THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

With a Few Square Roots, Quantum Computing Is as Easy as Pi

Citation for published version:
Carette, J, Heunen, C, Kaarsgaard, R & Sabry, A 2024, 'With a Few Square Roots, Quantum Computing Is as Easy as Pi', *Proceedings of the ACM on Programming Languages*, vol. 8, no. POPL, 19, pp. 546-574. https://doi.org/10.1145/3632861

Digital Object Identifier (DOI):
10.1145/3632861

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Proceedings of the ACM on Programming Languages

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

OPEN ACCESS

Download date: 28. Apr. 2025

arXiv:2310.14056v1 [cs.PL] 21 Oct 2023

With a Few Square Roots, Quantum Computing is as Easy as Π

JACQUES CARETTE, McMaster University, Canada
CHRIS HEUNEN, University of Edinburgh, United Kingdom
ROBIN KAARSGAARD, University of Southern Denmark, Denmark
AMR SABRY, Indiana University, United States of America

Rig groupoids provide a semantic model of Π, a universal classical reversible programming language over finite types. We prove that extending rig groupoids with just two maps and three equations about them results in a model of quantum computing that is computationally universal and equationally sound and complete for a variety of gate sets. The first map corresponds to an 8^{th} root of the identity morphism on the unit 1. The second map corresponds to a square root of the symmetry on $1+1$. As square roots are generally not unique and can sometimes even be trivial, the maps are constrained to satisfy a nondegeneracy axiom, which we relate to the Euler decomposition of the Hadamard gate. The semantic construction is turned into an extension of Π, called $\sqrt{\Pi}$, that is a computationally universal quantum programming language equipped with an equational theory that is sound and complete with respect to the Clifford gate set, the standard gate set of Clifford+T restricted to ≤ 2 qubits, and the computationally universal Gaussian Clifford+T gate set.

ACM Reference Format:
Jacques Carette, Chris Heunen, Robin Kaarsgaard, and Amr Sabry. 2023. With a Few Square Roots, Quantum Computing is as Easy as Π. 1, 1 (October 2023), 42 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Just like in the classical case, quantum computing can be built up from booleans and associated operations. The quantum version of boolean negation is the X gate defined by $\mathsf{X}\,|0\rangle = |1\rangle$ and $\mathsf{X}\,|1\rangle = |0\rangle$. The quantum circuit model also includes a gate $\sqrt{\mathsf{X}}$ (also known as the V gate) that is the "square root of X." Informally $\sqrt{\mathsf{X}}$ performs half of the action of the X gate, *i.e.*, if we imagine a trajectory from $|0\rangle$ to $|1\rangle$ and another trajectory from $|1\rangle$ to $|0\rangle$, then one application of $\sqrt{\mathsf{X}}$ follows half the relevant trajectory. The standard approach to model this behaviour is to explicitly express the intermediate midpoints as complex vectors [Hayes 1995; Satoh et al. 2022]:

$$\sqrt{\mathsf{X}}\,|0\rangle = \frac{1+i}{2}\,|0\rangle + \frac{1-i}{2}\,|1\rangle \qquad\qquad \sqrt{\mathsf{X}}\,|1\rangle = \frac{1-i}{2}\,|0\rangle + \frac{1+i}{2}\,|1\rangle$$

One can verify that:

$$\begin{aligned}
\sqrt{\mathsf{X}}(\sqrt{\mathsf{X}}\;|0\rangle) &= \sqrt{\mathsf{X}}(\tfrac{1+i}{2}\,|0\rangle + \tfrac{1-i}{2}\,|1\rangle) \\
&= \tfrac{1+i}{2}\sqrt{\mathsf{X}}\,|0\rangle + \tfrac{1-i}{2}\sqrt{\mathsf{X}}\,|1\rangle \\
&= \tfrac{1+i}{2}(\tfrac{1+i}{2}\,|0\rangle + \tfrac{1-i}{2}\,|1\rangle) + \tfrac{1-i}{2}(\tfrac{1-i}{2}\,|0\rangle + \tfrac{1+i}{2}\,|1\rangle) \\
&= \tfrac{i}{2}\,|0\rangle + \tfrac{1}{2}\,|1\rangle - \tfrac{i}{2}\,|0\rangle + \tfrac{1}{2}\,|1\rangle \\
&= |1\rangle
\end{aligned}$$

and similarly that $\sqrt{\mathsf{X}}(\sqrt{\mathsf{X}}\;|1\rangle) = |0\rangle$. As is evident in this tiny example, reasoning this way about quantum programs is overwhelmed by complex numbers and linear algebra.

Authors' addresses: Jacques Carette, carette@mcmaster.ca, McMaster University, Hamilton, Ontario, Canada; Chris Heunen, Chris.Heunen@ed.ac.uk, University of Edinburgh, Edinburgh, United Kingdom; Robin Kaarsgaard, kaarsgaard@imada.sdu.dk, University of Southern Denmark, Odense, Denmark; Amr Sabry, sabry@indiana.edu, Indiana University, Bloomington, Indiana, United States of America.

2023. XXXX-XXXX/2023/10-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Our first insight is that we do *not* need to explicitly represent the intermediate points. All we need to know about them are two things: (i) they exist, and (ii) they satisfy one critical axiom. Technically, we demonstrate that the following categorical model is, not only computationally universal for quantum computing, but also sound and complete for several modes of unitary quantum computing.

Definition of the Quantum Model. The model consists of a rig groupoid $(\mathbf{C}, \otimes, \oplus, O, I)$ equipped with maps $\omega\colon I \longrightarrow I$ and $\mathsf{V}\colon I \oplus I \longrightarrow I \oplus I$ satisfying the equations:

$$\text{(E1) } \omega^8 = \text{id} \qquad \text{(E2) } \mathsf{V}^2 = \sigma_\oplus \qquad \text{(E3) } \mathsf{V} \circ \mathsf{S} \circ \mathsf{V} = \omega^2 \bullet \mathsf{S} \circ \mathsf{V} \circ \mathsf{S}$$

where $\circ$ is sequential composition, $\bullet$ is scalar multiplication (cf. Def. 4), $\sigma_\oplus$ is the symmetry on $I \oplus I$, exponents are iterated sequential compositions, and $\mathsf{S}\colon I \oplus I \longrightarrow I \oplus I$ is defined as $\mathsf{S} = \text{id} \oplus \omega^2$.

In the definition, the rig groupoid $\mathbf{C}$ models an underlying reversible classical programming language. By convention, booleans in this language are represented as values of type $I \oplus I$ with one injection representing `false`, the other representing `true`, and the symmetry $\sigma_\oplus\colon I \oplus I \longrightarrow I \oplus I$ representing boolean negation. The quantum model has two additional morphisms ω and V. The map ω is a primitive 8^{th} root of the identity; its semantics is partially specified by (E1). The map V is the square root of boolean negation; its semantics is partially specified by (E2). So far, we have postulated the existence of square roots but without needing to write any actual complex numbers: they are just morphisms partially specified by (E1) and (E2). At this point, it would be consistent to choose $\omega = \text{id}$ but this would not lead to a universal quantum model. To understand how (E3) selects just the "right" square root, we recall that the *Euler decomposition* expresses any 1-qubit unitary gate as a product of a global phase and three rotations along two fixed orthogonal axes, and that S and V correspond to rotations in complementary bases. In that light, axiom (E3) picks the Z-basis and the X-basis as the two axes and enforces that decompositions along ZXZ or XZX are equal (up to a physically unimportant global phase). This ensures that it is immaterial which of S and V rotations is mapped to the Z- or X-basis and additionally ensures that the angle of the S rotation (induced by the ω^2 in the definition of S) is $\pi/2$. As a helpful illustration, Fig. 1 shows that, with the standard choice for the computational basis in the Z-direction, starting from an arbitrary state (near the North pole in the figure), a sequence of $\pi/2$-XZX rotations (top) is equivalent to a sequence of $\pi/2$-ZXZ rotations (bottom). Were the angle of the Z-rotation different due to a different choice of ω, the two sequences of rotations would not be equivalent.

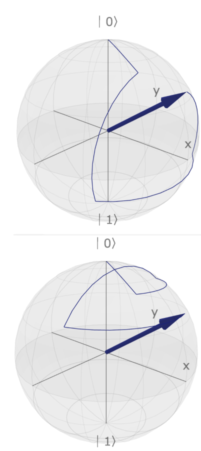


Fig. 1. XZX and ZXZ rotations with all angles at $\pi/2$.

This approach reduces reasoning about quantum programs to manipulating the coherence conditions of rig categories [Laplaza 1972] extended with the axioms (E1), (E2), and (E3). The calculation that $\sqrt{\mathsf{X}} \circ \sqrt{\mathsf{X}} = X$ follows by (E2). Many quantum equivalences follow similarly. For example, the proof that $\mathsf{S} \circ \mathsf{S}$ is equivalent to the Z gate defined as $\text{id} \oplus \omega^4$ follows by:

$$\mathsf{S} \circ \mathsf{S} = (\text{id} \oplus \omega^2) \circ (\text{id} \oplus \omega^2) = (\text{id} \circ \text{id}) \oplus (\omega^2 \circ \omega^2) = \text{id} \oplus \omega^4 = \mathsf{Z}$$

The proof uses just the coherence conditions of rig categories and is, along with many other results, formalised in an extension of the `agda-categories` library [Hu and Carette 2021] included in the supplementary material.

The equational theory extracted from the semantic model is sound and complete with respect to *arbitrary Clifford circuits*, *Clifford+T circuits of at most* 2 *qubits*, and *arbitrary Gaussian Clifford+T circuits*. These completeness theorems, Thms. 16, 19, and 25, form our main technical results:

- Completeness for *Arbitrary Clifford circuits* (cf. Thm 16). Circuits built from Clifford gates are important in quantum computing for two related reasons. First, Clifford gates are exactly those quantum gates that normalise the Pauli matrices, which provide a linear-algebraic basis for a single qubit. Clifford gates include, and are in fact generated by, H, S, and CX. Second, although Clifford circuits may "look quantum," they are in fact efficiently simulatable by a probabilistic classical computation, by the Gottesman-Knill theorem [Gottesman 1999].
- Completeness for *Clifford+T circuits of at most 2 qubits* (cf. Thm 19). To move beyond classical probabilistic machines in computational power, other quantum gates need to be considered. One popular choice is to extend the Clifford set with the T gate. The restriction to ≤ 2 qubits is a stepping stone to the next result.
- Completeness for *Arbitrary Gaussian Clifford+T circuits* (cf. Thm 21). Another universal quantum gate set is given by $\{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \mathsf{S}, \mathsf{K}\}$ [Amy et al. 2020; Bian and Selinger 2021]. Such circuits can be characterised algebraically as those unitary matrices with entries in the ring $\mathbb{Z}[\frac{1}{2}, i]$ of Gaussian dyadic rationals [Amy et al. 2020].

To summarise, we have developed a vastly simplified axiomatic treatment of quantum computation using the coherence conditions of rig categories extended with morphisms modeling roots of the identity and a square root of the symmetry $\sigma_{\oplus} \colon I \oplus I \to I \oplus I$.

This formalism provides, to our knowledge, the first sound and complete equational theory for a computationally universal unitary quantum programming language. As this approach avoids imposing specific assumptions about gate sets or implementation details, it could serve to bridge the gap between quantum programming languages and the various gate sets used in the quantum circuit model. Further, it could serve as a "theory of equational theories" capable of describing and analyzing various modes of quantum computing, such as different gate sets, without preference to any specific approach. While this paper primarily focuses on qubit circuits due to the abundance of finite presentation results, it does not reflect an inherent limitation or assumption within the formalism. In fact, we propose that this formalism could be used equally well to represent and analyse circuits from qudit gate sets (*e.g.*, qutrit Clifford+T [Yeh and Wetering 2022]).

Related work. Our result is distinguished from other calculi based on ZX [Coecke and Duncan 2011], notably ZH [Backens and Kissinger 2019] and PBS/LOv [Clément et al. 2023] in two fundamental aspects. First, ZX and ZH describe quantum theory, not quantum computation. That is, they are complete for all linear maps, not for unitary ones only. Indeed, one of the major problems associated with the ZX calculus is circuit extraction: to ensure that rewriting a quantum circuit ends up with a quantum circuit again. This problem is #P-hard [de Beaudrap et al. 2022]. Second, these calculi do not have universal equational theories, as some of the axiom schemas involve existential quantifiers, resulting from the Euler decomposition, that cannot be eliminated [Duncan and Perdrix 2009]. The theory presented here builds on a different line of research that led to advances in reversible quantum computing (*e.g.*, [Choudhury et al. 2022; Glück et al. 2019; Heunen and Kaarsgaard 2022; Heunen, Kaarsgaard, and Karvonen 2018]) and equational theories of quantum circuits and unitaries [Bian and Selinger 2021, 2022; Selinger 2015] (see also [Thomsen et al. 2015]) arising from number-theoretic insights (*e.g.*, [Amy et al. 2020; Giles and Selinger 2013]). Our resulting theory is sound, complete and universal, never considers more general linear maps (unlike ZH/ZX), and relies only on universally quantified equations (unlike PBS/LOv). Our work complements the work of Staton [2015], which provides a sound and complete equational theory of state preparation and measurement (which we do not consider here), but does not consider an equational theory of unitaries.

Outline. We assume familiarity with category theory (in particular rig categories, monoidal categories, and string diagrams) and with the fundamentals of quantum computing. We provide a brief review in the next section for the necessary notation and conventions. Sec 3 motivates the use of combinator-based languages to reason about quantum circuits. Sec. 4 introduces the formal syntax of the combinator language $\sqrt{\Pi}$ used as a technical device in this paper. Sec. 5 gives the denotational semantics of $\sqrt{\Pi}$ in extended rig groupoids. Sec. 6 includes the main technical results that establish soundness and completeness of $\sqrt{\Pi}$ for a variety of gate sets. Sec. 7 describes the equational theory in action. The concluding section puts the results in a larger context and discusses their significance. Some of the proofs are relegated to the appendix.

2 BACKGROUND

We recall here some basics of unitary quantum computing and rig categories.

2.1 Unitary quantum computing

For more details about this topic we refer to textbooks such as [Nielsen and Chuang 2010; Yanofsky and Mannucci 2008].

Closed quantum systems are modelled mathematically by complex Hilbert spaces H, which are complex vector spaces with an inner product $\langle - | - \rangle$ that are complete as metric spaces (with respect to the metric induced by the inner product). For example, a one-qubit system is represented by $\mathbb{C}^2$, with vectors $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ and $|1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ representing the two classical states. Hilbert spaces H and K can be combined to form new ones using the *direct sum* $H \oplus K$ and *tensor product* $H \otimes K$: these can be seen as analogues of sum types and product types in the sense that $\mathbb{C}^n \oplus \mathbb{C}^m \cong \mathbb{C}^{n+m}$ and $\mathbb{C}^n \otimes \mathbb{C}^m \cong \mathbb{C}^{nm}$.

Every linear map f on a Hilbert space is associated with a *(Hermitian) adjoint* $f^\dagger$ satisfying $\langle f\phi | \psi \rangle = \langle \phi | f^\dagger \psi \rangle$. The discrete time evolution of closed quantum systems is described by *unitaries*, which are linear isomorphisms U satisfying $U^{-1} = U^\dagger$. Some important examples of unitaries on $\mathbb{C}^2$ include the *Hadamard* gate H, the X gate (the quantum analogue of the classical NOT gate), and the *phase gates* Z, S, and T, given by the matrices:

$$\mathsf{H} = \tfrac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\1 & -1\end{smallmatrix}\right) \qquad \mathsf{X} = \left(\begin{smallmatrix}0 & 1\\1 & 0\end{smallmatrix}\right) \qquad \mathsf{Z} = \left(\begin{smallmatrix}1 & 0\\0 & -1\end{smallmatrix}\right) \qquad \mathsf{S} = \left(\begin{smallmatrix}1 & 0\\0 & i\end{smallmatrix}\right) \qquad \mathsf{T} = \begin{pmatrix}1 & 0\\0 & \frac{1+i}{\sqrt{2}}\end{pmatrix}$$

Any unitary U acting on H can be extended to a *controlled* variant acting on $C^2 \otimes H$, given in matrix form by the block diagonal matrix

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

where I is the identity on H. This controlled-U will apply U to H only if the given qubit was in the state $|1\rangle$; otherwise it will do nothing. For example, the controlled-X gate CX is given by

$$\mathsf{CX} = \left(\begin{smallmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{smallmatrix}\right)$$

Similar to classical hardware description, low-level quantum computations can be described at the level of qubits and gates using quantum circuits, which we describe in further detail in Sec. 3, save for one crucial definition concerning when a quantum gate set can be said to be universal:

Definition 1 (Computational universality [Aharonov 2003]). A set of quantum gates G is said to be *strictly universal* if there exists a constant n_0 such that for any $n \geq n_0$, the subgroup generated by

G is dense in $\mathrm{SU}(2^n)$. The set G is said to be *computationally universal* if it can be used to simulate to within ϵ error any quantum circuit which uses n qubits and t gates from a strictly universal set with only polylogarithmic overhead in $(n, t, 1/\epsilon)$.

2.2 Rig categories

We refer to [Awodey 2010; Heunen and Vicary 2019] for more on (monoidal) categories, and to [Johnson and Yau 2021] for a recent textbook on rig categories and their applications.

A category $\mathbf{C}$ is an algebraic structure capturing typed processes: a category consists of some types (*objects*) X, Y, Z and some processes (*morphisms*) f, g, h such that each process f is assigned an input type (*domain*) X and an output type (*codomain*) Y, written $f : X \to Y$. Processes $f : X \to Y$ and $g : Y \to Z$ can be composed to form a new process $g \circ f : X \to Z$ in such a way that composition is associative and unital (*i.e.*, every object X is associated with an *identity* $\mathrm{id}_X : X \to X$ such that $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f$ for all $f : X \to Y$). Thus, categories describe theories of processes that can be composed in sequence: if a morphism f has an inverse f^{-1} such that $f \circ f^{-1} = \mathrm{id}$ and $f^{-1} \circ f = \mathrm{id}$, we say that f is an *isomorphism*. A category which contains only isomorphisms is called a *groupoid*.

A *symmetric monoidal category* $(\mathbf{C}, \otimes, I)$ is a category that also permits parallel composition of objects and morphisms: whenever one has objects X and Y, there exists an object $X \otimes Y$; similarly, morphisms $f : X \to Y$ and $g : Z \to W$ give rise to $f \otimes g : X \otimes Z \to Y \otimes W$. Further, we require that there is a distinguished object I and families of isomorphisms (indexed by objects X, Y, Z) $\lambda_\otimes : I \otimes X \to X$ and $\rho_\otimes : I \otimes X \to X$ (the *unitors*); $\alpha_\otimes : (X \otimes Y) \otimes Z \to X \otimes (Y \otimes Z)$ (the *associator*); and $\sigma_\otimes : X \otimes Y \to Y \otimes X$ (the *symmetry*), satisfying some equations (see, *e.g.*, [Heunen and Vicary 2019, Chapter 1]).

A *rig category* (or *bimonoidal category*) $(\mathbf{C}, \otimes, \oplus, I, O)$ is a category which is symmetric monoidal in two different ways, such that one monoidal structure distributes over the other. Precisely, it is a category such that $(\mathbf{C}, \otimes, I)$ and $(\mathbf{C}, \oplus, O)$ are both symmetric monoidal categories, and there are families of isomorphisms (indexed by objects X, Y, Z) $\delta_L : X \otimes (Y \oplus Z) \to (X \otimes Y) \oplus (X \otimes Z)$ and $\delta_R : (X \oplus Y) \otimes Z \to (X \otimes Z) \oplus (Y \otimes Z)$ (the *distributors*) and $\delta_0^L : O \otimes X \to O$ and $\delta_0^R : X \otimes O \to O$ (the *annihilators*), subject again to some equations (see [Laplaza 1972]). A rig category which is simultaneously a groupoid is called a *rig groupoid*. The category **Unitary** of finite-dimensional Hilbert spaces and unitaries forms a rig groupoid with its tensor product $\otimes$ and direct sum $\oplus$.

3 REASONING ABOUT QUANTUM CIRCUITS WITH COMBINATORS

The *lingua franca* of quantum computing is that of quantum circuits. Like boolean circuits consisting of bit-carrying wires connecting boolean gates, quantum circuits consist of wires carrying qubits connecting quantum gates. For example, the circuit in Fig. 2 has 5 controlled unitary gates acting on 3 qubits. In order, the first three gates are: controlled-$\sqrt{\mathrm{X}}$ (aka CSX), controlled-not (aka CX), and controlled-inverse-$\sqrt{\mathrm{X}}$ (aka CSXdg).

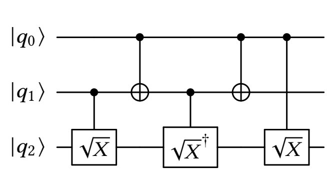


Fig. 2. Quantum circuit for CCX.

3.1 Circuits as Matrices

Quantum circuits have a canonical reading as complex matrices. The quantum gates stand for specific unitary matrices which are combined by matrix multiplication when gates are composed sequentially, and by tensor product when gates are composed in parallel. For example, the controlled gates used in the circuit above denote the following matrices:

$$\mathsf{CSX} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1+i & -1-i \\ 0 & 0 & -1-i & -1+i \end{pmatrix} \qquad \mathsf{CX} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \mathsf{CSXdg} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1-i & -1+i \\ 0 & 0 & -1+i & -1-i \end{pmatrix}$$

which when all multiplied following the layout of the circuit produce:

$$\begin{pmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{pmatrix}$$

The reader may recognise the resulting matrix as the denotation of the Toffoli (aka CCX) gate [Toffoli 1980]. Indeed the equivalence of CCX to the circuit in Fig. 2 is an instance of the Sleator-Weinfurter [1995] construction. Evidently, one way to establish the equivalence is to reduce both circuits to a common matrix. If such a low-level algebraic manipulation is undesirable, a high-level, but informal proof, would proceed by case analysis on the possible values of q_0q_1:

- if both q_0q_1 are 0, then no control gate is activated and the circuit behaves like the identity;
- if one of q_0q_1 is 1 and the other is 0, then both $\sqrt{\mathsf{X}}$ and its inverse are activated and the circuit is again equivalent to the identity;
- if both q_0q_1 are 1, then two instances of $\sqrt{\mathsf{X}}$ are activated which negates q_2.

