equation (t<sub>2</sub>) of quantum circuits.

For Equation (t<sub>1</sub>), for any  $\ell$ -mode optical circuit  $C$ , by definition of  $id_\ell$  and  $D_{k,n}$ ,

$$D_{k,n}(id_\ell \circ C) = (id_n \circ (id_n \circ (\dots \circ (id_n \circ id_n) \dots))) \circ D_{k,n}(C)$$

with  $\ell + 1$  occurrences of  $id_n$  in the right-hand side. This is equal to  $D_{k,n}(C)$  according to Equation (t<sub>1</sub>) of quantum circuits.

Similarly,  $D_{k,n}(C \circ id_\ell) \equiv D_{k,n}(C)$ .

For Equation (t<sub>3</sub>), for any  $\ell$ -mode optical circuit  $C$ ,

$$D_{k,n}(\begin{bmatrix} \square \\ \square \end{bmatrix} \otimes C) = D_{k,n}(C) \circ id_\ell$$

which is equal to  $D_{k,n}(C)$  according to Equation (t<sub>1</sub>) of quantum circuits. Similarly,  $D_{k,n}(C \otimes \begin{bmatrix} \square \\ \square \end{bmatrix}) \equiv D_{k,n}(C)$ .

For Equation (t<sub>6</sub>), for any optical circuits  $C_1, C_2 : \ell \rightarrow \ell$  and  $C_3, C_4 : m \rightarrow m$ ,

$$D_{k,n}((C_2 \circ C_1) \otimes (C_4 \circ C_3)) = (D_{k+\ell,n}(C_4) \circ D_{k+\ell,n}(C_3)) \circ (D_{k,n}(C_2) \circ D_{k,n}(C_1))$$

and

$$D_{k,n}((C_2 \otimes C_4) \circ (C_1 \otimes C_3)) = (D_{k+\ell,n}(C_4) \circ D_{k,n}(C_2)) \circ (D_{k+\ell,n}(C_3) \circ D_{k,n}(C_1)).$$

The result follows from Equation (t<sub>2</sub>) of quantum circuits and Lemma 61.

For Equation (t<sub>7</sub>), one has

$$D_{k,n}(\begin{array}{c} \diagup \quad \diagdown \\ \diagdown \quad \diagup \end{array}) = \Lambda_{y_{k,n}}^{x_{k,n}} X \circ \Lambda_{y_{k,n}}^{x_{k,n}} X$$

which by Proposition 21, implies that

$$\text{QC} \vdash D_{k,n}(\begin{array}{c} \diagup \quad \diagdown \\ \diagdown \quad \diagup \end{array}) = id_n.$$

On the other hand,

$$D_{k,n}(\text{---} \otimes \text{---}) = id_n \circ id_n \equiv id_n.$$

For Equation (t<sub>4</sub>), we proceed by induction on  $C$ .

- If  $C = C_1 \circ C_2$ , then  $\sigma_k \circ ((C_1 \circ C_2) \otimes \text{---}) \equiv (\sigma_k \circ (C_1 \otimes \text{---})) \circ (C_2 \otimes \text{---})$ , and the derivation of the equivalence does not use Equation (t<sub>4</sub>). Hence it follows from the paragraphs above that

$$\text{QC} \vdash D_{k,n}(\sigma_k \circ ((C_1 \circ C_2) \otimes \text{---})) = D_{k,n}((\sigma_k \circ (C_1 \otimes \text{---})) \circ (C_2 \otimes \text{---})).$$

It follows similarly from those paragraphs that

$$\text{QC} \vdash D_{k,n}((\text{---} \otimes (C_1 \circ C_2)) \circ \sigma_k) = D_{k,n}((C_1 \otimes \text{---}) \circ ((C_2 \otimes \text{---}) \circ \sigma_k)).$$

The equality modulo QC of the two right-hand sides follows from the induction hypothesis, together with the compatibility of  $D_{k,n}$  with Equation (t<sub>2</sub>) modulo QC, which is proved above.

- If  $C = C_1 \otimes C_2$  with  $C_1 : \ell_1 \rightarrow \ell_1$  and  $C_2 : \ell_2 \rightarrow \ell_2$ , then

$$\sigma_k \circ ((C_1 \otimes C_2) \otimes \text{---}) \equiv ((\sigma_{\ell_1} \circ (C_1 \otimes \text{---})) \otimes id_{\ell_2}) \circ (id_{\ell_1} \otimes (\sigma_{\ell_2} \circ (C_2 \otimes \text{---})))$$

and the derivation of the equivalence does not use Equation (t<sub>4</sub>), so that by the paragraphs above (together with Equation (t<sub>1</sub>) of quantum circuits),

$$\text{QC} \vdash D_{k,n}(\sigma_k \circ ((C_1 \otimes C_2) \otimes \text{---})) = D_{k,n}(\sigma_{\ell_1} \circ (C_1 \otimes \text{---})) \circ D_{k+\ell_1}(\sigma_{\ell_2} \circ (C_2 \otimes \text{---})).$$

The result follows by applying a similar transformation to the right-hand side of Equation (t<sub>4</sub>) and applying the induction hypothesis.

- If  $C = \begin{bmatrix} \square \\ \square \end{bmatrix}$  or  $\text{---}$ , then the result follows from Equations (t<sub>1</sub>) and (t<sub>3</sub>) of quantum circuits.

- If  $C = \boxed{\varphi}$ , let us write  $G_n(k)$  as  $xay$  with  $a \in \{0, 1\}$  and  $y = \epsilon$  if  $k$  is even or  $y = 1.0^q$  for some  $q$  if  $k$  is odd. Then by definition of  $D_{k,n}$  and Equation (23), if  $a = 1$  then

$$\text{QC} \vdash D_{k,n}(\sigma_1 \circ (\boxed{\varphi} \otimes \text{---})) = \Lambda_y^x X \circ \Lambda_y^x P(\varphi)$$

and

$$\text{QC} \vdash D_{k,n}(\text{---} \otimes \boxed{\varphi} \circ \sigma_1) = (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda_y^x P(\varphi) (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda_y^x X.$$

By Propositions 15, 16 and 21, the following equalities are true modulo QC:

$$\begin{aligned} \Lambda_y^x X \circ \Lambda_y^x P(\varphi) &= (id_{|x|} \otimes X \otimes id_{|y|}) \circ \bar{\Lambda}_y^x X \circ \Lambda_y^x P(\varphi) \\ &= (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda_y^x P(\varphi) \circ \bar{\Lambda}_y^x X \\ &= (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda_y^x P(\varphi) \circ (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda_y^x X \end{aligned}$$

which gives us the result. The case  $a = 0$  is similar.

- If  $C = \succ^{\theta} \zeta$ , by the properties of the Gray code, exactly one bit differs between  $G_n(k)$  and  $G_n(k+1)$ , as well as between  $G_n(k+1)$  and  $G_n(k+2)$ , and in exactly one of the two cases this is the last bit that differs (namely between  $G_n(k)$  and  $G_n(k+1)$  if  $k$  is even, and between  $G_n(k+1)$  and  $G_n(k+2)$  if  $k$  is odd). Hence we can write  $G_n(k)$  as  $xayb$  with  $a, b \in \{0, 1\}$ , in such a way that  $G_n(k+2) = x\bar{a}y\bar{b}$  and  $G_n(k+1) = xay\bar{b}$  or  $x\bar{a}yb$  depending on the parity of  $k$ . We treat the case where  $k$  is even, the case with  $k$  odd is similar. Then

$$D_{k,n}(\sigma_2 \circ (\succ^{\theta} \zeta \otimes \text{---})) \equiv \Lambda^{xay} X \circ \Lambda_{yb}^x X \circ \Lambda^{xay} R_X(-2\theta)$$

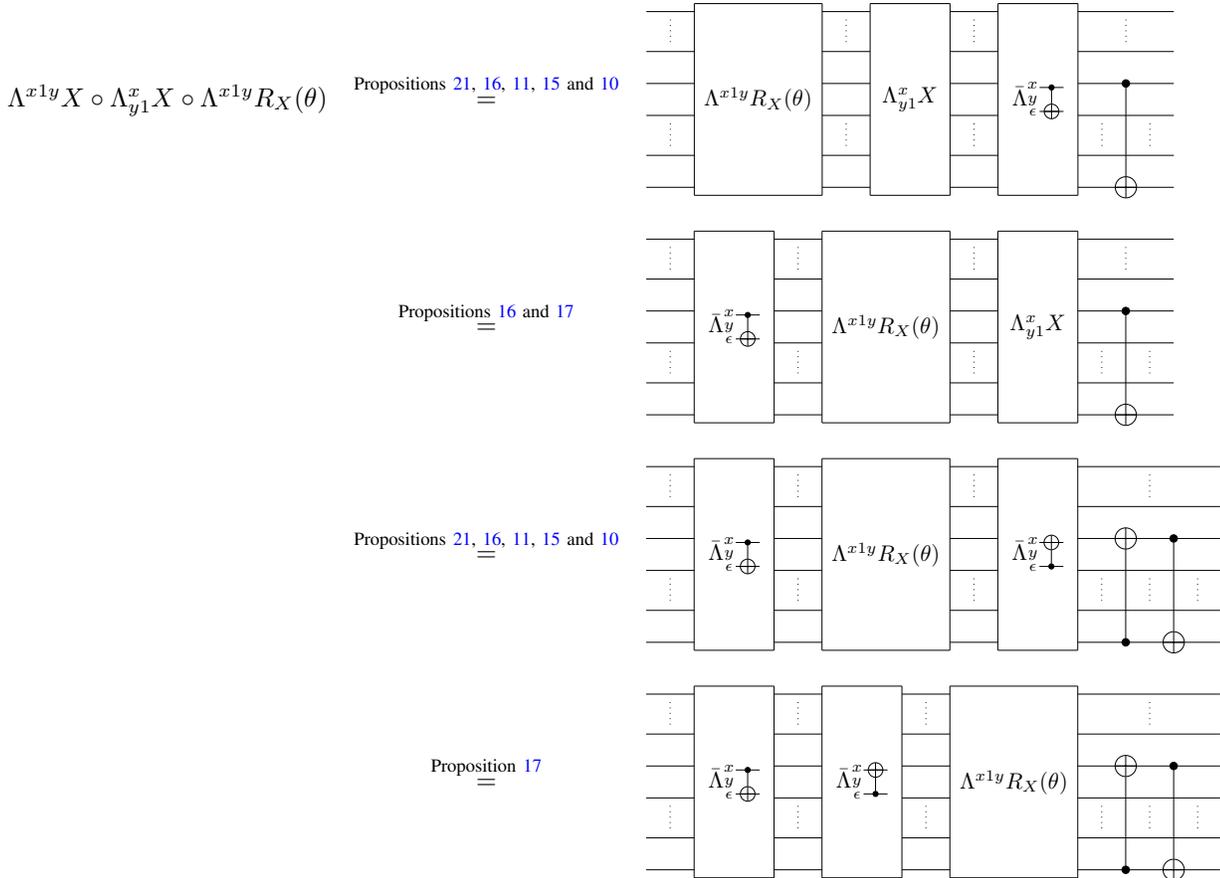
and

$$D_{k,n}(\text{---} \otimes \succ^{\theta} \zeta \circ \sigma_2) \equiv \Lambda_{yb}^x R_X(-2\theta) \circ \Lambda^{xay} X \circ \Lambda_{yb}^x X$$

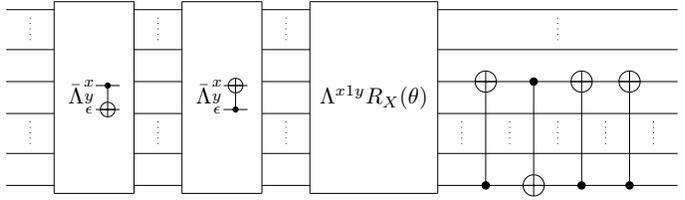
so by Lemma 52 and Equation (10), it suffices to prove that for any  $\theta$ ,

$$\text{QC} \vdash \Lambda^{x1y} X \circ \Lambda_{y1}^x X \circ \Lambda^{x1y} R_X(\theta) = \Lambda_{y1}^x R_X(\theta) \circ \Lambda^{x1y} X \circ \Lambda_{y1}^x X.$$

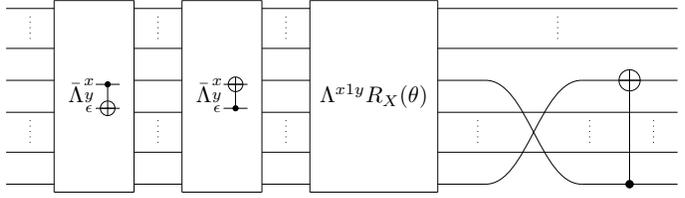
To prove this, one has, modulo QC (together with the topological rules of quantum circuits):



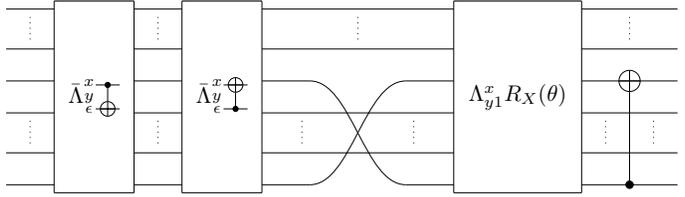
(e)



