A Complete Equational Theory for Real-Clifford+CH Quantum Circuits

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

Abstract

We introduce a complete equational theory for the fragment of quantum circuits generated by the real Clifford gates plus the two-qubit controlled-Hadamard gate. That is, we give a simple set of equalities between circuits of this fragment, and prove that any other true equation can be derived from these. This is the first such completeness result for a finitely-generated, universal fragment of quantum circuits, with no parameterized gates and no need for ancillas.

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

Keywords and phrases Quantum circuits, completeness, graphical language

Digital Object Identifier 10.4230/LIPIcs.LICS.2026.28

Related Version *Full Version*: `https://arxiv.org/abs/2602.06644` [9]

Funding This work has been partially funded by the French National Research Agency (ANR) within the framework of "Plan France 2030", under the research projects EPIQ ANR-22-PETQ-0007, HQI-Acquisition ANR-22-PNCQ-0001 and HQI-R&D ANR-22-PNCQ-0002.

1 Introduction

Quantum circuits form the basic language which is essentially at the core of quantum computing. The role that they play in practice is sometimes compared to that of an assembly language in classical computing. But formally, they are in fact the quantum equivalent of *boolean circuits*. Like boolean circuits, they consist of a sequence of *gates*, which are applied to some quantum data which is most often in the form of *qubits*, the quantum equivalent of bits.

Quantum computing can *a priori* be realized on a variety of physical platforms with various characteristics, and for now it is essentially impossible to predict what physical implementation will turn out to be the best, neither is it clear whether one technology will completely supplant the others; therefore, various different classes of quantum circuits are *a priori* relevant to formalize and study. Even staying inside the most standard model of quantum computing, where the data is encoded in qubits, several *fragments* of the language of quantum circuits, corresponding to particular sets of elementary gates with which to build the circuits, are relevant to consider. Some of them have received particular attention, such as the well-known Clifford+T and Toffoli-Hadamard fragments. An essential characteristic for a gate set is to be *computationally universal*, that is, to make it possible in principle to implement any arbitrary quantum program, up to arbitrarily small error. One reason that makes Clifford+T and Toffoli-Hadamard interesting is that they are universal while being generated by a very small and simple set of gates – in addition to being possibly relevant for promising implementations such as superconducting circuits.

A central task in quantum computing is to manipulate quantum circuits, and in particular to transform circuits into equivalent ones that are better according to some criterion: this has various practical applications such as optimization, satisfaction of hardware constraints, error correction, or verification. A promising approach towards manipulation of quantum

circuits is via graphical rewriting. In the recent years, several *graphical languages* for formal manipulation of quantum circuits (and of other aspects of quantum processes) have been introduced, such as the ZX-, ZW-, ZH-, and ZXW-calculi, among others [13, 20, 2, 17, 30]. A central question in the formalization of such languages is the completeness of their equational theory, that is, the fact that the set of rewriting rules with which they are equipped be powerful enough so that any semantically meaningful transformation can be done. A related important question is to make the complete equational theory as simple as possible, and if possible, to be finally able to prove that it is minimal in the sense that all redundancies have been simplified out. There are now various complete equational theories for graphical languages [24, 21, 25, 26, 36], some of which being minimal [15] or near-minimal [36, 3, 4, 33, 34, 35].

The language of quantum circuits itself can be viewed as a graphical language, and finding complete equational theories for it has its own added value compared to relying on external auxiliary languages like the ZX-calculus. For instance, applying arbitrary ZX transformations to a quantum circuit can produce a ZX-diagram from which it may be hard to get back a quantum circuit [17, 14]. Although the question of finding a complete equational theory for quantum circuits had been formulated in the early 2000's [23, 27], the first complete equational theory was found only a few years ago [12], followed by simplifications and a proof of minimality [11, 10]. Those results are for the full language of quantum circuits in the qubit setting. That is, the gate set is very simple but still contains a parameterized gate, and the minimal equational theory is relatively simple but involves non-trivial computations on the parameters.

In this paper, we introduce a complete equational theory for a finitely generated fragment of quantum circuits, without parameterized gates, namely the fragment generated by real Clifford gates – the Hadamard gate H, the Pauli Z gate, and the controlled-Z gate CZ – together with the controlled Hadamard gate CH. We call this fragment *Real-Clifford+CH*. This is a sub-fragment of Clifford+T, which contains Toffoli-Hadamard[1] and therefore is universal. To our knowledge, this is the first completeness result for a fragment of quantum circuits generated by a finite gate set, without parameterized gates.

Similarly to [12], our result is based on a back-and-forth translation into an auxiliary language for which a completeness result is known, namely a presentation of the matrix group $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ generated by one- and two-level matrices [18]. Those one- and two-level matrices have a similar structure to the optical circuits used in [12].

Related works. In addition to the graphical languages mentioned, other languages for quantum computing are equipped with complete equational theories [18, 16, 22]. The main difference is that those languages are equipped with a control constructor (or an equivalent construction) allowing one to express arbitrary multi-controlled gates, which means that they are not finitely generated from a quantum circuit point of view.

Structure of the Paper. The paper is organized as follows: In Section 2, we formally introduce Real-Clifford+CH quantum circuits and define some useful macros. In Section 3, we introduce the equational theory that we will prove to be complete. In Section 4, we state the completeness result upon which our result relies [18], and we adapt it so as to be able to lift the completeness to quantum circuits. In Sections 5 and 6, we give some additional insight about the proof of completeness. In Section 7, we prove the completeness of our equational theory for circuits on 1 and 2 qubits. Finally, in Section 8, we prove the completeness in the general case.

[1] Except in the case of 3-qubit circuits without ancillas.

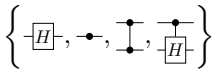
Proof Summary. More into details, the overall logical structure of the proof is as follows.

- We show that for $n \geq 3$, the matrices represented by n-qubits real-Clifford+CH circuits form a subgroup of $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ of index 4 (while for $n = 2$ they span the entire group $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}])$). We give generators for this subgroup, which consist of pairs of one- and two-level matrices **(Section 4.1)**.
- We slightly simplify the complete equational theory of [18] into that of Figure 7, in order to save effort in the following steps **(done in [9])**.
- We apply the Reidemeister-Schreier theorem for monoids introduced in [6], in order to turn the presentation of $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ (given by the generators of [18] together with the simplified complete equational theory) into a presentation of the subgroup, with the generators that we have introduced **(Section 4.2 and Appendix B, details in [9])**.
- We simplify the complete equational theory obtained (shown in [9]), into a more manageable one shown in Figure 8 **(done in [9])**.
- From the equational theory of Figure 4, we prove some auxiliary equations on 1- and 2-qubit real-Clifford+CH circuits **(given in [9], together with their derivations)**.
- We prove that the equational theory of Figure 4 is complete for 1-qubit real-Clifford+CH circuits, by means of a standard technique based on a normal form **(Lemma 20)**.
- We prove that the equational theory of Figure 4 is complete for 2-qubit real-Clifford+CH circuits, by means of a back-and forth translation similar to that of [12], relying on the presentation of $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}])$. The back-and-forth encoding technique yields a few proof obligations (Lemmas 23 and 24), which we handle using the auxiliary equations **(Section 7.2 and [9])**.
- From the equational theory of Figure 4, using in particular an induction argument (Lemma 19), we prove additional auxiliary equations on real-Clifford+CH circuits **(given in [9], together with their derivations)**.
- We prove that the equational theory of Figure 4 is complete for n-qubit real-Clifford+CH circuits, $n \geq 3$, by means of a back-and forth translation similar to that of [12], relying on the presentation of the corresponding subgroup of $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$. Again, the back-and-forth encoding technique yields a few proof obligations (Lemmas 32 and 33), which we handle using the auxiliary equations **(Section 8 and [9])**.

2 Real-Clifford+CH Quantum Circuits

2.1 The PROP of Real-Clifford+CH Quantum Circuits

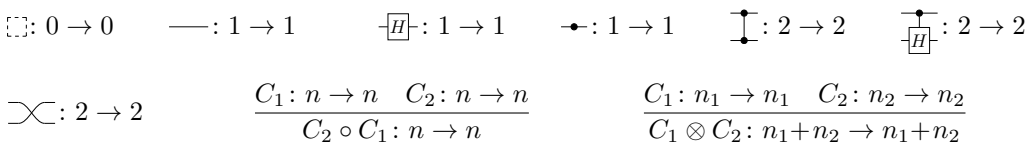
We consider the *real-Clifford+CH* fragment of quantum circuits, without ancillas, generated by the following gate set:



(A)

Following [12, 11, 10], we give a rigorous formalization to Real-Clifford+CH quantum circuits by using the structure of PROP, which originates from category theory [29, 37] but can be viewed purely as an algebraic structure [8]. We start by defining *raw circuits* [12], which are the terms freely built from the generators of (A), the empty circuit ⬚, the one-qubit identity —, and the swap ⨉, by means of the sequential composition $\circ$ and the parallel composition $\otimes$:

▶ **Definition 1.** *The set* $\mathbf{QC_{raw}}$ *of raw Real-Clifford+CH circuits is inductively defined as follows:*



▶ **Definition 2.** *The PROP of Real-Clifford+CH circuits, denoted by* $\mathbf{QC}$*, is obtained by taking the quotient of* $\mathbf{QC_{raw}}$ *by the axioms of PROP, shown in Figure 1.*

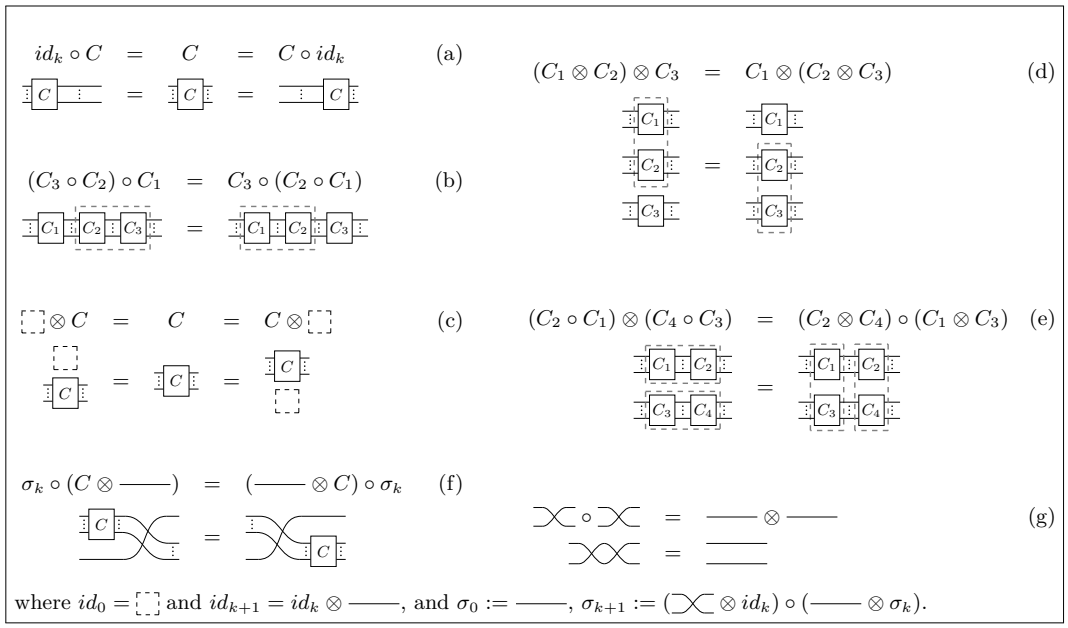
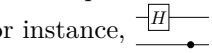


Figure 1 Axioms of PROP.

Roughly speaking, Equations (a)–(e) are the axioms needed to guarantee that two circuits with the same graphical representation are actually equal, and that the length of the wires does not matter (for instance, ). Equations (f) and (g) additionally give us the property that the circuits are defined up to deformation.

