Completeness of Sum-Over-Paths for Toffoli-Hadamard and the Dyadic Fragments of Quantum Computation

Renaud Vilmart

Completeness of Sum-Over-Paths for Toffoli-Hadamard and the Dyadic Fragments of Quantum Computation

Renaud Vilmart
Université Paris-Saclay, CNRS, ENS Paris-Saclay, Inria, LMF, 91190, Gif-sur-Yvette, France

Abstract

The "Sum-Over-Paths" formalism is a way to symbolically manipulate linear maps that describe quantum systems, and is a tool that is used in formal verification of such systems.

We give here a new set of rewrite rules for the formalism, and show that it is complete for "Toffoli-Hadamard", the simplest approximately universal fragment of quantum mechanics. We show that the rewriting is terminating, but not confluent (which is expected from the universality of the fragment). We do so using the connection between Sum-over-Paths and graphical language ZH-Calculus, and also show how the axiomatisation translates into the latter.

Finally, we show how to enrich the rewrite system to reach completeness for the dyadic fragments of quantum computation – obtained by adding phase gates with dyadic multiples of π to the Toffoli-Hadamard gate-set – used in particular in the Quantum Fourier Transform.

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

Keywords and phrases Quantum Computation, Verification, Sum-Over-Paths, Rewrite Strategy, Toffoli-Hadamard, Completeness

Digital Object Identifier 10.4230/LIPIcs...

1 Introduction

Sum-Over-Paths (SOP) is a formalism used to represent and manipulate quantum processes in a symbolic way, introduced in 2018 by Amy [3]. Its first important feature is its capacity to translate from most common descriptions of quantum processes in polynomial time and space. The formalism hence provides a intermediary view between usual (matrix) semantics and these usual process descriptions. Its second crucial feature is that it comes equipped with a rewrite system that simplifies the term, without altering its semantics.

Despite its links [17, 18] with graphical languages such as the ZH-Calculus [4] – which will be used in the following –, it provides a different view on the quantum processes, representing them as weighted sums of Dirac kets and bras (a very familiar notation in quantum mechanics).

The formalism has seen several applications, the first of which being verification. Verification is a crucial aspect of computations in the quantum realm, where physical constraints (like no-cloning, or the fundamental probabilistic nature of quantum) make it impossible to do debugging the way we do on classical algorithms. More specifically, the SOP formalism was introduced as a solution to circuit equivalence: To check the equivalence between two circuits $\mathcal{C}_1$ and $\mathcal{C}_2$, the system represents $\mathcal{C}_2^\dagger \circ \mathcal{C}_1$ as an SOP term (where $\mathcal{C}_2^\dagger$ can be seen as the inverse of $\mathcal{C}_2$, easy to describe from it). It then tries to reduce it to the identity. If successful, this shows $\mathcal{C}_1$ and $\mathcal{C}_2$ to represent the same unitary. Otherwise, the system searches for a witness that the term at hand does not represent the identity. As such, the system has been used in several different projects (e.g. [11, 15]) to check precisely for circuit equivalence. It was later extended to account for families of morphisms and used within environment Qbricks

[7, 8] together with automated solvers to verify algorithms and routines such as quantum phase estimation, Grover's search and Shor's algorithm.

Amongst other applications of the Sum-Over-Paths, we may cite noiseless simulation of quantum processes, where the rewrite strategy is used to reduce the number of variables in the term, effectively decreasing the number of summands when expanding the term to actually compute its semantics. It is for instance one of the simulators implemented in the supercomputer Atos QLM [13].

While the initial suggestion for Sum-Over-Paths focussed on the Clifford+T fragment – a universal fragment of quantum computing, i.e. a restriction still capable of approximating with arbitrary precision any quantum process –, it also provided some interesting result for the Clifford fragment. It is known that the latter is not universal [1], and actually efficiently simulable with a classical computer, so it is a good test for the relevance of a formalism to check how it handles them. And indeed, it was shown [3] a "weak" form of confluence of the rewrite system in the Clifford fragment. More precisely, in this fragment, $\mathcal{C}_2^\dagger \circ \mathcal{C}_1$ reduces (in polynomial time) to the identity if and only if $\mathcal{C}_2$ and $\mathcal{C}_1$ represent the same unitary operator.

However, SOP terms may represent more than unitary operator, but actually any linear map. With those, it is still possible to define the above restrictions, and the rewrite system was extended in [25] to get confluence for the – not necessarily unitary – Clifford fragment. When moving to a universal fragment – like Clifford+T – it is expected that we cannot provide a rewrite system with all the good properties of the Clifford case: either reduction is not polynomial, or there is no confluence, or we need an infinite number of rewrites, ... The reason for this is that if we could provide such a system, circuit equivalence would become polynomial, while we know that it is QMA-complete – a quantum variant of NP-complete – [6, 14]. A weaker property than that of confluence we can ask for is completeness: the question here is to decide whether two equivalent terms can be turned into one another, *with the assumption that rewrites can be used in both directions* (in that case, we rather speak of an equational theory, or axiomatisation, than a rewrite system).

Contributions. In this paper, we address the problem of completeness first for arguably the simplest universal fragment of quantum computing, which is *Toffoli-Hadamard*. We provide a fairly simple rewrite system that we show complete for the fragment, and also exhibit two important drawbacks: the non-confluence of the rewrite strategy and the potential explosion of the size of the morphisms during the rewrite. We then show how the rewrite strategy can be tweaked to reach completeness for every dyadic fragment – where we allow phase gates with phase a multiple of $\frac{\pi}{2^k}$ for some k –, a restriction that encompasses Clifford, Clifford+T and Toffoli-Hadamard, and is crucially used in the Quantum Fourier Transform, a central block for algorithms such as Shor's and Quantum Phase Estimation.

Structure of the paper. After reviewing the Sum-Over-Paths formalism in Section 2, the ZH-Calculus in Section 3 and the links between the two in Section 4, we show the completeness result for the Toffoli-Hadamard fragment in Section 5. The extension to the dyadic fragments is then handled in Section 6.
The missing proofs can be found in the appendix.

2 Sums-Over-Paths

2.1 The Morphisms

Sums-Over-Paths [3] are a way to symbolically describe linear maps of dimensions powers of 2 over the complex numbers. These linear maps form a †-compact monoidal category

[19, 21] denoted **Qubit** where the objects are natural numbers (this makes the category a PROP [16, 26]), where morphisms from n to m are linear maps $\mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$, and where $(\cdot \circ \cdot)$ (resp. $(\cdot \otimes \cdot)$) is the usual composition (resp. tensor product) of linear maps. The category is endowed with a *symmetric braiding* $\sigma_{n,m} : n+m \to m+n$, as well as a *compact structure* $(\eta_n : 0 \to 2n, \epsilon_n : 2n \to 0)$. Furthermore, there exists an inductive contravariant endofunctor $(\cdot)^\dagger$, that behaves properly with the symmetric braiding and the compact structure. For more information on these structures, see [21].

The formalism of SOP relies heavily on the Dirac notation for quantum states and operators of **Qubit**. The two canonical states of a single qubit are denoted $|0\rangle$ and $|1\rangle$. They form a basis of $\mathbb{C}^2$, and can be viewed as vectors $|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}^\intercal$ and $|1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}^\intercal$. A 1-qubit state is then merely a normalised linear combination of these two elements. Using $(\cdot \otimes \cdot)$, they can be used to build the basis states of larger systems, e.g. $|010\rangle := |0\rangle \otimes |1\rangle \otimes |0\rangle$ is a basis state of a 3-qubit system. Again, the state of an arbitrary n-qubit system is a normalised linear combination of the 2^n basis states. We will use extensively the following notation $\langle x|$ to represent the dagger (transpose conjugate) of $|x\rangle$. The identity on a qubit can then be expressed in Dirac notation as $\mathbb{I} := |0\rangle\langle 0| + |1\rangle\langle 1|$, where $|x\rangle\langle y| := |x\rangle \circ \langle y|$.

We give in the following the definition of Sum-Over-Paths of [25], which differs from [3] in the way the input qubits are treated, by making them more symmetric with the outputs. This makes some concepts, like the † or the compact structure, more natural.

▶ **Definition 1 (SOP).** *We define* **SOP** *as the collection of objects* $\mathbb{N}$ *and morphisms between them that are tuples* $f : n \to m := (s, \vec{y}, P, \vec{O}, \vec{I})$*, which we write:* $s \sum_{\vec{y} \in V^k} e^{2i\pi P(\vec{y})} \left|\vec{O}(\vec{y})\right\rangle\!\left\langle\vec{I}(\vec{y})\right|$

where $s \in \mathbb{R}$*,* $\vec{y} \in V^k$ *with* V *a set of variables,* $P \in \mathbb{R}[X_1, \ldots, X_k]/(X_i^2 - X_i)$ *is called the* phase polynomial *of* [1]*,* $\vec{O} \in (\mathbb{F}_2[X_1, \ldots, X_k])^m$ *and* $\vec{I} \in (\mathbb{F}_2[X_1, \ldots, X_k])^n$ *–* $\mathbb{F}_2$ *being the binary field, whose only two elements are its additive and multiplicative identities, denoted* 0 *and* 1*.*

Compositions are obtained as[2]*:*

- $f \circ g := \frac{s_f s_g}{2^m} \sum_{\substack{\vec{y}_f, \vec{y}_g \\ \vec{y} \in V^m}} e^{2i\pi\left(P_g + P_f + \frac{\vec{O}_g \cdot \vec{y} + \vec{I}_f \cdot \vec{y}}{2}\right)} \left|\vec{O}_f\right\rangle\!\left\langle\vec{I}_g\right|$ *where* $m = \left|\vec{I}_f\right| = \left|\vec{O}_g\right|$
- $f \otimes g := s_f s_g \sum_{\vec{y}_f, \vec{y}_g} e^{2i\pi(P_g + P_f)} \left|\vec{O}_f \vec{O}_g\right\rangle\!\left\langle\vec{I}_f \vec{I}_g\right|$