To summarise, the circuit in Fig. 2 negates q_2 exactly when both q_0q_1 are 1, which is exactly the behaviour of the Toffoli gate. We will formalise this example using our calculus in Sec. 7.

3.2 Circuits as Rig Morphisms

It is relatively easy to find *some* collection of local rewrite rules that are sound for quantum circuits composed of particular gate sets. It is much harder to find a *complete* collection that guarantee that any equivalent quantum circuits can be transformed to one another. We solve this problem as follows. First, we build on the completeness result for classical reversible circuits [Choudhury et al. 2022] by including all the coherence conditions for rig categories as a foundation for reasoning about the classical subset of gates (*e.g.*, X, CX, CCX, etc.) To reason about the purely quantum gates (*e.g.*, $\sqrt{\mathsf{X}}$, H, T, etc.) we build on a collection of insights explained below.

The first insight is to not worry about gates at all but instead exploit the rig groupoid structure that provides two constructors $\oplus$ and $\otimes$ that behave in a distributive way, like + and × in the rig of natural numbers. The $\oplus$ construct, which is not present in formalisms such as the ZX-calculus [Coecke and Duncan 2011] provides a way to build quantum gates from first principles by exploiting the fact that a qubit is a two-dimensional additive structure $\mathbb{1} \oplus \mathbb{1}$. For example, the rig structure provides, among others, the natural isomorphisms $\lambda_\otimes : I \otimes A \to A$, $\sigma_\oplus : A \oplus B \to B \oplus A$, and $\delta_R : (A \oplus B) \otimes C \to (A \oplus C) \otimes (B \oplus C)$ which can be used to define gates as follows. First, we isolate two patterns Mat and Ctrl to construct simple gates and their controlled versions:

$$\mathsf{Mat} ::= \lambda_\otimes \oplus \lambda_\otimes \circ \delta_R : (I \oplus I) \otimes A \to A \oplus A$$

$$\mathsf{Ctrl}\ m ::= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus m) \circ \mathsf{Mat} : (I \oplus I) \otimes A \to (I \oplus I) \otimes A$$

The definition of Ctrl above is parametric in $m : I \oplus I \to I \oplus I$, enabling the definitions of the classical gates:

$$\begin{aligned} \mathsf{X} &::= \sigma_\oplus : I \oplus I \to I \oplus I \\ \mathsf{CX} &::= \mathsf{Ctrl}\ \mathsf{X} : (I \oplus I) \otimes (I \oplus I) \to (I \oplus I) \otimes (I \oplus I) \\ \mathsf{CCX} &::= \mathsf{Ctrl}\ \mathsf{CX} : (I \oplus I) \otimes ((I \oplus I) \otimes (I \oplus I)) \to (I \oplus I) \otimes ((I \oplus I) \otimes (I \oplus I)) \end{aligned}$$

$$
\begin{aligned}
b &::= \mathbb{0} \mid \mathbb{1} \mid b + b \mid b \times b && \text{(value types)} \\
t &::= b \leftrightarrow b && \text{(combinator types)} \\
iso &::= id \mid swap^{+} \mid assocr^{+} \mid assocl^{+} \mid unite^{+}l \mid uniti^{+}l \mid absorbl \mid factorzr && \text{(isomorphisms)} \\
&\quad \mid swap^{\times} \mid assocr^{\times} \mid assocl^{\times} \mid unite^{\times}l \mid uniti^{\times}l \mid dist \mid factor \\
c &::= iso \mid c \fatsemi c \mid c + c \mid c \times c && \text{(combinators)}
\end{aligned}
$$

Fig. 3. The syntax of Π.

These patterns would also provide controlled versions of single qubit quantum gates if we managed to express them. To that end, we use the insight that, by the Euler decomposition, single qubit quantum gates can be expressed as a product $\phi \cdot PQP'$, where ϕ is a phase, P and P' are rotations in one basis, and Q is a rotation in a complementary basis. Thus, the categorical framework "only" needs to express phase gates in two complementary bases such as the canonical Z and X bases; it turns out that this is relatively straightforward once the framework includes roots of unity and a square root of $\sigma_{\oplus}$. Each root of unity ω directly provides phase gate $\mathrm{id} \oplus \omega$ in the Z-basis; phase gates in the X-basis are obtained by the change of basis induced by H which itself can be defined using roots of unity and the square root of $\sigma_{\oplus}$ (cf. Fig. 8). The technical challenge is that square roots are not unique, so for example postulating some V such that $\mathsf{V} \circ \mathsf{V} = \sigma_{\oplus}$ is not sufficient to determine V. Axiom (E_3), however, is sufficient to completely determine all the required square roots. The final product is an equational theory that provides (formalisable) proofs for circuit equivalences that only require a modest extension of conventional categorical reasoning.

4 A UNIVERSAL QUANTUM LANGUAGE: $\sqrt{\Pi}$

We present the syntax of $\sqrt{\Pi}$, whose underlying language is the classical reversible language Π that is universal for reversible computing over finite types and whose semantics is expressed in the rig groupoid of finite sets and bijections [James and Sabry 2012] . After reviewing the design of Π we introduce the extension $\sqrt{\Pi}$.

4.1 The Core Language: Π

In reversible boolean circuits, the number of input bits matches the number of output bits. Thus, a key insight for a programming language of reversible circuits is to ensure that each primitive operation preserves the number of bits, which is just a natural number. The algebraic structure of natural numbers as the free commutative semiring (or, commutative rig), with $(0, +)$ for addition, and $(1, \times)$ for multiplication then provides sequential, vertical, and horizontal circuit composition. Generalising these ideas, a typed programming language for reversible computing should ensure that every primitive expresses an isomorphism of finite types, *i.e.*, a permutation.

The syntax of the language Π, shown in Fig. 3, captures this concept. Type expressions b are built from the empty type ($\mathbb{0}$), the unit type ($\mathbb{1}$), the sum type ($+$), and the product type ($\times$). A type isomorphism $c : b_1 \leftrightarrow b_2$ models a reversible circuit that permutes the values in b_1 and b_2. These type isomorphisms are built from the primitive identities *iso* and their compositions. The Π-isomorphisms are not ad hoc: they correspond exactly to the laws of a *rig* operationalised into invertible transformations [Carette, James, et al. 2022; Carette and Sabry 2016] which have the types in Fig. 4. Each line in the top part of the figure has the pattern $c_1 : b_1 \leftrightarrow b_2 : c_2$ where c_1 and c_2 are self-duals; c_1 has type $b_1 \leftrightarrow b_2$ and c_2 has type $b_2 \leftrightarrow b_1$.

$$
\begin{array}{rcrcll}
id & : & b & \leftrightarrow & b & : id \\
swap^{+} & : & b_1 + b_2 & \leftrightarrow & b_2 + b_1 & : swap^{+} \\
assocr^{+} & : & (b_1 + b_2) + b_3 & \leftrightarrow & b_1 + (b_2 + b_3) & : assocl^{+} \\
unite^{+}l & : & \mathbb{0} + b & \leftrightarrow & b & : uniti^{+}l \\
swap^{\times} & : & b_1 \times b_2 & \leftrightarrow & b_2 \times b_1 & : swap^{\times} \\
assocr^{\times} & : & (b_1 \times b_2) \times b_3 & \leftrightarrow & b_1 \times (b_2 \times b_3) & : assocl^{\times} \\
unite^{\times}l & : & \mathbb{1} \times b & \leftrightarrow & b & : uniti^{\times}l \\
dist & : & (b_1 + b_2) \times b_3 & \leftrightarrow & (b_1 \times b_3) + (b_2 \times b_3) & : factor \\
absorbl & : & b \times \mathbb{0} & \leftrightarrow & \mathbb{0} & : factorzr
\end{array}
$$

$$
\frac{c_1 : b_1 \leftrightarrow b_2 \quad c_2 : b_2 \leftrightarrow b_3}{c_1 \fatsemi c_2 : b_1 \leftrightarrow b_3}
\qquad
\frac{c_1 : b_1 \leftrightarrow b_3 \quad c_2 : b_2 \leftrightarrow b_4}{c_1 + c_2 : b_1 + b_2 \leftrightarrow b_3 + b_4}
\qquad
\frac{c_1 : b_1 \leftrightarrow b_3 \quad c_2 : b_2 \leftrightarrow b_4}{c_1 \times c_2 : b_1 \times b_2 \leftrightarrow b_3 \times b_4}
$$

Fig. 4. Types for Π combinators

$$
\begin{aligned}
\textsc{ctrl}\ c &= dist \fatsemi id + (id \times c) \fatsemi factor \\
1 : \mathbb{1} \leftrightarrow \mathbb{1} &= id \\
\textsc{x} : \mathbb{2} \leftrightarrow \mathbb{2} &= swap^{+} \\
\textsc{cx} : \mathbb{2} \times \mathbb{2} \leftrightarrow \mathbb{2} \times \mathbb{2} &= \textsc{ctrl}\ swap^{+} \\
\textsc{ccx} : \mathbb{2} \times \mathbb{2} \times \mathbb{2} \leftrightarrow \mathbb{2} \times \mathbb{2} \times \mathbb{2} &= \textsc{ctrl}\ \textsc{cx}
\end{aligned}
$$

Fig. 5. Derived Π constructs.

The instance of *id* at type $\mathbb{1} \leftrightarrow \mathbb{1}$ plays an important role as it will induce *scalars*; it is given the distinguished name 1 when used as a scalar value. To see how this language expresses reversible circuits, we first define types that describe sequences of booleans ($\mathbb{2}^n$). We use the type $\mathbb{2} = \mathbb{1} + \mathbb{1}$ to represent booleans with the left injection representing `false` and the right injection representing `true`. Boolean negation (the X-gate) is straightforward to define using the primitive combinator $swap^{+}$. We can represent n-bit words using an n-ary product of boolean values. To express the CX- and CCX-gates we need to encode a notion of conditional expression. Such conditionals turn out to be expressible using the distributivity and factoring identities of rigs as shown in Fig. 5. An input value of type $\mathbb{2} \times b$ is processed by the *dist* operator, which converts it into a value of type $(\mathbb{1} \times b) + (\mathbb{1} \times b)$. Only in the right branch, which corresponds to the case when the boolean is `true`, is the combinator c applied to the value of type b. The inverse of *dist*, namely *factor* is applied to get the final result. Using this conditional, CX is defined as CTRL X and the Toffoli CCX gate is defined as CTRL CX. Because Π can express the Toffoli gate and can generate ancilla values of type $\mathbb{1}$ as needed, it is universal for classical reversible circuits.

Theorem 2 (Π Expressivity). *Π is universal for classical reversible circuits, i.e., boolean bijections $\mathbb{2}^n \to \mathbb{2}^n$ (for any natural number n).*

4.2 Classical Completeness

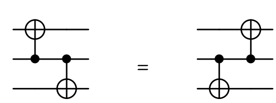
A crucial fact for the rest of the paper is the existence of an equational theory for Π that is sound and complete for the permutation semantics. The equations for the theory were collected in a second level of Π syntax as level-2 combinators [Carette and Sabry 2016]. Each level-2 combinator is of the form $c_1 \leftrightarrow_2 c_2$ for appropriate c_1 and c_2 of the same type $b_1 \leftrightarrow b_2$ and asserts that c_1

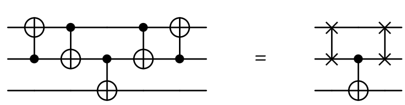
and c_2 denote the same bijection. For example, among the large number of equations, we have the following level-2 combinators dealing with associativity:

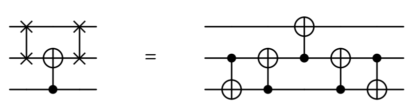
```
assoc⨾l  : c₁ ⨾ (c₂ ⨾ c₃) ↔₂ (c₁ ⨾ c₂) ⨾ c₃
assoc⨾r  : ((c₁ ⨾ c₂) ⨾ c₃) ↔₂ (c₁ ⨾ (c₂ ⨾ c₃))
assocl+l : ((c₁ + (c₂ + c₃)) ⨾ assocl₊) ↔₂ (assocl₊ ⨾ ((c₁ + c₂) + c₃))
assocl+r : (assocl₊ ⨾ ((c₁ + c₂) + c₃)) ↔₂ ((c₁ + (c₂ + c₃)) ⨾ assocl₊)
```

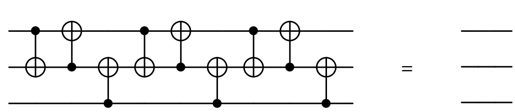
Theorem 3 (Π Full Abstraction and Adequacy [Choudhury et al. 2022]). *The equational theory of Π expressed using the level-2 combinators $\leftrightarrow_2$ is sound and complete with respect to its semantics in the weak symmetric rig groupoid of finite sets and permutations.*

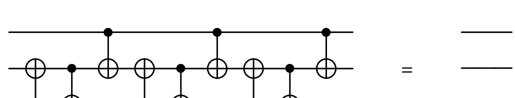
As a consequence, we may use any classical reversible circuit identity (*i.e.*, any identity involving only rig terms in the category of finite sets and permutations) without explicit proof, as such a proof can be reconstructed using the theorem above. In particular, we will freely use the classical identities below involving various combinations of CX and SWAP gates (which can all be straightforwardly verified by explicit computation):

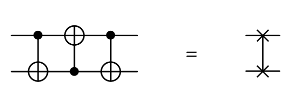

(P1)


(P2)


(P3)


(P4)


(P5)


(P6)

4.3 Adding Square Roots

The remarkable fact is that all it takes for a programming language to be universal for quantum computing with a sound and complete equational theory is the modest extension to Π in Fig. 6.

The extension consists of a square root v of x and an 8^{th} root w of the identity combinator 1. To maintain reversibility, we add not just these square roots but their inverses vi and wi as well. The semantics of the new combinators is partially specified by Eqs. (E1) and (E2). From these equations

Syntax

$$iso ::= \cdots \mid \textsc{v} \mid \textsc{vi} \mid \textsc{w} \mid \textsc{wi} \qquad \text{(isomorphisms)}$$

Types

$$\begin{array}{ccccccc} \textsc{v} & : & \mathbb{2} & \leftrightarrow & \mathbb{2} & : & \textsc{vi} \\ \textsc{w} & : & 1 & \leftrightarrow & 1 & : & \textsc{wi} \end{array}$$

Equations

(E1) $\textsc{v}^2 \leftrightarrow_2 \textsc{x}$
(E2) $\textsc{w}^8 \leftrightarrow_2 1$
(E3) $\textsc{v} \fatsemi (id + \textsc{w}^2) \fatsemi \textsc{v} \leftrightarrow_2 \mathit{uniti}^{\times}l \fatsemi \textsc{w}^2 \times ((id + \textsc{w}^2) \fatsemi \textsc{v} \fatsemi (id + \textsc{w}^2)) \fatsemi \mathit{unite}^{\times}l$

Fig. 6. The $\sqrt{\Pi}$ extension of Π.

and the original level-2 combinators, we can derive properties of the inverses, *e.g.*:

$$\begin{array}{rcll} \textsc{x} & \leftrightarrow_2 & \textsc{v} \fatsemi \textsc{v} & \text{(by 2-reversibility)} \\ \textsc{vi} \fatsemi \textsc{x} \fatsemi \textsc{x} & \leftrightarrow_2 & \textsc{vi} \fatsemi \textsc{v} \fatsemi \textsc{v} \fatsemi \textsc{x} & \text{(by compatibility)} \\ \textsc{vi} & \leftrightarrow_2 & \textsc{v} \fatsemi \textsc{x} & \text{(by inverses and unit)} \\ \\ 1 & \leftrightarrow_2 & \textsc{w}^8 & \text{(by 2-reversibility)} \\ \textsc{wi} \fatsemi 1 & \leftrightarrow_2 & \textsc{wi} \fatsemi \textsc{w}^8 & \text{(by compatibility)} \\ \textsc{wi} & \leftrightarrow_2 & \textsc{w}^7 & \text{(by inverses and unit)} \end{array}$$

As discussed earlier, Eqs. (E1) and (E2) do not completely determine the meaning of the new combinators, however. In particular, they do not exclude the trivial square root $\textsc{w} = 1$. To get a non-trivial semantics, we also impose Eq. (E3).

5 DENOTATIONAL SEMANTICS

By design, Π has a natural model in *rig groupoids* [Carette and Sabry 2016; Choudhury et al. 2022]. Indeed, every atomic isomorphism of Π corresponds to a coherence isomorphism in a rig category, while sequencing corresponds to composition, and the two parallel compositions are handled by the two monoidal structures. Inversion corresponds to the canonical dagger structure of groupoids. This interpretation is summarised in the top part of Fig. 7.

5.1 Postulating Square Roots

We will postulate the existence of certain square roots to a rig groupoid to obtain models of $\sqrt{\Pi}$. Ideally, there would be a universal categorical construction that formally adjoins nth roots of specified (endo)morphisms to a given (rig) category. The traditional way in commutative algebra to adjoin a square root of r to a ring R is to first move to the polynomial ring $R[x]$ in one variable x, and then to quotient out the ideal generated by $x^2 - r$ to force $x^2 = r$. This method is fraught with problems in the categorical case, because there is no analogue of the polynomial ring, no good analogue of quotients by ideals, and because it only works for endomorphisms.

Another way to formally adjoin a square root of $A \xrightarrow{f} B$ is to add a new object and two new morphisms $A \xrightarrow{{}^{1/2}f} \bullet \xrightarrow{f^{1/2}} B$, to take the free category on the resulting directed graph, and then quotient out composition that already existed in the base category, as well as quotienting out $f \sim f^{1/2} \circ {}^{1/2}f$. This does work in arbitrary categories, satisfies a universal property, and can be applied to arbitrary sets of morphisms f simultaneously. The new square roots automatically

Types

$$
\begin{array}{rcl@{\qquad}rcl}
[\![\mathbb{0}]\!] & = & O & [\![\mathbb{1}]\!] & = & I \\
[\![b_1 + b_2]\!] & = & [\![b_1]\!] \oplus [\![b_2]\!] & [\![b_1 \times b_2]\!] & = & [\![b_1]\!] \otimes [\![b_2]\!]
\end{array}
$$

Π Terms

$$
\begin{array}{rcl@{\qquad}rcl}
[\![id]\!] & = & \mathrm{id} & [\![c_1 \fatsemi c_2]\!] & = & [\![c_2]\!] \circ [\![c_1]\!] \\
[\![c_1 + c_2]\!] & = & [\![c_1]\!] \oplus [\![c_2]\!] & [\![c_1 \times c_2]\!] & = & [\![c_1]\!] \otimes [\![c_2]\!] \\
\\
[\![assocr^{+}]\!] & = & \alpha_{\oplus} & [\![assocl^{+}]\!] & = & \alpha_{\oplus}^{-1} \\
[\![uniti^{+}l]\!] & = & \lambda_{\oplus}^{-1} & [\![unite^{+}l]\!] & = & \lambda_{\oplus} \\
[\![assocr^{\times}]\!] & = & \alpha_{\otimes} & [\![assocl^{\times}]\!] & = & \alpha_{\otimes}^{-1} \\
[\![uniti^{\times}l]\!] & = & \lambda_{\otimes}^{-1} & [\![unite^{\times}l]\!] & = & \lambda_{\otimes} \\
[\![swap^{+}]\!] & = & \sigma_{\oplus} & [\![swap^{\times}]\!] & = & \sigma_{\otimes} \\
[\![dist]\!] & = & \delta_R & [\![factor]\!] & = & \delta_R^{-1} \\
[\![absorbl]\!] & = & \delta_0 & [\![factorzr]\!] & = & \delta_0^{-1}
\end{array}
$$

$\sqrt{\Pi}$ Terms

$$
\begin{array}{rcl@{\qquad}rcl}
[\![\mathrm{W}]\!] & = & \omega & [\![\mathrm{WI}]\!] & = & \omega^7 \\
[\![\mathrm{V}]\!] & = & \mathsf{V} & [\![\mathrm{VI}]\!] & = & \mathsf{V}^3
\end{array}
$$

Fig. 7. Semantics of Π in rig groupoids $(\mathbf{C}, \otimes, \oplus, O, I)$ and of $\sqrt{\Pi}$ in models of $\sqrt{\Pi}$.

interact well with inverses in groupoids. However, to respect rig structure we would have to take free combinations of $\oplus$ and $\otimes$, and the benefit of the universal property would be lost to bureaucracy.

Instead of pursuing general constructions, we will therefore simply postulate what we need of a categorical model. It will be clear that at least one model exists.

Definition 4. Given a scalar $s : I \to I$ and a morphism $f : X \to Y$, define the *scalar multiplication* of f by s on the left, written $s \bullet f$, as $\lambda_{\otimes} \circ s \otimes f \circ \lambda_{\otimes}^{-1} : X \to Y$. One similarly defines scalar multiplication on the right, $f \bullet s$, by replacing left unitors in the above by right unitors.

Definition 5. A *model of* $\sqrt{\Pi}$ consists of a rig category $(\mathbf{C}, \otimes, \oplus, O, I)$ equipped with maps $\omega : I \to I$ and $\mathsf{V} : I \oplus I \to I \oplus I$ satisfying the equations:

(E1) $\omega^8 = \mathrm{id}$,
(E2) $\mathsf{V}^2 = \sigma_{\oplus}$,
(E3) $\mathsf{V} \circ \mathsf{S} \circ \mathsf{V} = \omega^2 \bullet \mathsf{S} \circ \mathsf{V} \circ \mathsf{S}$

where $\mathsf{S} : I \oplus I \to I \oplus I$ is given by $\mathsf{S} = \mathrm{id} \oplus \omega^2$.

This model is strong enough to express the standard gate set of Clifford+T. It is not a minimal universal model, however: for example, the (computationally universal) gate set of Gaussian Clifford+T only requires a fourth root of unity, *i.e.*, the use of $\omega : I \to I$ with $\omega^8 = \mathrm{id}$ can be replaced by $i : I \to I$ with $i^4 = \mathrm{id}$ while still retaining computational universality.

