A Complete Equational Theory for Quantum Circuits with Generalized Control

William Schober
Università della Svizzera italiana
Lugano, Switzerland
`william.schober@usi.ch`

Scott Wesley
Dalhousie University
Halifax, Canada
`scott.wesley@dal.ca`

Controlled subcircuits are commonplace in quantum algorithms as they represent the quantum analogue of branching statements (`if then`). We introduce a generalization of controlled subcircuits in the form of a binary operation which sends pairs of unitary quantum circuits to a generalized controlled operation, whose semantics are based on matrix exponentials and logarithms. The family of quantum circuits with generalized controlled operations and circuit exponentiation is denoted **HQC** for Hierarchical Quantum Circuits. We formalize **HQC** as a modified prop category using a novel category-theoretic construction, and provide a sound and complete equational theory for diagrammatic reasoning in **HQC**.

1 Introduction

As quantum computing hardware continues to advance, so too does its software. While quantum circuits remain the de facto standard language for low-level quantum programming, they are cumbersome when designing large-scale programs with tens of thousands of gates. Higher-level abstractions of quantum circuits are on the horizon. Diagrammatic reasoning [8] is a natural fit for reasoning about such abstractions since quantum circuits are diagrams. Diagrammatic reasoning has already been applied to a variety of circuit-related tasks, including optimization [19], simulation [31, 32], equivalence checking [26], and error correction [18, 20, 27]. Equational theories are collections of equations that serve as toolboxes for performing diagrammatic reasoning.

Control is one such ubiquitous abstraction in quantum algorithm design. Controlled subcircuits appear in essentially every powerful quantum algorithm (e.g., [21, 30, 12, 14]). We generalize the existing notion of control by allowing a subcircuit to be controlled not just by one qubit in a particular basis, but by an arbitrary basis on any number of qubits. This notion of control is captured by a new binary operation ($\odot$) called the *control product* which joins two subcircuits together to create a generalized controlled operation. The simplest example is the CNOT, which is created by joining the Pauli Z and X gates together as $Z \odot X = \mathsf{CNOT}$. However unlike the normal notion of control, the control product allows any two subcircuits U and V of arbitrary sizes to control each other as $U \odot V$. Examples of how such a product can aid in circuit design and verification are found in [11] and [28], respectively.

We present the control product formally in the language of symmetric monoidal categories, as part of a universal algebraic (see [1]) extension of a prop category [24, 3, 7]. We then provide a sound and complete equational theory for performing diagrammatic reasoning on the category **HQC** of *hierarchical quantum circuits*, that is, quantum circuits with generalized control and circuit exponentiation. We note that the definition of circuit exponentiation used in this paper is consistent with the power modifier in OpenQASM 3 [9].

Submitted to:
CONF 0000

Related work. The first complete equational theory for uncontrolled quantum circuits was presented in [7] and improved in [5, 4]. Two recent works have provided equational theories for standard controlled quantum circuits using controlled props [10] and rig categories [15]. Another recent work introduced a related methodology for constructing controlled unitaries via subspace selection and phasing [16]. The control product we introduce here can be seen as a way to efficiently package exponentially many such selection-and-phasing statements together into one circuit object. Controlled operations have also recently been studied in the context of quantum control flow [35, 33] for its applications to quantum computer architectures with a quantum program counter.

Structure and contents. All proofs are found in the appendices. Section 2 provides the necessary mathematical background. Section 3 introduces the semantics of control and exponentiation on unitary matrices and provides a characterization in terms of control functors. Section 4 constructs the hierarchical quantum circuit language **HQC**. We describe the inductive construction that is used to generate **HQC** via closures over an increasing family of nested sub-languages, provide its semantics, and present a sound equational theory. In Section 5 we prove completeness of the equational theory for **HQC** via a reduction to a known complete equational theory for controlled quantum circuits found in [10]. This reduction includes a transpilation procedure which transforms hierarchical circuits into quantum circuits with standard controls.

2 Background

We assume familiarity with symmetric monoidal categories (see [23]) and introductory functional analysis (see [13]). Given a functor $F : \mathcal{C} \to \mathcal{D}$, we write $\mathrm{Ob}(F)$ for underlying mapping on objects and $\mathrm{Mor}(F)$ for the underlying mapping on morphisms. We write $\{X, Y, Z\}$ for the standard Pauli matrices, $\mathbb{I}_n$ for the $n \times n$ identity matrix, and $\mathbb{O}_n$ for the $n \times n$ zero matrix. As described in Section A, we write $P(\Sigma)$ for the free prop category on a signature Σ with symmetry (σ).

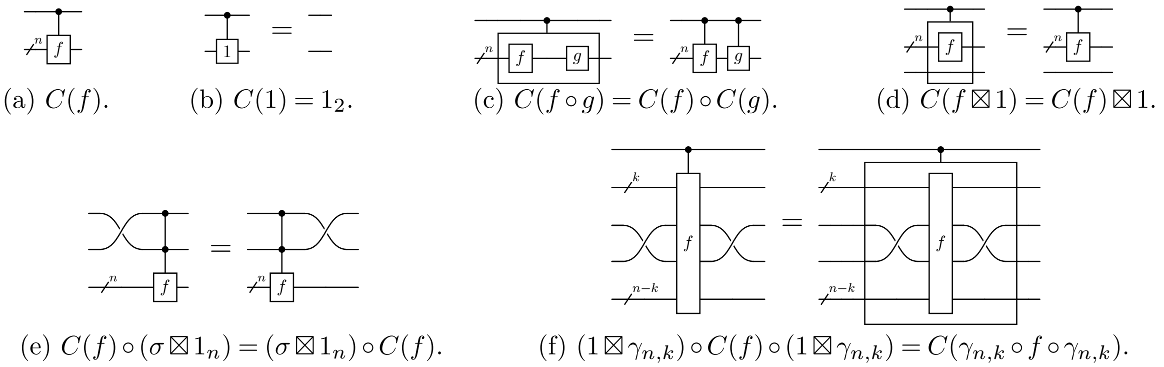
Matrix Exponentials. If M is a matrix, then $\exp(M) = \sum_{n=0}^{\infty} \frac{M^n}{n!}$. Clearly $\exp(\mathbb{O}_n) = \mathbb{I}_n$ and $\exp(M \otimes \mathbb{I}_n) = \exp(M) \otimes \mathbb{I}_n$. If H is a skew Hermitian matrix, then $U = \exp(H)$ is a unitary matrix and H is a *logarithm* of U. For each unitary matrix U, there exists a unique logarithm $H = \mathrm{Log}(U)$ of U such that all eigenvalues of H fall within $i(-\pi, \pi]$. If H is an n-dimensional Hermitian matrix with eigenvalues $\{\alpha_j\}_{j=1}^n$ and an associated orthonormal eigenbasis $\{b_j\}_{j=1}^n$, then $\exp(iH) = \sum_{j=1}^n e^{i\alpha_j} \left|b_j\right\rangle \left\langle b_j\right|$. The matrix exponential enjoys several useful properties [13].

$$\text{If } MN = NM, \text{ then } \exp(N+M) = \exp(N)\exp(M). \tag{1}$$

$$\text{If } U \text{ is unitary, then } \exp(iU^\dagger H U) = U^\dagger \exp(iH) U \text{ and } \mathrm{Log}(iU^\dagger H U) = U^\dagger \mathrm{Log}(iH) U. \tag{2}$$

Dagger Props. A functor $F : \mathcal{C} \to \mathcal{C}^{\mathbf{op}}$ is said to be *involutive* if $F \circ F = 1_{\mathcal{C}}$. A *dagger prop* is a prop category $\mathcal{C}$ with an involutive monoidal functor $\dagger : \mathcal{C} \to \mathcal{C}^{\mathrm{op}}$. The application of $\dagger$ to $f \in \mathcal{C}(n,m)$ is denoted $f^\dagger \in \mathcal{C}(m,n)$. Since $\dagger$ is contravariant, then $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$. If $f^\dagger$ is a two-sided inverse to f, then f is *unitary.*

Controlled Props. If $\mathcal{C}$ is a category, then $\mathcal{C}_{\mathbf{endo}}$ denotes the subcategory of endomorphisms in $\mathcal{C}$. A *controlled prop* [10] is a prop category $\mathcal{C}$ with an ordinary functor $C : \mathcal{C}_{\mathbf{endo}} \to \mathcal{C}_{\mathbf{endo}}$ such that $\mathrm{Ob}(C)(n) = n+1$ and the equations in Fig. 1 hold where $\gamma_{n,k} = 1_k \boxtimes \sigma \boxtimes 1_{n-k}$. A controlled



(a) $C(f)$. (b) $C(1) = 1_2$. (c) $C(f \circ g) = C(f) \circ C(g)$. (d) $C(f \boxtimes 1) = C(f) \boxtimes 1$.

(e) $C(f) \circ (\sigma \boxtimes 1_n) = (\sigma \boxtimes 1_n) \circ C(f)$. (f) $(1 \boxtimes \gamma_{n,k}) \circ C(f) \circ (1 \boxtimes \gamma_{n,k}) = C(\gamma_{n,k} \circ f \circ \gamma_{n,k})$.

Figure 1: The definition of a control functor stated in terms of graphical equations.

prop is (u,v)-*pointed* [10] when there exists $u, v \in \mathcal{C}(0,1)$ such that $C(f) \circ (u \boxtimes 1_n) = u \boxtimes f$ and $C(f) \circ (v \boxtimes 1_n) = v \boxtimes 1_n$ for each $f \in \mathcal{C}(n,n)$. A *dagger controlled prop* [10] is a dagger prop $(\mathcal{C}, \dagger)$ with a choice of control functor $C : \mathcal{C}_{\mathbf{endo}} \to \mathcal{C}_{\mathbf{endo}}$ satisfying the equation $C \circ \dagger = \dagger \circ C$. A *conjugated controlled prop* [10] is a dagger controlled prop $(\mathcal{C}, \dagger, C)$ which satsifies the equation $C(g^\dagger \circ f \circ g) = (1 \boxtimes g^\dagger) \circ C(f) \circ (1 \boxtimes g)$ for each $f \in \mathcal{C}(n,n)$ and $g \in \mathcal{C}(m,n)$. Given a prop signature Σ, it is possible to extend the construction of $P(\Sigma)$ to obtain a controlled prop $P_C(\Sigma)$. The morphisms in $P_C(\Sigma)$ must also satisfy the equation that $C(f) \in P_C(\Sigma)(n+1, n+1)$ for each $f \in P_C(\Sigma)(n,n)$. The morphisms in $P_C(\Sigma)$ are also subject to the following equations.

- **C-Functoriality**. $C(1) = 1_2$ and $C(g \circ f) = C(g) \circ C(f)$ for each $f : n \to n$ and $g : n \to n$.
- **Controlled Identity**. $C(f \boxtimes 1) = C(f) \boxtimes 1$ for each $f : m \to m$.
- **Control Symmetry**. $(\sigma \boxtimes 1_n) \circ C(C(f)) = C(C(f)) \circ (\sigma \boxtimes 1_n)$ for each $f : n \to n$.
- **Data Symmetry**. $(1 \boxtimes \gamma_{n,k}) \circ C(f) \circ (1 \boxtimes \gamma_{n,k}) = C(\gamma_{n,k} \circ f \circ \gamma_{n,k})$ for each $f : n+2 \to n+2$.

Just as $P(\Sigma)$ is free with respect to strict monoidal functors, it is straight-forward to show that the category $P_C(\Sigma)$ is free with respect to strict monoidal functors that preserve controls. A graphical language for $P_C(\Sigma)$ can be found in Fig. 1.

Rewriting in Props. Let Σ be a prop signature. A Σ-*equation* is a pair (f, g) of morphisms from $\mathrm{Mor}(P(\Sigma))$ such that $\mathrm{dom}(f) = \mathrm{dom}(g)$ and $\mathrm{cod}(f) = \mathrm{cod}(g)$. A set of Σ-equations is called a *prop congruence relation* if it is transitive, reflexive, symmetric, and closed under both sequential and parallel composition. In particular, the following congruence conditions hold for each $f, g \in P(\Sigma)(n,m)$.

1. If $(f,g) \in E$ with $h : s \to n$ and $k : t \to m$, then $(k \circ f \circ h, k \circ g \circ h) \in E$.
2. If $(f,g) \in E$ with $h : s \to t$ and $k : x \to y$, then $(h \boxtimes f \boxtimes k, h \boxtimes g \boxtimes k) \in E$.

A set of Σ-equations E from $\mathrm{Mor}(P_C(\Sigma))$ is called a *controlled prop congruence relation* if it also satisfies $(C(f), C(g)) \in E$ for each $(f,g) \in E$. Given a set of Σ-equations E, there exists a minimal congruence relation R such that $E \subseteq R$. There then exists a unique prop $P(\Sigma)/E$ with a unique projection $\pi_E : P(\Sigma) \to P(\Sigma)/E$ such that the following equations hold (see [6]).

1. $\pi_E(f) = \pi_E(g)$ if and only if $(f,g) \in R$.
2. If $F : P(\Sigma) \to \mathcal{C}$ is a prop functor and $F(f) = F(g)$ for each $(f,g) \in E$, then there exists a unique prop functor $F_E : P(\Sigma)/E \to \mathcal{C}$ such that $F_E \circ \pi_E = P(F)$.

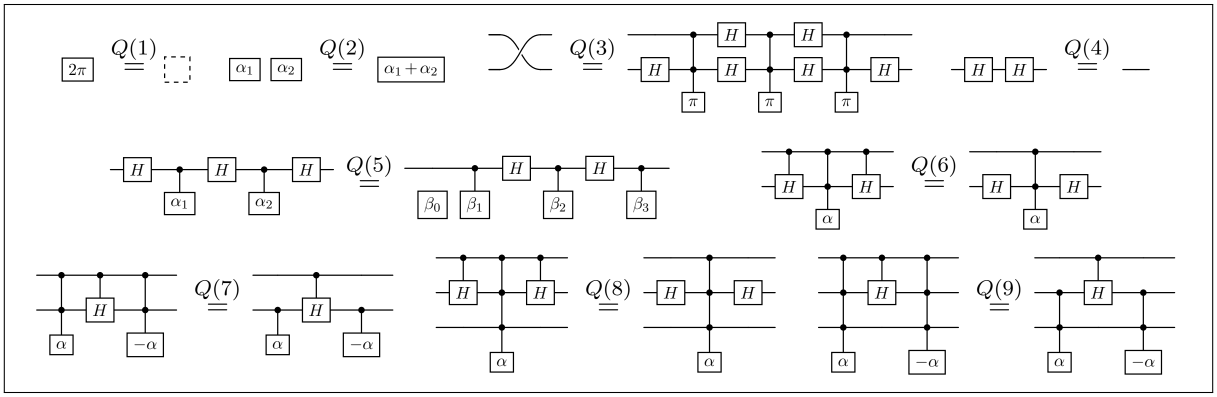


Figure 2: A known equational theory [10] for the category of controlled quantum circuits, where $\alpha, \alpha_1, \alpha_2 \in \mathbb{R}$ and $(\beta_0, \beta_1, \beta_2, \beta_3) = \mathsf{Euler}(\alpha_1, \alpha_2)$ as defined in Section B.

This extends readily to controlled prop categories and their functors. The pair (Σ, E) is said to be a *prop presentation* for the class of props isomorphic to $P(\Sigma)/E$. In particular, if $F : P(\Sigma) \to \mathcal{C}$ is surjective, then a presentation for $\mathcal{C}$ is a pair (Σ, E) such that $(f, g) \in E$ if and only if $F(f) = F(g)$. Often E is called a *complete equational theory* for $\mathcal{C}$ and F is called a *semantic interpretation* and is denoted $[\![-]\!]_{\mathcal{C}}$. We write $f \approx_E g$ when (f, g) is in the congruence relation induced by E.

Quantum Control. Let **Unitary** denote the prop category of unitary matrices and $\{|0\rangle, |1\rangle\}$ denote the computational basis for $\mathbb{C}^2$. It is well known that **Unitary** is a dagger prop with $\dagger : \mathbf{Unitary} \to \mathbf{Unitary}^{\mathrm{op}}$ sending each matrix U to its conjugate transpose $U^\dagger$. For each $d \in \mathbb{N}$, there is a prop subcategory $\mathbf{Unitary}_d$ of **Unitary** such that $\mathbf{Unitary}_d(n,n) = \mathbf{Unitary}(d^n, d^n)$. It was shown in [10] that $C(f : n \to n) = |0\rangle\langle 0| \otimes \mathbb{I}_n + |1\rangle\langle 1| \otimes f$ is a conjugated control functor for $\mathbf{Unitary}_2$ with points $(|0\rangle, |1\rangle)$. It was further shown that $\mathbf{Unitary}_2$ admits a controlled prop presentation **CQC** with generators $\Sigma_{\mathbf{CQC}} = \{ -\boxed{H}- \} \cup \{ \boxed{\alpha} : \alpha \in \mathbb{R} \}$ and relations Q as depicted in Fig. 2. The semantic interpretation for this theory is generated by $[\![-\boxed{H}-]\!]_C = H$ and $[\![\boxed{\alpha}]\!]_C = e^{i\alpha}$ where H is the Hadamard matrix.

3 The Semantics of Generalized Controls

This section introduces an operation $(\odot)$ called the *control product* which provides a symmetric generalization of controlled operations in unitary quantum circuits. We begin by defining an assignment $\odot : \mathbf{Unitary} \times \mathbf{Unitary} \to \mathbf{Unitary}$ on unitary matrices. If U and V are two unitary matrices, then we define $U \odot V = \exp(\mathrm{Log}(U) \otimes \mathrm{Log}(V)/(i\pi))$. The normalization factor $1/(i\pi)$ restricts the eigenvalues of the Hermitian matrix to $(-\pi, \pi]$, and consequently $(\odot)$ is associative.

Theorem 3.1. *The control product is unital and associative with unit* (-1). *Moreover, given a sequence* $U_1, U_2, \ldots, U_n \in \mathrm{Mor}(\mathbf{Unitary})$, $\bigodot_{j=1}^{n} U_j = \exp\left(i\pi \cdot \bigotimes_{j=1}^{n} \frac{\mathrm{Log}(U_j)}{i\pi} \right)$.

Unfortunately, the control product is not a bifunctor since $U \odot (V \circ W) \neq (U \odot V) \circ (U \odot W)$ in general. However, the control product does enjoy many desirable properties. For example, if the first coordinate is fixed to Z, then for each $U \in \mathbf{Unitary}(n,n)$, $Z \odot U = |0\rangle\langle 0| \otimes \mathbb{I}_n + |1\rangle\langle 1| \otimes U$. That is to say, $Z \odot (-)$ is the standard canonical control functor on $\mathbf{Unitary}_2$. It follows that $Z \odot X$ is a CNOT gate and $Z \odot Z$ is a CZ gate. Since $X \odot (-)$ is also a control functor, then this formalization suggests that the CNOT gate is also a Z-gate controlled in the X-basis. This insight can be used to explain phase kickback [25]. Of course, it is natural to ask for which $U \in \mathrm{Mor}(\mathbf{Unitary})$ will $U \odot (-)$ be a control functor. This is answered by the following theorem.

Theorem 3.2. *Let H be an n-dimensional Hermitian matrix with eigenvalues $\{\alpha_j\}_{j=1}^{n}$ in $(-1,1]$ and orthonormal eigenbasis $\{b_j\}_{j=1}^{n}$. If $U = \exp(iH\pi)$, then $U \odot V = \sum_{j=1}^{n} |b_j\rangle \langle b_j| \otimes V^{\alpha_j}$ for each $V \in \mathrm{Mor}(\mathbf{Unitary})$. In particular, $Z \odot V = |0\rangle\langle 0| \otimes \mathbb{I}_m + |1\rangle\langle 1| \otimes V$ for $V \in \mathbf{Unitary}(m,m)$.*

Corollary 3.3. *If $U \in \mathbf{Unitary}(d,d)$ and $F(-) = U \odot (-)$, then the following conditions hold.*

- ***C1**. $F(\mathbb{I}_n) = \mathbb{I}_{dn}$ for each $n \in \mathbb{N}$.*
- ***C2**. $F(V \otimes \mathbb{I}_n) = F(V) \otimes \mathbb{I}_n$ for each $n \in \mathbb{N}$ and $V \in \mathrm{Mor}(\mathbf{Unitary})$.*
- ***C3**. $F(F(V)) \circ (\sigma_{d,d} \otimes \mathbb{I}_n) = (\sigma_{d,d} \otimes \mathbb{I}_n) \circ F(F(V))$ for each $V \in \mathbf{Unitary}(n,n)$ where $\sigma_{d,d}$ is the monoidal symmetry $\mathbb{C}^d \otimes \mathbb{C}^d \cong \mathbb{C}^d \otimes \mathbb{C}^d$.*
- ***C4**. $F(P^\dagger \circ V \circ P) = (\mathbb{I}_d \otimes P^\dagger) \circ F(V) \circ (\mathbb{I}_d \otimes P)$ for each $V, P \in \mathbf{Unitary}(n,n)$.*

The assignment $F(-)$ is a functor if and only if U is Hermitian. Moreover, if $F(-)$ is a functor, then $F(-)$ restricts to a conjugated control functor on $\mathbf{Unitary}_d$. This control functor is (u,v)-pointed if and only if $U|u\rangle = -|u\rangle$ and $U|v\rangle = |v\rangle$.

Theorem 3.2 establishes a relation between control products and matrix powers. Moreover, if $\alpha \in (-1,1]$, then $U^\alpha = U \odot e^{i\alpha\pi}$. Unfortunately, matrix powers are only well-behaved for small choices of α, as illustrated by the following theorem. In general, the properties of exponentiation will depend on the eigenvalues of U. To this end, we will say that λ_j is *(α,β)-admissible* if either $\alpha\lambda_j \in (-1,1]$ or $\beta \in \mathbb{Q}$ with reduced denominator dividing $\lceil (\alpha\lambda_j - 1)/2 \rceil$.

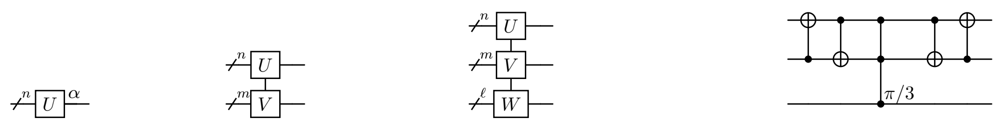
Theorem 3.4. *For $\alpha \in \mathbb{R}$, $U \odot e^{i\alpha\pi} = U^\alpha$ for all $U \in \mathrm{Mor}(\mathbf{Unitary})$ if and only if $\alpha \in (-1,1]$. If $U \in \mathrm{Mor}(\mathbf{Unitary})$ is Hermitian, then $U \odot e^{i\alpha\pi} = U^\alpha$ for all $\alpha \in \mathbb{R}$.*

Theorem 3.5. *Let $U \in \mathbf{Unitary}(n,n)$ with $\{\lambda_j\}_{j=1}^{n}$ the eigenvalues of $\mathrm{Log}(U)/(i\pi)$. For each $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$, $(U^\alpha)^\beta = U^{\alpha\beta}$ if and only if for each $j \in \{1,2,\ldots,n\}$, λ_j is (α,β)-admissible. This means that $\mathbb{Z}$ and $(-1,1]$ are maximal submonoids of $(\mathbb{R},\cdot)$ for which $(U,\alpha) \mapsto U^\alpha$ defines a monoid action on $\mathrm{Mor}(\mathbf{Unitary})$.*

It was shown in [28] that generalized controls emerge naturally when studying quantum algorithms using the techniques of [11]. Moreover, Theorem 3.2 and Theorem 3.4 show that generalized controls are inherently connected with the matrix powers already used in quantum programming languages such as OpenQASM 3 [9]. Ideally, one would hope that the intuition for standard controls and scalar powers would generalize to this setting. It is clear from Corollary 3.3 and Theorem 3.5 that neither of these hopes hold true. For example, integer exponentiation (i.e., repeating and inverting circuits) does not interact well with unit fraction exponentiation (i.e., computing roots of circuits), despite these two operations being fundamentally related. This motivates the study of complete equational theories, which could be used to work soundly with these constructs in the context of circuit optimization, simulation, and equivalence checking.

4 Props with Exponentiation and Generalized Control

Hierarchical quantum circuits build upon the prop formalism by introducing two new connectives, namely $(\odot)$ and $(\uparrow)$. The $(\odot)$ connective can be thought of as an abstraction of generalized



(a) $U \uparrow \alpha$. (b) $U \odot V$. (c) $U \odot V \odot W$. (d) $U \in \mathbf{HQC}[2](3,3) \setminus \mathbf{HQC}[1](3,3)$.

Figure 3: A graphical language for the morphisms in $\mathbf{HQC}$. In these diagrams we assume that $U : n \to n$, $V : m \to m$, and $W : \ell \to \ell$.

control, and the ($\uparrow$) connective can be thought of as an abstraction of circuit exponentiation. As outlined in the previous section, the ($\odot$) connective should be associative, though few assumptions can be made about the ($\uparrow$) connective. In particular, neither ($\odot$) nor ($\uparrow$) are functorial in general. This means that unlike a controlled prop, it does not suffice to simply complete a standard prop under the application of two functors. Instead, the hierarchical language will be constructed in levels, with the lowest level corresponding to a standard prop.

The basic idea of this construction is that given a free prop $P(\Sigma)$, the powers and generalized controls can be freely constructed as purely syntactic objects. Since circuits in $P(\Sigma)$ are equal up to diagram isomorphism, then their exponentiated and controlled forms will also be equal up to isomorphism of their subcircuit constituents. These syntactic objects are then combined with the gates in Σ to generate a strictly larger prop containing $P(\Sigma)$, and the process repeats. More formally, the construction proceeds as follows.

Exponentiation. Let $\mathcal{C}$ be a prop category. If $U \in \mathrm{Mor}(\mathcal{C})$ and $\alpha \in \mathbb{R}$, then there should be a unique term $U \uparrow \alpha$ which is thought of as exponentiating U by α. Since we do not require exponentiation to satisfy any further properties, then $\mathsf{Power}(\mathcal{C}) = \mathrm{Mor}(\mathcal{C}) \times \mathbb{R}$. We write $U \uparrow \alpha$ for an element $(U, \alpha) \in \mathsf{Power}(\mathcal{C})$. Of course, $\mathrm{dom}(U \uparrow \alpha) = \mathrm{dom}(U)$ and $\mathrm{cod}(U \uparrow \alpha) = \mathrm{cod}(U)$. A term of the form $U \uparrow \alpha$ is denoted by raising U to the power of α, as depicted in Fig. 3a.

Generalized Controls. Let $\mathcal{C}$ be a prop category. Since ($\odot$) is known to be associative, then it suffices to generate the free monoid $\mathrm{Mor}(\mathcal{C})^*$ on $\mathrm{Mor}(\mathcal{C})$. We write $U_1 \odot U_2 \odot \cdots \odot U_n$ for an element $(U_1, U_2, \ldots, U_n) \in \mathrm{Mor}(\mathcal{C}^*)$. Of course, only terms of length two or more correspond to valid generalized controls in the circuit language. We write $\mathsf{Tower}(\mathcal{C}) := \{T \in \mathrm{Mor}(\mathcal{C})^* : |T| \geq 2\}$. If $T \in \mathsf{Tower}(\mathcal{C})$, then $\mathrm{dom}(T) = \sum_{j=1}^{n} \mathrm{dom}(T_j)$ and $\mathrm{cod}(T) = \sum_{j=1}^{n} \mathrm{cod}(T_j)$ where $n = |T|$. An n-ary ($\odot$)-product is illustrated by a vertical wire joining the n factors, as in Fig. 3b and Fig. 3c.

Constructing the Hierarchy. The construction begins with a primitive gate set $\Sigma_{\mathbf{Prim}}$. In the case of this paper, $\Sigma_{\mathbf{Prim}} = \{$ ─●─ , ─○─ , ─⊕─ , ─⊖─ , ─$\boxed{H}$─ , • $\}$. This gives rise to a free prop $\mathbf{HQC}[0] = P(\Sigma^0_{\mathbf{HQC}})$ where $\Sigma^0_{\mathbf{HQC}} = \Sigma_{\mathbf{Prim}}$. The construction then proceeds inductively as follows. For each $n \in \mathbb{N}$, define a signature $\Sigma^{n+1}_{\mathbf{HQC}} = \Sigma^n_{\mathbf{HQC}} \cup \mathsf{Tower}(\mathbf{HQC}[n]) \cup \mathsf{Power}(\mathbf{HQC}[n])$ and a prop category $\mathbf{HQC}[n+1] = P(\Sigma^{n+1}_{\mathbf{HQC}})$. Since $\Sigma^n_{\mathbf{HQC}} \subseteq \Sigma^{n+1}_{\mathbf{HQC}}$, then this construction can be summarized by the following diagram.

$$\begin{tikzcd}
\Sigma^0_{\mathbf{HQC}} \arrow[r, hook] \arrow[d, hook] & \Sigma^1_{\mathbf{HQC}} \arrow[r, hook] \arrow[d, hook] & \Sigma^2_{\mathbf{HQC}} \arrow[r, hook] \arrow[d, hook] & \cdots \arrow[r, hook] & \Sigma^n_{\mathbf{HQC}} \arrow[r, hook] \arrow[d, hook] & \cdots \\
U(\mathbf{HQC}[0]) \arrow[r, hook] & U(\mathbf{HQC}[1]) \arrow[r, hook] & U(\mathbf{HQC}[2]) \arrow[r, hook] & \cdots \arrow[r, hook] & U(\mathbf{HQC}[n]) \arrow[r, hook] & \cdots
\end{tikzcd}$$

Since $\mathrm{Mor}(\mathbf{HQC}[n]) \subseteq \mathrm{Mor}(\mathbf{HQC}[n+1])$, then there is an identification of monoid generators such that $\mathsf{Tower}(\mathbf{HQC}[n]) \leq \mathsf{Tower}(\mathbf{HQC}[n+1])$. We will assume this identification, such that if $T \in \mathsf{Tower}(\mathbf{HQC}[n])$ and $S \in \mathsf{Tower}(\mathbf{HQC}[n+1])$, then $T \odot S = T_1 \odot (T_2 \odot (\cdots \odot (T_k \odot S)))$ where $k = |T|$. The categorical colimit of this construction is denoted $\mathbf{HQC}$, so that $\mathbf{HQC} = P(\Sigma_{\mathbf{HQC}})$ where $\Sigma_{\mathbf{HQC}} = \bigcup_{n=0}^{\infty} \Sigma_{\mathbf{HQC}}^{n}$. The following lemmas characterize how to map freely out of $\mathbf{HQC}$.

Lemma 4.1. *Let $\Sigma_0^* = \Sigma_{\mathbf{HQC}}^0$ and $\Sigma_{n+1}^* = \Sigma_{\mathbf{HQC}}^{n+1} \setminus \Sigma_{\mathbf{HQC}}^{n}$ for each $n \in \mathbb{N}$. If $\{\tau_n : \Sigma_n^* \to U(\mathcal{C})\}_{n=0}^{\infty}$ is a family of prop signature morphisms, then there exists a unique prop functor $F : \mathbf{HQC} \to \mathcal{C}$ such that $F(g) = \tau_n(g)$ for each $n \in \mathbb{N}$ and $g \in \Sigma_n^*$.*

Lemma 4.2. $\Sigma_{\mathbf{HQC}} = \Sigma_{\mathbf{Prim}} \sqcup \Sigma_{\mathbf{Ctrl}} \sqcup \Sigma_{\mathbf{Pow}}$ *where* $\Sigma_{\mathbf{Ctrl}} = \{U \odot V : U, V \in \mathrm{Mor}(\mathbf{HQC})\}$ *and* $\Sigma_{\mathbf{Pow}} = \{U \uparrow \alpha : U \in \mathrm{Mor}(\mathbf{HQC})$ *and* $\alpha \in \mathbb{R}\}$.

It should come as no surprise that the standard semantic interpretation for $\mathbf{HQC}$ is defined in terms of the generalized controls and exponentiation in $\mathbf{Unitary}$. It follows from Lemma 4.1 that the following set of equations defines a unique prop functor $[\![-]\!]_H : \mathbf{HQC} \to \mathbf{Unitary}$. Note that this is well-defined since $(\odot)$ is also associative for $\mathbf{Unitary}$ by Theorem 3.1.

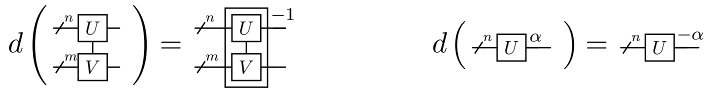
$$s_0(-\bullet-) = Z \qquad s_0(-\circ-) = -Z \qquad s_0(-\oplus-) = X \qquad s_0(-\ominus-) = -X \qquad s_0(\bullet) = -1$$

$$s_0\left(-\boxed{H}-\right) = H \qquad s_{n+1}(U_1 \odot \cdots \odot U_k) = s_n(U_1) \odot \cdots \odot s_n(U_k) \qquad s_{n+1}(U \uparrow \alpha) = s_n(U)^{\alpha}$$

The following set of equations are also well-defined by Lemma 4.2, and define a unique prop functor $\dagger : \mathbf{HQC} \to \mathbf{HQC}^{\mathrm{op}}$ which sends each circuit in $\mathbf{HQC}$ to its syntactic adjoint.

$$d(-\bullet-) = -\bullet- \qquad d(-\circ-) = -\circ- \qquad d(-\oplus-) = -\oplus- \qquad d(-\ominus-) = -\ominus- \qquad d\left(-\boxed{H}-\right) = -\boxed{H}-$$

$$d(\bullet) = \bullet$$



Theorem 4.3. *If $U \in \mathrm{Mor}(\mathbf{HQC})$, then $[\![U^\dagger]\!]_H = [\![U]\!]_H^\dagger$.*

Given the syntactic adjoint map $(\dagger)$, it is then possible to define syntactic diagonalization. Fix some $n \in \mathbb{N}$ which will denote the number of wires in these circuits. Then for each $x \in \{0,1\}^n$ and $\alpha \in \mathbb{R}$, there exists a circuit $\lambda(x,\alpha) \in \mathbf{HQC}(n,n)$ such that $[\![\lambda(x,\alpha)]\!]_H = \exp(iH)$ where $H = \alpha \bigotimes_{j=0}^{n-1} |x_j\rangle\langle x_j|$. Moreover, $\lambda(x,\alpha)$ can be constructed entirely from NOT-gates and global phase gates with zero or more Z-controls (see Section E). A circuit Λ is in *diagonal form* if there exists a bijection $f : \{1,2,\ldots,2^n\} \to \{0,1\}^n$ and function $\alpha : \{1,2,\ldots,2^n\} \to (-\pi,\pi]$ such that $\Lambda = \lambda(f(1),\alpha(1)) \circ \cdots \circ \lambda(f(2^n),\alpha(2^n))$. Then a syntactic diagonalization of $U \in \mathbf{HQC}(n,n)$ is a choice of diagonal form $\Lambda \in \mathbf{HQC}(n,n)$ and $P \in \mathbf{HQC}(n,n)$ such that $[\![U]\!]_H = [\![P^\dagger \circ \Lambda \circ P]\!]_H$.

4.1 A Sound Equational Theory with Unitary Controls

The equational theory E for hierarchical quantum circuits can be found in Fig. 4. Some care must be taken when defining this equational theory, since Fig. 4 also includes congruence relations, such as $(V \approx_E W) \Rightarrow (U \odot V \approx_E U \odot W)$. To avoid cyclic reasoning, E must be defined inductively. First, let E_0 denote the set of relations described by E(1) through E(21). Then for each $n \in \mathbb{N}$, define E_{n+1} as follows.

$$\begin{aligned} E_{n+1} = E_n &\cup \{(V \uparrow \alpha, W \uparrow \alpha) : \alpha \in \mathbb{R} \text{ and } V \approx_{E_n} W\} && \text{(see E(22))} \\ &\cup \{(U \odot V, U \odot W) : U \in \mathrm{Mor}(\mathbf{HQC}) \text{ and } V \approx_{E_n} W\} && \text{(see E(23))} \end{aligned}$$

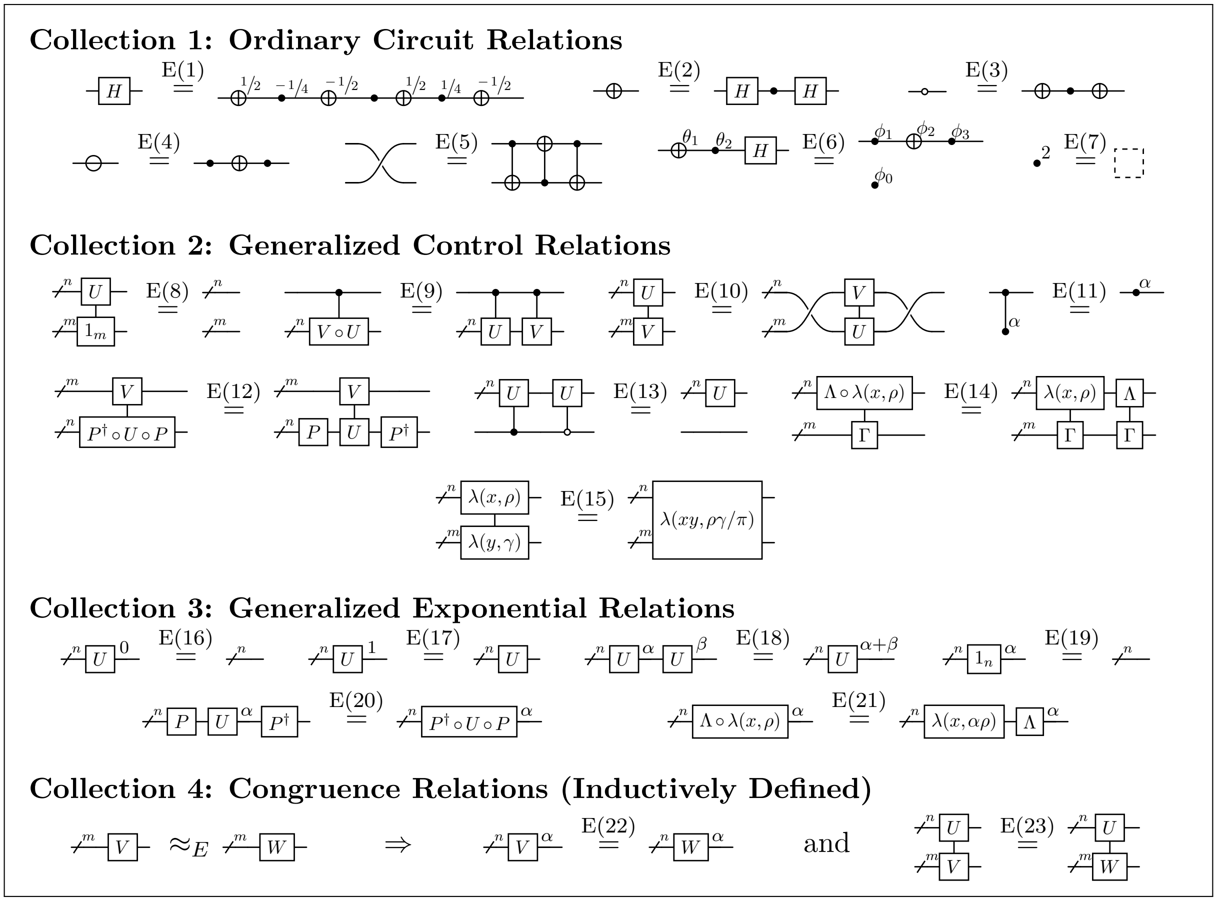


Figure 4: An equational theory for the category of hierarchical quantum circuits in which $\alpha, \beta, \theta_1, \theta_2 \in \mathbb{R}$, $(\phi_0\pi, \phi_1\pi, \phi_2\pi, \phi_3\pi) = \mathsf{Euler}(\theta_1\pi, \theta_2\pi)$, $x \in \{0,1\}^n$, $y \in \{0,1\}^m$, and $\rho, \gamma \in (-\pi, \pi]$. The circuits Λ and Γ are prefixes of diagonal forms such that a lambda generator with binary string x does not appear in Λ.