We distinguish particular morphisms:

- *Identity morphisms* $id_n : \sum_{\vec{y} \in V^n} |\vec{y}\rangle\langle\vec{y}|$
- *Symmetric braidings* $\sigma_{n,m} = \sum_{\vec{y}_1, \vec{y}_2} |\vec{y}_2, \vec{y}_1\rangle\langle\vec{y}_1, \vec{y}_2|$
- *Morphisms for compact structure* $\eta_n = \sum_{\vec{y}} |\vec{y}, \vec{y}\rangle\langle|$ *and* $\epsilon_n = \sum_{\vec{y}} |\rangle\langle\vec{y}, \vec{y}|$

We also distinguish two functors that have **SOP** *as a domain:*

- *The* †*-functor is given by:* $f^\dagger := s \sum_{\vec{y}} e^{-2i\pi P} \left|\vec{I}\right\rangle\!\left\langle\vec{O}\right|$

---

[1] The quotient in the phase polynomial means that we consider each occurrence of the square of a variable to be equal to the variable itself $X_i^2 - X_i = 0$, since they will be evaluated over $\{0, 1\}$. We can further constrain the polynomial by taking it modulo 1, but only when considered as an element of a group, once all the products have been evaluated, as otherwise all phase polynomials would be evaluated to 0 as $P = P \times 1 = P \times 0 = 0$.

[2] To avoid further clutter, we may not specify the variables of polynomials, e.g. P_g actually stands for $P_g(\vec{y}_g)$, $\vec{O}_g$ for $\vec{O}_g(\vec{y}_g)$ etc...

- *The functor* $[\![\cdot]\!] : \mathbf{SOP} \to \mathbf{Qubit}$ *is defined as:* $[\![f]\!] := s \sum_{\vec{y} \in \{0,1\}^k} e^{2i\pi P(\vec{y})} \left|\vec{O}(\vec{y})\right\rangle\!\left\langle \vec{I}(\vec{y})\right|$

The †-functor is particularly important to characterise maps that are unitary – the pure transformations that are allowed by quantum mechanics: f is called unitary if $[\![f^\dagger \circ f]\!] = id$.

▶ **Example 2.** The Hadamard and Toffoli gates (which justify the name of the first fragment we will consider in the following), can be represented in this formalism as:

$$H := \frac{1}{\sqrt{2}} \sum_{y_0,y_1} e^{2i\pi \frac{y_0 y_1}{2}} |y_1\rangle\langle y_0| \qquad \text{Tof} := \sum_{y_0,y_1,y_2} |y_0, y_1, y_2 \oplus y_0 y_1\rangle\langle y_0, y_1, y_2|$$

It can be checked that both operators are unitary.

As is customary, we consider equality of the SOP morphisms up to α-conversion, i.e. renaming of the variables. Notice that the definition of the composition $(\cdot \circ \cdot)$ gets somewhat involved. This is to cope with the way we deal with the inputs, which can be any boolean polynomial. The additional terms $\frac{\vec{O}_g \cdot \vec{y} + \vec{I}_f \cdot \vec{y}}{2}$ enforce that $O_{gi} = I_{fi}$ for all $0 \leq i < m$. Indeed, when summing over the variable y_i, we get $(1 + e^{i\pi(O_{gi} + I_{fi})})$ – which is non-null only when $O_{gi} = I_{fi}$ – as a factor of the whole morphism. This presentation has the advantage of keeping the size of the morphism polynomial with the size of the quantum circuit – or ZH-diagram, see below – it can be built from, no matter what gate set is used. A downside, however, is that the above does not directly constitute a category, as for instance $id \circ id \neq id$. However, it suffices to quotient the formalism with rewrite rules to turn it into a proper category [25], hence justifying the use of the term "functor" for the last two maps.

2.2 A Rewrite System

We hence give in Figure 1 a set of rewrite rules denoted $\xrightarrow[\text{TH}]{}$ that induces an equational theory $\underset{\text{TH}}{\sim}$ (the symmetric and transitive closure of $\xrightarrow[\text{TH}]{}$).

We need in the conditions of all the rules the function Var, that, given a set or list of polynomials, gives the set of all variables used in them. We call *internal variable* a variable that is present in the morphism t but not in its inputs/outputs, i.e. a variable y_0 such that $y_0 \in \text{Var}(t) \setminus \text{Var}(\vec{O}, \vec{I})$. It is worth noting that searching for an occurrence of, and applying any of these rules *once* can be done in polynomial time.

The rules (ket) and (bra) correspond to changes of variables that are necessary to get a unique normal form in the Clifford case [25], and the rule (Elim) simply gets rid of a variable that is used nowhere in the term and simply contributes to a global phase (since that variable is supposed to range over two values, it contributes to a multiplicative scalar 2).

The rules (HHgen), (HHnl) and (Z) all stem from a particular observation: In the morphism $t = \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q} + R\right)} \left|\vec{O}\right\rangle\!\left\langle \vec{I}\right|$ where y_0 is internal and not in R, if Q is evaluated to 1, then the whole morphism is interpreted as null. This is exactly what (Z) captures – and the conditions on R, $\vec{O}$ and I are simply here to avoid applying the rule indefinitely.

The rule (HHgen) deals with a case where the polynomial Q can be forced to 0, whilst the rule (HHnl) factorises different such polynomials Q into one.

▶ Remark 3. When performing certain rules, we have to substitute a variable by a boolean polynomial Q. We need to be able to understand Q as a phase polynomial, as the variable can occur in P. The map $\widehat{(\cdot)} : \mathbb{F}_2[X_1, \ldots, X_k] \to \mathbb{R}[X_1, \ldots, X_k]/(X_i^2 - X_i)$, serves this purpose. It is inductively defined as:

$$\widehat{Q_1 Q_2} = \widehat{Q_1}\widehat{Q_2} \qquad \widehat{Q_1 \oplus Q_2} = \widehat{Q_1} + \widehat{Q_2} - 2\widehat{Q_1}\widehat{Q_2} \qquad \widehat{y_i} = y_i \qquad \widehat{\alpha} = \alpha$$

$$\sum_{\vec{y}} e^{2i\pi P} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[y_0 \notin \mathrm{Var}(P,\vec{O},\vec{I})]{} 2 \sum_{\vec{y}\setminus\{y_0\}} e^{2i\pi P} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \tag{Elim}$$

$$t = \sum e^{2i\pi\left(\frac{y_0}{2}(y_i\widehat{Q}+\widehat{Q'}+1)+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[\substack{y_0 \notin \mathrm{Var}(Q,Q',R,\vec{O},\vec{I}) \\ y_i \notin \mathrm{Var}(Q,Q') \\ QQ'=Q'}]{} t[y_i \leftarrow 1 \oplus Q'] \tag{HHgen}$$

$$t = \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q}+\frac{y'_0}{2}\widehat{Q'}+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[y_0,y'_0 \notin \mathrm{Var}(Q,Q',R,\vec{O},\vec{I})]{} 2t[y'_0 \leftarrow y_0 \oplus y_0 Q] \tag{HHnl}$$

$$t = \sum_{\vec{y}} e^{2i\pi(P)} |\cdots, \overbrace{y_0 \oplus O'_i}^{O_i}, \cdots\rangle\!\left\langle\vec{I}\right| \xrightarrow[\substack{O'_i \neq 0 \\ y_0 \notin \mathrm{Var}(O_1,\ldots,O_{i-1},O'_i)}]{} t[y_0 \leftarrow O_i] \tag{ket}$$

$$t = \sum_{\vec{y}} e^{2i\pi(P)} \left|\vec{O}\right\rangle\!\langle\cdots, \overbrace{y_0 \oplus I'_i}^{I_i}, \cdots| \xrightarrow[\substack{I'_i \neq 0 \\ y_0 \notin \mathrm{Var}(\vec{O},I_1,\ldots,I_{i-1},I'_i)}]{} t[y_0 \leftarrow I_i] \tag{bra}$$

$$s \sum_{\vec{y}} e^{2i\pi\left(\frac{y_0}{2}+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[\substack{R\neq 0 \text{ or } \vec{O},\vec{I}\neq\vec{0} \\ y_0 \notin \mathrm{Var}(R,\vec{O},\vec{I})}]{} \sum_{y_0} e^{2i\pi\left(\frac{y_0}{2}\right)} |0,\cdots,0\rangle\langle 0,\cdots,0| \tag{Z}$$

Figure 1 Rewrite system $\xrightarrow[\mathrm{TH}]{}$

▶ Remark 4. When rewriting SOP-morphisms for simplification or verification, it can be beneficial to not only reduce the number of variables – which is what all rules but (ket/bra) do –, but also to keep the size of the phase polynomial as short as possible. In that respect, the rule (HHgen) can be generalised to:

$$t = \sum e^{2i\pi\left(\frac{y_0}{2}(y_i\widehat{Q}+\widehat{QQ'}+1)+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[\substack{y_0 \notin \mathrm{Var}(Q,Q',R,\vec{O},\vec{I}) \\ y_i \notin \mathrm{Var}(Q,Q')}]{} t[y_i \leftarrow 1 \oplus Q'] \tag{HHgen'}$$

where the polynomial Q' can here be smaller (in the number of terms) than the one in (HHgen). However, finding a "minimal" Q' for this rule is a hard problem, as it requires the use of boolean Groebner bases [20]. (HHgen) can be seen as a particular case of (HHgen'), where $Q' \leftarrow QQ'$, as $Q \times QQ' = QQ'$. The rule (HHgen) is sufficient for the scope of this paper.