▶ Remark 3. The structure obtained by quotienting $\mathbf{QC_{raw}}$ only by Equations (a)–(e) is called a PRO. Depending on the context, it may be more relevant to model quantum circuits as a PRO rather than a PROP (for instance when considering implementations where the swap gate is costly), or vice-versa. Note that our completeness result can be straightforwardly adapted to the PRO setup by simply adding Equations (f) and (g) to the complete equational theory of Figure 4. Moreover, Equation (f) actually does not need to be parameterized by an

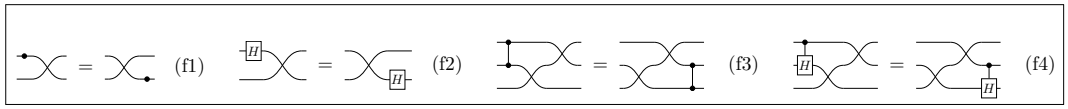


Figure 2 Alternative equations to Equation (f).

arbitrary circuit C: it is sufficient to only assume it for the generators, that is, Equation (f) can be replaced by the equations of Figure 2, since it can be recovered from them in the presence of the other axioms of PROP. Moreover, Equation (g) actually follows from the other equations.[2] Thus, there are only four equations to add to the complete equational theory in order to adapt it to the PRO setting.

▶ Remark 4. The other standard real Clifford gates can be recovered from those of (A) (see Figure 3). Note also that the swap gate can be expressed from the generators of (A) (see Equation (8)).

▶ **Definition 5** (Semantics). *For any n-qubit circuit C, let $[\![C]\!] : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ be the* semantics *of C inductively defined as*

$$[\![C_2 \circ C_1]\!] = [\![C_2]\!] \circ [\![C_1]\!] \qquad [\![\bullet\!-\!\bullet]\!] = |x\rangle \mapsto (-1)^x |x\rangle$$

$$[\![C_1 \otimes C_2]\!] = [\![C_1]\!] \otimes [\![C_2]\!] \qquad [\![-\boxed{H}-]\!] = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$$

$$[\![\,]\!] = 1 \mapsto 1 \qquad [\![\bullet\!-\!\bullet]\!] = |x,y\rangle \mapsto (-1)^{xy} |x,y\rangle$$

$$[\![-\!-]\!] = |x\rangle \mapsto |x\rangle \qquad \left[\!\!\left[\begin{smallmatrix}\bullet\\ \boxed{H}\end{smallmatrix}\right]\!\!\right] = |x,y\rangle \mapsto \begin{cases} |0,y\rangle \mapsto |0,y\rangle \\ |1,y\rangle \mapsto \frac{|1,0\rangle + (-1)^y |1,1\rangle}{\sqrt{2}} \end{cases}$$

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

▶ Remark 6. Strictly speaking, $[\![\cdot]\!]$ is defined on raw circuits. However, one can check that it is preserved by the equations of Figure 1, so that it is well-defined on (non-raw) circuits.

2.2 Shortcuts

We now define several shortcuts that will be useful in the rest of the paper, some of which corresponding to standard gates. Note that from a formal point of view, all circuits drawn throughout the paper are still considered as being composed only of gates from (A), the shortcuts being only a convenient way to represent particular circuits.

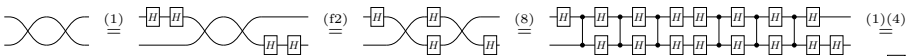
First, we will use CNOTs, as well as standard variants of the gates, which are defined in Figure 3.

Second, it will be particularly useful to consider a change-of-basis matrix which diagonalizes H into Z: we will use the following one:[3]

$$P \coloneqq R_Y(\tfrac{\pi}{4})Z = e^{-i\frac{\pi}{8}} SHTHS = \begin{pmatrix} \cos(\frac{\pi}{8}) & \sin(\frac{\pi}{8}) \\ \sin(\frac{\pi}{8}) & -\cos(\frac{\pi}{8}) \end{pmatrix}.$$

One can check that $P^2 = I$ and $PZP = H$. Note that P *cannot* be represented by a real-Clifford+CH circuit, since it is not in the group $U_n(\mathbb{Z}[\frac{1}{\sqrt{2}}])$. However, one has

$$P \otimes P = \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{2}+1 & 1 & 1 & \sqrt{2}-1 \\ 1 & -\sqrt{2}-1 & \sqrt{2}-1 & -1 \\ 1 & \sqrt{2}-1 & -\sqrt{2}-1 & -1 \\ \sqrt{2}-1 & -1 & -1 & \sqrt{2}+1 \end{pmatrix}$$

[2] Indeed,  .

[3] where H, Z, S, T and R_Y are the matrices corresponding to the standard gates: $H = [\![-\boxed{H}-]\!] = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, $Z = [\![\bullet\!-\!\bullet]\!] = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{smallmatrix}\right)$, and $R_Y(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$.

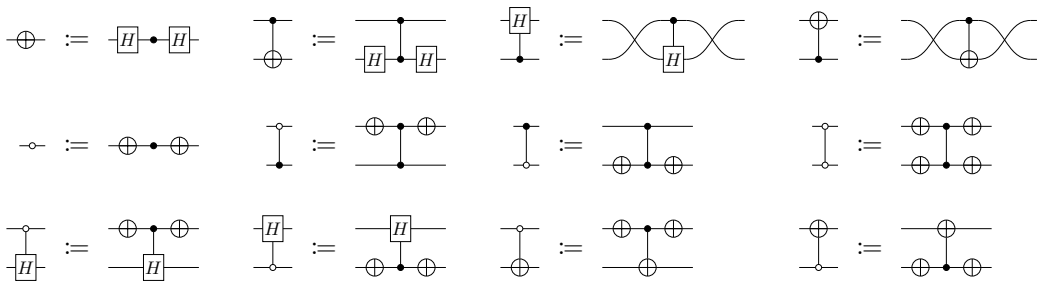
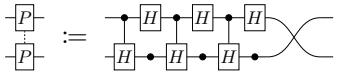
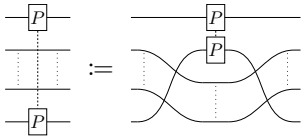


Figure 3 Standard one- and two-qubit gates, defined as shortcuts.

which is in that group, and can be represented by a real-Clifford+CH circuit. We draw this shortcut with a slight dashed line in order to keep track of the fact that it is actually defined using two-qubit gates:



It will also be useful to represent a pair of P gates acting on non-adjacent qubits:



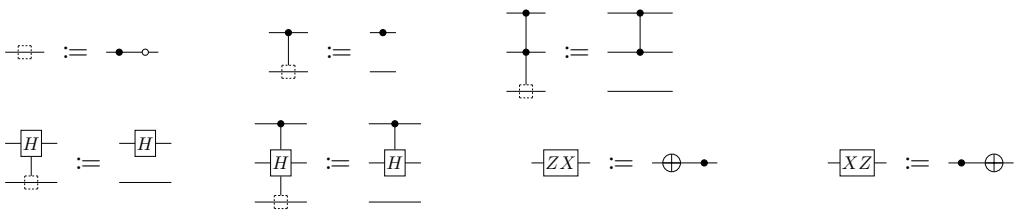
Finally, similarly to [12], another particularly useful class of shortcuts is *multi-controlled gates*.

On the one hand, we will use multi-controlled Z and H gates. Note that for $n \geq 3$, one cannot represent an n-qubit multi-controlled Z or H gate as an n-qubit real-Clifford+CH circuit.[4] However, one can represent an $(n-1)$-qubit multi-controlled Z or H gate tensored with the 1-qubit identity.

On the other hand, we will also use multi-controlled ZX and XZ gates (where ZX and XZ are just the product of the Z and X gates in both order), which do not have such a restriction.

The definition is by mutual induction as follows. Note that we draw multi-controlled Z and H gates using a small dashed box, in order to keep track of the fact that the shortcut actually uses one more qubit than the multi-controlled gate itself.[5]

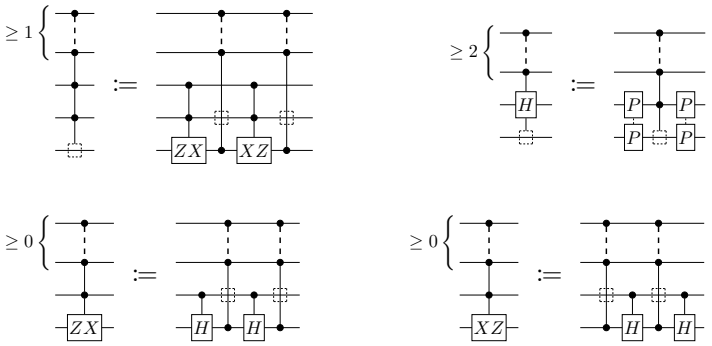
▶ **Definition 7** (Multi-Controlled Z, H, ZX and XZ Gates). *The base cases are as follows:*



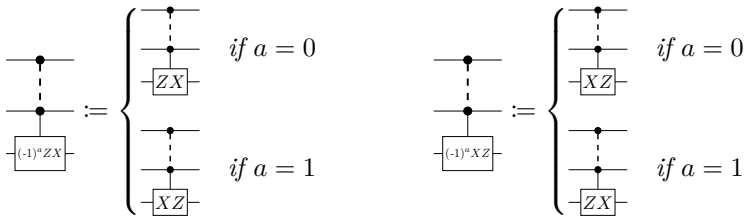
[4] This is due to the fact that it has determinant -1 and that we are only working with real matrices. See also Section 4.

[5] For the multi-controlled Z gate, one can interpret the dashed box as representing a 1-qubit $-I$ gate, and our drawing as representing a multi-controlled $-I$ gate. Similarly, one can see the multi-controlled H tensored by the identity as being a multi-controlled $H \otimes I$ gate.

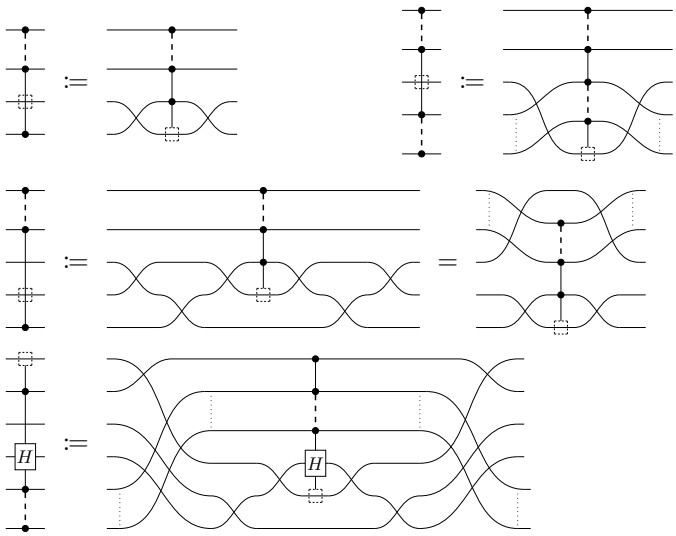
and the recursive steps are as follows:



Note that semantically, $XZ = -ZX$. This motivates the following notations: for $a \in \{0, 1\}$,

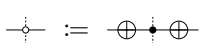


Additionally, it will be useful to consider multi-controlled gates acting on non-adjacent qubits or where the target qubits are not at the end (note that we have already used such notations in the inductive definition above). Similarly to the $P \otimes P$ gate, these are defined by conjugating with swaps. For instance:

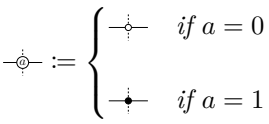


Note that since circuits are defined up to the topological rules, we do not need to specify the exact network of swaps to put on each side of the multi-controllled gate, but only the overall permutation that they realize. The only possible ambiguity could be in the ordering of the controls: by convention, we always take the permutation that preserves the vertical order of the controls.