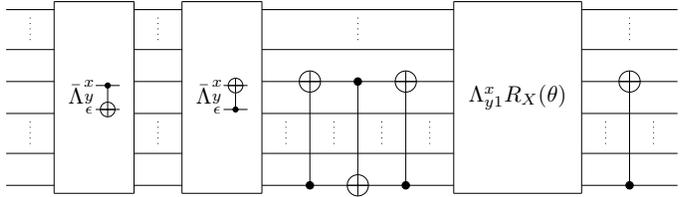
(h)



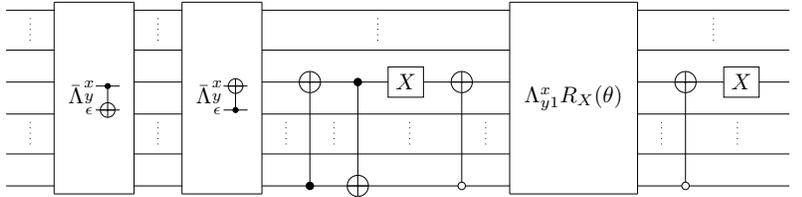
Proposition 11



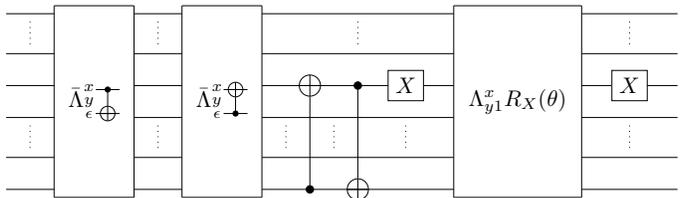
(h)



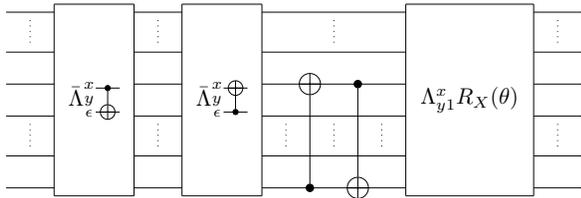
(10)(11)(12)

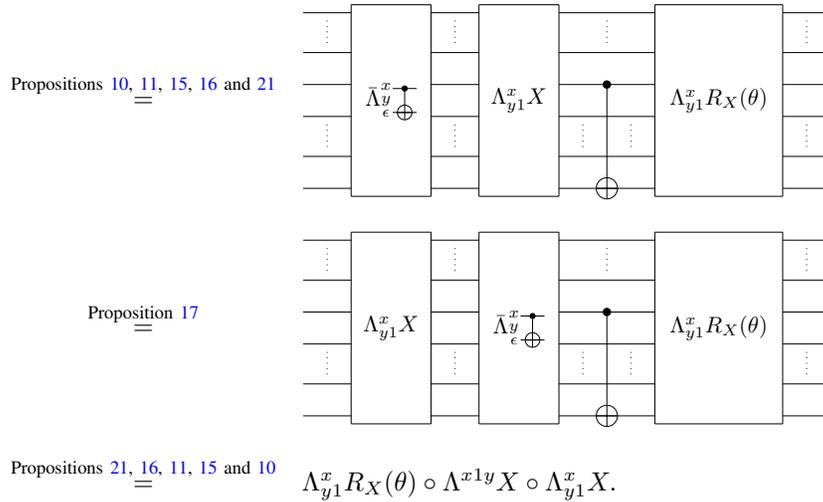


Propositions 10, 15 and 16



Lemma 52, (10)





- The case  $C = \bowtie$  is similar to the preceding one, with  $R_X(\theta)$  replaced by  $X$ .

#### F. Proof of Lemma 37

By Lemma 36, to prove Lemma 37, it suffices to prove that for each rule of Figure 6, of the form  $C_1 = C_2$  with  $C_1, C_2 \in \mathbf{LOPP}_{\text{raw}}(i, i)$  (see Footnote 10), and any  $2^n$ -mode raw context  $\mathcal{C}[\cdot]_i$ , one has  $\text{QC} \vdash D(\mathcal{C}[C_1]) = D(\mathcal{C}[C_2])$ . For this purpose, we prove a slightly more general result, namely that for any  $k, n$  and any  $\ell$ -mode raw context  $\mathcal{C}[\cdot]_i$  with  $k + \ell \leq 2^n$ , one has  $\text{QC} \vdash D_{k,n}(\mathcal{C}[C_1]) = D(\mathcal{C}[C_2])$ . We proceed by induction on  $\mathcal{C}[\cdot]_i$ :

- If  $\mathcal{C}[\cdot]_i = C \circ \mathcal{C}'[\cdot]_i$ , then  $D_{k,n}(\mathcal{C}[C_1]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_1])$  and  $D_{k,n}(\mathcal{C}[C_2]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_2])$ , so the result follows by induction hypothesis. The case  $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \circ C$  is similar.
- If  $\mathcal{C}[\cdot]_i = C \otimes \mathcal{C}'[\cdot]_i$  with  $C : \ell_1 \rightarrow \ell_1$ , then  $D_{k,n}(\mathcal{C}[C_1]) = D_{k+\ell_1,n}(\mathcal{C}'[C_1]) \circ D_{k,n}(C)$  and  $D_{k,n}(\mathcal{C}[C_2]) = D_{k+\ell_1,n}(\mathcal{C}'[C_2]) \circ D_{k,n}(C)$ , so the result follows by induction hypothesis. The case  $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \otimes C$  is similar.

It remains to prove for each rule of Figure 6, of the form  $C_1 = C_2$  with  $C_1, C_2 \in \mathbf{LOPP}_{\text{raw}}(i, i)$ , that for any  $k, n$  with  $k + i \leq 2^n$ , one has  $\text{QC} \vdash D_{k,n}(C_1) = D_{k,n}(C_2)$ . Again by Lemma 36, it suffices to prove that  $\text{QC} \vdash D_{k,n}(C'_1) = D_{k,n}(C'_2)$  for arbitrary  $C'_1$  and  $C'_2$  such that  $C'_1 \equiv C_1$  and  $C'_2 \equiv C_2$ .

For Equation (A), one has  $D_{k,n}(\text{---}) = \Lambda^{G_n(k)} s(0)$ ,  $D_{k,n}(\text{---}) = \Lambda^{G_n(k)} s(2\pi)$  and  $D_{k,n}(\text{---}) = id_n$ . The three are equal modulo QC by Propositions 13 and 22.

For Equation (B), one has  $D_{k,n}(\text{---}) = \Lambda_{y_{k,n}}^{x_{k,n}} R_X(0)$  (where  $x_{k,n}$  and  $y_{k,n}$  are defined in Definition 32) and  $D_{k,n}(\text{---}) = id_n \circ id_n \equiv id_n$ . The two are equal modulo QC by Proposition 13.

For Equation (C), one has  $D_{k,n}(\text{---}) = \Lambda_{y_{k,n}}^{x_{k,n}} X$ , and  $D_{k,n}(\text{---}) = \left( \prod_{j \in \{k, k+1\}} \Lambda^{G_n(j)} s(-\frac{\pi}{2}) \right) \circ \Lambda_{y_{k,n}}^{x_{k,n}} R_X(-\pi)$ . Note

that the definitions imply that

$$\{G_n(k), G_n(k+1)\} = \{x_{k,n} 0 y_{k,n}, x_{k,n} 1 y_{k,n}\}. \quad (55)$$

Therefore,

$$D_{k,n}(\text{---}) = \sigma_{1, |x_{k,n}|} \circ \left( \prod_{a \in \{0,1\}} \Lambda^{a x_{k,n} y_{k,n}} s(-\frac{\pi}{2}) \right) \circ \Lambda_{x_{k,n} y_{k,n}}^\epsilon R_X(-\pi) \circ \sigma_{|x_{k,n}|, 1}$$

Propositions 15 and 16

$$\stackrel{=}{=} \sigma_{1, |x_{k,n}|} \circ \left( \text{---} \otimes \Lambda^{x_{k,n} y_{k,n}} s(-\frac{\pi}{2}) \right) \circ \Lambda_{x_{k,n} y_{k,n}}^\epsilon R_X(-\pi) \circ \sigma_{|x_{k,n}|, 1}$$

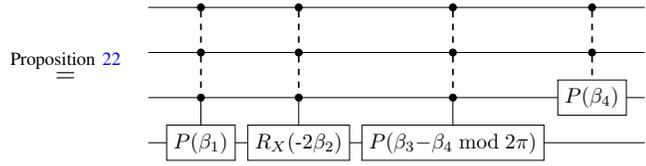
which by Lemma 48, Definition 8, Proposition 22, and Equation (a), is equal modulo QC to  $\Lambda_{y_{k,n}}^{x_{k,n}} X$ .

For Equation (D), one has  $D_{k,n}(\text{---}) = \Lambda^{G_n(k)} s(\varphi_2) \circ \Lambda^{G_n(k)} s(\varphi_1)$  and  $D_{k,n}(\text{---}) = \Lambda^{G_n(k)} s(\varphi_1 + \varphi_2)$ . Both are equal modulo QC by Proposition 13.

For Equation (E), one has

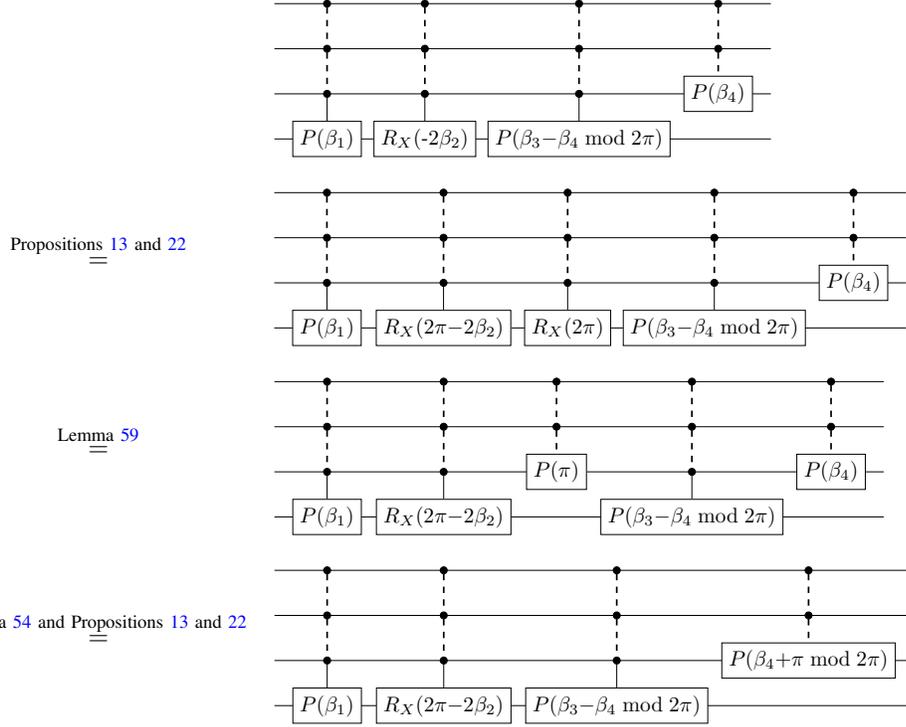
$$D_{k,n}(\text{---}) = \Lambda_{y_{k,n}}^{x_{k,n}} R_X(-2\theta) \circ \left( \prod_{j \in \{k, k+1\}} \Lambda^{G_n(j)} s(\varphi) \right)$$





Because of the conditions on the angles in the right-hand side of Equation (F), if  $\beta_2 = 0$  then the angles of the last circuit satisfy the conditions so that it matches the right-hand side of Equation (29). Hence, since it has the same semantics as  $\lambda^{n-1}R_X(-2\alpha_3) \circ \lambda^{n-1}P(\alpha_2) \circ \lambda^{n-1}R_X(-2\alpha_1)$ , both circuits are equal according to Equation (29).

If  $\beta_2 \neq 0$ , then



Because of the conditions on the angles in the right-hand side of Equation (F), one has  $\beta_2 \in (0, \pi)$ , so that  $2\pi - 2\beta_2 \in (0, 2\pi)$ , and if  $2\pi - 2\beta_2 = \pi$  then  $\beta_2 = \frac{\pi}{2}$ , so that  $\beta_1 = 0$ . Hence, the angles of the last circuit satisfy the conditions so that it matches the right-hand side of Equation (29). Again, since it has the same semantics as  $\lambda^{n-1}R_X(-2\alpha_3) \circ \lambda^{n-1}P(\alpha_2) \circ \lambda^{n-1}R_X(-2\alpha_1)$ , both circuits are equal according to Equation (29).