Then $E = \bigcup_{n=0}^{\infty} E_n$, so that $U \approx_E V$ if and only if there exists some $n \in \mathbb{N}$ such that $U \approx_{E_n} V$. It follows from $E(1-4)$ that all of $\mathbf{HQC}/E$ can be generated using only two of the three gates in { —•— , —⊕— , —H— } together with { • }. Moreover, the relations E(1) and E(2) are redundant and are only included to make these observations more evident (see Section J).

Theorem 4.4 (Soundness)**.** *If* $U \approx_E V$*, then* $[\![U]\!]_H = [\![V]\!]_H$*.*

Recall from the previous section that even though (†) mapped each circuit to its intended adjoint, it was not a dagger functor on **HQC**. This is because **HQC** was freely generated, and therefore unaware of the intended groupoid structure on **HQC**. However, it can be shown that $U \circ U^\dagger \approx_E 1_n \approx_E U^\dagger \circ_E U$ for each $U \in \mathbf{HQC}(n,n)$. In categorical terms, this means that (†) lifts to a dagger functor on the quotient category $\mathbf{HQC}/E$. Unfortunately, defining a dagger functor on a quotient of a free prop category can be tricky. To this end, Theorem 4.5 first introduces a general procedure which works in the case where all morphisms are intended to be unitary. The relations ensure that $P(\Sigma)/E$ is a groupoid and that H maps each morphism in $P(\Sigma)/E$ to its inverse. This theorem is then used in Theorem 4.7 to show that (†) lifts to a dagger functor.

Theorem 4.5. *Let Σ be a prop signature, $\tau : \Sigma \to U(P(\Sigma)^{op})$ a prop signature morphism, E a collection of Σ-equations, and $F : P(\Sigma) \to P(\Sigma)^{op}$ the unique prop functor satisfying the equation $\tau = U(F) \circ i$. If $F(g) \circ g \approx_E 1_{\mathrm{dom}(g)}$ and $g \circ F(g) \approx_E 1_{\mathrm{cod}(g)}$ for each $g \in \Sigma$, then there exists a unique prop functor $H : P(\Sigma)/E \to (P(\Sigma)/E)^{op}$ such that $H \circ \pi_E = \pi_E^{op} \circ F$. Moreover, H is a dagger functor and every morphism in $P(\Sigma)/E$ is unitary.*

Lemma 4.6. *If $U \in \mathbf{HQC}(n,n)$ and $\alpha \in \mathbb{R}$, then* $\overset{n}{\not-}\boxed{U}^{\alpha}\!-\!\boxed{U}^{-\alpha} \overset{E(18)}{\approx} \overset{n}{\not-}\boxed{U}^{0} \overset{E(16)}{\approx} \overset{n}{\not-}$.

Theorem 4.7. *$\pi_E^{op} \circ \dagger$ lifts to a unique dagger functor $\overline{\dagger} : \mathbf{HQC}/E \to (\mathbf{HQC}/E)^{op}$ and every morphism in $\mathbf{HQC}/E$ is unitary with respect to $(\overline{\dagger})$.*

It can then be shown that mapping each circuit U to a circuit $-\!\bullet\!- \odot U$ defines a dagger control functor on $\mathbf{HQC}/E$. This will be necessary to compare the prop presentation $(\Sigma_{\mathbf{HQC}}, E)$ with the controlled prop presentation $(\Sigma_{\mathbf{CQC}}, Q)$. To simplify this construction, it is first shown that every control functor on a category such as $\mathbf{HQC}/E$ must be unitary (Lemma 4.8). Using this lemma, a general procedure is then introduced for defining control functors on prop presentations (Theorem 4.9), which is then applied to $\mathbf{HQC}$ with $\tau_n(U : n \to n) = -\!\bullet\!- \odot U$ in Theorem 4.10. Note that all conditions except for (4) correspond directly to relations in E.

Lemma 4.8. *If $(\mathcal{C}, \dagger)$ is a dagger prop such that every morphism in $\mathcal{C}_{\mathbf{endo}}$ is unitary, then every control functor $C : \mathcal{C}_{\mathbf{endo}} \to \mathcal{C}_{\mathbf{endo}}$ is a dagger control functor.*

Theorem 4.9. *Let Σ be a prop signature consisting of endomorphic generators, E a collection of Σ-equations, and $\{\tau_n : P(\Sigma)(n,n) \to P(\Sigma)(n+1,n+1)\}_{n \in \mathbb{N}}$ be a family of ordinary functions. Consider the following list of properties which $\{\tau_n\}_{n \in \mathbb{N}}$ could satisfy.*

1. *If $n \in \mathbb{N}$, then $\tau_n(1_n) \approx_E 1_{n+1}$.*
2. *If $f : n \to n$ and $g : n \to n$, then $\tau_n(g \circ f) \approx_E \tau_n(g) \circ \tau_n(f)$.*
3. *If $f : n \to n$ and $(f,g) \in E$, then $\tau_n(f) \approx_E \tau_n(g)$.*
4. *If $f : n \to n$, then $\tau_{n+1}(f \boxtimes 1) \approx_E \tau(n) \boxtimes 1$.*
5. *If $f : n \to n$, then $\tau_{n+1}(\tau_n(f)) \approx_E (\sigma \boxtimes 1_n) \circ \tau_{n+1}(\tau_n(f)) \circ (\sigma \boxtimes 1_n)$.*
6. *If $f : n+2 \to n+2$ and $0 \le k \le n$, then $\tau_{n+2}(\gamma_{n,k} \circ f \circ \gamma_{n,k}) \approx_E (1 \boxtimes \gamma_{n,k}) \circ \tau_{n+2}(f) \circ (1 \boxtimes \gamma_{n,k})$.*

If conditions (1) and (2) hold, then there exists a unique ordinary functor $F : P(\Sigma) \to P(\Sigma)/E$ such that $\mathrm{Ob}(F)(n) = n+1$ and $F(f : n \to n) = \pi_E(\tau_n(f))$. If condition (3) also holds, then there exists a unique ordinary functor $H : P(\Sigma)/E \to P(\Sigma)/E$ such that $H \circ \pi_E = F$. If conditions (4) through to (6) also hold, then H is a control functor.

Theorem 4.10. *There exists a unique conjugated control functor $C : \mathbf{HQC}/E \to \mathbf{HQC}/E$ satisfying the equation $C(\pi_E(U)) = \pi_E(-\!\bullet\!- \odot U)$ for each $U \in \mathrm{Mor}(\mathbf{HQC})$.*

5 Equational Completeness

This section proves that E is a complete equational theory for $\mathbf{HQC}$ with respect to the semantic interpretation $[\![-]\!]_H$. The proof begins by showing that the equational theory is complete for the sub-language $\mathbf{Core}$ of $\mathbf{HQC}$ consisting of global phase gates, single qubit rotations, and controls in the Z-basis. The idea of this proof is to leverage the completeness of $(\Sigma_{\mathbf{CQC}}, Q)$ with respect to $[\![-]\!]_C$. We will first consider the simpler case, in which $(\Sigma_{\mathbf{CQC}}, Q)$ is a merely a prop presentation, as opposed to a controlled prop presentation.

1. Construct a functor $\mathsf{Enc} : \mathbf{Core} \to \mathbf{CQC}$ such that $[\![\mathsf{Enc}(-)]\!]_C = [\![-]\!]_H$. This means that if $[\![U]\!]_H = [\![V]\!]_H$, then $[\![\mathsf{Enc}(U)]\!]_C = [\![\mathsf{Enc}(V)]\!]_C$, which implies that $\mathsf{Enc}(U) \approx_Q \mathsf{Enc}(V)$.
2. Construct a functor $\mathsf{Dec} : \mathbf{CQC} \to \mathbf{Core}$ which respects the relations in Q. This means that for each relation $(X,Y) \in Q$ used to prove $\mathsf{Enc}(U) \approx_Q \mathsf{Enc}(V)$, there is a corresponding sequence of relations $\mathsf{Dec}(X) \approx_E \mathsf{Dec}(Y)$.
3. Ensure that $W \approx_E \mathsf{Dec}(\mathsf{Enc}(W))$ for all $W \in \mathrm{Mor}(\mathbf{HQC})$. This is because the decoder can only prove that $\mathsf{Dec}(\mathsf{Enc}(U)) \approx_E \mathsf{Dec}(\mathsf{Enc}(V))$.

Unfortunately, **CQC** is a free controlled prop, so Dec must map into the quotient $\mathbf{Core}/E$, as opposed to **Core**. This means that Dec maps each circuit in **CQC** to an equivalence class of circuits in **Core**, from which representative circuits must be chosen.

Theorem 5.1. *Let (Γ, Q) be a controlled prop presentation which is complete with respect to the interpretation $[\![-]\!]_\Gamma : P_C(\Gamma) \to \mathcal{C}$, and (Σ, E) be a prop presentation equipped with a control functor $C : P(\Sigma)/E \to P(\Sigma)/E$ and a prop functor $[\![-]\!]_\Sigma : P(\Sigma) \to \mathcal{C}$. Assume that there exists a prop functor $\mathsf{Enc} : P(\Sigma) \to P_C(\Gamma)$ and a controlled prop functor $\mathsf{Dec} : P_C(\Gamma) \to (P(\Sigma)/E, C)$ such that the following properties hold.*

1. *If $x \in \Sigma$, then $[\![\mathsf{Enc}(x)]\!]_\Gamma = [\![x]\!]_\Sigma$.*
2. *If $(X,Y) \in Q$, then there exists $X^* \in \mathsf{Dec}(X)$ and $Y^* \in \mathsf{Dec}(Y)$ such that $X^* \approx_E Y^*$.*
3. *If $x \in \Sigma$, then there exists $f \in \mathsf{Dec}(\mathsf{Enc}(x))$ such that $x \approx_E f$.*

Then (Σ, E) is complete with respect to the semantic interpretation $[\![-]\!]_\Sigma$.

It remains to show that the completeness results extend to all of **HQC**. The basic idea is to show that for each $U \in \mathrm{Mor}(\mathbf{HQC})$, there exists a $V \in \mathrm{Mor}(\mathbf{Core})$ such that $U \approx_E V$. This means that every circuit in **HQC** can be rewritten to a circuit in **Core**, in which E is already known to be complete.

Theorem 5.2. *Let $\Sigma \subseteq \Gamma$ be prop signatures with an equation theory (Σ, E) that is sound and complete with respect to $[\![-]\!] : P(\Gamma) \to \mathcal{C}$. If for each $g \in \Gamma$, there exists a $f \in P(\Sigma)$ such that $g \approx_E f$, then (Γ, E) is a complete equational theory with respect to $[\![-]\!]$.*

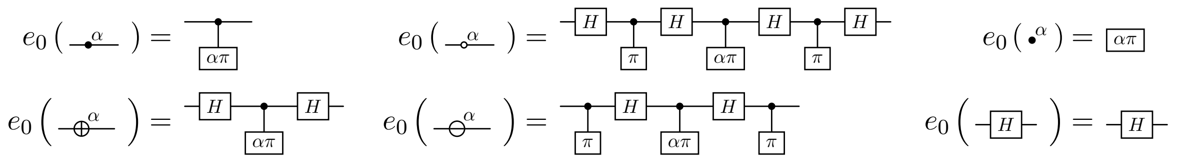
Constructing the Sub-Language. The sub-language is constructed inductively, starting from the gate set $\Sigma^0_{\mathbf{Core}} = \{ -\boxed{H}- \} \cup \{ \overset{\alpha}{-\bullet-}, \overset{\alpha}{-\circ-}, \overset{\alpha}{-\oplus-}, \overset{\alpha}{-\ominus-}, \bullet^{\alpha} : \alpha \in \mathbb{R}\}$. The construction then proceeds as follows. First, a free prop category $\mathbf{Core}[n] = P(\Sigma^n_{\mathbf{Core}})$ is constructed for each control depth $n \in \mathbb{N}$. The category at control depth n is then closed under a single application of the control functor, by setting $\Sigma^{n+1}_{\mathbf{Core}} = \Sigma^n_{\mathbf{Core}} \cup \{ -\bullet- \odot U : U \in \mathrm{Mor}(\mathbf{Core}[n])\}$ for each $n \in \mathbb{N}$. This yields an infinite diagram of chain of inclusions, as in Section 3. The categorical colimit of this sequence will be denoted **Core**. This means $\mathbf{Core} = P(\Sigma_{\mathbf{Core}})$ where $\Sigma_{\mathbf{Core}} = \bigcup_{n=0}^{\infty} \Sigma^n_{\mathbf{Core}}$. Clearly $C(-)$ restricts to $\mathbf{Core}/E$, since $-\bullet- \odot U$ is a representative of $C(\pi_E(U))$.

Lemma 5.3. *The functor $C : \mathbf{HQC}/E \to \mathbf{HQC}/E$ restricts to $\mathbf{Core}/E$.*

Unfortunately, $(\dagger)$ does not restrict to **Core** since $U \odot V \in \mathrm{Mor}(\mathbf{Core})$ does not imply that $(U \odot V) \uparrow (-1) \in \mathrm{Mor}(\mathbf{Core})$. However, there does exist a prop functor $\ddagger : \mathbf{Core} \to \mathbf{Core}^{\mathrm{op}}$ such that $U^\ddagger \approx_E U^\dagger$ for all $U \in \mathrm{Mor}(\mathbf{Core})$. It follows from Lemma 4.1 that the equations $d_0(g) = g^\dagger$ and $d_{n+1}(-\bullet- \odot U) = -\bullet- \odot d_n(U)$ define a prop functor $\ddagger : \mathbf{Core} \to \mathbf{Core}^{\mathrm{op}}$.

Lemma 5.4. *If $U \in \mathrm{Mor}(\mathbf{Core})$, then $U^\ddagger \approx_E U^\dagger$.*

Constructing the Encoder. The encode will be defined by the following set of equations, together with the inductive rule $e_{n+1}(\,\text{-}\bullet\text{-}\;\odot U)) = C(e_n(U))$ defined for each $n \in \mathbb{N}$.

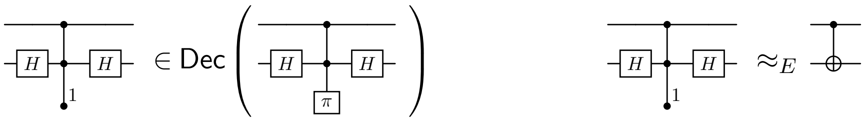


It follows immediately from Lemma 4.1 that this defines a prop functor $\mathsf{Enc} : \mathbf{Core} \to \mathbf{CQC}$. Moreover, this prop functor preserves the semantics of **HQC**. For gates in $\Sigma^0_{\mathbf{Core}}$, this follows by a direct matrix computation. For gates in $\Sigma^{n+1}_{\mathbf{Core}} \setminus \Sigma^n_{\mathbf{Core}}$, this follows from Theorem 3.2.

Lemma 5.5. *If* $g \in \Sigma_{\mathbf{Core}}$*, then* $[\![\mathsf{Enc}(g)]\!]_C = [\![g]\!]_H$.

Constructing the Decoder. Let $\mathsf{Dec} : \mathbf{CQC} \to (\mathbf{Core}/E, C)$ be the unique controlled prop functor defined by the equations $\mathsf{Dec}(\,\text{-}\boxed{H}\text{-}\,) = \pi_E(\,\text{-}\boxed{H}\text{-}\,)$ and $\mathsf{Dec}(\,\boxed{\alpha}\,) = \pi_E(\,\bullet^{\alpha/\pi}\,)$. The relations $Q(1)$, $Q(2)$, and $Q(5)$ appear in the set of relations for **HQC**, and are therefore respected by $\mathsf{Dec}(-)$. The relation $Q(4)$ is also respected by $\mathsf{Dec}(-)$ since it is an instance of unitarity. The relations $Q(6)$ through to $Q(9)$ also hold since $C(-)$ is conjugated. To show that relation $Q(3)$ is also respected, it suffices to prove Lemma 5.6.

Lemma 5.6. *The following equations hold.*



Lemma 5.7. *If* $(X,Y) \in Q$*, then* $X^* \approx_E Y^*$ *for some* $X^* \in \mathsf{Dec}(X)$ *and* $Y^* \in \mathsf{Dec}(Y)$*.*

Round-Trip Translation. At this point, an encoder $\mathsf{Enc} : \mathbf{Core} \to \mathbf{CQC}$ and a decoder $\mathsf{Dec} : \mathbf{CQC} \to \mathbf{Core}/E$ have been established. It remains to be shown that $\pi_E(g) = \mathsf{Dec}(\mathsf{Enc}(g))$ for each $g \in \Sigma_{\mathbf{Core}}$. Since $\mathsf{Dec}(-)$ is a free control functor, then it suffices to prove the condition for $g \in \mathcal{G}_0$. This follows via routine derivations and consequently establishes completeness.

Lemma 5.8. *If* $g \in \Sigma_{\mathbf{Core}}$*, then there exists* $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ *such that* $g \approx_E U$*.*

Theorem 5.9. $(\Sigma_{\mathbf{Core}}, E)$ *is complete with respect to the semantic interpretation* $[\![-]\!]_H$*.*

5.1 Completeness for the Full Language

It remains to be shown that every circuit in **HQC** can be reduced to a circuit in **Core**. The proof begins by showing that this is possible when a set of primitive gates is added to **Core**. This new language is denoted $\mathbf{CExt}[0]$. The proof then proceeds by induction on $\mathbf{CExt}[n]$, in which each step adds increasingly more complex gates to $\mathbf{CExt}[n]$. At each step of the proof, it is shown how a reduction procedure for $\mathbf{CExt}[n]$ can be used to obtain a reduction procedure for $\mathbf{CExt}[n+1]$. Formally, let $\Sigma^0_{\mathbf{CExt}} = \Sigma_{\mathbf{Core}} \cup \Sigma_{\mathbf{Prim}}$ and $\mathbf{CExt}[0] = P(\Sigma^0_{\mathbf{CExt}})$. Then for each $n \in \mathbb{N}$, let $\Sigma^{n+1}_{\mathbf{CExt}} = \Sigma^n_{\mathbf{CExt}} \cup \mathsf{Tower}(\mathbf{CExt}[n]) \cup \mathsf{Power}(\mathbf{CExt}[n])$ with $\mathbf{Core}[n+1] = P(\Sigma^n_{\mathbf{CExt}})$. It is not hard to see that $\Sigma^n_{\mathbf{HQC}} \subseteq \Sigma^n_{\mathbf{CExt}} \subseteq \Sigma_{\mathbf{HQC}}$ for each $n \in \mathbb{N}$. It follows that the categorical colimit of this sequence is **HQC**.

The Base Reduction. The only gates which appear in $\mathbf{CExt}[0]$ but not in **Core** are the primitive rotation gates free from exponents. Of course, the relation E(17) in E allows for these gate to be rewritten to the form $(g \uparrow 1)$. This motivates the following reduction.

$$r_0(-\bullet-) = -\bullet^{1}- \qquad r_0(-\circ-) = -\circ^{1}- \qquad r_0(-\oplus-) = -\oplus^{1}- \qquad r_0(-\ominus-) = -\ominus^{1}-$$

$$r_0(-\boxed{H}-) = -\boxed{H}- \qquad r_0(U \uparrow \alpha) = U \uparrow \alpha \qquad r_0(U \odot V) = U \odot V$$

Then by Lemma 4.2, these equations define a unique prop functor $\mathsf{Reduce}_0 : \mathbf{CExt}[0] \to \mathbf{Core}$ with the property that $U \approx_E \mathsf{Reduce}_0(U)$ for each $U \in \mathrm{Mor}(\mathbf{CExt}[0])$.

The Inductive Construction. Assume that there exists a functor $\mathsf{Reduce}_n : \mathbf{CExt}[n] \to \mathbf{Core}$ with the property that $U \approx_E \mathsf{Reduce}_n(U)$ for each $U \in \mathrm{Mor}(\mathbf{CExt}[n])$. The goal of this step is to construct a new functor $\mathsf{Reduce}_{n+1} : \mathbf{CExt}[n+1] \to \mathbf{Core}$ such that $U \approx_E \mathsf{Reduce}_{n+1}(U)$ for each $U \in \mathrm{Mor}(\mathbf{CExt}[n+1])$. Of course, the new gates in $\mathbf{CExt}[n+1]$ are gates of the form $U \odot V$ and $U \uparrow \alpha$ where $U \in \mathbf{CExt}[n]$ and $V \in \mathbf{CExt}[n]$. For simplicity, we will consider the case of exponentiation. Since $U \in \mathbf{CExt}[n]$, then $(U \uparrow \alpha)$ rewrites to $(V \uparrow \alpha)$ where $V = \mathsf{Reduce}_n(U)$. It is not hard to show that **Core** is universal for unitary qubit quantum computation. Then means that there exists a circuit P and a diagonal circuit Λ such that $[\![P^{\ddagger} \circ \Lambda \circ P]\!]_H = [\![V]\!]_H$. Since E is complete for **Core** with respect to $[\![-]\!]_H$, then $V \approx_E P^{\ddagger} \circ \Lambda \circ P$. It then follows from relations E(20), E(22), and Lemma 5.4 that $U \uparrow \alpha \approx_E P^{\ddagger} \circ (\Lambda \uparrow \alpha) \circ P$. Using relation E(17) and E(21), it is then possible to reduce $(\Lambda \uparrow \alpha)$ to a diagonal circuit in **Core**. A similar procedure can be carried out for $U \odot V$, using relations E(14) and E(15). These procedures are stated formally in Section H with proofs of termination, and are denoted $\mathsf{Drop}_n(U, \alpha)$ and $\mathsf{Expand}_n(U, V)$, respectively. Using these procedures, the following reduction is obtained.

$$r_{n+1}(g) = \begin{cases} r_n(g) & \text{if } g \in \Sigma^n_{\mathbf{CExt}} \\ \mathsf{Expand}_{n+1}(g) & \text{if } g \in \mathsf{Tower}(\mathbf{CExt}[n]) \cap \mathrm{Mor}(\mathbf{CExt}[n+1]) \\ \mathsf{Drop}_{n+1}(U, \alpha) & \text{if } g = U \uparrow \alpha \text{ for } U \in \mathrm{Mor}(\mathbf{CExt}[n]) \text{ and } \alpha \in \mathbb{R} \end{cases}$$

This defines a unique prop functor $\mathsf{Reduce}_{n+1} : \mathbf{CExt}[n+1] \to \mathbf{Core}$ with the property that $U \approx_E \mathsf{Reduce}_{n+1}(U)$ for each $U \in \mathrm{Mor}(\mathbf{CExt}[n+1])$.

Theorem 5.10. *$(\Sigma_{\mathbf{HQC}}, E)$ is complete with respect to the semantic interpretation $[\![-]\!]_H$.*

6 Conclusion

In this paper, we introduced the notion of generalized controls. We studied its algebraic properties and established its relation to circuit exponentiation and conjugated control functors. Based on these operations, we then introduced the notion of a hierarchical circuit language, which extends a standard prop category with an abstract notion of generalized control and exponentiation. It was then shown how the algebraic properties of generalized controls could be used to obtain a sound and complete equational theory for the category of hierarchical quantum circuits. A key insight obtained from this proof is that reducing hierarchical quantum circuits to controlled quantum circuits can be seen as a form of diagrammatic circuit diagonalization. There are several directions for future work.

1. Finding a purely categorical description for $(\odot)$ and $(\uparrow)$, and their pointed extensions.
2. Exploring quantum circuit compilation from the perspective of hierarchical circuits.
3. Identifying sub-languages for which diagrammatic diagonalization is efficiently computable.

References

[1] Franz Baader & Tobias Nipkow (1998): *Term Rewriting and All That*. Cambridge University Press, doi:10.1017/CBO9781139172752.

[2] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John Smolin & Harald Weinfurter (1995): *Elementary gates for quantum computation*. *Phys. Rev. A* 52, pp. 3457–3467.

[3] Ville Bergholm & Jacob D. Biamonte (2011): *Categorical quantum circuits*. *Journal of Physics A: Mathematical and Theoretical* 44(24), pp. 245–304, doi:10.1088/1751-8113/44/24/245304.

[4] Alexandre Clément, Noé Delorme & Simon Perdrix (2024): *Minimal Equational Theories for Quantum Circuits*. In: *Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pp. 1–14, doi:10.1145/3661814.3662088.

[5] Alexandre Clément, Noé Delorme, Simon Perdrix & Renaud Vilmart (2024): *Quantum Circuit Completeness: Extensions and Simplifications*. In: *Proceedings of the 32nd EACSL Annual Conference on Computer Science Logic (CSL)*, pp. 20:1–20:23, doi:10.4230/LIPIcs.CSL.2024.20.

[6] Florence Clerc & Samuel Mimram (2015): *Presenting a Category Modulo a Rewriting System*. In Maribel Fernández, editor: *26th International Conference on Rewriting Techniques and Applications (RTA 2015)*, *Leibniz International Proceedings in Informatics (LIPIcs)* 36, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, pp. 89–105, doi:10.4230/LIPIcs.RTA.2015.89.

[7] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix & Benoît Valiron (2023): *A Complete Equational Theory for Quantum Circuits*. In: *2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, IEEE, pp. 1–13, doi:10.1109/lics56636.2023.10175801.

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

[9] Andrew Cross, Ali Javadi-Abhari, Thomas Alexander, Niel De Beaudrap, Lev S. Bishop, Steven Heidel, Colm A. Ryan, Prasahnt Sivarajah, John Smolin, Jay M. Gambetta & Blake R. Johnson (2022): *OpenQASM 3: A Broader and Deeper Quantum Assembly Language*. *ACM Transactions on Quantum Computing* 3(3), pp. 1–50, doi:10.1145/3505636.

[10] Noé Delorme & Simon Perdrix (2025): *Diagrammatic Reasoning with Control as a Constructor, Applications to Quantum Circuits*. arXiv:2508.21756.

[11] Gidney, Craig (2017): *Thinking of Operations as Controls*. Available at `https://algassert.com/post/1706`. [Online; accessed 19-February-2026].

[12] Lov K. Grover (1996): *A fast quantum mechanical algorithm for database search*. arXiv:quant-ph/9605043.

[13] Brian C. Hall (2015): *Lie groups, Lie algebras, and representations : an elementary introduction*, second edition. Graduate texts in mathematics, 222, Springer, Cham, Switzerland.

[14] Aram W. Harrow, Avinatan Hassidim & Seth Lloyd (2009): *Quantum Algorithm for Linear Systems of Equations*. *Physical Review Letters* 103(15), doi:10.1103/physrevlett.103.150502.

[15] Chris Heunen, Robin Kaarsgaard & Louis Lemonnier (2025): *One rig to control them all*. arXiv:2510.05032.

[16] Chris Heunen, Louis Lemonnier, Christopher McNally & Alex Rice (2026): *Quantum Circuits Are Just a Phase*. *Proceedings of the ACM on Programming Languages* 10(POPL), p. 2586–2613, doi:10.1145/3776731. Available at `http://dx.doi.org/10.1145/3776731`.

[17] Günter Hotz (1965): *Eine Algebraisierung des Syntheseproblems von Schaltkreisen I*. *Elektronische Informationsverarbeitung und Kybernetik* 1(1), pp. 185–205.

[18] Andrey Boris Khesin, Jonathan Z. Lu & Peter W. Shor (2025): *Universal Graph Representation of Stabilizer Codes*. *PRX Quantum* 6(4), doi:10.1103/1gjs-2rhx.

[19] Aleks Kissinger & John van de Wetering (2020): *Reducing the number of non-Clifford gates in quantum circuits. Physical Review A* 102(2), doi:10.1103/physreva.102.022406.

[20] Aleks Kissinger & John van de Wetering (2024): *Scalable Spider Nests (…Or How to Graphically Grok Transversal Non-Clifford Gates). Electronic Proceedings in Theoretical Computer Science* 406, p. 79–95, doi:10.4204/eptcs.406.4.

[21] A. Yu. Kitaev (1995): *Quantum measurements and the Abelian Stabilizer Problem.* arXiv:quant-ph/9511026.

[22] Yves Lafont (2003): *Towards an algebraic theory of Boolean circuits.* Jour. of Pure and Applied *Algebra* 184(2), pp. 257–310, doi:10.1016/S0022-4049(03)00069-0.

[23] Saunders Mac Lane (2010): *Categories for the Working Mathematician.* Springer, doi:10.1007/978-1-4757-4721-8.

[24] Saunders MacLane (1965): *Categorical Algebra. Bull. Amer. Math. Soc.* 70(1), pp. 40–106.

[25] Joaquín Ossorio-Castillo, Ulises Pastor–Díaz & José M. Tornero (2023): *A Generalisation of the Phase Kick-Back. Quantum Information Processing* 22(3):143, doi:10.1007/s11128-023-03884-8.

[26] Tom Peham, Lukas Burgholzer & Robert Wille (2022): *Equivalence Checking of Quantum Circuits With the ZX-Calculus. IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 12(3), p. 662–675, doi:10.1109/jetcas.2022.3202204.

[27] Benjamin Rodatz, Boldizsár Poór & Aleks Kissinger (2024): *Floquetifying stabiliser codes with distance-preserving rewrites.* arXiv:2410.17240.

[28] William Schober (2024): *Extended quantum circuit diagrams.* arXiv:2410.02946.

[29] Peter Selinger (2010): *A Survey of Graphical Languages for Monoidal Categories*, pp. 289–355. Springer Berlin Heidelberg, doi:10.1007/978-3-642-12821-9_4.

[30] Peter W. Shor (1997): *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing* 26(5), p. 1484–1509, doi:10.1137/s0097539795293172.

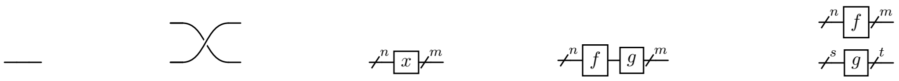
[31] Matthew Sutcliffe & Aleks Kissinger (2024): *Procedurally Optimised ZX-Diagram Cutting for Efficient T-Decomposition in Classical Simulation. Electronic Proceedings in Theoretical Computer Science* 406, p. 63–78, doi:10.4204/eptcs.406.3.

[32] Matthew Sutcliffe & Aleks Kissinger (2025): *Fast Classical Simulation of Quantum Circuits via Parametric Rewriting in the ZX-Calculus. Electronic Proceedings in Theoretical Computer Science* 426, p. 247–269, doi:10.4204/eptcs.426.10.

[33] Benoît Valiron (2022): *Semantics of quantum programming languages: Classical control, quantum control. Journal of Logical and Algebraic Methods in Programming* 128, p. 100790, doi:doi.org/10.1016/j.jlamp.2022.100790.

[34] Renaud Vilmart (2021): *A near-minimal axiomatisation of ZX-calculus for pure qubit quantum mechanics.* In: *Proceedings of the 34th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '19, IEEE Press, pp. 1–10.

[35] Charles Yuan, Agnes Villanyi & Michael Carbin (2024): *Quantum Control Machine: The Limits of Control Flow in Quantum Programming. Proceedings of the ACM on Programming Languages* 8(OOPSLA1), p. 1–28, doi:10.1145/3649811.



(a) $0 : 0 \to 0$. (b) $1 : 1 \to 1$. (c) $\sigma : 2 \to 2$. (d) $x : n \to m$. (e) $g \circ f : n \to m$. (f) $f \boxtimes g : n+s \to m+t$.

Figure 5: A graphical language for the morphisms in $P(\Sigma)$. Two morphisms in $P(\Sigma)$ are equal if and only if their diagrams are isomorphic [29]. A complete set of graphical rewrite rules to determine if two morphisms are isomorphic can be found in [7].

A Conventions for PROP Categories

A *prop category* is a strict symmetric monoidal category $(\mathcal{C}, \boxtimes, \mathbb{I})$ in which $(\text{Ob}(\mathcal{C}), \boxtimes)$ is the monoid of natural numbers [24]. A functor between two prop categories is a symmetric monoidal functor $F : \mathcal{C} \to \mathcal{D}$ such that $\text{Ob}(F)(1) = 1$. A *prop signature* is a collection of symbols Σ equipped with a domain operator $\text{dom} : \Sigma \to \mathbb{N}$ and a codomain operator $\text{cod} : \Sigma \to \mathbb{N}$. Prop signatures form a category in which the morphisms from Σ to Γ are the functions $\tau : \Sigma \to \Gamma$ which satisfy the equations $\text{dom}(\tau(x)) = \text{dom}(x)$ and $\text{cod}(\tau(x)) = \text{cod}(x)$ for each $x \in \Sigma$. There exists an underlying signature functor $U : \mathbf{Prop} \to \mathbf{Sig}$ which sends each prop category $\mathcal{C}$ to $U(\mathcal{C}) = \text{Mor}(\mathcal{C})$ and each prop functor $F : \mathcal{C} \to \mathcal{D}$ to $U(F) = \text{Mor}(F)$. For each prop signature Σ, there exists a prop category $P(\Sigma)$ such that the set of morphisms in $P(\Sigma)$ is the minimal solution to the following set of equations where $(\circ)$, $(\boxtimes)$, (0), (1), and (σ) are formal symbols [7].

- **Structure**. $0 \in P(\Sigma)(0,0)$, $1 \in P(\Sigma)(1,1)$ and $\sigma \in P(\Sigma)(2,2)$.
- **Generators**. If $x \in \Sigma$, then $g \in P(\Sigma)(\text{dom}(x), \text{cod}(x))$.
- **Sequential Comp**. If $f \in P(\Sigma)(n,x)$ and $g \in P(\Sigma)(x,m)$, then $(g \circ f) \in P(\Sigma)(n,m)$.
- **Parallel Comp**. If $f \in P(\Sigma)(n,m)$ and $g \in P(\Sigma)(s,t)$, then $(f \boxtimes g) \in P(\Sigma)(n+s, m+t)$.

The identity morphisms in $P(\Sigma)$ are $1_0 = 0$ and $1_{n+1} = 1 \boxtimes 1_n$, and σ is the generating permutation. In particular, $\sigma_{1,1} = \sigma$ and $\sigma_{1,k+1} = (\sigma \boxtimes 1_k) \circ (1 \boxtimes \sigma_{1,k})$ defines the family of permutations which swap 1 with k. The morphisms in $P(\Sigma)$ are subject to the following relations [7].

- **Sequential Unitality**. $1_m \circ f = f = f \circ 1_n$ for each $f : n \to m$.
- **Parallel Unitality**. $1_0 \boxtimes f = f = f \boxtimes 1_0$ for each $f : n \to m$.
- **Sequential Associativity**. $(h \circ g) \circ f = h \circ (g \circ f)$ for each $f : n \to x$ and $g : x \to m$.
- **Parallel Associativity**. $(f \boxtimes g) \boxtimes h = f \boxtimes (g \boxtimes h)$ for each $f, g, h \in \text{Mor}(P(\Sigma))$.
- **Bifunctoriality**. $(k \circ h) \boxtimes (g \circ f) = (k \boxtimes g) \circ (h \boxtimes f)$ for each $n \xrightarrow{f} x \xrightarrow{g} m$ and $s \xrightarrow{h} y \xrightarrow{k} t$.
- **Symmetry**. $\sigma \circ \sigma = 1_2$ and $(f \boxtimes 1) \circ \sigma_{1,k} = \sigma_{1,k} \circ (1 \boxtimes f)$ for each $f : n \to m$.

Note that from the **Symmetry** relations, it is possible to derive the standard permutation relations as defined [22]. Obviously, there exists an inclusion $i : \Sigma \to U(P(\Sigma))$ which maps each generator in Σ to its corresponding element in the free prop. Moreover, $P(\Sigma)$ is free in the sense that for each $\mathcal{C} \in \text{Ob}(\mathbf{Prop})$ and each $\tau \in \mathbf{Sig}(\Sigma, U(\mathcal{C}))$, there exists a unique functor $F : P(\Sigma) \to \mathcal{C}$ such that $U(F) \circ i = \tau$ [6]. Concretely, F is defined by the following equations where $x \in \Sigma$.

$$F(1) = 1 \qquad F(\sigma) = \sigma \qquad F(x) = f(x) \qquad F(g \circ f) = F(g) \circ F(f) \qquad F(f \boxtimes g) = F(f) \boxtimes F(g)$$

The morphisms in $P(\Sigma)$ can be understood as circuit diagrams [17], as depicted in Fig. 5.

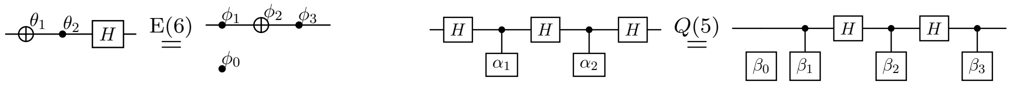


Figure 6: The Euler relation used in **HQC**/E (left) together with the equivalent relation used in **CQC**/Q from which it was derived (right).

B The Euler Relation

This appendix summarizes the details of relation E(6). This relation is a complex generalization of the Euler angle decomposition for 3D rotations, which describes how rotations on a sphere can be decomposed into rotations around any two chosen axes. There are many equivalent variations of this relation in the literature, varying in the choice of axes, exact number of parameters involved, and their corresponding algebraic relations to one another. Use of an Euler angle relation was shown to be necessary for completeness in [4, 34]. Relation E(6) is equivalent to the Euler relation used in [10] as described below (see Fig. 6). For details beyond about this Euler relation beyond what is listed here, we refer to [34, 4, 5, 10].

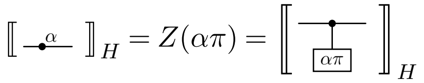
The relation $Q(5)$ involves a pair of arbitrary input angles $\alpha_1, \alpha_2 \in \mathbb{R}$ on the left-hand side, and quadruplet of corresponding angles $\beta_0, \beta_1, \beta_2, \beta_3 \in [0,2)$ on the right-hand side. In E(6), the powers θ_1 and θ_2 are related to the angles (α_1, α_2) by $\alpha_j = \theta_j \pi$. The angles β_0, β_1, β_2, and β_3 are related to α_1 and α_2 through the function $\mathsf{Euler}(\alpha_1, \alpha_2) = (\beta_0, \beta_1, \beta_2, \beta_3)$ as defined in [10], whose behavior is as follows.

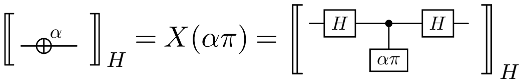
$$u := -\sin\left(\tfrac{\alpha_1+\alpha_2}{2}\right) + i\cos\left(\tfrac{\alpha_1-\alpha_2}{2}\right)$$
$$v := +\cos\left(\tfrac{\alpha_1+\alpha_2}{2}\right) - i\sin\left(\tfrac{\alpha_1-\alpha_2}{2}\right)$$

	β_1	β_2	β_3
if $v = 0$	$2\arg(u)$	0	0
if $u = 0$	$2\arg(v)$	π	0
otherwise	$\arg(u) + \arg(v)$	$2\arg\left(i + \left\lvert\frac{u}{v}\right\rvert\right)$	$\arg(u) - \arg(v)$

$$\beta_0 = \frac{(\pi + \alpha_1 + \alpha_2 - \beta_1 - \beta_2 - \beta_3)}{2}$$

Finally, the powers $(\phi_0, \phi_1, \phi_2, \phi_3)$ on the right-hand side of E(6) are related to $(\beta_0, \beta_1, \beta_2, \beta_3)$ by $\phi_j = \beta_j/\pi$. Since the following equations hold for each $\alpha \in \mathbb{R}$, then these relations are equivalent modulo their intended semantics.





C Proofs for Section 3

This section contains all proofs for Section 3.