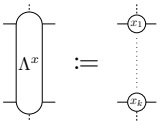
Moreover, we will also consider multi-controlled gates with negative controls (that is, with respect to $|0\rangle$ instead of $|1\rangle$), which we denote using the usual notation of white controls. These are defined by conjugating with the X gate:



Going further, we also define parameterized controls, whose color depends on a boolean parameter:



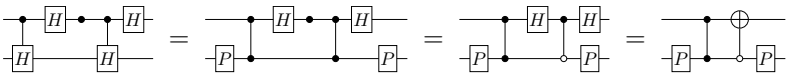
Finally, we denote series of parametrized controls as follows, mimicking the notation used in [12]: for any $x = x_1 ... x_k \in \{0,1\}^k$,



3 Equational Theory

The set QC of equations that we claim to be complete is given in Figure 4. We write $\mathrm{QC} \vdash C_1 = C_2$ when C_1 and C_2 can be transformed into one another by means of these equations.[6]

Equations (1)–(10) and (12)–(15) are relatively standard. Equations (16) and (17) also express a well-known property, namely that a positively-controlled circuit commutes with a negatively-controlled one. Equation (11) essentially also expresses this property, but from the point of view of the eigenbasis of H: reasoning from a purely semantic point of view, one could *informally* write



which makes the commutation clearly appear. Finally, Equation (18) says that the top part of  indeed behaves as a P gate (see Figure 5), and Equation (19) partly witnesses the fact that the shortcut behaves as if it did not touch the bottom qubit.

▶ **Proposition 8** (Soundness). *For any circuits $C_1, C_2 \in \mathbf{QC}$,*

if $\mathrm{QC} \vdash C_1 = C_2$ then $[\![C_1]\!] = [\![C_2]\!]$.

Proof. The semantics is compositional, therefore it suffices to check for each equation that both sides have the same semantics. This can be done by direct computation for Equations (1) to (18), and by a straightforward induction for Equation (19). ◀

4 Auxiliary Language

This paper relies essentially on a result of [18] which gives a presentation (that is, a set of generators together with a complete equational theory) of the group $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ of N-dimensional unitary matrices with entries in $\mathbb{Z}[\frac{1}{\sqrt{2}}]$. Similarly to [12], we will turn that

[6] That is, $\mathrm{QC} \vdash \cdot = \cdot$ is the smallest congruence on circuits which satisfies the equations of Figure 5.

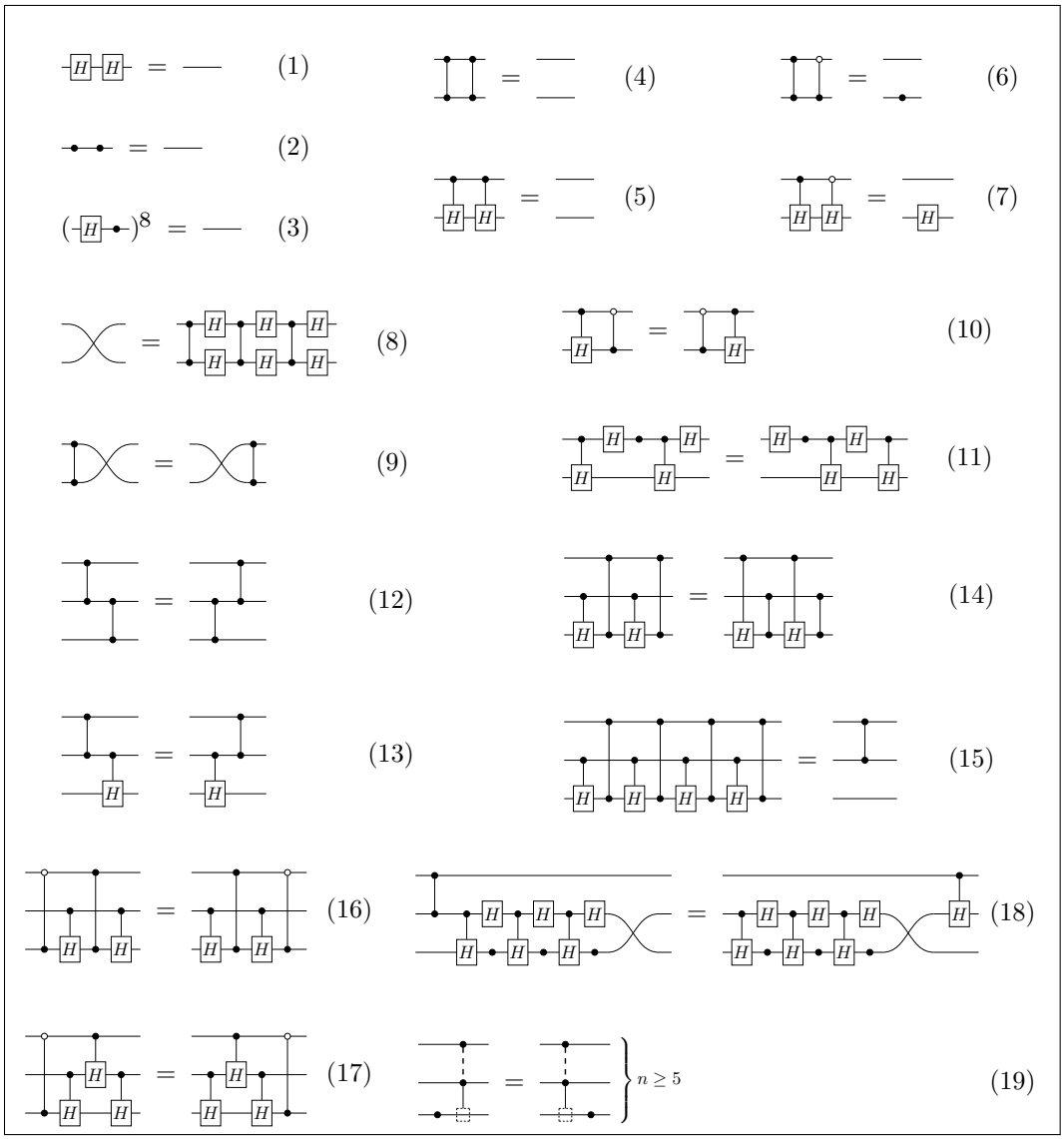


Figure 4 Complete equational theory for real-Clifford+CH quantum circuits. Equation (19) is an equation schema, consisting of an equation on n qubits for each $n \geq 5$. Equations (6), (7), (14)–(17), and (19) use shortcuts, defined in Section 2.2.

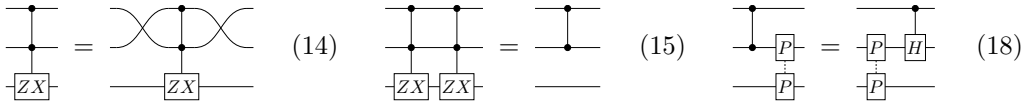


Figure 5 Some equations of Figure 4, written with more shortcuts.

$$(-1)^2_{[a]} \approx \varepsilon \quad \text{(a1)} \qquad H^2_{[a,b]} \approx \varepsilon \quad \text{(a3)}$$

$$X^2_{[a,b]} \approx \varepsilon \quad \text{(a2)}$$

$$(-1)_{[a]}H_{[b,c]} \approx H_{[b,c]}(-1)_{[a]} \quad \text{(b4)}$$

$$X_{[a,b]}H_{[c,d]} \approx H_{[c,d]}X_{[a,b]} \quad \text{(b5)}$$

$$H_{[a,b]}H_{[c,d]} \approx H_{[c,d]}H_{[a,b]} \quad \text{(b6)}$$

$$(-1)_{[a]}(-1)_{[b]} \approx (-1)_{[b]}(-1)_{[a]} \quad \text{(b1)}$$

$$(-1)_{[a]}X_{[b,c]} \approx X_{[b,c]}(-1)_{[a]} \quad \text{(b2)}$$

$$X_{[a,b]}X_{[c,d]} \approx X_{[c,d]}X_{[a,b]} \quad \text{(b3)}$$

$$H_{[b,c]}X_{[a,b]} \approx X_{[a,b]}H_{[a,c]} \quad \text{(c4)}$$

$$H_{[a,c]}X_{[b,c]} \approx X_{[b,c]}H_{[a,b]} \quad \text{(c5)}$$

$$(-1)_{[a]}X_{[a,b]} \approx X_{[a,b]}(-1)_{[b]} \quad \text{(c1)}$$

$$X_{[b,c]}X_{[a,b]} \approx X_{[a,b]}X_{[a,c]} \quad \text{(c2)}$$

$$X_{[a,c]}X_{[b,c]} \approx X_{[b,c]}X_{[a,b]} \quad \text{(c3)}$$

$$(-1)_{[a]}(-1)_{[b]}H_{[a,b]} \approx H_{[a,b]}(-1)_{[a]}(-1)_{[b]} \quad \text{(d1)}$$

$$(-1)_{[b]}H_{[a,b]} \approx H_{[a,b]}X_{[a,b]} \quad \text{(d2)}$$

$$(H_{[c,d]}H_{[a,c]}H_{[b,d]})^4 \approx H_{[a,b]}H_{[c,d]} \quad \text{(d3)}$$

$$(H_{[a,c]}H_{[b,d]}H_{[a,b]}H_{[a,c]}H_{[b,d]}X_{[c,e]}X_{[d,f]})^3 \approx H_{[c,e]}H_{[d,f]}H_{[e,f]}H_{[c,e]}H_{[d,f]}X_{[c,e]}X_{[d,f]} \quad \text{(d4)}$$

$$X_{[c,b]} \approx X_{[b,c]} \quad \text{(e1)} \qquad H_{[c,b]} \approx X_{[b,c]}H_{[b,c]}X_{[b,c]} \quad \text{(e2)}$$

Figure 6 The complete equational theory given in [18]. In each equation, all the indices must be distinct. In Equations (e1) and (e2), we require $b < c$, and in all other equations, the two indices of each H or X must be in increasing order.

complete equational theory into one for quantum circuits by means of a back-and-forth encoding. However, contrary to the situation in [12], the set of matrices represented by real-Clifford+CH circuits is not exactly $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$, but a subgroup of it that we need first to characterize.

4.1 Expressiveness of Real-Clifford+CH Circuits

First, recall the relevant generating set for $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$, made of what are called *1- and 2-level* matrices:

▶ **Definition 9** ([1, 18]). *Let M be an $m \times m$ matrix, let $m < N$, and let $0 \leq a_1, ..., a_m \leq N-1$. An m-level matrix of type M is the $N \times N$ matrix $M_{[a_1,...,a_m]}$ defined by*

$$(M_{[a_1,...,a_m]})_{i,j} = \begin{cases} M_{i',j'} & \text{if } i = a_{i'} \text{ and } j = a_{j'} \\ \delta_{i,j} & \text{otherwise.} \end{cases}$$

▶ **Proposition 10** ([1]). *For $N \geq 1$, a matrix belongs to the group $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ if and only if it can be expressed as a product of generators from*

$$\mathcal{G}_N \coloneqq \left\{ (-1)_{[a]}, X_{[a,b]}, H_{[a,b]} \;\middle|\; a, b \in \{0, ..., N-1\},\ a \neq b \right\}.$$

We can now state the completeness result of [18]:

▶ **Definition 11.** *The free monoid generated by $\mathcal{G}_N$ (i.e. the monoid of words over $\mathcal{G}_N$) is denoted by $\mathcal{G}_N^*$. The empty word is denoted by ϵ. The matrix associated with a word $w = G_1G_2...G_k \in \mathcal{G}_N^*$ is called its* semantics, *and denoted by $[\![w]\!] \coloneqq G_1 \cdot G_2 \cdot ... \cdot G_k$.*

$$(-1)^2_{[0]} \approx \varepsilon \qquad \text{(a1*)}$$

$$X^2_{[a,b]} \approx \varepsilon \qquad \text{(a2)}$$

$$(-1)_{[0]}(-1)_{[1]} \approx (-1)_{[1]}(-1)_{[0]} \qquad \text{(b1*)}$$

$$(-1)_{[a]}X_{[a,b]} \approx X_{[a,b]}(-1)_{[b]} \qquad \text{(c1)}$$

$$H^2_{[a,b]} \approx \varepsilon \qquad \text{(a3)}$$

$$(-1)_{[1]}H_{[0,2]} \approx H_{[0,2]}(-1)_{[1]} \qquad \text{(b4*)}$$

$$H_{[0,1]}H_{[2,3]} \approx H_{[2,3]}H_{[0,1]} \qquad \text{(b6*)}$$

$$H_{[a,c]}X_{[b,c]} \approx X_{[b,c]}H_{[a,b]} \qquad \text{(c5)}$$

$$(-1)_{[b]}H_{[a,b]} \approx H_{[a,b]}X_{[a,b]} \qquad \text{(d2)}$$

$$\begin{aligned} H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]} \;\approx\\ H_{[0,2]}H_{[1,3]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,2]}H_{[1,3]}H_{[0,1]} \end{aligned} \qquad \text{(d3*)}$$

$$\begin{aligned} H_{[0,1]}H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]} \;\approx\\ H_{[0,2]}H_{[1,3]}H_{[0,4]}H_{[1,5]}H_{[0,1]}(-1)_{[0]}(-1)_{[1]}H_{[0,4]}H_{[1,5]}H_{[0,2]}H_{[1,3]}H_{[0,1]} \end{aligned} \qquad \text{(d4*)}$$

$$H_{[c,b]}X_{[b,c]} \approx X_{[b,c]}H_{[b,c]} \qquad \text{(e2*)}$$

Figure 7 Simpler equational theory, equivalent to that of Figure 6. In each equation, all the indices must be distinct but are not required to be in a particular order.