In [3] was introduced a particular and important rule:

$$t = \sum e^{2i\pi\left(\frac{y_0}{2}(y_i+\widehat{Q})+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[\substack{y_0 \notin \mathrm{Var}(Q,R,\vec{O},\vec{I}) \\ y_i \notin \mathrm{Var}(Q)}]{} 2 \sum e^{2i\pi R[y_i \leftarrow \widehat{Q}]} \left(\left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|\right)[y_i \leftarrow Q] \tag{HH}$$

This one is a particular case of the rule (HHgen) (with additional use of the rule (Elim)), where $Q \leftarrow 1$, $Q' \leftarrow Q \oplus 1$. Moreover, the rule gave enough power to the formalism to become a †-compact PROP [25]. We can extend this result here thanks to:

▶ **Proposition 5.**

$$\forall t_1, t_2 \in \mathbf{SOP}, \quad t_1 \underset{\mathrm{TH}}{\sim} t_2 \implies \begin{cases} A \circ t_1 \circ B \underset{\mathrm{TH}}{\sim} A \circ t_2 \circ B & \textit{for all } A,\ B \textit{ composable} \\ A \otimes t_1 \otimes B \underset{\mathrm{TH}}{\sim} A \otimes t_2 \otimes B & \textit{for all } A,\ B \end{cases}$$

Proof. In appendix at page 17. ◀

Thanks to this Proposition, and since $\mathbf{SOP}/\underset{\text{HH}}{\sim}$ is a †-compact PROP by [25], we get:

▶ **Corollary 6.** $\mathbf{SOP}/\underset{\text{TH}}{\sim}$ *is a* †*-compact PROP.*

The set of rules was obviously chosen so as to preserve the semantics:

▶ **Proposition 7** (Soundness). *For any two* **SOP** *morphisms* t_1 *and* t_2*, if* $t_1 \xrightarrow[\text{TH}]{*} t_2$*, then* $[\![t_1]\!] = [\![t_2]\!]$.

Proof. In appendix at page 18. ◀

▶ **Example 8.** The following morphism:

$$\sum_{\vec{y}} e^{2i\pi(\frac{y_0y_1y_2}{2}+\frac{y_2}{2}+\frac{y_2y_3y_4}{2})} |y_4\rangle\langle y_0|$$

is irreducible using the rules of [3] and [25]. However, here it can be reduced to:

$$\sum_{y_0,y_1,y_2,y_3,y_4} e^{2i\pi(\frac{y_0y_1y_2}{2}+\frac{y_2}{2}+\frac{y_2y_3y_4}{2})} |y_4\rangle\langle y_0|$$

$$\xrightarrow[y_3\leftarrow y_1\oplus y_0y_1y_2]{\text{(HHnl)}} 2 \sum_{y_0,y_1,y_2,y_4} e^{2i\pi(\frac{y_0y_1y_2}{2}+\frac{y_2}{2}+\frac{y_1y_2y_4}{2}+\frac{y_0y_1y_2y_4}{2})} |y_4\rangle\langle y_0|$$

$$\xrightarrow[y_1\leftarrow 1]{\text{(HHgen)}} 2 \sum_{y_0,y_2,y_4} e^{2i\pi(\frac{y_0y_2}{2}+\frac{y_2}{2}+\frac{y_2y_4}{2}+\frac{y_0y_2y_4}{2})} |y_4\rangle\langle y_0|$$

The first rewrite can be made clearer by writing the phase polynomial as $\frac{y_1}{2}(y_0y_2)+\frac{y_3}{2}(y_2y_4)+\frac{y_2}{2}$, and the second one by writing it as $\frac{y_2}{2}(y_1(y_0+y_4+y_0y_4)+0+1)$. Recall that variables are binary variables, so $y_i^2 = y_i$.

3 The ZH-Calculus

The graphical calculi ZX, ZW and ZH [4, 9, 10] are calculi for quantum computing, with a tight link with the Sum-Over-Paths formalism [17, 18, 25], and whose completeness was proven in particular for the Toffoli-Hadamard fragment [5, 12, 23, 24].

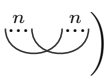
This fragment of quantum mechanics is approximately universal [2, 22], and it is arguably the simplest one with this property. This is the fragment we will be interested in, in most of the following of the paper; and the associated completeness result will be paramount in the development of the following.

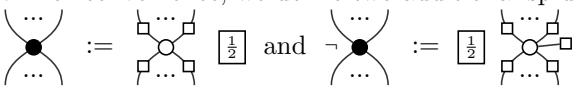
We choose to present here the ZH-Calculus, because of its proximity with both **SOP** and the Toffoli-Hadamard fragment. Notice however that there exist translations between all the aforementioned graphical calculi, so by composition, we can connect **SOP** to all of them.

ZH is a PROP whose morphisms – read here from top to bottom – are composed (sequentially $(\cdot \circ \cdot)$ or in parallel $(\cdot \otimes \cdot)$) from Z-spiders and H-spiders:

- $Z^n_m : n \to m ::$  , called Z-spider
- $H^n_m(r) : n \to m ::$  , called H-spider, with a parameter $r \in \mathbb{C}$

When r is not specified, the parameter in the H-spider is taken to be -1.

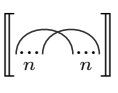
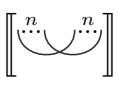
ZH is made a †-compact PROP, which means it also has a symmetric structure $\sigma_{n,m} ::$  , a compact structure $\left(\eta_n :: \right.$  , $\left.\epsilon_n :: \right.$  $\left.\right)$, and a †-functor $(\cdot)^\dagger : \mathbf{ZH}^{\mathrm{op}} \to \mathbf{ZH}$. It is defined by: $(Z^n_m)^\dagger := Z^m_n$ and $(H^n_m(r))^\dagger := H^m_n(\overline{r})$ where $\overline{r}$ is the complex conjugate of r. For convenience, we define two additional spiders:

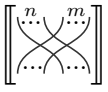


The language comes with a way of interpreting the morphisms as morphisms of **Qubit**. The standard interpretation $[\![\cdot]\!] : \mathbf{ZH} \to \mathbf{Qubit}$ is a †-compact-PROP-functor, defined as:


$= |0^m\rangle\langle 0^n| + |1^m\rangle\langle 1^n|$ 
$= |0\rangle\langle 0| + |1\rangle\langle 1|$


$= \sum_{j_k, i_k \in \{0,1\}} r^{j_1 \dots j_m i_1 \dots i_n} |j_1, \dots, j_m\rangle\langle i_1, \dots, i_n|$


$= \sum_{i_k \in \{0,1\}} |i_1, \dots, i_n, i_1, \dots, i_n\rangle =$  †

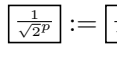

$= \sum_{i_k, j_k \in \{0,1\}} |j_1, \dots, j_m, i_1, \dots, i_n\rangle\langle i_1, \dots, i_n, j_1, \dots, j_m|$

Notice that we used the same symbol for two different functors: the two interpretations $[\![\cdot]\!] : \mathbf{SOP} \to \mathbf{Qubit}$ and $[\![\cdot]\!] : \mathbf{ZH} \to \mathbf{Qubit}$. It should be clear from the context which one is to be used.

The language is universal: $\forall f \in \mathbf{Qubit}$, $\exists D_f \in \mathbf{ZH}$, $[\![D_f]\!] = f$. In other words, the interpretation $[\![\cdot]\!]$ is surjective.

The language comes with an equational theory, which in particular gives the axioms for a †-compact PROP. We will not present it here.

We can easily define a restriction of **ZH** that exactly captures the Toffoli-Hadamard fragment of quantum mechanics [5, 23], as the language generated by:  .

Notice that the two black spiders can still be defined if we also define  $:=$ $^{\otimes p}$. We denote this restriction by $\mathbf{ZH}_{\mathrm{TH}}$.

This restriction is provided with an equational theory, given in Figure 2[3], that makes it complete.

▶ **Theorem 9** ([23] Completeness of $\mathbf{ZH}_{\mathrm{TH}}$/ $\mathrm{ZH}_{\mathrm{TH}}$).

$$\forall D_1, D_2 \in \mathbf{ZH}_{\mathrm{TH}}, \quad [\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZH}_{\mathrm{TH}} \vdash D_1 = D_2$$

[3] The axiomatisation provided here is that of [23]. It was later simplified in [5] in a fragment that is very close to the one we consider, but does *not* contain the scalar $\frac{1}{\sqrt{2}}$. As we would rather have this scalar in the language (to properly represent the Hadamard gate), instead of giving a mix of the two axiomatisation, we decided to stick to the first one.