For Equation (G), by the properties of the Gray code, exactly one bit differs between  $G_n(k)$  and  $G_n(k+1)$ , as well as between  $G_n(k+1)$  and  $G_n(k+2)$ , and in exactly one of the two cases this is the last bit that differs (namely between  $G_n(k)$  and  $G_n(k+1)$  if  $k$  is even, and between  $G_n(k+1)$  and  $G_n(k+2)$  if  $k$  is odd). Hence we can write  $G_n(k)$  as  $xayb$  with  $a, b \in \{0, 1\}$ , in such a way that  $G_n(k+2) = x\bar{a}y\bar{b}$  and  $G_n(k+1) = xay\bar{b}$  or  $x\bar{a}yb$  depending on the parity of  $k$ . We treat the case where  $k$  is even, the case with  $k$  odd is similar. One has

$$D_{k,n} \left( \begin{array}{c} \text{Circuit with gates } \gamma_1, \gamma_2, \gamma_3, \gamma_4 \end{array} \right) \equiv \Lambda^{xay}R_X(-2\gamma_4) \circ \Lambda_{y\bar{b}}^x R_X(-2\gamma_3) \circ \Lambda^{xayb}s(\gamma_2) \circ \Lambda^{xay}R_X(-2\gamma_1)$$

and

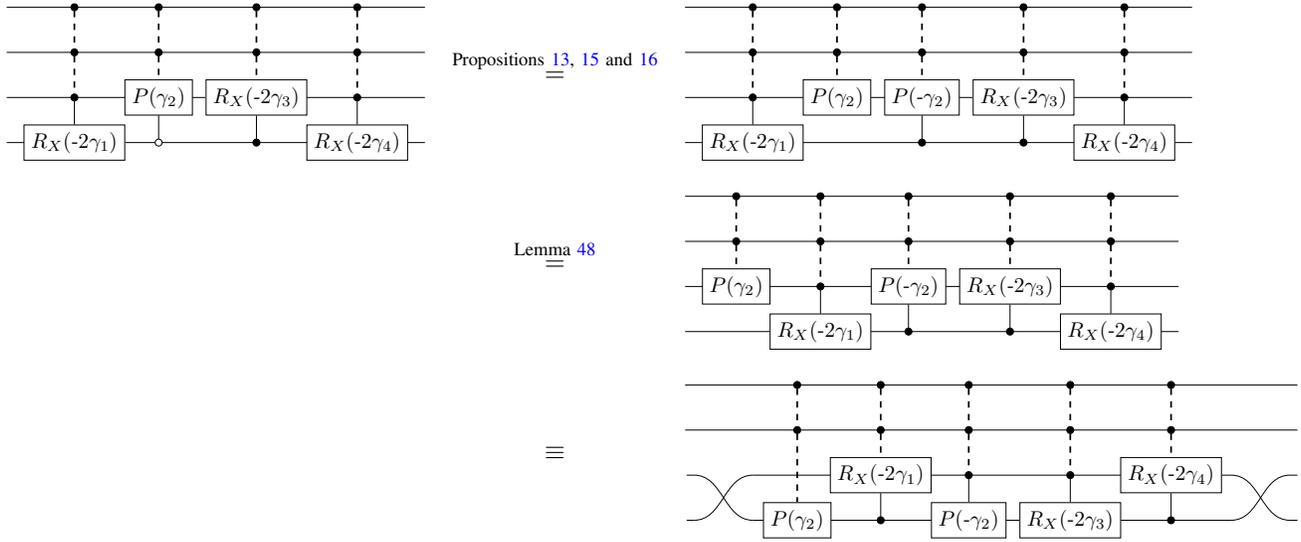
$$D_{k,n} \left( \begin{array}{c} \text{Circuit with gates } \delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9 \end{array} \right) \equiv \Lambda^{x\bar{a}y\bar{b}}s(\delta_9) \circ \Lambda^{xay\bar{b}}s(\delta_8) \circ \Lambda^{xayb}s(\delta_7) \circ \Lambda_{y\bar{b}}^x R_X(-2\delta_6) \circ \Lambda^{xay\bar{b}}s(\delta_5) \\ \circ \Lambda^{xay}R_X(-2\delta_4) \circ \Lambda_{y\bar{b}}^x R_X(-2\delta_3) \circ \Lambda^{xayb}s(\delta_2) \circ \Lambda^{xay\bar{b}}s(\delta_1).$$

Up to using Equation (10), we can assume that the components of  $x$  and  $y$  are all equal to 1. Up to using additionally Lemma 52, we can assume that  $a = 1$  and  $b = 0$ . Finally, up to deforming the circuits, we can assume that  $y = \epsilon$ . Thus, it suffices to prove that

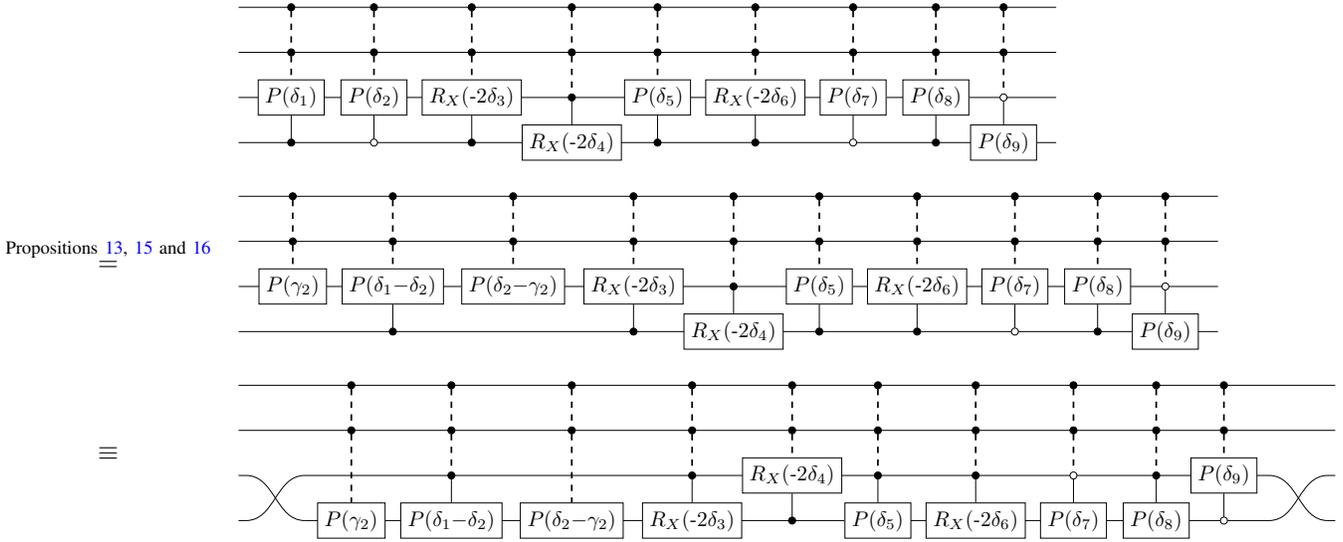
$$\text{QC} \vdash \Lambda^{x^1}R_X(-2\gamma_4) \circ \Lambda_1^x R_X(-2\gamma_3) \circ \Lambda^{x^{10}}s(\gamma_2) \circ \Lambda^{x^1}R_X(-2\gamma_1) = \Lambda^{x^{01}}s(\delta_9) \circ \Lambda^{x^{11}}s(\delta_8) \circ \Lambda^{x^{10}}s(\delta_7) \circ \Lambda_1^x R_X(-2\delta_6) \circ \Lambda^{x^{11}}s(\delta_5) \circ \\ \Lambda^{x^1}R_X(-2\delta_4) \circ \Lambda_1^x R_X(-2\delta_3) \circ \Lambda^{x^{10}}s(\delta_2) \circ \Lambda^{x^{11}}s(\delta_1)$$

where  $x = 1^{n-2}$ .

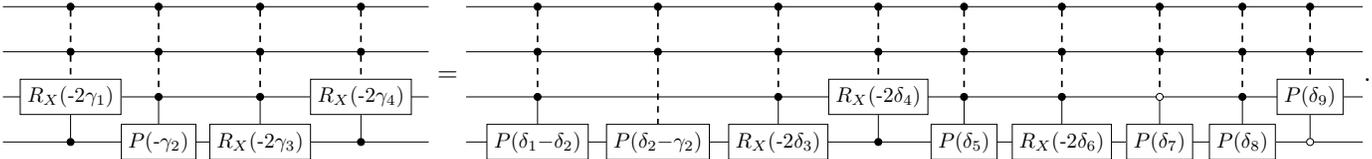
The left-hand side is equal to



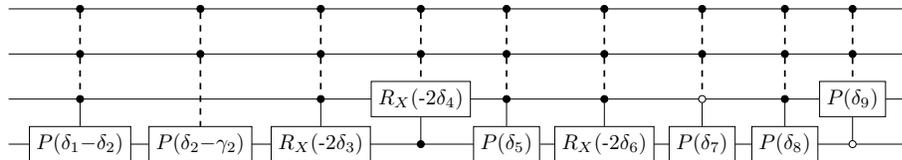
while the right-hand side is equal to



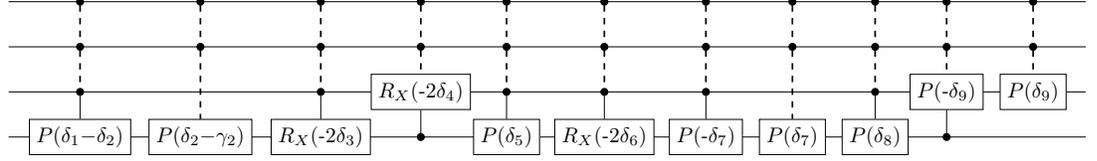
Hence, it suffices to prove that



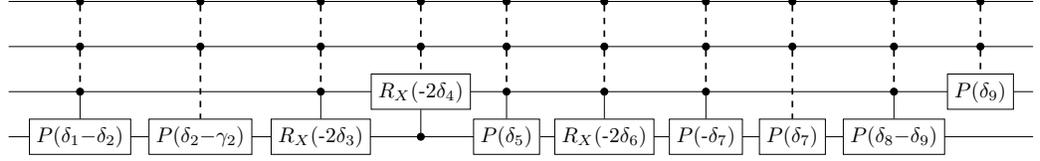
The left-hand side matches the left-hand side of Equation (r), hence it suffices to prove that the right-hand side can be put in the form of the right-hand side of Equation (r) with the angles satisfying the conditions. One has