We denote by $\approx$ the smallest congruence satisfying the equations of Figure 6. That is, for any two words $w_1, w_2 \in \mathcal{G}_N^*$, one has $w_1 \approx w_2$ iff w_1 and w_2 can be transformed into one another using the equations of Figure 6.

▶ **Theorem 12** (Soundness and Completeness of $\approx$ for $\mathcal{G}_N^*$ [18]). *Let $w_1, w_2 \in \mathcal{G}_N^*$. Then $[\![w_1]\!] = [\![w_2]\!]$ if and only if $w_1 \approx w_2$.*

Note that contrary to [18], we have not *a priori* required that $a < b$ in $X_{[a,b]}$ or $H_{[a,b]}$, hence the additional conditions in the caption of Figure 6, and the fact that Equations (e1) and (e2) are here considered as axioms, whereas in [18] they were just shortcut definitions.

We can now express the parity conditions needed to characterize the matrix group spanned by real-Clifford+CH circuits:

▶ **Lemma 13.** *Given any $A \in U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$, the parity of the number of generators of the form $H_{[a,b]}$ (resp. of the form $(-1)_{[a]}$ or $X_{[a,b]}$) in an arbitrary decomposition of A as a product of generators from $\mathcal{G}_N$ only depends on A.*

Proof. By Theorem 12, any two decompositions of A as a product of generators from $\mathcal{G}_N$ can be transformed into one another using the equations of Figure 6. One can check that all those equations preserve both the parity of the number of generators of the form $H_{[a,b]}$, and the parity of the number of generators of the form $(-1)_{[a]}$ or $X_{[a,b]}$. ◀

In the following, the parity of the number of $H_{[a,b]}$ in an arbitrary decomposition of A will be called the *H-parity* of A, and the parity of the total number of $(-1)_{[a]}$ and $X_{[a,b]}$ in such a decomposition will be called the *ZX-parity* of A.

▶ **Proposition 14.** *For $N \geq 1$, a matrix belongs to the group $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ and has even ZX- and H-parities if and only if it can be expressed as a product of generators from*

$$\mathcal{P}_N \coloneqq \Big\{ \big((-1)_{[a]}(-1)_{[c]}\big), \big((-1)_{[a]}X_{[c,d]}\big), \big(X_{[a,b]}X_{[c,d]}\big), \big(H_{[a,b]}H_{[c,d]}\big) \\ \Big| \; a,b,c,d \in \{0,...,n-1\},\, a \neq b \wedge c \neq d \Big\}.$$

Proof. The algorithm given in [18] for decomposing a given element of $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ into a product of generators of $\mathcal{P}_N$ can be slightly modified so that its output just consists of a sequence of $H_{[a,b]}$ followed by a sequence of $(-1)_{[a]}$ and $X_{[a,b]}$ (the modified algorithm is described in Appendix A). By Lemma 13, these two sequences are of even length, so we can group the generators by pairs in each. Finally, it remains to get rid of the pairs of the form $\big(X_{[c,d]}(-1)_{[a]}\big)$ by noticing that this is semantically equivalent to $\big((-1)_{[a]}X_{[c,d]}\big)$ if $a \notin \{c,d\}$, to $\big((-1)_{[d]}X_{[c,d]}\big)$ if $a = c$, and to $\big((-1)_{[c]}X_{[c,d]}\big)$ if $a = d$. ◀

▶ **Lemma 15.** *For $n = 2$, the set of matrices that can be represented by an n-qubit real-Clifford+CH circuit is exactly $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$. For $n \geq 3$, it is the subset of $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ consisting of the matrices with even ZX- and H-parities.*

Proof. First, it is clear from the definition of the semantics that any real-Clifford+CH circuit represents an element of $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$.

For $n = 2$, we need to show that any element of $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ can be represented by a real-Clifford+CH circuit. To do so, it suffices to give for every generator of $\mathcal{G}_4$ a circuit with corresponding semantics. This is done in Definition 22.

For $n \geq 3$, similarly, it suffices to express each generator of $\mathcal{P}_{2^n}$ as a real-Clifford+CH circuit. This is done in Definition 28. ◀

4.2 A Complete Equational Theory for $\mathcal{P}_N^*$

Thus, for $n \geq 3$, the matrices represented by n-qubit real-Clifford+CH circuits form a subgroup of $U_{2^n}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ of index 4.

Although we are talking about groups, note that in the following we will essentially only work with the monoid structure. Indeed, this does not fundamentally change the presentations since all inverses are easy to express from the original generators, and makes more sense from a quantum circuit point of view.

There is a standard technique for obtaining a complete equational theory for a subgroup when one is known for the whole group, based on the *Reidemeister-Schreier theorem* [31, 32]. This theorem has been adapted to monoids in [6] and used for obtaining complete equational theories for 2-qubit Clifford+T [6] and 3-qubit Clifford+CS [7] quantum circuits. One drawback of this technique is that it often leads to a combinatorial explosion that makes it computationally costly, even in relatively simple cases. This is the reason that the completeness result of [7] is limited to 3 qubit, whereas the presentation of the underlying matrix group is *a priori* valid in arbitrary dimension.

Rather than trying to obtain a complete equational theory for real-Clifford+CH quantum circuits directly by applying the Reidemeister-Schreier theorem to the equational theory of [18], we adopt an alternative approach in two steps:

- first, we use the Reidemeister-Schreier theorem to obtain a presentation of the submonoid of $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ generated by $\mathcal{P}_N$
- then we use a back-and-forth encoding similar to that of [12] in order to turn this presentation into a complete equational theory for real-Clifford+CH circuits.

Additionally, we perform some simplifications of the equational theories before and after each step. In particular, we start by slightly simplifying the equational theory of [18]; the simplified complete equational theory is shown in Figure 7.

▶ **Proposition 16** (Soundness and Completeness of the Equational Theory of Figure 7 w.r.t. $\approx$)**.** *For any $w_1, w_2 \in \mathcal{G}_N^*$, one has $w_1 \approx w_2$ if and only if w_1 and w_2 can be transformed into one another using the equations of Figure 7. In other words, $\approx$ is the smallest congruence satisfying the relations of Figure 7.*

Proof. One can check that the equations of Figure 7 are semantically sound. Hence, by Theorem 12, they can be derived from those of Figure 6. Conversely, it remains to prove that the equations of Figure 6 can be derived from those of Figure 7. This is done in [9]. ◀

A few details about how we use the Reidemeister-Schreier theorem are given in Appendix B. The full details, including the raw complete equational theory obtained by applying the Reidemeister-Schreier theorem, are given in [9]. Note that the equational theory contains many equations, which are not necessarily well-suited for the next step which is to translate them using the decoding function defined in Section 8; hence, before proceeding to the back-and-forth encoding, we simplify this equational theory into a smaller one, shown in Figure 8. The equational theory of Figure 8 is actually not the simplest possible from the point of view of a human reader (although much simpler than the raw one produced by the Reidemeister-Schreier theorem), but is optimized so as to ease the decoding step.

This gives us the following completeness result:

▶ **Definition 17.** *The free monoid generated by $\mathcal{P}_N$ (i.e. the monoid of words over $\mathcal{P}_N$) is denoted by $\mathcal{P}_N^*$. The empty word is denoted by ϵ. The matrix associated with a word $w = P_1 P_2 ... P_k \in \mathcal{P}_N^*$ is called its* semantics*, and denoted by $[\![w]\!] := P_1 \cdot P_2 \cdot ... \cdot P_k$.*

We denote by $\approx$ the smallest congruence satisfying the equations of Figure 8. That is, for any two words $w_1, w_2 \in \mathcal{P}_N^*$, one has $w_1 \approx w_2$ iff w_1 and w_2 can be transformed into one another using the equations of Figure 8.

▶ **Theorem 18** (Soundness and Completeness of $\approx$ for $\mathcal{P}_N^*$)**.** *Let $w_1, w_2 \in \mathcal{P}_N^*$ with $N \geq 8$. Then $[\![w_1]\!] = [\![w_2]\!]$ if and only if $w_1 \approx w_2$.*

Proof. To prove the soundness, it suffices to check that all the equations of Figure 8 preserve the semantics. The proof of completeness is given in [9]. ◀

5 Auxiliary Equations/Properties of Multi-Controlled Gates

Similarly to [12], the complete equational theory for Real-Clifford+CH circuits that we would obtain naively by the back-and-forth encoding technique described in Sections 7 and 8 consists mainly of equations involving a large (possibly unbounded) number of multi-controlled gates. One of the main contributions of this paper is to derive those equations from the much simpler equational theory shown in Figure 4. To do so, we rely on auxiliary equations, that we derive from those of Figure 4 in [9]. Note that like in [12], a key role is played by basic properties of multi-controlled gates.

Note that in the proof of completeness, we essentially prove the completeness for n-qubit circuits, for each n separately. Therefore, we can instead reason by induction on n (the base cases being given by Lemmas 20 and 25), which does not change the way that the proof of completeness itself is done, but is useful for proving auxiliary equations. This can be reformulated as the fact that we can use the following lemma:

$$((-1)_{[a]}(-1)_{[a]}) \approx \epsilon \tag{20}$$
$$((-1)_{[a]}(-1)_{[b]}) \approx ((-1)_{[b]}(-1)_{[a]}) \tag{21}$$
$$((-1)_{[a]}(-1)_{[b]})\,((-1)_{[b]}(-1)_{[c]}) \approx ((-1)_{[a]}(-1)_{[c]}) \tag{22}$$
$$((-1)_{[a]}(-1)_{[a+1]}) \approx ((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a]}X_{[a,a+1]}) \tag{23}$$
$$((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a+1,a+2]})\,((-1)_{[a]}X_{[a,a+1]}) \approx ((-1)_{[a+1]}X_{[a+1,a+2]})\,((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a+1,a+2]}) \tag{24}$$
$$((-1)_{[a]}X_{[a,c]}) \approx ((-1)_{[a+1]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a+1,c]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a{+}1{<}c,\ \ c{-}a \text{ odd} \tag{25}$$
$$((-1)_{[c]}X_{[a,c]}) \approx ((-1)_{[a+1]}X_{[a,a+1]})\,((-1)_{[c]}X_{[a+1,c]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a{+}1{<}c,\ \ c{-}a \text{ odd} \tag{26}$$
$$((-1)_{[a]}X_{[a,c]}) \approx ((-1)_{[c-1]}X_{[c-1,c]})\,((-1)_{[a]}X_{[a,c-1]})\,((-1)_{[c]}X_{[c-1,c]}) \quad a{+}1{<}c,\ \ c{-}a \text{ even} \tag{27}$$
$$((-1)_{[c]}X_{[a,c]}) \approx ((-1)_{[c-1]}X_{[c-1,c]})\,((-1)_{[c-1]}X_{[a,c-1]})\,((-1)_{[c]}X_{[c-1,c]}) \quad a{+}1{<}c,\ \ c{-}a \text{ even} \tag{28}$$
$$((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a+1]}X_{[a,a+1]}) \approx \epsilon \tag{29}$$
$$((-1)_{[c]}X_{[a,b]}) \approx ((-1)_{[c]}(-1)_{[a]})\,((-1)_{[a]}X_{[a,b]}) \quad c \neq a, b \tag{30}$$
$$((-1)_{[a+1]}(-1)_{[c]})\,((-1)_{[a]}X_{[a,a+1]}) \approx ((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[a]}(-1)_{[c]}) \quad c \neq a, a{+}1 \tag{31}$$
$$((-1)_{[a]}X_{[a,a+1]})\,((-1)_{[b]}X_{[b,b+1]}) \approx ((-1)_{[b]}X_{[b,b+1]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a{+}1 < b \tag{32}$$
$$((-1)_{[b]}X_{[a,b]}) \approx ((-1)_{[b]}X_{[b,a]}) \tag{33}$$
$$(X_{[a,b]}X_{[c,d]}) \approx ((-1)_{[a]}X_{[a,b]})\,((-1)_{[b]}X_{[c,d]}) \tag{34}$$
$$(H_{[a,b]}H_{[c,d]}) \approx \Sigma_{a,b,c,d} \circ (H_{[0,1]}H_{[3,2]}) \circ \Sigma'_{a,b,c,d} \quad \text{see caption} \tag{35}$$
$$(H_{[a,b]}H_{[c,d]}) \approx \mathcal{W}_1 \quad \text{see caption} \tag{36}$$
$$(H_{[a,b]}H_{[c,d]}) \approx \mathcal{W}_2 \quad \text{see caption} \tag{37}$$
$$((-1)_{[a]}X_{[a,a+1]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,((-1)_{[a]}X_{[a,a+1]}) \quad a \geq 4 \tag{38}$$
$$((-1)_{[0]}(-1)_{[1]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,((-1)_{[0]}(-1)_{[1]}) \tag{39}$$
$$((-1)_{[3]}(-1)_{[4]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,((-1)_{[3]}(-1)_{[4]})\,((-1)_{[2]}X_{[2,3]}) \tag{40}$$
$$(H_{[0,1]}H_{[3,2]})\,(H_{[0,1]}H_{[3,2]}) \approx \epsilon \tag{41}$$
$$(H_{[a,b]}H_{[e,f]})\,(H_{[e,f]}H_{[c,d]}) \approx (H_{[a,b]}H_{[c,d]}) \quad \text{see caption} \tag{42}$$
$$(H_{[0,1]}H_{[3,2]})\,(H_{[3,2]}H_{[4,5]}) \approx (X_{[0,3]}X_{[1,2]})\,(H_{[3,2]}H_{[4,5]})\,(X_{[0,3]}X_{[1,2]}) \tag{43}$$
$$(X_{[0,3]}X_{[1,2]})\,(H_{[0,1]}H_{[3,2]}) \approx (H_{[0,1]}H_{[3,2]})\,(X_{[0,3]}X_{[1,2]}) \tag{44}$$

$$\begin{aligned}(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\,((-1)_{[0]}(-1)_{[1]})\,(H_{[0,3]}H_{[1,2]}) \approx \\ (H_{[0,3]}H_{[1,2]})\,((-1)_{[0]}(-1)_{[1]})\,(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\end{aligned} \tag{45}$$

$$\begin{aligned}(H_{[0,1]}H_{[7,6]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[7,6]}H_{[4,5]})\,((-1)_{[2]}(-1)_{[3]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]}) \approx \\ (H_{[0,3]}H_{[1,2]})\,(H_{[3,4]}H_{[2,5]})\,((-1)_{[2]}(-1)_{[3]})\,(H_{[7,6]}H_{[4,5]})\,(H_{[3,2]}H_{[4,5]})\,(H_{[3,4]}H_{[2,5]})\,(H_{[0,3]}H_{[1,2]})\,(H_{[0,1]}H_{[7,6]})\end{aligned} \tag{46}$$

Figure 8 Complete equational theory for $\mathcal{P}^*_N$, valid for $N \geq 8$. In Equation (36), we require that the tuple $(G_n(a), G_n(b), G_n(c), G_n(d))$ be of the form $(x0y0z, x1y0z, x0y1z, x1y1z)$ for some bitstrings x, y, z; in Equation (37), we require that it be of the form $(x0y0z, x0y1z, x1y0z, x1y1z)$; and in Equation (35), we require that it be in neither of these two forms. $\Sigma_{a,b,c,d}$ and $\Sigma'_{a,b,c,d}$ are defined in Definition 28. In Equation (42), we require that $|\{a, b, c, d\}| \leq 3$ and that $e < f$ be the two smallest elements of $\{0, ..., 2^n - 1\} \setminus \{a, b, c, d\}$. The right-hand sides of Equations (36) and (37) are words specifically tailored to behave well with respect to decoding (cf. how those equations are treated in the proof of Lemma 33 given in [9]); they are defined in Appendix C.

▶ **Lemma 19** (Induction Hypothesis for the Proof of Completeness). *For any real-Clifford+CH circuits C_1, C_2, if $[\![C_1]\!] = [\![C_2]\!]$ then* $\mathrm{QC} \vdash (—— \otimes C_1) = (—— \otimes C_2)$ *and* $\mathrm{QC} \vdash (C_1 \otimes ——) = (C_2 \otimes ——)$.

6 The Category of Sequentialized Circuits

As we have said, the proof of completeness is based on a back-and-forth translation, similar to that of [12], between the PROP of real-Clifford+CH circuits and the monoids $\mathcal{G}_N^*$ and $\mathcal{P}_N^*$. However, real-Clifford+CH circuits have a richer structure: they form not only a monoid (for every particular number of qubits) – which corresponds to Equations (a) and (b) of Figure 1 – but they also satisfy the other coherence relations of a PROP. Hence, we cannot directly encode circuits into words since those relations would not be preserved and therefore the encoding would be ill-defined. Instead, we use what we call *sequentialized circuits*, that is, elements of the category $\mathbf{QC_{seq}}$ of raw circuits quotiented only by Equations (a) and (b).

The PROP $\mathbf{QC}$ of usual real-Clifford+CH circuits is recovered by quotienting by the remaining topological rules, namely Equations (c)–(g).[7] Given a sequentialized circuit $C \in \mathbf{QC_{seq}}$, we denote by $|C|$ its image by the canonical projection onto $\mathbf{QC}$. Conversely, any circuit $C \in \mathbf{QC}$ has several representants C' in $\mathbf{QC_{seq}}$, satisfying $|C'| = C$.

We are now ready to prove the main result of the paper. We proceed as follows: first, we prove the completeness for 1-qubit circuits, which is easy to do by using a normal form, in Section 7.1; then we prove the completeness for 2-qubit circuits by means of a back-and-forth encoding into $\mathcal{G}_4^*$, in Section 7.2. Finally, we prove the completeness for circuits on $n \geq 3$ qubits by means of a back-and-forth encoding into $\mathcal{P}_{2^n}^*$, in Section 8. Note that while the encoding function needs to be defined on sequentialized circuits, the decoding function can be defined directly into the PROP $\mathbf{QC}$.

7 One- and Two-Qubit Completeness

7.1 One-Qubit Completeness

▶ **Lemma 20** (1-Qubit Completeness). *For any 1-qubit quantum circuits C_1, C_2 over $\{-\boxed{H}-, -\bullet-\}$, if $[\![C_1]\!] = [\![C_2]\!]$ then* $\mathrm{QC} \vdash C_1 = C_2$.

Proof. We say that a 1-qubit circuit is in *normal form* if it is of the form

$(-\boxed{H}-\bullet-)^k$ or $-\boxed{H}- \circ (-\boxed{H}-\bullet-)^k$

where $k \in \{0, ..., 7\}$.

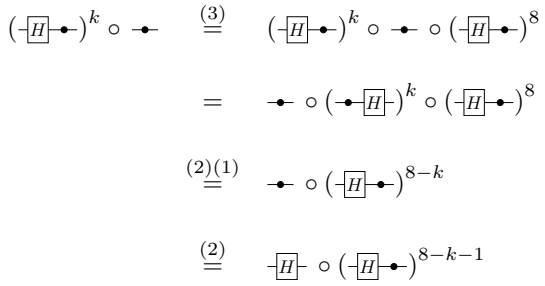
One can check by direct computation that if two circuits in normal form have the same semantics then they are equal. Thus, it remains to prove that any 1-qubit circuit can be put in normal form.

Note that a 1-qubit circuit is just a sequence of $-\boxed{H}-$ and $-\bullet-$ gates. By repeatedly applying Equations (1) and (2), we can ensure that it does not contain two consecutive identical gates. That is, it alternates between $-\boxed{H}-$ and $-\bullet-$, or in other words, it is of one of the following three forms:

$(-\boxed{H}-\bullet-)^k$ $-\boxed{H}- \circ (-\boxed{H}-\bullet-)^k$ $(-\boxed{H}-\bullet-)^k \circ -\bullet-$

[7] More precisely, by quotienting by the variants of Equations (c)–(g) obtained by projecting the two sides of each equation according to the canonical projection $\mathbf{QC_{raw}} \to \mathbf{QC_{raw}}/\{(a), (b)\}$.

By applying Equation (3) $\lfloor \frac{k}{8} \rfloor$ times, we can ensure that $k \in \{0, ..., 7\}$. Thus, if the circuit is in one of the first two forms, then it is in normal form. If it is of the third form, then we do the following transformations:



which gives us a circuit in normal form. ◀

7.2 Two-Qubit Completeness

▶ **Definition 21** (2-Qubit Encoding). *Let $E : \mathbf{QC}^{(2)}_{\mathbf{seq}} \to \mathcal{G}_4^*$ be defined as follows: for any 2-qubit sequentialized circuit C, let $E(C) = E_{0,0}(C)$, where $E_{k,\ell}$ is defined on any m-qubit sequentialized circuit satisfying $k + m + \ell = 2$, inductively as follows:*

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

and for the generators:

- $E_{k,\ell}($  $) = \epsilon$,
- $E_{k,\ell}($  $) = \epsilon$,
- $E_{0,0}($  $) = X_{[1,2]}$,
- $E_{1,0}($$) = (-1)_{[1]}(-1)_{[3]}$,
- $E_{0,1}($  $) = (-1)_{[2]}(-1)_{[3]}$,
- $E_{0,0}($$) = (-1)_{[3]}$,
- $E_{1,0}($$) = H_{[0,1]}H_{[2,3]}$,
- $E_{0,1}($$) = H_{[0,2]}H_{[1,3]}$,
- $E_{0,0}($  $) = H_{[2,3]}$.

▶ **Definition 22** (2-Qubit Decoding). *Let $D\colon \mathcal{G}_4^* \to \mathbf{QC}^{(2)}$ be the monoid homomorphism defined as follows on the generators:*

- $D((-1)_{[0]}) =$  ,
- $D((-1)_{[1]}) =$  ,
- $D((-1)_{[2]}) =$  ,
- $D((-1)_{[3]}) =$  ,
- $D(X_{[2,3]}) = D(X_{[3,2]}) =$  ,
- $D(X_{[0,1]}) = D(X_{[1,0]}) =$  ,
- $D(X_{[0,2]}) = D(X_{[2,0]}) =$  ,
- $D(X_{[1,3]}) = D(X_{[3,1]}) =$  ,
- $D(X_{[1,2]}) = D(X_{[2,1]}) =$,
- $D(X_{[0,3]}) = D(X_{[3,0]}) =$,

- $D(H_{[2,3]}) =$  ,
- $D(H_{[3,2]}) =$  ,
- $D(H_{[0,1]}) =$  ,
- $D(H_{[1,0]}) =$  ,
- $D(H_{[0,2]}) =$  ,
- $D(H_{[2,0]}) =$  ,
- $D(H_{[1,3]}) =$  ,
- $D(H_{[3,1]}) =$  ,
- $D(H_{[2,1]}) =$,
- $D(H_{[1,2]}) =$,
- $D(H_{[0,3]}) =$  ,
- $D(H_{[3,0]}) =$  .