Proposition 6. *The rig groupoid* **Unitary** *of finite-dimensional Hilbert spaces and unitaries is a model of* $\sqrt{\Pi}$.

Proof. Choosing $\omega = \exp(i\pi/4)$ and $\mathsf{V} = \mathsf{H}\left(\begin{smallmatrix} -1 & 0 \\ 0 & i \end{smallmatrix}\right)\mathsf{H}$ (with H the usual Hadamard gate, *i.e.*, $\mathsf{H} = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$), it is verified by straightforward calculation that the three equations are satisfied. □

Name	Signature	Meaning
i	$I \to I$	ω^2
-1	$I \to I$	ω^4
$-i$	$I \to I$	ω^6
X	$I \oplus I \to I \oplus I$	$\sigma_\oplus$
$P(s)$	$I \oplus I \to I \oplus I$ (for $s : I \to I$)	$\mathrm{id} \oplus s$
Z	$I \oplus I \to I \oplus I$	$P(-1)$
S	$I \oplus I \to I \oplus I$	$P(i)$
T	$I \oplus I \to I \oplus I$	$P(\omega)$
H	$I \oplus I \to I \oplus I$	$\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}$
K	$I \oplus I \to I \oplus I$	$\omega^{-1} \bullet \mathsf{H}$
$\mathsf{Midswap}$	$(A \oplus B) \oplus (C \oplus D) \to (A \oplus C) \oplus (B \oplus D)$	$\alpha_\oplus^{-1} \circ (\mathrm{id} \oplus \alpha_\oplus) \circ (\mathrm{id} \oplus (\sigma_\oplus \oplus \mathrm{id})) \circ (\mathrm{id} \oplus \alpha_\oplus^{-1}) \circ \alpha_\oplus$
Mat	$(I \oplus I) \otimes A \to A \oplus A$	$\lambda_\otimes \oplus \lambda_\otimes \circ \delta_R$
$\mathsf{Ctrl}\ m$	$(I \oplus I) \otimes A \to (I \oplus I) \otimes A$ given $m : A \to A$	$\mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus m) \circ \mathsf{Mat}$
$\mathsf{nCtrl}\ m$	$(I \oplus I) \otimes A \to (I \oplus I) \otimes A$ given $m : A \to A$	$\mathsf{Mat}^{-1} \circ (m \oplus \mathrm{id}) \circ \mathsf{Mat}$
SWAP	$(I \oplus I) \otimes (I \oplus I) \to (I \oplus I) \otimes (I \oplus I)$	$\sigma_\otimes$
CX	$(I \oplus I) \otimes (I \oplus I) \to (I \oplus I) \otimes (I \oplus I)$	$\mathsf{Ctrl}\ \mathsf{X}$
CZ	$(I \oplus I) \otimes (I \oplus I) \to (I \oplus I) \otimes (I \oplus I)$	$\mathsf{Ctrl}\ \mathsf{Z}$
CCX	$(I\oplus I)\otimes((I\oplus I)\otimes(I\oplus I)) \to (I\oplus I)\otimes((I\oplus I)\otimes(I\oplus I))$	$\mathsf{Ctrl}\ \mathsf{CX}$

Fig. 8. Shorthands for some maps in models of $\sqrt{\Pi}$.

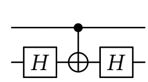
We will consider **Unitary** to be the standard model of $\sqrt{\Pi}$. A semantics of $\sqrt{\Pi}$ can, more generally, be given in any model satisfying Def. 5 by interpreting all the "classical" morphisms as in Π, and additionally interpreting the additional combinators as shown at the bottom of Fig. 7.

Definition 7 (Models). We use $[\![-]\!]$ to denote the interpretation of a $\sqrt{\Pi}$ term in an arbitrary model of $\sqrt{\Pi}$, and $(\!|-|\!)$ to denote its interpretation in the standard model **Unitary**.

In this way, given $\sqrt{\Pi}$ terms c_1 and c_2, we can only ever establish $[\![c_1]\!] = [\![c_2]\!]$ if this holds from the axioms of models of $\sqrt{\Pi}$ alone. On the other hand, we can establish $(\!|c_1|\!) = (\!|c_2|\!)$ by any means sound for unitaries (*e.g.*, matrix computation, circuit rewriting rules, ZX-calculus derivations, etc.).

5.2 Representing Quantum Gates

Let $(\mathbf{C}, \otimes, \oplus, O, I)$ be a model of $\sqrt{\Pi}$. We demonstrate that, in any such model, all the familiar quantum gates can be represented *internally* as shown in Fig. 8. We can combine these gates into circuits using the tensor product and composition as usual. For example, the circuit



is represented by the morphism $\mathrm{id} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathrm{id} \otimes \mathsf{H}$ in a model of $\sqrt{\Pi}$. Besides familiar gates, Fig. 8 also defines the convenient map Mat which is so named because it can be seen as a way to construct maps from *matrix representations*. This powerful technique was implicitly used in the definition of Ctrl-gates in Sec. 3.2. More generally, we think of g as an *abstract block matrix representation* of f when $g \circ \mathsf{Mat} = \mathsf{Mat} \circ f$, as this means in turn that $\mathsf{Mat}^{-1} \circ g \circ \mathsf{Mat} = f$.

It is straightforward to confirm that the internal gates correspond to their usual definitions in **Unitary**, the standard model of $\sqrt{\Pi}$. Here, we focus on properties that are valid in every model.

We begin by establishing some basic facts about *scalars* (morphisms $I \longrightarrow I$) in a rig (or, more generally, monoidal) category.

Proposition 8. *Let s and t be scalars and f and g be morphisms.*

(i) $s \circ t = t \circ s$,
(ii) *if* $s^2 = t$ *then* $s^{-1} = t^{-1} \circ s$
(iii) $s \bullet f = f \bullet s$
(iv) $1 \bullet f = f$,
(v) $s \bullet (t \bullet f) = (s \circ t) \bullet f$,
(vi) $s \bullet (f \oplus g) = (s \bullet f) \oplus (s \bullet g)$,
(vii) $s \bullet (g \circ f) = (s \bullet g) \circ f$,
(viii) $s \bullet (g \circ f) = g \circ (s \bullet f)$.

Proof. All but the second property are shown in the literature, *e.g.*, [Heunen and Vicary 2019]. For (ii), we see that $t^{-1} \circ s \circ s = t^{-1} \circ t = \mathrm{id}_I$ and $s \circ t^{-1} \circ s = t^{-1} \circ s \circ s = t^{-1} \circ t = \mathrm{id}_I$ using commutativity of scalars, so $s^{-1} = t^{-1} \circ s$ follows by unicity of inverses. □

The next three lemmas establish basic properties of the internal gates and scalars; the straightforward but tedious proofs are collected in Appendix A.

Lemma 9. *Let s and t be scalars.*

(i) $-1^2 = \mathrm{id}$ *and* $i^2 = -1$,
(ii) $\mathsf{X}^2 = \mathrm{id}$,
(iii) $\mathsf{P}(s)^2 = \mathsf{P}(s^2)$,
(iv) $\mathsf{P}(s)^{-1} = \mathsf{P}(s^{-1})$,
(v) $\mathsf{P}(s) \circ \mathsf{P}(t) = \mathsf{P}(s \circ t) = \mathsf{P}(t) \circ \mathsf{P}(s)$,
(vi) $\mathsf{P}(s) \circ \mathsf{X} \circ \mathsf{P}(s) = s \bullet \mathsf{X}$,
(vii) $\mathsf{X} \circ \mathsf{V} = \mathsf{V} \circ \mathsf{X}$,
(viii) $\mathsf{CX}^2 = \mathrm{id}$,
(ix) $\mathsf{CZ}^2 = \mathrm{id}$,
(x) $\mathsf{CCX}^2 = \mathrm{id}$,
(xi) $\mathsf{X} \circ \mathsf{P}(s) = s \bullet \mathsf{P}(s^{-1}) \circ \mathsf{X}$.

Lemma 10. *Let $f : X \longrightarrow Y$, $g : X \longrightarrow X$, and $h : X \longrightarrow X$ be maps, and s and t be scalars. Then:*

(i) $\mathsf{Mat} \circ (\mathrm{id}_{I \oplus I} \otimes f) = (f \oplus f) \circ \mathsf{Mat}$,
(ii) $\mathsf{Mat} \circ \mathsf{SWAP} = \mathsf{Midswap} \circ \mathsf{Mat}$,
(iii) $\mathsf{SWAP} \circ \mathsf{Mat}^{-1} = \mathsf{Mat}^{-1} \circ \mathsf{Midswap}$,
(iv) $\mathsf{Mat} \circ (f \otimes \mathrm{id}_{I \oplus I}) = \mathsf{Midswap} \circ (f \oplus f) \circ \mathsf{Midswap} \circ \mathsf{Mat}$,
(v) $\mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{P}(s) \circ \mathsf{SWAP} = \mathsf{Ctrl}\ \mathsf{P}(s)$,
(vi) $\mathsf{Ctrl}\ \mathsf{P}(s) \circ \mathsf{Ctrl}\ \mathsf{P}(t) = \mathsf{Ctrl}\ \mathsf{P}(t) \circ \mathsf{Ctrl}\ \mathsf{P}(s)$,
(vii) $\mathsf{Ctrl}\ \mathsf{P}(s) \circ (\mathrm{id}_{I \oplus I} \otimes \mathsf{P}(t)) = (\mathrm{id}_{I \oplus I} \otimes \mathsf{P}(t)) \circ \mathsf{Ctrl}\ \mathsf{P}(s)$,
(viii) $\mathsf{Mat} \circ (\mathsf{X} \otimes \mathrm{id}_{I \oplus I}) = \sigma_\oplus \circ \mathsf{Mat}$,
(ix) $\mathsf{Mat} \circ (\mathsf{P}(s) \otimes \mathrm{id}_{I \oplus I}) = (\mathrm{id}_{I \oplus I} \oplus (s \bullet \mathrm{id})) \circ \mathsf{Mat}$.
(x) $\mathsf{Ctrl}\ g \circ \mathsf{Ctrl}\ h = \mathsf{Ctrl}(g \circ h)$

Lemma 11. *Any model of* $\sqrt{\Pi}$ *satisfies* $\mathsf{H} \circ \mathsf{X} \circ \mathsf{H} = \mathsf{Z}$ *and* $\mathsf{H} \circ \mathsf{Z} \circ \mathsf{H} = \mathsf{X}$.

6 SOUNDNESS AND COMPLETENESS

We present our main technical development: $\sqrt{\Pi}$ is *equationally sound and complete* for a variety of gate sets, including the computationally universal *Gaussian Clifford+T* [Amy et al. 2020]. This is

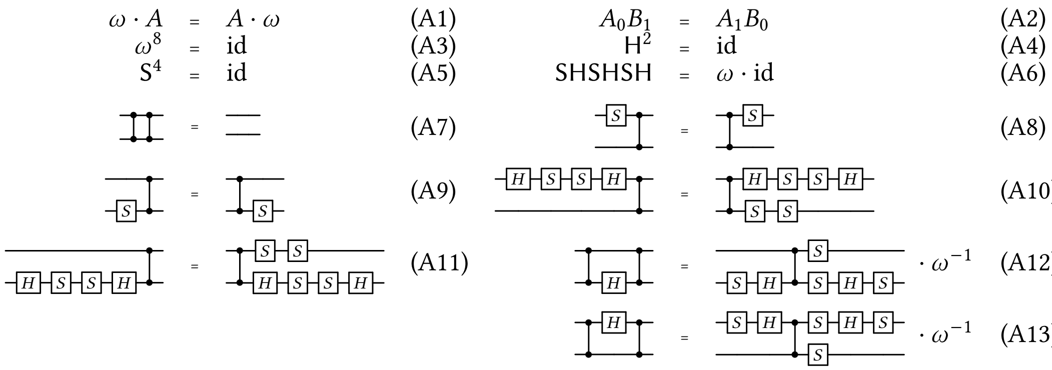


Fig. 9. A sound and complete equational theory of ≤ 2-qubit Clifford circuits due to Selinger [2015]. What we call (A3)–(A13) refer to relations (C1)–(C11) in the original paper by Selinger [2015] (equations (A1) and (A2) become relevant once we consider ≤ 2-qubit Clifford+T circuits [Bian and Selinger 2022]). Note that we swap the order of (A12) and (A13) compared to the original presentation by Selinger [2015].

expressed in terms of a series of *full abstraction* results, showing that fragments of $\sqrt{\Pi}$ are fully abstract for certain classes of unitaries.

To our knowledge, this is the first presentation of a computationally universal quantum programming language with a sound and complete equational theory.

6.1 ≤ 2-qubit Clifford Circuits

We begin by proving that models of $\sqrt{\Pi}$ satisfy the sound and complete equational theory of ≤ 2-qubit Clifford circuits shown in Fig. 9. Clifford circuits are those which can be formed using the gates $\{\mathsf{CZ}, \mathsf{S}, \mathsf{H}\}$ and the scalar $\omega = e^{i\pi/4}$.

Definition 12. In a model of $\sqrt{\Pi}$, a *representation of a Clifford circuit* is any morphism which can be written in terms of morphisms from the sets $\{\omega, \mathsf{S}, \mathsf{H}, \mathsf{CZ}\}$ and $\{\alpha_\otimes, \alpha_\otimes^{-1}, \lambda_\otimes, \lambda_\otimes^{-1}, \rho_\otimes, \rho_\otimes^{-1}, \sigma_\otimes\}$, composed arbitrarily in parallel (using ⊗) and in sequence (using ∘). A representation of a ≤ 2-qubit Clifford circuit is one with signature $I \oplus I \longrightarrow I \oplus I$ or $(I \oplus I) \otimes (I \oplus I) \longrightarrow (I \oplus I) \otimes (I \oplus I)$.

Note that this definition permits both scalar multiplication by powers of ω (since this is formulated using the coherence isomorphisms) and use of the SWAP gate (since this is precisely $\sigma_\otimes$). This result relies on the generators and relations for Clifford circuits due to Selinger [2015], which we prove are all satisfied in any model of $\sqrt{\Pi}$:

(A1) $\omega \bullet f = f \bullet \omega$ for all f follows by Prop. 8 (iii).
(A2) That $(f \otimes \mathrm{id}) \circ (\mathrm{id} \otimes g) = (\mathrm{id} \otimes g) \circ (f \otimes \mathrm{id})$ follows by bifunctoriality of ⊗.
(A3) $\omega^8 = \mathrm{id}$ follows immediately by (E1).
(A4) We derive

$$
\begin{aligned}
\mathsf{H} \circ \mathsf{H} &= (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) \circ (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(def. H)} \\
&= \omega^2 \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && \text{(Prop. 8)} \\
&= \omega^2 \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && (\mathsf{X}^2 = \mathrm{id}) \\
&= \omega^2 \bullet \mathsf{X} \circ (\omega^{-2} \bullet \mathsf{V} \circ \mathsf{S} \circ \mathsf{V}) \circ (\omega^{-2} \bullet \mathsf{V} \circ \mathsf{S} \circ \mathsf{V}) \circ \mathsf{X} && (E3) \\
&= \omega^{-2} \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} && \text{(Prop. 8)}
\end{aligned}
$$

$$
\begin{aligned}
&= \omega^{-2} \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} && (E2)\\
&= \omega^{-2} \bullet \mathsf{X} \circ \mathsf{V} \circ (\omega^{2} \bullet \mathsf{X}) \circ \mathsf{V} \circ \mathsf{X} && \text{(Lem. 9 (vi))}\\
&= \mathsf{X} \circ \mathsf{V} \circ \mathsf{X} \circ \mathsf{V} \circ \mathsf{X} && \text{(Prop. 8)}\\
&= \mathsf{X} \circ \mathsf{X} \circ \mathsf{V} \circ \mathsf{V} \circ \mathsf{X} && \text{(Lem. 9 (vii))}\\
&= \mathsf{X} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{X} && (E2)\\
&= \mathrm{id} && (\mathsf{X}^2 = \mathrm{id})
\end{aligned}
$$

(A5) $\mathsf{S}^4 = (\mathrm{id} \oplus i)^4 = (\mathrm{id} \oplus \omega^2)^4 = \mathrm{id}^4 \oplus \omega^8 = \mathrm{id} \oplus \mathrm{id} = \mathrm{id}$ by bifunctoriality and (E1).

(A6) We compute

$$
\begin{aligned}
(\mathsf{S} \circ \mathsf{H})^3 &= (\mathsf{S} \circ (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}))^3 && \text{(def. H)}\\
&= (\omega \bullet \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X})^3 && \text{(Prop. 8)}\\
&= (\omega \bullet (\omega^2 \bullet \mathsf{X}) \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X})^3 && \text{(Lem. 9 (vi))}\\
&= (\omega^3 \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X})^3 && \text{(Prop. 8)}\\
&= (\omega^3 \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) \circ (\omega^3 \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) \circ (\omega^3 \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(expand)}\\
&= \omega^9 \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && \text{(Prop. 8)}\\
&= \omega \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && ((E1), \mathsf{X}^2 = \mathrm{id})\\
&= \omega \bullet \mathsf{X} \circ (\omega^2 \bullet \mathsf{S} \circ \mathsf{V} \circ \mathsf{S}) \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && (E3)\\
&= \omega^3 \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && \text{(Prop. 8)}\\
&= \omega^3 \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && (\mathsf{X}^2 = \mathrm{id})\\
&= \omega \bullet (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) \circ (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(Prop. 8)}\\
&= \omega \bullet (\mathsf{H} \circ \mathsf{H}) && \text{(def. H)}\\
&= \omega \bullet \mathrm{id} && (A4)
\end{aligned}
$$

(A7) By Lem. 9 (ix).

(A8) We have

$$
\begin{aligned}
\mathrm{Ctrl}\,\mathsf{Z} \circ (\mathsf{S} \otimes \mathrm{id}) &= \mathsf{SWAP} \circ \mathrm{Ctrl}\,\mathsf{Z} \circ \mathsf{SWAP} \circ (\mathsf{S} \otimes \mathrm{id}) && \text{(Lem. 10 (v))}\\
&= \mathsf{SWAP} \circ \mathrm{Ctrl}\,\mathsf{Z} \circ (\mathrm{id} \otimes \mathsf{S}) \circ \mathsf{SWAP} && \text{(naturality SWAP)}\\
&= \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{S}) \circ \mathrm{Ctrl}\,\mathsf{Z} \circ \mathsf{SWAP} && \text{(Lem. 10}(vii))\\
&= (\mathsf{S} \otimes \mathrm{id}) \circ \mathsf{SWAP} \circ \mathrm{Ctrl}\,\mathsf{Z} \circ \mathsf{SWAP} && \text{(naturality SWAP)}\\
&= (\mathsf{S} \otimes \mathrm{id}) \circ \mathrm{Ctrl}\,\mathsf{Z} && \text{(Lem. 10 (v))}
\end{aligned}
$$

(A9) By Lem. 10 (v).

(A10) Since $\mathsf{S} \circ \mathsf{S} = \mathsf{Z}$ and $\mathsf{H} \circ \mathsf{S} \circ \mathsf{S} \circ \mathsf{H} = \mathsf{H} \circ \mathsf{Z} \circ \mathsf{H} = \mathsf{X}$ by Lems. 9 and 11, it suffices to show $\mathrm{Ctrl}\,\mathsf{Z} \circ (\mathsf{X} \otimes \mathrm{id}) = \mathsf{X} \otimes \mathsf{Z} \circ \mathrm{Ctrl}\,\mathsf{Z}$. This follows by

$$
\begin{aligned}
\mathrm{Ctrl}\,\mathsf{Z} \circ (\mathsf{X} \otimes \mathrm{id}) &= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \circ (\mathsf{X} \otimes \mathrm{id}) && \text{(def. Ctrl)}\\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \sigma_{\oplus} \circ \mathsf{Mat} && \text{(Lem. 10}(viii))\\
&= \mathsf{Mat}^{-1} \circ \sigma_{\oplus} \circ (\mathsf{Z} \oplus \mathrm{id}) \circ \mathsf{Mat} && (\text{naturality } \sigma_{\oplus})
\end{aligned}
$$

$$
\begin{aligned}
&= (\mathsf{X} \otimes \mathsf{id}) \circ \mathsf{Mat}^{-1} \circ (\mathsf{Z} \oplus \mathsf{id}) \circ \mathsf{Mat} && \text{(Lem. 10}(viii)\text{)} \\
&= (\mathsf{X} \otimes \mathsf{id}) \circ \mathsf{Mat}^{-1} \circ (\mathsf{Z} \oplus (\mathsf{Z} \circ \mathsf{Z})) \circ \mathsf{Mat} && (\mathsf{Z}^2 = \mathsf{id}) \\
&= (\mathsf{X} \otimes \mathsf{id}) \circ \mathsf{Mat}^{-1} \circ (\mathsf{Z} \oplus \mathsf{Z}) \circ (\mathsf{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus) \\
&= (\mathsf{X} \otimes \mathsf{id}) \circ (\mathsf{id} \otimes \mathsf{Z}) \circ \mathsf{Mat}^{-1} \circ (\mathsf{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} && \text{(Lem. 10}(i)\text{)} \\
&= (\mathsf{X} \otimes \mathsf{Z}) \circ \mathsf{Mat}^{-1} \circ (\mathsf{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} && \text{(bifunctoriality } \otimes) \\
&= \mathsf{X} \otimes \mathsf{Z} \circ \mathsf{Ctrl}\ \mathsf{Z} && \text{(def. Ctrl)}
\end{aligned}
$$

(A11) Similarly, since it has already been established that $\mathsf{H} \circ \mathsf{S} \circ \mathsf{S} \circ \mathsf{H} = \mathsf{X}$ and $\mathsf{S} \circ \mathsf{S} = \mathsf{Z}$, it suffices to show $\mathsf{Ctrl}\ \mathsf{Z} \circ (\mathsf{id} \otimes \mathsf{X}) = \mathsf{Z} \otimes \mathsf{X} \circ \mathsf{Ctrl}\ \mathsf{Z}$:

$$
\begin{aligned}
\mathsf{Ctrl}\ \mathsf{Z} \circ (\mathsf{id} \otimes \mathsf{X}) &= \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} \circ (\mathsf{id} \otimes \mathsf{X}) && \text{(Lem. 9}(v)\text{)} \\
&= \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ (\mathsf{X} \otimes \mathsf{id}) \circ \mathsf{SWAP} && \text{(naturality SWAP)} \\
&= \mathsf{SWAP} \circ \mathsf{X} \otimes \mathsf{Z} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} && (A10) \\
&= \mathsf{Z} \otimes \mathsf{X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} && \text{(naturality SWAP)} \\
&= \mathsf{Z} \otimes \mathsf{X} \circ \mathsf{Ctrl}\ \mathsf{Z} && \text{(Lem. 9}(v)\text{)}
\end{aligned}
$$

(A12) We defer the derivation of this identity to Appendix B.