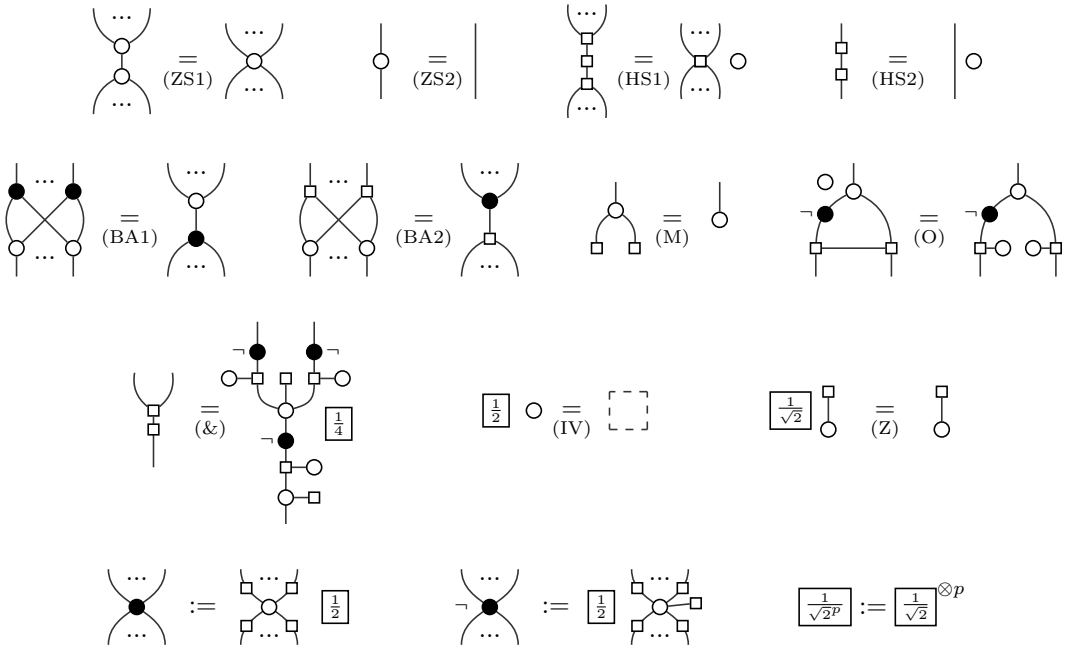


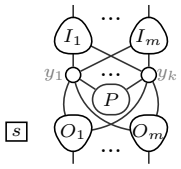
Figure 2 Set of rules $\mathrm{ZH}_{\mathrm{TH}}$ [23].

4 Translations between SOP and ZH

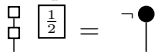
4.1 From SOP to ZH

It is possible to translate **SOP** morphisms to ZH-diagrams using interpretation $[\cdot]^{\mathrm{ZH}} : \mathbf{SOP} \to \mathbf{ZH}$. A description of $[\cdot]^{\mathrm{ZH}} : \mathbf{SOP} \to \mathbf{ZH}$ was defined in [17, 18] and in [25]. We choose the latter definition as it fits our definition of **SOP**.

$$\left[s \sum_{\vec{y}} e^{2i\pi P} \, |O_1, \ldots, O_m\rangle\langle I_1, \ldots, I_n| \right]^{\mathrm{ZH}} :=$$



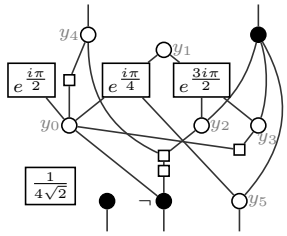
where the row of Z-spiders represents the variables $y_1, \ldots, y_k$. Informally:

- each monomial $\alpha y_{i_1} \ldots y_{i_s}$ in P gives a single H-spider with parameter $e^{i\frac{\alpha}{2\pi}}$ and connected to the Z-spiders that represent y_{i_1},...,y_{i_s}
- each monomial $y_{i_1} \ldots y_{i_s}$ in O_i is represented by  where the inputs are connected to the Z-spiders that represent y_{i_1},...,y_{i_s}. Notice that the only (non-zero) constant monomial is 
- these monomials are then added to form O_i thanks to 
- the nodes I_i are defined similarly, but upside-down

For more details, see [25].

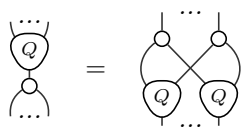
▶ **Example 10.** The **SOP** morphism:

$$\frac{1}{2\sqrt{2}} \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0 + \frac{1}{2}y_4y_0 + \frac{1}{8}y_5y_0y_1 + \frac{3}{4}y_1y_2y_3 + \frac{1}{2}y_0y_3\right)} \, |0, 1 \oplus y_0 \oplus y_4y_2, y_5\rangle\langle y_4, y_5 \oplus y_2 \oplus y_3|$$

is mapped to 

The boolean polynomials as defined above are given in their (unique) expanded form. These can easily be shown to be copied through the white node:

▶ **Lemma 11.**



Proof. In appendix at page 19. ◀

This translation preserves the semantics:

▶ **Proposition 12** ([25]). $[\![[\cdot]^{\mathrm{ZH}}]\!] = [\![\cdot]\!]$.

4.2 From ZH to SOP

Any **ZH**-diagram can be understood as a **SOP**-morphism. To do so, we use the PROP-functor $[\cdot]^{\mathrm{sop}} : \mathbf{ZH} \to \mathbf{SOP}$ defined as:

$$\left[\begin{array}{c}\vdots\\ e^{i\alpha}\\ \vdots\end{array}\right]^{\mathrm{sop}} := \sum e^{2i\pi\frac{\alpha}{2\pi}x_1\dots x_n y_1\dots y_m}\,|y_1,\dots,y_m\rangle\langle x_1,\dots,x_n|$$

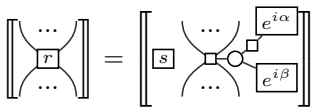
$$[\,\boxed{s}\,]^{\mathrm{sop}} := s\,|\rangle\langle| \qquad \text{for } s\in\mathbb{R}$$

$$\left[\begin{array}{c}\vdots\\ \\ \vdots\end{array}\right]^{\mathrm{sop}} := \sum_y |y,\dots,y\rangle\langle y,\dots,y| \qquad \left[\begin{array}{c}\vdots\\ \boxed{0}\\ \vdots\end{array}\right]^{\mathrm{sop}} := \left[\begin{array}{c}\vdots\\ \boxed{\frac{1}{2}}\\ \vdots\end{array}\right]^{\mathrm{sop}}$$

The functor furthermore maps the symmetric braiding (resp. the compact structure) of **ZH** to the symmetric braiding (resp. the compact structure) of **SOP**.

This does not give a full description of $[\cdot]^{\mathrm{sop}}$, as we did not describe the interpretation of the H-spider for all parameters, but only for phases and 0. However, any H-spider can be decomposed using the previous ones:

▶ **Lemma 13.** *For any $r\in\mathbb{C}$ such that $|r|\notin\{0,1\}$, there exist $s\in\mathbb{C}$, $\alpha,\beta\in\mathbb{R}$ such that:*



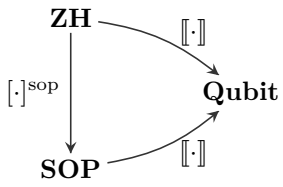
Proof. In appendix, at page 19. ◀

As a consequence, we extend the definition of $[\cdot]^{\mathrm{sop}}$ by:

$$\left[\begin{array}{c}\vdots\\ \boxed{r}\\ \vdots\end{array}\right]^{\mathrm{sop}} := \left[\begin{array}{c}\boxed{e^{i\alpha}}\\ \boxed{s}\ \vdots\\ \boxed{e^{i\beta}}\end{array}\right]^{\mathrm{sop}}$$

This interpretation of ZH-diagrams as **SOP**-morphisms preserves the semantics:

▶ **Proposition 14** ([25]). $[\![[\cdot]^{\mathrm{sop}}]\!] = [\![\cdot]\!]$. *In other words, the following diagram commutes:*



The composition of the two interpretations is the identity up to small rewrites:

▶ **Proposition 15** ([25]). $\left[[\cdot]^{\mathrm{ZH}}\right]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} (\cdot)$

4.3 Restrictions of SOP

Recall that $\mathbf{ZH}_{\mathrm{TH}}$ exactly captures the Toffoli-Hadamard fragment of quantum mechanics. We can then use the two interpretations to define the Toffoli-Hadamard fragment of **SOP**. We actually go a step beyond and define a family of fragments indexed by n:

▶ **Definition 16** ($\mathbf{SOP}[\frac{1}{2^n}]$). *We define* $\mathbf{SOP}[\frac{1}{2^n}]$ *as the restriction of* **SOP** *to morphisms of the form:* $t = \frac{1}{\sqrt{2}^p} \sum e^{2i\pi \frac{P}{2^n}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$ *where* $p \in \mathbb{Z}$ *and* P *has integer coefficients.*

The Toffoli-Hadamard fragment is then the first such restriction ($n = 1$):

▶ **Proposition 17.** $\mathbf{SOP}[\frac{1}{2}]$ *captures exactly the Toffoli-Hadamard fragment of quantum mechanics.*

Proof. We can prove this by showing that $[\mathbf{ZH}_{\mathrm{TH}}]^{\mathrm{sop}} \subseteq \mathbf{SOP}[\frac{1}{2}]$ and that $\left[\mathbf{SOP}[\frac{1}{2}]\right]^{\mathrm{ZH}} \subseteq \mathbf{ZH}_{\mathrm{TH}}$. The two claims are straightforward verifications, and use the fact that compositions of $\mathbf{SOP}[\frac{1}{2}]$-morphisms give $\mathbf{SOP}[\frac{1}{2}]$-morphisms.
Then, $[\![\mathbf{ZH}_{\mathrm{TH}}]\!] = [\![[\mathbf{ZH}_{\mathrm{TH}}]^{\mathrm{sop}}]\!] \subseteq \left[\!\left[\mathbf{SOP}[\frac{1}{2}]\right]\!\right] = \left[\!\left[\left[\mathbf{SOP}[\frac{1}{2}]\right]^{\mathrm{ZH}}\right]\!\right] \subseteq [\![\mathbf{ZH}_{\mathrm{TH}}]\!]$, so:

$$\left[\!\left[\mathbf{SOP}[\tfrac{1}{2}]\right]\!\right] = [\![\mathbf{ZH}_{\mathrm{TH}}]\!]$$ ◀

Notice in particular that the Hadamard and Toffoli gates given in Example 2 lie in this fragment. Not all of $\mathbf{SOP}[\frac{1}{2}]$ can be generated by these two gates however, as $\mathbf{SOP}[\frac{1}{2}]$ comprises linear maps that are not unitary, i.e. such that $[\![t^\dagger \circ t]\!] \neq id$.