C.1 Proof of Theorem 3.1

Proof. First, it must be shown that $(\odot)$ is unital with unit (-1). Since $\mathrm{Log}(-1) = i\pi$, then the following equations hold for all $U \in \mathrm{Mor}(\mathbf{Unitary})$.

$$\begin{aligned}(-1) \odot U &= \exp(\mathrm{Log}(-1) \otimes \mathrm{Log}(U)/(i\pi)) = \exp(\mathrm{Log}(U)) = U\\ U \odot (-1) &= \exp(\mathrm{Log}(U) \otimes \mathrm{Log}(-1)/(i\pi)) = \exp(\mathrm{Log}(U)) = U\end{aligned}$$

Then $(-1) \odot U = U = U \odot (-1)$ for all $U \in \mathrm{Mor}(\mathbf{Unitary})$. In other words, $(\odot)$ is unital with unit (-1). It remains to be shown that $(\odot)$ is associative. To this end, let $U, V, W \in \mathrm{Mor}(\mathbf{Unitary})$. Let $\{\alpha_j\}_{j=1}^{n}$ denote the eigenvalues of $\mathrm{Log}(U)$ with orthonormal eigenbasis $\{b_j\}_{j=1}^{n}$ and $\{\beta_j\}_{j=1}^{m}$ denote the eigenvalues of $\mathrm{Log}(V)$ with orthonormal eigenbasis $\{c_j\}_{j=1}^{m}$. Then then following equation holds where $A = \mathrm{Log}(U) \otimes \mathrm{Log}(V)/(i\pi)$, since $(\otimes)$ is bilinear.

$$A = \frac{1}{i\pi}\left(\sum_{j=1}^{n} \alpha_j \left|b_j\right\rangle\left\langle b_j\right|\right) \otimes \left(\sum_{k=1}^{m} \beta_k \left|c_k\right\rangle\left\langle c_k\right|\right) = \sum_{j=1}^{n}\sum_{k=1}^{m} \frac{\alpha_j \beta_k}{i\pi}(\left|b_j\right\rangle \otimes \left|c_k\right\rangle)(\left\langle b_j\right| \otimes \left\langle c_k\right|)$$

Then $\{\left|b_j\right\rangle \otimes \left|c_k\right\rangle : j \in \{1, 2, \ldots, n\}, k \in \{1, 2, \ldots, m\}\}$ is an orthonormal eigenbasis for A. Moreover, for each $j \in \{1, 2, \ldots, n\}$ and $k \in \{1, 2, \ldots, m\}$, the eigenvalue associated with $\left|b_j\right\rangle \otimes \left|c_k\right\rangle$ is $(\alpha_j \beta_k)/(i\pi)$. Since $\beta_k \in i(-\pi, \pi]$, then $\beta_k/(i\pi) \in (-1, 1]$. Consequently, $(\alpha_j \beta_k)/(i\pi) \in i(-\pi, \pi]$. Since j and k were arbitrary, then all eigenvalues of A fall within $i(-\pi, \pi]$. Consequently, $\mathrm{Log}(U \odot V) = A$ and the following equation holds by the associativity and bilinearity of $(\otimes)$.

$$(U \odot V) \odot W = \exp\left(\frac{\mathrm{Log}(U \odot V) \otimes \mathrm{Log}(W)}{i\pi}\right) = \exp\left(\frac{\mathrm{Log}(U) \otimes \mathrm{Log}(V) \otimes \mathrm{Log}(W)}{(i\pi)^2}\right)$$

By a similar argument, $\mathrm{Log}(V \odot W) = B$ where $B = \mathrm{Log}(V) \otimes \mathrm{Log}(W)/(i\pi)$. Then the following equation also holds by the associativity and bilinearity of $(\otimes)$.

$$U \odot (V \odot W) = \exp\left(\frac{\mathrm{Log}(U) \otimes \mathrm{Log}(V \odot W)}{i\pi}\right) = \exp\left(\frac{\mathrm{Log}(U) \otimes \mathrm{Log}(V) \otimes \mathrm{Log}(W)}{(i\pi)^2}\right)$$

In conclusion, $(U \odot V) \odot W = U \odot (V \odot W)$. Since U, V, and W were arbitrary, then $(\odot)$ is associative. Next, the equation for $\bigodot_{j=1}^{n} U_j$ will be derived. The proof follows by induction.

- **Base Case**. $\bigodot_{j=1}^{0} U_j = -1$ and $\mathrm{Log}(-1) = i\pi = i\pi \cdot 1 = i\pi \bigotimes_{j=1}^{n} \frac{\mathrm{Log}(U_j)}{i\pi}$.
- **Inductive Hypothesis**. For some $n \in \mathbb{N}$, if $\{U_j\}_{j=1}^{n}$ is a sequence over $\mathrm{Mor}(\mathbf{Unitary})$, then $\mathrm{Log}\left(\bigodot_{j=1}^{n} U_j\right) = i\pi \bigotimes_{j=1}^{n} \frac{\mathrm{Log}(U_j)}{i\pi}$.
- **Inductive Step**. Assume for some $n \in \mathbb{N}$, if $\{U_j\}_{j=1}^{n}$ is a sequence over $\mathrm{Mor}(\mathbf{Unitary})$, then $\mathrm{Log}\left(\bigodot_{j=1}^{n} U_j\right) = i\pi \bigotimes_{j=1}^{n} \frac{\mathrm{Log}(U_j)}{i\pi}$. Let $\{U_j\}_{j=1}^{n+1}$ be a sequence over $\mathrm{Mor}(\mathbf{Unitary})$. As shown previously, $\mathrm{Log}\left(\bigodot_{j=1}^{n+1} U_j\right) = \mathrm{Log}\left(\bigodot_{j=1}^{n} U_j\right) \otimes \mathrm{Log}(U_{n+1})/(i\pi)$. Then by the inductive hypothesis, $\mathrm{Log}\left(\odot_{j=1}^{n+1} U_j\right) = \left(i\pi \bigotimes_{j=1}^{n} \frac{\mathrm{Log}(U_j)}{i\pi}\right) \otimes \frac{\mathrm{Log}(U_{n+1})}{i\pi} = i\pi \bigotimes_{j=1}^{n+1} \frac{\mathrm{Log}(U_j)}{i\pi}$. Then the inductive step holds.

Then by the principle of induction, $\mathrm{Log}\left(\bigodot_{j=1}^{n}\right) = i\pi \bigotimes_{j=1}^{n} \frac{\mathrm{Log}(U_j)}{i\pi}$ for each sequence $\{U_j\}_{j=1}^{n}$ over $\mathrm{Mor}(\mathbf{Unitary})$. In other words, $\bigodot_{j=1}^{n} U_j = \exp\left(i\pi \bigotimes_{j=1}^{n} \frac{\mathrm{Log}(U_j)}{i\pi}\right)$. □

C.2 Proof of Theorem 3.2

Proof. Let M be an $m \times m$ matrix. If H were diagonal, then $H \otimes M$ would be block diagonal. This equation follows by the bilinearity of $(\otimes)$.

$$\left(\sum_{j=1}^{n} \alpha_j \left| e_j \right\rangle \left\langle e_j \right| \right) \otimes M = \sum_{j=1}^{n} \alpha_j \left| e_j \right\rangle \left\langle e_j \right| \otimes M = \sum_{j=1}^{n} \left| e_j \right\rangle \left\langle e_j \right| \otimes \alpha_j M = \begin{bmatrix} \alpha_1 M & & \\ & \ddots & \\ & & \alpha_n M \end{bmatrix}$$

Since H is Hermitian, then there exists a $P \in \textbf{Unitary}(m,m)$ such that P unitarily diagonalizes N. That is to say, $P \left| j \right\rangle = \left| b_j \right\rangle$ for each $j \in \{1,2,\ldots,n\}$. It follows that $H \otimes M$ is block diagonal with respect to the basis $\{b_j\}_{j=1}^{n}$ with blocks $\{\alpha_j M\}_{j=1}^{n}$.

$$H \otimes M = (P \otimes \mathbb{I}_m) \left(\left(\sum_{j=1}^{n} \alpha_j \left| e_j \right\rangle \left\langle e_j \right| \right) \otimes M \right) (P^\dagger \otimes \mathbb{I}_m) = (P \otimes \mathbb{I}_m) \begin{bmatrix} \alpha_1 M & & \\ & \ddots & \\ & & \alpha_n M \end{bmatrix} (P^\dagger \otimes \mathbb{I}_m)$$

Let $Q = P \otimes \mathbb{I}_m$. Then by Eq. (2), the following equation also holds.

$$\exp(H \otimes M) = \exp\left(Q \begin{bmatrix} \alpha_1 M & & \\ & \ddots & \\ & & \alpha_n M \end{bmatrix} Q^\dagger \right) = Q \exp\left(\begin{bmatrix} \alpha_1 M & & \\ & \ddots & \\ & & \alpha_n M \end{bmatrix} \right) Q^\dagger$$

Since $\exp(-)$ acts pointwise on block diagonal matrices, then we conclude that for each Hermitian matrix $M = \sum_{j=1}^{n} \beta_j \left| b_j \right\rangle \left\langle b_j \right|$ and $n \times n$ matrix M, the matrix $\exp(N \otimes M)$ is block diagonal with respect to $\{b_j\}_{j=1}^{n}$ with blocks $\{\exp(\alpha_j M)\}_{j=1}^{n}$.

$$\exp(H \otimes M) = (P \otimes \mathbb{I}_m) \begin{bmatrix} \exp(\alpha_1 M) & & \\ & \ddots & \\ & & \exp(\alpha_n M) \end{bmatrix} (P^\dagger \otimes \mathbb{I}_m)$$

Returning to the original basis, the following equataion holds.

$$\exp(H \otimes M) = (P \otimes \mathbb{I}_m) \left(\sum_{j=1}^{n} \left| e_j \right\rangle \left\langle e_j \right| \otimes \exp(\alpha_j M) \right) (P^\dagger \otimes \mathbb{I}_m) = \sum_{j=1}^{n} \left| b_j \right\rangle \left\langle b_j \right| \otimes \exp(\alpha_j M)$$

Letting $M = \operatorname{Log}(V)$, it follows that $\exp(H \otimes \operatorname{Log}(V)) = \sum_{j=1}^{n} \left| b_j \right\rangle \left\langle b_j \right| \otimes V^{\alpha_j}$. Then the following equation holds.

$$U \odot V = \exp(\operatorname{Log}(U) \otimes \operatorname{Log}(V)/(i\pi)) = \exp\left(H \otimes \operatorname{Log}(V) \right) = \sum_{j=1}^{n} \left| b_j \right\rangle \left\langle b_j \right| \otimes V^{\alpha_j}$$

In particular, letting $U = Z = \left| 0 \right\rangle \left\langle 0 \right| - \left| 1 \right\rangle \left\langle 1 \right|$, we have $\operatorname{Log}(Z)/(i\pi) = 0 \cdot \left| 0 \right\rangle \left\langle 0 \right| + 1 \cdot \left| 1 \right\rangle \left\langle 1 \right|$, and hence $Z \odot V = \left| 0 \right\rangle \left\langle 0 \right| \otimes V^0 + \left| 1 \right\rangle \left\langle 1 \right| \otimes V^1 = \left| 0 \right\rangle \left\langle 0 \right| \otimes \mathbb{I}_m + \left| 1 \right\rangle \left\langle 1 \right| \otimes V$. □

C.3 Proof of Corollary 3.3

Proof. Let $U \in \textbf{Unitary}(d,d)$ and define $F(-) = U \odot (-)$. Let $\{\alpha_j\}_{j=1}^{d}$ denote the eigenvalues of $\operatorname{Log}(U)/(i\pi)$ with orthonormal eigenbasis $\{b_j\}_{j=1}^{d}$. There are four properties to verify.

1. $F(1_n) = \exp(\operatorname{Log}(U) \otimes \operatorname{Log}(1_n)/(i\pi)) = \exp(\operatorname{Log}(U) \otimes \mathbb{O}_n/(i\pi)) = \exp(\mathbb{O}_{dn}) = \mathbb{I}_{dn}$ for $n \in \mathbb{N}$.

2. Let $n \in \mathbb{N}$ and $V \in \mathrm{Mor}(\mathbf{Unitary})$. Then the following equation holds.

$$\begin{aligned}
U \odot (V \otimes \mathbb{I}_n) &= \sum_{j=1}^{d} |b_j\rangle \langle b_j| \otimes (V \otimes \mathbb{I}_n)^{\alpha_j} && \text{(by Cor. 3.2)} \\
&= \sum_{j=1}^{d} |b_j\rangle \langle b_j| \otimes \exp(\alpha_j \operatorname{Log}(V \otimes \mathbb{I}_n)) \\
&= \sum_{j=1}^{d} |b_j\rangle \langle b_j| \otimes \exp(\alpha_j \operatorname{Log}(V) \otimes \mathbb{I}_n) \\
&= \sum_{j=1}^{d} |b_j\rangle \langle b_j| \otimes \exp(\alpha_j \operatorname{Log}(V)) \otimes \mathbb{I}_n \\
&= \left(\sum_{j=1}^{d} |b_j\rangle \langle b_j| \otimes \exp(\alpha_j \operatorname{Log}(V)) \right) \otimes \mathbb{I}_n \\
&= \left(\sum_{j=1}^{d} |b_j\rangle \langle b_j| \otimes V^{\alpha_j} \right) \otimes \mathbb{I}_n = F(V) \otimes \mathbb{I}_n && \text{(by Cor. 3.2)}
\end{aligned}$$

3. Let $V \in \mathbf{Unitary}(n,n)$. Since $\sigma_{d,d}$ is a monoidal symmetry, then $\sigma_{d,d}$ is self-adjoint with $\sigma_{d,d} \cdot (\operatorname{Log}(U) \otimes \operatorname{Log}(U)) \cdot \sigma_{d,d} = \operatorname{Log}(U) \otimes \operatorname{Log}(U)$. Then the following equation holds where $H = \operatorname{Log}(V)$.

$$\begin{aligned}
F(F(V)) &= U \odot (U \odot V) \\
&= \exp(\operatorname{Log}(U) \otimes \operatorname{Log}(U) \otimes H/(i\pi)^2) && \text{(by Thm. 3.1)} \\
&= \exp((\sigma_{d,d} \cdot (\operatorname{Log}(U) \otimes \operatorname{Log}(U)) \cdot \sigma_{d,d}) \otimes H/(i\pi)^2) \\
&= \exp((\sigma_{d,d} \otimes \mathbb{I}_n) \cdot (\operatorname{Log}(U) \otimes \operatorname{Log}(U) \otimes H/(i\pi)^2) \cdot (\sigma_{d,d} \otimes \mathbb{I}_n)) \\
&= (\sigma_{d,d} \otimes \mathbb{I}_n) \cdot \exp(\operatorname{Log}(U) \otimes \operatorname{Log}(U) \otimes H/(i\pi)^2) \cdot (\sigma_{d,d} \otimes \mathbb{I}_n) && \text{(by Eq. (2))} \\
&= (\sigma_{d,d} \otimes \mathbb{I}_n) \cdot (U \odot (U \odot V)) \cdot (\sigma_{d,d} \otimes \mathbb{I}_n) && \text{(by Thm. 3.1)} \\
&= (\sigma_{d,d} \otimes \mathbb{I}_n) \cdot F(F(V)) \cdot (\sigma_{d,d} \otimes \mathbb{I}_n)
\end{aligned}$$

Then $F(F(V)) = (\sigma_{d,d} \otimes \mathbb{I}_n) \cdot F(F(V)) \cdot (\sigma_{d,d} \otimes \mathbb{I}_n)$. Since $\sigma_{d,d} \otimes \mathbb{I}_n$ is also self-adjoint, then $(\sigma_{d,d} \otimes \mathbb{I}_n) \cdot F(F(V)) = F(F(V)) \cdot (\sigma_{d,d} \otimes \mathbb{I}_n)$.

4. If $V \in \mathbf{Unitary}(n,n)$ and $P \in \mathbf{Unitary}(n,n)$, then the following equation holds.

$$\begin{aligned}
F(P^\dagger \circ V \circ P) &= \exp(\operatorname{Log}(U) \otimes \operatorname{Log}(P^\dagger \circ V \circ P)/(i\pi)) \\
&= \exp(\operatorname{Log}(U) \otimes (P^\dagger \circ \operatorname{Log}(V) \circ P)/(i\pi)) && \text{(by Eq. (2))} \\
&= \exp((\mathbb{I}_d \otimes P^\dagger) \circ (\operatorname{Log}(U) \otimes \operatorname{Log}(V)/(i\pi)) \circ (\mathbb{I}_d \otimes P)) \\
&= (\mathbb{I}_d \otimes P^\dagger) \circ \exp(\operatorname{Log}(U) \otimes \operatorname{Log}(V)/(i\pi)) \circ (\mathbb{I}_d \otimes P) && \text{(by Eq. (2))} \\
&= (\mathbb{I}_d \otimes P^\dagger) \circ F(V) \circ (\mathbb{I}_d \otimes P)
\end{aligned}$$

Functoriality. Next, it must be shown that $F(-)$ is an ordinary functor if and only if U is Hermitian. As a preliminary result, a general equation will be computed for $F(V \circ W)$. Let

$V, W \in \mathbf{Unitary}(n,n)$. Then by Theorem 3.2, the following equations hold.

$$F(V) = \sum_{j=1}^{d} |b_j\rangle\langle b_j| \otimes V^{\alpha_j} \qquad\qquad F(W) = \sum_{j=1}^{d} |b_j\rangle\langle b_j| \otimes W^{\alpha_j}$$

Since $\{b_j\}_{j=1}^{d}$ is orthonormal, then $\langle b_j|b_k\rangle = \delta_{j,k}$ where δ is the Kronecker delta function. Then the following equation holds by the bilinearity of $(\otimes)$.

$$F(V) \circ F(W) = \sum_{j=1}^{d}\sum_{k=1}^{d} \delta_{j,k} |b_j\rangle\langle b_k| \otimes (V^{\alpha_j} \circ W^{\alpha_k}) = \sum_{j=1}^{d} |b_j\rangle\langle b_j| \otimes (V^{\alpha_j} \circ W^{\alpha_j})$$

Since V and W were arbitrary, then this equation holds in general. Now it can be shown that $F(-)$ is a functor if and only if U is Hermitian.

- Assume that $F(-)$ is a functor. Let $j \in \{1,2,\ldots,d\}$. Observe that the following equations hold where $M = |b_j\rangle \otimes \mathbb{I}_2$.

  $$M^\dagger \circ F(-Z) \circ M = \sum_{k=1}^{d} \delta_{j,k}\delta_{k,j}(-Z)^{\alpha_k} = (-Z)^{\alpha_j}$$
  $$M^\dagger \circ F(-\mathbb{I}_2) \circ F(Z) \circ M = \sum_{k=1}^{d} \delta_{j,k}\delta_{k,j}(-\mathbb{I}_2)^{\alpha_k} Z^{\alpha_k} = (-\mathbb{I}_2)^{\alpha_j} \circ Z^{\alpha_j}$$

  Since $F(-)$ is a functor, then the following equation holds.

  $$(-Z)^{\alpha_j} = M \circ F(-Z) \circ M = M \circ F(-\mathbb{I}_2) \circ F(Z) \circ M = (-\mathbb{I}_2)^{\alpha_j} \circ Z^{\alpha_j} = e^{i\alpha_j\pi} Z^{\alpha_j}$$

  Since $\mathrm{Log}(-Z) = i|0\rangle\langle 0|\pi$ and $\mathrm{Log}(Z) = i|1\rangle\langle 1|\pi$, then the following equation holds.

  $$(-Z)^{\alpha_j} = \exp(i\alpha_j\pi|0\rangle\langle 0|) = \begin{bmatrix} e^{i\alpha_j\pi} & 0 \\ 0 & 1 \end{bmatrix} \qquad Z^{\alpha_j} = \exp(i\alpha_j\pi|1\rangle\langle 1|) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha_j\pi} \end{bmatrix}$$

  Then the following equation also holds.

  $$1 = \langle 1|1\rangle = \langle 1|(-Z)^{\alpha_j}|1\rangle = e^{i\alpha_j\pi}\langle 1|Z^{\alpha_j}|1\rangle = e^{i\alpha_j\pi}\left(e^{i\alpha_j\pi}\langle 1|1\rangle\right) = e^{i\alpha_j(2\pi)}$$

  Then $\alpha_j(2\pi)$ is a multiple of 2π. Then α_j is an integer. Then $e^{i\alpha_j\pi}$ is either -1 or 1. Since j was arbitrary, then all eigenvalues of U are either -1 or 1. Since U is unitary, then this means U is also Hermitian.

- Assume that U is Hermitian. Since $U = \exp(iH\pi)$, then the eigenvalues of U are $\{e^{i\alpha_j\pi}\}_{j=1}^{d}$. Let $j \in \{1,2,\ldots,d\}$. Since U is Hermitian and unitary, then $e^{i\alpha_j\pi}$ is either 1 or -1. Then $\alpha_j\pi$ is a multiple of π. Since $\alpha_j \in (-1,1]$, then $\alpha_j \in \{0,1\}$. Then either $\alpha_j = 0$ and $V^{\alpha_j} \circ W^{\alpha_j} = \mathbb{I}_m = (V \circ W)^{\alpha_j}$ or $\alpha_j = 1$ and $V^{\alpha_j} \circ W^{\alpha_j} = V \circ W = (V \circ W)^{\alpha_j}$. Since j was arbitrary, then $V^{\alpha_j} \circ W^{\alpha_j} = (V \circ W)^{\alpha_j}$. Then the following equation holds.

  $$F(V) \circ F(W) = \sum_{j=1}^{d} |b_j\rangle\langle b_j| \otimes (V^{\alpha_j} \circ W^{\alpha_j}) = \sum_{j=1}^{d} |b_j\rangle\langle b_j| \otimes (V \circ W)^{\alpha_j} = F(V \circ W)$$

  Since V and W were arbitrary, then $F(-)$ preserves composition. It was already shown in (**C1**) that $F(-)$ preserves identities, so $F(-)$ is a functor.

Then $F(-)$ is a functor if and only if U is Hermitian.

Control Functoriality. By definition, $(\mathbf{Unitary}_d)_{\mathbf{endo}} = \mathbf{Unitary}_d$. Notice that for each $k \in \mathbb{N}$, $\mathrm{Ob}(F)(d^k) = dd^k = d^{k+1}$. Then there exists a functor $C : \mathbf{Unitary}_d \to \mathbf{Unitary}_d$ such that $C(V : k \to k) = F(V) \in \mathbf{Unitary}(d^{k+1}, d^{k+1}) = \mathbf{Unitary}_d(k+1, k+1)$. It can then be shown that $C(-)$ is a conjugated control functor.

- If $V \in \mathbf{Unitary}_d(k,k)$, then $C(V \otimes 1) = F(V \otimes \mathbb{I}_d) = F(V) \otimes \mathbb{I}_d = C(V) \otimes 1$ by (**C2**).
- Let $V \in \mathbf{Unitary}_d(k,k)$ and write $n = d^k$. It follows from (**C3**) that $(\sigma \otimes 1_k) \circ C(C(V)) = (\sigma_{d,d} \otimes \mathbb{I}_n) \circ F(F(V)) = F(F(V)) \circ (\sigma_{d,d} \otimes \mathbb{I}_n) = C(C(V)) \circ (\sigma \otimes 1_k)$. Since V was arbitrary, then $C(-)$ satisfies Fig. 1e.
- Let $V \in \mathbf{Unitary}_d(k,k)$ and $j \in \{1, 2, \ldots, d\}$. Since $\gamma_{k,j}$ is self-adjoint, then it follows by (**C4**) that $C(\gamma_{k,j} \circ V \circ \gamma_{k,j}) = (1 \otimes \gamma_{k,j}) \circ C(V) \circ (1 \otimes \gamma_{k,j})$. Since V and j were arbitrary, then $C(-)$ satisfies Fig. 1f.

This means that $C(-)$ is a control functor. Since every morphism in $\mathbf{Unitary}_d$ is unitary, then $C(-)$ is a dagger control functor by Lemma 4.8. Finally, if $V, P \in \mathbf{Unitary}_d(k,k)$, then by (**C4**), $C(P^\dagger \circ V \circ P) = F(P^\dagger \circ V \circ P) = (\mathbb{I}_d \otimes P^\dagger) \circ F(V) \circ (\mathbb{I}_d \otimes P) = (1 \otimes P^\dagger) \circ C(V) \circ (1 \otimes P)$. Since V and P were arbitrary, then $C(-)$ is a conjugated control functor.

Pointed Control Functors. Assume that $|u\rangle \in \mathbb{C}^d$ and $|v\rangle \in \mathbb{C}^d$. Since U is Hermitian, then $\mathbb{C}^d$ can be partitioned into the $(+1)$ and (-1) eigenspaces of U, where $\alpha_j = 0$ and $\alpha_j = 1$ respectively. To this end, define the following two sets where $[n] = \{1, 2, \ldots, n\}$.

$$X = \{b_j : j \in [d] \text{ and } \alpha_j = 0\} \qquad\qquad Y = \{b_j : j \in [d] \text{ and } \alpha_j = 1\}$$

It follows that $\{b_j : j \in [d]\} = X \cup Y$. This partitioning will be used to determine the conditions under which $|u\rangle$ and $|v\rangle$ are points of $C(-)$.

- Assume that $C(-)$ is (u,v)-pointed. It will be shown that $U|u\rangle = -|u\rangle$. It then follows by a symmetric argument that $U|v\rangle = |v\rangle$. Construct a matrix $M = \sum_{j=0}^{d-1} |d-j\rangle\langle j|$, so that M is a permutation of the standard basis vectors within $\mathbb{C}^d$. Since M is a permutation matrix, then M is unitary, and hence $M \in \mathbf{Unitary}_d(1,1)$. Since $C(-)$ is a (u,v)-pointed control functor, then the following equation holds where $\gamma_x = \langle x|u\rangle$.

$$\begin{aligned} |u\rangle \otimes M &= C(M) \circ (|u\rangle \otimes \mathbb{I}_d) \\ &= \sum_{j=1}^{n} |b_j\rangle\langle b_j|u\rangle \otimes M^{\alpha_j} && \text{(by Theorem 3.2)} \\ &= \sum_{b_j \in X} \gamma_{b_j} |b_j\rangle \otimes M^0 + \sum_{b_j \in Y} \gamma_{b_j} |b_j\rangle \otimes M^1 \\ &= \sum_{b_j \in X} \gamma_{b_j} |b_j\rangle \otimes \mathbb{I}_d + \sum_{b_j \in Y} \gamma_{b_j} |b_j\rangle \otimes M \end{aligned}$$

Since $\otimes$ is bilinear, then the following equation holds.

$$\left(|u\rangle - \sum_{b_j \in Y} \gamma_{b_j} |b_j\rangle \right) \otimes M = \left(\sum_{b_j \in X} \gamma_{b_j} |b_j\rangle \right) \otimes \mathbb{I}_d$$

Since $\{|\ell\rangle\langle k|\}_{j=1,\ell=1}^{d}$ is a basis for $\mathbf{Unitary}_d(1,1)$, then $\mathbb{I}_d$ and M are not linear combinations of one-another. Then the left-hand side and right-hand side also not linear combinations of one-another. Then by equating components, $|u\rangle = \sum_{b_j \in Y} \gamma_{b_j} |b_j\rangle$. Then $|u\rangle$ is in the (-1)-eigenspace of U. In conclusion, $U|u\rangle = -|u\rangle$.

- Assume that $U|u\rangle = -|u\rangle$ and $U|v\rangle = |v\rangle$. Since $U|u\rangle = -|u\rangle$, then by definition $|u\rangle$ is in the (-1)-eigenspace of U. This means that $|u\rangle = \sum_{b_j \in Y} \gamma_j |b_j\rangle$ where $\gamma_j = \langle b_j|u\rangle$. Recall that $\langle b_j|b_k\rangle = \delta_{j,k}$ where δ is the Kronecker delta function. Let $V \in \mathbf{Unitary}_d(k,k)$ and $n = d^k$. Then the following equation holds.

$$\begin{aligned}
C(V) \circ (|u\rangle \otimes \mathbb{I}_n) &= \sum_{j=1}^{n} |b_j\rangle \langle b_j|u\rangle \otimes V^{\alpha_j} && \text{(by Theorem 3.2)} \\
&= \sum_{j=1}^{n} |b_j\rangle \left(\sum_{b_k \in X} \gamma_k \langle b_j|b_k\rangle \right) \otimes V^{\alpha_j} && \text{(by the bilinearity of } \langle -|-\rangle\text{)} \\
&= \sum_{j=1}^{n} |b_j\rangle \left(\sum_{b_k \in X} \gamma_x \delta_{j,k} \right) \otimes V^{\alpha_j} \\
&= \sum_{j=1}^{n} \sum_{b_k \in X} \gamma_k \delta_{j,k} |b_j\rangle \otimes V^{\alpha_j} && \text{(by the bilinearity of } \otimes\text{)} \\
&= \sum_{b_j \in X} \gamma_j |b_j\rangle \otimes V^{1} \\
&= \sum_{b_j \in X} \gamma_j |b_j\rangle \otimes V \\
&= \left(\sum_{b_j \in X} \gamma_j |b_j\rangle \right) \otimes V = |u\rangle \otimes V && \text{(by the bilinearity of } \otimes\text{)}
\end{aligned}$$

Since V was arbitrary, then $C(V) \circ (|u\rangle \otimes \mathbb{I}_n) = |u\rangle \otimes V$ for all $V \in \mathbf{Unitary}_d(k,k)$ with $n = d^k$. By a symmetric argument, starting from the fact that $|v\rangle$ in the $(+1)$-eigenspace of U, it follows that $C(V) \circ (|v\rangle \otimes \mathbb{I}_n) = |v\rangle \otimes \mathbb{I}_n$ for all $V \in \mathbf{Unitary}_d(k,k)$ with $n = d^k$. Then $C(-)$ is (u,v)-pointed.

In conclusion, $C(-)$ is (u,v)-pointed if and only if $U|u\rangle = -|u\rangle$ and $U|v\rangle = |v\rangle$. □

C.4 Proof of Theorem 3.4

Proof. Let $\alpha \in \mathbb{R}$. First, it must be shown that $U \odot e^{i\alpha\pi} = U^\alpha$ for all $U \in \mathrm{Mor}(\mathbf{Unitary})$ if and only if $\alpha \in (-1,1]$.

- Assume that $\alpha \in (-1,1]$. Then $i\alpha\pi \in i(-\pi,\pi]$. Then $\mathrm{Log}(e^{i\alpha\pi}) = i\alpha\pi$ since $\mathrm{Log}(-)$ is the principle branch of $\log(-)$. Let $U \in \mathrm{Mor}(\mathbf{Unitary})$. Then the following equation holds.

$$U \odot e^{i\alpha\pi} = \exp\left(\mathrm{Log}(U) \otimes (i\alpha\pi)/(i\pi)\right) = \exp(\alpha\,\mathrm{Log}(U)) = U^\alpha$$

Since U was arbitrary, then $U \odot e^{i\alpha\pi} = U^\alpha$ for all $U \in \mathrm{Mor}(\mathbf{Unitary})$.

- Assume that $\alpha \notin (-1,1]$. Then there exists a unique $k \in \mathbb{Z} \setminus \{0\}$ such that $\alpha - 2k \in (-1,1]$. Then $i\alpha\pi - i2k\pi \in i(-\pi,\pi]$, which implies that $\text{Log}(e^{i\alpha\pi}) = i\alpha\pi - i2k\pi$. Since $k \neq 0$, then let $U = Z^{1/|4k|}$, so that $\text{Log}(U) = i\frac{\pi}{|4k|} |1\rangle\langle 1|$. Then the following equations hold.

$$U^\alpha = \exp\left(\alpha\left(i\frac{\pi}{|4k|}|1\rangle\langle 1|\right)\right) = \exp\left(i\frac{\alpha\pi}{|4k|}|1\rangle\langle 1|\right)$$
$$U \odot e^{i\alpha\pi} = \exp\left(\left(i\frac{\pi}{|4k|}|1\rangle\langle 1|\right) \otimes (i\alpha\pi - i2k\pi)/(i\pi)\right) = \exp\left(i\frac{(\alpha-2k)\pi}{|4k|}|1\rangle\langle 1|\right)$$

  Since $-1 < \alpha - 2k \leq 1$, then $2k-1 < \alpha < 2k+1$. The value of $\alpha/|4k|$ then depends on the value of k. If $k > 0$, then the following equations hold.

$$(2k-1)/|4k| = 2k/|4k| - 1/|4k| = 1/2 - 1/|4k| \geq 1/2 - 1/4 > -1$$
$$(2k+1)/|4k| = 2k/|4k| + 1/|4k| = 1/2 + 1/|4k| \leq 1/2 + 1/4 < 1$$

  This means that $\alpha/|4k| \in (-1,1)$. If $k < 0$, then the following equations hold.

$$(2k-1)/|4k| = 2k/|4k| - 1/|4k| = -1/2 - 1/|4k| \geq -1/2 - 1/4 > -1$$
$$(2k+1)/|4k| = 2k/|4k| + 1/|4k| = -1/2 + 1/|4k| \leq -1/2 + 1/4 < 1$$

  This means that $\alpha/|4k| \in (-1,1)$. Then in either case, $\alpha/|4k| \in (-1,1)$. It follows that $\text{Log}(U^\alpha) = i\frac{\alpha\pi}{|4k|}|1\rangle\langle 1|$. Since $i(\alpha-2k)\pi \in i(-\pi,\pi]$, then $i\frac{(\alpha-2k)\pi}{|4k|} \in i(-\pi,\pi]$. It follows that $\text{Log}(U \odot e^{i\alpha\pi}) = i\frac{(\alpha-2k)\pi}{|4k|}|1\rangle\langle 1|$. Clearly $\text{Log}(U^\alpha) \neq \text{Log}(U \odot e^{i\alpha\pi})$. Then $U^\alpha \neq U \odot e^{i\alpha\pi}$. Then there exists a $U \in \text{Mor}(\textbf{Unitary})$ such that $U \odot e^{i\alpha\pi} \neq U^\alpha$.

It remains to be shown that if $U \in \text{Mor}(\textbf{Unitary})$ is Hermitian, then $U \odot e^{i\alpha\pi} = U^\alpha$. Assume that $U \in \text{Mor}(\textbf{Unitary})$ with U Hermitian. Let $\{\beta_j\}_{j=1}^n$ denote the eigenvalues of $\text{Log}(U)/(i\pi)$ with orthonormal eigenbasis $\{b_j\}_{j=1}^n$. Then the following equation holds where $z = e^{i\alpha\pi}$.

$$U \odot z = \exp(\text{Log}(U) \otimes \text{Log}(z)/(i\pi)) = \exp\left(\sum_{j=1}^n \text{Log}(z)\beta_j |b_j\rangle\langle b_j|\right) = \sum_{j=1}^n e^{\text{Log}(z)\beta_j}|b_j\rangle\langle b_j|$$

Let $j \in \{1,2,\ldots,n\}$. Then $\exp(i\beta_j\pi)$ is an eigenvalue of U. Since U is Hermitian, then $e^{i\beta_j\pi}$ is either -1 or 1. Then $\beta_j\pi$ is a multiple of π. Since $\beta_j\pi \in (-\pi,\pi]$, then β_j is either 0 or 1. If $\beta_j = 0$, then the following equation holds.

$$\exp(\text{Log}(z)\beta_j) = \exp(0\,\text{Log}(z)) = \exp(0) = \exp(0(i\alpha\beta_j)) = \exp(i\alpha\beta_j\pi)$$

If $\beta_j = 1$, then the following equation holds.

$$\exp(\text{Log}(z)\beta_j) = \exp(1\,\text{Log}(z)) = \exp(\text{Log}(z)) = \exp(i\alpha\pi) = \exp(1(i\alpha\pi)) = \exp(i\alpha\beta_j\pi)$$

In either case, $e^{\text{Log}(z)\beta_j} = e^{i\alpha\beta_j\pi}$. Since j was arbitrary, then the following equation holds.

$$\sum_{j=1}^n e^{\text{Log}(z)\beta_j}|b_j\rangle\langle b_j| = \sum_{j=1}^n e^{i\alpha\beta_j\pi}|b_j\rangle\langle b_j| = \exp\left(\sum_{j=1}^n i\alpha\beta_j\pi|b_j\rangle\langle b_j|\right) = \exp(\alpha\,\text{Log}(U)) = U^\alpha$$

In conclusion, $U \odot e^{i\alpha\pi} = U^\alpha$. Since U was arbitrary, then $U \odot e^{i\alpha\pi} = U^\alpha$ for each Hermitian $U \in \text{Mor}(\textbf{Unitary})$. Since α was arbitrary, then this completes the proof. □

C.5 Proof of Theorem 3.5

Proof. Let $\{b_j\}_{j=1}^n$ denote the orthonormal eigenbasis associated with $\{\lambda_j\}_{j=1}^n$. Then let $\alpha \in \mathbb{R}$ and $\beta \in \mathbb{R}$. First, equations will be found for $(U^\alpha)^\beta$ and $U^{\alpha\beta}$. Observe that the following equation holds.

$$U^\alpha = \exp(\alpha \operatorname{Log}(U)) = \exp\left(\alpha \sum_{j=1}^n i\lambda_j\pi \left|b_j\right\rangle \left\langle b_j\right|\right) = \exp\left(\sum_{j=1}^n i\alpha\lambda_j\pi \left|b_j\right\rangle \left\langle b_j\right|\right) = \sum_{j=1}^n e^{i\alpha\lambda_j\pi} \left|b_j\right\rangle \left\langle b_j\right|$$

This can then be used to compute $\operatorname{Log}(U^\alpha)$ where $\zeta_j = \operatorname{Log}\left(e^{\alpha\lambda_j}\right)$.

$$\operatorname{Log}(U^\alpha) = \operatorname{Log}\left(\sum_{j=1}^n e^{i\alpha\lambda_j\pi} \left|b_j\right\rangle \left\langle b_j\right|\right) = \sum_{j=1}^n \operatorname{Log}\left(e^{i\alpha\lambda_j\pi}\right) \left|b_j\right\rangle \left\langle b_j\right| = \sum_{j=1}^n \zeta_j \left|b_j\right\rangle \left\langle b_j\right|$$

This can then be used to compute $(U^\alpha)^\beta$.

$$(U^\alpha)^\beta = \exp(\beta \operatorname{Log}(U^\alpha)) = \exp\left(\beta \sum_{j=1}^n \zeta_j \left|b_j\right\rangle \left\langle b_j\right|\right) = \exp\left(\sum_{j=1}^n \beta\zeta_j \left|b_j\right\rangle \left\langle b_j\right|\right) = \sum_{j=1}^n e^{\beta\zeta_j} \left|b_j\right\rangle \left\langle b_j\right|$$

Likewise, $U^{\alpha\beta} = \sum_{j=1}^n e^{i\alpha\beta\lambda_j\pi} \left|b_j\right\rangle \left\langle b_j\right|$. Next an explicit equation will be calculated for each ζ_j in terms of α and λ_j. Let $j \in \{1,2,\dots,n\}$. Since $\zeta_j = \operatorname{Log}(\exp(i\alpha\lambda_j\pi))$, then there exists a $k \in \mathbb{Z}$ such that $i\alpha\lambda_j\pi = \zeta_j + k(i2\pi)$. Then the following sequence of statements hold.

$$\begin{aligned}
\zeta_j &\in i(-\pi,\pi] && \text{(since } \zeta_j = \operatorname{Log}(\exp(\alpha\lambda_j))\text{)}\\
i\alpha\lambda_j\pi &\in i(-\pi + k(2\pi), \pi + k(2\pi)] && \text{(since } \alpha\lambda_j = \zeta_j + k(i2\pi)\text{)}\\
\alpha\lambda_j/2 &\in (k - 1/2, k + 1/2] &&\\
\alpha\lambda_j/2 - 1/2 &\in (k-1, k] &&
\end{aligned}$$

Since $k - 1 < (\alpha\lambda_j - 1)/2 \leq k$, then $\lceil(\alpha\lambda_j - 1)/2\rceil = k$. Since j was arbitrary, then it follows that $\alpha\lambda_j = \zeta_j + \lceil(\alpha\lambda_j - 1)/2\rceil(i2\pi)$ for each $j \in \{1,2,\dots,n\}$. Next, it must be shown that $(U^\alpha)^\beta = U^{\alpha\beta}$ if and only if for each $j \in \{1,2,\dots,n\}$, either $\alpha\lambda_j \in (-1,1]$ or $\beta \in \mathbb{Q}$ with reduced denominator dividing $\lceil(\alpha\lambda_j - 1)/2\rceil$.