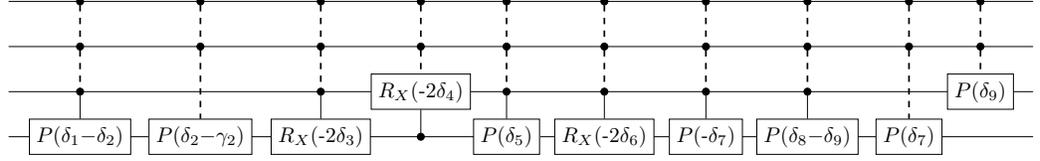
Propositions 13 and 15



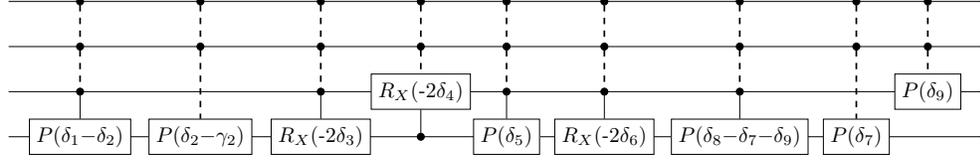
Propositions 12 and 13



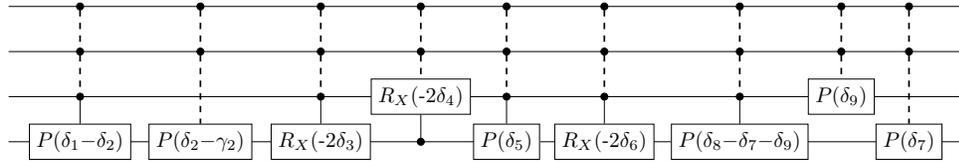
Propositions 13, 15 and 16



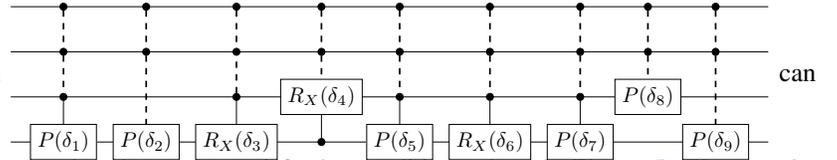
Proposition 13



Propositions 12, 13, 15 and 16



It remains to prove that any circuit of the form

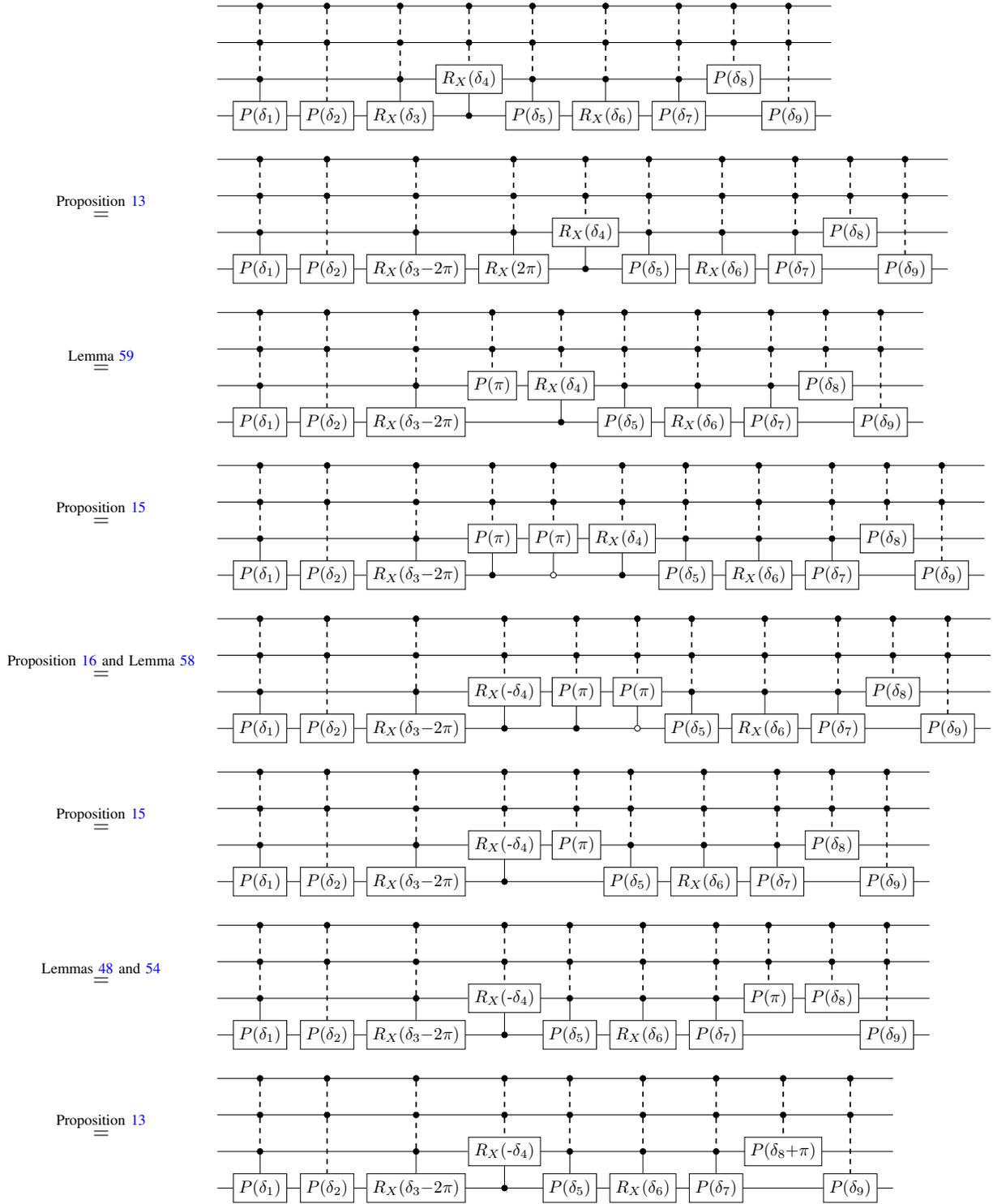


can be transformed using the axioms of QC in such a way that the angles satisfy the conditions given in Figure 5. We treat the conditions in the following order (note that some of the conditions of Figure 5 have been split into two parts):

- $\delta_3 \in [0, 2\pi)$
- $\delta_4 \in [0, 2\pi)$
- $\delta_6 \in [0, 2\pi)$
- if  $\delta_3 = 0$  then  $\delta_2 = 0$
- if  $\delta_3 \neq 0$  but  $\delta_4 = \pi$  then  $\delta_2 = 0$
- if  $\delta_3 = 0$  and  $\delta_4 = \pi$  then  $\delta_1 = 0$
- if  $\delta_3 = \pi$  then  $\delta_1 = 0$
- if  $\delta_4 = 0$  then  $\delta_1 = \delta_2 = \delta_3 = 0$
- if  $\delta_3 \neq 0$  then  $\delta_1 \in [0, \pi)$
- if  $\delta_3 = 0$  then  $\delta_1 \in [0, \pi)$
- if  $\delta_6 = 0$  then  $\delta_5 = 0$
- if  $\delta_6 = \pi$  then  $\delta_5 = 0$
- $\delta_2 \in [0, \pi)$
- $\delta_5 \in [0, \pi)$
- $\delta_7, \delta_8, \delta_9 \in [0, 2\pi)$ .

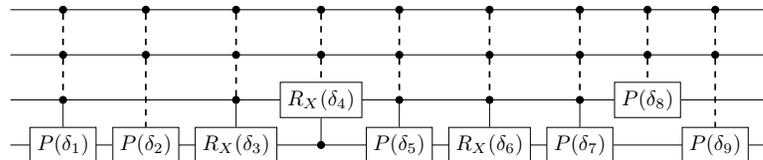
For each of them, we prove that given a circuit satisfying the previous conditions, we can transform it into a circuit satisfying also the considered condition.

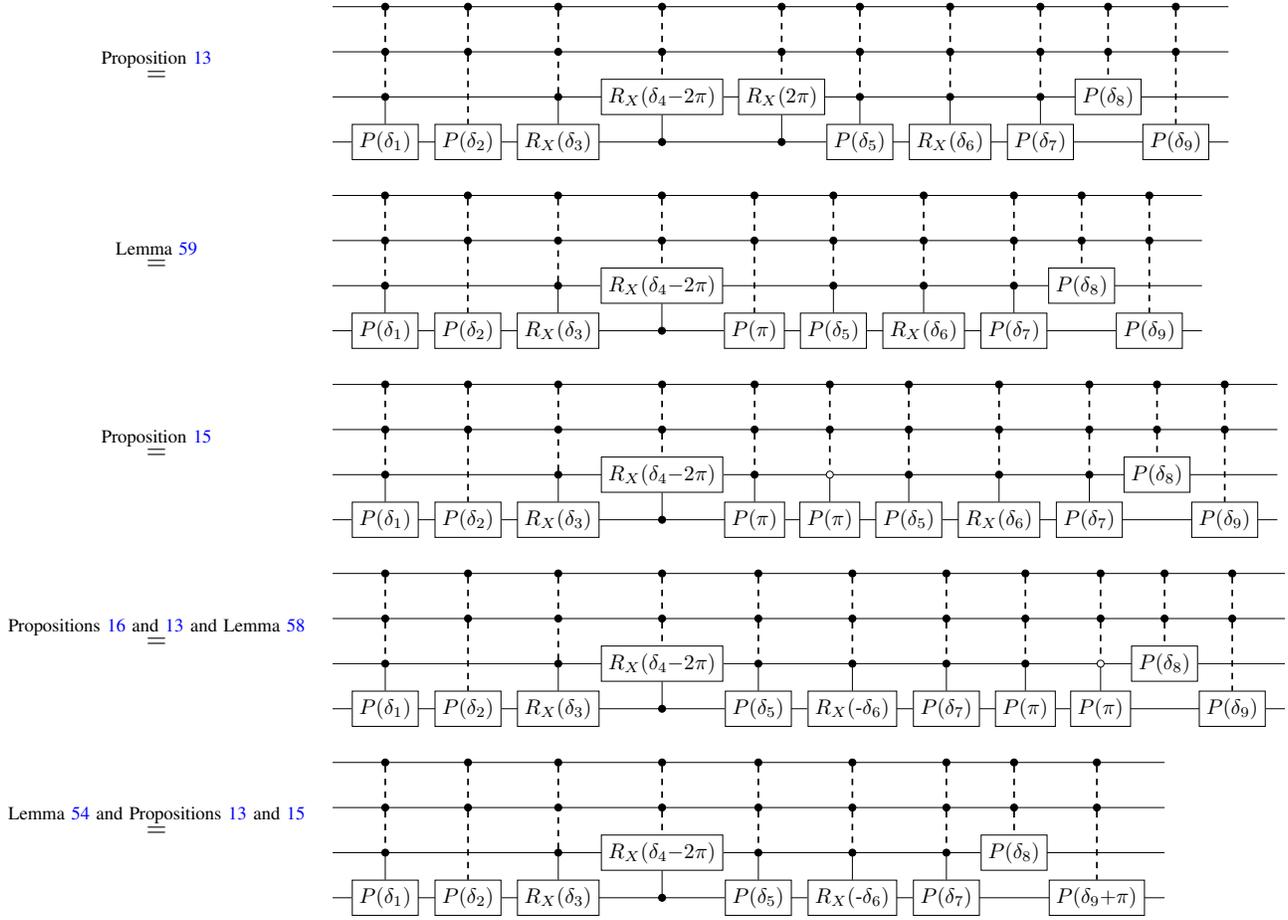
If  $\delta_3 \notin [0, 2\pi)$ , then by Proposition 22, we can assume that it is in  $[0, 4\pi)$ , and then if it is in  $[2\pi, 4\pi)$ , then:



with  $\delta_3 - 2\pi \in [0, 2\pi)$ . Hence, we can assume that  $\delta_3 \in [0, 2\pi)$ .

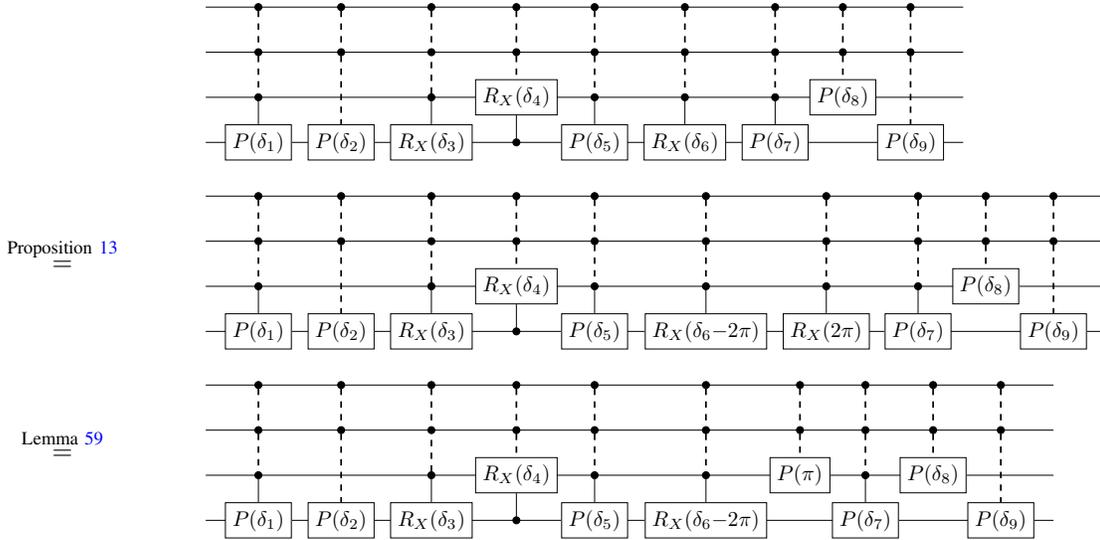
If  $\delta_4 \notin [0, 2\pi)$ , then by Proposition 22, we can ensure that it is in  $[0, 4\pi)$ , and then if it is in  $[2\pi, 4\pi)$ , then:



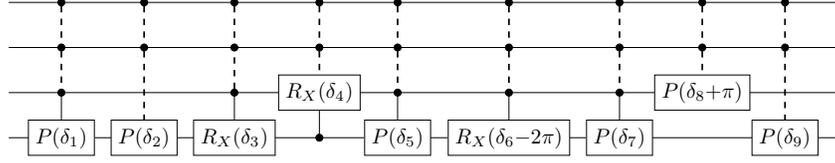


with  $\delta_4 - 2\pi \in [0, 2\pi)$ . Hence, we can assume additionally that  $\delta_4 \in [0, 2\pi)$ .

If  $\delta_6 \notin [0, 2\pi)$ , then by Proposition 22, we can ensure that it is in  $[0, 4\pi)$ , and then if it is in  $[2\pi, 4\pi)$ , then:



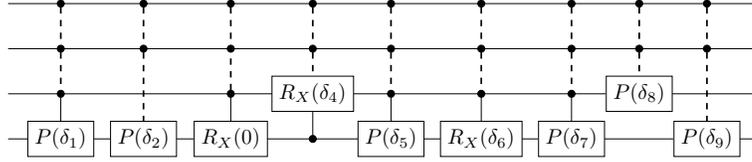
Lemma 54 and Proposition 13



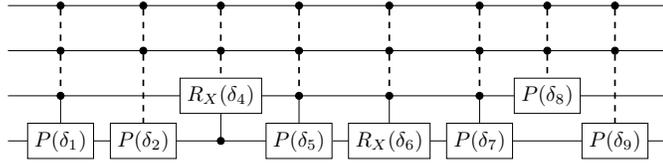
with  $\delta_6 - 2\pi \in [0, 2\pi)$ . Hence, we can assume additionally that  $\delta_6 \in [0, 2\pi)$ .