5 Completeness for Toffoli-Hadamard

In this section, we aim to show that the set of rules $\underset{\mathrm{TH}}{\longrightarrow}$ captures the whole Toffoli-Hadamard fragment of quantum mechanics. We do so by transporting the similar result from $\mathbf{ZH}_{\mathrm{TH}}$ to $\mathbf{SOP}[\frac{1}{2}]$. First, we show:

▶ **Proposition 18.** $\forall D_1, D_2 \in \mathbf{ZH}_{\mathrm{TH}}, \quad \mathrm{ZH}_{\mathrm{TH}} \vdash D_1 = D_2 \implies [D_1]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} [D_2]^{\mathrm{sop}}$

Proof. In appendix at page 20. ◀

We can then use the previous proposition to show the main result of this paper:

▶ **Theorem 19.** $\mathbf{SOP}[\frac{1}{2}]/\underset{\mathrm{TH}}{\sim}$ *is complete, i.e.:* $\forall t_1, t_2 \in \mathbf{SOP}[\frac{1}{2}], \quad [\![t_1]\!] = [\![t_2]\!] \iff t_1 \underset{\mathrm{TH}}{\sim} t_2$

Proof. Let t_1 and t_2 be two $\mathbf{SOP}[\frac{1}{2}]$-morphisms such that $[\![t_1]\!] = [\![t_2]\!]$. By Proposition 12: $[\![[t_1]^{\mathrm{ZH}}]\!] = [\![[t_2]^{\mathrm{ZH}}]\!]$.
By completeness of $\mathbf{ZH}_{\mathrm{TH}}/\,\mathrm{ZH}_{\mathrm{TH}}$ (Theorem 9): $\mathrm{ZH}_{\mathrm{TH}} \vdash [t_1]^{\mathrm{ZH}} = [t_2]^{\mathrm{ZH}}$
Thanks to Proposition 18: $\left[[t_1]^{\mathrm{ZH}}\right]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} \left[[t_2]^{\mathrm{ZH}}\right]^{\mathrm{sop}}$. Finally, by Proposition 15:

$$t_1 \underset{\mathrm{TH}}{\sim} \left[[t_1]^{\mathrm{ZH}}\right]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} \left[[t_2]^{\mathrm{ZH}}\right]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} t_2 \qquad \blacktriangleleft$$

The rewrite system is however not sufficient to get to a unique normal form, as:

▶ **Lemma 20** (Non-Confluence). *The rewrite system* $\underset{\mathrm{TH}}{\longrightarrow}$ *is not confluent.*

Proof. The $\mathbf{SOP}[\frac{1}{2}]$-morphism: $t = \sum e^{2i\pi\left(\frac{1}{2}y_0y_6+\frac{1}{2}y_8y_9y_6+\frac{1}{2}y_4y_5y_6+\frac{1}{2}y_8y_9y_{12}\right)}\,|y_0\rangle$
can be reduced to (at least) three different non-reducible morphisms:

- $t \xrightarrow[\mathrm{HH}(y_6,[y_0\leftarrow y_4y_5\oplus y_8y_9])]{} 2\sum e^{2i\pi\left(\frac{1}{2}y_8y_9y_{12}\right)}\,|y_4y_5\oplus y_8y_9\rangle$
- $t \xrightarrow[\mathrm{HHnl}(y_4,y_8)]{} 2\sum e^{2i\pi\left(\frac{1}{2}y_9y_4y_5y_6+\frac{1}{2}y_0y_6+\frac{1}{2}y_9y_4y_6+\frac{1}{2}y_9y_{12}y_4+\frac{1}{2}y_4y_5y_6y_9y_{12}+\frac{1}{2}y_4y_5y_6\right)}\,|y_0\rangle$

  $\xrightarrow[\mathrm{HH}(y_6,[y_0\leftarrow y_9y_{12}y_4y_5\oplus y_9y_4\oplus y_9y_4y_5\oplus y_4y_5])]{} 4\sum e^{2i\pi\left(\frac{1}{2}y_9y_{12}y_4\right)}\,|y_9y_{12}y_4y_5\oplus y_9y_4\oplus y_9y_4y_5\oplus y_4y_5\rangle$
- $t \xrightarrow[\mathrm{HHnl}(y_6,y_{12})]{} 2\sum e^{2i\pi\left(\frac{1}{2}y_0y_8y_9y_6+\frac{1}{2}y_0y_6+\frac{1}{2}y_8y_9y_6+\frac{1}{2}y_4y_5y_6y_8y_9+\frac{1}{2}y_4y_5y_6\right)}\,|y_0\rangle$

  $\xrightarrow[\mathrm{HHgen}(y_6,[y_0\leftarrow y_4y_5\oplus y_8y_9\oplus y_4y_5y_8y_9])]{} 2\sum e^{2i\pi\left(\frac{1}{2}y_8y_9y_6\right)}\,|y_4y_5\oplus y_8y_9\oplus y_4y_5y_8y_9\rangle$ ◀

Another important downside is the potential explosion of the size of the phase polynomial:

▶ **Lemma 21.** *Applying (HHnl) k times in a row on an SOP morphism with phase polynomial of size $O(k)$ may give a morphism with phase polynomial of size $O(2^k)$.*

Proof. For any $k \geq 1$ we can define the following term:

$$t_k := \sum e^{2i\pi \sum_{i=0}^{k} \frac{y_{i0}}{2}(y_{i1}+y_{i2}+1)}$$

on which we can apply (HHnl) k times in a row. In that case we end up with:

$$t_k \to^k 2^k \sum e^{2i\pi\left(\frac{y_0}{2}\prod_{i=0}^{k}(y_{i1}+y_{i2})+1\right)}$$

While t_k has only $3(k+1)$ terms (each of degree at most 2) in its phase polynomial, it can rewrite into a morphism with $2^{k+1}+1$ terms (each of degree at most 3). ◀

Hence, if one were to perform simplifications with this rewrite system, they ought to give special attention as to where and in which order to apply the rules.

6 Completeness for the Dyadic Fragment

We show here how we can turn an $\mathbf{SOP}[\frac{1}{2^{n+1}}]$-morphism into an $\mathbf{SOP}[\frac{1}{2^n}]$-morphism in a "reversible" manner. This will allow us to extend the completeness result to all the restrictions $\mathbf{SOP}[\frac{1}{2^n}]$. This is particularly interesting as the phase gates with dyadic multiples of π, used in particular in the quantum Fourier transform, belong in these fragments:

$$R_Z\left(p\frac{\pi}{2^k}\right) := \sum_{y_0} e^{2i\pi\cdot\frac{p}{2^{k-1}}}\,|y_0\rangle\langle y_0|$$

6.1 Ascending the Dyadic Levels

These transformations between restrictions of **SOP** are more easily defined on **SOP**-morphisms of a particular shape, namely, when their phase polynomial is reduced to a single monomial. Because of this, we show how a **SOP**-morphism can be turned into a composition of these.

▶ **Lemma 22.** *Let* $P = \sum m_i \in \mathbb{R}[X_1, \dots, X_k]/(X_i^2 - X_i)$*, and* $t = s \sum e^{2i\pi P} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$*. Then:*

$$\left[\begin{array}{l} \left(s \sum \left|\vec{O}\right\rangle\langle y_0, ..., y_k|\right) \circ \\ \left(\sum e^{2i\pi m_1} |y_0, ..., y_k\rangle\langle y_0, ..., y_k|\right) \circ \dots \circ \left(\sum e^{2i\pi m_\ell} |y_0, ..., y_k\rangle\langle y_0, ..., y_k|\right) \\ \qquad\qquad \circ \left(\sum |y_0, ..., y_k\rangle\!\left\langle\vec{I}\right|\right) \end{array}\right] \xrightarrow[\text{HH}]{*} t$$

Notice that this decomposed form is not unique, as different orderings on the monomials of P define different orderings of the compositions. However, this will not matter.

A particular care is sadly needed for the overall scalar. Because of this, we will first focus on a slightly different notion of restriction of **SOP**.

▶ **Definition 23** (**SOP**$[\frac{1}{2^n}]'$)**.** *We define* **SOP**$[\frac{1}{2^n}]'$ *as the restriction of* **SOP** *to morphisms of the form:* $t = \frac{1}{2^p} \sum e^{2i\pi \frac{P}{2^n}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$ *where* P *has integer coefficients.*

The only difference with **SOP**$[\frac{1}{2^n}]$ is that the overall scalar is now a power of $\frac{1}{2}$ and not of $\frac{1}{\sqrt{2}}$. There always exists a **SOP**$[\frac{1}{2^n}]'$-morphism that represents the same linear map as any **SOP**$[\frac{1}{2^n}]$-morphism.