- Assume that $U^{\alpha\beta} = (U^\alpha)^\beta$. Let $j \in \{1,2,\dots,n\}$. Since $\{b_j\}_{j=1}^n$ is an orthonormal basis, then $e^{\beta\zeta_j} = e^{i\alpha\beta\lambda_j\pi}$ by equating components in $(U^\alpha)^\beta = U^{\alpha\beta}$. Then $\beta\zeta_j - i\alpha\beta\lambda_j\pi$ is a multiple of $i2\pi$. Then there exists some $m \in \mathbb{Z}$ such that $m(i2\pi) = \beta(i\alpha\lambda_j\pi - \zeta_j) = \beta k(i2\pi)$ where $k = \lceil(\alpha\lambda_j - 1)/2\rceil$. In other words, $\beta k \in \mathbb{Z}$. If $k = 0$, then clearly $\beta k \in \mathbb{Z}$. This happens precisely when $\zeta_j = i\alpha\lambda_j\pi$, which implies that $\alpha\lambda_j \in (-1,1]$. Assume instead that $k \neq 0$. Then $\beta \in \mathbb{Q}$, otherwise βk is irrational. Then there exists some $d \in \mathbb{Z}$ and $q \in \mathbb{N}$ such that $\gcd(d,q) = 1$ and $\beta = d/q$. Then $dk/q \in \mathbb{Z}$. Then q divides dk. Since $\gcd(q,d) = q$, then q divides k. This means that λ_j is (α,β)-admissible. Since j was arbitrary, then λ_j is (α,β)-admissible for each $j \in \{1,2,\dots,n\}$.
- Assume that for each $j \in \{1,2,\dots,n\}$, λ_j is (α,β)-admissible. Let $j \in \{1,2,\dots,n\}$. There are two cases to consider. If $\alpha\lambda_j \in (-1,1]$, then $\zeta_j = i\alpha\lambda_j\pi$, and consequently $\beta\zeta_j = i\alpha\beta\lambda_j\pi = i\alpha\beta\pi + 0(i2\pi)$. Assume instead that $\beta \in \mathbb{Q}$ with reduced denominator dividing

$k = \lceil(\alpha\lambda_j - 1)/2\rceil$. Then there exists $q \in \mathbb{Z}$ and $d \in \mathbb{N}$ such that $\beta = q/d$, $\gcd(q,d) = 1$ and d divides k. It follows that $\beta\zeta_j = \beta(i\alpha\lambda_j\pi + k) = i\alpha\beta\lambda_j\pi + qk(i2\pi)/d$. Since d divides k, then there exists a $m \in \mathbb{Z}$ such that $\beta\zeta_j = i\alpha\beta\lambda_j\pi + m(i2\pi)$. In either case, there exists an $m \in \mathbb{N}$ such that $\beta\zeta_j = i\alpha\beta\lambda_j\pi + m(i2\pi)$. Then $\exp(\beta\zeta_j) = \exp(i\alpha\beta\lambda_j\pi)$. Since j was arbitrary, then $\exp(\beta\zeta_j) = \exp(i\alpha\beta\lambda_j\pi)$ for each $j \in \{1,2,\ldots,n\}$. Then the following equation holds.

$$(U^\alpha)^\beta = \sum_{j=1}^{n} e^{\beta\zeta_j} |b_j\rangle\langle b_j| = \sum_{j=1}^{n} e^{i\alpha\beta\lambda_j\pi} |b_j\rangle\langle b_j| = U^{\alpha\beta}$$

Then $(U^\alpha)^\beta = U^{\alpha\beta}$ if and only if for each $j \in \{1,2,\ldots,n\}$, either $\alpha\lambda_j \in (-1,1]$ or $\beta \in \mathbb{Q}$ with reduced denominator dividing $\lceil(\alpha\lambda_j - 1)/2\rceil$. It remains to be shown that $\mathbb{Z}$ and $(-1,-1]$ are maximal submonoids of $\mathbb{R}$ for which for which $(U,\alpha) \mapsto U^\alpha$ is a monoid action on Mor(**Unitary**).

- Let $\alpha \in \mathbb{Z}$, $\beta \in \mathbb{Z}$, and $U \in$ Mor(**Unitary**). It must be shown that $(U^\alpha)^\beta = U^{\alpha\beta}$. To this end, let $\{\lambda_j\}_{j=1}^n$ denote the eigenvalues of $\mathrm{Log}(U)/(i\pi)$. Let $j \in \{1,2,\ldots,n\}$. Assume that $\alpha\lambda_j \notin (-1,1]$. Since $\beta \in \mathbb{Z}$, then its reduced denominator is 1. Then clearly the reduced denominator of β divides $\lceil(\alpha\lambda_j - 1)/2\rceil$. Then either $\alpha\lambda_j \in (-1,1]$ or $\beta \in \mathbb{Q}$ with reduced denominator dividing $\lceil(\alpha\lambda_j - 1)/2\rceil$. Since j was arbitrary, then $(U^\alpha)^\beta = U^{\alpha\beta}$. Since α, β, and U were arbitrary, then $(U,\alpha) \mapsto U^\alpha$ is a monoid action on Mor(**Unitary**) with respect to $\mathbb{Z}$. It remains to be shown that $\mathbb{Z}$ is maximal. Assume that M is a submonoid of $\mathbb{R}$ for which $(U,\alpha) \mapsto U^\alpha$ is a monoid action on Mor(**Unitary**) and $\mathbb{Z}$ is a submonoid of M. Let $\beta \in M$. Then $(Z^2)^\beta = Z^{2\beta}$ by definition of M. Since $\lambda = 1$ is an eigenvalue of $\mathrm{Log}(Z)/(i\pi)$ and $2\lambda \notin (-1,1]$, then it follows by the first result of this proof that $\beta \in \mathbb{Q}$. Then there exists some $q \in \mathbb{Z}$ and $d \in \mathbb{N}$ such that $\beta = q/d$ and $\gcd(q,d) = 1$. Since $2d+3 \in \mathbb{Z} \subseteq M$, then $(Z^{2d+3})^\beta = Z^{\beta(2d+3)}$ by definition of M. Since $\lambda = 1$ is an eigenvalue of $\mathrm{Log}(Z)/(i\pi)$ and $(2d+3) \notin (-1,1]$, then by the first result of this proof d divides $\lceil((2d+3)-1)/2\rceil = d+1$. This is only possible when $d = 1$. Then $\beta = q/d = q \in \mathbb{Z}$. Since β was arbitrary, then $M \subseteq \mathbb{Z}$. In conclusion, $\mathbb{Z}$ is maximal.
- Let $\alpha \in (-1,1]$, $\beta \in (-1,1]$, and $U \in$ Mor(**Unitary**). It must be shown that $(U^\alpha)^\beta = U^{\alpha\beta}$. To this end, let $\{\lambda_j\}_{j=1}^n$ denote the eigenvalues of $\mathrm{Log}(U)/(i\pi)$. Since $\alpha \in (-1,1]$ and $i\lambda_j\pi \in (-\pi,\pi]$ for each $j \in \{1,2,\ldots,n\}$, then $\alpha\lambda_j \in (-1,1]$ for each $j \in \{1,2,\ldots,n\}$. Then by the first result of this proof, $(U^\alpha)^\beta = U^{\alpha\beta}$ regardless of the value of β. It remains to be shown that $(-1,1]$ is maximal. Assume that M is a submonoid of $\mathbb{R}$ for which $(U,\alpha) \mapsto U^\alpha$ is a monoid action on Mor(**Unitary**) and $(-1,1]$ is a submonoid of M. Let $\alpha \in \mathbb{R}$. There are three cases to consider.
  1. If $\alpha \in (-1,1]$, then $\alpha \in M$ by definition.
  2. If $\alpha = -1$, then $(Z^\alpha)^{1/2} = (Z^{-1})^{1/2} = Z^{1/2} = S \neq S^\dagger = Z^{-1/2} = Z^{\alpha/2}$. Since $1/2 \in M$, then $\alpha \notin M$, since M acts on Mor(**Unitary**) by exponentiation.
  3. Assume that $\alpha \notin [-1,1]$. Then $\alpha^2 > 1$ and there exists some $m \in \mathbb{N}$ such that $\alpha^{2m} > 2$. Let $\hat{\alpha} = \alpha^{2m}$. Then $(\hat{\alpha} - 1)/2 > 1/2$. Then $\lceil(\hat{\alpha}/2\rceil \geq 1$. Let $k = \lceil(\hat{\alpha} - 1)/2\rceil$ and $\beta = 1/(k+1)$. Since $\lambda = 1$ is an eigenvalue of $\mathrm{Log}(Z)/(i\pi)$ and $\hat{\alpha}\lambda = \hat{\alpha} \notin (-1,1]$, then it follows from the first result of this proof that $(U\hat{\alpha})^\beta = U^{\hat{\alpha}\beta}$ if and only if $k+1$ divides k. Since $k \neq 0$ and $k+1 > k$, then clearly $k+1$ does not divide k. This means that $(U^{\hat{\alpha}})^\beta \neq U^{\hat{\alpha}\beta}$. Since M acts on Mor(**Unitary**) by exponentiation and $\beta \in M$, then $\hat{\alpha} \notin M$. Then $\alpha \notin M$, since otherwise $\hat{\alpha} = \alpha^{2m} \in M$.

This means that if $\alpha \in M$, then $\alpha \in (-1,1]$. In other words, $M \cap \mathbb{R} = (-1,1]$. However, M was a submonoid of $\mathbb{R}$, so $M = (-1,1]$. In conclusion, $(-1,1]$ is maximal.

Then $\mathbb{Z}$ and $(-1,1]$ are maximal submonoids of $\mathbb{R}$ for which for which $(U,\alpha) \mapsto U^\alpha$ is a monoid action on $\mathrm{Mor}(\mathbf{Unitary})$. □

D Proofs for Section 4

This section contains all proofs for Section 4, except for those which appear in Section 4.1.

D.1 Proof of Lemma 4.1

Proof. First, it must be shown that $\Sigma_{\mathbf{HQC}} = \bigsqcup_{n=0}^{\infty} \Sigma_n^*$. This will require showing that if $j \neq k$, then Σ_j^* is disjoint from Σ_k^*. To this end, let $j \in \mathbb{N}$ and $k \in \mathbb{N}$ such that $j \neq k$. Assume, without loss of generality, that $j < k$. There are two cases to consider.

1. If $j = 0$, then $\Sigma_j^* = \Sigma_{\mathbf{HQC}}^j \subseteq \Sigma_{\mathbf{HQC}}^j$.
2. If $j > 0$, then $\Sigma_j^* = \Sigma_{\mathbf{HQC}}^j \setminus \Sigma_{\mathbf{HQC}}^{j-1} \subseteq \Sigma_{\mathbf{HQC}}^j$.

In either case, $\Sigma_j^* \subseteq \Sigma_{\mathbf{HQC}}^j$. Since $j \le k-1$, then by the inductive construction $\Sigma_j^* \subseteq \Sigma_{\mathbf{HQC}}^{k-1}$. Since $\Sigma_k^* = \Sigma_{\mathbf{HQC}}^k \setminus \Sigma_{\mathbf{HQC}}^{k-1}$, then $\Sigma_j^* \cap \Sigma_k^* = \varnothing$. Since j and k were arbitrary, then Σ_j^* and Σ_k^* are disjoint for each $j \in \mathbb{N}$ and $k \in \mathbb{N}$. Then $\bigsqcup_{n=0}^{\infty} \Sigma_n^* \subseteq \bigcup_{n=0}^{\infty} \Sigma_{\mathbf{HQC}}^n = \Sigma_{\mathbf{HQC}}$. Then let $g \in \Sigma_{\mathbf{HQC}}$. Then there exists some least $n \in \mathbb{N}$ such that $g \in \Sigma_{\mathbf{HQC}}^n$. There are two cases to consider.

1. If $n = 0$, then $g \in \Sigma_{\mathbf{HQC}}^n = \Sigma_n^*$.
2. If $n > 0$, then $g \notin \Sigma_{\mathbf{HQC}}^{n-1}$. Then $g \in \Sigma_{\mathbf{HQC}}^n \setminus \Sigma_{\mathbf{HQC}}^{n-1} = \Sigma_n^*$.

In either case, $g \in \Sigma_n^*$. Since g was arbitrary, then $\Sigma_{\mathbf{HQC}} = \bigsqcup_{n=0}^{\infty} \Sigma_n^*$. Then for each $g \in \Sigma_{\mathbf{HQC}}$, there exists a unique $\nu(g) \in \mathbb{N}$ such that $g \in \Sigma_{\nu(g)}^*$. This defines an assignment $\nu : \Sigma_{\mathbf{HQC}} \to \mathbb{N}$. This define a prop signature morphism $\rho : \Sigma_{\mathbf{HQC}} \to U(\mathcal{C})$ such that $\rho(g) = \tau_{\nu(g)}(g)$. This is well-defined since $g \in \Sigma_{\nu(g)}^*$ and $\tau_{\nu(g)} : \Sigma_{\nu(g)}^* \to U(\mathcal{C})$. Then there exists a unique prop functor $F : \mathbf{HQC} \to \mathcal{C}$ such that $F(g) = \rho(g)$ for each $g \in \Sigma_{\mathbf{HQC}}$. Moreover, if $n \in \mathbb{N}$ and $g \in \Sigma_n^*$, then $\nu(g) = n$ and consequently $F(g) = \rho(g) = \tau_{\nu(g)}(g) = \tau_n(g)$. It remains to be shown that F is unique. Assume that $G : \mathbf{HQC} \to \mathcal{C}$ is a prop functor such that $G(g) = \tau_n(g)$ for each $n \in \mathbb{N}$ and $g \in \Sigma_n^*$. Let $g \in \Sigma_{\mathbf{HQC}}$. Then $g \in \Sigma_{\nu(g)}^*$. Then $G(g) = \tau_{\nu(g)}(g) = F(g)$. Since g was arbitrary, then $G \circ i = F \circ i$. Then by the universal property of free prop categories, $G = F$. Since G was arbitrary, then F is unique. □

D.2 Proof of Lemma 4.2

Proof. Clearly $\Sigma_{\mathbf{Prim}}$, $\Sigma_{\mathbf{Ctrl}}$, and $\Sigma_{\mathbf{Pow}}$ are pairwise disjoint. This is because $(\odot)$ and $(\uparrow)$ are distinct term constructors and $\Sigma_{\mathbf{Prim}}$ consists only of base terms. This means that the set $\Sigma_{\mathbf{Prim}} \sqcup \Sigma_{\mathbf{Ctrl}} \sqcup \Sigma_{\mathbf{Pow}}$ is well-defined. Moreover, $\Sigma_{\mathbf{Prim}}$, $\Sigma_{\mathbf{Ctrl}}$, and $\Sigma_{\mathbf{Pow}}$ are all subsets of $\Sigma_{\mathbf{HQC}}$ by construction. Then it suffices to show that $\Sigma_{\mathbf{HQC}}$ is a subset of $\Sigma_{\mathbf{Prim}} \sqcup \Sigma_{\mathbf{Ctrl}} \sqcup \Sigma_{\mathbf{Pow}}$. Let $g \in \Sigma_{\mathbf{HQC}}$. Then there exists some least $n \in \mathbb{N}$ such that $g \in \Sigma_{\mathbf{HQC}}^n$. If $n = 0$, then it follows that $g \in \Sigma_{\mathbf{HQC}}^0 = \Sigma_{\mathbf{Prim}}$. Otherwise, $n > 0$ and $g \in \Sigma_{\mathbf{HQC}}^n \setminus \Sigma_{\mathbf{HQC}}^{n-1}$. By definition, the following equation holds.

$$\Sigma_{\mathbf{HQC}}^n \backslash_{\mathbf{HQC}}^{n-1} = \left(\Sigma_{\mathbf{HQC}}^{n-1} \cup \mathsf{Tower}(\mathbf{HQC}[n-1]) \cup \mathsf{Power}(\mathbf{HQC}[n-1]) \right) \setminus \Sigma_{\mathbf{HQC}}^{n-1}$$

$$\subseteq \mathsf{Tower}(\mathbf{HQC}[n-1]) \cup \mathsf{Power}(\mathbf{HQC}[n-1])$$

Then either $g \in \mathsf{Tower}(\mathbf{HQC}[n-1])$ or $g \in \mathsf{Power}(\mathbf{HQC}[n-1])$. There are three cases to consider.

1. Assume that $g \in \mathsf{Tower}(\mathbf{HQC}[n-1])$ and $|g| = 2$ Then $g_1 \in \mathrm{Mor}(\mathbf{HQC}[n-1]) \subseteq \mathbf{HQC}$ and $g_2 \in \mathrm{Mor}(\mathbf{HQC}[n-1]) \subseteq \mathbf{HQC}$. Moreover, $g = g_1 \odot g_2$. In conclusion, $g \in \Sigma_{\mathbf{Ctrl}}$.
2. Assume that $g \in \mathsf{Tower}(\mathbf{HQC}[n-1])$ and $|g| > 2$ Then $g_1 \in \mathrm{Mor}(\mathbf{HQC}[n-1]) \subseteq \mathbf{HQC}$. Define $V = g_2 \odot g_3 \odot \cdots \odot g_k$ where $k = |g|$. Then the following sequence of inclusions holds.
$$V \in \mathsf{Tower}(\mathbf{HQC}[n-1]) \subseteq \Sigma^n_{\mathbf{HQC}} \subseteq \mathbf{HQC}[n] \subseteq \mathbf{HQC}$$
Moreover, $g = g_1 \odot V$. In conclusion, $g \in \Sigma_{\mathbf{Ctrl}}$.
3. Assume that $g \in \mathsf{Power}(\mathbf{HQC}[n-1])$. Then there exists a $U \in \mathbf{HQC}[n-1]$ and $\alpha \in \mathbb{R}$ such that $g = U \uparrow \alpha$. Since $\mathbf{HQC}[n-1] \subseteq \mathbf{HQC}$, then $g \in \Sigma_{\mathbf{Pow}}$.

In either case, $g \in \Sigma_{\mathbf{Ctrl}} \sqcup \Sigma_{\mathbf{Pow}}$. Then $g \in \Sigma_{\mathbf{Prim}} \sqcup \Sigma_{\mathbf{Ctrl}} \sqcup \Sigma_{\mathbf{Pow}}$ regardless of the value of n. Since g was arbitrary, then $\Sigma_{\mathbf{HQC}} \subseteq \Sigma_{\mathbf{Prim}} \sqcup \Sigma_{\mathbf{Ctrl}} \sqcup \Sigma_{\mathbf{Pow}}$. This completes the proof. □

D.3 Proof of Therem 4.3

Proof. Clearly $[\![-]\!]_H \circ \dagger$ and $\dagger \circ [\![-]\!]_H$ are both contravariant prop functors from $\mathbf{HQC}$ to a subcategory of $\mathbf{HQC}$. Then $[\![-]\!]_H \circ \dagger = \dagger \circ [\![-]\!]_H$ if and only if $[\![-]\!] \circ \dagger \circ i = \dagger \circ [\![-]\!]_H \circ i$. In other words, $[\![U^\dagger]\!]_H = [\![U]\!]_H^\dagger$ for all $U \in \mathrm{Mor}(\mathbf{HQC})$ if and only if $[\![g^\dagger]\!]_H = [\![g]\!]_H^\dagger$ for all $g \in \Sigma_{\mathbf{HQC}}$. Let $g \in \Sigma_{\mathbf{HQC}}$. There are three cases to consider.

1. Assume $g \in \Sigma_{\mathbf{Prim}}$. By definition, $g^\dagger = g$ and $[\![g]\!]_H$ is Hermitian and unitary. Since $[\![g]\!]_H$ is both Hermitian and unitary, then $[\![g]\!]_H = [\![g]\!]_H^\dagger$. In conclusion, $[\![g^\dagger]\!]_H = [\![g]\!]_H = [\![g]\!]_H^\dagger$.
2. Assume $g \in \Sigma_{\mathbf{Ctrl}}$ with $\mathrm{dom}(g) = n$. Then by definition, $[\![g^\dagger]\!]_H = [\![g\uparrow(-1)]\!]_H = [\![g]\!]_H^{-1}$. Then the following equation holds.
$$\begin{aligned} [\![g]\!]_H [\![g^\dagger]\!]_H &= [\![g]\!]_H^1 [\![g]\!]_H^{-1} \\ &= \exp(\mathrm{Log}[\![g]\!]_H) \cdot \exp(\mathrm{Log}[\![g]\!]_H(-1)) \\ &= \exp(\mathrm{Log}[\![g]\!]_H + \mathrm{Log}[\![g]\!]_H(-1)) && \text{(by Eq. (1))} \\ &= \exp(\mathbb{O}_{2^n}) = \mathbb{I}_{2^n} \end{aligned}$$
In other words, $[\![g^\dagger]\!]_H$ is the inverse to $[\![g]\!]_H$. Since $[\![g]\!]_H$ is unitary, then $[\![g^\dagger]\!]_H = [\![g]\!]_H^\dagger$.
3. Assume $g \in \Sigma_{\mathbf{Pow}}$. Then there exists a $U \in \mathrm{Mor}(\mathbf{HQC})$ and an $\alpha \in \mathbb{R}$ such that $g = U \uparrow \alpha$. Then $g^\dagger = U \uparrow (-\alpha)$. Then by definition, $[\![g]\!]_H = [\![U]\!]_H^\alpha$ and $[\![g^\dagger]\!] = [\![U]\!]_H^{-\alpha}$. Then the following equation holds.
$$\begin{aligned} [\![g]\!]_H [\![g^\dagger]\!]_H &= [\![U]\!]_H^\alpha [\![U]\!]_H^{-\alpha} \\ &= \exp(\mathrm{Log}[\![g]\!]_H \alpha) \cdot \exp(\mathrm{Log}[\![g]\!]_H(-\alpha)) \\ &= \exp(\mathrm{Log}[\![g]\!]_H \alpha + \mathrm{Log}[\![g]\!]_H(-\alpha)) && \text{(by Eq. (1))} \\ &= \exp(\mathbb{O}_{2^n}) = \mathbb{I}_{2^n} \end{aligned}$$
In other words, $[\![g^\dagger]\!]_H$ is the inverse to $[\![g]\!]_H$. Since $[\![g]\!]_H$ is unitary, then $[\![g^\dagger]\!]_H = [\![g]\!]_H^\dagger$.

In each case, $[\![g^\dagger]\!]_H = [\![g]\!]_H^\dagger$. Since g was arbitrary, then $[\![g^\dagger]\!]_H = [\![g]\!]_H^\dagger$ for all $g \in \Sigma_{\mathbf{HQC}}$. In conclusion, $[\![U^\dagger]\!]_H = [\![U]\!]_H^\dagger$ for all $U \in \mathrm{Mor}(\mathbf{HQC})$. □

E Lambda Generators for Diagonal Circuits

This section shows how to construct the $\lambda(x,\alpha)$ circuits as described in Section 4. It is also shown that these circuits belong to the sub-language **Core** as defined in in Section 5. Up to a change of basis, every $\lambda(x,\alpha)$ generator can be thought of as an n-fold controlled global phase by an angle of $\alpha\pi$. The aforementioned change of basis should apply X-gates to the qubits, so that the state $|x\rangle := \bigotimes_{j=0}^{n-1} |x_j\rangle$ is sent to the state $|\mathsf{One}(n)\rangle := \bigotimes_{j=1}^{n} |1\rangle$.

E.1 Constructing the Change of Basis

Let $x \in \{0,1\}^n$. Then define $\mathsf{Nots}(x) = \boxed{\times}_{j=0}^{n-1} \left(-\oplus^{1-x_j}- \right)$. Note that in $\mathsf{Nots}(x)$, each X-gate has been exponentiated by either 0 or 1. This ensures that $\mathsf{Nots}(x) \in \mathbf{Core}(n,n)$. It follows that $[\![\mathsf{Nots}(x)]\!]_H = \bigotimes_{j=0}^{n-1} X^{1-x_j}$. To see how this operation acts on $|x\rangle$, there are two cases to consider.

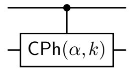
- If $x_j = 0$, then $X^{1-x_j}|x_j\rangle = X^1|0\rangle = |1\rangle$.
- If $x_j = 1$, then $X^{1-x_j}|x_j\rangle = X^0|1\rangle = |1\rangle$.

In either case, $X^{1-x_j}|x_j\rangle = |1\rangle$. This means that $[\![\mathsf{Nots}(x)]\!]_H |x\rangle = \bigotimes_{j=0}^{n-1} X^{1-x_j}|x_j\rangle = |\mathsf{One}(n)\rangle$, as desired. Since $[\![\mathsf{Nots}(x)]\!]_H$ is unitary, then $[\![\mathsf{Nots}(x)]\!]_H |\psi\rangle = |\mathsf{One}(n)\rangle$ if and only if $|\psi\rangle = |x\rangle$. Moreover, $[\![\mathsf{Nots}(x)]\!]_H$ is self-inverse.

E.2 Constructing the Controlled Phases

Let $n \in \mathbb{N}$ and $\alpha \in \mathbb{R}$. Then the n-fold controlled phase gate can be defined inductively as follows.

$\mathsf{CPh}(\alpha,0) = \bullet^{\alpha/\pi}$ $\mathsf{CPh}(\alpha,k+1) =$



Since $\mathsf{CPh}(\alpha,0)$ is a generator for **Core** which is closed under the application of Z-controls, then $\mathsf{CPh}(\alpha,n) \in \mathbf{Core}(n,n)$ for each $n \in \mathbb{N}$. It follows by induction that the following equation holds.

$$[\![\mathsf{CPh}(\alpha,n)]\!]_H |y\rangle = \begin{cases} e^{i\alpha}|y\rangle & \text{if } |y\rangle = |\mathsf{One}(n)\rangle \\ |y\rangle & \text{otherwise} \end{cases} \tag{3}$$

The proof proceeds as follows.

- **Base Case**. Since $|\mathsf{One}(0)\rangle$ is the only basis vector for $\mathbb{C}^1$ and $\mathsf{CPh}(\alpha,0) = e^{i\alpha}$, then Eq. (3) holds when $n = 0$.
- **Inductive Hypothesis**. The equation Eq. (3) holds for some $k \in \mathbb{N}$.
- **Inductive Step**. Assume that the inductive hypothesis holds for some $k \in \mathbb{N}$. This means that Eq. (3) holds for k. To show that Eq. (3) holds for $k+1$, let $x \in \{0,1\}^{k+1}$. Then there exists some $a \in \{0,1\}$ and $y \in \{0,1\}^k$ such that $x = ay$. This means that $|x\rangle = |a\rangle \otimes |y\rangle$. Now recall from Theorem 3.2 that $[\![\mathsf{CPh}(\alpha,k+1)]\!]_H = |0\rangle\langle 0| \otimes \mathbb{I}_{2^k} + |1\rangle\langle 1| \otimes [\![\mathsf{CPh}(\alpha,k)]\!]_H$. There are three cases to consider.
  1. Assume that $a = 0$. Then $[\![\mathsf{CPh}(\alpha,k+1)]\!]_H |x\rangle = |a\rangle \otimes |y\rangle = |x\rangle$, since $\langle 0|a\rangle = 1$ and $\langle 1|a\rangle = 0$. Then $|x\rangle \neq |\mathsf{One}(k+1)\rangle$ and $[\![\mathsf{CPh}(\alpha,k+1)]\!] |x\rangle = |x\rangle$.

2. Assume $a = 1$ and $|y\rangle \neq |\mathsf{One}(k)\rangle$. Then $\llbracket \mathsf{CPh}(\alpha, k+1) \rrbracket_H |x\rangle = |a\rangle \otimes \llbracket \mathsf{CPh}(\alpha, k) \rrbracket |y\rangle$, since $\langle 0|a\rangle = 1$ and $\langle 1|a\rangle = 0$. Since Eq. (3) holds for k and $|y\rangle \neq |\mathsf{One}(k)\rangle$, then $\llbracket \mathsf{CPh}(\alpha, k) \rrbracket |y\rangle = |y\rangle$. It follows that $\llbracket \mathsf{CPh}(\alpha, k+1) \rrbracket |x\rangle = |a\rangle \otimes |y\rangle = |x\rangle$. In conclusion, $|x\rangle \neq |\mathsf{One}(k+1)\rangle$ and $\llbracket \mathsf{CPh}(\alpha, k+1) \rrbracket |x\rangle = |x\rangle$.
3. Assume $a = 1$ and $|y\rangle = |\mathsf{One}(k)\rangle$. Then $\llbracket \mathsf{CPh}(\alpha, k+1) \rrbracket_H |x\rangle = |a\rangle \otimes \llbracket \mathsf{CPh}(\alpha, k) \rrbracket |y\rangle$, since $\langle 0|a\rangle = 1$ and $\langle 1|a\rangle = 0$. Since Eq. (3) holds for k and $|y\rangle = |\mathsf{One}(k)\rangle$, then $\llbracket \mathsf{CPh}(\alpha, k) \rrbracket |y\rangle = e^{i\alpha} |y\rangle$. It follows that $\llbracket \mathsf{CPh}(\alpha, k+1) \rrbracket |x\rangle = |a\rangle \otimes e^{i\alpha} |y\rangle = e^{i\alpha} |x\rangle$. In conclusion, $|x\rangle \neq |\mathsf{One}(k+1)\rangle$ and $\llbracket \mathsf{CPh}(\alpha, k+1) \rrbracket |x\rangle = e^{i\alpha} |x\rangle$.

Then Eq. (3) holds for $k+1$ by case distinction.

Then by the principle of induction, Eq. (3) holds for each $n \in \mathbb{N}$.

E.3 Constructing the Lambda Generators

Let $x \in \{0,1\}^*$ and $\alpha \in (-\pi, \pi]$. Since $x \in \{0,1\}^*$, then x is a possibly empty word over the alphabet $\{0,1\}$. The (x,α)-*lambda generator* is the circuit $\lambda(x,\alpha) = \mathsf{Nots}(x) \circ \mathsf{CPh}(\alpha, n) \circ \mathsf{Nots}(x)$ where $n = |x|$. Since $\mathsf{Nots}(x) \in \mathbf{Core}(n,n)$ and $\mathsf{CPh}(\alpha, n) \in \mathbf{Core}(n,n)$, then $\lambda(x,\alpha) \in \mathbf{Core}(n,n)$ as well. It must be shown that $\lambda(x,\alpha)$ has the intended semantics. Clearly $\{|y\rangle : y \in \{0,1\}^n\}$ is a basis for $\mathbb{C}^{2^n}$. Let $y \in \{0,1\}^n$. There are two cases to consider.

1. Assume that $|y\rangle = |x\rangle$. Then the following equation holds.

$$\begin{aligned} \llbracket \lambda(x,\alpha) \rrbracket_H |y\rangle &= \llbracket \mathsf{Nots}(x) \rrbracket_H \circ \llbracket \mathsf{CPh}(\alpha, n) \rrbracket_H \circ \llbracket \mathsf{Nots}(x) \rrbracket_H |y\rangle \\ &= \llbracket \mathsf{Nots}(x) \rrbracket_H \circ \llbracket \mathsf{CPh}(\alpha, n) \rrbracket_H |\mathsf{One}(n)\rangle \\ &= e^{i\alpha\pi} \llbracket \mathsf{Nots}(x) \rrbracket_H |\mathsf{One}(n)\rangle = e^{i\alpha} |x\rangle \end{aligned}$$

Then $|y\rangle$ is an eigenvector of $\llbracket \lambda(x,\alpha) \rrbracket_H$ with eigenvalue $e^{i\alpha}$.

2. Assume that $|y\rangle = |x\rangle$. Then there exists some $z \in \{0,1\}^n$ such that $|z\rangle = \llbracket \mathsf{Nots}(x) \rrbracket_H |y\rangle$ with $z \neq x$. Then the following equation holds.

$$\begin{aligned} \llbracket \lambda(x,\alpha) \rrbracket_H |y\rangle &= \llbracket \mathsf{Nots}(x) \rrbracket_H \circ \llbracket \mathsf{CPh}(\alpha, n) \rrbracket_H \circ \llbracket \mathsf{Nots}(x) \rrbracket_H |y\rangle \\ &= \llbracket \mathsf{Nots}(x) \rrbracket_H \circ \llbracket \mathsf{CPh}(\alpha, n) \rrbracket_H |z\rangle \\ &= \llbracket \mathsf{Nots}(x) \rrbracket_H |z\rangle = |y\rangle \end{aligned}$$

Then $|y\rangle$ is an eigenvector of $\llbracket \lambda(x,\alpha) \rrbracket_H$ with eigenvalue 1.

Then $\llbracket \lambda(x,\alpha) \rrbracket_H$ has eigenvalue $e^{i\alpha}$ with eigenspace $\mathrm{span}\{|x\rangle\}$ and eigenvalue 1 with eigenspace $\mathrm{span}\{|y\rangle : y \in \{0,1\}^n \setminus \{x\}\}$. Since $\alpha \in (-\pi, \pi]$, then $\mathrm{Log}\llbracket \lambda(x,\alpha) \rrbracket_H = i\alpha |x\rangle \langle x| = i\alpha \bigotimes_{j=0}^{n-1} |x_j\rangle \langle x_j|$. In other words, $\llbracket \lambda(x,\alpha) \rrbracket_H = \exp(iH)$ where $H = \alpha \bigotimes_{j=0}^{n-1} |x_j\rangle \langle x_j|$.

Theorem E.1. *If $x \in \{0,1\}^n$ and $\alpha \in \mathbb{R}$, then $\lambda(x,\alpha) \in \mathbf{Core}(n,n)$ and $\llbracket \lambda(x,\alpha) \rrbracket_H = \exp(iH)$ where $H = \alpha \bigotimes_{j=0}^{n-1} |x_j\rangle \langle x_j|$. If $\alpha \in (-\pi, \pi]$, then $\mathrm{Log}\llbracket \lambda(x,\alpha) \rrbracket_H = iH$ as well.*

Corollary E.2. *Let $n \in \mathbb{N}$ with a bijection $f : \{1, 2, \ldots, 2^n\} \to \{0,1\}^n$. If $M \in \mathbf{Unitary}(2^n, 2^n)$ is a diagonal matrix, then there exists a unique function $\alpha : \{1, 2, \ldots, 2^n\} \to (-\pi, \pi]$ such that $M = \llbracket C \rrbracket_H$ where $C = \lambda(f(1), \alpha(1)) \circ \lambda(f(2), \alpha(2)) \circ \cdots \circ \lambda(f(2^n), \alpha(2^n))$.*

Proof. Since M is a diagonal matrix, then M has eigenbasis $\{|y\rangle : y \in \{0,1\}^n\}$. For each $j \in \mathbb{N}$, let $|b_j\rangle$ denote $|f(j)\rangle$ and β_j denote the eigenvalue associated to $|b_j\rangle$. Then define $\alpha(j) = \mathrm{Log}(\beta_j)/i$. It remains to be shown that $[\![C]\!]_H = M$. By Theorem E.1, $\mathrm{Log}[\![\lambda(f(j), \alpha(j))]\!]_H = i\alpha(j) |b_j\rangle \langle b_j|$ for each $j \in \{1, 2, \ldots, 2^n\}$. Then it suffices to show that each $\mathrm{Log}[\![\lambda(f(j), \alpha(j))]\!]_H$ commutes with each $\mathrm{Log}[\![\lambda(f(k), \alpha(k))]\!]_H$. To this end, let $j \in \{1, 2, \ldots, 2^n\}$ and $k \in \{1, 2, \ldots, 2^n\}$ such that $j \neq k$. Since f is a bijection, then $f(j) \neq f(k)$. Then $\langle b_j | b_k\rangle = \delta_{j,k} = 0 = \delta_{k,j} = \langle b_k | b_j\rangle$ where δ is the Kronecker delta function. Then the following equation holds.

$$\mathrm{Log}[\![\lambda(f(j), \alpha(j))]\!]_H \, \mathrm{Log}[\![\lambda(f(k), \alpha(k))]\!]_H = \mathbb{O}_{2^n} = \mathrm{Log}[\![\lambda(f(k), \alpha(k))]\!]_H \, \mathrm{Log}[\![\lambda(f(j), \alpha(j))]\!]_H$$

Since j and k were arbitrary, then $\mathrm{Log}[\![\lambda(f(j), \alpha(j))]\!]_H$ commutes $\mathrm{Log}[\![\lambda(f(k), \alpha(k))]\!]_H$ for each $j \in \{1, 2, \ldots, 2^n\}$ and $k \in \{1, 2, \ldots, 2^n\}$. Then the following equation holds.

$$\begin{aligned}
[\![C]\!]_H = \prod_{j=1}^{2^n} [\![\lambda(f(j), \alpha(j)]\!]_H &= \prod_{j=1}^{2^n} \exp(i\alpha(j) |b_j\rangle \langle b_j|) \\
&= \exp\left(\sum_{j=1}^{2^n} i\alpha(j) |b_j\rangle \langle b_j|\right) && \text{(by Eq. (1))} \\
&= \sum_{j=1}^{2^n} \exp(i\alpha(j)) |b_j\rangle \langle b_j| \\
&= \sum_{j=1}^{2^n} \exp(i \, \mathrm{Log}(\beta_j)/i) |b_j\rangle \langle b_j| \\
&= \sum_{j=1}^{2^n} \beta_j |f(j)\rangle \langle f(j)| = M
\end{aligned}$$

It remains to be shown that α is unique. Assume that there exists some $\gamma : \{1, 2, \ldots, 2^n\} \to (-\pi, \pi]$ such that $M = [\![D]\!]_H$ where $D = \lambda(f(1), \gamma(1)) \circ \lambda(f(2), \gamma(2)) \circ \cdots \circ \lambda(f(2^n), \gamma(2^n))$. It suffices to show that α and γ agree pointwise. Let $j \in \{1, 2, \ldots, 2^n\}$. Then the following equation holds.

$$e^{i\alpha(j)} = \sum_{k=1}^{2^n} e^{i\alpha(j)} \delta_{j,k} \delta_{k,j} = \langle b_j | \, [\![C]\!]_H \, |b_j\rangle = \langle b_j | \, [\![D]\!]_H \, |b_j\rangle = \sum_{k=1}^{2^n} e^{i\gamma(j)} \delta_{j,k} \delta_{k,j} = e^{i\gamma(j)}$$

Since $\alpha(j) \in (-\pi, \pi]$ and $\beta(j) \in (-\pi, \pi]$, then the following equation holds.

$$\alpha(j) = i\alpha(j)/i = \mathrm{Log}(\exp(i\alpha(j)))/i = \mathrm{Log}(\exp(i\gamma(j)))/i = i\gamma(j)/i = \gamma(j)$$

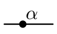
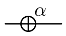
Since j was arbitrary, then $\alpha = \gamma$. Since γ was arbitrary, then α is unique. □

F Proofs for Section 4

This section contains all proofs for Section 4.1.

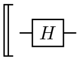
F.1 Proof of Theorem 4.4

Proof. First it must be shown that each relation in E_0 is sound. Let $(X,Y) \in E_0$. Start by noting the following.

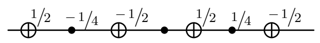
$[\![$  $]\!]_H = e^{\mathrm{Log}(Z)\alpha} = \begin{bmatrix}1&0\\0&e^{i\alpha\pi}\end{bmatrix} = Z(\alpha\pi)$ $[\![$  $]\!]_H = e^{\mathrm{Log}(X)\alpha} = \frac{1}{2}\begin{bmatrix}1+e^{i\alpha\pi}&1-e^{i\alpha\pi}\\1-e^{i\alpha\pi}&1+e^{i\alpha\pi}\end{bmatrix} = X(\alpha\pi)$

There are several cases to consider.

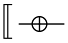
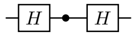
- Assume that (X,Y) is E(1). Then the following equation holds.