If  $\delta_3 = 0$  but  $\delta_2 \neq 0$ , then:

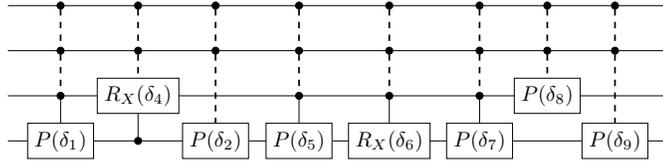
Proposition 13



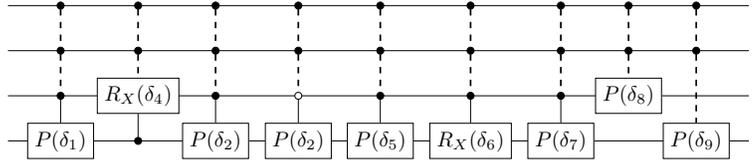
Lemma 48



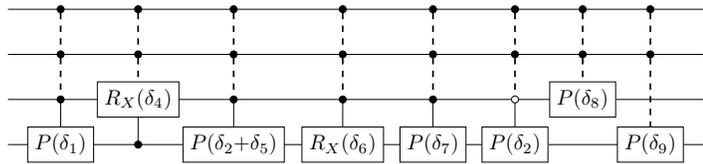
Proposition 15



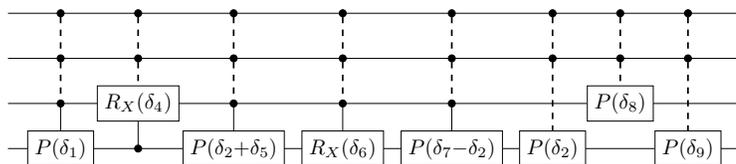
Propositions 16 and 13



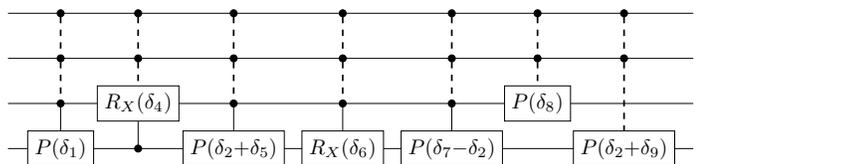
Propositions 13 and 15



Propositions 12, 13, 15 and 16

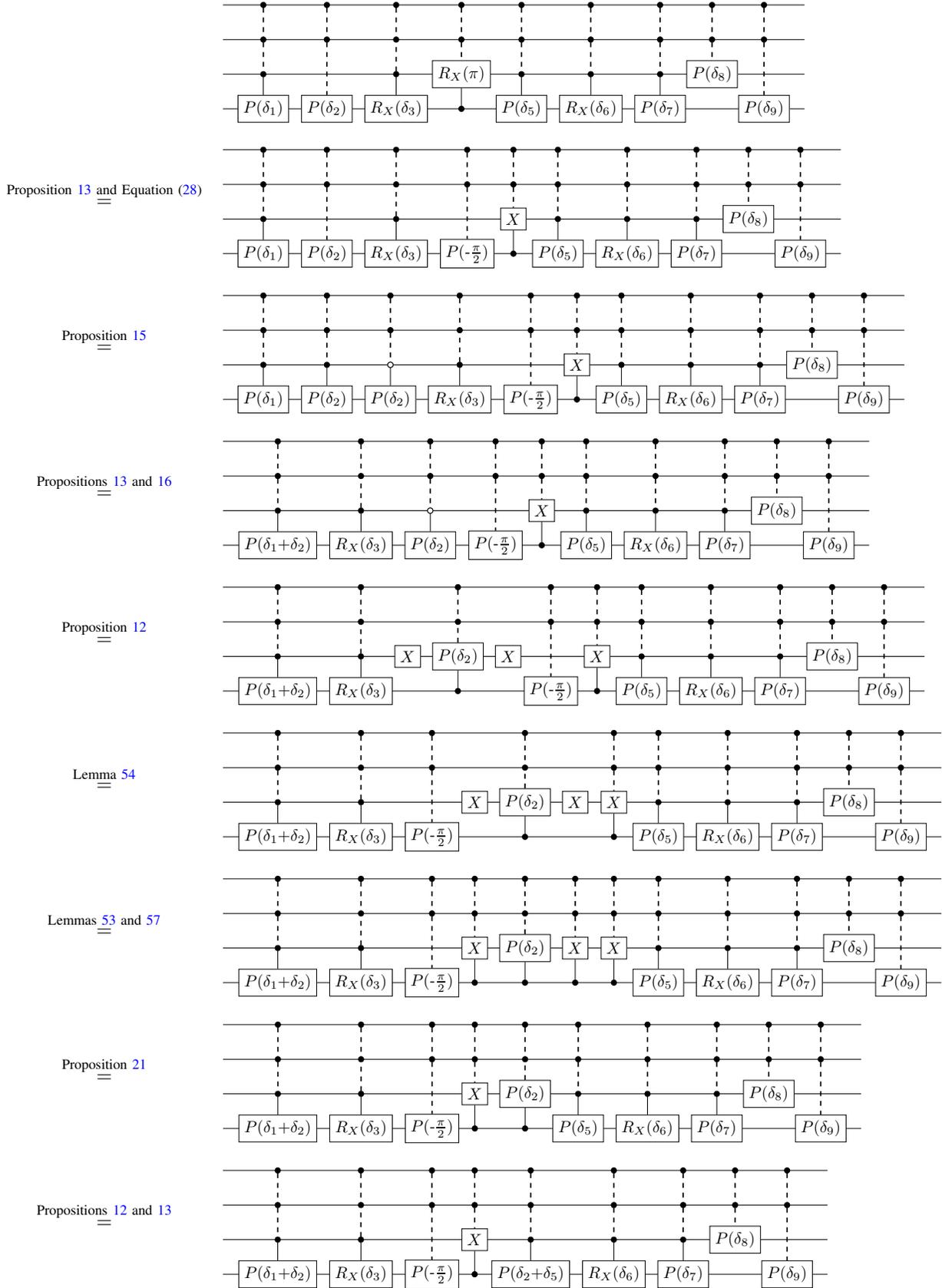


Proposition 13

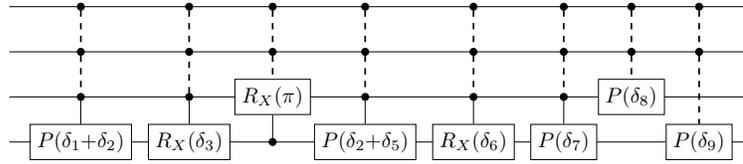


Hence, we can assume additionally that if  $\delta_3 = 0$  then  $\delta_2 = 0$ .

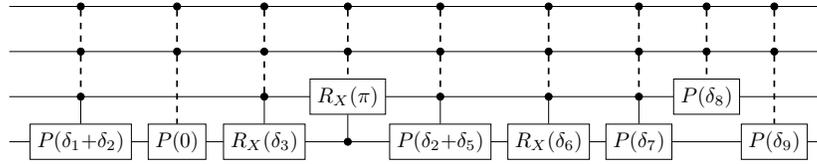
If  $\delta_3 \neq 0$ , and  $\delta_4 = \pi$  but  $\delta_2 \neq 0$ , then:



Equation (28) and Proposition 13

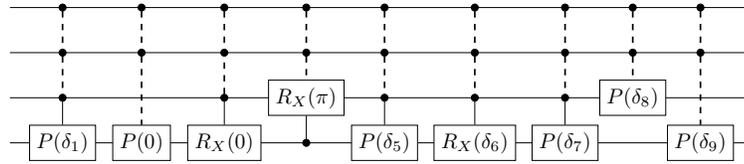


Proposition 13

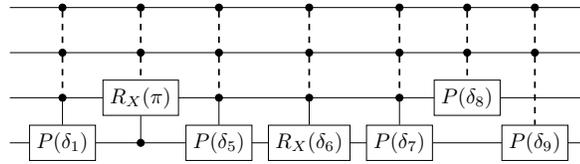


Hence, we can assume additionally that if  $\delta_4 = \pi$  then  $\delta_2 = 0$  (note that by the previous assumption we already had  $\delta_2 = 0$  when  $\delta_3 = 0$ ).

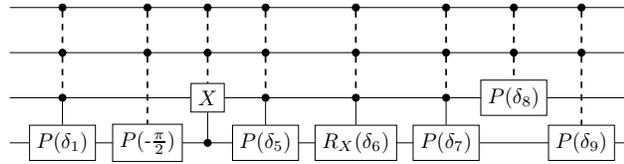
If  $\delta_3 = 0$  and  $\delta_4 = \pi$ , then by assumption,  $\delta_2 = 0$ . If we do not have additionally that  $\delta_1 = 0$ , then:



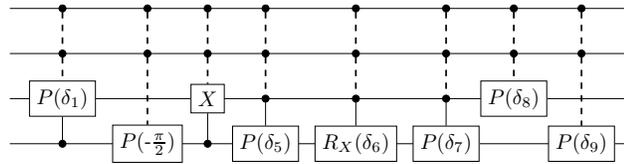
Proposition 13



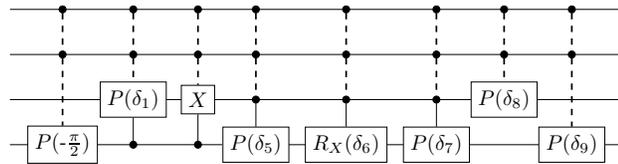
Proposition 13 and Equation (28)



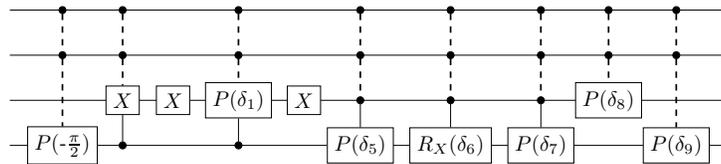
Proposition 12

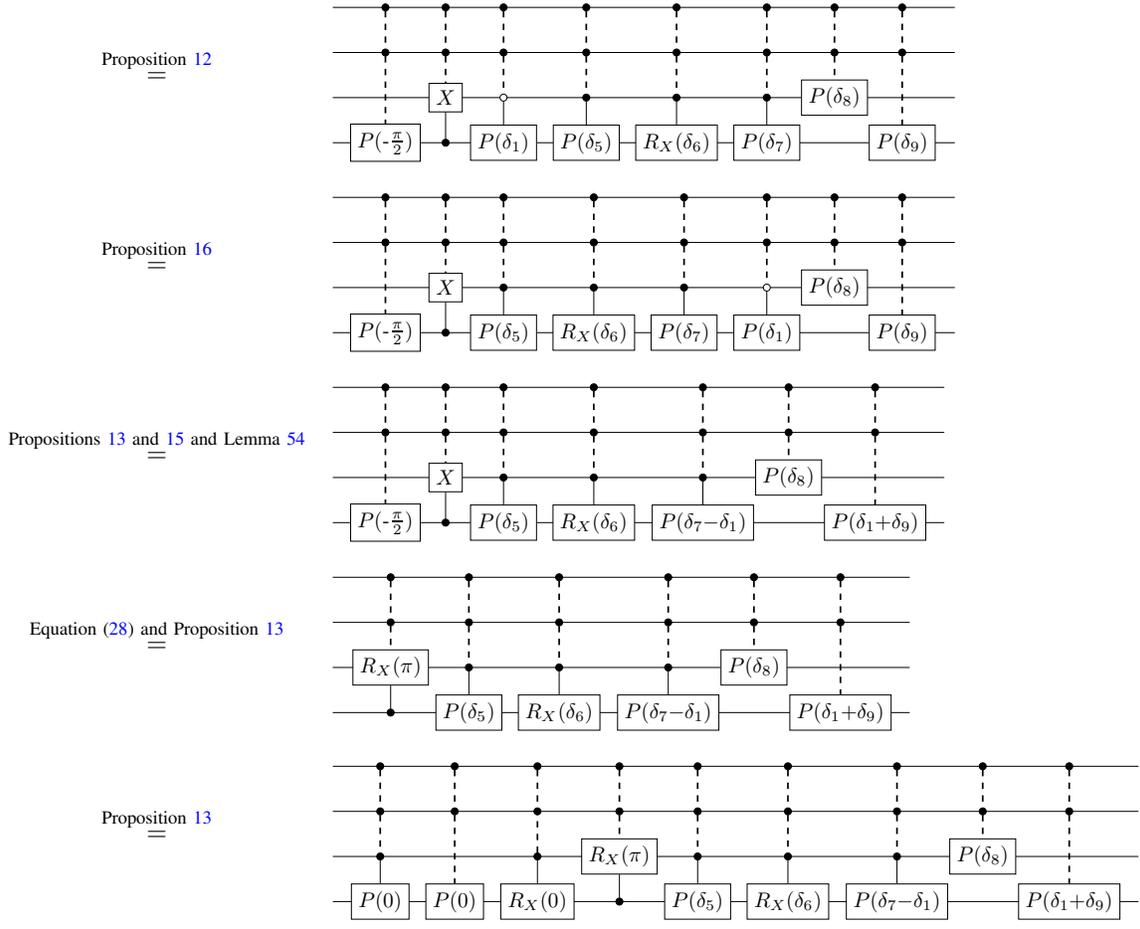


Lemma 54



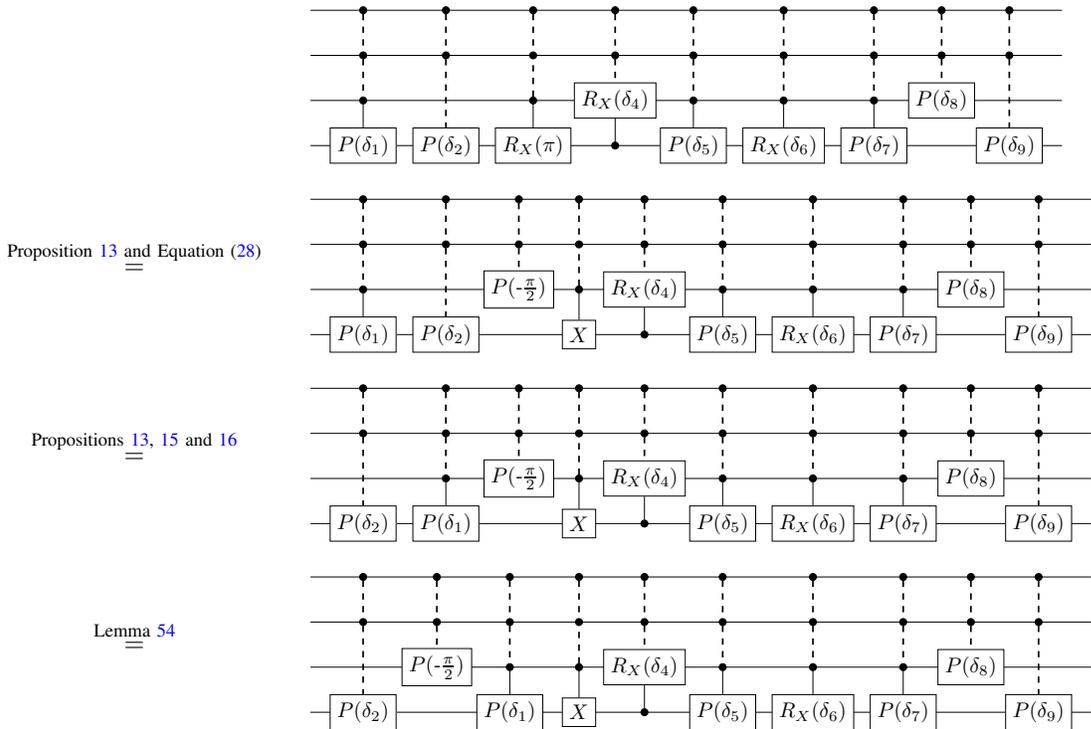
Proposition 21 and Lemmas 57 and 53



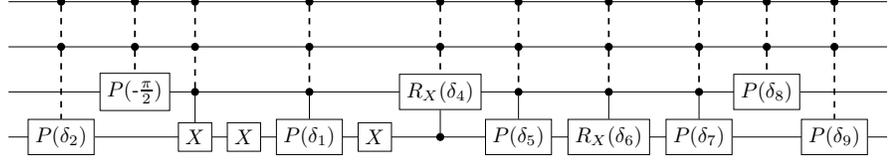


Hence, we can assume additionally that if  $\delta_3 = 0$  and  $\delta_4 = \pi$  then  $\delta_1 = 0$ .