▶ **Lemma 24.** $\left[\!\left[\frac{1}{\sqrt{2}} \sum_{y_0 \in V} e^{2i\pi\left(\frac{1}{8} + \frac{3}{4} y_0\right)}\right]\!\right] = 1$*. Hence:*

$$\forall t \in \mathbf{SOP}[\tfrac{1}{2^n}],\ \exists t' \in \mathbf{SOP}[\tfrac{1}{2^{\max(3,n)}}]',\quad [\![t]\!] = [\![t']\!]$$

Proof. If $t \in \mathbf{SOP}[\frac{1}{2^n}]$ and $t \notin \mathbf{SOP}[\frac{1}{2^n}]'$, then:
$t' := t \otimes \left(\frac{1}{\sqrt{2}} \sum e^{2i\pi\left(\frac{1}{8} + \frac{3}{4} y_0\right)}\right) \in \mathbf{SOP}[\frac{1}{2^{\max(3,n)}}]'$ and $[\![t']\!] = [\![t]\!]$. ◀

We can now define the family of maps that will link the different levels of the "dyadic levels":

▶ **Definition 25.** *For any* $k \geq 1$*, we define the functor* $\lfloor \cdot \rfloor_k : \mathbf{SOP}[\frac{1}{2^{k+1}}]' \to \mathbf{SOP}[\frac{1}{2^k}]'$*, first for morphisms* $t = s \sum e^{2i\pi \frac{\ell}{2^{k+1}} y_{i_1} \dots y_{i_q}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$ *with phase polynomial of size 0 or 1:*

$$t \mapsto \begin{cases} s \sum e^{2i\pi \frac{\ell/2}{2^k} y_{i_1} \dots y_{i_q}} \left|\vec{O}, y'\right\rangle\!\left\langle\vec{I}, y'\right| = t \otimes id & \text{if } \ell \bmod 2 = 0 \\ s \sum e^{2i\pi \frac{y_{i_1} \cdots y_{i_q}}{2^k} \left((\ell-1)/2 + y'\right)} \left|\vec{O}, y'\right\rangle\!\left\langle\vec{I}, y' \oplus y_{i_1} \dots y_{i_q}\right| & \text{if } \ell \bmod 2 = 1 \end{cases}$$

The functor is then extended to any **SOP**$[\frac{1}{2^{k+1}}]'$*-morphism by the decomposition of Lemma 22 (and given a particular ordering on the monomials of the phase polynomial).*

Since $\lfloor \cdot \rfloor_k$ is defined to be a functor, we have $\lfloor \cdot \circ \cdot \rfloor_k = \lfloor \cdot \rfloor_k \circ \lfloor \cdot \rfloor_k$. We can show that the ordering of the monomials has no real importance. Indeed, suppose $t_1 = \sum e^{2i\pi \frac{\ell_1}{2^{k+1}} y_{i_1} \dots y_{i_q}} |\vec{y}\rangle\langle\vec{y}|$

and $t_2 = \sum e^{2i\pi \frac{\ell_2}{2^{k+1}} y_{j_1}\dots y_{j_r}} |\vec{y}\rangle\langle\vec{y}|$. Then: $\lfloor t_1 \circ t_2 \rfloor_k = \lfloor t_2 \circ t_1 \rfloor_k$ quite obviously when either $\ell_1 \bmod 2 = 0$ or $\ell_2 \bmod 2 = 0$, but also when $\ell_1 \bmod 2 = \ell_2 \bmod 2 = 1$:

$$\lfloor t_1 \circ t_2 \rfloor_k \underset{\text{HH}}{\longrightarrow} \sum e^{2i\pi \left(\begin{array}{c} \frac{y_{i_1}\dots y_{i_q}}{2^k}\left((\ell_1-1)/2+y'\right)+\frac{y_{j_1}\dots y_{j_r}}{2^k}\left((\ell_2-1)/2+y'\right) \\ +\frac{y_{i_1}\dots y_{i_q} y_{j_1}\dots y_{j_r}}{2^k}(1-2y') \end{array} \right)} |\vec{y}, y'\rangle\langle\vec{y}, y' \oplus y_{i_1}\dots y_{i_q} \oplus y_{j_1}\dots y_{j_r}| \underset{\text{HH}}{\longleftarrow} \lfloor t_2 \circ t_1 \rfloor_k$$

Notice however that $\lfloor \cdot \rfloor_k$ adds an input and an output, so necessarily $\lfloor \cdot \otimes \cdot \rfloor_k \neq \lfloor \cdot \rfloor_k \otimes \lfloor \cdot \rfloor_k$.

The functors $\lfloor \cdot \rfloor_k$ map terms with the same semantics to terms with the same semantics:

▶ **Proposition 26.** $\forall t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]', \quad [\![t_1]\!] = [\![t_2]\!] \implies [\![\lfloor t_1 \rfloor_k]\!] = [\![\lfloor t_2 \rfloor_k]\!]$

Proof. In appendix at page 21. ◀

6.2 Going Back

We now show how to reverse the functors $\lfloor \cdot \rfloor_k$.

▶ **Definition 27.** *For any $k \geq 1$, we define the (partial) map $\lceil \cdot \rceil_k : \mathbf{SOP}[\frac{1}{2^k}]' \to \mathbf{SOP}[\frac{1}{2^{k+1}}]'$ as:*

$$\forall t : n+1 \to m+1 \in \mathbf{SOP}[\tfrac{1}{2^k}]', \quad \lceil t \rceil_k := (id_m \otimes \langle 0|) \circ t \circ (id_n \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle)$$

Notice that $\lceil \cdot \rceil_k$ can only be applied on morphisms that have at least one input and one output.

$\lceil \cdot \rceil_k$ reverses the action of $\lfloor \cdot \rfloor_k$ (up to some rewrites):

▶ **Proposition 28.** $\lceil \lfloor \cdot \rfloor_k \rceil_k \underset{\text{TH}}{\sim} (\cdot)$ *and* $t_1 \underset{\text{TH}}{\sim} t_2 \implies \lceil t_1 \rceil \underset{\text{TH}}{\sim} \lceil t_2 \rceil$ *for any two terms t_1, t_2.*

Proof. In appendix at page 22. ◀

6.3 Completeness

We may now show completeness first for $\mathbf{SOP}[\frac{1}{2^{k+1}}]'$ and then tweak the equational theory to extend the result to $\mathbf{SOP}[\frac{1}{2^{k+1}}]$.

▶ **Theorem 29** (Completeness of $\mathbf{SOP}[\frac{1}{2^{k+1}}]'/\underset{\text{TH}}{\sim}$)**.**

$$\forall t_1, t_2 \in \mathbf{SOP}[\tfrac{1}{2^{k+1}}]', \quad [\![t_1]\!] = [\![t_2]\!] \iff t_1 \underset{\text{TH}}{\sim} t_2$$

Proof. Let $t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]'$ such that $[\![t_1]\!] = [\![t_2]\!]$. By Proposition 26:

$$[\![\lfloor \dots \lfloor t_1 \rfloor_k \dots \rfloor_1]\!] = [\![\lfloor \dots \lfloor t_2 \rfloor_k \dots \rfloor_1]\!]$$

Since $\lfloor \dots \lfloor t_i \rfloor_k \dots \rfloor_1 \in \mathbf{SOP}[\frac{1}{2}]' \subset \mathbf{SOP}[\frac{1}{2}]$, by completeness of this fragment (Theorem 19):

$$\lfloor \dots \lfloor t_1 \rfloor_k \dots \rfloor_1 \underset{\text{TH}}{\sim} \lfloor \dots \lfloor t_2 \rfloor_k \dots \rfloor_1$$

Finally, by Proposition 28: $t_1 \underset{\text{TH}}{\sim} \lceil \dots \lceil \lfloor \dots \lfloor t_1 \rfloor_k \dots \rfloor_1 \rceil_1 \dots \rceil_k \underset{\text{TH}}{\sim} \lceil \dots \lceil \lfloor \dots \lfloor t_2 \rfloor_k \dots \rfloor_1 \rceil_1 \dots \rceil_k \underset{\text{TH}}{\sim} t_2$. ◀

This is not entirely satisfactory, as we would like to relate any two morphisms of the same interpretation. However:

▶ **Lemma 30.** *If* $t_1 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]'$ *and* $t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}] \setminus \mathbf{SOP}[\frac{1}{2^{k+1}}]'$, *then* $t_1 \underset{\mathrm{TH}}{\not\sim} t_2$.

Proof. There is no rule in $\underset{\mathrm{TH}}{\longrightarrow}$ that changes the overall scalar from an odd power of $\frac{1}{\sqrt{2}}$ to an even one, or vice-versa. ◀

However, adding a single rule:

$$\sum_{\vec{y}} e^{2i\pi\left(\frac{1}{8}+\frac{3}{4}y_0+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[y_0 \notin \mathrm{Var}(R,\vec{O},\vec{I})]{} \sqrt{2} \sum_{\vec{y}\setminus\{y_0\}} e^{2i\pi R} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \tag{$\sqrt{2}$}$$

fixes this caveat. This rule can also be recovered from the more general one:

$$\sum_{\vec{y}} e^{2i\pi\left(\frac{y_0}{4}+\frac{y_0}{2}\widehat{Q}+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \xrightarrow[y_0 \notin \mathrm{Var}(Q,R,\vec{O},\vec{I})]{} \sqrt{2} \sum_{\vec{y}\setminus\{y_0\}} e^{2i\pi\left(\frac{1}{8}-\frac{1}{4}\widehat{Q}+R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \tag{ω}$$

which was already used in [3, 18, 25] to deal with the Clifford fragment of quantum mechanics.

With this additional rule at hand, we can derive the general completeness theorem:

▶ **Theorem 31** (Completeness of $\mathbf{SOP}[\frac{1}{2^{k+1}}]/\underset{\mathrm{TH}'}{\sim}$). *Let us write* $\underset{\mathrm{TH}'}{\longrightarrow} := \underset{\mathrm{TH}}{\longrightarrow} + \{(\sqrt{2})\}$. *Then:* $\forall t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}],\quad [\![t_1]\!] = [\![t_2]\!] \iff t_1 \underset{\mathrm{TH}'}{\sim} t_2$

Proof. Let $t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]$ such that $[\![t_1]\!] = [\![t_2]\!]$. Let us also write:

$$t_{\sqrt{2}} := \frac{1}{\sqrt{2}} \sum e^{2i\pi\left(\frac{1}{8}+\frac{3}{4}y_0\right)}$$

We define t_i' as: $\quad t_i' := \begin{cases} t_i & \text{if } t_i \in \mathbf{SOP}[\frac{1}{2^{k+1}}]' \\ t_i \otimes t_{\sqrt{2}} & \text{if } t_i \notin \mathbf{SOP}[\frac{1}{2^{k+1}}]' \end{cases}$.