$[\![X]\!]_H = [\![$  $]\!]_H = \frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$

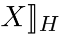
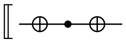
$$= \overbrace{\underbrace{\tfrac{1}{2}\begin{bmatrix}1-i&1+i\\1+i&1-i\end{bmatrix}}_{X(-\pi/2)}\underbrace{\begin{bmatrix}1&0\\0&e^{i\pi/4}\end{bmatrix}}_{Z(\pi/4)}\underbrace{\tfrac{1}{2}\begin{bmatrix}1+i&1-i\\1-i&1+i\end{bmatrix}}_{X(\pi/2)}}^{Y(\pi/4)}\underbrace{\begin{bmatrix}1&0\\0&-1\end{bmatrix}}_{Z}\overbrace{\underbrace{\tfrac{1}{2}\begin{bmatrix}1-i&1+i\\1+i&1-i\end{bmatrix}}_{X(-\pi/2)}\underbrace{\begin{bmatrix}1&0\\0&e^{-i\pi/4}\end{bmatrix}}_{Z(-\pi/4)}\underbrace{\tfrac{1}{2}\begin{bmatrix}1+i&1-i\\1-i&1+i\end{bmatrix}}_{X(\pi/2)}}^{Y(-\pi/4)}$$

$= [\![$  $]\!]_H = [\![Y]\!]_H$

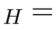
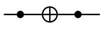
- Assume that (X,Y) is E(2). Then the following equation holds.

$[\![X]\!]_H = [\![$  $]\!]_H = \begin{bmatrix}0&1\\1&0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1&0\\0&-1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix} = [\![$  $]\!]_H = [\![Y]\!]_H$

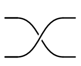
- Assume that (X,Y) is E(3). Then the following equation holds.

$[\![X]\!]_H = [\![$  $]\!]_H = \begin{bmatrix}-1&0\\0&1\end{bmatrix} = \begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1&0\\0&-1\end{bmatrix}\begin{bmatrix}0&1\\1&0\end{bmatrix} = [\![$  $]\!]_H = [\![Y]\!]_H$

- Assume that (X,Y) is E(4). Then the following equation holds.

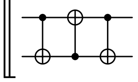
$[\![X]\!]_H = [\![$  $]\!]_H = \begin{bmatrix}0&-1\\-1&0\end{bmatrix} = \begin{bmatrix}1&0\\0&-1\end{bmatrix}\begin{bmatrix}0&1\\1&0\end{bmatrix}\begin{bmatrix}1&0\\0&-1\end{bmatrix} = [\![$  $]\!]_H = [\![Y]\!]_H$

- Assume that (X,Y) is E(5). Then the following equation holds.

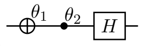
$[\![X]\!]_H = [\![$  $]\!]_H = \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$

$$= \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

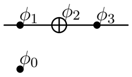
$$= [\![Z \odot X]\!]_H [\![X \odot Z]\!]_H [\![Z \odot X]\!]_H$$

$= [\![$  $]\!]_H = [\![Y]\!]_H$

- Assume that (X,Y) is an instance of the relation E(6). Then let $\theta_1, \theta_2 \in \mathbb{R}$ and define $(\phi_0\pi, \phi_1\pi, \phi_2\pi, \phi_3\pi) = \mathsf{Euler}(\theta_1\pi, \theta_2\pi)$ as in an arbitrary instance of E(6). Then by the soundness of Q(5), the equation $HZ(\theta_1\pi)HZ(\theta_2\pi)H = e^{i\phi_0\pi}Z(\phi_1\pi)HZ(\phi_2\pi)HZ(\phi_3\pi)$ holds. As explained in [4], $X(\alpha) = HZ(\alpha)H$ for $\alpha \in \mathbb{R}$. Then the following equation holds.

$[\![X]\!]_H = [\![$  $]\!]_H = HZ(\theta_2\pi)X(\theta_1\pi)$

$$
\begin{aligned}
&= HZ(\theta_2\pi)HZ(\theta_1\pi)H\\
&= e^{i\phi_0\pi}Z(\phi_1\pi)HZ(\phi_2\pi)HZ(\phi_3\pi)\\
&= e^{i\phi_0\pi}Z(\phi_1\pi)X(\phi_2\pi)Z(\phi_3\pi)
\end{aligned}
$$

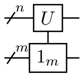
$= \llbracket$ 

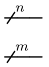
$\rrbracket_H = \llbracket Y\rrbracket_H$

- Assume that (X,Y) is E(7). Then the following equation holds.

$$\llbracket X\rrbracket_H = \llbracket \bullet^2 \rrbracket_H = \exp(2\,\mathrm{Log}\llbracket \bullet \rrbracket_H) = \exp(2\,\mathrm{Log}(-1)) = \exp(2(i\pi)) = \mathbb{I}_1 = \llbracket 1_0\rrbracket_H = \llbracket Y\rrbracket_H$$

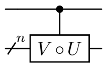
- Assume that (X,Y) is an instance of E(8). Then the following holds by Corollary 3.3.

$\llbracket X\rrbracket_H = \llbracket$ 

$\rrbracket_H = \llbracket U\rrbracket_H \odot \llbracket 1_m\rrbracket_H = \mathbb{I}_{2^{n+m}} = \mathbb{I}_{2^n}\otimes\mathbb{I}_{2^m} = \llbracket$ 

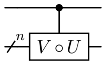
$\rrbracket_H = \llbracket Y\rrbracket_H$

- Assume that (X,Y) is an instance of E(9). Since Z is unitary with eigenvalues $\{-1,1\}$, then Z is Hermitian. Then the following equation holds.

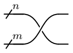
$\llbracket X\rrbracket_H = \llbracket$ 

$\rrbracket_H = Z\odot\llbracket V\circ U\rrbracket_H$

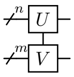
$$
\begin{aligned}
&= Z\odot(\llbracket V\rrbracket_H\circ\llbracket U\rrbracket_H)\\
&= (Z\odot\llbracket V\rrbracket_H)\circ(Z\odot\llbracket U\rrbracket)_H \qquad \text{(by Cor. Corollary 3.3)}
\end{aligned}
$$

$= \llbracket$ 

$\rrbracket_H = \llbracket Y\rrbracket_H$

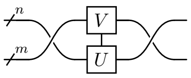
- Assume that (X,Y) is an instance of E(10). Since $\llbracket - \rrbracket_H : \mathbf{HQC}\to\mathbf{Unitary}$ is symmetric monoidal, then $\llbracket$ 

$\rrbracket_H$ is the monoidal symmetry $\sigma_{2^n,2^m} : \mathbb{C}^{2^n}\otimes\mathbb{C}^{2^m}\cong\mathbb{C}^{2^m}\otimes\mathbb{C}^{2^n}$. Then $\sigma_{2^n,2^m}$ is the self-adjoint unitary operator whose action is $\sigma_{2^n,2^m}\cdot(N\otimes M)\cdot\sigma_{2^n,2^m} = M\otimes N$ for all $M\in\mathbf{Unitary}(2^n,2^n)$ and $N\in\mathbf{Unitary}(2^m,2^m)$. Then the following equation holds.

$\llbracket X\rrbracket = \llbracket$ 

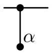
$\rrbracket_H = \exp(\mathrm{Log}\llbracket U\rrbracket_H\otimes\mathrm{Log}\llbracket V\rrbracket_H/(i\pi))$

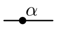
$$
\begin{aligned}
&= \exp(\sigma_{2^n,2^m}\cdot(\mathrm{Log}\llbracket V\rrbracket_H\otimes\mathrm{Log}\llbracket U\rrbracket_H/(i\pi))\cdot\sigma_{2^n,2^m})\\
&= \sigma_{2^n,2^m}\cdot\exp(\mathrm{Log}\llbracket V\rrbracket_H\otimes\mathrm{Log}\llbracket U\rrbracket_H/(i\pi))\cdot\sigma_{2^n,2^m} \qquad \text{(by Eq. (2))}
\end{aligned}
$$

$= \llbracket$ 

$\rrbracket_H = \llbracket Y\rrbracket_H$

- Assume that (X,Y) is an instance of E(11). Then the following holds by Theorem 3.4.

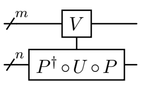
$\llbracket X\rrbracket_H = \llbracket$ 

$\rrbracket_H = Z\odot\llbracket \bullet^{\alpha} \rrbracket = Z\odot e^{i\alpha\pi} = Z^{\alpha} = \llbracket$ 

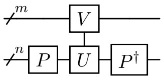
$\rrbracket_H = \llbracket Y\rrbracket_H$

- Assume that (X,Y) is an instance of E(12). Then the following equation holds.

$$[\![X]\!]_H = [\![$$



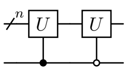
$$
\begin{aligned}
]\!]_H &= [\![V]\!]_H \odot [\![P^\dagger \circ U \circ P]\!] \\
&= [\![V]\!]_H \odot ([\![P^\dagger]\!]_H \circ [\![U]\!]_H \circ [\![P]\!]_H) \\
&= [\![V]\!]_H \odot ([\![P]\!]_H^\dagger \circ [\![U]\!]_H \circ [\![P]\!]_H) && \text{(by Thm. 4.3)} \\
&= (\mathbb{I}_{2^m} \otimes [\![P]\!]_H^\dagger)([\![V]\!] \odot [\![U]\!])(\mathbb{I}_{2^m} \otimes [\![P]\!]_H) && \text{(by Cor. 3.3)} \\
&= (\mathbb{I}_{2^m} \otimes [\![P^\dagger]\!]_H)([\![V]\!] \odot [\![U]\!])(\mathbb{I}_{2^m} \otimes [\![P]\!]_H) && \text{(by Thm. 4.3)} \\
&= [\![
\end{aligned}
$$



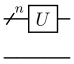
$$]\!]_H = [\![Y]\!]_H$$

- Assume that (X,Y) is an instance of E(13). First, note that for each $M \in \textbf{Unitary}(2^n, 2^n)$, the matrix $M \otimes |0\rangle\langle 0|$ commutes with the matrix $M \otimes |1\rangle\langle 1|$ since $\langle 0|1\rangle = 0 = \langle 1|0\rangle$. Then the following equation holds where $A = \mathrm{Log}(-Z) = i\,|0\rangle\langle 0|\,\pi$ and $B = \mathrm{Log}(Z) = i\,|1\rangle\langle 1|\,\pi$.

$$[\![X]\!]_H = [\![$$



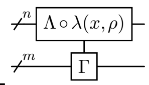
$$
\begin{aligned}
]\!]_H &= \exp(\mathrm{Log}[\![U]\!]_H \otimes A/(i\pi)) \exp(\mathrm{Log}[\![U]\!]_H \otimes B/(i\pi)) \\
&= \exp(\mathrm{Log}[\![U]\!]_H \otimes |0\rangle\langle 0|) \exp(\mathrm{Log}[\![U]\!]_H \otimes |1\rangle\langle 1|) && \text{(by Eq. (1))} \\
&= \exp\left((\mathrm{Log}[\![U]\!]_H \otimes |0\rangle\langle 0|) + (\mathrm{Log}[\![U]\!]_H \otimes |1\rangle\langle 1|)\right) \\
&= \exp(\mathrm{Log}[\![U]\!]_H \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|)) \\
&= \exp(\mathrm{Log}[\![U]\!]_H \otimes \mathbb{I}_2) \\
&= \exp(\mathrm{Log}[\![U]\!]_H) \otimes \mathbb{I}_2 \\
&= [\![U]\!]_H \otimes \mathbb{I}_2 \\
&= [\![
\end{aligned}
$$



$$]\!]_H = [\![Y]\!]_H$$

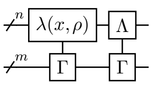
- Assume that (X,Y) is an instance of E(14). As in Section E, let $|x\rangle = \bigotimes_{j=0}^{n-1} |x_j\rangle$. Moreover, let Λ be the prefix of a diagonal form for which the term $\lambda(x,\rho)$ does not appear. This means that the eigenvalue of $|x\rangle \in [\![\Lambda]\!]_H$ is 1, and consequently $[\![\Lambda]\!]_H$ has the form $[\![\Lambda]\!]_H = \exp\left(\sum_{y \in \mathcal{B}} i\theta_y |y\rangle\langle y|\right)$ where $\mathcal{B} = \{0,1\}^n \setminus \{x\}$ and $\theta_y \in (-\pi, \pi]$ for each $y \in \mathcal{B}$ (see Corollary E.2). Since $x \notin \mathcal{B}$, then for each $y \in \mathcal{B}$, $\langle x|y\rangle = 0 = \langle y|x\rangle$ and consequently the matrix $|x\rangle\langle x|$ commutes with $|y\rangle\langle y|$. Then the following equation holds for $M = \mathrm{Log}[\![\Gamma]\!]_H/(i\pi)$.

$$[\![X]\!]_H = [\![$$

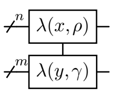


$$
\begin{aligned}
]\!]_H & \\
&= \exp\left(\mathrm{Log}[\![\Lambda \circ \lambda(x,\rho)]\!]_H \otimes M\right) \\
&= \exp\left(\mathrm{Log}\left([\![\Lambda]\!]_H [\![\lambda(x,\rho)]\!]_H\right) \otimes M\right) \\
&= \exp\left(\mathrm{Log}\left(\exp\left(\sum_{y \in \mathcal{B}} i\theta_y |y\rangle\langle y|\right) \exp(i\rho |x\rangle\langle x|)\right) \otimes M\right) && \text{(by Thm. E.1)}
\end{aligned}
$$

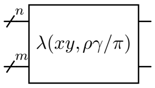
$$\begin{aligned}
&= \exp\left(\mathrm{Log}\left(\exp\left(\sum_{y\in\mathcal{B}} (i\theta_y\,|y\rangle\langle y|) + i\rho\,|x\rangle\langle x|\right)\right)\otimes M\right) && \text{(by Eq. (1))}\\
&= \exp\left(\mathrm{Log}\left(\sum_{y\in\mathcal{B}}\left(e^{i\theta_y}\,|y\rangle\langle y|\right) + e^{i\rho}\,|x\rangle\langle x|\right)\otimes M\right)\\
&= \exp\left(\left(\sum_{y\in\mathcal{B}}\left(\mathrm{Log}\left(e^{i\theta_y}\right)|y\rangle\langle y|\right) + \mathrm{Log}\left(e^{i\rho}\right)|x\rangle\langle x|\right)\otimes M\right)\\
&= \exp\left(\left(\left(\sum_{y\in\mathcal{B}} i\theta_y\,|y\rangle\langle y|\right) + i\rho\,|x\rangle\langle x|\right)\otimes M\right)\\
&= \exp\left((\mathrm{Log}\llbracket\Lambda\rrbracket_H + \mathrm{Log}\llbracket\lambda(x,\rho)\rrbracket_H)\otimes M\right)\\
&= \exp\left((\mathrm{Log}\llbracket\Lambda\rrbracket_H \otimes M) + (\mathrm{Log}\llbracket\lambda(x,\rho)\rrbracket_H\otimes M)\right)\\
&= \exp\left(\mathrm{Log}\llbracket\Lambda\rrbracket_H \otimes M\right)\exp\left(\mathrm{Log}\llbracket\lambda(x,\rho)\rrbracket_H\otimes M\right) && \text{(by Eq. (1))}
\end{aligned}$$

$= \Big\llbracket$  $\Big\rrbracket_H = \llbracket Y\rrbracket_H$

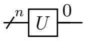
- Assume that (X,Y) is an instance of E(15). Then let $\rho\in(-\pi,\pi]$ and $\gamma\in(-\pi,\pi]$ as in an arbitrary instance of E(15). Then the following equation holds.

$\llbracket X\rrbracket_H = \Big\llbracket$  $\Big\rrbracket_H$

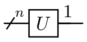
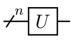
$$\begin{aligned}
&= \exp(\mathrm{Log}\llbracket\lambda(x,\rho)\rrbracket_H \otimes \mathrm{Log}\llbracket\lambda(y,\gamma)\rrbracket_H/(i\pi))\\
&= \exp\left((i\rho\,|x\rangle\langle x|)\otimes(i\gamma\,|y\rangle\langle y|)/(i\pi)\right) && \text{(by Thm. E.1)}\\
&= \exp\left(\left(i^2\rho\gamma\,|xy\rangle\langle xy|\right)/(i\pi)\right)\\
&= \exp(i(\rho\gamma/\pi)\,|xy\rangle\langle xy|)
\end{aligned}$$

$= \Big\llbracket$  $\Big\rrbracket_H = \llbracket Y\rrbracket_H$

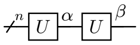
- Assume that (X,Y) is an instance of E(16). Then the following equation holds.

$\llbracket X\rrbracket_H = \Big\llbracket$  $\Big\rrbracket_H = \exp(0\,\mathrm{Log}\llbracket U\rrbracket_H) = \exp(\mathbb{O}_{2^n}) = \mathbb{I}_{2^n} = \llbracket$ $\rrbracket_H = \llbracket Y\rrbracket_H$

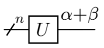
- Assume that (X,Y) is an instance of E(17). Then the following equation holds.

$\llbracket X\rrbracket_H = \Big\llbracket$  $\Big\rrbracket_H = \exp(1\,\mathrm{Log}\llbracket U\rrbracket_H) = \exp(\mathrm{Log}\llbracket U\rrbracket_H) = U = \Big\llbracket$  $\Big\rrbracket_H = \llbracket Y\rrbracket_H$

- Assume that (X,Y) is an instance of E(18). Then the following equation holds.

$\llbracket X\rrbracket_H = \Big\llbracket$  $\Big\rrbracket_H$

$$\begin{aligned}
&= \exp(\beta\,\mathrm{Log}\llbracket U\rrbracket_H)\exp(\alpha\,\mathrm{Log}\llbracket U\rrbracket_H)\\
&= \exp((\alpha+\beta)\,\mathrm{Log}\llbracket U\rrbracket_H) && \text{(by Eq. (1))}
\end{aligned}$$

$= \Big\llbracket$  $\Big\rrbracket_H = \llbracket Y\rrbracket_H$

- Assume that (X,Y) is an instance of E(19). Then the following equation holds.

$$\llbracket X\rrbracket_H = \left\llbracket \not{-}^{n}\boxed{1_n}^{\alpha}- \right\rrbracket_H = \exp(\alpha\,\mathrm{Log}(\mathbb{I}_{2^n})) = \exp(\alpha\mathbb{O}_{2^n}) = \exp(\mathbb{O}_{2^n}) = \mathbb{I}_{2^n} = \llbracket \not{-}^{n}- \rrbracket_H = \llbracket Y\rrbracket_H$$

- Assume that (X,Y) is an instance of E(20). Then the following equation holds.

$$\begin{aligned}
\llbracket X\rrbracket_H = \left\llbracket \not{-}^{n}\boxed{P}-\boxed{U}^{\alpha}-\boxed{P^\dagger}- \right\rrbracket_H &= \llbracket P^\dagger\rrbracket_H \exp(\mathrm{Log}\llbracket U\rrbracket_H\alpha)\llbracket P\rrbracket_H \\
&= \llbracket P\rrbracket_H^\dagger \exp(\mathrm{Log}\llbracket U\rrbracket_H\alpha)\llbracket P\rrbracket_H && \text{(by Thm. 4.3)} \\
&= \exp\left(\llbracket P\rrbracket_H^\dagger \,\mathrm{Log}\llbracket U\rrbracket_H\llbracket P\rrbracket_H\alpha\right) && \text{(by Eq. (2))} \\
&= \exp\left(\mathrm{Log}\left(\llbracket P\rrbracket_H^\dagger\llbracket U\rrbracket_H\llbracket P\rrbracket_H\right)\alpha\right) && \text{(by Eq. (2))} \\
&= \left\llbracket \not{-}^{n}\boxed{P^\dagger\circ U\circ P}^{\alpha}- \right\rrbracket_H = \llbracket Y\rrbracket_H
\end{aligned}$$

- Assume that (X,Y) is an instance of E(21). As in Section E, let $|x\rangle = \bigotimes_{j=0}^{n-1}|x_j\rangle$. Moreover, let Λ be the prefix of a diagonal form for which the term $\lambda(x,\rho)$ does not appear. This means that the eigenvalue of $|x\rangle \in \llbracket\Lambda\rrbracket_H$ is 1, and consequently $\llbracket\Lambda\rrbracket_H$ has the form $\llbracket\Lambda\rrbracket_H = \exp\left(\sum_{y\in\mathcal{B}} i\theta_y|y\rangle\langle y|\right)$ where $\mathcal{B} = \{0,1\}^n\setminus\{x\}$ and $\theta_y\in(-\pi,\pi]$ for each $y\in\mathcal{B}$ (see Corollary E.2). Since $x\notin\mathcal{B}$, then for each $y\in\mathcal{B}$, $\langle x|y\rangle = 0 = \langle y|x\rangle$ and consequently the matrix $|x\rangle\langle x|$ commutes with $|y\rangle\langle y|$. Then the following equation holds.

$$\begin{aligned}
\llbracket X\rrbracket_H &= \left\llbracket \not{-}^{n}\boxed{\Lambda\circ\lambda(x,\rho)}^{\alpha}- \right\rrbracket_H \\
&= \exp(\mathrm{Log}\llbracket\Lambda\circ\lambda(x,\rho)\rrbracket_H\alpha) \\
&= \exp(\mathrm{Log}(\llbracket\Lambda\rrbracket_H\llbracket\lambda(x,\rho)\rrbracket_H)\alpha) \\
&= \exp\left(\mathrm{Log}\left(\exp\left(\sum_{y\in\mathcal{B}} i\theta_y|y\rangle\langle y|\right)\exp(i\rho|x\rangle\langle x|)\right)\alpha\right) && \text{(by Thm. E.1)} \\
&= \exp\left(\mathrm{Log}\left(\exp\left(\sum_{y\in\mathcal{B}}(i\theta_y|y\rangle\langle y|) + i\rho|x\rangle\langle x|\right)\right)\alpha\right) && \text{(by Eq. (1))} \\
&= \exp\left(\mathrm{Log}\left(\sum_{y\in\mathcal{B}}\left(e^{i\theta_y}|y\rangle\langle y|\right) + e^{i\rho}|x\rangle\langle x|\right)\alpha\right) \\
&= \exp\left(\left(\sum_{y\in\mathcal{B}}\left(\mathrm{Log}\left(e^{i\theta_y}\right)|y\rangle\langle y|\right) + \mathrm{Log}\left(e^{i\rho}\right)|x\rangle\langle x|\right)\alpha\right) \\
&= \exp\left(\sum_{y\in\mathcal{B}}(i\theta_y\alpha|y\rangle\langle y|) + i\alpha\rho|x\rangle\langle x|\right) \\
&= \exp\left(\sum_{y\in\mathcal{B}} i\theta_y\alpha|y\rangle\langle y|\right)\exp\left(i\alpha\rho|x\rangle\langle x|\right) && \text{(by Eq. (1))} \\
&= \exp(\mathrm{Log}\llbracket\Lambda\rrbracket_H\alpha)\cdot\llbracket\lambda(x,\alpha\rho)\rrbracket_H \\
&= \left\llbracket \not{-}^{n}\boxed{\lambda(x,\alpha\rho)}-\boxed{\Lambda}^{\alpha}- \right\rrbracket_H = \llbracket Y\rrbracket_H
\end{aligned}$$

Since (X,Y) was arbitrary, then $[\![-]\!]_H$ is sound with respect to E_0. It then follows by induction on E_n that E is sound with respect to $[\![-]\!]_H$.

- **Base Case**. It follows by the proceeding analysis that E_0 is sound with respect to $[\![-]\!]_H$.
- **Inductive Hypothesis**. For some $n \in \mathbb{N}$, E_n is sound with respect to $[\![-]\!]_H$.
- **Inductive Step**. Assume that for some $n \in \mathbb{N}$, that E_n is sound with respect to $[\![-]\!]_H$. Then let $(X,Y) \in E_{n+1}$. There are three cases to consider.
  1. Assume that $(X,Y) \in E_n$. Then $[\![X]\!]_H = [\![Y]\!]_H$ by the inductive hypothesis.
  2. Assume that there exists some $U \in \mathrm{Mor}(\mathbf{Core})$ and $V \approx_{E_n} W$ such that $X = U \odot V$ and $Y = U \odot W$. Then by the inductive hypothesis, $[\![V]\!]_H = [\![W]\!]_H$. It follows that $[\![X]\!]_H = \exp(\mathrm{Log}[\![U]\!]_H \otimes [\![V]\!]_H/(i\pi)) = \exp(\mathrm{Log}[\![U]\!]_H \otimes [\![W]\!]_H/(i\pi)) = [\![Y]\!]_H$.
  3. Assume that there exists some exponent $\alpha \in \mathbb{R}$ and $V \approx_{E_n} W$ such that $X = V \uparrow \alpha$ and $Y = W \uparrow \alpha$. Then by the inductive hypothesis, $[\![V]\!]_H = [\![W]\!]_H$. It follows that $[\![X]\!]_H = \exp(\alpha \,\mathrm{Log}[\![U]\!]_H) = \exp(\alpha \,\mathrm{Log}[\![W]\!]_H) = [\![Y]\!]_H$.

  In each case, $[\![X]\!]_H = [\![Y]\!]_H$. Since (X,Y) was arbitrary, then E_{n+1} is sound with respect to $[\![-]\!]_H$. Then the inductive step holds.

Then by the principle of inductive, E_n is sound with respect to $[\![-]\!]_H$ for each $n \in \mathbb{N}$. Assume that $(X,Y) \in E$. Then there exists some $n \in \mathbb{N}$ such that $(X,Y) \in E_n$. Then $[\![X]\!]_H = [\![Y]\!]_H$. Since (X,Y) was arbitrary, then E is sound with respect to $[\![-]\!]_H$. □

F.2 Proof of Theorem 4.5

Proof. First, it must be shown that $F(f) \circ f \approx_E 1_n$ and $f \circ F(f) \approx_E 1_m$ for each $f \in P(\Sigma)(n,m)$. This follows by structural induction on the morphisms in $P(\Sigma)$.

- **Identity**. Assume that $f = 1_n$. Since F is a prop functor, then $F(f) = F(1_n) = 1_n$. Then $F(f) \circ f = 1_n \circ 1_n = 1_n$ and $f \circ F(f) = 1_n \circ 1_n = 1_n$. Since $\approx_E$ is reflexive, then $F(f) \circ f \approx_E 1_n$ and $f \circ F(f) \approx_E 1_n$.
- **Symmetries**. Assume that $f = \sigma$. Since F is a strict symmetric monoidal functor, then $F(\sigma) = \sigma$. By definition, $F(f) \circ f = \sigma \circ \sigma = 1_2$ and $f \circ F(f) = \sigma \circ \sigma = 1_2$. Since $\approx_E$ is reflexive, then $F(f) \circ f \approx_E 1_2$ and $f \circ F(f) \approx_E 1_2$.
- **Generators**. Assume that $f = x$ for some $x \in \Sigma$. Then $n = \mathrm{dom}(x)$ and $m = \mathrm{cod}(x)$. Moreover, $F(f) \circ f = F(x) \circ x \approx_E 1_n$ and $f \circ F(f) = x \circ F(x) \approx_E 1_m$.
- **Sequential Composition**. Assume that $f = b \circ a$ for $a : n \to s$ and $b : s \to m$. Then by the inductive hypothesis, the following equations hold.

  $$F(a) \circ a \approx_E 1_n \qquad a \circ F(a) \approx_E 1_x \qquad F(b) \circ b \approx_E 1_x \qquad b \circ F(b) \approx_E 1_m$$

  Since F is a contravariant functor, then the following equation holds.

  $$\begin{aligned} F(f) \circ f &= (F(a) \circ F(b)) \circ (b \circ a) \approx_E F(a) \circ 1_x \circ a = F(a) \circ a \approx_E 1_n \\ f \circ F(f) &= (b \circ a) \circ (F(a) \circ F(b)) \approx_E b \circ 1_x \circ F(b) = b \circ F(b) \approx_E 1_m \end{aligned}$$

  Then $F(f) \circ f \approx_E 1_n$ and $f \circ F(f) \approx_E 1_m$ by the transitivity of $\approx_E$.

- **Parallel Composition**. Assume that $f = a \boxtimes b$ for $a : s \to t$ and $b : x \to y$. Clearly $n = s + x$ and $m = t + y$. Then by the inductive hypothesis, the following equations hold.

$$F(a) \circ a \approx_E 1_n \qquad a \circ F(a) \approx_E 1_x \qquad F(b) \circ b \approx_E 1_x \qquad b \circ F(b) \approx_E 1_m$$

Since F is a strict monoidal functor, then the following equation holds.

$$F(f) \circ f = (F(a) \boxtimes F(b)) \circ (a \boxtimes b) = (F(a) \circ a) \boxtimes (F(b) \circ b) \approx_E 1_s \boxtimes (F(b) \circ b) \approx_E 1_s \boxtimes 1_x$$
$$f \circ F(f) = (a \boxtimes b) \circ (F(a) \boxtimes F(b)) = (a \circ F(a)) \boxtimes (b \circ F(b)) \approx_E 1_t \boxtimes (b \circ F(b)) \approx_E 1_t \boxtimes 1_y$$

Then $F(f) \circ f \approx_E 1_s \boxtimes 1_x = 1_n$ and $f \circ F(f) \approx_E 1_t \boxtimes 1_y = 1_m$ by the transitivity of $\approx_E$.

Then by the principle of structural induction, $F(f) \circ f \approx_E 1_n$ and $f \circ F(f) \approx_E 1_m$ for each $f \in P(\Sigma)(n,m)$. Next, let $(f,g) \in E$ where $f : n \to m$. Then $f \approx_E g$, $F(f) \circ f \approx_E 1_n$, and $g \circ F(g) \approx_E 1_m$ by the previous result. Then the following equation holds.

$$F(f) = F(f) \circ 1_m \approx_E F(f) \circ g \circ F(g) \approx_E F(f) \circ f \circ F(g) \approx_E 1_n \circ F(g) = F(g)$$

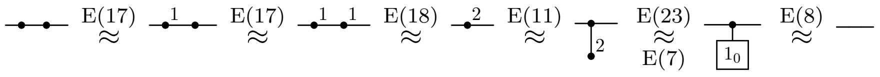
Then $F(f) \approx_E F(g)$ by the transitivity of $(\approx_E)$. Then $\pi_E^{\mathrm{op}}(F(f)) = \pi_E^{\mathrm{op}}(F(g))$. Then by the universal property of prop quotients, there exists a unique prop functor $H : P(\Sigma)/E \to (P(\Sigma)/E)^{\mathrm{op}}$ such that $H \circ \pi_E = \pi_E^{\mathrm{op}} \circ F$. It remains to be shown that H is a dagger functor. To this end, let $f \in P(\Sigma)(n,m)$. Then $f \circ F(f) \approx_E 1_m$. Likewise, $F(f) \circ F^{\mathrm{op}}(F(f)) \approx 1_n$. This means that $f = f \circ 1_n \approx_E f \circ F(f) \circ F^{\mathrm{op}}(F(f)) \approx_E 1_m \circ F^{\mathrm{op}}(F(f))F(F^{\mathrm{op}}(f))$. Then it follows that $\pi_E(f) = \pi_E(F^{\mathrm{op}}(F(f))) = H^{\mathrm{op}}(\pi_E^{\mathrm{op}}(F(f))) = H^{\mathrm{op}}(H(\pi_E(f)))$. Since f was an arbitrary, then $\pi_E = H^{\mathrm{op}} \circ H \circ \pi_E$. Then by uniqueness, $H^{\mathrm{op}} \circ H = 1_{P(\Sigma)/E}$. Then H is a dagger functor. Finally, let $f : n \to n$. Then $F(f) \circ f \approx_E 1_n$ and $f \circ F(f) \approx_E 1_m$. This means that $H(\pi_E(f)) \circ \pi_E(f) = 1_n$ and $\pi_E(f) \circ H(\pi_E(f)) = 1_n$. Since f was arbitrary and π_E is surjective, then $H(f) \circ f = 1_n$ and $f \circ H(f) = 1_m$ for each $f \in P(\Sigma)/E$. In other words, every morphism in $P(\Sigma)/E$ is unitary. □

F.3 Proof of Theorem 4.7

Proof. First it must be shown that $g^\dagger \circ g \approx_E 1_{\mathrm{dom}(g)}$ and $g \circ g^\dagger \approx_E 1_{\mathrm{cod}(g)}$ for each $g \in \Sigma_{\mathbf{HQC}}$. Let $g \in \Sigma_{\mathbf{HQC}}$. There are three cases to consider.

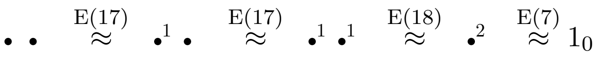
1. Assume that $g \in \Sigma_{\mathbf{Prim}}$. Then $g^\dagger = g$ and $n = \mathrm{dom}(g) = \mathrm{cod}(g)$. Then it suffices to show that $g \circ g \approx_E 1_n$. There are six cases to consider.

   (a) Assume that $g =$. Then the following equation holds.



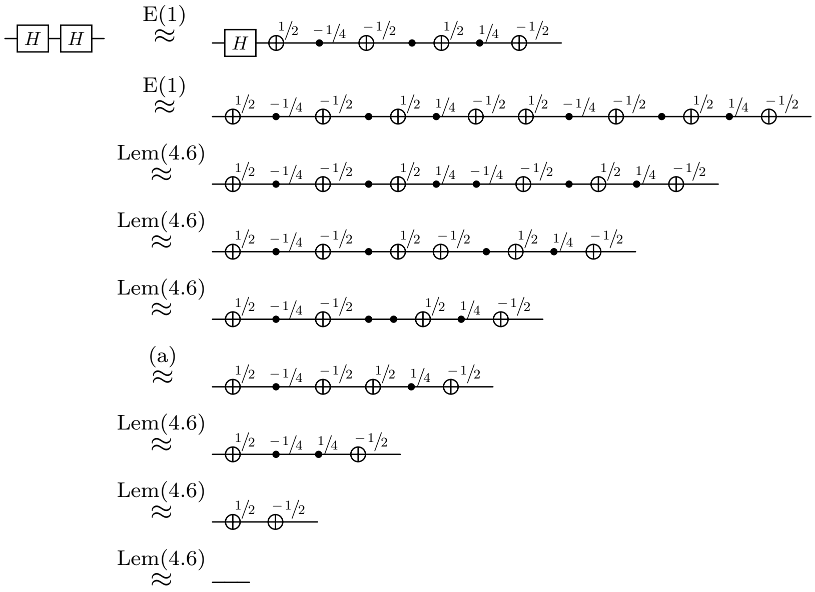
   Then $g \circ g \approx_E 1_n$ by transitivity.

   (b) Assume that $g =$. Then the following equation holds.



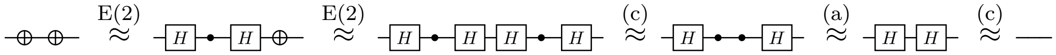
   Then $g \circ g \approx_E 1_n$ by transitivity.

(c) Assume that $g = \boxed{H}$. Then the following equation holds.

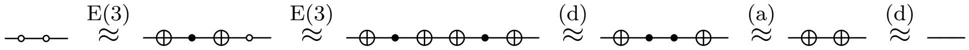


Then $g \circ g \approx_E 1_n$ by transitivity.

(d) Assume that $g = \oplus$. Then the following equation holds.

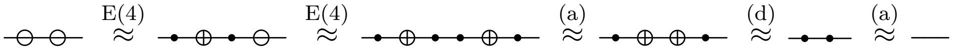


(e) Assume that $g = \circ$. Then the following equation holds.



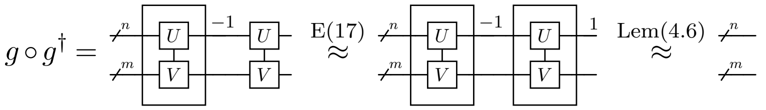
Then $g \circ g \approx_E 1_n$ by transitivity.

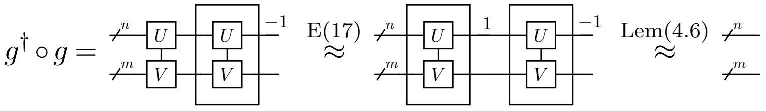
(f) Assume that $g = \bigcirc$. Then the following equation holds.



In each case $g \circ g \approx_E 1_n$. Then $g^\dagger \circ g \approx_E 1_{\mathrm{dom}(g)}$ and $g \circ g^\dagger \approx_E 1_{\mathrm{cod}(g)}$.

2. Assume $g \in \Sigma_{\mathbf{Ctrl}}$. Then there exists $U \in \mathrm{Mor}(\mathbf{HQC})$ and $V \in \mathrm{Mor}(\mathbf{HQC})$ such that $g = U \odot V$. Then the following equations hold.





Then $g^\dagger \circ g \approx_E 1_{\mathrm{dom}(g)}$ and $g \circ g^\dagger \approx_E 1_{\mathrm{cod}(g)}$ by transitivity.

3. Assume $g \in \Sigma_{\mathbf{Pow}}$. Then there exists $U \in \mathrm{Mor}(\mathbf{HQC})$ and $\alpha \in \mathbb{R}$ such that $g = U \uparrow \alpha$. It follows that $g^\dagger = U \uparrow (-\alpha)$. Then $g^\dagger \circ g \approx_E 1_{\mathrm{dom}(g)}$ and $g \circ g^\dagger \approx_E 1_{\mathrm{cod}(g)}$ by Lemma 4.6.

In each case, $g^\dagger \circ g \approx_E 1_{\mathrm{dom}(g)}$ and $g \circ g^\dagger \approx_E 1_{\mathrm{cod}(g)}$. Since g was an arbitrary generator, then $g^\dagger \circ g \approx_E 1_{\mathrm{dom}(g)}$ and $g \circ g^\dagger \approx_E 1_{\mathrm{cod}(g)}$ for each $g \in \Sigma_{\mathbf{HQC}}$. Then by Theorem 4.5, there exists a unique functor $\bar{\dagger} : \mathbf{HQC}/E \to \mathbf{HQC}/E$ such that $\bar{\dagger} \circ \pi_E = \pi_E^{\mathrm{op}} \circ \dagger$ with every morphism in $\mathbf{HQC}/E$ unitary with respect to $(\bar{\dagger})$. □

F.4 Proof of Lemma 4.8

Proof. Let $f \in \mathcal{C}(n,n)$. By assumption, f and $C(f)$ are unitary. This means that $f^\dagger \circ f = 1_n$ and $C(f) \circ C(f)^\dagger = 1_{n+1}$. Since C is a functor, then $C(f^\dagger) \circ C(f) = C(f^\dagger \circ f) = C(1_n) = 1_{n+1}$. Then $C(f^\dagger) = C(f^\dagger) \circ C(f) \circ C(f)^\dagger = C(f)^\dagger$. Since f was arbitrary, then C is a dagger functor. □

F.5 Proof of Theorem 4.9

Proof. Assume that conditions (1) and (2) hold and define an assignment $F : P(\Sigma) \to P(\Sigma)/E$ such that $F_0(n) = n+1$ and $F(f : n \to n) = \pi_E(\tau_n(f))$. Then F is fully determined, and is therefore unique. It remains to be shown that F is a functor.

- **Identities**. Let $n \in \mathbb{N}$. Since $\tau_n(1_n) \approx_E 1_{n+1}$ by condition (1), then the following holds.

$$F(1_n) = \pi_E(\tau_n(1_n)) = \pi_E(1_{n+1}) = 1_{n+1}$$

  Since n was arbitrary, then F respects identities.

- **Composition**. Let $f : n \to n$ and $g : n \to n$. Since $\tau_n(g \circ f) \approx_E \tau_n(g) \circ \tau_n(f)$ by condition (2), then the following holds.

$$F(g \circ f) = \pi_E(\tau_n(g \circ f)) = \pi_E(\tau_n(g) \circ \tau_n(f)) = \pi_E(\tau_n(g)) \circ \pi_E(\tau_n(f)) = F(g) \circ F(f)$$

  Since f and g were arbitrary, then F respects composition.