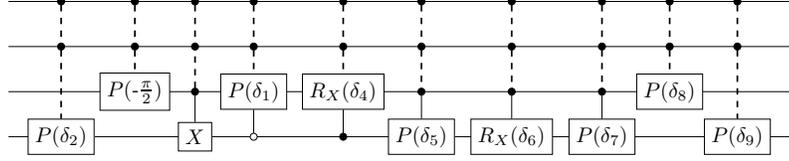
If  $\delta_3 = \pi$  but  $\delta_1 \neq 0$ , then:



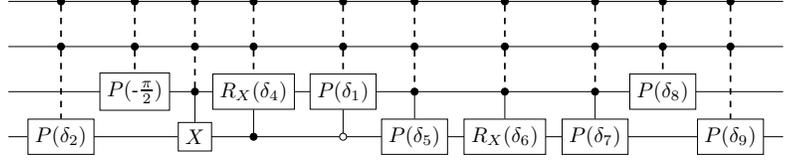
Proposition 21 and Lemmas 57 and 53



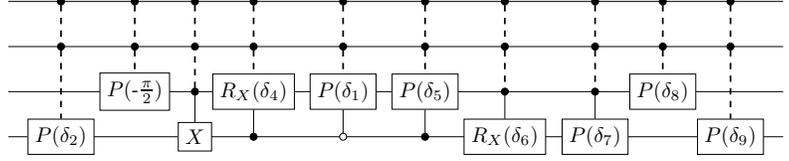
Proposition 12



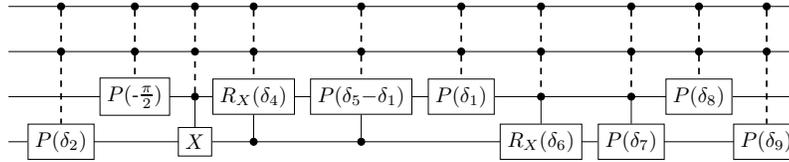
Proposition 16



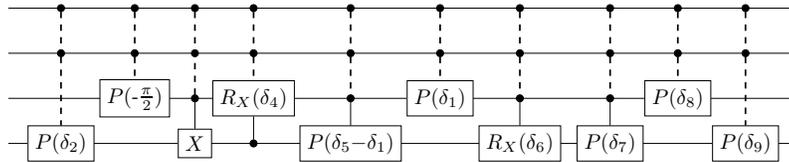
Proposition 12



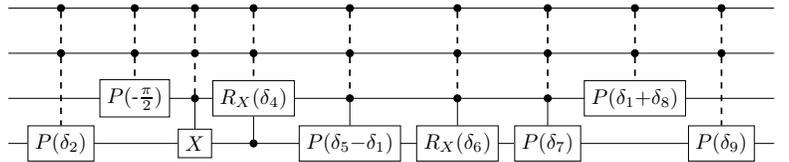
Propositions 13, 15 and 16



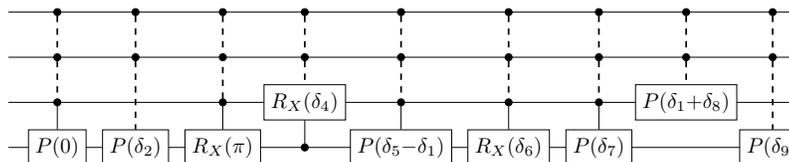
Proposition 12



Lemmas 48 and 54 and Proposition 13

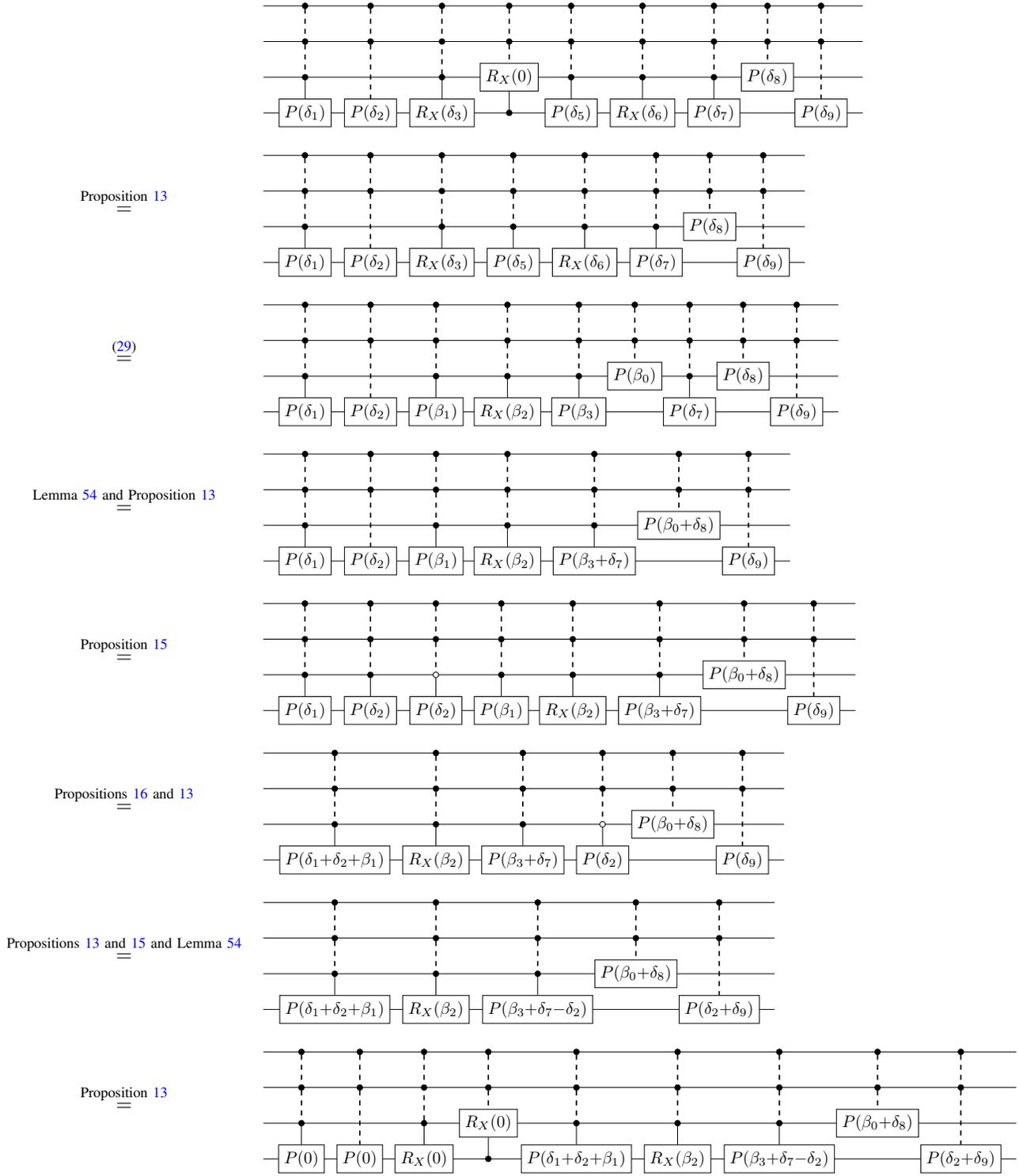


Equation (28) and Proposition 13



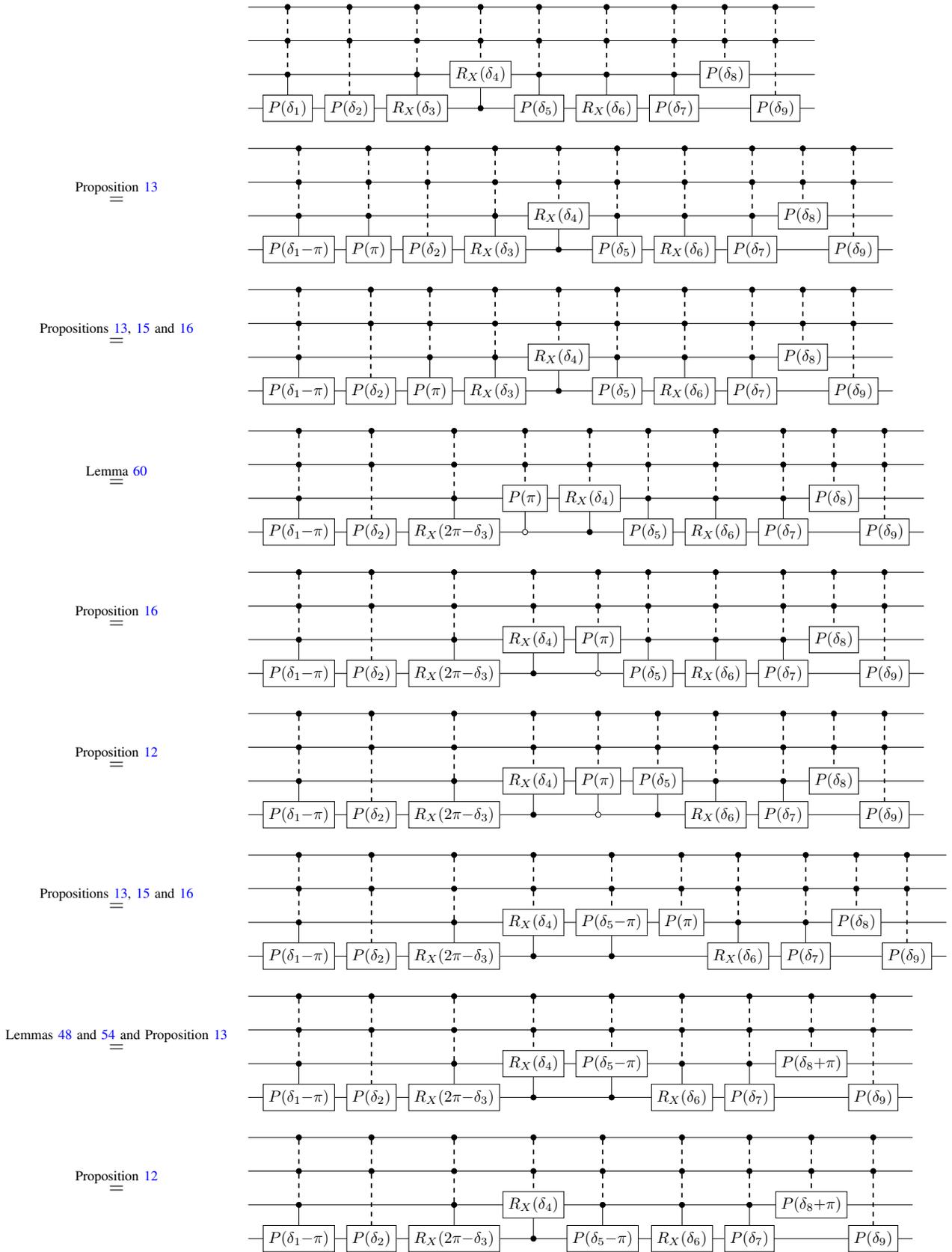
Hence, we can assume additionally that if  $\delta_3 = \pi$  then  $\delta_1 = 0$ .