It is easy to check that $t_i' \in \mathbf{SOP}[\frac{1}{2^{\max(3,k+1)}}]'$ and that $t_i \underset{\mathrm{TH}'}{\sim} t_i'$. By Theorem 29:

$$t_1 \underset{\mathrm{TH}'}{\sim} t_1' \underset{\mathrm{TH}'}{\sim} t_2' \underset{\mathrm{TH}'}{\sim} t_2$$ ◀

We hence have completeness for all dyadic fragments of quantum computation. By taking their union, we can get completeness for the "whole dyadic fragment".

▶ **Definition 32.** *Let* $\mathbf{SOP}[\mathbb{D}] := \bigcup_{k=1}^{\infty} \mathbf{SOP}[\frac{1}{2^k}]$ *be the whole dyadic fragment of quantum computation.*

▶ **Corollary 33** (Completeness of $\mathbf{SOP}[\mathbb{D}]/\underset{\mathrm{TH}'}{\sim}$).

$$\forall t_1, t_2 \in \mathbf{SOP}[\mathbb{D}],\quad [\![t_1]\!] = [\![t_2]\!] \iff t_1 \underset{\mathrm{TH}'}{\sim} t_2$$

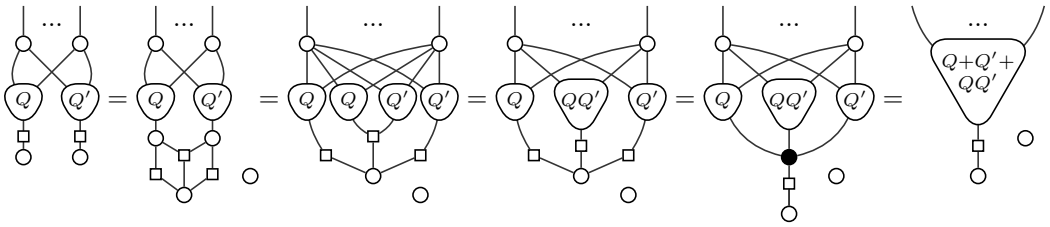
7 Conclusion and Discussion

We have given a new rewrite system for the Toffoli-Hadamard fragment of Sums-Over-Paths, and showed the induced equational theory to be complete. We then extended this rewrite strategy by adding a single new rewrite, which we then proved to be complete for the whole dyadic fragment. As expected from the universality of the fragments at hand, we do not get

all the nice properties of the rewriting in the Clifford fragment. In particular, we showed that the rewrite strategies given above are not confluent, and that the size of the terms may grow exponentially when rules are applied carelessly. Whether one of the above two drawbacks can be removed by a different rewrite system remains an open question.

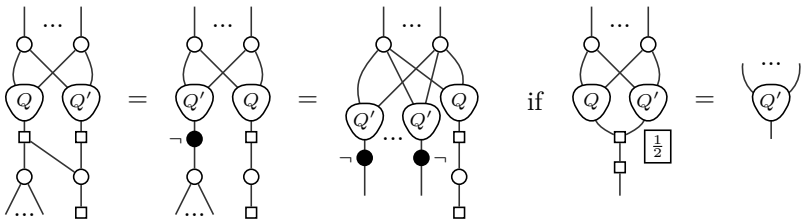
Using the translation from **SOP** to **ZH**, this time, we can make sense of the **SOP** rewrite rules as graphical ones. We will focus on the two rules that were not present in the previous works on **SOP**, namely (HHgen) and (HHnl). Let us start with the latter.

(HHnl) turns an occurrence of $\frac{y_0}{2}\widehat{Q}+\frac{y_0'}{2}\widehat{Q}'$ into $\frac{y_0}{2}(\widehat{Q}+\widehat{Q}'+\widehat{Q}\widehat{Q}')$, when the two variables are linked to nothing else than their respective polynomials Q and Q'. The induced **ZH** identity can be derived using its rules:



(where the first equality uses Lemma 34 (in appendix), the second, third and last use Lemma 11, and the fourth uses (ZS1), (HS2) and the definition of the black node).
Although the overall number of nodes usually increases, the number of white nodes that amount to **SOP**-variables (i.e. white nodes that are not part of a polynomial) decreases.

Rule (HHgen) is a bit more tricky to deal with in particular as it involves a non-trivial side condition. Hence, we do not provide a derivation of the equality, but only state it. With the pattern $\frac{y_0}{2}(y_i\widehat{Q}+\widehat{Q}'+1)$ we get $\frac{y_0}{2}(y_i\widehat{Q}+1)$ with all other occurrences of y_i replaced by $Q'\oplus 1$:



This paper, together with the above small study of how the rewrites translate as ZH transformations, really shows how the two formalisms (SOP and ZH) give different and complementary approaches to rewriting and simplifying representations of quantum processes.

We provided new rewrites that allow simplification in the terms – in that they decrease the number of variables – with the aim of completeness. A next important step for verification, simulation and simplification using SOP is to determine which rewrites, or which variants, are the most relevant to the task at hand.

References

1 Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, Nov 2004. URL: `https://link.aps.org/doi/10.1103/PhysRevA.70.052328`, `doi:10.1103/PhysRevA.70.052328`.

2 Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. *eprint arXiv:quant-ph/0301040*, Jan 2003. `arXiv:quant-ph/0301040`.

3 Matthew Amy. Towards large-scale functional verification of universal quantum circuits. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 1–21, 2019. doi:10.4204/EPTCS.287.1.

4 Miriam Backens and Aleks Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 23–42, 2019. doi:10.4204/EPTCS.287.2.

5 Miriam Backens, Aleks Kissinger, Hector Miller-Bakewell, John van de Wetering, and Sal Wolffs. Completeness of the ZH-calculus, 2021. arXiv:2103.06610.

6 Adam D. Bookatz. QMA-complete problems. *Quantum Information and Computation*, 14(5&6):361–383, may 2014. URL: https://doi.org/10.26421%2Fqic14.5-6-1, doi:10.26421/qic14.5-6-1.

7 Christophe Chareton, Sébastien Bardin, François Bobot, Valentin Perrelle, and Benoît Valiron. An automated deductive verification framework for circuit-building quantum programs. In Nobuko Yoshida, editor, *Programming Languages and Systems*, pages 148–177, Cham, 2021. Springer International Publishing.

8 Christophe Chareton, Sébastien Bardin, Dongho Lee, Benoît Valiron, Renaud Vilmart, and Zhaowei Xu. Formal methods for quantum programs: A survey, 2021. URL: https://arxiv.org/abs/2109.06493, doi:10.48550/ARXIV.2109.06493.

9 Bob Coecke and Ross Duncan. Interacting quantum observables: Categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, Apr 2011. URL: https://doi.org/10.1088%2F1367-2630%2F13%2F4%2F043016, doi:10.1088/1367-2630/13/4/043016.

10 Bob Coecke and Aleks Kissinger. The compositional structure of multipartite quantum entanglement. In *Automata, Languages and Programming*, pages 297–308. Springer Berlin Heidelberg, 2010. URL: https://doi.org/10.1007%2F978-3-642-14162-1_25, doi:10.1007/978-3-642-14162-1_25.

11 Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and Effective Techniques for T-Count Reduction via Spider Nest Identities. In Steven T. Flammia, editor, *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, volume 158 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:23, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. URL: https://drops.dagstuhl.de/opus/volltexte/2020/12070, doi:10.4230/LIPIcs.TQC.2020.11.

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

13 Mohammad Haidar, Marko J. Rančić, Thomas Ayral, Yvon Maday, and Jean-Philip Piquemal. Open source variational quantum eigensolver extension of the quantum learning machine (qlm) for quantum chemistry, 2022. URL: https://arxiv.org/abs/2206.08798, doi:10.48550/ARXIV.2206.08798.

14 Dominik Janzing, Pawel Wocjan, and Thomas Beth. Non-identity check is qma-complete. *International Journal of Quantum Information*, 03(03):463–473, sep 2005. URL: https://doi.org/10.1142%2Fs0219749905001067, doi:10.1142/s0219749905001067.

15 Aleks Kissinger and John van de Wetering. Reducing the number of non-Clifford gates in quantum circuits. *Phys. Rev. A*, 102:022406, Aug 2020. URL: https://link.aps.org/doi/10.1103/PhysRevA.102.022406, doi:10.1103/PhysRevA.102.022406.

16 Stephen Lack. Composing PROPs. In *Theory and Applications of Categories*, volume 13, pages 147–163, 2004. URL: http://www.tac.mta.ca/tac/volumes/13/9/13-09abs.html.

17 Louis Lemonnier. Relating high-level frameworks for quantum circuits. Master's thesis, Radbound University, 2019. URL: https://www.cs.ox.ac.uk/people/aleks.kissinger/papers/lemonnier-high-level.pdf.

18 Louis Lemonnier, John van de Wetering, and Aleks Kissinger. Hypergraph simplification: Linking the path-sum approach to the ZH-calculus. In Benoît Valiron, Shane Mansfield, Pablo Arrighi, and Prakash Panangaden, editors, Proceedings 17th International Conference on *Quantum Physics and Logic,* Paris, France, June 2 - 6, 2020, volume 340 of *Electronic Proceedings in Theoretical Computer Science*, pages 188–212. Open Publishing Association, 2021. doi:10.4204/EPTCS.340.10.

19 Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5. Springer Science & Business Media, 2013.

20 Yosuke Sato, Shutaro Inoue, Akira Suzuki, Katsusuke Nabeshima, and Ko Sakai. Boolean gröbner bases. *J. Symb. Comput.*, 46(5):622–632, May 2011. URL: https://doi.org/10.1016/j.jsc.2010.10.011, doi:10.1016/j.jsc.2010.10.011.

21 Peter Selinger. A survey of graphical languages for monoidal categories. In *New Structures for Physics*, pages 289–355. Springer, 2010.