Since F respects identities and composition, then F is a functor. Next, assume that condition (3) holds. It must be shown that there exists a unique functor $H : P(\Sigma)/E \to P(\Sigma)/E$ such that $H \circ \pi_E = F$. Let $(f,g) \in E$. Since $\tau_E(f) \approx_E \tau_E(g)$, then $F(f) = \pi_E(\tau_n(f)) = \pi_E(\tau_n(g)) = F(g)$. Since (f,g) was arbitrary, then there exists a unique functor $H : P(\Sigma)/E \to P(\Sigma)/E$ such that $H \circ \pi_E = F$. Finally, assume that conditions (4) through to (6) hold. It remains to be shown that H is a control functor.

1. Let $f \in (P(\Sigma)/E)(n,n)$. Then there exists a $g \in P(\Sigma)(n,n)$ such that $\pi_E(g) = f$. Then $H(f \boxtimes 1) = H(\pi_E(g) \boxtimes 1) = H(\pi_E(g \boxtimes 1)) = F(g \boxtimes 1)$. Since $\tau_{n+1}(g \boxtimes 1) \approx_E \tau_n(g) \boxtimes 1$ by condition (4), then the following holds.

$$H(f \boxtimes 1) = F(g \boxtimes 1) = \pi_E(\tau_n(g \boxtimes 1)) = \pi_E(\tau_n(g) \boxtimes 1) = \pi_E(\tau_n(g)) \boxtimes 1 = F(g) \boxtimes 1 = H(f) \boxtimes 1$$

   Since f was arbitrary, then $H(f \boxtimes 1) = H(f) \boxtimes 1$ for each $f \in (P(\Sigma)/E)(n,n)$.

2. Let $f \in (P(\Sigma)/E)(n,n)$. Then there exists a $g \in P(\Sigma)(n,n)$ such that $\pi_E(g) = f$. Then the following equation holds.

$$H(H(f)) = H(H(\pi_E(g))) = H(F(g)) = H(\pi_E(\tau_n(g))) = F(\tau_n(g)) = \pi_E(\tau_{n+1}(\tau_n(g)))$$

Since $\tau_{n+1}(\tau_n(g)) \approx_E (\sigma \boxtimes 1_n) \circ \tau_{n+1}(\tau_n(g)) \circ (\sigma \boxtimes 1_n)$ by condition (5), then the following equation holds where $\sigma = \sigma \boxtimes 1_n$ and $\overline{\sigma} = \pi_E(\sigma)$.

$$\pi_E(\tau_{n+1}(\tau_n(g))) = \pi_E(\sigma \circ \tau_{n+1}(\tau_n(g)) \circ \sigma) = \overline{\sigma} \circ \pi_E(\tau_{n+1}(\tau_n(g))) \circ \overline{\sigma}$$

In conclusion, the following equation holds.

$$H(H(f)) = \pi_E(\tau_{n+1}(\tau_n(g))) = \overline{\sigma} \circ \pi_E(\tau_{n+1}(\tau_n(g))) \circ \overline{\sigma} = \overline{\sigma} \circ H(H(f)) \circ \overline{\sigma}$$

Since f was arbitrary, then $H(H(f)) = \overline{\sigma} \circ H(H(f)) \circ \overline{\sigma}$ for each $f \in (P(\Sigma)/E)(n,n)$.

3. Let $f \in (P(\Sigma)/E)(n+2,n+2)$ and $0 \le k \le n$. Then there exists a $g \in P(\Sigma)(n+2,n+2)$ such that $\pi_E(g) = f$. Then $H(f) = H(\pi_E(g)) = F(g)$ the following equation holds.

$$H(\gamma_{n,k} \circ f \circ \gamma_{n,k}) = H(\gamma_{n,k} \circ \pi_E(g) \circ \gamma_{n,k}) = H(\pi_E(\gamma_{n,k} \circ g \circ \gamma_{n,k})) = F(\gamma_{n,k} \circ g \circ \gamma_{n,k})$$

Since $\tau_{n+2}(\gamma_{n,k} \circ g \circ \gamma_{n,k}) = (1 \boxtimes \gamma_{n,k}) \circ \tau_{n+2}(g) \circ (1 \boxtimes \gamma_{n,k})$, then the following equation holds.

$$\begin{aligned} F(\gamma_{n,k} \circ g \circ \gamma_{n,k}) &= \pi_E(\tau_{n+2}(\gamma_{n,k} \circ g \circ \gamma_{n,k})) \\ &= \pi_E((1 \boxtimes \gamma_{n,k}) \circ \tau_{n+2}(g) \circ (1 \boxtimes \gamma_{n,k})) \\ &= (1 \boxtimes \gamma_{n,k}) \circ \pi_E(\tau_{n+2}(g)) \circ (1 \boxtimes \gamma_{n,k}) \\ &= (1 \boxtimes \gamma_{n,k}) \circ F(g) \circ (1 \boxtimes \gamma_{n,k}) \\ &= (1 \boxtimes \gamma_{n,k}) \circ H(f) \circ (1 \boxtimes \gamma_{n,k}) \end{aligned}$$

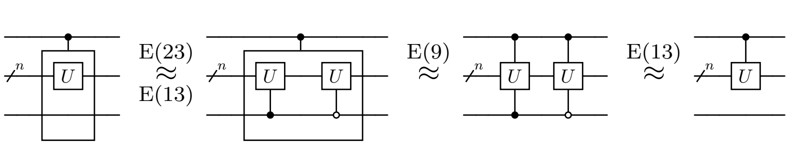
Since f was an arbitrary morphism, then $H(\gamma_{n,k} \circ f \circ \gamma_{n,k}) = (1 \boxtimes \gamma_{n,k}) \circ H(f) \circ (1 \boxtimes \gamma_{n,k})$ for each $f \in (P(\Sigma)/E)(n+2,n+2)$ and $0 \le k \le n$.

Then H is a control functor. □

F.6 Proof of Theorem 4.10

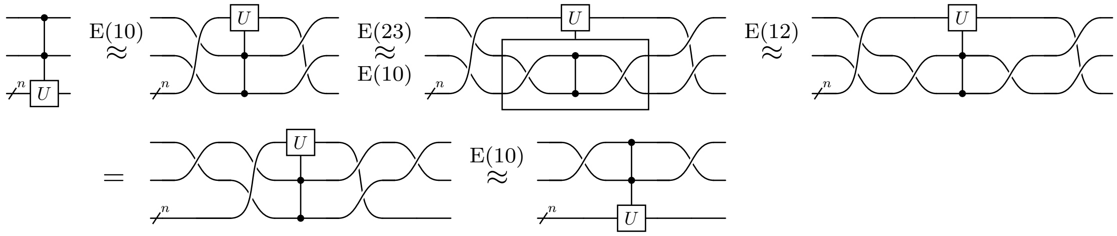
Proof. Since all generators in $\Sigma_{\mathbf{HQC}}$ are endomorphic, then Theorem 4.9 is applicable to **HQC**. Let $\{\tau_n : \mathbf{HQC}(n,n) \to \mathbf{HQC}(n+1,n+1)\}_{n \in \mathbb{N}}$ be the family of functions defined by the equation $\tau_n(U) =$ ─●─ $\odot U$. The six conditions hold as follows.

1. If $n \in \mathbb{N}$, $\tau_n(1_n) \approx_E 1 \boxtimes 1_n = 1_{n+1}$ by E(8).
2. If $U : n \to n$ and $V : n \to n$, then $\tau_n(V \circ U) = \tau_n(V) \circ \tau_n(U)$ by E(9).
3. If $U : n \to n$ and $(U,V) \in E$, then $\tau_n(U) \approx_E \tau_n(V)$ by E(23).
4. Let $U : n \to n$. Then the following derivation holds.



Then $\tau_{n+1}(U \boxtimes 1) \approx_E \tau_n(U) \boxtimes 1$.

5. Let $U : n \to n$. Then the following implication holds. Since $\sigma^\dagger = \sigma$, then the following derivation also holds.



Then $\tau_{n+1}(\tau_n(U)) \approx_E (\sigma \boxtimes 1_n) \circ \tau_{n+1}(\tau_n(U)) \circ (\sigma \boxtimes 1_n)$.

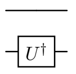
6. Let $U : n+2 \to n+2$ and $0 \le k \le n$. Since $1_k^\dagger = 1_k$, $1_{n-k}^\dagger = 1_{n-k}$, and $\sigma^\dagger = \sigma$, then it follows that $\gamma_{n,k}^\dagger = (1_k \boxtimes \sigma \boxtimes 1_{n-k})^\dagger = 1_k^\dagger \boxtimes \sigma^\dagger \boxtimes 1_{n-k}^\dagger = \gamma_{n,k}$. Since $\gamma_{n,k}^\dagger = \gamma_{n,k}$, then it follows by E(12) that $\tau_{n+2}(\gamma_{n,k} \circ U \circ \gamma_{n,k}) \approx_E (1 \boxtimes \gamma_{n,k}) \circ \tau_{n+2}(U) \circ (1 \boxtimes \gamma_{n,k})$.

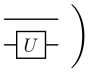
Since conditions (1) and (2) hold, then by Theorem 4.9 there exists a unique ordinary functor $F : \mathbf{HQC} \to \mathbf{HQC}/E$ such that $F_0(n) = n+1$ and $F(U : n \to n) = \pi_E(\tau_n(U))$. Since condition (3) also holds, then by Theorem 4.9 exists a unique ordinary functor $C : \mathbf{HQC}/E \to \mathbf{HQC}/E$ such that $H \circ \pi_E = F$. Then $C(\pi_E(U)) = F(U) = \pi_E($ —•— $\odot U)$ for each $U \in \mathbf{HQC}(n,n)$. Since conditions (4) through to (6) hold, then C is a control functor. Since every morphism in $\mathbf{HQC}/E$ is unitary with respect to $(\bar{\dagger})$ by Theorem 4.7, then C is a dagger control functor with respect to $(\bar{\dagger})$ by Lemma 4.8.

It remains to be shown that C is a conjugated control functor. Let $X \in (\mathbf{HQC}/E)(n,n)$ and $Y \in (\mathbf{HQC}/E)(n,n)$. Then there exists $U \in \mathbf{HQC}(n,n)$ and $V \in \mathbf{HQC}(n,n)$ such that $\pi_E(U) = X$ and $\pi_E(V) = Y$. Then $(1 \boxtimes U^\dagger) \circ ($ —•— $\odot V) \circ (1 \boxtimes U) \approx_E ($ —•— $\odot (U^\dagger \circ V \circ U))$ by E(12). Then the following equation holds.

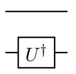
$\left(1 \boxtimes X^{\bar{\dagger}}\right) \circ C(\pi_E(V)) \circ (1 \boxtimes X) = \left(1 \boxtimes \pi_E(U)^{\bar{\dagger}}\right) \circ C(\pi_E(V)) \circ (1 \boxtimes \pi_E(U))$

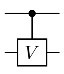
$= \left(1 \boxtimes \pi_E\left(U^\dagger\right)\right) \circ C(\pi_E(V)) \circ (1 \boxtimes \pi_E(U))$ (by Theorem 4.7)

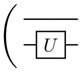
$= \pi_E\Bigg($ 

$\Bigg) \circ C(\pi_E(V)) \circ \pi_E\Bigg($ 

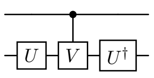
$\Bigg)$

$= \pi_E\Bigg($ 

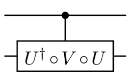
$\Bigg) \circ \pi_E\Bigg($ 

$\Bigg) \circ \pi_E\Bigg($ 

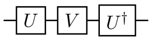
$\Bigg)$ (by Theorem 4.10)

$= \pi_E\Bigg($ 

$\Bigg)$

$= \pi_E\Bigg($ 

$\Bigg)$ (by $\approx_E$)

$= C\left(\pi_E\left(\right.\right.$ 

$\left.\left.\right)\right)$ (by Theorem 4.10)

$= C\left(\pi_E\left(U^\dagger\right) \circ \pi_E(V) \circ \pi_E(U)\right)$

$= C\left(\pi_E(U)^{\bar{\dagger}} \circ \pi_E(V) \circ \pi_E(U)\right)$

$= C\left(X^{\bar{\dagger}} \circ Y \circ X\right)$ (by Theorem 4.7)

Since X and Y were arbitrary, then $C(-)$ is conjugated. □

G Proofs for Section 5

This section contains all proofs for Section 5, except for those which appear in Section 5.1.

G.1 Proof of Theorem 5.1

Proof. In assumptions (1) through to (3), local properties placed on $\mathsf{Enc}(-)$ and $\mathsf{Dec}(-)$ in terms of generators and relations. These local properties lift to global properties as follows.

1. **Derivation (1)**. Assumption (1) states that $[\![\mathsf{Enc}(x)]\!]_\Gamma = [\![x]\!]_\Sigma$ for all $x \in \Sigma$. This means that $[\![-]\!]_\Gamma \circ \mathsf{Enc} \circ i = [\![-]\!]_\Sigma \circ i$. Then $[\![-]\!]_\Gamma \circ \mathsf{Enc} = [\![-]\!]_\Sigma$ by the universal property of free prop categories.
2. **Derivation (2)**. Let $(X,Y) \in Q$. By assumption (3), there exists an $X^* \in \mathsf{Dec}(X)$ and $Y^* \in \mathsf{Dec}(Y)$ such that $X^* \approx_E Y^*$. Since $X^* \in \mathsf{Dec}(X)$, then $\pi_E(X^*) = \mathsf{Dec}(X)$. Since $Y^* \in \mathsf{Dec}(Y)$, then $\pi_E(Y^*) = \mathsf{Dec}(Y)$. Since $X^* \approx_E Y^*$, then $\pi_E(X^*) = \pi_E(Y^*)$. Then in conclusion, $\mathsf{Dec}(X) = \pi_E(X^*) = \pi_E(Y^*) = \mathsf{Dec}(Y)$. Since (X,Y) was an arbitrary relation in Q, then there exists a unique controlled prop functor $\mathsf{Dec}_Q : P_C(\Gamma)/Q \to P(\Sigma)/E$ such that $\mathsf{Dec}_Q \circ \pi_Q = \mathsf{Dec}$.
3. **Derivation (3)**. Let $x \in \Sigma$. Then by assumption (2), there exists a $f \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $x \approx_E f$. Since $f \in \mathsf{Dec}(\mathsf{Enc}(x))$, then $\pi_E(f) = \mathsf{Dec}(\mathsf{Enc}(x))$. Since $x \approx_E f$, then $\pi_E(x) = \pi_E(f)$. Then $\pi_E(x) = \pi_E(f) = \mathsf{Dec}(\mathsf{Enc}(x))$. Since x was as arbitrary generator, then $\pi_E \circ i = \mathsf{Dec} \circ \mathsf{Enc} \circ i$. Then $\pi_E = \mathsf{Dec} \circ \mathsf{Enc}$ by the universal property of prop categories.

Next, it will be shown that (Σ, E) is complete with respect to $[\![-]\!]_\Sigma$. Let $f, g \in P(\Sigma)$ such that $[\![f]\!]_\Sigma = [\![g]\!]_\Sigma$. Then $[\![\mathsf{Enc}(f)]\!]_\Gamma = [\![f]\!]_\Sigma = [\![g]\!]_\Sigma = [\![\mathsf{Enc}(g)]\!]_\Gamma$ by derivation (1). Since (Γ, Q) is complete with respect to $[\![-]\!]_\Gamma$, then $\mathsf{Enc}(f) \approx_Q \mathsf{Enc}(g)$. This means that $\pi_Q(\mathsf{Enc}(f)) = \pi_Q(\mathsf{Enc}(g))$, which implies that $\mathsf{Dec}_Q(\pi_Q(\mathsf{Enc}(f))) = \mathsf{Dec}_Q(\pi_Q(\mathsf{Enc}(g)))$. Then $\mathsf{Dec}(\mathsf{Enc}(f)) = \mathsf{Dec}(\mathsf{Enc}(g))$ by derivation (2). Since $\pi_E = \mathsf{Dec} \circ \mathsf{Enc}$ by derivation (3), then $\pi_E(f) = \pi_E(g)$. Then $f \approx_E g$. Since f and g were arbitrary, then (Σ, E) is complete with respect to $[\![-]\!]_\Sigma$. □

G.2 Proof of Theorem 5.2

Proof. First it must be shown that for each $f \in P(\Gamma)$, there exists a $g \in P(\Sigma)$ such that $f \approx_E g$. The proof follows by structural induction on $P(\Gamma)$.

- **Identity**. Assume that $f = 1_n$. Since $P(\Sigma)$ is a subcategory of $P(\Gamma)$, then $f \in P(\Sigma)$. Since $(\approx_E)$ is reflexive, then $f \approx_E f$.
- **Symmetries**. Assume that $f = \sigma$. Since $P(\Sigma)$ is a subcategory of $P(\Gamma)$, then $f \in P(\Sigma)$. Since $(\approx_E)$ is reflexive, then $f \approx_E f$.
- **Generators**. Assume that $f = x$ for some $x \in \Gamma$. Then by assumption, there exists some $g \in P(\Sigma)$ such that $f \approx_E g$.
- **Sequential Composition**. Assume that $f = b \circ a$ for $a : n \to s$ and $b : s \to m$. Then by the inductive hypothesis, there exists some $g \in P(\Sigma)(n,s)$ and $h \in P(\Sigma)(s,m)$ such that $a \approx_E g$ and $b \approx_E h$. Then $f \approx_E h \circ a \approx_E h \circ g$. Then $f \approx_E h \circ g$ by the transitivity of $(\approx_E)$. Moreover, $h \circ g \in P(\Sigma)(n,m)$.

- **Parallel Composition**. Assume that $f = a \boxtimes b$ for $a : n \to m$ and $b : s \to t$. Then by the inductive hypothesis, there exists some $g \in P(\Sigma)(n,m)$ and $h \in P(\Sigma)(s,t)$ such that $a \approx_E g$ and $b \approx_E h$. Then $f \approx_E g \otimes b \approx_E g \otimes h$. Then $f \approx_E g \otimes h$ by the transitivity of $(\approx_E)$. Moreover, $g \otimes h \in P(\Sigma)(n+s, m+t)$.

Then for all $f \in P(\Gamma)$, there exists a $g \in P(\Sigma)$ such that $f \approx_E g$. It remains to be shown that (Γ, E) is complete with respect to $[\![-]\!]$. Let $f \in P(\Gamma)(n,m)$ and $g \in P(\Gamma)(n,m)$ with $[\![f]\!] = [\![g]\!]$. By the first result, there exists some $h \in P(\Sigma)(n,m)$ and $k \in P(\Gamma)(n,m)$ such that $f \approx_E h$ and $g \approx_E k$. Since E is sound with respect to E, then $[\![f]\!] = [\![h]\!]$ and $[\![g]\!] = [\![k]\!]$. Then $[\![h]\!] = [\![f]\!] = [\![g]\!] = [\![k]\!]$. Since (Σ, E) is complete with respect to $[\![-]\!]$, then $h \approx_E k$. Since $(\approx_E)$ is transitive, then $f \approx_E g$. Since f and g were arbitrary, then (Γ, E) is complete with respect to $[\![-]\!]$. □

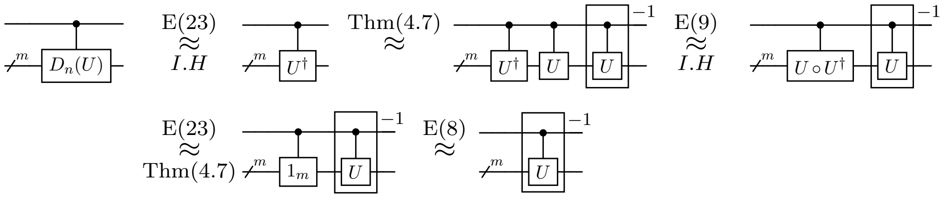
G.3 Proof of Lemma 5.3

Proof. Let $U \in \mathrm{Mor}(\mathbf{Core}/E)$. Then there exists some $V \in \mathrm{Mor}(\mathbf{Core})$ such that $\pi_E(V) = U$. Then there exists some $n \in \mathbb{N}$ such that $V \in \mathrm{Mor}(\mathcal{D}_n)$. Then ─●─ $\odot V \in \mathcal{G}_{n+1}$ by definition of the gate set. It follows that $C(U) = C(\pi(V)) = \pi($ ─●─ $\odot V) \in \mathrm{Mor}(\mathbf{Core}/E)$. Since U was arbitrary, then $C(U) \in \mathrm{Mor}(\mathbf{Core}/E)$ for all $U \in \mathrm{Mor}(\mathbf{Core}/E)$. In conclusion, $C : \mathbf{HQC}/E \to \mathbf{HQC}/E$ restricts to $\mathbf{Core}/E$. □

G.4 Proof of Lemma 5.4

Proof. For each $n \in \mathbb{N}$, let $D_n : \mathbf{Core}[n] \to \mathbf{Core}[n]$ denote the unique prop functor such that $D_n \circ i = \ddagger \circ i$. The proof follows by induction on n.

- **Base Case**. Let $g \in \Sigma^0_{\mathbf{Core}}$. Then by definition, $D_0(g) = g^\dagger$. Since g was arbitrary, then $D_0 \circ i = \dagger \circ i$. Then by uniqueness, $D_0(U) = U^\dagger$ for all $U \in \mathrm{Mor}(\mathbf{Core}[0])$. Then by reflexivity, $D_0(U) \approx_E U^\dagger$ for all $U \in \mathrm{Mor}(\mathbf{Core}[n])$.
- **Inductive Hypothesis**. For some $n \in \mathbb{N}$, if $U \in \mathrm{Mor}(\mathbf{Core}[n])$, then $D_0(U) \approx_E U^\dagger$.
- **Inductive Step**. Assume that for an $n \in \mathbb{N}$, if $U \in \mathrm{Mor}(\mathbf{Core}[n])$, then $D_n(U) \approx_E U^\dagger$. Let $g \in \Sigma^{n+1}_{\mathbf{Core}}$. If $g \in \Sigma^n_{\mathbf{Core}}$ as well, then $D_{n+1}(U) = D_n(U) \approx_E g$ by the inductive hypothesis. Assume instead that $g \notin \Sigma^n_{\mathbf{Core}}$. Then there exists some $U \in \mathrm{Mor}(\mathbf{Core}[n])$ such that $g =$ ─●─ $\odot D_n(U)$. Then by the inductive hypothesis, $D_n(U) \approx_E U^\dagger$. Then the following derivation holds.

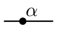


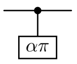
In either case, $D_{n+1}(g) \approx_E g^\dagger$. Since g was arbitrary, then $D_{n+1} \circ i = \dagger \circ i$. Then by uniqueness, $D_{n+1}(U) \approx_E U^\dagger$ for all $U \in \mathrm{Mor}(\mathbf{Core}[n])$. Then the inductive step holds.

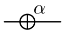
Then by the principle of induction, for each $n \in \mathbb{N}$, if $U \in \mathrm{Mor}(\mathbf{Core}[n])$, then $D_n(U) \approx_E U^\dagger$. Then let $U \in \mathrm{Mor}(\mathbf{Core})$. There there exists some $n \in \mathbb{N}$ such that $U \in \mathrm{Mor}(\mathbf{Core}[n])$. Then $U^\ddagger = D_n(U) \approx_E U^\dagger$. Since U was arbitrary, then $U^\ddagger \approx_E U^\dagger$ for all $U \in \mathrm{Mor}(\mathbf{Core})$. □

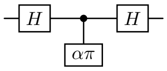
G.5 Proof of Lemma 5.5

Proof. The proof follows by induction.

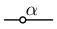
- **Base Case**. Let $g \in \Sigma^0_{\mathbf{Core}}$. There are six cases to consider.
  1. Let $g = \bullet^{\alpha}$. Then $[\![\mathsf{Enc}(g)]\!]_C = \left[\!\!\left[\boxed{\alpha\pi} \right]\!\!\right]_C = e^{i\alpha\pi} = \exp(\alpha \operatorname{Log}(-1)) = [\![g]\!]_H$.
  2. Let $g = -\boxed{H}-$. Then $[\![\mathsf{Enc}(g)]\!]_C = \left[\!\!\left[-\boxed{H}- \right]\!\!\right]_C = \frac{1}{\sqrt{2}}\left[\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right] = [\![g]\!]_H$.
  3. Let $g =$  . Recall that $\operatorname{Log}(Z) = i\pi\,|1\rangle\langle 1|$. Then the following equation holds.

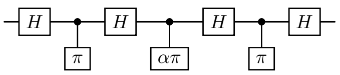
     $$[\![\mathsf{Enc}(g)]\!]_C = \left[\!\!\left[$$  $$\right]\!\!\right]_C = |0\rangle\langle 0| \otimes \mathbb{I}_1 + |1\rangle\langle 1| \otimes e^{i\alpha\pi} = \exp(i\alpha\pi\,|1\rangle\langle 1|) = [\![g]\!]_H$$

  4. Let $g =$  . Recall that $HZH = X$. Then the following equation holds

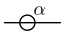
     $$[\![\mathsf{Enc}(g)]\!]_C = \left[\!\!\left[$$  $$\right]\!\!\right]_C$$

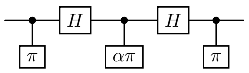
     $$\begin{aligned} &= H\exp(\alpha \operatorname{Log}(Z))H && \text{(by case (3))}\\ &= \exp(\alpha H \operatorname{Log}(Z) H) && \text{(by Eq. (2))}\\ &= \exp(\alpha \operatorname{Log}(HZH)) && \text{(by Eq. (2))}\\ &= \exp(\alpha \operatorname{Log}(X)) = [\![g]\!]_H \end{aligned}$$

  5. Let $g =$  . Recall that $XZX = -Z$. Then the following equation holds.

     $$[\![\mathsf{Enc}(g)]\!]_C = \left[\!\!\left[$$  $$\right]\!\!\right]_C$$

     $$\begin{aligned} &= \exp(\operatorname{Log}(X))\exp(\alpha \operatorname{Log}(Z))\exp(\operatorname{Log}(X)) && \text{(by cases (3) and (4))}\\ &= X\exp(\alpha \operatorname{Log}(Z))X &&\\ &= \exp(\alpha X \operatorname{Log}(Z) X) && \text{(by Eq. (2))}\\ &= \exp(\alpha \operatorname{Log}(XZX)) && \text{(by Eq. (2))}\\ &= \exp(\alpha \operatorname{Log}(-Z)) = [\![g]\!]_H \end{aligned}$$

  6. Let $g =$  . Recall that $XZX = -Z$. Then the following equation holds.

     $$[\![\mathsf{Enc}(g)]\!]_C = \left[\!\!\left[$$  $$\right]\!\!\right]_C$$

     $$\begin{aligned} &= \exp(\operatorname{Log}(Z))\exp(\alpha \operatorname{Log}(X))\exp(\operatorname{Log}(Z)) && \text{(by cases (3) and (4))}\\ &= Z\exp(\alpha \operatorname{Log}(X))Z &&\\ &= \exp(\alpha Z \operatorname{Log}(X) Z) && \text{(by Eq. (2))}\\ &= \exp(\alpha \operatorname{Log}(ZXZ)) && \text{(by Eq. (2))}\\ &= \exp(\alpha \operatorname{Log}(-X)) = [\![g]\!]_H \end{aligned}$$

  Since $g \in \Sigma^0_{\mathbf{Core}}$ was arbitrary, then $[\![\mathsf{Enc}(g)]\!]_C = [\![g]\!]_H$ for all $g \in \Sigma^0_{\mathbf{Core}}$.
- **Inductive Hypothesis**. For some $n \in \mathbb{N}$, if $g \in \Sigma^n_{\mathbf{Core}}$, then $[\![\mathsf{Enc}(g)]\!]_C = [\![g]\!]_H$.

- **Inductive Step**. Assume that the inductive hypothesis holds for some $n \in \mathbb{N}$ and let $g \in \Sigma^{n+1}_{\mathbf{Core}}$. If $g \in \Sigma^{n}_{\mathbf{Core}}$ as well, then $[\![\mathsf{Enc}(g)]\!]_C = [\![g]\!]_H$ by the inductive hypothesis. Assume instead that $g \in \Sigma^{n+1}_{\mathbf{Core}} \setminus \Sigma^{n}_{\mathbf{Core}}$. Then there exists some $U \in \mathrm{Mor}(\mathbf{Core}[n])$ such that $g = -\!\bullet\!- \odot U$. Then by the inductive hypothesis, since $[\![\mathsf{Enc}(-)]\!]_C$ and $[\![-]\!]_H$ agree on all generators, then $[\![\mathsf{Enc}(U)]\!]_C = [\![U]\!]_H$. Then by Theorem 3.2, the following holds.

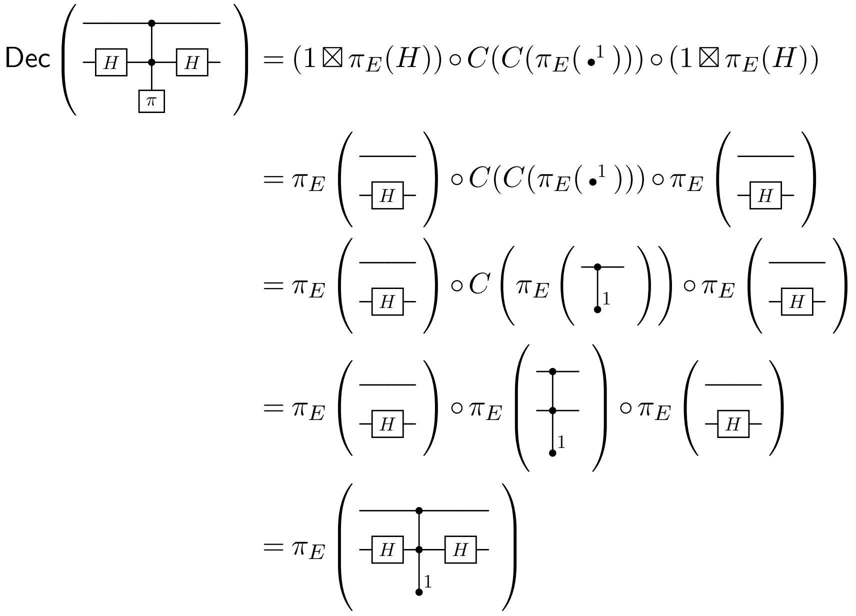
$$[\![g]\!]_H = Z \odot [\![U]\!]_H = Z \odot [\![\mathsf{Enc}(U)]\!]_C = |0\rangle\langle 0| \otimes \mathbb{I}_{2^n} + |1\rangle\langle 1| \otimes [\![\mathsf{Enc}(U)]\!]_C = [\![\mathsf{Enc}(g)]\!]_C$$

  In either case, $[\![g]\!]_H = [\![\mathsf{Enc}(g)]\!]_C$. Then the inductive step holds.

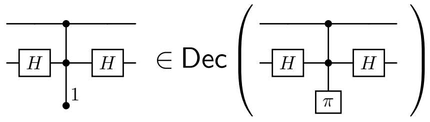
Then by the principle of induction, $[\![\mathsf{Enc}(g)]\!]_H = [\![g]\!]_C$ for each $g \in \Sigma_{\mathbf{Core}}$. □

G.6 Proof of Lemma 5.6

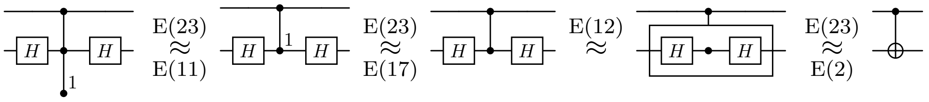
Proof. By Theorem 4.10, the following theorem holds.



In other words, the following equation holds.



Since $H = H^\dagger$, then the following derivation also holds.

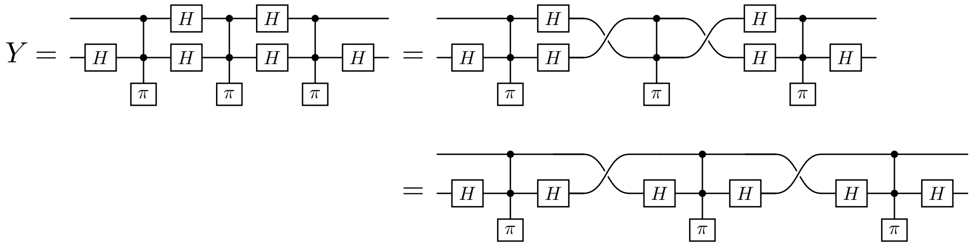


This completes the proof. □

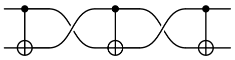
G.7 Proof of Lemma 5.7

Proof. Let $(X,Y) \in Q$. There are 9 cases to consider.

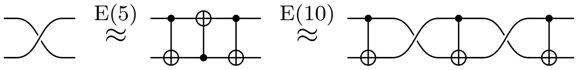
1. Assume that (X,Y) is rule Q(1). Clearly $\bullet^2 \in \mathsf{Dec}(X)$ and $0 \in \mathsf{Dec}(Y)$. It then follows by E(7) that $\bullet^2 \approx_E 0$.
2. Assume that (X,Y) is rule Q(2). Clearly $\overset{\alpha_1/\pi}{\bullet}\ \overset{\alpha_2/\pi}{\bullet} \in \mathsf{Dec}(X)$ and $\overset{(\alpha_1+\alpha_2)/\pi}{\bullet} \in \mathsf{Dec}(Y)$. It then follows by E(18) that $\overset{\alpha_1/\pi}{\bullet}\ \overset{\alpha_2/\pi}{\bullet} \approx_E \overset{\alpha_1/\pi+\alpha_2/\pi}{\bullet} = \overset{(\alpha_1+\alpha_2)/\pi}{\bullet}$.
3. Assume that (X,Y) is rule Q(3). Clearly $\sigma \in \mathsf{Dec}(X)$. Since **CQC** is a controlled prop category, then the following equation holds.



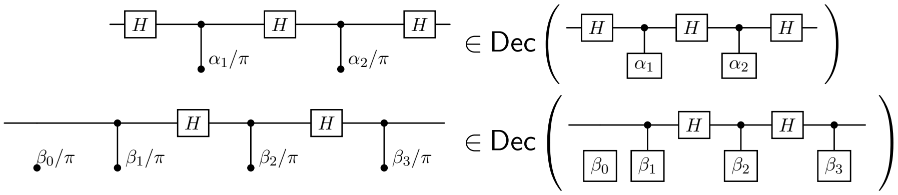
Then by Lemma 5.6, the following equation also holds.

 $\in \mathsf{Dec}(Y)$

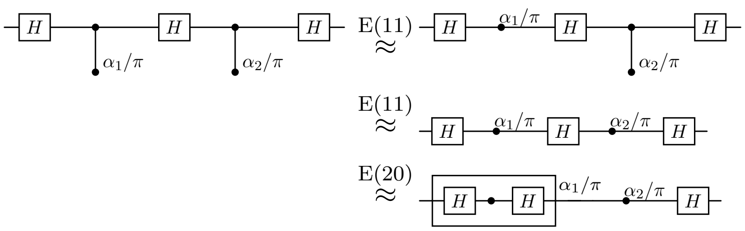
Moreover, the following derivation holds.

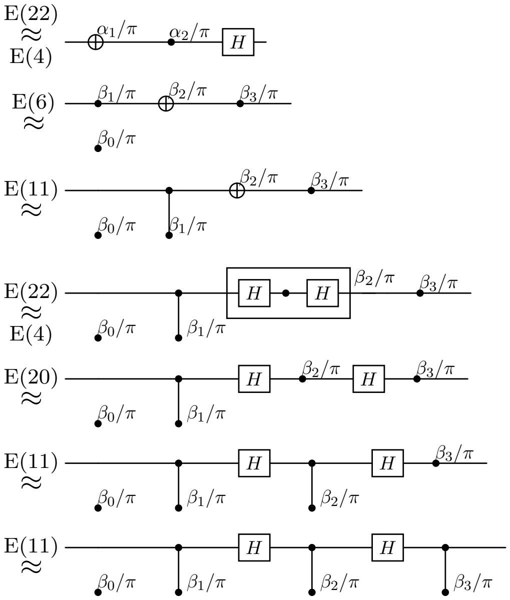


4. Assume that (X,Y) is rule Q(4). Clearly $-\boxed{H}-\boxed{H}- \in \mathsf{Dec}(X)$ and $— \in \mathsf{Dec}(Y)$. Since $H = H^\dagger$, then $-\boxed{H}-\boxed{H}- \approx_E —$ by Theorem 4.7.
5. Assume that (X,Y) is rule Q(5). Then $\alpha_1 \in \mathbb{R}$, $\alpha_2 \in \mathbb{R}$, and $(\beta_0,\beta_1,\beta_2,\beta_2) = \mathsf{Euler}(\alpha_1,\alpha_2)$. Clearly the following equations hold (see Section G.6).

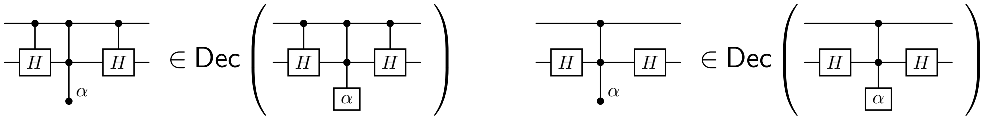


Then the following derivation holds since $H = H^\dagger$.

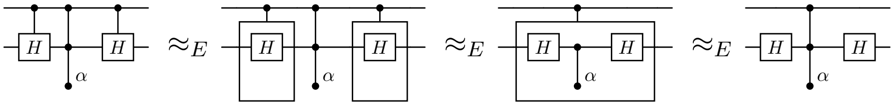




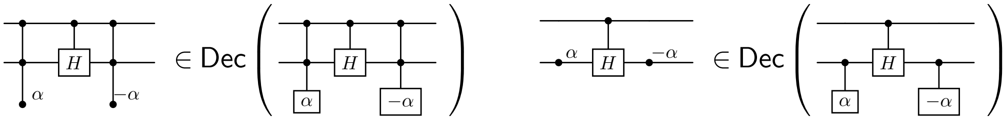
6. Assume that (X, Y) is rule Q(6). Clearly the following equations hold (see Section G.6).



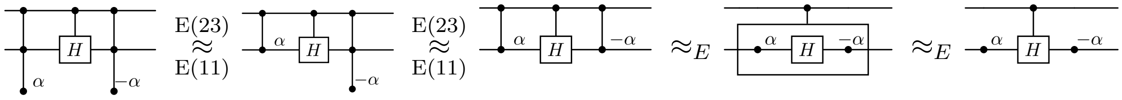
Since $C(-)$ is a conjugated control functor and $(H \boxtimes 0)^\dagger = H^\dagger \boxtimes 0^\dagger = H \boxtimes 0$, then the following derivation holds.



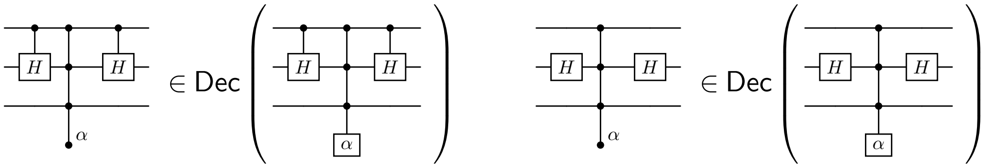
7. Assume that (X, Y) is rule Q(7). Clearly the following equations hold (see Section G.6).



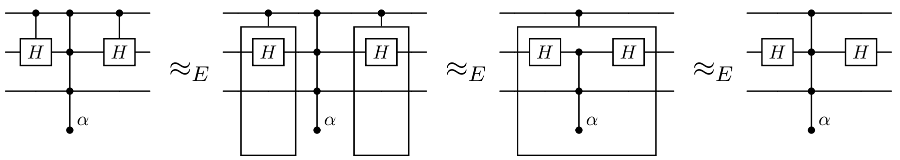
Since $C(-)$ is a conjugated control functor and $(U \uparrow \alpha)^\dagger = U \uparrow (-\alpha)$ for each unitary U, then the following derivation holds.