(A13) This relation follows by the above since

$$
\begin{aligned}
&\omega^{-1} \bullet ((\mathsf{S} \circ \mathsf{H} \circ \mathsf{S}) \otimes \mathsf{S}) \circ \mathsf{Ctrl}\ \mathsf{Z} \circ ((\mathsf{H} \circ \mathsf{S}) \otimes \mathsf{id}) \\
&= \omega^{-1} \bullet ((\mathsf{S} \circ \mathsf{H} \circ \mathsf{S}) \otimes \mathsf{S}) \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} \circ ((\mathsf{H} \circ \mathsf{S}) \otimes \mathsf{id}) && \text{(Lem. 10 (v))} \\
&= \omega^{-1} \bullet \mathsf{SWAP} \circ (\mathsf{S} \otimes (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Ctrl}\ \mathsf{Z} \circ (\mathsf{id} \otimes (\mathsf{H} \circ \mathsf{S})) \circ \mathsf{SWAP} && \text{(naturality SWAP)} \\
&= \mathsf{SWAP} \circ (\omega^{-1} \bullet ((\mathsf{S} \otimes (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Ctrl}\ \mathsf{Z} \circ (\mathsf{id} \otimes (\mathsf{H} \circ \mathsf{S}))) \circ \mathsf{SWAP} && \text{(Prop. 8)} \\
&= \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ (\mathsf{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} && B \\
&= \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} \circ \mathsf{SWAP} \circ (\mathsf{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} && \text{(SWAP involutive)} \\
&= \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} \circ (\mathsf{H} \otimes \mathsf{id}) \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} && \text{(naturality SWAP)} \\
&= \mathsf{Ctrl}\ \mathsf{Z} \circ (\mathsf{H} \otimes \mathsf{id}) \circ \mathsf{Ctrl}\ \mathsf{Z} && \text{(Lem. 10 (v))}
\end{aligned}
$$

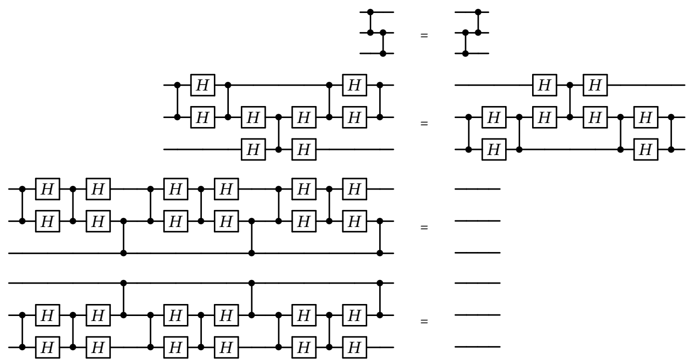
These derivations lead us, as a first step, to full abstraction for $\leq$ 2-qubit Clifford circuits.

THEOREM 13 (FULL ABSTRACTION FOR $\leq$ 2-QUBIT CLIFFORD). *Let c_1 and c_2 be $\sqrt{\Pi}$ terms representing Clifford circuits of at most two qubits. Then $[\![c_1]\!] = [\![c_2]\!]$ iff $(\!|c_1|\!) = (\!|c_2|\!)$.*

PROOF. The identities (A3)–(A13) are complete for $\leq$ 2-qubit Clifford circuits by [Selinger 2015, Prop. 7.1] (see Remark 7.2 regarding the special case of $\leq$ 2-qubit circuits), and have been shown above to hold in any model of $\sqrt{\Pi}$. ◻

6.2 *n*-qubit Clifford Circuits

To extend Thm. 13 to Clifford circuits with an arbitrary number of qubits, it suffices by a result of Selinger [2015] to prove just four identities (shown in Fig. 10). Interestingly, by showing that models of $\sqrt{\Pi}$ admit a few circuit rewriting rules and applying these, we will see that the heavy lifting of these four identities can be done entirely by *classical* reasoning. This lets us exploit the soundness and completeness of Π with respect to its permutation semantics, which greatly simplifies these proofs.



(B1)

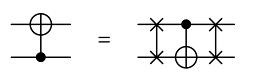
(B2)

(B3)

(B4)

Fig. 10. The 3-qubit identities of Clifford circuits due to Selinger [2015] which, together with (A3)–(A13) of Fig. 9, form a sound and complete equational theory of Clifford circuits.

Recall that we interpret controlled gates in $\sqrt{\Pi}$ using the Ctrl macro, such that, *e.g.*, a controlled-X gate  becomes Ctrl X. If we're interested in a controlled gate where the target line is above rather than below, we can simply conjugate it by a swap, *e.g.*,



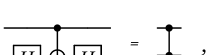
Thus a "bottom-controlled" X is interpreted in $\sqrt{\Pi}$ as SWAP ∘ Ctrl X ∘ SWAP. We first collect some useful additional properties of Ctrl X and Ctrl Z, with proofs located in Appendix B.

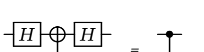
Lemma 14. *The following identities hold in any model of* $\sqrt{\Pi}$*:*

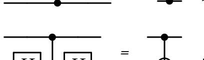
(i) id ⊗ H ∘ Ctrl X ∘ id ⊗ H = Ctrl Z,
(ii) H ⊗ id ∘ SWAP ∘ Ctrl X ∘ SWAP ∘ H ⊗ id = Ctrl Z,
(iii) id ⊗ H ∘ Ctrl Z ∘ id ⊗ H = Ctrl X,
(iv) H ⊗ id ∘ Ctrl Z ∘ H ⊗ id = SWAP ∘ Ctrl X ∘ SWAP,
(v) H ⊗ id ∘ Ctrl X ∘ H ⊗ id = id ⊗ H ∘ SWAP ∘ Ctrl X ∘ SWAP ∘ id ⊗ H

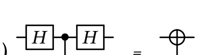
These have direct interpretations as circuit identities, which we will use to simplify (B1)–(B4).

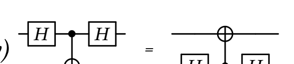
Corollary 15. *The following circuit identities hold in any model of* $\sqrt{\Pi}$*:*

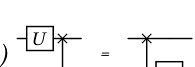
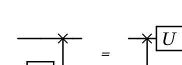
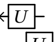
(i) 

(ii) 

(iii) 

(iv) 

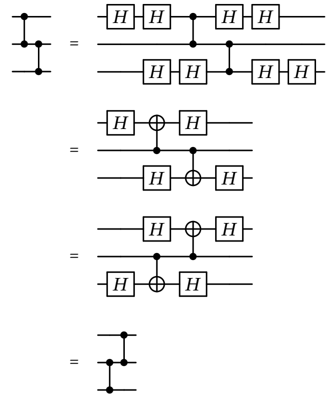
(v) 

(vi)  *and* 
for any gate  .

Proof. Points (i)–(v) hold by Lem. 14, while (vi) is naturality of SWAP. □

We can now tackle the four 3-qubit rules for Clifford circuits, named (C12)–(C15) in the presentation of Selinger [2015], which we call (B1)–(B4).

(B1) This rule is can be derived using the circuit identities and classical completeness.



(A4)

(Cor. 15)

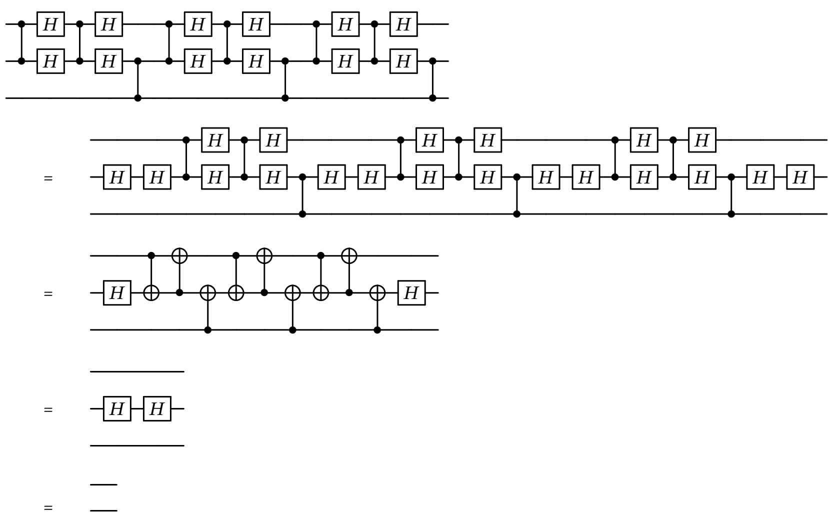
(P1)

(Cor. 15)

Notice how the essential argument of this proof is the classical identity (P1).

(B2) We defer the proof of this identity to Appendix B.

(B3) This identity and the next follow by reducing the circuit to one with a large classical subcircuit, which turns out (by classical completeness) to be the identity circuit.



(A4)

(Cor. 15)

(P4)

(A4)

(B4) We defer the proof of this identity to Appendix B.

From this follows an equational completeness result for Clifford circuits of arbitrary size.

Theorem 16 (Full abstraction for Clifford circuits). *Let c_1 and c_2 be $\sqrt{\Pi}$ terms representing Clifford circuits of arbitrary size. Then $[\![c_1]\!] = [\![c_2]\!]$ iff $(\!|c_1|\!) = (\!|c_2|\!)$.*

Proof. The identities (A3)–(A13) and (B1)–(B4) are complete for Clifford circuits of arbitrary size by Selinger [2015, Thm. 7.1], and have been shown above to hold in any model of $\sqrt{\Pi}$. □

6.3 $\leq$ 2-qubit Clifford+T

We extend Thm. 13 to show that models of $\sqrt{\Pi}$ are sound and complete for all $\leq$ 2-qubit Clifford+T circuits. We do this by showing the remaining identities of Bian and Selinger [2022] (see Fig. 11), which, together with (A1)–(A13) from Sec. 6.1, are equationally sound and complete for $\leq$ 2-qubit Clifford+T circuits. Recall that Clifford+T circuits are those which can be formed using the scalar ω

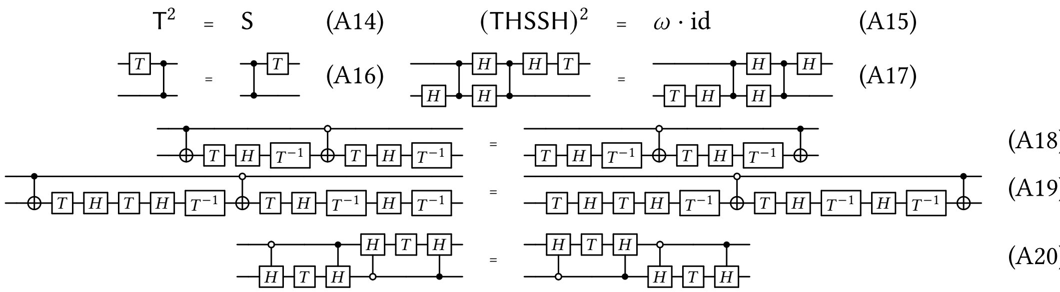


Fig. 11. The remaining identities which, along with (A1)–(A13) of Fig. 9, form a sound and complete equational theory of ≤ 2-qubit Clifford+T circuits [Bian and Selinger 2022].

and gates {S, H, CZ, T}. This leads us to the following definition of representations of Clifford+T circuits in models of $\sqrt{\Pi}$:

Definition 17. In a model of $\sqrt{\Pi}$, a *representation of a Clifford+T circuit* is any morphism which can be written in terms of morphisms from the sets $\{\omega, \mathsf{S}, \mathsf{H}, \mathsf{CZ}, \mathsf{T}\}$ and $\{\alpha_\otimes, \alpha_\otimes^{-1}, \lambda_\otimes, \lambda_\otimes^{-1}, \rho_\otimes, \rho_\otimes^{-1}, \sigma_\otimes\}$, composed arbitrarily in parallel (using $\otimes$) and in sequence (using $\circ$). A representation of a ≤ 2-qubit Clifford+T circuit is one with signature $I \oplus I \to I \oplus I$ or $(I \oplus I) \otimes (I \oplus I) \to (I \oplus I) \otimes (I \oplus I)$.

We start by showing an equivalence of representations of negatively controlled gates, as the definition of nCtrl in Fig. 8 may be considered non-standard. One usually thinks of a negatively controlled gate as a positively controlled one conjugated by X on the control line, and we show that our definition nCtrl is a convenient reduced form for stating this. Bian and Selinger [2022] uses yet another representation of negatively controlled X and H, which we also show to be equivalent.

Lemma 18 (Negative control). *Let $f : X \to X$ be a map in a rig category. Then*
(i) $\mathsf{nCtrl}\, f = \mathsf{X} \otimes \mathrm{id} \circ \mathsf{Ctrl}\, f \circ \mathsf{X} \otimes \mathrm{id}$,
(ii) $\mathsf{nCtrl}\, f = \mathsf{Ctrl}\, f \circ \mathrm{id} \otimes f$ *when f is involutive.*

Proof. We derive (i) by

$$
\begin{aligned}
&\mathsf{X} \otimes \mathrm{id} \circ \mathsf{Ctrl}\, f \circ \mathsf{X} \otimes \mathrm{id} \\
&\quad = \mathsf{X} \otimes \mathrm{id} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus f) \circ \mathsf{Mat} \circ \mathsf{X} \otimes \mathrm{id} && \text{(definition Ctrl)} \\
&\quad = \mathsf{Mat}^{-1} \circ \sigma_\oplus \circ (\mathrm{id} \oplus f) \circ \sigma_\oplus \circ \mathsf{Mat} && \text{(Lem. 10 (viii))} \\
&\quad = \mathsf{Mat}^{-1} \circ (f \oplus \mathrm{id}) \circ \sigma_\oplus \circ \sigma_\oplus \circ \mathsf{Mat} && \text{(naturality } \sigma_\oplus\text{)} \\
&\quad = \mathsf{Mat}^{-1} \circ (f \oplus \mathrm{id}) \circ \mathsf{Mat} && (\sigma_\oplus \text{ involutive}) \\
&\quad = \mathsf{nCtrl}\, f && \text{(definition nCtrl)}
\end{aligned}
$$

and we show (ii) by

$$
\begin{aligned}
\mathsf{Ctrl}\, f \circ (\mathrm{id} \otimes f) &= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus f) \circ \mathsf{Mat} \circ (\mathrm{id} \otimes f) && \text{(definition Ctrl)} \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus f) \circ (f \oplus f) \circ \mathsf{Mat} && \text{(Lem. 10 (i))} \\
&= \mathsf{Mat}^{-1} \circ (f \oplus (f \circ f)) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus\text{)} \\
&= \mathsf{Mat}^{-1} \circ (f \oplus \mathrm{id}) \circ \mathsf{Mat} && (f \text{ involutive}) \\
&= \mathsf{nCtrl}\, f && \text{(definition nCtrl)}
\end{aligned}
$$

□

We are now ready to derive the remaining identities.

(A14) By Lem. 9 and definition of S and T, $\mathsf{T}^2 = \mathsf{P}(\omega)^2 = \mathsf{P}(\omega^2) = \mathsf{S}$.

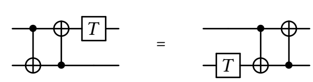
(A15) We derive

$$\begin{aligned}
(\mathsf{T} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{S} \circ \mathsf{H})^2 &= (\mathsf{T} \circ \mathsf{H} \circ \mathsf{Z} \circ \mathsf{H})^2 && (\mathsf{S}^2 = \mathsf{Z}) \\
&= (\mathsf{T} \circ \mathsf{X})^2 && (\text{Lem. } 11) \\
&= \mathsf{T} \circ \mathsf{X} \circ \mathsf{T} \circ \mathsf{X} && (\text{expand}) \\
&= (\omega \bullet \mathsf{X}) \circ \mathsf{X} && (\text{Lem. } 9) \\
&= \omega \bullet (\mathsf{X} \circ \mathsf{X}) && (\text{Prop. } 8) \\
&= \omega \bullet \mathrm{id} && (\mathsf{X}^2 = \mathrm{id})
\end{aligned}$$

(A16) This is a special case of commutativity of phase gates:

$$\begin{aligned}
\mathsf{Ctrl\ Z} \circ (\mathsf{T} \otimes \mathrm{id}) &= \mathsf{SWAP} \circ \mathsf{Ctrl\ Z} \circ \mathsf{SWAP} \circ (\mathsf{T} \otimes \mathrm{id}) && (\text{Lem. } 10) \\
&= \mathsf{SWAP} \circ \mathsf{Ctrl\ Z} \circ (\mathrm{id} \otimes \mathsf{T}) \circ \mathsf{SWAP} && (\text{naturality } \mathsf{SWAP}) \\
&= \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{T}) \circ \mathsf{Ctrl\ Z} \circ \mathsf{SWAP} && (\text{Lem. } 10) \\
&= (\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ Z} \circ \mathsf{SWAP} && (\text{naturality } \mathsf{SWAP}) \\
&= (\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{Ctrl\ Z} && (\text{Lem. } 10)
\end{aligned}$$

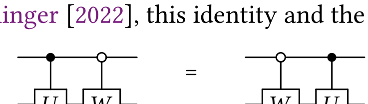
(A17) By first applying circuit identities from Cor. 15, this identity amounts to showing that



We then derive this:

$$\begin{aligned}
&(\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \\
&= (\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{Ctrl\ X} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} && ((\mathsf{Ctrl\ X})^2 = \mathrm{id}) \\
&= (\mathsf{T} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl\ Z} \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} && (\text{Lem. } 14) \\
&= (\mathrm{id} \otimes \mathsf{H}) \circ (\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{Ctrl\ Z} \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} && (\text{bifunctoriality } \oplus) \\
&= (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl\ Z} \circ (\mathsf{T} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} && (A16) \\
&= (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl\ Z} \circ (\mathrm{id} \otimes \mathsf{H}) \circ (\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} && (\text{bifunctoriality } \oplus) \\
&= \mathsf{Ctrl\ X} \circ (\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} && (\text{Lem. } 14) \\
&= \mathsf{Ctrl\ X} \circ (\mathsf{T} \otimes \mathrm{id}) \circ \mathsf{SWAP} && (P6) \\
&= \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{T}) && (\text{naturality } \mathsf{SWAP}) \\
&= \mathsf{Ctrl\ X} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ (\mathrm{id} \otimes \mathsf{T}) && (P6) \\
&= \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ \mathsf{SWAP} \circ \mathsf{Ctrl\ X} \circ (\mathrm{id} \otimes \mathsf{T}) && ((\mathsf{Ctrl\ X})^2 = \mathrm{id})
\end{aligned}$$

(A18) As noted by Bian and Selinger [2022], this identity and the next are both of the form



for some $U : I \oplus I \to I \oplus I$ and $W : I \oplus I \to I \oplus I$. This is because

$$\begin{aligned}
&\mathrm{id} \otimes g^{-1} \circ \mathsf{nCtrl}\ f \circ \mathrm{id} \otimes g \\
&\quad = \mathrm{id} \otimes g^{-1} \circ \mathsf{Mat}^{-1} \circ (f \oplus \mathrm{id}) \circ \mathsf{Mat} \circ \mathrm{id} \otimes g && (\text{definition } \mathsf{nCtrl})
\end{aligned}$$

$$
\begin{array}{rclr}
i^4_{[j]} & = & \mathrm{id} & \text{(D1)} \\
\mathsf{X}^2_{[j,k]} & = & \mathrm{id} & \text{(D2)} \\
\mathsf{K}^8_{[j,k]} & = & \mathrm{id} & \text{(D3)} \\
i_{[j]} i_{[k]} & = & i_{[k]} i_{[j]} & \text{(D4)} \\
i_{[j]} \mathsf{X}_{[k,l]} & = & \mathsf{X}_{[k,l]} i_{[j]} & \text{(D5)} \\
i_{[j]} \mathsf{K}_{[k,l]} & = & \mathsf{K}_{[k,l]} i_{[j]} & \text{(D6)} \\
\mathsf{X}_{[j,k]} \mathsf{X}_{[l,m]} & = & \mathsf{X}_{[l,m]} \mathsf{X}_{[j,k]} & \text{(D7)} \\
\mathsf{X}_{[j,k]} \mathsf{K}_{[l,m]} & = & \mathsf{K}_{[l,m]} \mathsf{X}_{[j,k]} & \text{(D8)} \\
\mathsf{K}_{[j,k]} \mathsf{K}_{[l,m]} & = & \mathsf{K}_{[l,m]} \mathsf{K}_{[j,k]} & \text{(D9)}
\end{array}
\qquad
\begin{array}{rclr}
i_{[k]} X_{[j,k]} & = & X_{[j,k]} i_{[j]} & \text{(D10)} \\
\mathsf{X}_{[k,l]} \mathsf{X}_{[j,k]} & = & \mathsf{X}_{[j,k]} \mathsf{X}_{[j,l]} & \text{(D11)} \\
\mathsf{X}_{[j,l]} \mathsf{X}_{[k,l]} & = & \mathsf{X}_{[k,l]} \mathsf{X}_{[j,k]} & \text{(D12)} \\
\mathsf{K}_{[k,l]} \mathsf{X}_{[j,k]} & = & \mathsf{X}_{[j,k]} \mathsf{K}_{[j,l]} & \text{(D13)} \\
\mathsf{K}_{[j,l]} \mathsf{X}_{[k,l]} & = & \mathsf{X}_{[k,l]} \mathsf{K}_{[j,k]} & \text{(D14)} \\
\mathsf{K}_{[j,k]} i^2_{[k]} & = & \mathsf{X}_{[j,k]} \mathsf{K}_{[j,k]} & \text{(D15)} \\
\mathsf{K}_{[j,k]} i^3_{[k]} & = & i_{[k]} \mathsf{K}_{[j,k]} i_{[k]} \mathsf{K}_{[j,k]} & \text{(D16)} \\
\mathsf{K}_{[j,k]} i_{[j]} i_{[k]} & = & i_{[j]} i_{[k]} \mathsf{K}_{[j,k]} & \text{(D17)} \\
\mathsf{K}^2_{[j,k]} i_{[j]} i_{[k]} & = & \mathrm{id} & \text{(D18)} \\
\mathsf{K}_{[j,k]} \mathsf{K}_{[l,m]} \mathsf{K}_{[j,l]} \mathsf{K}_{[k,m]} & = & \mathsf{K}_{[j,l]} \mathsf{K}_{[k,m]} \mathsf{K}_{[j,k]} \mathsf{K}_{[l,m]} & \text{(D19)}
\end{array}
$$

Fig. 12. The sound and complete equational theory of Gaussian dyadic rational unitaries due to [Bian and Selinger 2021].

$$
\begin{aligned}
&= \mathsf{Mat}^{-1} \circ (g^{-1} \oplus g^{-1}) \circ (f \oplus \mathrm{id}) \circ (g \oplus g) \circ \mathsf{Mat} && \text{(Lem. 10 (i))} \\
&= \mathsf{Mat}^{-1} \circ \circ((g^{-1} \circ f \circ g) \oplus (g^{-1} \circ g) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus\text{)} \\
&= \mathsf{Mat}^{-1} \circ ((g^{-1} \circ f \circ g) \oplus \mathrm{id}) \circ \mathsf{Mat} && (g \text{ invertible})
\end{aligned}
$$

In other words, conjugating a negatively controlled f-gate by g on the target line yields a negatively controlled $g^{-1} \circ f \circ g$-gate (idem for positively controlled gates). Thus, it suffices to show that positively controlled gates commute with negatively controlled gates.

$$
\begin{aligned}
&\mathsf{Ctrl}\, f \circ \mathsf{nCtrl}\, g \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus f) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (g \oplus \mathrm{id}) \circ \mathsf{Mat} && \text{(definition Ctrl, nCtrl)} \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus f) \circ (g \oplus \mathrm{id}) \circ \mathsf{Mat} && \text{(Mat invertible)} \\
&= \mathsf{Mat}^{-1} \circ (g \oplus \mathrm{id}) \circ (\mathrm{id} \oplus f) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus\text{)} \\
&= \mathsf{Mat}^{-1} \circ (g \oplus \mathrm{id}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus f) \circ \mathsf{Mat} && \text{(Mat invertible)} \\
&= \mathsf{nCtrl}\, g \circ \mathsf{Ctrl}\, f && \text{(definition Ctrl, nCtrl)}
\end{aligned}
$$

(A19) As above.
(A20) We defer the derivation of this identity to Appendix B.