▶ **Lemma 23.** *For any 2-qubit circuit C, and any sequentialized circuit C' such that $|C'| = C$,*

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

Proof. The proof is done by structural induction in [9]. ◀

▶ **Lemma 24.** *For any words $w_1, w_2 \in \mathcal{G}_4^*$,*

$$\text{if } \; w_1 \approx w_2 \; \text{ then } \; \mathrm{QC} \vdash D(w_1) = D(w_2).$$

Proof. By Proposition 16, it suffices to prove that for each rule of Figure 7, of the form $w_1 \approx w_2$ where $w_1, w_2 \in \mathcal{G}_4^*$, and for any two words $w_0, w_3 \in \mathcal{G}_4^*$, one has $\mathrm{QC} \vdash D(w_0 w_1 w_3) = D(w_0 w_2 w_3)$. Since D is a monoid homomorphism, it suffices to prove that $\mathrm{QC} \vdash D(w_1) = D(w_2)$. This is done in [9]. Note that since we are only working in dimension 4, we do not need to treat Equation (d4*). ◀

▶ **Lemma 25** (2-Qubit Completeness). *For any 2-qubit real-Clifford+CH quantum circuits C_1, C_2,*

$$\text{if } [\![C_1]\!] = [\![C_2]\!] \text{ then } \mathrm{QC} \vdash C_1 = C_2.$$

Proof. Let C_1', C_2' be representatives in $\mathbf{QC}_{\mathbf{seq}}^{(2)}$ of respectively C_1 and C_2, so that $|C_1'| = C_1$ and $|C_2'| = C_2$. Since $[\![C_1]\!] = [\![C_2]\!]$ and the encoding preserves the semantics, one has $[\![E(C_1')]\!] = [\![E(C_1')]\!]$. Hence, by Theorem 12, we have $E(C_1') \approx E(C_2')$. By Lemma 24, this implies that $\mathrm{QC} \vdash D(E(C_1')) = D(E(C_2'))$. In turn, by Lemma 23, this implies that $\mathrm{QC} \vdash C_1 = C_2$. ◀

8 Completeness in the General Case

To define the back-and-forth encoding between n-qubits circuits and the elements of $\mathcal{P}_{2^n}$ which represent 2^n-dimensional matrices, it will be handful, like in [12], to encode the integers $0, ..., 2^n - 1$ as n-length bitstrings, by using not the usual binary encoding but rather the *Gray code*, which has the advantage that the encodings of two consecutive integers always differ by exactly one bit:

▶ **Definition 26** (Gray Code [12]). *The n-bit Gray code of an integer $k \in \{0, ..., 2^n - 1\}$ is the word $G_n(k) \in \{0,1\}^n$, inductively defined by $G_0(0) = \epsilon$ and*

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

One can easily check that $G_n \colon \{0, ..., 2^n - 1\} \to \{0,1\}^n$ is a bijection.

▶ **Definition 27** (Encoding). *For any $n \geq 3$, let $E : \mathbf{QC}_{\mathbf{seq}} \to \mathcal{P}_{2^n}^*$ be defined as follows: for any n-qubit sequentialized circuit C, let $E(C) = E_{0,0}(C)$, where $E_{k,\ell}$ is defined on any m-qubit sequentialized circuit satisfying $k + m + \ell = n$, inductively as follows (where the order of the products is left unspecified since it does not matter in the proof):*

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

- $E_{k,\ell}(\text{——}) = \epsilon$;

if $\ell \geq 1$, *then*

- $E_{k,\ell}(\text{-•-}) = \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell-1}}} \Big((-1)_{[G_n^{-1}(x10y)]}(-1)_{[G_n^{-1}(x11y)]}\Big)$;
- $E_{k,\ell}(\text{-•-}\atop\text{-•-}) = \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell-1}}} \Big((-1)_{[G_n^{-1}(x110y)]}(-1)_{[G_n^{-1}(x111y)]}\Big)$;
- $E_{k,\ell}(\text{-}\boxed{H}\text{-}) = \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell-1}}} \Big(H_{[G_n^{-1}(x00y),G_n^{-1}(x10y)]}H_{[G_n^{-1}(x01y),G_n^{-1}(x11y)]}\Big)$;
- $E_{k,\ell}(\text{-•-}\atop\text{-}\boxed{H}\text{-}) = \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell-1}}} \Big(H_{[G_n^{-1}(x100y),G_n^{-1}(x110y)]}H_{[G_n^{-1}(x101y),G_n^{-1}(x111y)]}\Big)$;

and if $\ell = 0$ *(note that because of the condition* $k+m+\ell = n$*, we necessarily have* $k \geq 1$ *in this case), then*

- $E_{k,0}(\text{-•-}) = \prod_{x\in\{0,1\}^{k-1}} \Big((-1)_{[G_n^{-1}(0x1)]}(-1)_{[G_n^{-1}(1x1)]}\Big)$;
- $E_{k,0}(\text{-•-}\atop\text{-•-}) = \prod_{x\in\{0,1\}^{k-1}} \Big((-1)_{[G_n^{-1}(0x11)]}(-1)_{[G_n^{-1}(1x11)]}\Big)$;
- $E_{k,0}(\text{-}\boxed{H}\text{-}) = \prod_{x\in\{0,1\}^{k-1}} \Big(H_{[G_n^{-1}(0x0),G_n^{-1}(0x1)]}H_{[G_n^{-1}(1x0),G_n^{-1}(1x1)]}\Big)$;
- $E_{k,0}(\text{-•-}\atop\text{-}\boxed{H}\text{-}) = \prod_{x\in\{0,1\}^{k-1}} \Big(H_{[G_n^{-1}(0x10),G_n^{-1}(0x11)]}H_{[G_n^{-1}(1x10),G_n^{-1}(1x11)]}\Big)$;

finally, for any $\ell \geq 0$,

- $E_{k,\ell}(\text{-X-}\atop\text{-X-}) = E_{k,\ell}(\text{-•-}\atop\text{-•-}) \circ \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell}}} \Big((-1)_{[G_n^{-1}(x11y)]}X_{[G_n^{-1}(x10y),G_n^{-1}(x11y)]}\Big) \circ$

$$\prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell}}} \Big((-1)_{[G_n^{-1}(x01y)]}X_{[G_n^{-1}(x01y),G_n^{-1}(x11y)]}\Big) \circ \prod_{\substack{x\in\{0,1\}^k \\ y\in\{0,1\}^{\ell}}} \Big((-1)_{[G_n^{-1}(x11y)]}X_{[G_n^{-1}(x10y),G_n^{-1}(x11y)]}\Big).$$

▶ **Definition 28** (Decoding). *For any* $n \geq 3$, *let* $D\colon \mathcal{P}_{2^n}^* \to \mathbf{QC}$ *be the monoid homomorphism defined as follows on the generators:*

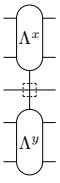
Case of $((-1)_{[a]}(-1)_{[b]})$

- *For any* $a \in \{0, ..., 2^n - 1\}$, *we define*

$$D((-1)_{[a]}(-1)_{[a]}) \coloneqq (\text{——})^{\otimes n}.$$

- *For any* $a \in \{0, ..., 2^n - 2\}$, *we define*

$$D\left((-1)_{[a]}(-1)_{[a+1]}\right) \coloneqq$$



where $\beta \in \{0,1\}$, $x \in \{0,1\}^k$, *and* $y \in \{0,1\}^{n-k-1}$ *are such that* $G_n(a) = x\beta y$ *and* $G_n(a+1) = x\bar{\beta}y$.[8]

- *If* $a \leq b$, *then we define*[9]

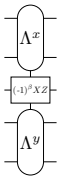
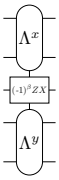
$$D\left((-1)_{[a]}(-1)_{[b]}\right) \coloneqq \prod_{k=a}^{\overleftarrow{b-1}} D\left((-1)_{[k]}(-1)_{[k+1]}\right)$$

where we use the notations $\prod_{k=n}^{\overleftarrow{m}} C_k \coloneqq C_m \circ \cdots \circ C_n$ *and* $\prod_{k=n}^{\overrightarrow{m}} C_k \coloneqq C_n \circ \cdots \circ C_m$, *with by convention the products being the identity if they are empty (i.e. if* $m < n$*).*

- *Finally, if* $a > b$, *we define* $D\left((-1)_{[a]}(-1)_{[b]}\right) \coloneqq D\left((-1)_{[b]}(-1)_{[a]}\right)$.

Case of $\left((-1)_{[c]}X_{[a,b]}\right)$

- *For any* $a \in \{0, ..., 2^n - 2\}$, *we define*

$D\left((-1)_{[a]}X_{[a,a+1]}\right) \coloneqq$  , $D\left((-1)_{[a+1]}X_{[a,a+1]}\right) \coloneqq$ 

where $\beta \in \{0,1\}$, $x \in \{0,1\}^k$, *and* $y \in \{0,1\}^{n-k-1}$ *are such that* $G_n(a) = x\beta y$ *and* $G_n(a+1) = x\bar{\beta}y$.

- *If* $a < b$, *then we define inductively on* $b - a$ *(using the previous case as base case):*
  - *if* $b - a$ *is odd,* $D\left((-1)_{[a]}X_{[a,b]}\right) \coloneqq$

$$D\left((-1)_{[a+1]}X_{[a,a+1]}\right) \circ D\left((-1)_{[a+1]}X_{[a+1,b]}\right) \circ D\left((-1)_{[a]}X_{[a,a+1]}\right)$$

and $D\left((-1)_{[b]}X_{[a,b]}\right) \coloneqq$

$$D\left((-1)_{[a+1]}X_{[a,a+1]}\right) \circ D\left((-1)_{[b]}X_{[a+1,b]}\right) \circ D\left((-1)_{[a]}X_{[a,a+1]}\right);$$

  - *if* $b - a$ *is even,* $D\left((-1)_{[a]}X_{[a,b]}\right) \coloneqq$

$$D\left((-1)_{[b-1]}X_{[b-1,b]}\right) \circ D\left((-1)_{[a]}X_{[a,b-1]}\right) \circ D\left((-1)_{[b]}X_{[b-1,b]}\right)$$

and $D\left((-1)_{[b]}X_{[a,b]}\right) \coloneqq$

$$D\left((-1)_{[b-1]}X_{[b-1,b]}\right) \circ D\left((-1)_{[b-1]}X_{[a,b-1]}\right) \circ D\left((-1)_{[b]}X_{[b-1,b]}\right).$$

- *If* $a > b$, *then we define*

$$D\left((-1)_{[a]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[a]}X_{[b,a]}\right),$$

$$D\left((-1)_{[b]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[b]}X_{[b,a]}\right).$$

- *Finally, if* $c \neq a, b$, *then we define*[10]

$$D\left((-1)_{[c]}X_{[a,b]}\right) \coloneqq D\left((-1)_{[c]}(-1)_{[a]}\right) \circ D\left((-1)_{[a]}X_{[a,b]}\right).$$

---

[8] β, x, y necessarily exist by the properties of the Gray code.

[9] Note that the definition is consistent in the cases where $b = a$ and $b = a + 1$.

[10] Note that since $D\left((-1)_{[a]}(-1)_{[a]}\right)$ is defined as the identity, the equality is still true if $a = c$ or $a = d$.

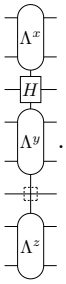
Case of $\left(\boldsymbol{X}_{[a,b]}\boldsymbol{X}_{[c,d]}\right)$

For any a, b, c, d with $a \neq b$ and $c \neq d$, we define

$$D\left(X_{[a,b]}X_{[c,d]}\right) \coloneqq D\left((-1)_{[a]}X_{[a,b]}\right) \circ D\left((-1)_{[b]}X_{[c,d]}\right).$$

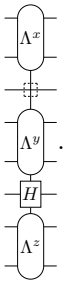
Case of $\left(\boldsymbol{H}_{[a,b]}\boldsymbol{H}_{[c,d]}\right)$

- *If there exist x, y, z such that $G_n(a) = x0y0z$, $G_n(b) = x1y0z$, $G_n(c) = x0y1z$, and $G_n(d) = x1y1z$, then we define*

$D\left(H_{[a,b]}H_{[c,d]}\right) \coloneqq$ 

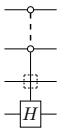
.