If  $\delta_4 = 0$  but  $(\delta_1, \delta_2, \delta_3) \neq (0, 0, 0)$ , then:

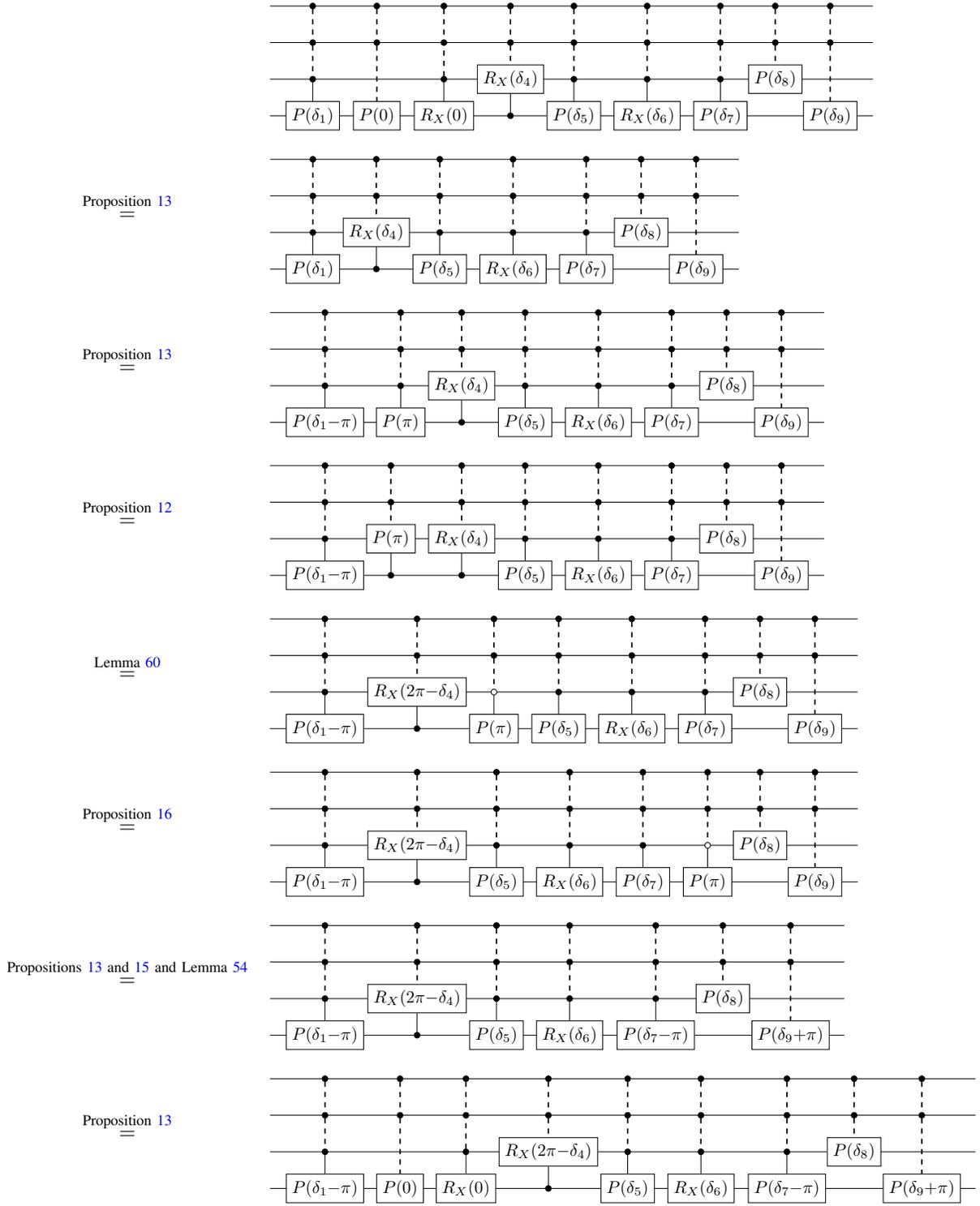


where  $\beta_0, \beta_1, \beta_2$  and  $\beta_3$  satisfy the conditions given in Figure 5. In particular,  $\beta_2 \in [0, 2\pi)$ , so that the previous assumptions are preserved. This implies that we can assume additionally that if  $\delta_4 = 0$  then  $\delta_1 = \delta_2 = \delta_3 = 0$ .

If  $\delta_1 \notin [0, \pi)$ , then by Proposition 22, we can ensure that it is in  $[0, 2\pi)$ , and then if it is in  $[\pi, 2\pi)$ , then, if  $\delta_3 \neq 0$ :

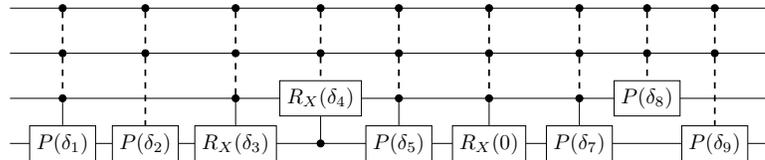


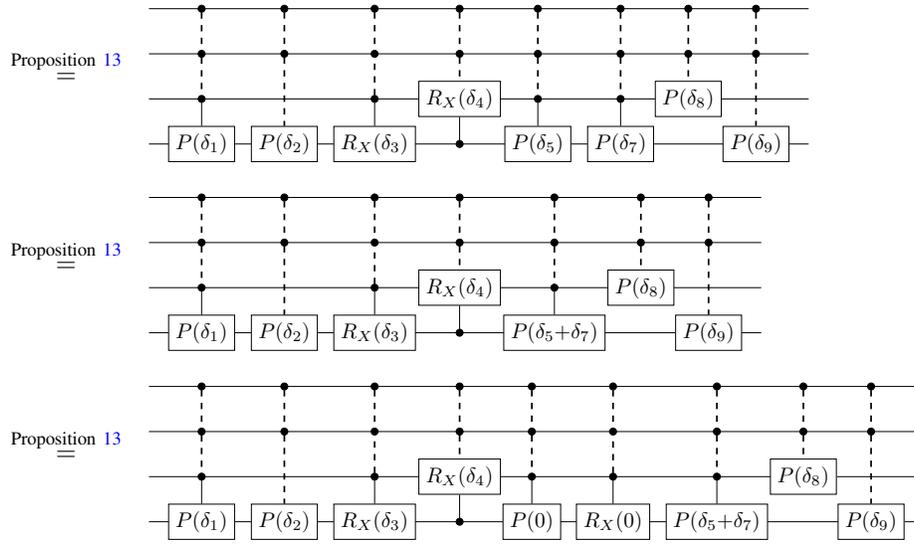
with  $\delta_1 - \pi \in [0, \pi)$ . Moreover, since  $\delta_3 \neq 0$ , one has  $2\pi - \delta_3 \in [0, 2\pi)$ , so that the previous assumptions are preserved. And, still in the case where  $\delta_1 \in [\pi, 2\pi)$ , if  $\delta_3 = 0$ , then by assumption,  $\delta_2 = 0$ , and one has:



with  $\delta_1 - \pi \in [0, \pi)$ .

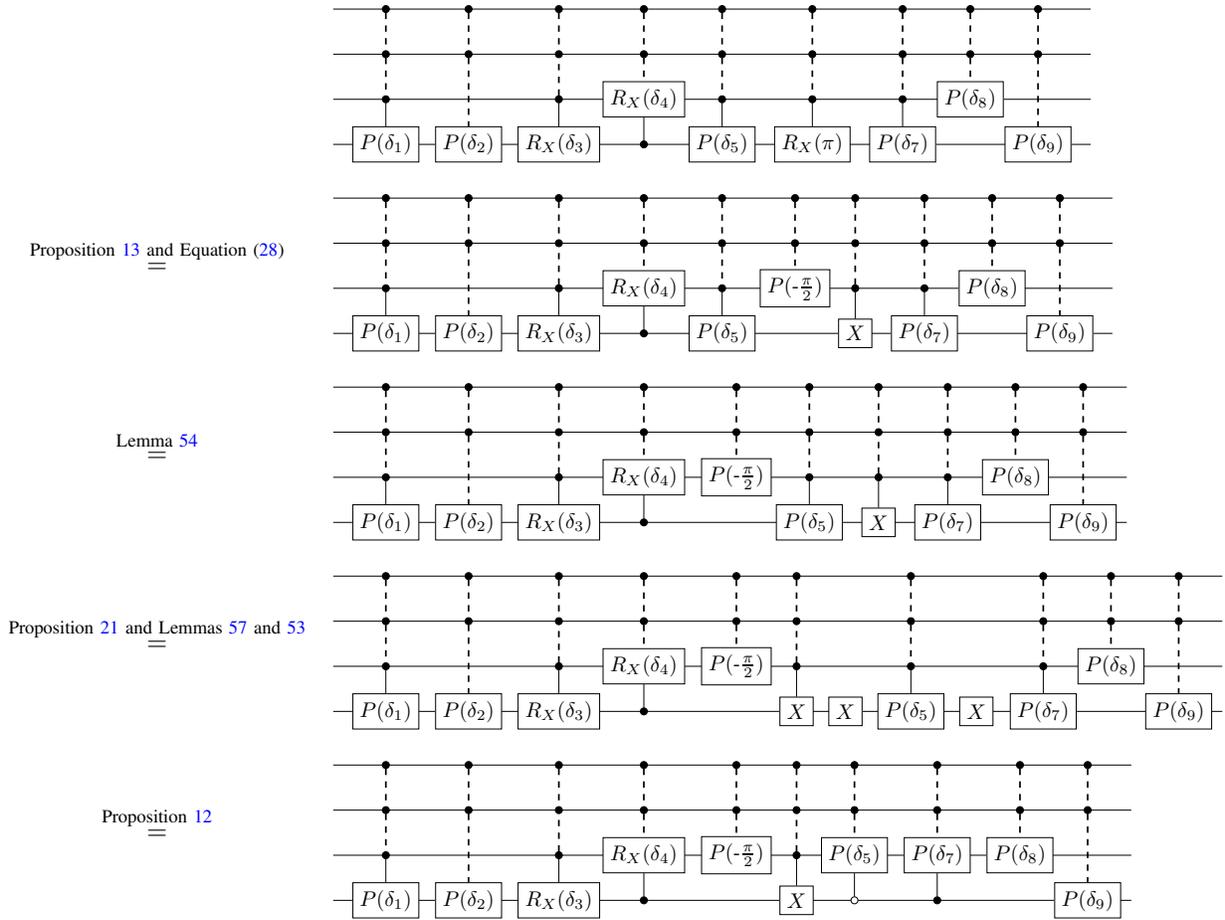
If  $\delta_6 = 0$  but  $\delta_5 \neq 0$ , then:



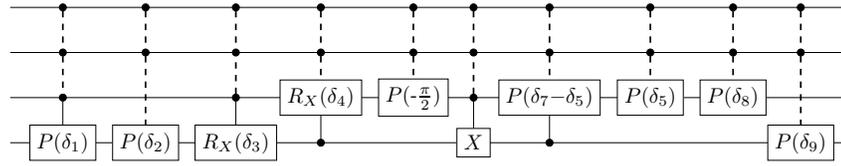


Hence, we can assume additionally that if  $\delta_6 = 0$  then  $\delta_5 = 0$ .

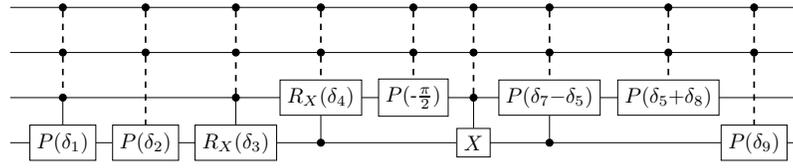
If  $\delta_6 = \pi$  but  $\delta_5 \neq 0$ , then:



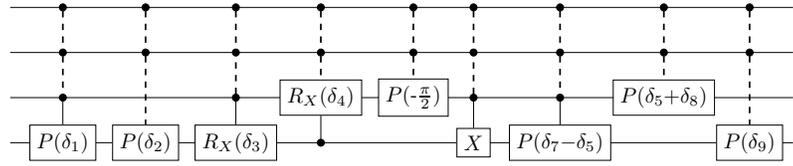
Propositions 16, 13 and 15



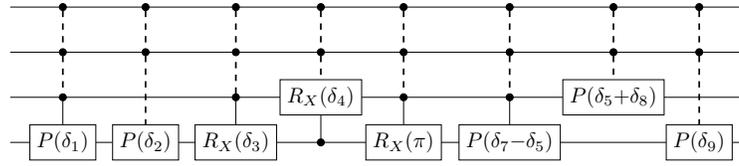
Proposition 13



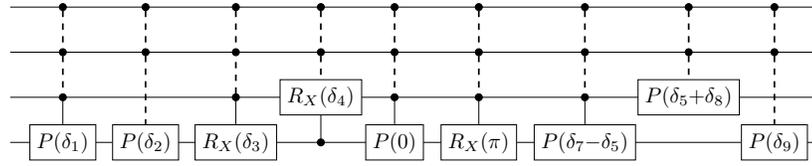
Proposition 12



Equation (28) and Proposition 13

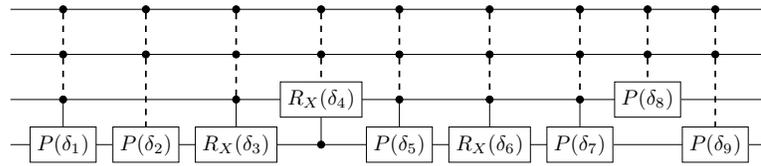


Proposition 13

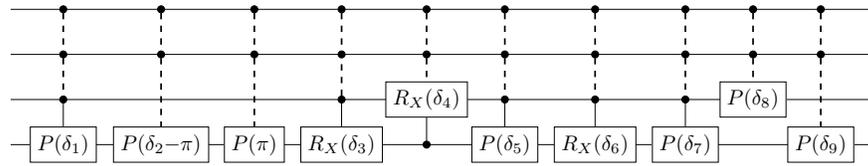


Hence, we can assume additionally that if  $\delta_6 = \pi$  then  $\delta_5 = 0$ .