Summing up:

Theorem 19. *Let c_1 and c_2 be $\sqrt{\Pi}$ terms representing Clifford+T circuits of at most two qubits. Then $[\![c_1]\!] = [\![c_2]\!]$ iff $(\!|c_1|\!) = (\!|c_2|\!)$.*

Proof. (A1)–(A20) are sound and complete for Clifford+T circuits of at most two qubits [Bian and Selinger 2022], and have been shown to hold in any model of $\sqrt{\Pi}$ (see also Thm. 13). □

6.4 Unitaries with entries in $\mathbb{Z}[\frac{1}{2}, i]$

We now show that models of $\sqrt{\Pi}$ are equationally sound and complete for unitaries with entries from the ring $\mathbb{Z}[\frac{1}{2}, i]$ (*i.e.*, the ring of integers extended with $\frac{1}{2}$ and i). We call these *Gaussian dyadic rational unitaries*. It was shown by Amy et al. [2020] that every circuit in the computationally universal *Gaussian Clifford+T* gate set has an *exact* representation as a unitary matrix with entries in $\mathbb{Z}[\frac{1}{2}, i]$. A sound and complete equational theory for these unitaries was given by Bian and Selinger [2021] (see Fig. 12). In other words, these unitaries are enough to approximate any other finite quantum computation to any desired degree of error, and they can be reasoned about using a sound and complete equational theory.

In this section, we show that this equational theory is subsumed by that of $\sqrt{\Pi}$. Then we show that the easy direction of [Amy et al. 2020] can also be internalised in models of $\sqrt{\Pi}$, thus proving equational soundness and completeness for Gaussian Clifford+T circuits.

Unlike the previous results, which concerned circuits (formed using $\otimes$), this result concerns only matrices (formed using $\oplus$). This also means that the presentation (in Fig. 12) is quite different. Gaussian dyadic rational unitaries are generated by i, X, and K, where K is a variant of the Hadamard gate given by $\mathsf{K} = \omega^{-1} \bullet \mathsf{H}$[1]. In Fig. 12, these are additionally given indices, assumed distinct, corresponding to the component(s) that the generator is applied to. When proving these identities, we further assume indices to start from 1 and to be consecutive in the order written. We are free to do so since we can simply conjugate by the appropriate permutation to make it so (recalling that Π can express all permutations). Likewise, we will assume identities to be minimal, and only consider the case that uses the number of distinct indices; any other case reduces to this by appending an identity morphism as necessary using the direct sum and conjugating by a permutation. For example, in the context on an $n \times n$ unitary (*i.e.*, a morphism $I^{\oplus n} \to I^{\oplus n}$, where $I^{\oplus n}$ is taken as usual to mean the n-fold direct sum of I with itself), $\mathsf{X}_{[2,3]}$ is taken to mean $\mathrm{id}_I \oplus \mathsf{X} \oplus \mathrm{id}_{I^{\oplus n-3}}$ (up to associativity). To form $\mathsf{X}_{[2,4]}$ would require us to conjugate this by the permutation swapping the third and fourth components.

Definition 20. In a model of $\sqrt{\Pi}$, a *representation of a Gaussian dyadic rational unitary* is any morphism which can be written in terms of morphisms from the sets $\{i, \mathsf{K}\}$ and $\{\alpha_\oplus, \alpha_\oplus^{-1}, \lambda_\oplus, \lambda_\oplus^{-1}, \rho_\oplus, \rho_\oplus^{-1}, \sigma_\oplus\}$, composed arbitrarily in parallel (using $\oplus$) and in sequence (using $\circ$).

Note that the above definition permits the use of X since $\mathsf{X} = \sigma_\oplus$ by definition. It is additionally important to realise that the notion of parallel composition is different between the above the previous definitions concerning circuits, as this uses the direct sum $\oplus$ for parallel composition whereas the circuits used the tensor product $\otimes$.

We show that the identities of Fig. 12 are all satisfied in any model of $\sqrt{\Pi}$.

(D1) $i^4 = (\omega^2)^4 = \omega^8 = \mathrm{id}$ by (E1).
(D2) $\mathsf{X}^2 = \sigma_\oplus^2 = \mathrm{id}$ by the rig axioms.
(D3) We start by seeing that

$$\begin{aligned}
\mathsf{K}^2 &= (\omega^{-1} \bullet \mathsf{H}) \circ (\omega^{-1} \bullet \mathsf{H}) && \text{(def. K)}\\
&= (\omega^{-1} \circ \omega^{-1}) \bullet \mathsf{H} \circ \mathsf{H} && \text{(Prop. 8)}\\
&= (\omega^7 \circ \omega^7) \bullet \mathrm{id} && \text{(A4)}\\
&= (\omega^8 \circ \omega^6) \bullet \mathrm{id} && (\circ \text{ associative})\\
&= \omega^6 \bullet \mathrm{id} && \text{(E1)}
\end{aligned}$$

and so $K^8 = (K^2)^4 = (\omega^6 \bullet \mathrm{id})^4 = \omega^{24} \bullet \mathrm{id} = (\omega^8 \circ \omega^8 \circ \omega^8) \bullet \mathrm{id} = \mathrm{id}$ by (E1) and Prop. 8.

(D4–9) These are all instances of bifunctoriality for $\oplus$, *i.e.*, $(f \oplus \mathrm{id}) \circ (\mathrm{id} \oplus g) = (\mathrm{id} \oplus g) \circ (f \oplus \mathrm{id})$.

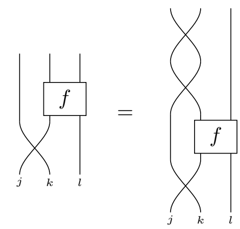
(D10) We have

$$\begin{aligned}
(\mathrm{id} \oplus i) \circ \mathsf{X} &= (\mathrm{id} \oplus i) \circ \sigma_\oplus && \text{(definition X)}\\
&= \sigma_\oplus \circ (i \oplus \mathrm{id}) && (\text{naturality } \sigma_\oplus)
\end{aligned}$$

[1]Note the slight discrepancy in the literature that Bian and Selinger [2021] take $\mathsf{K} = \omega^{-1} \bullet \mathsf{H}$ while Amy et al. [2020] use $\mathsf{K} = \omega \bullet \mathsf{H}$. However, since one definition is inverse to the other, and $U_n(\mathbb{Z}[\frac{1}{2}, i])$ is closed under inversion, the particular choice doesn't matter so long as it is done consistently.

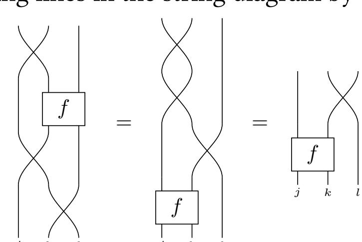
$$= \mathsf{X} \circ (i \oplus \mathrm{id}) \qquad \text{(definition X)}$$

(D11) We show the more general case for any f, from which this identity follows as the case of $f = \mathsf{X}$. Marking lines in the string diagram by indices, we see that this is nothing but



which follows by invertibility of the symmetry.

(D12) Likewise, we show the more general case for any f, from which this identity will follows as the case where $f = \mathsf{X}$. Marking lines in the string diagram by indices, we get



which follows by (respectively) naturality and invertibility of the symmetry.

(D13) This follows by the generalised form of (D11) with $f = \mathsf{K}$.

(D14) This follows by the generalised form of (D12) with $f = \mathsf{K}$.

(D15) We have

$$\begin{aligned}
\mathsf{K} \circ \mathsf{Z} &= \mathsf{K} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{H} && \text{(A4)} \\
&= \mathsf{K} \circ \mathsf{Z} \circ \mathsf{H} \circ (\omega \bullet \mathsf{K}) && \text{(definition H)} \\
&= (\omega \bullet \mathsf{K}) \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{K} && \text{(Prop. 8)} \\
&= \mathsf{H} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{K} && \text{(definition H)} \\
&= \mathsf{X} \circ \mathsf{K} && \text{(Lem. 11)}
\end{aligned}$$

(D16) We reduce

$$\begin{aligned}
\mathsf{K} \circ \mathsf{Z} \circ \mathsf{S} &= \mathsf{X} \circ \mathsf{K} \circ \mathsf{S} && \text{(D15)} \\
&= \mathsf{X} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} && \text{(definition K)} \\
&= \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} && \text{(X involutive)} \\
&= \mathsf{S} \circ \mathsf{V} \circ (i \bullet \mathsf{X}) && \text{(Lem. 9 (vi))} \\
&= i \bullet \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} && \text{(Prop. 8)}
\end{aligned}$$

and

$$\begin{aligned}
\mathsf{S} \circ \mathsf{K} \circ \mathsf{S} \circ \mathsf{K} &= \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && \text{(definition K)} \\
&= (i \bullet \mathsf{X}) \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ (i \bullet \mathsf{X}) \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && \text{(Lem. 9 (vi))} \\
&= i^2 \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && \text{(Prop. 8)} \\
&= -1 \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} && \text{(X involutive)}
\end{aligned}$$

$$
\begin{aligned}
&= -1 \bullet \mathsf{X} \circ \mathsf{V} \circ (-i \bullet \mathsf{V} \circ \mathsf{S} \circ \mathsf{V}) \circ \mathsf{X} && \text{(E3)} \\
&= -1 \circ -i \bullet \mathsf{X} \circ \mathsf{V} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} && \text{(Prop. 8)} \\
&= i \bullet \mathsf{X} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} && \text{(E2)} \\
&= i \bullet \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} && \text{(X involutive)}
\end{aligned}
$$

so $\mathsf{K} \circ \mathsf{Z} \circ \mathsf{S} = i \bullet \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} = \mathsf{S} \circ \mathsf{K} \circ \mathsf{S} \circ \mathsf{K}$.

(D17) It follows that

$$
\begin{aligned}
\mathsf{K} \circ (i \oplus i) &= \mathsf{K} \circ (i \bullet (\mathrm{id} \oplus \mathrm{id})) && \text{(Prop. 8)} \\
&= i \bullet \mathsf{K} \circ \mathrm{id} && \text{(bifunctoriality } \oplus) \\
&= i \bullet \mathsf{K} && \text{(Prop. 8)} \\
&= i \bullet (\mathrm{id} \oplus \mathrm{id}) \circ \mathsf{K} && \text{(bifunctoriality } \oplus) \\
&= (i \oplus i) \circ \mathsf{K} && \text{(Prop. 8)}
\end{aligned}
$$

(D18) We derive

$$
\begin{aligned}
\mathsf{K}^2 \circ (i \oplus i) &= \mathsf{K}^2 \circ (i \bullet (\mathrm{id} \oplus \mathrm{id})) && \text{(Prop. 8)} \\
&= i \bullet \mathsf{K}^2 && \text{(Prop. 8)} \\
&= i \bullet (\omega^{-1} \bullet \mathsf{H}) \circ (\omega^{-1} \bullet \mathsf{H}) && \text{(definition K)} \\
&= i \circ \omega^{-1} \circ \omega^{-1} \bullet \mathsf{H} \circ \mathsf{H} && \text{(Prop. 8)} \\
&= i \circ -i \bullet \mathrm{id} && \text{(A4)} \\
&= \mathrm{id} && \text{(E1)}
\end{aligned}
$$

(D19) We derive this final identity by showing that it is an instance of bifunctoriality of the tensor product in disguise:

$$
\begin{aligned}
&\mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} && \text{(Mat invertible)} \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(i)) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Mat} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(ii)) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(i)) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Mat} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(ii)) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Mat} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{K}) \circ (\mathsf{K} \otimes \mathrm{id}) \circ \mathsf{SWAP} \circ \mathsf{Mat}^{-1} && \text{(naturality SWAP)} \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Mat} \circ \mathsf{SWAP} \circ (\mathsf{K} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{SWAP} \circ \mathsf{Mat}^{-1} && \text{(bifunctoriality } \oplus) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{SWAP} \circ \mathsf{Mat}^{-1} && \text{(naturality SWAP)} \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Mat} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{SWAP} \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(i)) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{K}) \circ \mathsf{SWAP} \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(ii)) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Mat} \circ \mathsf{SWAP} \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(i)) \\
&= \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} && \text{(Lem. 10}(ii)) \\
&= (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} \circ (\mathsf{K} \oplus \mathsf{K}) \circ \mathsf{Midswap} && \text{(Mat invertible)}
\end{aligned}
$$

We obtain yet another equational completeness result:

Theorem 21 (Full abstraction for Gaussian dyadic rational unitaries). *Let c_1 and c_2 be $\sqrt{\Pi}$ terms representing unitaries with entries in the ring $\mathbb{Z}[\frac{1}{2}, i]$. Then $[\![c_1]\!] = [\![c_2]\!]$ iff $(\!|c_1|\!) = (\!|c_2|\!)$.*

Proof. Identities (D1)–(D19) form a sound and complete equational theory for Gaussian dyadic rational unitaries [Bian and Selinger 2021]. □

6.5 Gaussian Clifford+T Circuits

We mentioned in Sec. 6.4 the one-to-one correspondence (due to [Amy et al. 2020]) between circuits in the (computationally universal) Gaussian Clifford+T gate set $\{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \mathsf{K}, \mathsf{S}\}$ and Gaussian dyadic rational unitaries.

Definition 22. In a model of $\sqrt{\Pi}$, a *representation of a Gaussian Clifford+T circuit* is any morphism which can be written in terms of morphisms from the sets $\{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \mathsf{K}, \mathsf{S}\}$ and $\{\alpha_\otimes, \alpha_\otimes^{-1}, \lambda_\otimes, \lambda_\otimes^{-1}, \rho_\otimes, \rho_\otimes^{-1}, \sigma_\otimes\}$, composed arbitrarily in parallel (using $\otimes$) and in sequence (using $\circ$).

We argue that we can reason about Gaussian Clifford+T circuits in models of $\sqrt{\Pi}$ by reasoning about their matrices, using the coherence theorem for rig categories. Recall that a *bipermutative category* is a rig category where both symmetric monoidal structures are strict, and the annihilators and right distributor are all identities. (The explicit definition can be found in [May 1977].)

The coherence theorem for rig categories can be stated in terms of bipermutative categories as follows:

Theorem 23. *Any rig category is rig equivalent to a bipermutative category.*

Proof. See [May 1977, VI, Prop. 3.5]. □

We can use this theorem to make the rig structure in any model of $\sqrt{\Pi}$ bipermutative. This is very handy since we notice that in a bipermutative category, the isomorphism $\mathsf{Mat} : (I \oplus I) \otimes A \longrightarrow A \oplus A$ is the identity, as it is composed of the right distributor and some unitors; similarly, $\mathsf{Midswap} : (A \oplus B) \oplus (C \oplus D) \longrightarrow (A \oplus C) \oplus (B \oplus D)$ is $\mathrm{id} \oplus \sigma_\oplus \oplus \mathrm{id}$ (we don't need to worry about associativity due to strictness). Since in a general model of $\sqrt{\Pi}$ we have

$$\mathsf{CX} = \mathsf{Ctrl}\ \mathsf{X} = \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{X}) \circ \mathsf{Mat},$$

in a bipermutative model of $\sqrt{\Pi}$ we have $\mathsf{CX} = \mathrm{id} \oplus \mathsf{X}$; and $\mathsf{CCX} = (\mathrm{id} \oplus (\mathrm{id} \oplus \mathsf{X}))$. As

$$\mathsf{SWAP} = \mathsf{Mat}^{-1} \circ \mathsf{Mat} \circ \mathsf{SWAP} = \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ \mathsf{Mat}$$

by invertibility of Mat and Lem. 10, we have that $\mathsf{SWAP} = \mathsf{Midswap} = \mathrm{id} \oplus \mathsf{X} \oplus \mathrm{id}$ in the bipermutative case, so even swapping two circuit lines reduces to applying X. As such, X, CX, CCX, K, S, and SWAP are all Gaussian dyadic rational unitaries in a bipermutative model of $\sqrt{\Pi}$. This is the key observation in obtaining equational soundness and completeness for Gaussian Clifford+T circuits (as it was for classical reversible circuits as well [Choudhury et al. 2022]).

We will need a small lemma (with proof in Appendix B). Let $\mathsf{SWAPASSOC} : (I \oplus I) \otimes ((I \oplus I) \otimes A) \longrightarrow (I \oplus I) \otimes ((I \oplus I) \otimes A)$ denote the natural isomorphism $\alpha_\otimes \circ \mathsf{SWAP} \otimes \mathrm{id} \circ \alpha_\otimes^{-1}$.

Lemma 24. *In any model of $\sqrt{\Pi}$, we have*

$$(\mathsf{Mat} \oplus \mathsf{Mat}) \circ \mathsf{Mat} \circ \mathsf{SWAPASSOC} = \mathsf{Midswap} \circ (\mathsf{Mat} \oplus \mathsf{Mat}) \circ \mathsf{Mat}.$$

Theorem 25 (Full abstraction for Gaussian Clifford+T circuits). *Let c_1 and c_2 be $\sqrt{\Pi}$ terms representing Gaussian Clifford+T circuits. Then $[\![c_1]\!] = [\![c_2]\!]$ iff $(\!|c_1|\!) = (\!|c_2|\!)$.*

Proof. Let $c_1, c_2 : (I \oplus I)^{\otimes n} \longrightarrow (I \oplus I)^{\otimes n}$. By coherence, we may assume every model of $\sqrt{\Pi}$ in sight to be bipermutative.

As noted above, the gates of the Gaussian Clifford+T gate set are all representations of Gaussian dyadic rational unitaries in this bipermutative model: X and K are so directly, and $\mathsf{S} = \mathrm{id} \oplus i$, CX = id $\oplus$ X and CCX = id $\oplus$ (id $\oplus$ X) are so too by closure under direct sums. To see that the tensor product of two representations is also a representation, it suffices to show that tensoring by identities on $(I \oplus I)^{\otimes m}$ on either side preserves this property, since we have $(f \otimes \mathrm{id}) \circ (\mathrm{id} \otimes g) = f \otimes g$:

- By Lem. 10, tensoring by $\mathrm{id}_{I\oplus I}$ on the left yields $\mathrm{id}_{I\oplus I} \otimes f = \mathsf{Mat}^{-1} \circ (f \oplus f) \circ \mathsf{Mat}$, so in the bipermutative case $\mathrm{id}_{I\oplus I} \otimes f = f \oplus f$, which is again a representation of a Gaussian dyadic rational unitary unitary when f is, by closure under direct sum. But then we can repeat this process $m - 1$ times to tensor by $\mathrm{id}_{(I\oplus I)^{\otimes m}}$.
- By naturality, $f \otimes \mathrm{id}_{(I\oplus I)^{\otimes m}} = \sigma_\otimes \circ \mathrm{id}_{(I\oplus I)^{\otimes m}} \otimes f \circ \sigma_\otimes$, so this reduces to the case above since (in the bipermutative case, using Lems. 24 and 10) the symmetry $\sigma_\otimes$ on $(I \oplus I)^{\otimes p} \otimes (I \oplus I)^{\otimes q}$ is nothing but a series of direct sums of identities and $\oplus$-symmetries on $I \oplus I$ (*i.e.*, X gates).