- *If there exist x, y, z such that $G_n(a) = x0y0z$, $G_n(b) = x0y1z$, $G_n(c) = x1y0z$, and $G_n(d) = x1y1z$, then we define*

$D\left(H_{[a,b]}H_{[c,d]}\right) \coloneqq$ 

.

- *In the other cases where $|\{a, b, c, d\}| = 4$, we define:*

$D\left(H_{[a,b]}H_{[c,d]}\right) \coloneqq D(\Sigma_{a,b,c,d}) \circ$  $\circ\, D(\Sigma'_{a,b,c,d})$

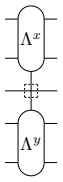
where $\Sigma_{a,b,c,d}$ and $\Sigma'_{a,b,c,d}$ are words over $\mathcal{P}_N$, not containing any generators of the form $\left(H_{[e,f]}H_{[g,h]}\right)$, such that $\left[\!\left[\Sigma'_{a,b,c,d}\right]\!\right] = \left[\!\left[\Sigma_{a,b,c,d}\right]\!\right]^{-1}$, and either $\left[\!\left[\Sigma_{a,b,c,d}\right]\!\right] = \sigma$ or $\left[\!\left[\Sigma_{a,b,c,d}\right]\!\right] = \sigma \circ \left[\!\left[(-1)_{[\mu]}\right]\!\right]$, where $\mu \notin \{0, 1, 3, 2\}$ and σ is a permutation matrix mapping respectively $|0\rangle, |1\rangle, |3\rangle, |2\rangle$ to $|a\rangle, |b\rangle, |c\rangle, |d\rangle$.

Note that the precise definitions of $\Sigma_{a,b,c,d}$ and $\Sigma'_{a,b,c,d}$ do not matter in the proof. Nonetheless, an example of possible definitions is given in [9].

- *Finally, if $|\{a, b, c, d\}| < 4$, then we define $D\left(H_{[a,b]}H_{[c,d]}\right) \coloneqq D\left(H_{[a,b]}H_{[e,f]}\right) \circ D\left(H_{[e,f]}H_{[c,d]}\right)$, where e, f with $e < f$ are the two smallest elements of $\{0, ..., 2^n - 1\} \setminus \{a, b, c, d\}$.*

▶ **Lemma 29.** *For any bitstrings $x \in \{0,1\}^k$ and $y \in \{0,1\}^\ell$ with $k, \ell \geq 0$ and $k + \ell = n - 1$,*

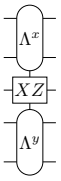
$$\mathrm{QC} \vdash D\left((-1)_{[G_n^{-1}(x0y)]}(-1)_{[G_n^{-1}(x1y)]}\right) =$$



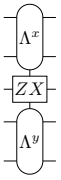
Proof. The proof is given in [9]. ◀

▶ **Lemma 30.** *For any bitstrings $x \in \{0,1\}^k$ and $y \in \{0,1\}^\ell$ with $k, \ell \geq 0$ and $k + \ell = n - 1$,*

$$\mathrm{QC} \vdash D\left((-1)_{[G_n^{-1}(x0y)]}X_{[G_n^{-1}(x0y),G_n^{-1}(x1y)]}\right) =$$



$$\mathrm{QC} \vdash D\left((-1)_{[G_n^{-1}(x1y)]}X_{[G_n^{-1}(x0y),G_n^{-1}(x1y)]}\right) =$$



Proof. The proof is given in [9]. ◀

▶ **Lemma 31.** *For any n-qubit circuit $C \in \mathbf{QC}$, any $C' \in \mathbf{QC_{seq}}$ such that $|C'| = C$, and any k, ℓ such that $k + n + \ell \geq 3$,*

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

Proof. The proof is by structural induction, and the base cases rely on elementary properties of multi-controlled gates. The details are given in [9]. ◀

▶ **Lemma 32.** *For any n-qubit circuit $C \in \mathbf{QC}$ with $n \geq 3$, and any $C' \in \mathbf{QC_{seq}}$ such that $|C'| = C$,*

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

Proof. This follows directly from Lemma 31. ◀

▶ **Lemma 33.** *For any $w_1, w_2 \in \mathcal{P}_{2^n}^*$ with $n \geq 3$,*

$$\text{if } \; w_1 \approx w_2 \; \text{ then } \; \mathrm{QC} \vdash D(w_1) = D(w_2).$$

Proof. It suffices to prove that for each rule of Figure 8, of the form $w_1 = w_2$ where $w_1, w_2 \in \mathcal{G}_{2^n}^*$, and for any two words $w_0, w_3 \in \mathcal{G}_{2^n}^*$, one has $\mathrm{QC} \vdash D(w_0 w_1 w_3) = D(w_0 w_2 w_3)$. Since D is a monoid homomorphism, it suffices to prove that $\mathrm{QC} \vdash D(w_1) = D(w_2)$. This is done in [9]. ◀

▶ **Theorem 34** (Completeness). *For any circuits $C_1, C_2 \in \mathbf{QC}$,*

$$\text{if } [\![C_1]\!] = [\![C_2]\!] \text{ then } \mathrm{QC} \vdash C_1 = C_2.$$

Proof. Let C_1, C_2 be n-qubit circuits such that $[\![C_1]\!] = [\![C_2]\!]$.

If $n = 0$, then the result is trivial since $\boxed{\ }$ is the only 0-qubit circuit. If $n = 1$ or $n = 2$, then the result is given by Lemmas 20 and 25 respectively.

If $n \geq 3$, let C_1', C_2' be representatives in $\mathbf{QC_{seq}}$ of respectively C_1 and C_2, so that $|C_1'| = C_1$ and $|C_2'| = C_2$. Since $[\![C_1]\!] = [\![C_2]\!]$ and the encoding preserves the semantics, one has $[\![E(C_1')]\!] = [\![E(C_1')]\!]$. Hence, by Theorem 18, we have $E(C_1') \approx E(C_2')$. By Lemma 33, this implies that $\mathrm{QC} \vdash D(E(C_1')) = D(E(C_2'))$. In turn, by Lemma 32, this implies that $\mathrm{QC} \vdash C_1 = C_2$. ◀

9 Conclusion and Perspectives

We have introduced a complete equational theory for unitary quantum circuits over the gate set $\left\{ -\boxed{H}-,\ -\bullet-,\ \begin{smallmatrix}\bullet\\|\\\bullet\end{smallmatrix},\ \begin{smallmatrix}\bullet\\|\\\boxed{H}\end{smallmatrix} \right\}$. To our knowledge, this is the second universal fragment of unitary quantum circuits to be given a complete axiomatization, and the first which is finitely generated. One can note the relative similarity between our complete equational theory and that of [10], which is proved to be minimal: both equational theories are composed of a few simple equations on at most 3 qubits, plus an equation schema consisting of one equation for each number of qubits; in both cases, the equation schema has a trivial semantic interpretation, and its meaning comes from the fact that the multi-controlled gate is expressed as a macro built from 1- and 2- qubit gates. A difference between our equational theory and that of [10] is that since we are working in a discrete setting, ours does not require working with continuous parameters.

An obvious follow-up question for future work is whether the unbounded equation schema of Equation (19) is actually necessary, or can be derived from a finite number of equations. In the second case, one would have to find a derivation of it; in the first case, one would have to find an argument to show its necessity. Note that the necessity argument used in [10] does not apply to our case.

Our result is for unitary circuits, without ancillas. One could proceed in the same way as in [11] to extend the equational theory and its completeness to circuits with qubit initializations, ancillas, and qubit discarding (i.e. trace-out). If Equation (19) turned out to be necessary in the unitary case, then another open question would be whether it can be derived in the presence of ancillas, similarly to what is done in [11, 10].

Another open problem is to find complete equational theories for other relevant fragments of quantum circuits. In particular, one could *a priori* proceed in the same way as we do in this paper in order to obtain complete equational theories for the Toffoli-Hadamard and Clifford+CS fragments, relying on the corresponding matrix group presentations given respectively in [28] and [5]. Doing the same for Clifford+T would require first to extend the presentation of [19] to arbitrary dimension.

References

1 Matthew Amy, Andrew N. Glaudell, and Neil J. Ross. Number-theoretic characterizations of some restricted Clifford+T circuits. *Quantum*, 4:252, April 2020. doi:10.22331/q-2020-04-06-252.

2 Miriam Backens and Aleks Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity. *Electronic Proceedings in Theoretical Computer Science*, 287:23–42, January 2019. doi:10.4204/eptcs.287.2.

3 Miriam Backens, Simon Perdrix, and Quanlong Wang. A simplified stabilizer ZX-calculus. In Ross Duncan and Chris Heunen, editors, *Proceedings 13th International Conference on Quantum Physics and Logic, QPL 2016, Glasgow, Scotland, 6-10 June 2016*, volume 236 of *EPTCS*, pages 1–20, 2016. doi:10.4204/EPTCS.236.1.

4 Miriam Backens, Simon Perdrix, and Quanlong Wang. Towards a minimal stabilizer ZX-calculus. *Log. Methods Comput. Sci.*, 16(4), 2020. doi:10.23638/LMCS-16(4:19)2020.

5 Xiaoning Bian and Peter Selinger. Generators and relations for Un(Z[1/2,i]). In Chris Heunen and Miriam Backens, editors, Proceedings 18th International Conference on *Quantum Physics and Logic,* Gdansk, Poland, and online, 7-11 June 2021, volume 343 of *Electronic Proceedings in Theoretical Computer Science*, pages 145–164. Open Publishing Association, 2021. doi:10.4204/EPTCS.343.8.

6 Xiaoning Bian and Peter Selinger. Generators and relations for 2-qubit Clifford+T operators. In Stefano Gogioso and Matty Hoban, editors, *Proceedings 19th International Conference on Quantum Physics and Logic, QPL 2022, Wolfson College, Oxford, UK, 27 June - 1 July 2022*, volume 394 of *EPTCS*, pages 13–28, 2022. doi:10.4204/EPTCS.394.2.

7 Xiaoning Bian and Peter Selinger. Generators and relations for 3-qubit Clifford+CS operators. In Shane Mansfield, Benoît Valiron, and Vladimir Zamdzhiev, editors, *Proceedings of the Twentieth International Conference on Quantum Physics and Logic, QPL 2023, Paris, France, 17-21st July 2023*, volume 384 of *EPTCS*, pages 114–126, 2023. doi:10.4204/EPTCS.384.7.

8 Titouan Carette and Emmanuel Jeandel. A recipe for quantum graphical languages. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 118:1–118:17, Dagstuhl, Germany, 2020. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ICALP.2020.118.

9 Alexandre Clément. A complete equational theory for real-Clifford+CH quantum circuits. *arXiv preprint*, February 2026. doi:10.48550/arXiv.2602.06644.

10 Alexandre Clément, Noé Delorme, and Simon Perdrix. Minimal equational theories for quantum circuits. In *LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 1–14, Tallinn, Estonia, July 2024. ACM. doi:10.1145/3661814.3662088.

11 Alexandre Clément, Noé Delorme, Simon Perdrix, and Renaud Vilmart. Quantum circuit completeness: Extensions and simplifications. In *32nd EACSL Annual Conference on Computer Science Logic (CSL 2024)*, Naples, Italy, February 2024. doi:10.4230/LIPIcs.CSL.2024.20.

12 Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. A complete equational theory for quantum circuits. In *2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–13, Boston, United States, June 2023. IEEE. doi:10.1109/LICS56636.2023.10175801.

13 Bob Coecke and Ross Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, 2011. doi:10.1088/1367-2630/13/4/043016.

14 Niel de Beaudrap, Aleks Kissinger, and John van de Wetering. Circuit extraction for ZX-diagrams can be #P-hard. *arXiv preprint*, 2022. arXiv:2202.09194.