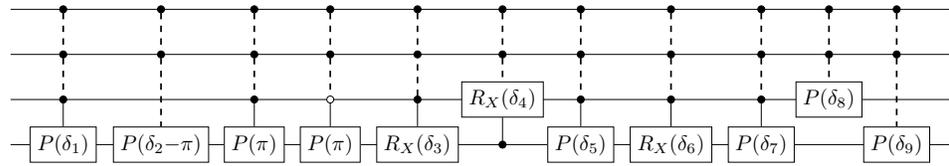
If  $\delta_2 \notin [0, \pi)$ , then by Proposition 22, we can ensure that it is in  $[0, 2\pi)$ , and then if it is in  $[\pi, 2\pi)$ , then:



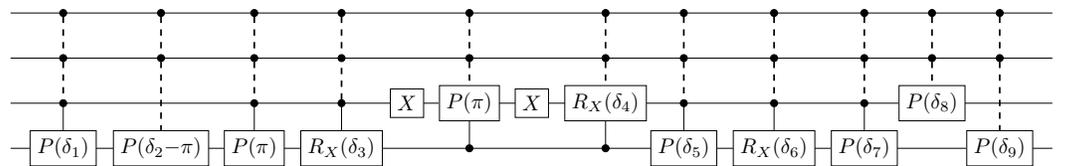
Proposition 13



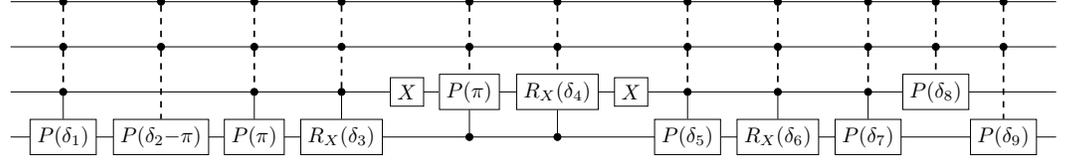
Proposition 15



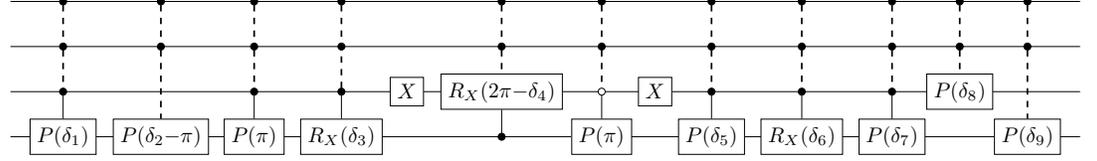
Propositions 16 and 12



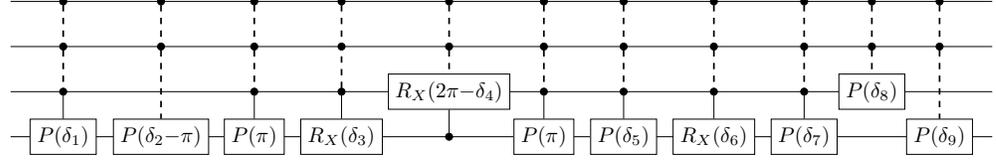
Lemma 52



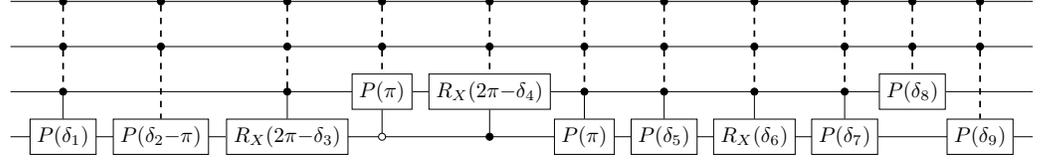
Lemma 60



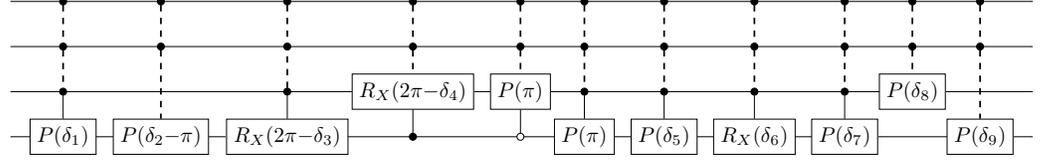
Lemma 52 and Equation (10)



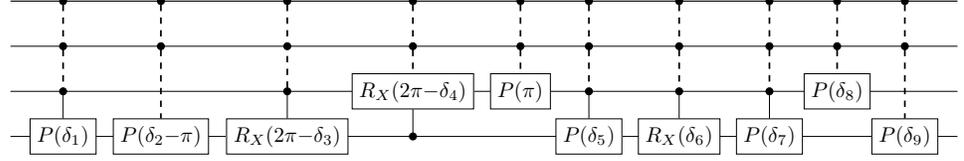
Lemma 60



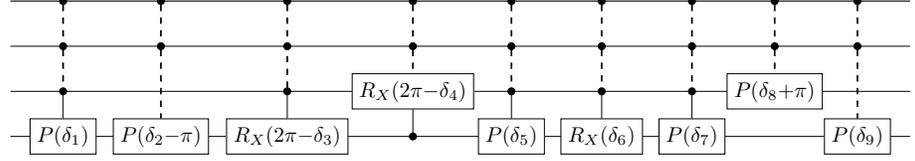
Proposition 16



Propositions 12, 16 and 15

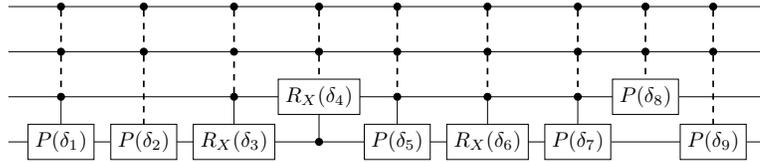


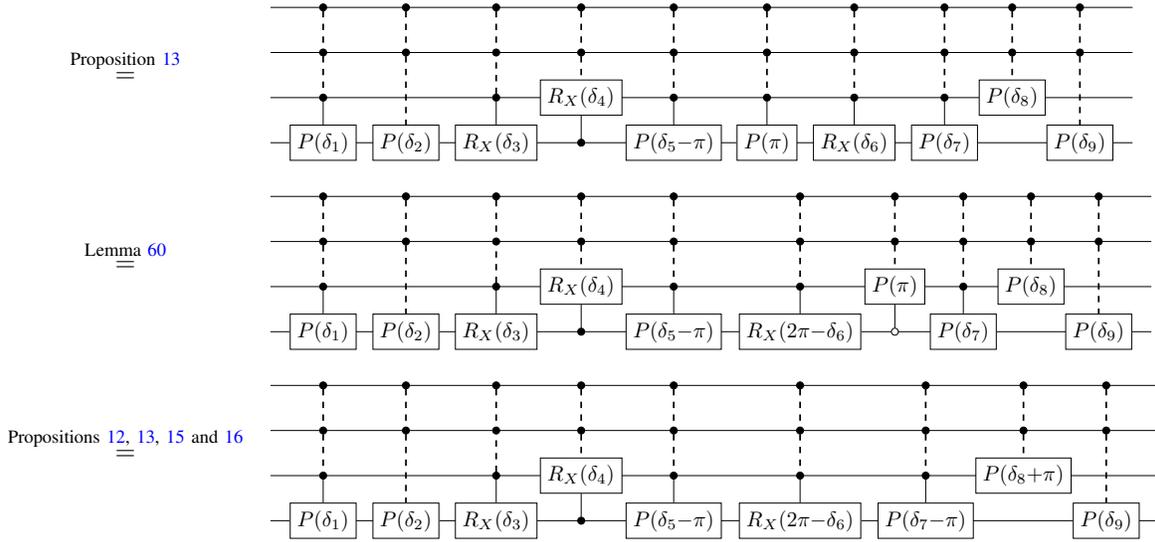
Lemmas 48 and 54 and Proposition 13



with  $\delta_2 - \pi \in [0, \pi)$ . Moreover, since  $\delta_2 \neq 0$ , by assumption  $\delta_3 \neq 0$  and  $\delta_4 \neq 0$ , so that  $2\pi - \delta_3$  and  $2\pi - \delta_4$  are still in  $[0, 2\pi)$  and the previous assumptions are preserved.

If  $\delta_5 \notin [0, \pi)$ , then by Proposition 22, we can ensure that it is in  $[0, 2\pi)$ , and then if it is in  $[\pi, 2\pi)$ , then:





with  $\delta_5 - \pi \in [0, \pi)$ . Moreover, since  $\delta_5 \neq 0$ , by assumption  $\delta_6 \neq 0$ , so that  $2\pi - \delta_6 \in [0, 2\pi)$  and the previous assumptions are preserved.

Finally, by Proposition 22 we can put  $\delta_7$ ,  $\delta_8$  and  $\delta_9$  in  $[0, 2\pi)$  without modifying the other angles.

G. Definition of  $\sigma_{k,n,\ell}$

$\sigma_{k,0,\ell} := (\text{---})^{\otimes 2^{k+\ell}}$  and  $\forall n \geq 2$ ,  $\sigma_{k,n,\ell} := \sigma_{k,1,\ell+n-1}^n$ , with

$$\sigma_{k,1,\ell} = \prod_{j=k+1}^{k+\ell} \mathcal{P}_j \mathcal{Q}_j \mathcal{P}_j$$

where

- given a family of  $N$ -mode circuits  $C_A, \dots, C_B$ ,  $\prod_{i=A}^B C_i := (\dots ((C_B \circ C_{B-1}) \circ C_{B-2}) \circ \dots) \circ C_A$ ,

- $M := k + \ell + 1$

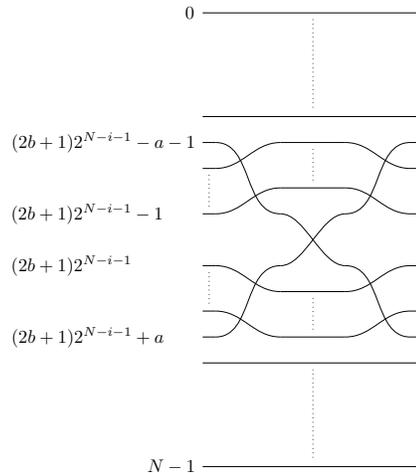
- $\mathcal{P}_j$  is a raw optical circuit such that  $\mathfrak{G}_n \circ [\mathcal{P}_j] \circ \mathfrak{G}_n^{-1} = id_{j-1} \otimes \left[ \begin{array}{c} \oplus \\ \vdots \\ \oplus \end{array} \right] \otimes id_{M-j-1}$ , defined as

$$\mathcal{P}_j := \prod_{\substack{b=0 \\ b \bmod 4 \in \{1,2\}}}^{2^j-1} \prod_{a=0}^{2^{M-j-1}-1} v_{M,j,b,a}$$

- $\mathcal{Q}_j$  is a raw optical circuit such that  $\mathfrak{G}_n \circ [\mathcal{Q}_j] \circ \mathfrak{G}_n^{-1} = id_{j-1} \otimes \left[ \begin{array}{c} \oplus \\ \vdots \\ \oplus \end{array} \right] \otimes id_{M-j-1}$ , defined as

$$\mathcal{Q}_j := \prod_{b=0}^{2^{j-1}-1} \prod_{a=0}^{2^{M-j-3}-1} v_{M,j-1,b,a}$$

- $v_{N,i,b,a}$  is a raw optical circuit such that  $v_{N,i,b,a} \equiv$



. It is defined for any  $N \geq 1$ ,

$i \in \{0, \dots, N-1\}$ ,  $b \in \{0, \dots, 2^i - 1\}$  and  $a \in \{0, \dots, 2^{N-i-1} - 1\}$ , by finite induction on  $a$  by

$$U_{N,i,b,0} := \begin{array}{c} (2b+1)2^{N-i-1}-1 \{ \begin{array}{c} \hline \vdots \\ \hline \end{array} \\ \times \\ 2^N - (2b+1)2^{N-i-1}-1 \{ \begin{array}{c} \hline \vdots \\ \hline \end{array} \end{array}$$

and for  $a \in \{1, \dots, 2^{N-i-1} - 1\}$ ,

$$U_{N,i,b,a} := s_{-a} \circ s_{+a} \circ U_{N,i,b,a-1} \circ s_{+a} \circ s_{-a},$$

where  $s_{+a} := \begin{array}{c} (2b+1)2^{N-i-1}+a-1 \{ \begin{array}{c} \hline \vdots \\ \hline \end{array} \\ \times \\ 2^N - (2b+1)2^{N-i-1}-a-1 \{ \begin{array}{c} \hline \vdots \\ \hline \end{array} \end{array}$  and  $s_{-a} := \begin{array}{c} (2b+1)2^{N-i-1}-a-1 \{ \begin{array}{c} \hline \vdots \\ \hline \end{array} \\ \times \\ 2^N - (2b+1)2^{N-i-1}+a-1 \{ \begin{array}{c} \hline \vdots \\ \hline \end{array} \end{array}$ .