Finally, since representations of Gaussian dyadic rational unitaries are also closed under composition, it follows that any representation of a Gaussian Clifford+T circuit in a bipermutative category is directly also a representation of a Gaussian dyadic rational unitary.

From this it follows for terms c_1 and c_2 representing Gaussian Clifford+T circuits that $[\![c_1]\!] = [\![c_2]\!]$ iff they are equal as representations of Gaussian dyadic rational unitaries, which in turn happens (by Thm. 21) iff they are equal as actual unitaries in **Unitary** (so specifically as Gaussian Clifford+T circuits), *i.e.*, iff $(\!|c_1|\!) = (\!|c_2|\!)$. □

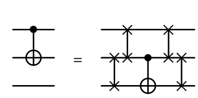
7 CIRCUIT EQUIVALENCES

As a supplement to this paper, we have developed an Agda library and used it to formalise some of our results. We discuss its use in proving the Sleator-Weinfurter decomposition of CCX mentioned in Sec. 3, as well as keys aspects of the implementation.

7.1 Decomposing CCX

In the previous section, we noted that every gate in the Gaussian Clifford+T gate set has a "matrix representation", *i.e.*, that it can be written as $\mathsf{Mat}^{-1} \circ g \circ \mathsf{Mat}$ for some g that only uses K, X, i, direct sums and composition. To prove the correctness of the Sleator-Weinfurter decomposition (see Fig. 2 on page 5), we will use a common technique: find the matrix form of each gate, compose them to form the circuit, and use elementary reasoning to take care of the rest.

The first step seems simple given that each elementary gate has a matrix representation, but additional work is required in the case of multi-qubit circuits. This is because the exact positioning of the gate alters its representation. For example, to find the matrix representation of a CX applied to the top two qubits of a three qubit circuit, we apply it instead to the bottom two qubits and apply SWAP gates to "rewire" the circuit appropriately, as in



This form allows us to use Lems. 10 and 24 to find its matrix representation, which turns out (with a bit of work) to be

$$\mathsf{Mat}^{-1} \circ (\mathsf{Mat}^{-1} \oplus \mathsf{Mat}^{-1}) \circ (\mathrm{id} \oplus \sigma_\oplus^{I\oplus I, I\oplus I}) \circ (\mathsf{Mat} \oplus \mathsf{Mat}) \circ \mathsf{Mat} \quad .$$

We use the same technique to find the matrix representation of the remaining gates in the circuit and compose them, yielding (after removing a number of superfluous $\mathsf{Mat}^{-1} \circ \mathsf{Mat}$)

$$\mathsf{Mat}^{-1} \circ (\mathsf{Mat}^{-1} \oplus \mathsf{Mat}^{-1}) \circ (\mathrm{id} \oplus (\mathsf{V} \oplus \mathsf{V})) \circ (\mathrm{id} \oplus \sigma_\oplus^{I\oplus I, I\oplus I}) \circ ((\mathrm{id} \oplus \mathsf{V}^{-1}) \oplus (\mathrm{id} \oplus \mathsf{V}^{-1})) \circ$$
$$(\mathrm{id} \oplus \sigma_\oplus^{I\oplus I, I\oplus I}) \circ ((\mathrm{id} \oplus \mathsf{V}) \oplus (\mathrm{id} \oplus \mathsf{V})) \circ (\mathsf{Mat} \oplus \mathsf{Mat}) \circ \mathsf{Mat}$$

Expanding out and applying naturality of $\sigma_\oplus$, invertibility of V, and bifunctoriality a few times show that this is equivalent to our previous definition of CCX, *i.e.*

$$\mathsf{Mat}^{-1} \circ \left(\mathrm{id} \oplus \left(\mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus X) \circ \mathsf{Mat}\right)\right) \circ \mathsf{Mat}.$$

An Agda program implementing the formal proof can be found in the supplementary material. The equational proofs are reasonably readable by humans (much more so than tactic proofs would be) but not so enlightening that including them here would be warranted.

7.2 Agda implementation

Presented with the choice of working in the syntax of $\sqrt{\Pi}$ (Sec. 4) or in its generic models (Def. 5), we chose to work in the latter for purely practical considerations: the library `agda-categories` already contains a wealth of reasoning combinators for both categories and monoidal categories that we would have to reproduce in the syntax of the language. Furthermore, it also has proofs of useful results, such as Kelly's various coherence lemmas, and defines useful extra combinators like "middle exchange" (our Midswap). As we would have had to reproduce all of that, this seemed like a simple choice.

However, everything in `agda-categories` is *weak*, so that we have to worry about units and association in our formal proofs. Doing this manually is overwhelmingly tedious. Luckily, there are a lot of combinators already defined that make this essentially bearable. The translation from the proofs presented in the paper, which ignore associativity altogether, does require some care.

We have not yet had a chance to formalise everything. We did formalise all of Sec. 5, all results in Sec. 6.1, Lem. 14 of Sec. 6.2, Lem. 18, and (A14) to (A17) in Sec. 6.3. We foresee no additional difficulties for other parts, except that many of the later equations are larger. Going at "full speed," a proof like that of Sleator-Weinfurter takes a little over an hour of dedicated work. However, identities like (B1)–(B4) and (A20) are likely to take several hours each.

We did not find any errors in any of the paper proofs while formalising them. We did find several cross-referencing errors (*i.e.*, the wrong lemma justifying the step had been written down), which were subsequently corrected. Interestingly, we did find an error in `agda-categories` itself: it was missing some coherences for `RigCategory`. This error has been fixed in the library.

We did find that some classical coherences used in the proofs of Lem. 8 and 9 were significantly more work to prove than the diagrammatic sketches let on. Three of the sub-parts of these "preliminary lemmas" accounted for more than a day's work each.

Nevertheless, we conclude that doing categorical meta-theory for quantum programming languages absolutely can be formalised at a reasonable cost.

8 CONCLUDING REMARKS

In this paper we have studied square roots from a purely axiomatic perspective. We have shown that with a remarkably small extension to the classical reversible programming language Π, one can obtain a language which is computational universal as well as sound and complete for a variety of modes of unitary quantum computing. A key feature of our approach (also found in other successful calculi such as the ZX-calculus) is the treatment of gates as white boxes that can be decomposed and recomposed during rewriting. This is in contrast to the circuit based approach that treat gates as black boxes. For example, while a circuit theory will allow one to derive that TT = S, it is unable to provide justification for this in terms of the definitions of S and T. On the other hand, our approach reduces this equation to the bifunctoriality of ⊕ and the definition of S and T. This style of reasoning is very close to the kind of semi-formal reasoning used to justify matrix equalities (employed, e.g., in [Bian and Selinger 2022] to justify their relations).

Physically, square roots are a key feature of quantum hardware. To understand this point, we briefly delve under the computational abstraction to the level of energy flow. At that level, the quantum mechanical description of a system is expressed using a Hamiltonian that is continuous in time (and assumed here to be time independent). Given a Hamiltonian H and some initial state $|\psi(0)\rangle$, the state of the system at a subsequent time t is given by:

$$|\psi(t)\rangle \;=\; e^{-iHt}\,|\psi(0)\rangle$$

In the circuit model of quantum computing, the quantity e^{-iHt} denotes a unitary U that is implemented by a gate or collection of gates. Mathematically, it is clearly legitimate to decompose $U = e^{-iHt}$ into $\sqrt{U} \circ \sqrt{U} = e^{-iHt/2} \cdot e^{-iHt/2}$. This decomposition has a simple operational realisation: if the application of U requires an energy pulse lasting k units of time, then applying the pulse for $k/2$ units implements $\sqrt{U}$ [Arute et. al. 2019, VII.F.2]. It turns out that the classical computing abstraction generally does not allow such decompositions, whereas quantum computing is distinguished by this feature.

The fact that a function and its square root operate at different time scales suggests evidence for the widely-believed exponential speedup that distinguishes quantum from classical computing. Indeed the simple Haskell module in Appendix D shows that, if we arrange for boolean negation to take *two steps*, then it is possible to model the analogue of a square root of boolean negation by just taking one of the two steps, and most importantly, this leads to the same quantum speedup observed Deutsch's problem [Deutsch 1985; Deutsch and Jozsa 1992]. Taking this idea further, it is arguably the case that more and more square roots, for example by providing additional roots of unity, would unlock additional speedup opportunities. We consider a formal investigation of these connections to be an important direction of future work.

ACKNOWLEDGEMENTS

We are indebted to the reviewers for their thoughtful and detailed comments. Jacques Carette is supported by NSERC grant RGPIN-2018-05812. Amr Sabry was supported by US National Science Foundation grant OMA-1936353.

REFERENCES

D. Aharonov. 2003. "A simple proof that Toffoli and Hadamard are quantum universal." arXiv:quant-ph/0301040. (2003).

M. Amy, A. N. Glaudell, and N. J. Ross. Apr. 2020. "Number-Theoretic Characterizations of Some Restricted Clifford+T Circuits." *Quantum*, 4, (Apr. 2020), 252. DOI: 10.22331/q-2020-04-06-252.

F. Arute et. al.. 2019. "Quantum supremacy using a programmable superconducting processor - supplementary information." *Nature*, 574, 505–510.

S. Awodey. 2010. *Category Theory*. Oxford University Press.

M. Backens and A. Kissinger. 2019. "ZH: A complete graphical calculus for quantum computations involving classical non-linearity." In: *Quantum Physics and Logic* (Electronic Proceedings in Theoretical Computer Science) 287, 23–42.

X. Bian and P. Selinger. 2021. "Generators and Relations for $U_n(\mathbb{Z}[\frac{1}{2}, i])$." In: *Quantum Physics and Logic* (Electronic Proceedings in Theoretical Computer Science). Vol. 343, 145–164. DOI: 10.4204/EPTCS.343.8.

X. Bian and P. Selinger. 2022. "Generators and Relations for 2-qubit Clifford+T operators." In: *Quantum Physics and Logic* (Electronic Proceedings in Theoretical Computer Science).

J. Carette, R. P. James, and A. Sabry. 2022. "Embracing the laws of physics: Three reversible models of computation." In: Advances in Computers. Vol. 126. Ed. by A. R. Hurson. Elsevier, 15–63. DOI: https://doi.org/10.1016/bs.adcom.2021.11.009.

J. Carette and A. Sabry. 2016. "Computing with Semirings and Weak Rig Groupoids." In: *Programming Languages and Systems*. Ed. by P. Thiemann. Springer Berlin Heidelberg, Berlin, Heidelberg, 123–148. ISBN: 978-3-662-49498-1.

V. Choudhury, J. Karwowski, and A. Sabry. Jan. 2022. "Symmetries in Reversible Programming: From Symmetric Rig Groupoids to Reversible Programming Languages." *Proc. ACM Program. Lang.*, 6, POPL, Article 6, (Jan. 2022), 32 pages. DOI: 10.1145/3498667.

A. Clément, N. Heurtel, S. Mansfield, S. Perdrix, and B. Valiron. 2023. "A complete equational theory for quantum circuits." In: *Logic in Computer Science*. DOI: 10.48550/arXiv.2206.10577.

B. Coecke and R. Duncan. 2011. “Interacting quantum observables: categorical algebra and diagrammatics.” *New Journal of Physics*, 13, 043016.

N. de Beaudrap, A. Kissinger, and J. van de Wetering. 2022. “Circuit extraction for ZX-diagrams can be #P-hard.” In: *ICALP*, 119:1–119:19.

D. Deutsch. 1985. “Quantum theory, the Church–Turing principle and the universal quantum computer.” *Proc. R. Soc. Lond. A 400*.

D. Deutsch and R. Jozsa. 1992. “Rapid solution of problems by quantum computation.” *Proc. R. Soc. Lond. A 439*.

R. Duncan and S. Perdrix. 2009. “Graph states and the necessity of Euler decomposition.” In: *Computability in Europe* (Lecture Notes in Computer Science). Vol. 5635. Springer, 167–177. doi: 10.1007/978-3-642-03073-4_18.

B. Giles and P. Selinger. 2013. “Exact synthesis of multiqubit Clifford+T circuits.” *Phys. Rev. A*, 87, 3.

R. Glück, R. Kaarsgaard, and T. Yokoyama. 2019. “Reversible programs have reversible semantics.” In: *Formal Methods. FM 2019 International Workshops* (Lecture Notes in Computer Science). Vol. 12232. Springer, 413–427.

D. Gottesman. 1999. “The Heisenberg representation of quantum computers.” In: *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, 32–43. doi: 10.48550/arXiv.quant-ph/9807006.

B. Hayes. 1995. “The square root of NOT.” *American Scientist*, 83, 304–308. doi: https://www.jstor.org/stable/29775474.

C. Heunen and R. Kaarsgaard. 2022. “Quantum Information Effects.” *Proceedings of the ACM on Programming Languages*, 6, POPL, 1–27.

C. Heunen, R. Kaarsgaard, and M. Karvonen. 2018. “Reversible effects as inverse arrows.” In: *Proceedings of the Thirty-Fourth Conference on the Mathematical Foundations of Programming Semantics (MFPS XXXIV)* (Electronic Notes in Theoretical Computer Science). Vol. 341. Elsevier, 179–199.

C. Heunen and J. Vicary. 2019. *Categories for quantum theory*. Oxford University Press.

J. Hu and J. Carette. 2021. “Formalizing Category Theory in Agda.” In: *Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs* (CPP 2021). Association for Computing Machinery, Virtual, Denmark, 327–342. isbn: 9781450382991. doi: 10.1145/3437992.3439922.

R. P. James and A. Sabry. 2012. “Information Effects.” In: *POPL ’12: Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of programming languages*. ACM, 73–84. doi: 10.1145/2103656.2103667.

N. Johnson and D. Yau. 2021. “Bimonoidal Categories, E_n-Monoidal Categories, and Algebraic K-Theory.” arXiv:2107.10526. (2021).

M. L. Laplaza. 1972. “Coherence for distributivity.” In: *Coherence in categories* (Lecture Notes in Mathematics) 281. Springer, 29–65.

J. P. May. 1977. *E_∞ Ring Spaces and E_∞ Ring Spectra*. Springer.

M. A. Nielsen and I. Chuang. 2010. *Quantum Computation and Quantum Information*. Cambridge University Press.

T. Satoh, S. Oomura, M. Sugawara, and N. Yamamoto. 2022. “Pulse-engineered controlled-V gate and its applications on superconducting quantum device.” *IEEE Transactions on Quantum Engineering*, 3, 3101610. doi: 10.1109/TQE.2022.3170008.

P. Selinger. June 2015. “Generators and relations for n-qubit Clifford operators.” *Logical Methods in Computer Science*, Volume 11, Issue 2, (June 2015). doi: 10.2168/LMCS-11(2:10)2015.

T. Sleator and H. Weinfurter. May 1995. “Realizable Universal Quantum Logic Gates.” *Phys. Rev. Lett.*, 74, (May 1995), 4087–4090, 20, (May 1995). doi: 10.1103/PhysRevLett.74.4087.

S. Staton. 2015. “Algebraic Effects, Linearity, and Quantum Programming Languages.” In: *Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages* (POPL ’15). ACM, 395–406.

M. K. Thomsen, R. Kaarsgaard, and M. Soeken. 2015. “Ricercar: A Language for Describing and Rewriting Reversible Circuits with Ancillae and Its Permutation Semantics.” In: *Reversible Computation*. Springer International Publishing, 200–215.

T. Toffoli. 1980. “Reversible computing.” In: *Automata, Languages and Programming*. Ed. by J. de Bakker and J. van Leeuwen. Springer Berlin Heidelberg, Berlin, Heidelberg, 632–644. isbn: 978-3-540-39346-7.

N. Yanofsky and M. A. Mannucci. 2008. *Quantum Computing for Computer Scientists*. Cambridge University Press.

L. Yeh and J. van de Wetering. 2022. “Constructing All Qutrit Controlled Clifford+T gates in Clifford+T.” In: *Reversible Computation*. Springer, 28–50.

A SUPPLEMENTARY MATERIAL FOR SEC. 5

Lemma 9. *Let s and t be scalars.*

(i) $-1^2 = \mathrm{id}$ *and* $i^2 = -1$,
(ii) $\mathsf{X}^2 = \mathrm{id}$,
(iii) $\mathsf{P}(s)^2 = \mathsf{P}(s^2)$,
(iv) $\mathsf{P}(s)^{-1} = \mathsf{P}(s^{-1})$,
(v) $\mathsf{P}(s) \circ \mathsf{P}(t) = \mathsf{P}(s \circ t) = \mathsf{P}(t) \circ \mathsf{P}(s)$,
(vi) $\mathsf{P}(s) \circ \mathsf{X} \circ \mathsf{P}(s) = s \bullet \mathsf{X}$,
(vii) $\mathsf{X} \circ \mathsf{V} = \mathsf{V} \circ \mathsf{X}$,
(viii) $\mathsf{CX}^2 = \mathrm{id}$,
(ix) $\mathsf{CZ}^2 = \mathrm{id}$,
(x) $\mathsf{CCX}^2 = \mathrm{id}$,
(xi) $\mathsf{X} \circ \mathsf{P}(s) = s \bullet \mathsf{P}(s^{-1}) \circ \mathsf{X}$.

Proof. We consider each property in turn:

(i) $i^2 = (\omega^2)^2 = \omega^4 = -1$ and $(-1)^2 = (\omega^4)^2 = \omega^8 = \mathrm{id}$ by (E1).
(ii) $\mathsf{X}^2 = \sigma_\oplus \circ \sigma_\oplus = \mathrm{id}$ by laws of rig categories.
(iii) $\mathsf{P}(s)^2 = (\mathrm{id} \oplus s) \circ (\mathrm{id} \oplus s) = (\mathrm{id} \circ \mathrm{id}) \oplus (s \circ s) = \mathrm{id} \oplus s^2 = \mathsf{P}(s^2)$ by bifunctoriality.
(iv) $\mathsf{P}(s) \circ \mathsf{P}(s^{-1}) = (\mathrm{id} \oplus s) \circ (\mathrm{id} \oplus s^{-1}) = (\mathrm{id} \circ \mathrm{id}) \oplus (s \circ s^{-1}) = \mathrm{id} \oplus \mathrm{id} = \mathrm{id}$ by bifunctoriality, and similarly $\mathsf{P}(s^{-1}) \circ \mathsf{P}(s) = (\mathrm{id} \circ \mathrm{id}) \oplus (s^{-1} \circ s) = \mathrm{id} \oplus \mathrm{id} = \mathrm{id}$, so $\mathsf{P}(s^{-1}) = \mathsf{P}(s)^{-1}$ by unicity of inverses.
(v) $\mathsf{P}(s) \circ \mathsf{P}(t) = (\mathrm{id} \oplus s) \circ (\mathrm{id} \oplus t) = \mathrm{id} \oplus (s \circ t) = \mathsf{P}(s \circ t) = \mathrm{id} \oplus (s \circ t) = \mathrm{id} \oplus (t \circ s) = (\mathrm{id} \oplus t) \circ (\mathrm{id} \oplus s) = \mathsf{P}(t) \circ \mathsf{P}(s)$ by bifunctoriality and commutativity of scalars.
(vi) $\mathsf{P}(s) \circ \mathsf{X} \circ \mathsf{P}(s) = (\mathrm{id} \oplus s) \circ \sigma_\oplus \circ (\mathrm{id} \oplus s) = (\mathrm{id} \oplus s) \circ (s \oplus \mathrm{id}) \circ \sigma_\oplus = (s \oplus s) \circ \sigma_\oplus = (s \bullet (\mathrm{id} \oplus \mathrm{id})) \circ \sigma_\oplus = s \bullet ((\mathrm{id} \oplus \mathrm{id}) \circ \sigma_\oplus) = s \bullet \sigma_\oplus = s \bullet \mathsf{X}$ by naturality of $\sigma_\oplus$, bifunctoriality, and Prop. 8.
(vii) $\mathsf{X} \circ \mathsf{V} = (\mathsf{V} \circ \mathsf{V}) \circ \mathsf{V} = \mathsf{V} \circ (\mathsf{V} \circ \mathsf{V}) = \mathsf{V} \circ X$ by $(E2)$.
(viii) We compute:

$$\begin{aligned} \mathsf{CX}^2 &= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{X}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{X}) \circ \mathsf{Mat} \\ &= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{X}) \circ (\mathrm{id} \oplus \mathsf{X}) \circ \mathsf{Mat} \\ &= \mathsf{Mat}^{-1} \circ ((\mathrm{id} \circ \mathrm{id}) \oplus (\mathsf{X} \circ \mathsf{X})) \circ \mathsf{Mat} \\ &= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathrm{id}) \circ \mathsf{Mat} \\ &= \mathsf{Mat}^{-1} \circ \mathsf{Mat} \\ &= \mathrm{id} \end{aligned}$$

(ix) By analogous argument.
(x) By analogous argument.
(xi) We compute:

$$\begin{aligned} \mathsf{X} \circ \mathsf{P}(s) &= \sigma_\oplus \circ (\mathrm{id} \oplus s) \\ &= (s \oplus \mathrm{id}) \circ \sigma_\oplus \\ &= ((s \circ \mathrm{id}) \oplus (s \circ s^{-1})) \circ \sigma_\oplus \\ &= s \bullet (\mathrm{id} \oplus s^{-1}) \circ \sigma_\oplus \\ &= s \bullet \mathsf{P}(s^{-1}) \circ \mathsf{X} \end{aligned}$$

□

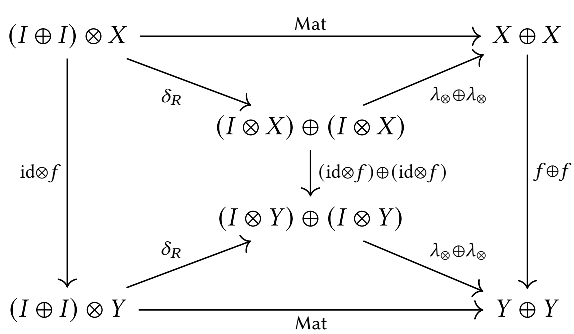
Lemma 10. *Let $f : X \to Y$, $g : X \to X$, and $h : X \to X$ be maps, and s and t be scalars. Then:*

(i) $\mathsf{Mat} \circ (\mathrm{id}_{I\oplus I} \otimes f) = (f \oplus f) \circ \mathsf{Mat}$,
(ii) $\mathsf{Mat} \circ \mathsf{SWAP} = \mathsf{Midswap} \circ \mathsf{Mat}$,
(iii) $\mathsf{SWAP} \circ \mathsf{Mat}^{-1} = \mathsf{Mat}^{-1} \circ \mathsf{Midswap}$,
(iv) $\mathsf{Mat} \circ (f \otimes \mathrm{id}_{I\oplus I}) = \mathsf{Midswap} \circ (f \oplus f) \circ \mathsf{Midswap} \circ \mathsf{Mat}$,
(v) $\mathsf{SWAP} \circ \mathsf{Ctrl\ P}(s) \circ \mathsf{SWAP} = \mathsf{Ctrl\ P}(s)$,
(vi) $\mathsf{Ctrl\ P}(s) \circ \mathsf{Ctrl\ P}(t) = \mathsf{Ctrl\ P}(t) \circ \mathsf{Ctrl\ P}(s)$,
(vii) $\mathsf{Ctrl\ P}(s) \circ (\mathrm{id}_{I\oplus I} \otimes \mathsf{P}(t)) = (\mathrm{id}_{I\oplus I} \otimes \mathsf{P}(t)) \circ \mathsf{Ctrl\ P}(s)$,
(viii) $\mathsf{Mat} \circ (\mathsf{X} \otimes \mathrm{id}_{I\oplus I}) = \sigma_{\oplus} \circ \mathsf{Mat}$,
(ix) $\mathsf{Mat} \circ (\mathsf{P}(s) \otimes \mathrm{id}_{I\oplus I}) = (\mathrm{id}_{I\oplus I} \oplus (s \bullet \mathrm{id})) \circ \mathsf{Mat}$.
(x) $\mathsf{Ctrl}\ g \circ \mathsf{Ctrl}\ h = \mathsf{Ctrl}(g \circ h)$

Proof. Below, the word Laplaza followed by a numeral refers to the coherence conditions of rig categories, first described in [Laplaza 1972].