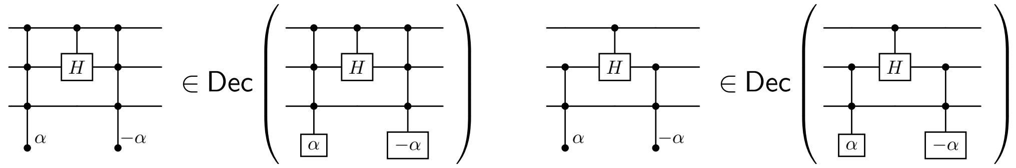
8. Assume that (X, Y) is rule Q(8). Clearly the following equations hold (see Section G.6).



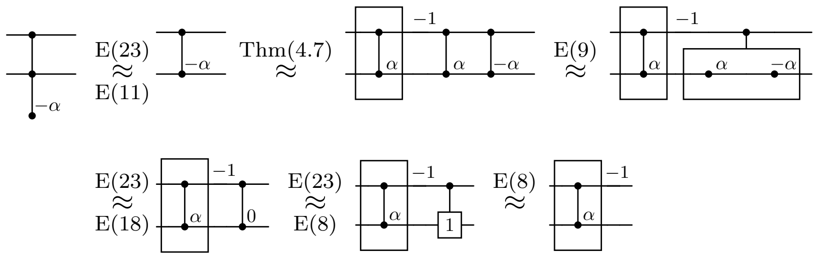
Since $C(-)$ is a conjugated control functor and $(H \boxtimes 1 \boxtimes 0)^\dagger = H^\dagger \boxtimes 1^\dagger \boxtimes 0^\dagger = H \boxtimes 1 \boxtimes 0$, then the following derivation holds.



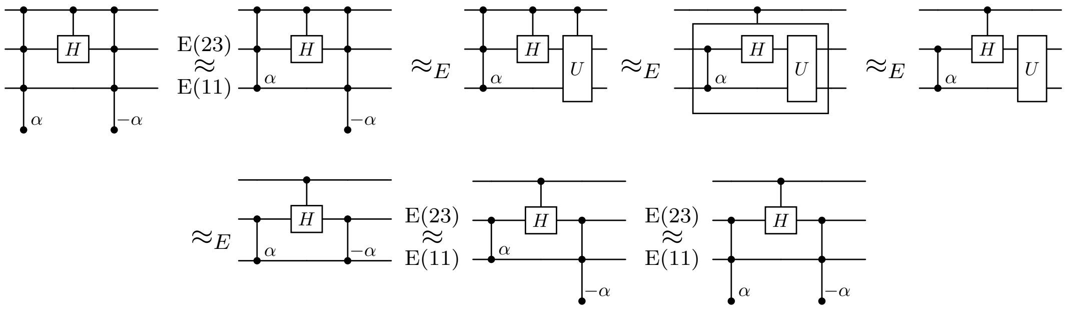
9. Assume that (X,Y) is rule Q(9). Clearly the following equations hold (see Section G.6).



As in the previous proofs, this case will be handled using the property that $C(-)$ is a conjugated control functor. First, it must be shown that the third gate on the left-hand side is the adjoint to the first gate on the left-hand side.



Let U denote the final string in this derivation. Since $C(-)$ is a conjugated control functor and $C(V)^\dagger = C(V)\uparrow(-1)$ for each unitary V, then the following derivation holds.



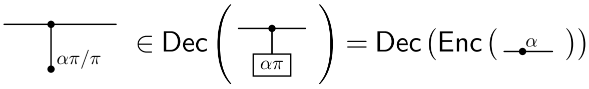
In each case, there exists a $U \in \mathsf{Dec}(X)$ and $V \in \mathsf{Dec}(Y)$ such that $U \approx_E V$. Since (X,Y) was arbitrary, then this completes the proof. □

G.8 Proof of Lemma 5.8

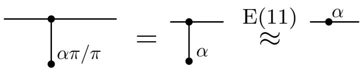
Proof. The proof follows by induction.

- **Base Case**. Assume that $g \in \Sigma^0_{\mathbf{Core}}$. There are six cases to consider.

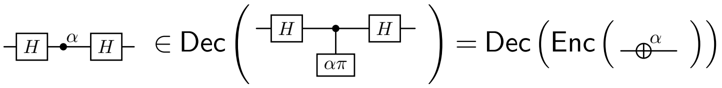
1. Assume that $g = -\boxed{H}-$. Then by definition $-\boxed{H}- \in \mathsf{Dec}(-\boxed{H}-) = \mathsf{Dec}(\mathsf{Enc}(-\boxed{H}-))$. Since $(\approx_E)$ is reflexive and $g \in \mathsf{Dec}(\mathsf{Enc}(g))$, then there exists some $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $g \approx_E U$.
2. Assume that $g = \bullet^{\alpha}$. Then by definition $\bullet^{\alpha\pi/\pi} \in \mathsf{Dec}(\boxed{\alpha\pi}) = \mathsf{Dec}(\mathsf{Enc}(\bullet^{\alpha}))$. Since $\alpha\pi/\pi = \pi$, then $g \in \mathsf{Dec}(\mathsf{Enc}(g))$. Since $(\approx_E)$ is also reflexive, then there exists some $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $g \approx_E U$.
3. Assume that $g = -\bullet^{\alpha}-$. Then the following equation holds (see Section G.6).



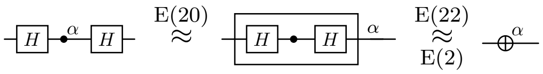
Then the following derivation holds.



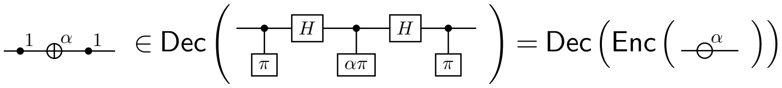
4. Assume that $g = -\oplus^{\alpha}-$. It follows from case (3) that following equation holds.



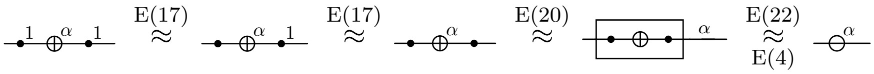
Then the following derivation holds.



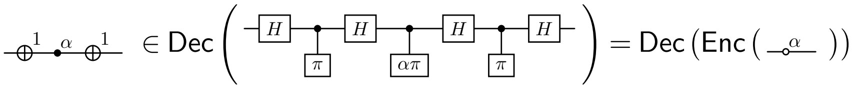
5. Assume that $g = -\ominus^{\alpha}-$. It follows from cases (3–4) that following equation holds.



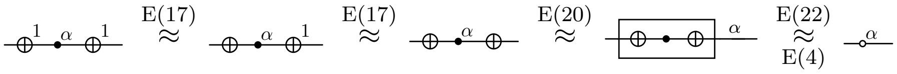
Then the following derivation holds.



6. Assume that $g = -\circ^{\alpha}-$. It follows from cases (3–4) that following equation holds.



Then the following derivation holds.

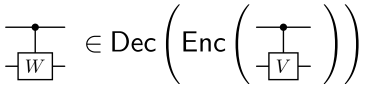


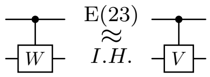
In each case, there exists a $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $g \approx_E U$.

- **Inductive Hypothesis**. For each $n \in \mathbb{N}$, if $g \in \Sigma^n_{\mathbf{Core}}$, then there exists some circuit $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $g \approx_E U$.
- **Inductive Step**. Assume that the inductive hypothesis holds for some $n \in \mathbb{N}$ and let $g \in \Sigma^{n+1}_{\mathbf{Core}}$. If $g \in \Sigma^n_{\mathbf{Core}}$ as well, then there exists some $U \in \mathsf{Dec}(\mathsf{Enc}(U))$ such that $g \approx_E U$ by the inductive hypothesis. Assume instead that $g \in \Sigma^{n+1}_{\mathbf{Core}} \setminus \Sigma^n_{\mathbf{Core}}$. Then there exists some $V \in \mathrm{Mor}(\mathbf{Core}[n])$ such that $g =$ $\odot V$. Then by the definitions of $\mathsf{Enc}(-)$ and $\mathsf{Dec}(-)$, the following equation holds.

  $$\mathsf{Dec}(\mathsf{Enc}(g)) = \mathsf{Dec}(C(\mathsf{Enc}(V))) = C(\mathsf{Dec}(\mathsf{Enc}(V)))$$

  Then by the inductive hypothesis, there exists some $W \in \mathsf{Dec}(\mathsf{Enc}(V))$ such that $V \approx_E W$. Then the following equations hold (see Section G.6).

  Then there exists some $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $g \approx_E U$

Then by the principle of inductive, for each $g \in \Sigma_{\mathbf{Core}}$, there exists some $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $g \approx_E U$. □

G.9 Proof of Theorem 5.9

Proof. By Theorem 4.4, $(\Sigma_{\mathbf{Core}}, E)$ is sound with respect to $[\![-]\!]_H$. By Lemma 5.5, if $g \in \Sigma_{\mathbf{Core}}$, then $[\![\mathsf{Enc}(g)]\!]_C = [\![g]\!]_H$. By Lemma 5.7, if $(X,Y) \in Q$, then there exists some $X^* \in \mathsf{Dec}(X)$ and $Y^* \in \mathsf{Dec}(Y)$ such that $X^* \approx_E Y^*$. By Lemma 5.8, if $g \in \Sigma_{\mathbf{Core}}$, then there exists some $U \in \mathsf{Dec}(\mathsf{Enc}(g))$ such that $g \approx_E U$. Then by Theorem 5.1, $(\Sigma_{\mathbf{Core}}, E)$ is complete with respect to the semantic interpretation $[\![-]\!]_H$. □

H Circuit Normalization Routines

This section introduces the algorithms used in Section 5. The first sub-section establishes the correctness of $\mathsf{Drop}(-,-)$ along with its relevant helper functions. The second sub-section establishes the correctness of $\mathsf{Expand}(-,-)$ along with its relevant helper functions. Both cases rely on an oracle function $\mathsf{Diag}(U) = (P, \Lambda)$ which returns a diagonalization of U. In particular, if $U \in \mathbf{Core}(n,n)$ and $(P,\Lambda) = \mathsf{Diag}(U)$, then $P \in \mathbf{Core}(n,n)$ and $\Lambda \in \mathbf{Core}(n,n)$ with Λ in diagonal form and $[\![U]\!]_H = [\![P^\dagger \circ \Lambda \circ P]\!]_H$. We note that $\mathsf{Diag}(-)$ need not be computable, and is best thought of as a choice function. For the interested reader, the underlying choices are elucidated in the proofs of the following theorems.

Remark H.1. In this section, we think of each diagonal form Λ as a sequence of lambda generators. This means that the prefixes of Λ are also sequences of lambda generators. We write $|\Lambda|$ for the number of lambda generators in Λ. If $\Lambda \in \mathbf{Core}(n,n)$ is the prefix of a diagonal form, then $|\Lambda| \in \{0, 1, \ldots, 2^n\}$.

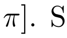
Proposition H.2 ([2, 4])**.** *Let $\mathcal{C}$ be a prop category and $F : \mathcal{C} \to$ **Unitary** a symmetric monoidal functor such that $\mathrm{Ob}(F)(1) = \mathbb{C}^2$. Then F is full if and only if the following conditions hold.*

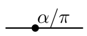
1. *For each $\alpha \in (-\pi, \pi]$, there exists a $U \in \mathcal{C}(0,0)$ such that $F(U) = e^{i\alpha}$.*

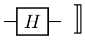
2. *For each* $\alpha \in (-\pi,\pi]$*, there exists a* $U \in \mathcal{C}(1,1)$ *such that* $F(U) = \exp(i\,|1\rangle\langle 1|\,\alpha)$.
3. *There exists a* $U \in \mathcal{C}(1,1)$ *such that* $F(U) = H$.
4. *There exists a* $U \in \mathcal{C}(2,2)$ *such that* $F(U) = |0\rangle\langle 0| \otimes \mathbb{I}_2 + |1\rangle\langle 1| \otimes X$.

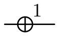
Lemma H.3. *The functor* $\llbracket - \rrbracket_H$ *is full when restricted to* **Core***.*

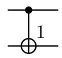
Proof. By construction, $\llbracket - \rrbracket_H$ is a prop functor such that $\mathrm{Ob}(\llbracket - \rrbracket_H)(1) = \mathbb{C}^2$. Then to show that $\llbracket - \rrbracket_H$ is full, it suffices to show that the conditions of Proposition H.2 hold.

1. Let $\alpha \in (-\pi,\pi]$. Since $\mathrm{Log}(\llbracket \bullet \rrbracket_H) = \mathrm{Log}(e^{i\pi}) = i\pi$, then $\llbracket \bullet^{\alpha/\pi} \rrbracket_H = e^{i(\alpha/\pi)\pi} = e^{i\alpha}$. Since α was arbitrary, then for each $\alpha \in (-\pi,\pi]$, there exists $U \in \mathbf{Core}(0,0)$ such that $\llbracket U \rrbracket_H = e^{i\alpha}$.
2. Let $\alpha \in (-\pi,\pi]$. Since $\mathrm{Log}(\llbracket$  $\rrbracket_H) = i\,|1\rangle\langle 1|\,\pi$, then the following equation holds.

   $\llbracket$  $\rrbracket_H$ $= \exp(i(\alpha/\pi)\,|1\rangle\langle 1|\,\pi) = \exp(i\,|1\rangle\langle 1|\,\alpha)$

   Since α was arbitrary, then for each $\alpha \in (-\pi,\pi]$, there exists $U \in \mathbf{Core}(1,1)$ such that $\llbracket U \rrbracket_H = \exp(i\,|1\rangle\langle 1|\,\alpha)$.
3. Since $\llbracket$  $\rrbracket_H = H$, then there exists a $U \in \mathbf{Core}(1,1)$ such that $\llbracket U \rrbracket_H = H$.

4. Clearly $\llbracket$  $\rrbracket_H = X^1 = X$. Then by Theorem 3.2, the following equation holds.

   $\llbracket$  $\rrbracket_H$ $= Z \odot X = |0\rangle\langle 0| \otimes \mathbb{I}_2 + |1\rangle\langle 1| \otimes X$

   Then there exists a $U \in \mathbf{Core}(2,2)$ such that $\llbracket U \rrbracket = I \otimes X$.

Then $\llbracket - \rrbracket_H$ is full by Proposition H.2. □

Theorem H.4. *There exists a function* $\mathsf{Diag} : \mathrm{Mor}(\mathbf{HQC}) \to \mathrm{Mor}(\mathbf{Core}) \times \mathrm{Mor}(\mathbf{Core})$ *such that for each* $U \in \mathrm{Mor}(\mathbf{HQC})$*, if* $(P,\Lambda) = \mathsf{Diag}(U)$*, then* $\llbracket U \rrbracket_H = \llbracket P^\dagger \circ \Lambda \circ P \rrbracket_H$ *with* Λ *in diagonal form. If* $U \in \mathrm{Mor}(\mathbf{Core})$*, then* $U \approx_E P^\dagger \circ \Lambda \circ P$*.*

Proof. Let $U \in \mathbf{HQC}(n,n)$. Since $\llbracket U \rrbracket_H$ is unitary (and therefore normal), then by the spectral decomposition theorem there exists a unitary matrix $M \in \mathbf{Unitary}(2^n,2^n)$ and a diagonal matrix $D \in \mathbf{Unitary}(2^n,2^n)$ such that $\llbracket U \rrbracket_H = M^\dagger D M$. Since $\llbracket - \rrbracket_H$ is full by Lemma H.3, there exists a choice of circuit $P \in \mathbf{Core}(n,n)$ such that $\llbracket P \rrbracket_H = M$. Since D is diagonal, then for each choice of bijection $f : \{1,2,\ldots,2^n\} \to \{0,1\}^n$, there exists a unique diagonal form $\Lambda \in \mathbf{Core}(n,n)$ such that $\llbracket \Lambda \rrbracket_H = D$. Then there exists some pair of circuits $(P,\Lambda) \in \mathrm{Mor}(\mathbf{Core}) \times \mathrm{Mor}(\mathbf{Core})$ such that $\llbracket U \rrbracket_H = \llbracket P^\dagger \circ \Lambda \circ P \rrbracket_H$. Since U was arbitrary, then for each $U \in \mathrm{Mor}(\mathbf{HQC})$, there exists some $(P,\Lambda) \in \mathrm{Mor}(\mathbf{Core}) \times \mathrm{Mor}(\mathbf{Core})$ such that $\llbracket U \rrbracket_H = \llbracket P^\dagger \circ \Lambda \circ P \rrbracket_H$ with Λ in diagonal form. Then $\mathsf{Diag} : \mathrm{Mor}(\mathbf{HQC}) \to \mathrm{Mor}(\mathbf{Core}) \times \mathrm{Mor}(\mathbf{Core})$ exists. Next, assume that $U \in \mathbf{Core}(n,n)$ and let $(P,\Lambda) = \mathsf{Diag}(U)$. Then by assumption $\llbracket U \rrbracket_H = \llbracket P^\dagger \circ \Lambda \circ P \rrbracket_H$. Since $P \in \mathbf{Core}(n,n)$ and $\Lambda \in \mathbf{Core}(n,n)$, then $P^\dagger \circ \Lambda \circ P \in \mathbf{Core}(n,n)$. Since $(\Sigma_{\mathbf{Core}}, E)$ is complete with respect to the semantic interpretation $\llbracket - \rrbracket_H$ by Theorem 5.9, then $U \approx_E P^\dagger \circ \Lambda \circ P$. Since U was arbitrary, then this completes the proof. □

Algorithm 1 $\mathsf{DiagDrop}(\Lambda, \alpha)$

```
**Input:** $\Lambda \in \mathbf{HQC}(k,k)$ in diagonal form and $\alpha \in \mathbb{R}$.
**Output:** A circuit $U \in \mathbf{Core}(k,k)$ such that $U \approx_E \Lambda \uparrow \alpha$.
  if $|\Lambda| = 0$ then return $1_k$
  let $\Lambda' \circ \lambda(x,\beta) \leftarrow \Lambda$
  let $U \leftarrow \mathsf{DiagDrop}(\Lambda', \alpha)$
  return $U \circ \lambda(x, \alpha\beta)$
```

Algorithm 2 $\mathsf{Drop}_{n+1}(U, \alpha)$

```
**Input:** $U \in \mathbf{CExt}[n](k,k)$, and $\alpha \in \mathbb{R}$.
**Output:** A circuit $U \in \mathbf{Core}(k,k)$ such that $U \approx_E U \uparrow \alpha$.
  let $V \leftarrow \mathsf{Reduce}_n(U)$
  let $(P, \Lambda) \leftarrow \mathsf{Diag}(V)$
  let $W \leftarrow \mathsf{DiagDrop}(\Lambda, \alpha)$
  return $P^{\ddagger} \circ W \circ P$
```

H.1 The Drop Routine

The special case of diagonal circuits is handled first by Algorithm 1. The algorithm iterates over each lambda generator in the diagonal form Λ, and then performs the necessary rewrites to reduce the circuit $(\Lambda \uparrow \alpha)$ to **Core**. This is then used by Algorithm 2 to handle all powers in $\mathbf{CExt}[n]$, through subcircuit diagonalization. Of course, the correctness of $\mathsf{Drop}_{n+1}(-,-)$ relies on the correctness of $\mathsf{Reduce}_n(-)$.

Lemma H.5. *If* $\Lambda \in \mathbf{Core}(k,k)$ *in diagonal form and* $\alpha \in \mathbb{R}$*, then* $\mathsf{DiagDrop}(-,-)$ *terminates when applied to* (Λ, α) *with* $\mathsf{DiagDrop}(\Lambda, \alpha) \in \mathbf{Core}(k,k)$ *and* $(\Lambda \uparrow \alpha) \approx_E \mathsf{DiagDrop}(\Lambda, \alpha)$*.*

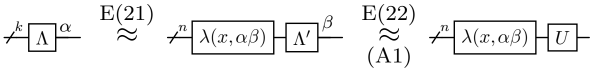
Proof. The proof follows by induction on $|\Lambda|$ where Λ is a prefix of a diagonal form.

- **Base Case**. If $|\Lambda| = 0$, then the first line is reached and 1_k is returned. In other words, $\mathsf{DiagDrop}(-,-)$ terminates when applied to (Λ, α) and $\mathsf{DiagDrop}(\Lambda, \alpha) = 1_k \in \mathbf{Core}(k,k)$. Since $|\Lambda| = 0$, then $\Lambda = 1_k$. Then $(\Lambda \uparrow \alpha) = (1_k \uparrow \alpha) \approx_E 1_k = \mathsf{DiagDrop}(\Lambda, \alpha)$ by E(19).
- **Inductive Hypothesis**. For some $\ell \in \mathbb{N}$, if Λ is a diagonal form prefix with $|\Lambda| = \ell$, then $\mathsf{DiagDrop}(-,-)$ terminates when applied to (Λ, α) with $\mathsf{DiagDrop}(\Lambda, \alpha) \in \mathbf{Core}(k,k)$ and $(\Lambda \uparrow \alpha) \approx_E \mathsf{DiagDrop}(\Lambda, \alpha)$.
- **Inductive Step**. Assume that for some $\ell \in \mathbb{N}$, if Λ is a diagonal form prefix with $|\Lambda| = \ell$, then $\mathsf{DiagDrop}(-,-)$ terminates when applied to (Λ, α) with $\mathsf{DiagDrop}(\Lambda, \alpha) \in \mathbf{Core}(k,k)$ and $(\Lambda \uparrow \alpha) \approx_E \mathsf{DiagDrop}(\Lambda, \alpha)$. Let Λ be a diagonal form prefix with $|\Lambda| = \ell + 1$. Since $|\Lambda| = \ell + 1 > 0$, then the if-condition on the first line fails, and the program continues to line two. Then after executing line two, $\lambda(x, \beta)$ is assigned to the last symbol in Λ and Λ' is assigned to the rest of Λ. This means that Λ' is also a prefix of a diagonal form with $|\Lambda'| = \ell$. Then by the the inductive hypothesis, the third line terminates with $U \leftarrow \mathsf{DiagDrop}(\Lambda', \alpha)$, $U \in \mathbf{Core}(k,k)$, and (A1) : $(\Lambda' \uparrow \alpha) \approx_E U$. Then the fourth line is reached, at which point $U \circ \lambda(x, \alpha\beta)$ is returned. In other words, $\mathsf{Diag}(-,-)$ terminates when applied to (Λ, α) and

Algorithm 3 $\mathsf{LambdaExpand}(x,\alpha,\Gamma)$

```
Input: $x \in \{0,1\}^n$, $\alpha \in (-\pi,\pi]$, and $\Gamma \in \mathbf{Core}(m,m)$ the prefix of a diagonal form.
Output: A circuit $U \in \mathbf{Core}(n+m,n+m)$ such that $\lambda(x,\alpha) \odot \Gamma \approx_E U$.
  if $|\Gamma| = 0$ then return $1_{n+m}$
  $\Gamma' \circ \lambda(y,\beta) \leftarrow \Gamma$
  $U \leftarrow \mathsf{LambdaExpand}(x,\alpha,\Gamma')$
  return $U \circ \lambda(xy,\alpha\beta/\pi)$
```

$\mathsf{DiagDrop}(\Lambda,\alpha) = U \circ \lambda(x,\alpha\beta) \in \mathbf{Core}(k,k)$. Moreover, the following derivation holds.

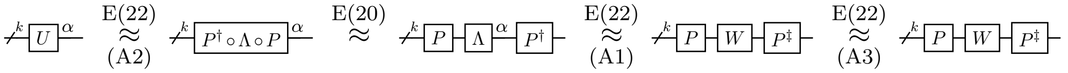


Then $(\Lambda \uparrow \alpha) \approx_E \mathsf{DiagDrop}(\Lambda,\alpha)$ and the inductive step holds.

It follows by the principle of induction that if $\Lambda \in \mathbf{Core}(k,k)$ is a diagonal form prefix and $\alpha \in \mathbb{R}$, then $\mathsf{DiagDrop}(-,-)$ terminates when applied to (Λ,α) with $\mathsf{DiagDrop}(\Lambda,\alpha) \in \mathbf{Core}(k,k)$ and $(\Lambda \uparrow \alpha) \approx_E \mathsf{DiagDrop}(\Lambda,\alpha)$. Since every diagonal form is a prefix of itself, then this completes the proof. □

Theorem H.6. *If $U \in \mathbf{CExt}[n](k,k)$, $\alpha \in \mathbb{R}$, and $\mathsf{Reduce}_n(-)$ terminates when applied to U, then $\mathsf{Drop}_{n+1}(-,-)$ terminates when applied to (U,α) with $\mathsf{Drop}_{n+1}(U,\alpha) \in \mathbf{Core}(k,k)$. Moreover, if $U \approx_E \mathsf{Reduce}_n(U)$, then $(U \uparrow \alpha) \approx_E \mathsf{Drop}_{n+1}(U,\alpha)$*

Proof. Let $U \in \mathbf{CExt}[n](k,k)$ and $\alpha \in \mathbb{R}$. Assume that $\mathsf{Reduce}_n(-)$ terminates when applied to U. Then by assumption, the first line terminates and $V \leftarrow \mathsf{Reduce}_n(U)$ with $V \in \mathbf{Core}(k,k)$. Then by Theorem H.4, the second line terminates and $(P,\Lambda) \leftarrow \mathsf{Diag}(V)$ with $P \in \mathbf{Core}(k,k)$ and $\Lambda \in \mathbf{Core}(k,k)$ in diagonal form with $V \approx_E P^\dagger \circ \Lambda \circ P$. Since Λ is in diagonal form, then by Lemma H.5 the third line also terminates and $W \leftarrow \mathsf{DiagDrop}(\Lambda,\alpha)$ with $W \in \mathbf{Core}(k,k)$ and $(\mathrm{A1}) : (\Lambda \uparrow \alpha) \approx_E W$. Then the fourth line is reached, at which point $P^\dagger \circ W \circ P$ is returned. In other words, $\mathsf{Drop}(-,-)$ terminates when applied to (U,α) and $\mathsf{Drop}(U,\alpha) = P^\ddagger \circ W \circ P$. Since $P^\ddagger \in \mathbf{Core}(k,k)$, then $\mathsf{Drop}(U,\alpha) \in \mathbf{Core}(k,k)$. Now assume that $U \approx_E \mathsf{Reduce}_n(U) = V$. Since $V \approx_E P^\dagger \circ \Lambda \circ P$ as well, then $(\mathrm{A2}) : U \approx_E P^\dagger \circ \Lambda \circ P$ by the transitivity of $(\approx_E)$. Then by Lemma 5.4, $(\mathrm{A3}) : P^\ddagger \approx_E P^\dagger$, and the following derivation holds.



In conclusion, $(U \uparrow \alpha) \approx_E P^\ddagger \circ W \circ P = \mathsf{Drop}(U,\alpha)$. □

H.2 The Expand Routine

First, Algorithm 3 is introduced to handle diagonal circuits controlled by lambda generators. This algorithm iterates over each lambda generator in the diagonal form Γ, and then performs the necessary rewrites to reduce the circuit $\lambda(x,\alpha) \odot \Gamma$ to **Core**. This is then used by Algorithm 4 to handle the slightly more general case of diagonal circuits controlled by diagonal circuits. This algorithm iterates over each lambda generator in the diagonal form Λ, and the performs the

Algorithm 4 $\mathsf{DiagExpand}(\Lambda,\Gamma)$

```
Input: $\Lambda \in \mathbf{Core}(n,n)$ the prefix of a diagonal form and $\Gamma \in \mathbf{Core}(m,m)$ in diagonal form.
Output: A circuit $U \in \mathbf{Core}(n+m,n+m)$ such that $\Lambda \odot \Gamma \approx_E U$.
  if $|\Lambda| = 0$ then return $1_{n+m}$
  $\Lambda' \circ \lambda(x,\alpha) \leftarrow \Lambda$
  $U \leftarrow \mathsf{DiagExpand}(\Lambda',\Gamma)$
  $V \leftarrow \mathsf{LambdaExpand}(x,\alpha,\Gamma)$
  return $U \circ V$
```

Algorithm 5 $\mathsf{Expand}_{n+1}(T)$

```
Input: $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $\mathrm{dom}(T) = k$, $|T| \geq 1$, and $T = T_1 \odot T'$.
Output: A circuit $U \in \mathbf{Core}(k,k)$ such that $T \approx_E U$.
  let $U \leftarrow \mathsf{Reduce}_n(T_1)$
  if $|T| = 1$ then return $U$
  let $(P,\Lambda) \leftarrow \mathsf{Diag}(U)$
  let $V \leftarrow \mathsf{Expand}_{n+1}(T')$
  let $(Q,\Gamma) \leftarrow \mathsf{Diag}(V)$
  let $W \leftarrow \mathsf{DiagExpand}(\Lambda,\Gamma)$
  return $(P^{\ddagger} \boxtimes Q^{\ddagger}) \circ W \circ (P \boxtimes Q)$
```

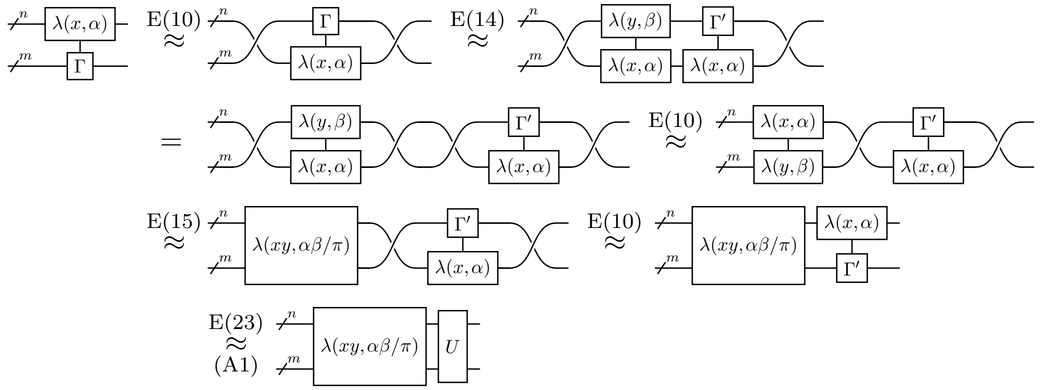
necessary rewrites to reduce the circuit $\Lambda \odot \Gamma$ to **Core**. This is then used by Algorithm 5 to handle all generalized controls in $\mathbf{CExt}[n]$, through subcircuit diagonalization. This algorithm iterates over each subcircuit in the control tower. Of course, the correctness of $\mathsf{Expand}_{n+1}(-)$ relies on the correctness of $\mathsf{Reduce}_n(-)$.

Lemma H.7. *If $x \in \{0,1\}^n$, $\alpha \in (-\pi,\pi]$, and Γ is in diagonal form, then $\mathsf{LambdaExpand}(-,-,-)$ terminates when applied to the tuple (x,α,Γ) with $\mathsf{LambdaExpand}(x,\alpha,\Gamma) \in \mathbf{Core}(n+m,n+m)$ and $\lambda(x,\alpha) \odot \Gamma \approx_E \mathsf{LambdaExpand}(x,\alpha,\Gamma)$ where $m = \mathrm{dom}(\Lambda)$.*

Proof. Let $x \in \{0,1\}^n$ and $\alpha \in (-\pi,\pi]$. The proof follows by induction on $|\Gamma|$ where Γ is a prefix of a diagonal form.

- **Base Case**. Let $\Gamma \in \mathbf{Core}(m,m)$. If $|\Gamma| = 0$, then the first line is reached and 1_{n+m} is returned. In other words, $\mathsf{LambdaExpand}(-,-,-)$ terminates when applied to (x,α,Γ) and $\mathsf{LambdaExpand}(x,\alpha,\Gamma) = 1_{n+m} \in \mathbf{Core}(n+m,n+m)$. Since $|\Gamma| = 0$, then $\Gamma = 1_m$. It follows by E(8) that $\lambda(x,\alpha) \odot \Gamma = \lambda(x,\alpha) \odot 1_m \approx_E 1_{n+m} = \mathsf{LambdaExpand}(x,\alpha,\Gamma)$.
- **Inductive Hypothesis**. For some $\ell \in \mathbb{N}$, if $\Gamma \in \mathbf{Core}(m,m)$ is a diagonal form prefix and $|\Gamma| = \ell$, then $\mathsf{LambdaExpand}(-,-,-)$ terminates when applied to (x,α,Γ) with $\mathsf{LambdaExpand}(x,\alpha,\Gamma) \in \mathbf{Core}(n+m,n+m)$ and $\lambda(x,\alpha) \odot \Gamma \approx_E \mathsf{LambdaExpand}(x,\alpha,\Gamma)$.
- **Inductive Step**. Assume that for some $\ell \in \mathbb{N}$, if $\Gamma \in \mathbf{Core}(m,m)$ is a diagonal form prefix and $|\Gamma| = \ell$, then $\mathsf{LambdaExpand}(-,-,-)$ terminates when applied to (x,α,Γ) with $\mathsf{LambdaExpand}(x,\alpha,\Gamma) \in \mathbf{Core}(n+m,n+m)$ and $\lambda(x,\alpha) \odot \Gamma \approx_E \mathsf{LambdaExpand}(x,\alpha,\Gamma)$. Let $\Gamma \in \mathbf{Core}(m,m)$ such that Γ is the prefix of a diagonal form with $|\Gamma| = \ell + 1$. Since $|\Gamma| = \ell + 1 > 0$, then the if-condition on the first line fails, and the program continues to line two. Then after executing line two, $\lambda(y,\beta)$ is assigned to the last symbol in Γ

and Γ' is assigned to the rest of Γ. This means that Γ' is a prefix of a diagonal form with $|\Gamma'| = \ell$ and $|y| = m$. Then by the inductive hypothesis, the third line terminates and $U \leftarrow \mathsf{LambdaExpand}(x,\alpha,\Gamma')$ with $U \in \mathbf{Core}(n+m,n+m)$ and $(\text{A1}) : \lambda(x,\alpha) \odot \Gamma' \approx_E U$. Then the fourth line is reached, at which point $U \circ \lambda(xy,\alpha\beta/\pi)$ is returned. Since $|x| = n$ and $|y| = m$, then $|xy| = n+m$, and therefore $\lambda(xy,\alpha\beta/\pi) \in \mathbf{Core}(n+m,n+m)$. Since $U \circ \lambda(xy,\alpha\beta/\pi)$ was returned, then $\mathsf{LambdaExpand}(-,-,-)$ terminates when applied to (x,α,Γ) with $\mathsf{LambdaExpand}(x,\alpha,\Gamma) \in \mathbf{Core}(n+m,n+m)$. Moreover, the following derivation holds.



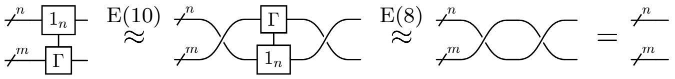
Then $\lambda(x,\alpha) \odot \Gamma \approx_E U \odot \lambda(xy,\alpha\beta/\pi) = \mathsf{LambdaExpand}(x,\alpha,\Gamma)$ and the inductive step holds.

It follows by the principle of induction that if $\Gamma \in \mathbf{Core}(m,m)$ is a diagonal form prefix, then $\mathsf{LambdaExpand}(-,-,-)$ terminates when applied to (x,α,Γ) with $\mathsf{LambdaExpand}(x,\alpha,\Gamma) \in \mathbf{Core}(n+m,n+m)$ and $\lambda(x,\alpha) \odot \Gamma \approx_E \mathsf{LambdaExpand}(x,\alpha,\Gamma)$. Since every diagonal form is a prefix of itself, then this establishes that the proof holds for a fixed x and α. Since x and α were arbitrary, then this completes the proof. □

Lemma H.8. *If Λ and Γ are both in diagonal form, then* $\mathsf{DiagExpand}(-,-)$ *terminates when applied to* (Λ,Γ) *with* $\mathsf{DiagExpand}(\Lambda,\Gamma) \in \mathbf{Core}(k,k)$ *and* $\Lambda \odot \Gamma \approx_E \mathsf{DiagExpand}(\Lambda,\Gamma)$ *where* $k = \mathrm{dom}(\Lambda) + \mathrm{dom}(\Gamma)$.

Proof. Let $\Gamma \in \mathbf{Core}(m,m)$ in diagonal form and for a given $n \in \mathbb{N}$ write $k = n+m$. The proof follows by induction on $|\Lambda|$ where Λ is a prefix of a diagonal form.

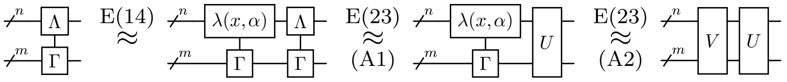
- **Base Case**. Let $\Lambda \in \mathbf{Core}(n,n)$. If $|\Lambda| = 0$, then the first line is reached and 1_{n+m} is returned. In other words, $\mathsf{DiagExpand}(-,-)$ terminates when applied to (Λ,Γ) and $\mathsf{DiagExpand}(\Lambda,\Gamma) = 1_{n+m} \in \mathbf{Core}(k,k)$. Since $|\Lambda| = 0$, then $\Lambda = 1_n$ and the following derivation holds.



Then $\Lambda \odot \Gamma = 1_n \odot \Gamma \approx_E 1_{n+m} = \mathsf{DiagExpand}(\Lambda,\Gamma)$.

- **Inductive Hypothesis**. For some $\ell \in \mathbb{N}$, if $\Lambda \in \mathbf{Core}(n,n)$ is a diagonal form prefix and $|\Lambda| = \ell$, then $\mathsf{DiagExpand}(-,-)$ terminates when applied to (Λ,Γ) with $\mathsf{DiagExpand}(\Lambda,\Gamma) \in \mathbf{Core}(k,k)$ and $\Lambda \odot \Gamma \approx_E \mathsf{DiagExpand}(\Lambda,\Gamma)$.

- **Inductive Step**. Assume that for some $\ell \in \mathbb{N}$, if $\Lambda \in \mathbf{Core}(n,n)$ is a diagonal form prefix and $|\Lambda| = \ell$, then $\mathsf{DiagExpand}(-,-)$ terminates when applied to (Λ,Γ) with $\Lambda \odot \Gamma \approx_E \mathsf{DiagExpand}(\Lambda,\Gamma)$ and $\mathsf{DiagExpand}(\Lambda,\Gamma) \in \mathbf{Core}(k,k)$. Let $\Lambda \in \mathbf{Core}(n,n)$ such that Λ is the prefix of a diagonal form with $|\Lambda| = \ell + 1$. Since $|\Lambda| = \ell + 1 > 0$, then the if-condition on the first line fails, and the program continues to line two. Then after executing line two, $\lambda(x,\alpha)$ is assigned to the last symbol in Λ and Λ' is assigned to the rest of Λ. This means that Λ' is a prefix of a diagonal form with $|\Lambda'| = \ell$. Then by the inductive hypothesis, the third line terminates and $U \leftarrow \mathsf{DiagExpand}(\Lambda',\Gamma)$ with $(\mathrm{A1}) : \Lambda' \odot \Gamma \approx_E U$ and $U \in \mathbf{Core}(k,k)$. Then by Lemma H.7, the fourth line terminates and $V \leftarrow \mathsf{LambdaExpand}(x,\alpha,\Gamma)$ with $V \in \mathbf{Core}(k,k)$ and $(\mathrm{A2}) : \lambda(x,\alpha) \odot \Gamma \approx_E V$. Then the fourth line is reached, at which point $U \circ V$ is returned. That is, $\mathsf{DiagExpand}(-,-)$ terminates when applied to (Λ,Γ) with $\mathsf{DiagExpand}(\Lambda,\Gamma) = U \circ V \in \mathbf{Core}(k,k)$. Moreover, the following derivation holds.