15 Marc de Visme and Renaud Vilmart. Minimality in Finite-Dimensional ZW-Calculi. In *Computer Science Logic (CSL)*, volume 33rd EACSL Annual Conference on Computer Science Logic (CSL 2025), Amsterdam, Netherlands, February 2025. doi:10.4230/LIPIcs.CSL.2025.49.

16 Noé Delorme and Simon Perdrix. Diagrammatic reasoning with control as a constructor, applications to quantum circuits. In Nathalie Bertrand and Stefan Milius, editors, *29th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS)*, pages 240–261, Cham, 2026. Springer Nature Switzerland. doi:10.1007/978-3-032-22730-0_12.

17 Ross Duncan, Aleks Kissinger, Simon Perdrix, and John van de Wetering. Graph-theoretic simplification of quantum circuits with the ZX-calculus. *Quantum*, 4:279, June 2020. doi:10.22331/q-2020-06-04-279.

18 Wang Fang, Chris Heunen, and Robin Kaarsgaard. Hadamard-Pi: Equational quantum programming. *Proc. ACM Program. Lang.*, 10(POPL), 2026. doi:10.1145/3776647.

19 Seth Eveson Murray Greylyn. *Generators and relations for the group* $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. MSc thesis, Dalhousie University, 2014. Available from arXiv:1408.6204.

20 Amar Hadzihasanovic. A diagrammatic axiomatisation for qubit entanglement. In *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 573–584, 2015. doi:10.1109/LICS.2015.59.

21 Amar Hadzihasanovic, Kang Feng Ng, and Quanlong Wang. Two complete axiomatisations of pure-state qubit quantum computing. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 502–511. ACM, 2018. doi:10.1145/3209108.3209128.

22 Chris Heunen, Robin Kaarsgaard, and Louis Lemonnier. One rig to control them all. *arXiv preprint*, 2025. To appear in LICS 2026. doi:10.48550/arXiv.2510.05032.

23 Kazuo Iwama, Yahiko Kambayashi, and Shigeru Yamashita. Transformation rules for designing CNOT-based quantum circuits. In *Proceedings of the 39th annual Design Automation Conference*, pages 419–424, 2002. doi:10.1145/513918.514026.

24 Emmanuel Jeandel, Simon Perdrix, and Renaud 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*, pages 559–568, 2018. doi:10.1145/3209108.3209131.

25 Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 569–578, 2018. doi:10.1145/3209108.3209139.

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

27 Yves Lafont. Towards an algebraic theory of boolean circuits. *Journal of Pure and Applied Algebra*, 184(2):257–310, 2003. doi:10.1016/S0022-4049(03)00069-0.

28 Sarah Meng Li, Neil J. Ross, and Peter Selinger. Generators and relations for the group On(Z[1/2]). In Chris Heunen and Miriam Backens, editors, Proceedings 18th International Conference on *Quantum Physics and Logic,* Gdansk, Poland, and online, 7-11 June 2021, volume 343 of *Electronic Proceedings in Theoretical Computer Science*, pages 210–264. Open Publishing Association, 2021. doi:10.4204/EPTCS.343.11.

29 Saunders MacLane. Categorical algebra. *Bulletin of the American Mathematical Society*, 71(1):40–106, 1965. doi:10.1090/S0002-9904-1965-11234-4.

30 Boldizsár Poór, Quanlong Wang, Razin A. Shaikh, Lia Yeh, Richie Yeung, and Bob Coecke. Completeness for arbitrary finite dimensions of ZXW-calculus, a unifying calculus. In *2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, June 2023. doi:10.1109/lics56636.2023.10175672.

31 Kurt Reidemeister. Knoten und Gruppen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):7–23, 1927. doi:10.1007/BF02952506.

32 Otto Schreier. Die Untergruppen der freien Gruppen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):161–183, 1927. doi:10.1007/BF02952517.

33 Borun Shi. Towards minimality of Clifford+T ZX-calculus. *Master's thesis University of Oxford*, 2018.

34 John van de Wetering and Sal Wolffs. Completeness of the phase-free ZH-calculus. *arXiv preprint*, 2019. arXiv:1904.07545.

35 Thomas van Ouwerkerk, Aleks Kissinger, and Freek Wiedijk. Investigating the minimality of the ZH-calculus, 2019.

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

37 Fabio Zanasi. *Interacting Hopf Algebras- the Theory of Linear Systems*. PhD thesis, Ecole normale supérieure de lyon - ENS LYON, October 2015. arXiv:1805.03032.

A Modified Exact Synthesis Algorithm

Algorithm 1 Exact synthesis for $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ (cf. [18]).

Input: An element A of $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$
Output: A sequence $\mathbf{W}_1, \dots, \mathbf{W}_\ell$ of words over $\mathcal{G}_N$ such that $\mathbf{W}_\ell \cdots \mathbf{W}_1 A = I$

$B \leftarrow A$
for $j \leftarrow N-1, N-2, \dots, 0$ **do**
  $k \leftarrow \mathrm{lde}(Be_j)$ ▷ See [18] for the definition of lde
  while $k > 0$ **do**
    Let i_1 be the least integer such that $\sqrt{2}^k B[i_1, j] \equiv 1 \pmod 2$ or $\equiv 1+\sqrt{2} \pmod 2$
    Let i_2 be the least integer $> i_1$ such that $\sqrt{2}^k B[i_2, j] \equiv \sqrt{2}^k B[i_1, j] \pmod 2$ ▷ See [1] for the existence of i_1 and i_2
    $\mathbf{W} \leftarrow H_{[i_1,i_2]}$
    Output $\mathbf{W}$
    $B \leftarrow \mathbf{W}B, k \leftarrow \mathrm{lde}(Be_j)$
  end while
end for ▷ $\mathrm{lde}(Be_j) = 0$ for all j, therefore B is now a permutation matrix
for $j \leftarrow N-1, N-2, \dots, 0$ **do**
  $v \leftarrow Be_j$
  if $v \neq e_j$ **then**
    There are $a \leq j$ and $\tau \in \{0, 1\}$ such that $v = (-1)^\tau e_a$.
    if $a = j$ **then** $\mathbf{W} \leftarrow (-1)^\tau_{[a]}$
    if $a < j$ **then** $\mathbf{W} \leftarrow X_{[a,j]}(-1)^\tau_{[a]}$
    Output $\mathbf{W}$
    $B \leftarrow \mathbf{W}B$
  end if
end for

B Sketch of the Reidemeister-Schreier Theorem for Monoids

We denote by $U_N^{\mathrm{even}}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ the submonoid (or subgroup) of $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ consisting of the matrices with even H- and ZX-parities.

In order to apply the Reidemeister-Schreier theorem for monoids described in [6] (Section 4.2), it suffices to provide the following elements:

- a set C, consisting of a representative of each of the four cosets of $U_N^{\mathrm{even}}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ as a subgroup of $U_N(\mathbb{Z}[\frac{1}{\sqrt{2}}])$, the representative of $U_N^{\mathrm{even}}(\mathbb{Z}[\frac{1}{\sqrt{2}}])$ itself being necessarily the identity I
- a function $f\colon \mathcal{P}_N \to \mathcal{G}_N^*$ (where $\mathcal{G}_N^*$ denotes the free monoid generated by $\mathcal{G}_N$) preserving the semantics
- a function $h\colon C \times \mathcal{G}_N \to \mathcal{P}_N^* \times C$ such that for any (c, g), if $(p, c') = h(c, g)$ then $[\![cg]\!] = [\![pc']\!]$.

Then, let $h^{**}\colon C \times \mathcal{G}_N^* \to \mathcal{P}_N^* \times C$ be the function defined by $h^{**}(c_0, x_1 ... x_k) = (w_1 \cdot ... \cdot w_k, c_k)$, where $h(c_{i-1}, x_i) = (w_i, c_i)$ for all $i = 1, ..., k$. The Reidemeister-Schreier theorem for monoids stated in [6] tells us that the equational theory consisting of the following equations is complete:

(a) for every $x \in \mathcal{P}_N$, an equation $x \approx v$, where v is such that $h^{**}(I, f(x)) = (v, c)$ (note that in this case, the preservation of the semantics implies that $c = I$)

(b) for every equation of Figure 7, of the form $w \approx w'$, and every $c \in C$, an equation $v \approx v'$, where v, v' are such that $h^{**}(c, w) = (v, c')$ and $h^{**}(c, w') = (v', c'')$ (note that in this case, the preservation of the semantics implies that $c' = c''$).

C Definition of the right-hand sides of Equations (36) and (37)

$$\mathcal{W}_1 \coloneqq \left(\prod_{j=m+1}^{\overleftarrow{m+\ell}} E_{n-j-2,j}(\times)\right) \circ \left(\prod_{j=0}^{\overleftarrow{m-1}} E_{n-j-2,j}(\times) \circ E_{n-j-3,j+1}(\times)\right) \circ E_{n-2,0}(\times) \circ$$

$$\left(\prod_{j=k+\ell}^{\overleftarrow{n-3}} \mathcal{E}^{1-z_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=k}^{\overleftarrow{k+\ell-1}} \mathcal{E}^{1-y_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=0}^{\overleftarrow{k-1}} \mathcal{E}^{1-x_j}_{j,n-j-2}(\oplus)\right) \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ$$

$$\left(\prod_{j=0}^{\overrightarrow{k-1}} \mathcal{E}^{1-x_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=k}^{\overrightarrow{k+\ell-1}} \mathcal{E}^{1-y_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=k+\ell}^{\overrightarrow{n-3}} \mathcal{E}^{1-z_j}_{j,n-j-2}(\oplus)\right) \circ$$

$$E_{n-2,0}(\times) \circ \left(\prod_{j=0}^{\overrightarrow{m-1}} E_{n-j-3,j+1}(\times) \circ E_{n-j-2,j}(\times)\right) \circ \left(\prod_{j=m+1}^{\overrightarrow{m+\ell}} E_{n-j-2,j}(\times)\right)$$

$$\mathcal{W}_2 \coloneqq \left(\prod_{j=m+1}^{\overleftarrow{m+\ell}} E_{n-j-2,j}(\times)\right) \circ \left(\prod_{j=0}^{\overleftarrow{m-1}} E_{n-j-2,j}(\times) \circ E_{n-j-3,j+1}(\times)\right) \circ$$

$$\left(\prod_{j=k+\ell}^{\overleftarrow{n-3}} \mathcal{E}^{1-z_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=k}^{\overleftarrow{k+\ell-1}} \mathcal{E}^{1-y_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=0}^{\overleftarrow{k-1}} \mathcal{E}^{1-x_j}_{j,n-j-2}(\oplus)\right) \circ \left(H_{[0,1]} H_{[3,2]}\right) \circ$$

$$\left(\prod_{j=0}^{\overrightarrow{k-1}} \mathcal{E}^{1-x_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=k}^{\overrightarrow{k+\ell-1}} \mathcal{E}^{1-y_j}_{j,n-j-2}(\oplus)\right) \circ \left(\prod_{j=k+\ell}^{\overrightarrow{n-3}} \mathcal{E}^{1-z_j}_{j,n-j-2}(\oplus)\right) \circ$$

$$\left(\prod_{j=0}^{\overrightarrow{m-1}} E_{n-j-3,j+1}(\times) \circ E_{n-j-2,j}(\times)\right) \circ \left(\prod_{j=m+1}^{\overrightarrow{m+\ell}} E_{n-j-2,j}(\times)\right)$$

where the notations $\prod^{\overleftarrow{\ }}$ and $\prod^{\overrightarrow{\ }}$ are introduced in Definition 28, and $\mathcal{E}^{1-x}_{k,\ell}(\oplus)$ is a shortcut defined as follows (where the order of the product is left unspecified):

$$\mathcal{E}^{1-x}_{k,\ell}(\oplus) \coloneqq \begin{cases} \epsilon & \text{if } x = 1 \\ E_{k,\ell}(\bullet) \circ \prod_{\substack{x \in \{0,1\}^k \\ y \in \{0,1\}^\ell}} \left((-1)_{[G_n^{-1}(x1y)]} X_{[G_n^{-1}(x0y), G_n^{-1}(x1y)]}\right) & \text{if } x = 0. \end{cases}$$