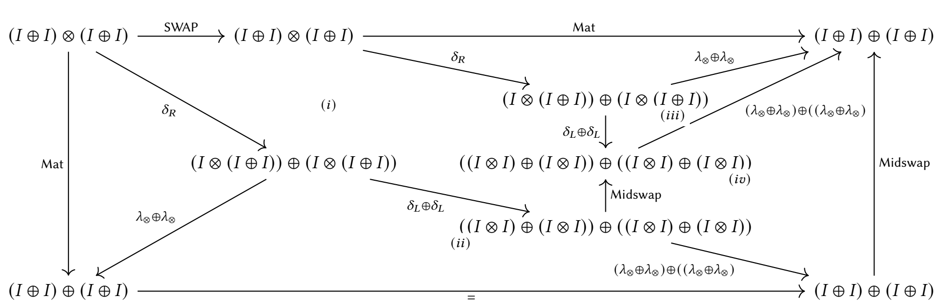
We consider each property in turn:

(i) follows by commutativity of the diagram



where the left and right cells commute by naturality, and the top and bottom cells by definition.

(ii) then follows by chasing



where (i) commutes by coherence (Laplaza (II) + (IX)), (ii) and (iii) by coherence (Laplaza (XXIII)), and (iv) by naturality. But then

(iii) follows by

$$
\begin{aligned}
\mathsf{SWAP} \circ \mathsf{Mat}^{-1} &= \mathsf{SWAP}^{-1} \circ \mathsf{Mat}^{-1} && \text{(SWAP involutive)} \\
&= (\mathsf{Mat} \circ \mathsf{SWAP})^{-1} && ((-)^{-1} \text{ contravariant functorial}) \\
&= (\mathsf{Midswap} \circ \mathsf{Mat})^{-1} && \text{Lem. 10 (2)}
\end{aligned}
$$

$$= \mathsf{Mat}^{-1} \circ \mathsf{Midswap}^{-1} \qquad ((-)^{-1} \text{ contravariant functorial})$$
$$= \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \qquad (\mathsf{Midswap} \text{ involutive})$$

(iv) by

$$\begin{aligned}
\mathsf{Mat} \circ (f \otimes \mathrm{id}) &= \mathsf{Mat} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes f) \circ \mathsf{SWAP} && (\text{naturality SWAP}) \\
&= \mathsf{Midswap} \circ \mathsf{Mat} \circ (\mathrm{id} \otimes f) \circ \mathsf{SWAP} && \text{Lem. 10 (2)} \\
&= \mathsf{Midswap} \circ (f \oplus f) \circ \mathsf{Mat} \circ \mathsf{SWAP} && \text{Lem. 10 (1)} \\
&= \mathsf{Midswap} \circ (f \oplus f) \circ \mathsf{Midswap} \circ \mathsf{Mat} && \text{Lem. 10 (2)}
\end{aligned}$$

(v) by

$$\begin{aligned}
&\mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{P}(s) \circ \mathsf{SWAP} \\
&= \mathsf{SWAP} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} \circ \mathsf{SWAP} && (\text{def. Ctrl}) \\
&= \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Midswap} \circ \mathsf{Mat} && (\text{Lem. 10 (2)+(3)}) \\
&= \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ ((\mathrm{id} \oplus \mathrm{id}) \oplus (\mathrm{id} \oplus s)) \circ \mathsf{Midswap} \circ \mathsf{Mat} && (\text{def. } \mathsf{P}(s)) \\
&= \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ \mathsf{Midswap} \circ ((\mathrm{id} \oplus \mathrm{id}) \oplus (\mathrm{id} \oplus s)) \circ \mathsf{Mat} && (\text{naturality Midswap}) \\
&= \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \mathrm{id}) \oplus (\mathrm{id} \oplus s)) \circ \mathsf{Mat} && (\text{Midswap involutive}) \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} && (\text{def. } \mathsf{P}(s)) \\
&= \mathsf{Ctrl}\ \mathsf{P}(s) && (\text{def. Ctrl})
\end{aligned}$$

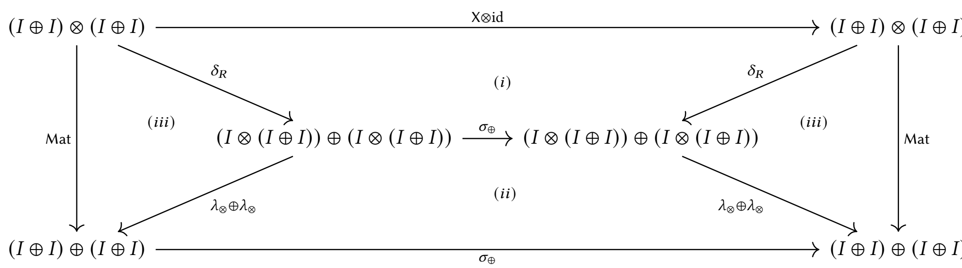
(vi) by

$$\begin{aligned}
\mathsf{Ctrl}\ \mathsf{P}(s) \circ \mathsf{Ctrl}\ \mathsf{P}(t) &= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(t)) \circ \mathsf{Mat} && (\text{def. Ctrl}) \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ (\mathrm{id} \oplus \mathsf{P}(t)) \circ \mathsf{Mat} && (\text{Mat invertible}) \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus (\mathsf{P}(s) \circ \mathsf{P}(t))) \circ \mathsf{Mat} && (\oplus \text{ bifunctoriality}) \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus (\mathsf{P}(t) \circ \mathsf{P}(s))) \circ \mathsf{Mat} && (\text{Lem. 9}(v)) \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(t)) \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} && (\oplus \text{ bifunctoriality}) \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(t)) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} && (\text{Mat invertible}) \\
&= \mathsf{Ctrl}\ \mathsf{P}(t) \circ \mathsf{Ctrl}\ \mathsf{P}(s) && (\text{def. Ctrl})
\end{aligned}$$

(vii) by

$$\begin{aligned}
\mathsf{Ctrl}\ \mathsf{P}(s) \circ (\mathrm{id} \otimes \mathsf{P}(t)) &= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{P}(t)) && (\text{def. Ctrl}) \\
&= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ (\mathsf{P}(t) \oplus \mathsf{P}(t)) \circ \mathsf{Mat} && (\text{Lem. 10(1)}) \\
&= \mathsf{Mat}^{-1} \circ ((\mathrm{id} \circ \mathsf{P}(t)) \oplus (\mathsf{P}(s) \circ \mathsf{P}(t))) \circ \mathsf{Mat} && (\oplus \text{ bifunctoriality}) \\
&= \mathsf{Mat}^{-1} \circ ((\mathsf{P}(t) \circ \mathrm{id}) \oplus (\mathsf{P}(t) \circ \mathsf{P}(s))) \circ \mathsf{Mat} && (\text{Lem. 9}(v)) \\
&= \mathsf{Mat}^{-1} \circ (\mathsf{P}(t) \oplus \mathsf{P}(t)) \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} && (\oplus \text{ bifunctoriality}) \\
&= ((\mathsf{P}(t)^{-1} \oplus \mathsf{P}(t)^{-1}) \circ \mathsf{Mat})^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} && ((-)^{-1} \text{ contrav. funct.}) \\
&= (\mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{P}(t)^{-1}))^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} && (\text{Lem. 10(1)}) \\
&= (\mathrm{id} \otimes \mathsf{P}(t)) \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{P}(s)) \circ \mathsf{Mat} && ((-)^{-1} \text{ contrav. funct.}) \\
&= (\mathrm{id} \otimes \mathsf{P}(t)) \circ \mathsf{Ctrl}\ \mathsf{P}(s) && (\text{def. Ctrl})
\end{aligned}$$

(viii) by commutativity of the diagram



where (i) commutes by Laplaza (I)+(II) (recalling that X is just defined to be $\sigma_\oplus$ on $I \oplus I$), (ii) by naturality of $\sigma_\oplus$, and (iii) by definition of Mat.

(ix) follows by

$$\begin{aligned}
\mathsf{Mat} \circ (\mathsf{P}(s) \otimes \mathrm{id}) &= \mathsf{Midswap} \circ (\mathsf{P}(s) \oplus \mathsf{P}(s)) \circ \mathsf{Midswap} \circ \mathsf{Mat} && \text{(Lem. 10 (4))} \\
&= \mathsf{Midswap} \circ ((\mathrm{id} \oplus s) \oplus (\mathrm{id} \oplus s)) \circ \mathsf{Midswap} \circ \mathsf{Mat} && \text{(def. P}(s)\text{)} \\
&= \mathsf{Midswap} \circ \mathsf{Midswap} \circ ((\mathrm{id} \oplus \mathrm{id}) \oplus (s \oplus s)) \circ \mathsf{Mat} && \text{(naturality Midswap)} \\
&= ((\mathrm{id} \oplus \mathrm{id}) \oplus (s \oplus s)) \circ \mathsf{Mat} && \text{(Midswap involutive)} \\
&= ((\mathrm{id} \oplus \mathrm{id}) \oplus ((s \bullet \mathrm{id}) \oplus (s \bullet \mathrm{id})) \circ \mathsf{Mat} && \text{(Prop. 8)} \\
&= ((\mathrm{id} \oplus \mathrm{id}) \oplus (s \bullet (\mathrm{id} \oplus \mathrm{id})) \circ \mathsf{Mat} && \text{(Prop. 8)} \\
&= (\mathrm{id} \oplus (s \bullet \mathrm{id})) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus\text{)}
\end{aligned}$$

(x) follows by

$$\begin{aligned}
\mathsf{Ctrl}\ g \circ \mathsf{Ctrl}\ h &= \mathsf{Mat}^{-1} \circ \mathrm{id} \oplus g \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathrm{id} \oplus h \circ \mathsf{Mat} && \text{(def. Ctrl)} \\
&= \mathsf{Mat}^{-1} \circ \mathrm{id} \oplus g \circ \mathrm{id} \oplus h \circ \mathsf{Mat} && \text{(Mat invertible)} \\
&= \mathsf{Mat}^{-1} \circ \mathrm{id} \oplus (g \circ h) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus\text{)} \\
&= \mathsf{Mat}^{-1} \circ \mathrm{id} \oplus (g \circ h) \circ \mathsf{Mat} && \text{(def. Ctrl)}
\end{aligned}$$

□

LEMMA 11. *Any model of* $\sqrt{\Pi}$ *satisfies* $\mathsf{H} \circ \mathsf{X} \circ \mathsf{H} = \mathsf{Z}$ *and* $\mathsf{H} \circ \mathsf{Z} \circ \mathsf{H} = \mathsf{X}$.

PROOF.

$$\begin{aligned}
\mathsf{H} \circ \mathsf{X} \circ \mathsf{H} &= (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) \circ \mathsf{X} \circ (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(def. H)} \\
&= \omega^2 \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(Prop. 8)} \\
&= i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && (X^2 = \mathrm{id}, \omega^2 = i) \\
&= i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ (i \bullet \mathsf{X}) \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(Prop. 8)} \\
&= i^2 \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{X} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(Prop. 8)} \\
&= -1 \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{V} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && (\text{Lem. 9}, i^2 = -1) \\
&= -1 \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{X}) && (\mathsf{V}^2 = \mathsf{X}) \\
&= -1 \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{S} \circ \mathsf{X}) && (\mathsf{X}^2 = \mathrm{id}) \\
&= -1 \bullet (\mathsf{X} \circ \mathsf{Z} \circ \mathsf{X}) && (\mathsf{S}^2 = \mathsf{Z}) \\
&= -1 \bullet ((-1 \bullet \mathsf{Z} \circ \mathsf{X}) \circ \mathsf{X}) && \text{(Lem. 9)}
\end{aligned}$$

$$
\begin{aligned}
&= (-1)^2 \bullet \mathsf{Z} \circ \mathsf{X} \circ \mathsf{X} && \text{(Prop. 8)}\\
&= \mathsf{Z} && ((-1)^2 = \mathrm{id}, \mathsf{X}^2 = \mathrm{id})
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{H} \circ \mathsf{Z} \circ \mathsf{H} &= (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) \circ \mathsf{Z} \circ (\omega \bullet \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(def. H)}\\
&= \omega^2 \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{Z} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(Prop. 8)}\\
&= i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ (-1 \bullet \mathsf{Z} \circ \mathsf{X}) \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && (\text{Lem. 9}, \omega^2 = i)\\
&= -i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{Z} \circ \mathsf{X} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(Prop. 8)}\\
&= -i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{Z} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && (\mathsf{X}^2 = \mathrm{id})\\
&= -i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{Z} \circ \mathsf{S} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && \text{(Lem. 9)}\\
&= -i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{Z} \circ \mathsf{Z} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && (\mathsf{S}^2 = \mathsf{Z})\\
&= -i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{V} \circ \mathsf{V} \circ \mathsf{S} \circ \mathsf{X}) && (\mathsf{Z}^2 = \mathrm{id})\\
&= -i \bullet (\mathsf{X} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{X}) && (\mathsf{V}^2 = \mathsf{X})\\
&= -i \bullet (\mathsf{X} \circ (i \bullet \mathsf{X}) \circ \mathsf{X}) && \text{(Lem. 9)}\\
&= -i \circ i \bullet (\mathsf{X} \circ \mathsf{X} \circ \mathsf{X}) && \text{(Prop. 8)}\\
&= \mathsf{X} && (-i \circ i = \mathrm{id}, \mathsf{X}^2 = \mathrm{id})
\end{aligned}
$$

□

B SUPPLEMENTARY MATERIAL FOR SEC. 6

Proof of (A12). We start by showing some identities that will be helpful in showing this relation and the one that follows. We first observe that

$$
\begin{aligned}
\mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} &= \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{H} && (A4)\\
&= (\omega \bullet \mathrm{id}) \circ \mathsf{H} && (A6)\\
&= \omega \bullet \mathsf{H} && \text{(Prop. 8)}
\end{aligned}
$$

and that

$$
\begin{aligned}
i \bullet \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{S} &= i \bullet \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{H} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{S} && (A4)\\
&= i \bullet \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{X} \circ \mathsf{S} && \text{(Lem. 11)}\\
&= i \bullet \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ (i \bullet \mathsf{S} \circ \mathsf{Z} \circ X) && \text{(Lem. 9 (xi))}\\
&= i^2 \bullet \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{Z} \circ X && \text{(Prop. 8)}\\
&= -1 \circ \omega \bullet \mathsf{H} \circ \mathsf{Z} \circ \mathsf{X} && (\text{Lem.}, i^2 = -1)\\
&= -1 \circ \omega \bullet \mathsf{H} \circ (-1 \bullet \mathsf{X} \circ \mathsf{Z}) && \text{(Lem. 9 (xi))}\\
&= (-1)^2 \circ \omega \bullet \mathsf{H} \circ \mathsf{X} \circ \mathsf{Z} && \text{(Prop. 8)}\\
&= \omega \bullet \mathsf{H} \circ \mathsf{X} \circ \mathsf{H} \circ \mathsf{H} \circ \mathsf{Z} && ((A4), (-1)^2 = \mathrm{id})\\
&= \omega \bullet \mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z} && \text{(Lem. 11)}
\end{aligned}
$$

But then we have

$$
\begin{aligned}
&\omega^{-1} \bullet (\mathsf{S} \otimes (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Ctrl}\ \mathsf{Z} \circ (\mathrm{id} \otimes (\mathsf{H} \circ \mathsf{S}))\\
&= \omega^{-1} \bullet (\mathsf{S} \otimes (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \circ (\mathrm{id} \otimes (\mathsf{H} \circ \mathsf{S})) && \text{(def. Ctrl)}\\
&= \omega^{-1} \bullet (\mathsf{S} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \circ (\mathrm{id} \otimes (\mathsf{H} \circ \mathsf{S})) && (\text{bifunctoriality } \otimes)\\
&= \omega^{-1} \bullet (\mathsf{S} \otimes \mathrm{id}) \circ \mathsf{Mat}^{-1} \circ ((\mathsf{S} \circ \mathsf{H} \circ \mathsf{S}) \oplus (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S})) \circ (\mathrm{id} \oplus \mathsf{Z}) \circ ((\mathsf{H} \circ \mathsf{S}) \oplus (\mathsf{H} \circ \mathsf{S})) \circ \mathsf{Mat} && \text{(Lem. 10 (i) twice)}
\end{aligned}
$$

$$= \omega^{-1} \bullet (\mathsf{S} \otimes \mathrm{id}) \circ \mathsf{Mat}^{-1} \circ ((\mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S}) \oplus (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Mat} \qquad \text{(bifunctoriality } \oplus\text{)}$$
$$= \omega^{-1} \bullet \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus (i \bullet \mathrm{id})) \circ ((\mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S}) \oplus (\mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Mat} \qquad \text{(Lem. 10 (ix))}$$
$$= \omega^{-1} \bullet \mathsf{Mat}^{-1} \circ ((\mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S}) \oplus (i \bullet \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{S})) \circ \mathsf{Mat} \qquad \text{(bifunctoriality } \oplus\text{)}$$
$$= \omega^{-1} \bullet \mathsf{Mat}^{-1} \circ ((\omega \bullet \mathsf{H}) \oplus (\omega \bullet \mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z})) \circ \mathsf{Mat} \qquad \text{(inner lemmas)}$$
$$= \omega^{-1} \bullet \mathsf{Mat}^{-1} \circ \omega \bullet (\mathsf{H} \oplus (\mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z})) \circ \mathsf{Mat} \qquad \text{(Prop. 8)}$$
$$= \omega^{-1} \circ \omega \bullet \mathsf{Mat}^{-1} \circ (\mathsf{H} \oplus (\mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z})) \circ \mathsf{Mat} \qquad \text{(Prop. 8)}$$
$$= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ (\mathsf{H} \oplus \mathsf{H}) \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \qquad \text{(bifunctoriality } \oplus\text{)}$$
$$= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathsf{H} \oplus \mathsf{H}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \qquad \text{(Mat invertible)}$$
$$= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \qquad \text{(Lem. 10 (i))}$$
$$= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \qquad \text{(Mat invertible)}$$
$$= \mathsf{Ctrl}\ \mathsf{Z} \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl}\ \mathsf{Z} \qquad \text{(def. Ctrl)}$$

as desired. □

Lemma 14. *The following identities hold in any model of $\sqrt{\Pi}$:*

(i) $\mathrm{id} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathrm{id} \otimes \mathsf{H} = \mathsf{Ctrl}\ \mathsf{Z}$,
(ii) $\mathsf{H} \otimes \mathrm{id} \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{SWAP} \circ \mathsf{H} \otimes \mathrm{id} = \mathsf{Ctrl}\ \mathsf{Z}$,
(iii) $\mathrm{id} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathrm{id} \otimes \mathsf{H} = \mathsf{Ctrl}\ \mathsf{X}$,
(iv) $\mathsf{H} \otimes \mathrm{id} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{H} \otimes \mathrm{id} = \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{SWAP}$,
(v) $\mathsf{H} \otimes \mathrm{id} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{H} \otimes \mathrm{id} = \mathrm{id} \otimes \mathsf{H} \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{SWAP} \circ \mathrm{id} \otimes \mathsf{H}$