  Then $\Lambda \odot \Gamma \approx_E U \circ V \approx_E \mathsf{DiagExpand}(\Lambda,\Gamma)$ and the inductive step holds.

It follows by the principle of induction that if $\Lambda \in \mathbf{Core}(n,n)$ is a diagonal form prefix, then $\mathsf{DiagExpand}(-,-)$ terminates when applied to (Λ,Γ) such that $\Lambda \odot \Gamma \approx_E \mathsf{DiagExpand}(\Lambda,\Gamma)$ and $\mathsf{DiagExpand}(\Lambda,\Gamma) \in \mathbf{Core}(k,k)$. Since every diagonal form is a prefix of itself, then this establishes the proof for a fixed Γ. Since Γ were arbitrary, then this completes the proof. □

Theorem H.9. *Assume that* $\mathsf{Reduce}_n(-)$ *terminates when applied to each* $U \in \mathrm{Mor}(\mathbf{CExt}[n])$. *If* $T \in \mathsf{Tower}(\mathbf{CExt}[n]) \cap \mathbf{CExt}[n+1](k,k)$, *then* $\mathsf{Expand}_{n+1}(-)$ *terminates when applied to* T *with* $\mathsf{Expand}_{n+1}(U) \in \mathbf{Core}(k,k)$. *Moreover, if* $U \approx_E \mathsf{Reduce}_n(U)$ *for all* $U \in \mathrm{Mor}(\mathbf{CExt}[n])$, *then* $T \approx_E \mathsf{Expand}_{n+1}(T)$.

Proof. Let $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $|T| \geq 1$. The proof follows by induction on $|T|$.

- **Base Case**. Let $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $k = \mathrm{dom}(T)$ and $|T| = 1$. By assumption, the first line terminates and $U \leftarrow \mathsf{Reduce}_n(T_1)$. Since $|T| = 1$, then the if-condition on the second line will succeed and $\mathsf{Expand}_n(-)$ will return U. In other words, $\mathsf{Expand}_{n+1}(-)$ terminates when applied to T with $\mathsf{Expand}_{n+1}(T) = U$. Moreover, since $|T| = 1$, then $T = T_1$ with $k = \mathrm{dom}(T_1)$. This means that $\mathsf{Expand}_{n+1}(T) = U \in \mathbf{Core}(k,k)$.

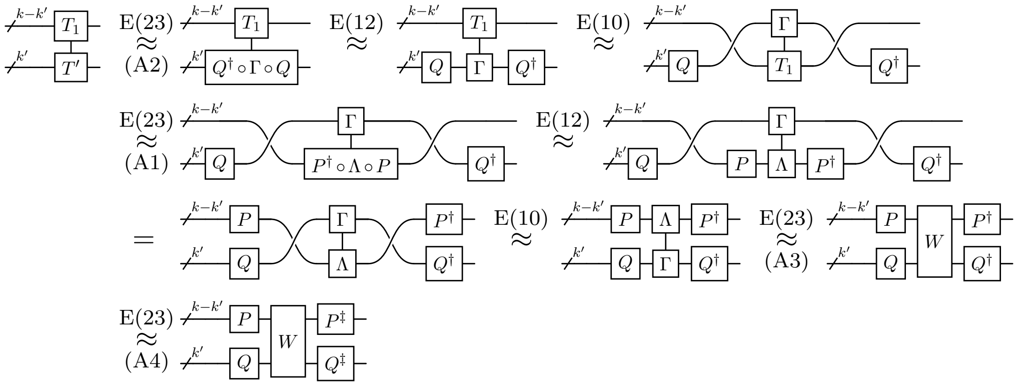
- **Inductive Hypothesis**. For some strictly positive integer ℓ, if $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $\mathrm{dom}(T) = k$ and $|T| = \ell$, then $\mathsf{Expand}_{n+1}(-)$ terminates when applied to T with $\mathsf{Expand}_{n+1}(T) \in \mathbf{Core}(k,k)$.

- **Inductive Step**. Assume that for some strictly positive integer ℓ, if $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $\mathrm{dom}(T) = k$ and $|T| = \ell$, then $\mathsf{Expand}_{n+1}(-)$ terminates when applied to T with $\mathsf{Expand}_{n+1}(T) \in \mathbf{Core}(k,k)$. Let $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $|T| = \ell + 1$ and $k = \mathrm{dom}(T)$. Then there exists some $T' \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $|T'| = \ell > 0$ and $T = T_1 \odot T'$. Now consider applying $\mathsf{Expand}_{n+1}(-)$ to T and let $k' = \mathrm{dom}(T')$. By assumption, the first line terminates and $U \leftarrow \mathsf{Reduce}_n(T_1)$ with $U \in \mathbf{Core}(k-k',k-k')$. Since $|T| = \ell + 1 > 1$, then the if-condition on the second line fails, and the program continues to line three. Then by Theorem H.4, the third line terminates and $(P,\Lambda) \leftarrow \mathsf{Diag}(U)$ with $P \in \mathbf{Core}(k-k',k-k')$

and $\Lambda \in \mathbf{Core}(k-k', k-k')$ in diagonal form. Since $|T'| = \ell > 0$, then by the inductive hypothesis the fourth line terminates and $V \leftarrow \mathsf{Expand}_{n+1}(T')$ with $V \in \mathbf{Core}(k', k')$. Then by Theorem H.4, the fifth line terminates and $(Q, \Gamma) \leftarrow \mathsf{Diag}(V)$ with $P \in \mathbf{Core}(k', k')$ and $\Lambda \in \mathbf{Core}(k', k')$ in diagonal form. Then by Lemma H.8, the sixth line terminates and $W \leftarrow \mathsf{DiagExpand}(\Lambda, \Gamma)$ with $W \in \mathbf{Core}(k, k)$. Then the seventh line is reached, at which point $(P^\ddagger \boxtimes Q^\ddagger) \circ W \circ (P \boxtimes Q)$ is returned. That is, $\mathsf{Expand}_{n+1}(-)$ terminates when applied to T with $\mathsf{Expand}_{n+1}(T) = (P^\ddagger \boxtimes Q^\ddagger) \circ W \circ (P \boxtimes Q)$. Since $(P^\ddagger \boxtimes Q^\ddagger) = (P \boxtimes Q)^\ddagger \in \mathbf{Core}(k, k)$ by definition, then $\mathsf{Expand}_{n+1}(T) \in \mathbf{Core}(k, k)$. Then the inductive step holds.

Then by the principle of induction, if $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $\mathrm{dom}(T) = k$, then $\mathsf{Expand}_{n+1}(-)$ terminates when applied to T with $\mathsf{Expand}_{n+1}(T) \in \mathbf{Core}(k, k)$. Next, if $U \approx_E \mathsf{Reduce}_n(U)$ for each $U \in \mathrm{Mor}(\mathbf{CExt}[n])$, then it follows by induction on $|T|$ that $T \approx_E \mathsf{Expand}_{n+1}(T)$.

- **Base Case**. Let $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ and $|T| = 1$. By the start of this proof, $\mathsf{Expand}_{n+1}(-)$ terminates when applied to T. Then by the second assumption, $U \leftarrow \mathsf{Reduce}_n(T_1)$ after the first line with $T_1 \approx_E U$. Since $|T| = 1$, then the if-condition on the second line succeeds and $\mathsf{Expand}_n(-)$ is return U. This means that $T = T_1 \approx_E \mathsf{Reduce}_n(T_1) = \mathsf{Expand}_{n+1}(T)$.
- **Inductive Hypothesis**. For some strictly positive integer ℓ, if $T \in \mathsf{Tower}(\mathbf{CExt}[n])$, then $T \approx_E \mathsf{Expand}_{n+1}(T)$.
- **Inductive Step**. Assume that for some strictly positive integer ℓ, if $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $|T| = \ell$, then $T \approx_E \mathsf{Expand}_{n+1}(T)$. Let $T \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $|T| = \ell + 1$. Then there exists some $T' \in \mathsf{Tower}(\mathbf{CExt}[n])$ with $|T| = \ell$ and $T = T_1 \odot T'$. Now consider applying $\mathsf{Expand}_{n+1}(-)$ to T. From the start of this proof, $\mathsf{Expand}_{n+1}(-)$ terminates when applied to T. By assumption, $U \leftarrow \mathsf{Reduce}_n(T_1)$ after the first line with $T_1 \approx_E U$. Since $|T| = \ell + 1 > 1$, then the if-condition on the second line fails, and the program continues to line three. Then by Theorem H.4, $(P, \Lambda) \leftarrow \mathsf{Diag}(U)$ after the third line with $U \approx_E P^\dagger \circ \Lambda \circ P$. Since $T_1 \approx_E U$, then $(\mathrm{A1}) : T_1 \approx_E P^\dagger \circ \Lambda \circ P$ by the transitivity of $(\approx_E)$. Since $|T'| = \ell$, then by the inductive hypothesis, $V \leftarrow \mathsf{Expand}_{n+1}(T')$ after the fourth line with $T' \approx_E V$. Then by Theorem H.4, $(Q, \Gamma) \leftarrow \mathsf{Diag}(V)$ after the fifth line with $V \approx_E Q^\dagger \circ \Gamma \circ Q$. Since $T' \approx_E V$, then $(\mathrm{A2}) : T' \approx_E Q^\dagger \circ \Gamma \circ Q$ by the transitivity of $(\approx_E)$. Then by Lemma H.8, $W \leftarrow \mathsf{DiagExpand}(\Lambda, \Gamma)$ after the sixth line with $(\mathrm{A3}) : \Lambda \odot \Gamma \approx_E W$. Then the seventh line is reached, at which point $(P^\ddagger \boxtimes Q^\ddagger) \circ W \circ (P \boxtimes Q)$ is returned. Since $(P^\ddagger \boxtimes Q^\ddagger) = (P \boxtimes Q)^\ddagger$ by definition, then by Lemma 5.4, $(\mathrm{A4}) : (P^\dagger \boxtimes Q^\dagger) = (P \boxtimes Q)^\dagger \approx_E (P \boxtimes Q)^\ddagger = (P^\ddagger \boxtimes Q^\ddagger)$. Then the following derivation holds.



Then $T \approx_E (P^\ddagger \boxtimes Q^\ddagger) \circ W \circ (P \boxtimes Q) = \mathsf{Expand}_{n+1}(T)$ and the inductive step holds.

Then by the principle of induction, if $T \in \mathsf{Tower}(\mathbf{CExt}[n])$, then $T \approx_E \mathsf{Expand}_{n+1}(T)$. □

I Proof of Theorem 5.10

Proof. First, a partitioning will be constructed for $\Sigma^0_{\mathbf{CExt}}$. Since $\Sigma^0_{\mathbf{CExt}} \subseteq \Sigma_{\mathbf{HQC}}$, then the following equation holds by Lemma 4.2.

$$\Sigma^0_{\mathbf{CExt}} = \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{HQC}} = \left(\Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Prim}}\right) \sqcup \left(\Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Ctrl}}\right) \sqcup \left(\Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Pow}}\right)$$

Next, it must be shown that $r_n(-)$ is well-defined for each $n \in \mathbb{N}$. This means that $r_n(-)$ assigns each $g \in \Sigma^n_{\mathbf{CExt}}$ to a unique word $r_n(g)$ with $r_n(g) \in \mathrm{Mor}(\mathbf{Core})$. The proof follows by induction on n.

- **Base Case**. Let $g \in \Sigma^0_{\mathbf{CExt}}$. Then there are three cases to consider.
  1. Assume that $g \in \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Prim}} = \Sigma_{\mathbf{Prim}} \subseteq \Sigma^0_{\mathbf{Core}}$. Since $r_0(g) = g \uparrow 1$ by definition, then $r_0(g) \in \mathsf{Power}(\Sigma^0_{\mathbf{Core}}) \subseteq \Sigma^1_{\mathbf{Core}} \subseteq \mathrm{Mor}(\mathbf{Core})$. Then $r_0(g)$ is well-defined.
  2. Assume that $g \in \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Ctrl}}$ or $g \in \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Pow}}$. Then $g \notin \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Prim}}$. Since $\Sigma^0_{\mathbf{CExt}} = \Sigma_{\mathbf{Core}} \cup \Sigma_{\mathbf{Prim}}$, then $g \in \Sigma_{\mathbf{Core}} \subseteq \mathrm{Mor}(\mathbf{Core})$ Since $r_0(g) = g$ by definition, then $r_0(g)$ is well-defined.

  In each case, $r_0(g)$ is well-defined. Since g was arbitrary, then $r_0(-)$ is well-defined.
- **Inductive Hypothesis**. For some $n \in \mathbb{N}$, $r_n : \Sigma^n_{\mathbf{CExt}} \to U(\mathbf{Core})$ is well-defined.
- **Inductive Step**. Assume that for some $n \in \mathbb{N}$, $r_n : \Sigma^n_{\mathbf{CExt}} \to U(\mathbf{Core})$ is well-defined. Then there exists a well-defined functor $\mathsf{Reduce}_n = P(r_n)$. In particular this means that $\mathsf{Reduce}_n(-)$ terminates when applied to each $U \in \mathrm{Mor}(\mathbf{CExt}[n])$. Let $g \in \Sigma^{n+1}_{\mathbf{CExt}}$. There are three cases to consider.
  1. Assume that $g \in \Sigma^n_{\mathbf{CExt}}$. By assumption, $r_n(-)$ is well-defined, which means that $r(g)$ is unique with $r(g) \in \mathrm{Mor}(\mathbf{Core})$. Since $r_{n+1}(-)$ assigns g to $r_n(g) \in \mathrm{Mor}(\mathbf{Core})$, then $r_{n+1}(g)$ is well-defined.
  2. Assume $g \in \mathsf{Tower}(\mathbf{CExt}[n]) \cap \mathbf{CExt}[n+1](k,k)$ for some $k \in \mathbb{N}$. Since $\mathsf{Reduce}_n(-)$ terminates when applied to each $U \in \mathrm{Mor}(\mathbf{CExt}[n])$, then it follows from Theorem H.9 that $\mathsf{Expand}_{n+1}(-)$ terminates when applied to g with $\mathsf{Expand}_{n+1}(g) \in \mathbf{Core}(k,k)$. Since $r_{n+1}(-)$ assigns g to $\mathsf{Expand}_{n+1}(g)$, then $r_{n+1}(g)$ is well-defined.
  3. Assume that $g \in \mathsf{Power}(\mathbf{CExt}[n]) \cap \mathbf{CExt}[n+1](k,k)$ for some $k \in \mathbb{N}$. Then there exists a $U \in \mathbf{CExt}[n](k,k)$ and $\alpha \in \mathbb{R}$ such that $g = U \uparrow \alpha$. Since $\mathsf{Reduce}_n(-)$ terminates when applied to each U, then it follows from Theorem H.6 that $\mathsf{Drop}_{n+1}(-,-)$ terminates when applied to (U, α) with $\mathsf{Drop}_{n+1}(U,\alpha) \in \mathbf{Core}(k,k)$. Since $r_{n+1}(-)$ assigns g to $\mathsf{Drop}_{n+1}(U,\alpha)$, then $r_{n+1}(g)$ is well-defined.

  In each case, $r_{n+1}(g)$ is well-defined. Since g was arbitrary, then $r_{n+1}(-)$ is well-defined. Then the inductive step holds.

The by the principle of induction, each $r_n(-)$ is well-defined. Since $\bigcup_{n=0}^{\infty} \Sigma^n_{\mathbf{CExt}} = \Sigma_{\mathbf{HQC}}$, then this defines a signature morphism $r : \Sigma_{\mathbf{HQC}} \to U(\mathbf{Core})$ such that $r(g) = r_n(g)$ for each $n \in \mathbb{N}$ and $g \in \Sigma^n_{\mathbf{CExt}}$. Define $\mathsf{Reduce} = P(r)$. It remains to be shown that if $g \in \Sigma_{\mathbf{HQC}}$, then $\mathsf{Reduce}(g) \approx_E g$. The proof follows by induction on $\mathbf{CExt}[n] \hookrightarrow \mathbf{HQC}$.

- **Base Case**. Let $g \in \Sigma^0_{\mathbf{CExt}}$. Then there are two cases to consider.
  1. Assume that $g \in \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Ctrl}}$. Then $r_0(g) = g \uparrow 1$. Then $r_0(g) \approx_E g$ by E(17).

2. Assume that $g \in \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Ctrl}}$ or $g \in \Sigma^0_{\mathbf{CExt}} \cap \Sigma_{\mathbf{Pow}}$. Then $r_0(g) = g$ by definition. Since $(\approx_E)$ is reflexive, then $r_0(g) \approx_E g$.

In each case, $\mathsf{Reduce}(g) = r_0(g) \approx_E g$. Then $\pi_E(\mathsf{Reduce}(g)) = \pi_E(g)$. Since g was arbitrary, then $\pi_E \circ \mathsf{Reduce} \circ i = \pi_E \circ i$ where $i : \Sigma^0_{\mathbf{CExt}} \to \mathbf{CExt}[0]$. Then by the universal property of free prop categories, $\pi_E \circ \mathsf{Reduce} = \pi_E$ when restricted to $\mathbf{CExt}[0]$. Let $U \in \mathrm{Mor}(\mathbf{CExt}[0])$. Then $\pi_E(\mathsf{Reduce}(U)) = \pi_E(U)$, which implies that $\mathsf{Reduce}(U) \approx_E U$. Since U was arbitrary, then $\mathsf{Reduce}(U) \approx_E U$ for all $U \in \mathrm{Mor}(\mathbf{CExt}[0])$.

- **Inductive Hypothesis**. For some $n \in \mathbb{N}$, if $U \in \mathrm{Mor}(\mathbf{CExt}[n])$, then $\mathsf{Reduce}(U) \approx_E U$.
- **Inductive Step**. Assume that for some $n \in \mathbb{N}$, if $U \in \mathrm{Mor}(\mathbf{CExt}[n])$, then the derivation $\mathsf{Reduce}(U) \approx_E U$ holds. Let $g \in \Sigma^{n+1}_{\mathbf{CExt}}$. There are three cases to consider.
  1. Assume that $g \in \Sigma^n_{\mathbf{CExt}}$. Then $\mathsf{Reduce}(g) \approx_E g$ by the inductive hypothesis.
  2. Assume that $g \in \mathsf{Tower}(\mathbf{CExt}[n])$. Then $\mathsf{Expand}(g) = r_{n+1}(g) = r(g) = \mathsf{Reduce}(g)$. By the inductive hypothesis, $U \approx_E \mathsf{Reduce}(U) = \mathsf{Reduce}_n(U)$ for each $U \in \mathrm{Mor}(\mathbf{CExt}[n])$. It then follows from Theorem H.9 that $g \approx_E \mathsf{Expand}(g) = \mathsf{Reduce}(g)$.
  3. Assume that $g \in \mathsf{Power}(\mathbf{CExt}[n])$. Then there exists some $U \in \mathrm{Mor}(\mathbf{CExt}[n])$ and $\alpha \in \mathbb{R}$ such that $g = U \uparrow \alpha$. Then by definition $\mathsf{Drop}(U, \alpha) = r_{n+1}(g) = r(g) = \mathsf{Reduce}(g)$. Then by the inductive hypothesis, $U \approx_E \mathsf{Reduce}(U) = \mathsf{Reduce}_n(U)$. It then follows from Theorem H.6 that $g = U \uparrow \alpha \approx_E \mathsf{Drop}(U, \alpha) = \mathsf{Reduce}(g)$.

  In each case, $\mathsf{Reduce}(g) \approx_E g$, which implies that $\pi_E(\mathsf{Reduce}_{n+1}(g)) = \pi_E(g)$. Since g was arbitrary, then $\pi_E \circ \mathsf{Reduce} \circ i = \pi_E \circ i$ for $i : \Sigma^{n+1}_{\mathbf{CExt}} \hookrightarrow \mathbf{CExt}[n+1]$. Then by the universal property of free prop categories, $\pi_E \circ \mathsf{Reduce} = \pi_E$ when restricted to $\mathbf{CExt}[n+1]$. Let $U \in \mathbf{CExt}[n+1]$. Then $\pi_E(\mathsf{Reduce}(U)) = \pi_E(U)$. Then $\mathsf{Reduce}(U) \approx_E U$. Since U was arbitrary, then $\mathsf{Reduce}_{n+1}(U) \approx_E U$ for all $U \in \mathbf{CExt}[n+1]$. Then the inductive step holds.

Then by the principle of induction, $\mathsf{Reduce}(U) \approx_E U$ for each $n \in \mathbb{N}$ and $U \in \mathrm{Mor}(\mathbf{CExt}[n])$. This implies that $\mathsf{Reduce}(g) \approx_E g$ for each $g \in \Sigma_{\mathbf{HQC}}$. Let $g \in \Sigma_{\mathbf{HQC}}$. Since $\Sigma_{\mathbf{HQC}} = \bigcup_{n=0}^{\infty} \Sigma^n_{\mathbf{CExt}}$, then there exists an $n \in \mathbb{N}$ such that $g \in \Sigma^n_{\mathbf{CExt}} \subseteq \mathrm{Mor}(\mathbf{CExt}[n])$. Then $\mathsf{Reduce}(g) \approx_E g$. Since g was arbitrary, then $\mathsf{Reduce}(g) \approx_E g$ for each $g \in \Sigma_{\mathbf{HQC}}$ with $\mathsf{Reduce} : \mathbf{HQC} \to \mathbf{Core}$. Moreover, $(\Sigma_{\mathbf{Core}}, E)$ is complete with respect to $[\![-]\!]_H$ by Theorem 5.9. Then $(\Sigma_{\mathbf{HQC}}, E)$ is complete with respect to $[\![-]\!]_H$ by Theorem 5.2. □

J Redundant Relations in the HQC Equational Theory

Two presentations (Σ, E) and (Γ, Q) are equivalent if $P(\Sigma)/E \cong P(\Gamma)/Q$ as prop categories. It can be shown that (Σ, E) and (Γ, Q) are equivalent if and only if (Γ, Q) can be obtained from (Σ, E) via a sequence of Tietze transformations [6]. The transformations are as follow.

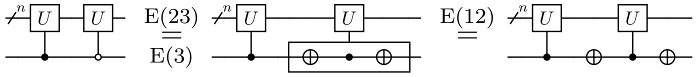
- **Removing a Generator**. Let $f \in \Sigma$, $\Gamma = \Sigma \setminus \{f\}$, and $g \in P(\Gamma)(\mathrm{dom}(f), \mathrm{cod}(f))$. If $f \approx_E g$, then (Σ, E) is equivalent to (Γ, Q) where Q is obtained from E by replacing every instance of f by g.
- **Removing a Relation**. Let $(f, g) \in E$ and $Q = E \setminus \{(f, g)\}$. If $f \approx_Q g$, then (Σ, E) is equivalent to (Σ, Q).

These transformations can then be used to prove that specific generators and relations in $(\Sigma_{\mathbf{HQC}}, E)$ are redundant.

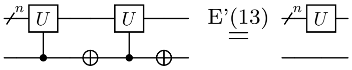
Using these transformations, this section derives several minimal generating sets for $\mathbf{HQC}/E$. It is well-known that all single-qubit circuits can be generated (up-to global phase) using any two of the three generators $\{X(\theta), Z(\theta), H\}$. This corresponds to single-qubit hierarchical circuits generated from $\{ -\bullet- , -\oplus- , -\boxed{H}- \}$. Regardless of the choice of generators, it is then possible to find circuits U and V such that $[\![U]\!]_H = Z$ and $[\![V]\!]_H = X$. The circuit $U \odot V$ can then act as a controlled-not gate, and all multi-qubit circuits can be generated (up-to global phase). Finally, the global phase gate can be used to generate all multi-qubit circuits exactly, as described in Proposition H.2. These minimal gate sets can be obtained via Tietze transformations.

First, it will be shown that $g_1 = -\ominus-$ can be eliminated from $(\Sigma_{\mathbf{HQC}}, E)$. First, note that g_1 appears as the left-hand side of E(4), and does not appear on the right-hand side of E(4). This means that g_1 and E(4) can be removed from $(\Sigma_{\mathbf{HQC}}, E)$ via a Tietze transformation. Moreover, since g_1 does not appear in any other relations, then the relations in E need not be modified.

Next, it will be shown that $g_2 = -\circ-$ can be eliminated from $(\Sigma_{\mathbf{HQC}}, E)$. As in the case of g_1, there exists a relation E(3) which can be used to eliminate g_2 via a Tietze transformation. However, g_2 also appears in E(13), and must therefore be modified. To simplify the process, we will manually replace E(13) before removing g_2. Observe that the following derivation holds for each $U \in \mathbf{HQC}(n, n)$, since H is self-adjoint.



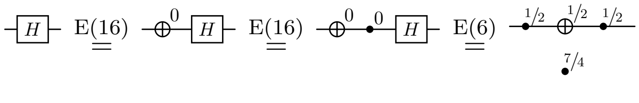
Using the derivation, it is then possible to introduce a new relation E'(13), which can then be used to eliminate E(13).



Since g_2 does not appear in any instance of E'(13), then g_2 can be removed using E(3) without any further modifications to the relation set. This yields a new presentation, (Γ, Q) where Γ and Q are defined as follows.

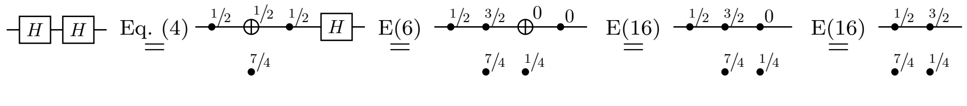
$$\Gamma = \{ -\bullet- , -\oplus- , -\boxed{H}- , \bullet \} \qquad\qquad Q = E \setminus \{E(4), E(3), E(13)\} \cup \{E'(13)\}$$

It remains to be shown that Γ can be reduced to the global phase gate with only two of the three single-qubit gates. Before proceeding, it will be shown that E(1) is redundant, and can be removed from the presentation. In principle, E(1) can be derived via several applications of E(6), though this process is tedious. Instead, it should be noted that in the proof of completeness, E(1) is used precisely once, to prove that the Hadamard gate is self-inverse. Then, it suffices to prove that the Hadamard gate is self-inverse without the use of E(1). It then follows from completeness, together with the soundness of E, that E(1) is derivable from $Q \setminus \{E(1)\}$. As a first step, E(6) is used to derive an alternative definition for the Hadamard gate.



(4)

This alternative definition can then be used to prove that the Hadamard gate is self-inverse.



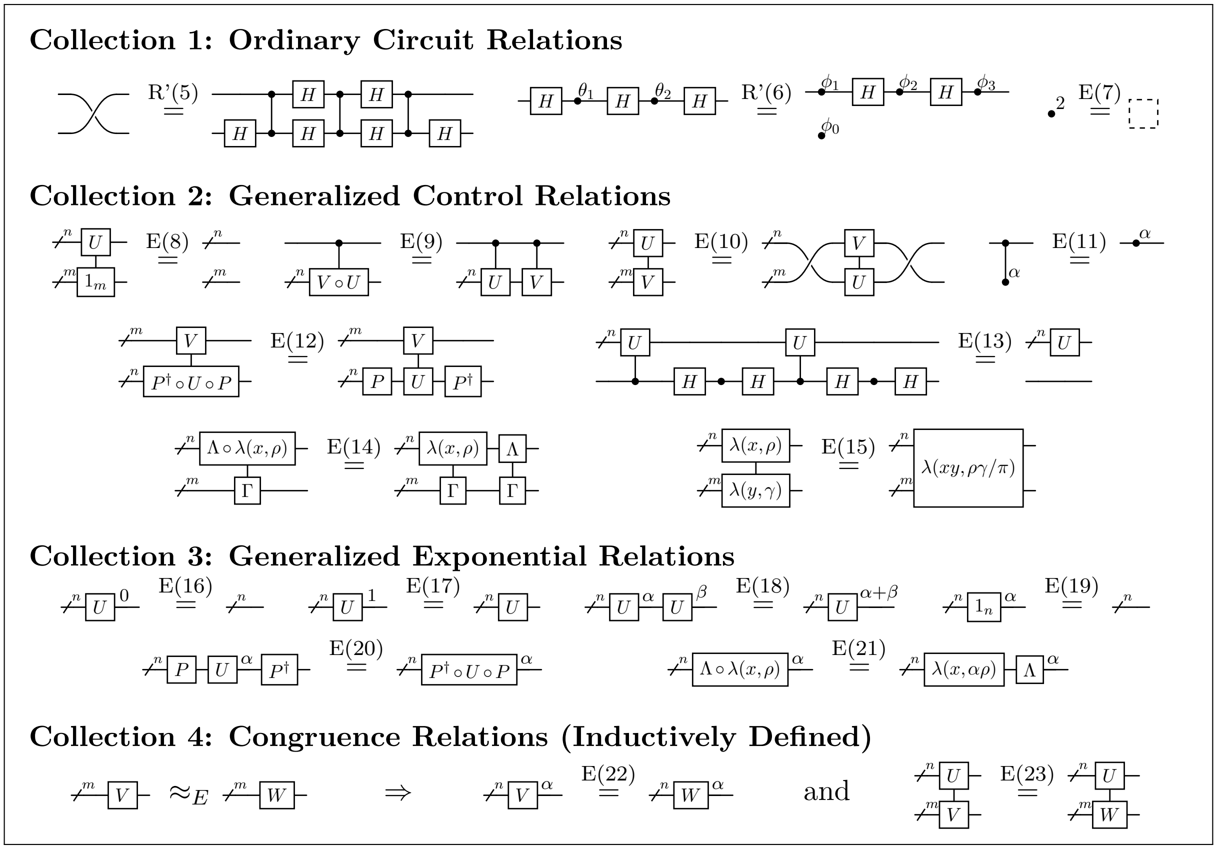
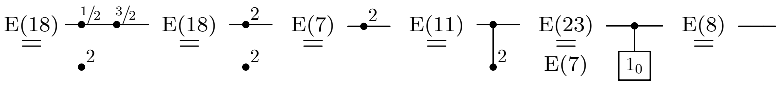
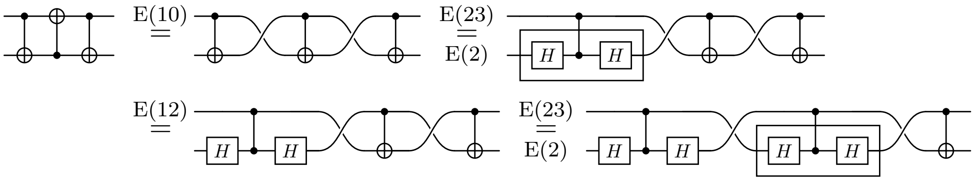


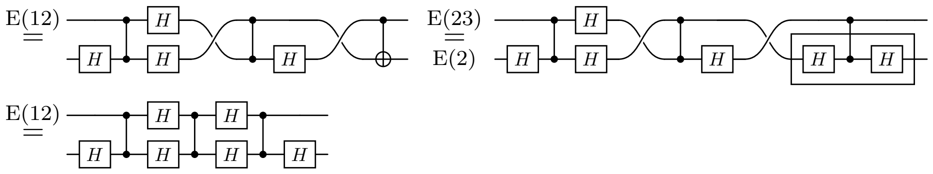
Figure 7: An alternative equational theory for **HQC**, using only the generators in Γ_X.



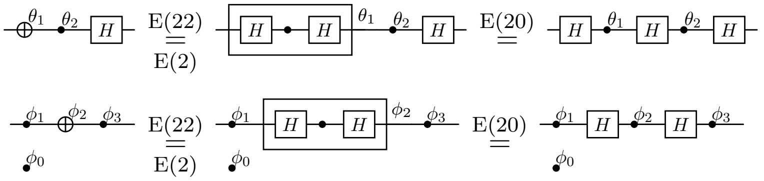
In conclusion, (Γ, Q) is equivalent to (Γ, R) where $R = Q \setminus \{\text{E}(1)\}$. It remains to be shown that Γ can be further reduced.

Eliminating the Pauli-X Gate. Let $g_X = -\oplus-$. Since g_X appears as the left-hand side of E(2), and does not appear on the right-hand side of E(2), then g_X and E(2) can be removed via a Tietze transformation. Unfortunately, g_X still appears in relations {E(5),E(6),E'(13)}, meaning that some care must be taken before g_X can be fully removed from (Γ, R). To simplify the process, we will manually replace {E(5),E(6),E'(13)} before removing g_X. This is possible since H is self-adjoint. To replace E(5), the following derivation suffices.

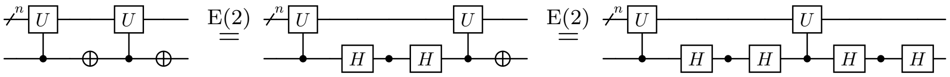




To replace E(6), the following derivations suffice.



To replace E'(13), the following derivation suffices.

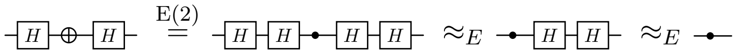


Using these derivations, relations {R'(5),R'(6),R'(13)} can be introduced (see Fig. 7), which can ten be used to eliminate {E(5),E(6),E'(13)}. Since g_X does not appear in any instance of E'(5) or E'(6), then g_X can be removed using E(2) without any further modifications to the relation set. This yields a new presentation, (Γ_X, R_X) where Γ_X and R_X are defined as follows.

$$\Gamma = \{ -\bullet- \,,\, -\boxed{H}- \,,\, \bullet \} \qquad R_X = R \setminus \{\text{E(2)},\text{E(5)},\text{E(6)}\} \cup \{\text{E'(5)},\text{E'(6)}\}$$

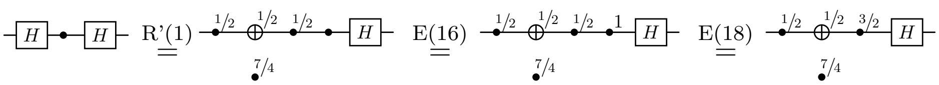
The relations in Q_X are depicted in Fig. 7.

Eliminating the Pauli-Z Gate. Let $g_Z = -\bullet-$. A-priori, there does not exist a relation to eliminate g_Z. However, the following derivation can be used to introduce such a relation, via a Tietze transformation.



Since the generalized control relations in $(\Sigma_{\mathbf{HQC}}, E)$ are written in terms of the X-basis, then obtaining concise relations for $\Gamma \setminus \{g_Z\}$ is somewhat tedious. For this reason, the equational theory has been omitted. Intuitively, this theory corresponds to writing the generalized control relations with respect to the Z-basis, as opposed to the X-basis.

Eliminating the Hadamard Gate. Let $g_H = -\boxed{H}-$. To eliminate g_H, it is necessary to first introduce Eq. (4) as a relation R'(1) via a Tietze transformation. Since g_H appears as the left-hand side of R'(1), and does not appear on the right-hand side of R'(1), then g_H and R'(1) can be eliminated via a Tietze transformation. Unfortunately, g_H still appears in relations {E(2),E(6)}, meaning that some care must be taken before g_H can be fully removed from (Γ, R). In turns out that the relation E(2) is redundant, as illustrated by the following derivation.



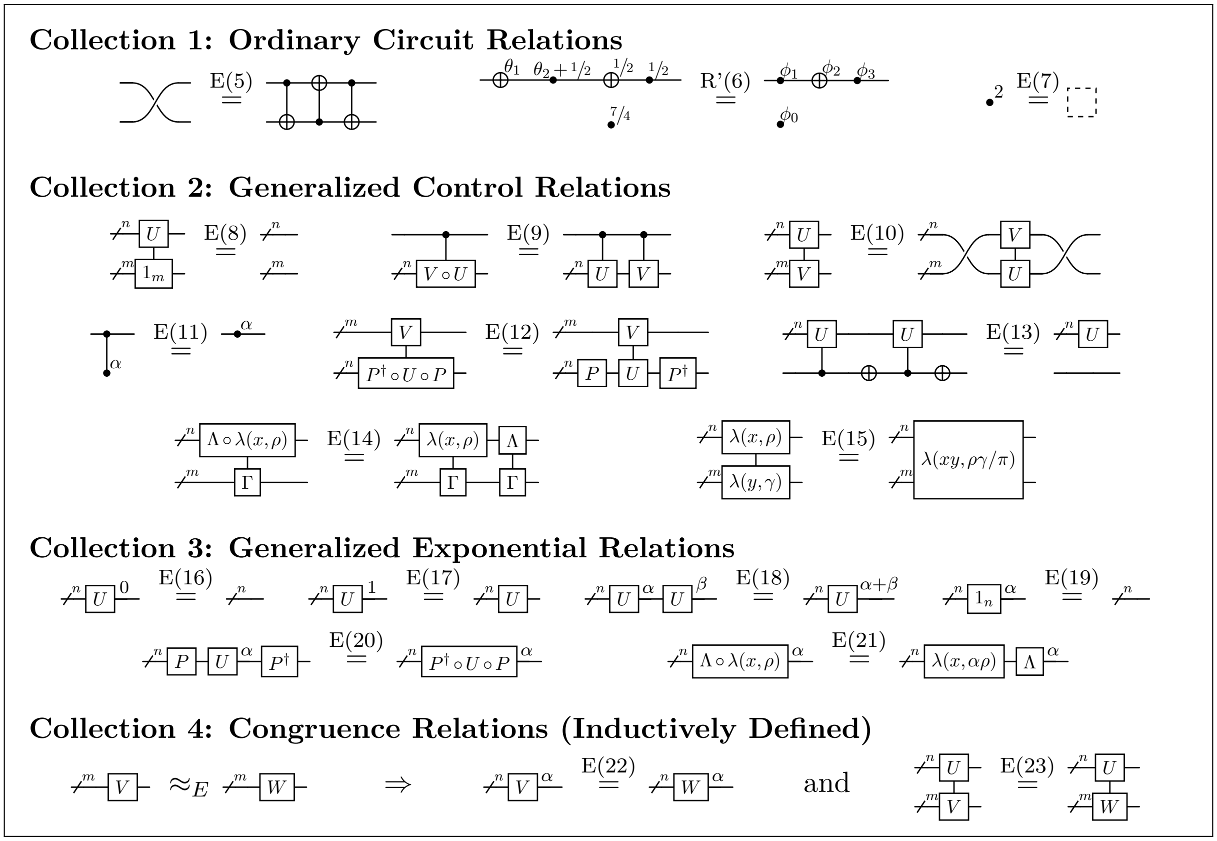
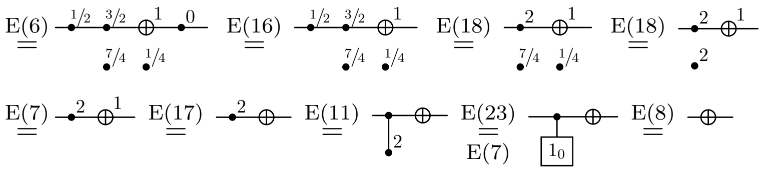
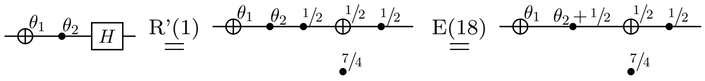

Collection 1: Ordinary Circuit Relations
E(5)
R'(6)
E(7)
Collection 2: Generalized Control Relations
E(8)
E(9)
E(10)
E(11)
E(12)
E(13)
E(14)
E(15)
Collection 3: Generalized Exponential Relations
E(16)
E(17)
E(18)
E(19)
E(20)
E(21)
Collection 4: Congruence Relations (Inductively Defined)
≈E
⇒
E(22)
and
E(23)

Figure 8: An alternative equational theory for **HQC**, using only the generators in Γ_H.



To replace E(6), the following derivation suffices.



Using this derivation, it is then possible to introduce a new relation R'(6) as in Fig. 8, which is then used to eliminate E(6). Since E(2) has been eliminated and g_H does not appear in any instance of R'(6), then g_H can be removed using R'(1) without any further modifications to the relation set. This yields a new presentation, (Γ_H, R_H) where Γ_H and R_H are defined as follows.

$\Gamma = \{$ —•— , —⊕— , • $\}$ $\qquad R_H = R \setminus \{\text{E(2)}, \text{E(6)}\} \cup \{\text{E'(6)}\}$

The relations in Q_H are depicted in Fig. 8.