Proof. For (i),

$$\mathrm{id} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathrm{id} \otimes \mathsf{H} = \mathrm{id} \otimes \mathsf{H} \circ \mathsf{Mat}^{-1} \circ \mathrm{id} \oplus \mathsf{X} \circ \mathsf{Mat} \circ \mathrm{id} \otimes \mathsf{H} \qquad \text{(def. Ctrl)}$$
$$= \mathsf{Mat}^{-1} \circ (\mathsf{H} \oplus \mathsf{H}) \circ (\mathrm{id} \oplus \mathsf{X}) \circ (\mathsf{H} \oplus \mathsf{H}) \circ \mathsf{Mat} \qquad \text{(Lem. 9 (i))}$$
$$= \mathsf{Mat}^{-1} \circ (\mathsf{H} \circ \mathsf{H}) \oplus (\mathsf{H} \circ \mathsf{X} \circ \mathsf{H}) \circ \mathsf{Mat} \qquad \text{(bifunctoriality } \oplus\text{)}$$
$$= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus (\mathsf{H} \circ \mathsf{X} \circ \mathsf{H})) \circ \mathsf{Mat} \qquad \text{(A4)}$$
$$= \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{Z}) \circ \mathsf{Mat} \qquad \text{(Lem. 11)}$$
$$= \mathsf{Ctrl}\ \mathsf{Z} \qquad \text{(def. Ctrl)}$$

and (ii),

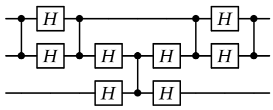
$$\mathsf{H} \otimes \mathrm{id} \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{SWAP} \circ \mathsf{H} \otimes \mathrm{id}$$
$$= \mathsf{SWAP} \circ \mathrm{id} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathrm{id} \otimes \mathsf{H} \circ \mathsf{SWAP} \qquad \text{(naturality SWAP)}$$
$$= \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} \qquad \text{(Lem. 14 (i))}$$
$$= \mathsf{Ctrl}\ \mathsf{Z} \qquad \text{(Lem. 10 (v))}$$

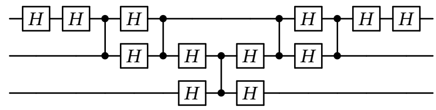
Points (iii) and (iv) follow entirely analogously to (i) and (ii) respectively. As for (v),

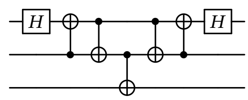
$$\mathsf{H} \otimes \mathrm{id} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{H} \otimes \mathrm{id}$$
$$= \mathsf{H} \otimes \mathrm{id} \circ \mathrm{id} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathrm{id} \otimes \mathsf{H} \circ \mathsf{H} \otimes \mathrm{id} \qquad \text{(Lem. 14 (iii))}$$
$$= \mathsf{H} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{H} \otimes \mathsf{H} \qquad \text{(bifunctoriality } \otimes\text{)}$$
$$= \mathsf{H} \otimes \mathsf{H} \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{SWAP} \circ \mathsf{H} \otimes \mathsf{H} \qquad \text{(Lem. 10 (v))}$$
$$= \mathsf{SWAP} \circ \mathsf{H} \otimes \mathsf{H} \circ \mathsf{Ctrl}\ \mathsf{Z} \circ \mathsf{H} \otimes \mathsf{H} \circ \mathsf{SWAP} \qquad \text{(naturality SWAP)}$$
$$= \mathsf{SWAP} \circ \mathsf{H} \otimes \mathrm{id} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{H} \otimes \mathrm{id} \circ \mathsf{SWAP} \qquad \text{(Lem. 14 (iii))}$$
$$= \mathrm{id} \otimes \mathsf{H} \circ \mathsf{SWAP} \circ \mathsf{Ctrl}\ \mathsf{X} \circ \mathsf{SWAP} \circ \mathrm{id} \otimes \mathsf{H} \qquad \text{(naturality SWAP)}$$

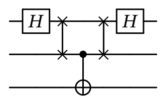
□

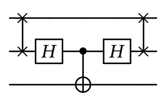
PROOF OF (B2). Once again, we derive this from the circuit identities and a classical lemma:

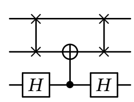


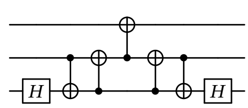
=  (A4)

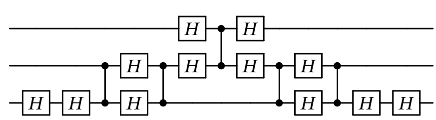
=  (Cor. 15)

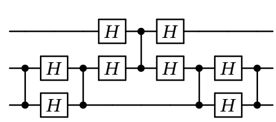
=  (P2)

=  (Cor. 15)

=  (Cor. 15)

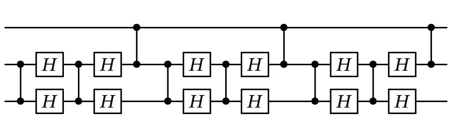
=  (P3)

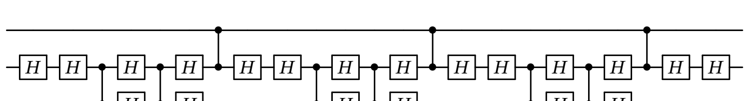
=  (Cor. 15)

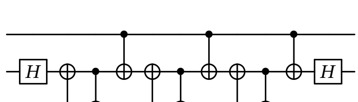
=  (A4)

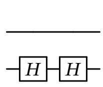
□

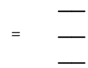
PROOF OF (B4).



=  (A4)

=  (Cor. 15)

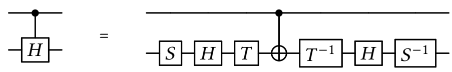
=  (P5)



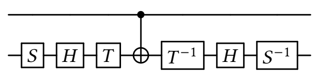
(A4)

□

Proof of (A20). To start, this identity involves a controlled Hadamard gate, which by [Bian and Selinger 2022] is taken as the shorthand



Since this representation is very inconvenient, we start by showing that it is equal to the far simpler Ctrl H. Since, as previously observed regarding controlled gates conjugated by other gates on the target line,



is a controlled $\mathsf{S}^{-1} \circ \mathsf{H} \circ \mathsf{T}^{-1} \circ \mathsf{X} \circ \mathsf{T} \circ \mathsf{H} \circ \mathsf{S}$ gate, it suffices to show that $\mathsf{S}^{-1} \circ \mathsf{H} \circ \mathsf{T}^{-1} \circ \mathsf{X} \circ \mathsf{T} \circ \mathsf{H} \circ \mathsf{S}$ is nothing more than H, which follows by

$$
\begin{aligned}
\mathsf{S}^{-1} \circ \mathsf{H} \circ \mathsf{T}^{-1} \circ \mathsf{X} \circ \mathsf{T} \circ \mathsf{H} \circ \mathsf{S} &= \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z} \circ \mathsf{S} \circ \mathsf{T} \circ \mathsf{X} \circ \mathsf{T} \circ \mathsf{H} \circ \mathsf{S} && \text{(Lem. 9 (iv))} \\
&= \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z} \circ \mathsf{S} \circ (\omega \bullet \mathsf{X}) \circ \mathsf{H} \circ \mathsf{S} && \text{(Lem. 9 (vi))} \\
&= \omega \bullet \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z} \circ \mathsf{S} \circ \mathsf{X} \circ \mathsf{H} \circ \mathsf{S} && \text{(Prop. 8)} \\
&= \omega \bullet \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z} \circ \mathsf{X} \circ (i \bullet \mathsf{Z} \circ \mathsf{S}) \circ \mathsf{H} \circ \mathsf{S} && \text{(Lem.. 9 (vi))} \\
&= i \circ \omega \bullet \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{Z} \circ \mathsf{X} \circ \mathsf{Z} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} && \text{(Prop. 8)} \\
&= i \circ \omega \bullet \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ (-1 \bullet \mathsf{X}) \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} && \text{(Lem.. 9 (vi))} \\
&= -1 \circ i \circ \omega \bullet \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} && \text{(Prop. 8)} \\
&= \omega^{-1} \bullet \mathsf{S} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{X} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} && \text{(Prop. 8)} \\
&= \omega^{-1} \bullet \mathsf{S} \circ \mathsf{Z} \circ \mathsf{Z} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} && \text{(Lem. 11)} \\
&= \omega^{-1} \bullet \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} \circ \mathsf{H} \circ \mathsf{S} && \text{(Lem. 9 (v))} \\
&= \omega^{-1} \bullet (\omega \bullet \mathsf{H}) && \text{(see B)} \\
&= (\omega^{-1} \circ \omega) \bullet \mathsf{H} && \text{(Prop. 8)} \\
&= \mathsf{H} && (\omega \text{ invertible})
\end{aligned}
$$

With that shown, we can move on to showing the final identity. We do this by showing four smaller identities which, together, imply this last identity, namely equations (5)–(8) in [Bian and Selinger 2022].

(i) Directly by Lem. 10 (v).
(ii) This is straightforwardly derived as

$$
\begin{aligned}
&\mathsf{Ctrl\ T} \circ \mathsf{nCtrl\ T} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathsf{id} \oplus \mathsf{T}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathsf{T} \oplus \mathsf{id}) \circ \mathsf{Mat} && \text{(definition Ctrl, nCtrl)} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathsf{id} \oplus \mathsf{T}) \circ (\mathsf{T} \oplus \mathsf{id}) \circ \mathsf{Mat} && \text{(Mat invertible)} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathsf{T} \oplus \mathsf{T}) \circ \mathsf{Mat} && (\text{bifunctoriality } \oplus) \\
&\quad = \mathsf{Mat}^{-1} \circ \mathsf{Mat} \circ (\mathsf{id} \otimes \mathsf{T}) && \text{(Lem. 10 (1))} \\
&\quad = \mathsf{id} \otimes \mathsf{T} && \text{(Mat invertible)}
\end{aligned}
$$

(iii) We first see that

$$
\begin{aligned}
&\mathsf{SWAP} \circ \mathsf{nCtrl\ T} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{T}) \\
&\quad = \mathsf{SWAP} \circ \mathsf{Mat}^{-1} \circ (\mathsf{T} \oplus \mathrm{id}) \circ \mathsf{Mat} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{T}) && \text{(def. nCtrl)} \\
&\quad = \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ (\mathsf{T} \oplus \mathrm{id}) \circ \mathsf{Midswap} \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{T}) && \text{(Lem. 10 (ii, iii))} \\
&\quad = \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ (\mathsf{T} \oplus \mathrm{id}) \circ \mathsf{Midswap} \circ (\mathsf{T} \oplus \mathsf{T}) \circ \mathsf{Mat} && \text{(Lem. 10 (i))} \\
&\quad = \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ ((\mathrm{id} \oplus \omega) \oplus \mathrm{id}) \circ \mathsf{Midswap} \circ (\mathsf{T} \oplus \mathsf{T}) \circ \mathsf{Mat} && \text{(def. T)} \\
&\quad = \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \mathrm{id}) \oplus (\omega \oplus \mathrm{id})) \circ \mathsf{Midswap} \circ \mathsf{Midswap} \circ (\mathsf{T} \oplus \mathsf{T}) \circ \mathsf{Mat} && \text{(naturality Midswap)} \\
&\quad = \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \mathrm{id}) \oplus (\omega \oplus \mathrm{id})) \circ (\mathsf{T} \oplus \mathsf{T}) \circ \mathsf{Mat} && \text{(Midswap invertible)} \\
&\quad = \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \omega) \oplus (\omega \oplus \omega)) \circ \mathsf{Mat} && \text{(def. T, bifunctoriality } \oplus\text{)}
\end{aligned}
$$

and then derive

$$
\begin{aligned}
&\mathsf{nCtrl\ T} \circ (\mathsf{T} \otimes \mathrm{id}) \\
&\quad = \mathsf{nCtrl\ T} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{T}) \circ \mathsf{SWAP} && \text{(naturality SWAP)} \\
&\quad = \mathsf{SWAP} \circ \mathsf{SWAP} \circ \mathsf{nCtrl\ T} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{T}) \circ \mathsf{SWAP} && \text{(SWAP invertible)} \\
&\quad = \mathsf{SWAP} \circ \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \omega) \oplus (\omega \oplus \omega)) \circ \mathsf{Mat} \circ \mathsf{SWAP} && \text{(above)} \\
&\quad = \mathsf{SWAP} \circ \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \omega) \oplus (\omega \oplus \omega)) \circ \mathsf{Midswap} \circ \mathsf{Mat} && \text{(Lem. 10 (ii))} \\
&\quad = \mathsf{SWAP} \circ \mathsf{Mat}^{-1} \circ \mathsf{Midswap} \circ ((\mathrm{id} \oplus \omega) \oplus (\omega \oplus \omega)) \circ \mathsf{Mat} && \text{(naturality Midswap)} \\
&\quad = \mathsf{SWAP} \circ \mathsf{SWAP} \circ \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \omega) \oplus (\omega \oplus \omega)) \circ \mathsf{Mat} && \text{(Lem. 10 (iii))} \\
&\quad = \mathsf{Mat}^{-1} \circ ((\mathrm{id} \oplus \omega) \oplus (\omega \oplus \omega)) \circ \mathsf{Mat} && \text{(SWAP invertible)} \\
&\quad = \mathsf{SWAP} \circ \mathsf{nCtrl\ T} \circ \mathsf{SWAP} \circ (\mathrm{id} \otimes \mathsf{T}) && \text{(above)}
\end{aligned}
$$

(iv) We derive

$$
\begin{aligned}
&\mathsf{Ctrl\ H} \circ (\mathrm{id} \otimes \mathsf{T}) \circ \mathsf{nCtrl\ H} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{H}) \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{T}) \circ \mathsf{Mat}^{-1} \circ (\mathsf{H} \oplus \mathrm{id}) \circ \mathsf{Mat} && \text{(def. Ctrl, nCtrl)} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{H}) \circ (\mathsf{T} \oplus \mathsf{T}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathsf{H} \oplus \mathrm{id}) \circ \mathsf{Mat} && \text{(Lem. 10 (1))} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{H}) \circ (\mathsf{T} \oplus \mathsf{T}) \circ (\mathsf{H} \oplus \mathrm{id}) \circ \mathsf{Mat} && \text{(Mat invertible)} \\
&\quad = \mathsf{Mat}^{-1} \circ ((\mathsf{T} \circ \mathsf{H}) \oplus (\mathsf{H} \circ \mathsf{T})) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus\text{)} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathsf{T} \oplus \mathrm{id}) \circ (\mathsf{H} \oplus \mathsf{H}) \circ (\mathrm{id} \oplus \mathsf{T}) \circ \mathsf{Mat} && \text{(bifunctoriality } \oplus\text{)} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathsf{T} \oplus \mathrm{id}) \circ (\mathsf{H} \oplus \mathsf{H}) \circ \mathsf{Mat} \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{T}) \circ \mathsf{Mat} && \text{(Mat invertible)} \\
&\quad = \mathsf{Mat}^{-1} \circ (\mathsf{T} \oplus \mathrm{id}) \circ \mathsf{Mat} \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Mat}^{-1} \circ (\mathrm{id} \oplus \mathsf{T}) \circ \mathsf{Mat} && \text{(Lem. 10 (1))} \\
&\quad = \mathsf{nCtrl\ T} \circ (\mathrm{id} \otimes \mathsf{H}) \circ \mathsf{Ctrl\ T} && \text{(def. Ctrl, nCtrl)}
\end{aligned}
$$

□

LEMMA 24. *In any model of $\sqrt{\Pi}$, we have*

$$(\mathsf{Mat} \oplus \mathsf{Mat}) \circ \mathsf{Mat} \circ \mathsf{SWAPASSOC} = \mathsf{Midswap} \circ (\mathsf{Mat} \oplus \mathsf{Mat}) \circ \mathsf{Mat}.$$

PROOF. This follows by commutativity of the diagram in Fig. 13.

Here (i) commutes by definition , (ii) by Laplaza (VII), (iii) monoidal coherence for ⊗, (iv) by Lem. 10, (v) by naturality of δ_R, and (vi) using Laplaza (I). □

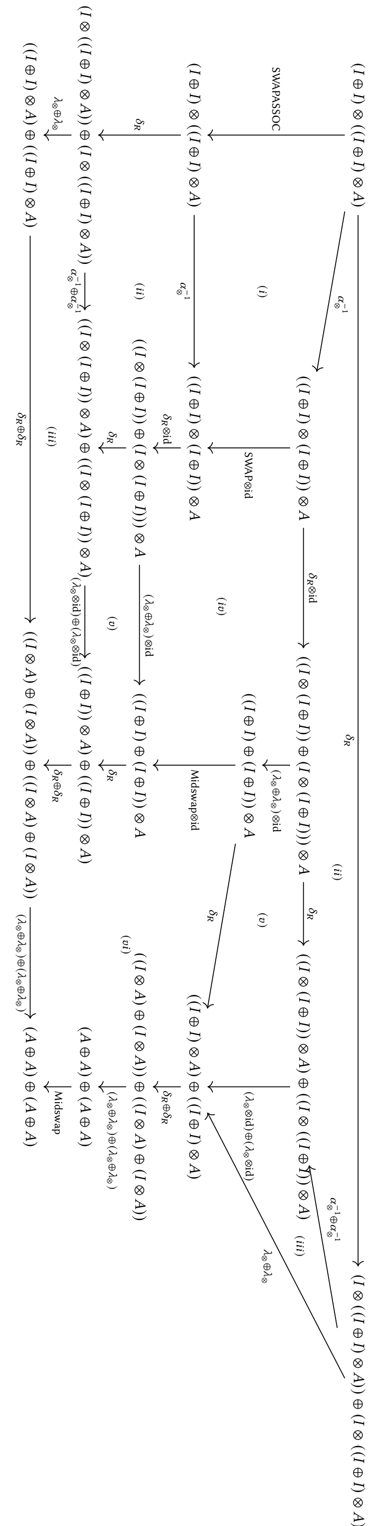


Fig. 13. Diagram for proving Lem. 24.

C DEFINITION OF BIPERMUTATIVE CATEGORY

Definition 26. A *bipermutative category* is a rig category where

(1) the associators $\alpha_\otimes : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$ and $\alpha_\oplus : (A \oplus B) \oplus C \to A \oplus (B \oplus C)$ and unitors $\lambda_\oplus : O \oplus A \to A$, $\rho_\oplus : A \oplus O \to A$, $\lambda_\otimes : I \otimes A \to A$, and $\rho_\otimes : A \otimes I \to A$ are all identities.

(2) the annihilators $\delta^0_R : A \otimes O \to O$ and $\delta^0_L : O \otimes A \to O$ and right distributor $\delta_R : (A \oplus B) \otimes C \to (A \otimes C) \oplus (B \otimes C)$ are identities, and the following diagram commutes:

$$\begin{array}{ccc}
(A \oplus B) \otimes C & \xrightarrow{=} & (A \otimes C) \oplus (B \otimes C) \\
{\scriptstyle \sigma_\oplus \otimes \mathrm{id}} \big\downarrow & & \big\downarrow {\scriptstyle \sigma_\oplus} \\
(B \oplus A) \otimes C & \xrightarrow[=]{} & (B \otimes C) \oplus (A \otimes C)
\end{array}$$

(3) The left distributor $\delta_L : A \otimes (B \oplus C) \to (A \otimes B) \oplus (A \otimes C)$ makes the diagrams below commute:

$$\begin{array}{ccc}
A \otimes (B \oplus C) & \xrightarrow{\sigma_\otimes} & (B \oplus C) \otimes A \\
{\scriptstyle \delta_L} \big\downarrow & & \big\downarrow {\scriptstyle =} \\
(A \otimes B) \oplus (A \otimes C) & \xleftarrow[\sigma_\otimes \oplus \sigma_\otimes]{} & (B \otimes A) \oplus (C \otimes A)
\end{array}$$

$$\begin{array}{ccc}
(A \oplus B) \otimes (C \oplus D) & \xrightarrow{=} & (A \otimes (C \oplus D)) \oplus (B \otimes (C \oplus D)) \\
{\scriptstyle \delta_L} \big\downarrow & & \big\downarrow {\scriptstyle \delta_L \oplus \delta_L} \\
((A \oplus B) \otimes C) \oplus ((A \oplus B) \otimes D) & & (A \otimes C) \oplus (A \otimes D) \oplus (B \otimes C) \oplus (B \otimes D) \\
 & \searrow^{=} & \big\downarrow {\scriptstyle \mathrm{id} \oplus \sigma_\oplus \oplus \mathrm{id}} \\
 & & (A \otimes C) \oplus (B \otimes C) \oplus (A \otimes D) \oplus (B \otimes D)
\end{array}$$

D SUPPLEMENTARY MATERIAL FOR SEC. 8

```haskell
module Demo where

-- A class for booleans with, possibly,
-- a square root of negation

class Enum a => B a where
  falseB    :: a
  trueB     :: a
  notB      :: a -> a
  sqrtNotB  :: a -> a
  evenB     :: a -> Bool
  evenB     = even . fromEnum

-- The classical instance has no square root

instance B Bool where
  falseB    = False
  trueB     = True
  notB      = not
  sqrtNotB  = error "No classical sqrt of not"
```

```haskell
-- Now define "big" booleans: Zero and Two are the
-- classical booleans; One and Three are intermediate
-- values along the negation trajectories

data Four = Zero | One | Two | Three

-- Create the trajectories for boolean negation:
-- Zero -> One -> Two
-- Two -> Three -> Zero

instance Enum Four where
  toEnum 0 = Zero
  toEnum 1 = One
  toEnum 2 = Two
  toEnum 3 = Three
  toEnum n = toEnum (n `mod` 4)
  fromEnum Zero = 0
  fromEnum One = 1
  fromEnum Two = 2
  fromEnum Three = 3

instance B Four where
  falseB    = Zero
  trueB     = Two
  notB      = succ . succ
  sqrtNotB  = succ

-- When boolean negation is applied to Zero, it produces Two after
-- "internally" visiting the intermediate value One. Although
-- the particular internal values are not exposed, the evenB
-- method reveals whether the underlying value is a "whole" or
-- "partial" boolean.

data Classification = Balanced | Constant

-- An analogue of Deutsch's problem.
-- We have four functions defined on abstract booleans:
-- two constant functions (f0 and f1) and two balanced
-- functions (f2 and f3)

f0, f1, f2, f3 :: B a => a -> a
f0 a = falseB
f1 a = trueB
f2 a = a
f3 a = notB a

-- Classically the given function is applied twice to
```

```haskell
-- classify it as Balanced or Constant

deutschC :: (Bool -> Bool) -> Classification
deutschC f = if f False == f True then Constant else Balanced

-- If we can observe the values introduced by the square
-- roots, we only need one application!

deutschF :: (Four -> Four) -> Classification
deutschF f = if evenB (f (sqrtNotB falseB)) then Constant else Balanced
```