22 Yaoyun Shi. Both Toffoli and controlled-not need little help to do universal quantum computing. *Quantum Information & Computation*, 3(1):84–92, 2003. URL: http://portal.acm.org/citation.cfm?id=2011515.

23 John van de Wetering and Sal Wolffs. Completeness of the Phase-free ZH-calculus, April 2019. arXiv:1904.07545. arXiv:1904.07545.

24 Renaud Vilmart. A ZX-calculus with triangles for Toffoli-Hadamard, Clifford+T, and beyond. In Peter Selinger and Giulio Chiribella, editors, *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, volume 287 of *Electronic Proceedings in Theoretical Computer Science*, pages 313–344, 2019. doi:10.4204/EPTCS.287.18.

25 Renaud Vilmart. The structure of sum-over-paths, its consequences, and completeness for clifford. In Stefan Kiefer and Christine Tasson, editors, *Foundations of Software Science and Computation Structures*, pages 531–550, Cham, 2021. Springer International Publishing.

26 Fabio Zanasi. *Interacting Hopf Algebras – the theory of linear systems.* PhD thesis, Université de Lyon, 2015. URL: http://www.zanasi.com/fabio/#/publications.html.

Appendix

Proof of Proposition 5. The result is obvious for the tensor product $(. \otimes .)$. For the composition, we show that if $t_1 \underset{\text{TH}}{\longrightarrow} t_2$ in one step, then $A \circ t_1 \circ B \underset{\text{TH}}{\sim} A \circ t_2 \circ B$. In other words, we have to show it for every rule in $\underset{\text{TH}}{\longrightarrow}$:

- (Elim): Obvious.
- (HHgen):

$$A \circ t_1 \circ B = \sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}(y_i\widehat{Q}+\widehat{Q'}+1)+R+\frac{\vec{O}\cdot\vec{x}+\vec{I}_A\cdot\vec{x}+\vec{I}\cdot\vec{x}'+\vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\left\langle\vec{I}_B\right|$$

$$\underset{\text{HHgen}}{\longrightarrow} \sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}(\widehat{Q}+1)+R[y_i\leftarrow\widehat{1\oplus Q'}]+\frac{\vec{O}[y_i\leftarrow\widehat{1\oplus Q'}]\cdot\vec{x}+\vec{I}_A\cdot\vec{x}+\vec{I}[y_i\leftarrow\widehat{1\oplus Q'}]\cdot\vec{x}'+\vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\left\langle\vec{I}_B\right|$$

$$= A \circ t_1[y_i \leftarrow 1\oplus Q'] \circ B = A \circ t_2 \circ B$$

- (HHnl):

$$A \circ t_1 \circ B = \sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}\widehat{Q}+\frac{y_0'}{2}\widehat{Q'}+R+\frac{\vec{O}\cdot\vec{x}+\vec{I}_A\cdot\vec{x}+\vec{I}\cdot\vec{x}'+\vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\left\langle\vec{I}_B\right|$$

$$\underset{\text{HHnl}}{\longrightarrow} 2\sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}(\widehat{Q}+\widehat{Q'}+\widehat{QQ'})+R+\frac{\vec{O}\cdot\vec{x}+\vec{I}_A\cdot\vec{x}+\vec{I}\cdot\vec{x}'+\vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\left\langle\vec{I}_B\right|$$

$$= A \circ (2t_1[y_0' \leftarrow y_0 \oplus y_0 Q]) \circ B = A \circ t_2 \circ B$$

- (ket):

$$A \circ t_1 \circ B = \sum e^{2i\pi\left(P_A + P_B + P + \frac{(\widehat{O_1}+\widehat{I_{A1}})x_1 + \ldots + (y_0 + \widehat{O_i'} + \widehat{I_{Ai}})x_i + \ldots + (\widehat{O_m}+\widehat{I_{Am}})x_m + \vec{I}\cdot\vec{x}' + \vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\!\left\langle\vec{I}_B\right|$$

$$\xrightarrow[\text{HH}]{} 2\sum e^{2i\pi\left(P_A + P_B + P[y_0 \leftarrow \widehat{O_i' \oplus I_{Ai}}] + \frac{\vec{O}[y_0 \leftarrow \widehat{O_i' \oplus I_{Ai}}]\cdot\vec{x} + \vec{I}_A\cdot\vec{x} + \vec{I}[y_0 \leftarrow \widehat{O_i' \oplus I_{Ai}}]\cdot\vec{x}' + \vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\!\left\langle\vec{I}_B\right|$$

$$\xleftarrow[\text{HH}]{} \sum e^{2i\pi\left(P_A + P_B + P[y_0 \leftarrow \widehat{y_0 \oplus O_i'}] + \frac{\vec{O}[y_0 \leftarrow \widehat{y_0 \oplus O_i'}]\cdot\vec{x} + \vec{I}_A\cdot\vec{x} + \vec{I}[y_0 \leftarrow \widehat{y_0 \oplus O_i'}]\cdot\vec{x}' + \vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\!\left\langle\vec{I}_B\right|$$

$$= A \circ t_1[y_0 \leftarrow y_0 \oplus O_i'] \circ B = A \circ t_2 \circ B$$

- (bra): Similar to (ket).
- (Z):

$$A \circ t_1 \circ B = \sum e^{2i\pi\left(P_A + P_B + \frac{y_0}{2} + R + \frac{\vec{O}\cdot\vec{x} + \vec{I}_A\cdot\vec{x} + \vec{I}\cdot\vec{x}' + \vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\!\left\langle\vec{I}_B\right| \xrightarrow[\text{Z}]{} \sum e^{2i\pi\left(\frac{y_0}{2}\right)} \left|\vec{0}\right\rangle\!\left\langle\vec{0}\right|$$

$$\xleftarrow[\text{Z}]{} \sum e^{2i\pi\left(P_A + P_B + \frac{y_0}{2} + \frac{\vec{0}\cdot\vec{x} + \vec{I}_A\cdot\vec{x} + \vec{0}\cdot\vec{x}' + \vec{O}_B\cdot\vec{x}'}{2}\right)} \left|\vec{O}_A\right\rangle\!\left\langle\vec{I}_B\right| = A \circ t_2 \circ B$$

◀

Proof of Proposition 7.

(HHgen): If $t = \sum_{\vec{y}\in V^k} e^{2i\pi\left(\frac{y_0}{2}(y_i\widehat{Q} + \widehat{Q'} + 1) + R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$ such that $QQ' = Q'$:

$$[\![t]\!] = \sum_{\vec{y}\in\{0,1\}^k} e^{2i\pi\left(\frac{y_0}{2}(y_i\widehat{Q} + \widehat{Q'} + 1) + R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| = \sum_{\vec{y}\in\{0,1\}^{k-1}} (1 + e^{i\pi(y_i\widehat{Q} + \widehat{Q'} + 1)}) e^{2i\pi R} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$$

$$= \sum_{\vec{y}\in\{0,1\}^{k-2}} (1 + e^{i\pi(\widehat{Q'}\widehat{Q} + \widehat{Q'} + 1)}) e^{2i\pi R[y_i \leftarrow \widehat{Q'}]}(\left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|)[y_i \leftarrow Q']$$

$$+ \sum_{\vec{y}\in\{0,1\}^{k-2}} (1 + e^{i\pi(\widehat{1\oplus Q'}\widehat{Q} + \widehat{Q'} + 1)}) e^{2i\pi R[y_i \leftarrow \widehat{1\oplus Q'}]}(\left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|)[y_i \leftarrow 1 \oplus Q']$$

$$= 0 + \sum_{\vec{y}\in\{0,1\}^{k-2}} (1 + e^{i\pi(\widehat{1\oplus Q'}\widehat{Q} + \widehat{Q'} + 1)}) e^{2i\pi R[y_i \leftarrow \widehat{1\oplus Q'}]}(\left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|)[y_i \leftarrow 1 \oplus Q']$$

$$= [\![t[y_i \leftarrow 1 \oplus Q']]\!]$$

(HHnl) : If $t = \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q} + \frac{y_0'}{2}\widehat{Q'} + R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$:

$$[\![t]\!] = \sum_{\vec{y}\in\{0,1\}^k} e^{2i\pi\left(\frac{y_0}{2}\widehat{Q} + \frac{y_0'}{2}\widehat{Q'} + R\right)} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$$

$$= \sum_{\vec{y}\in\{0,1\}^{k-2}} \left(1 + e^{i\pi\widehat{Q}} + e^{i\pi\widehat{Q'}} + e^{i\pi\widehat{Q\oplus Q'}}\right) e^{2i\pi R} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$$

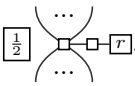
$$= \sum_{\vec{y}\in\{0,1\}^{k-2}} 2\left(1 + e^{i\pi Q \oplus \widehat{Q'\oplus QQ'}}\right) e^{2i\pi R} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$$

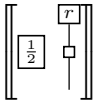
$$= 2 \sum_{\vec{y} \in \{0,1\}^{k-1}} e^{2i\pi\left(\frac{y_0}{2}(\widehat{Q}+\widehat{Q'}+\widehat{QQ'})+R\right)} \left|\vec{O}\right\rangle\!\left\langle \vec{I}\right|$$
$$= [\![2t[y_0' \leftarrow y_0 \oplus y_0 Q]]\!]$$

The third equality is obtained by checking that the equality is true for all values of $\widehat{Q}$ and $\widehat{Q'}$:

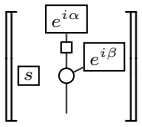
$\widehat{Q}$	$\widehat{Q'}$	$\left(1+e^{i\pi\widehat{Q}}+e^{i\pi\widehat{Q'}}+e^{i\pi\widehat{Q\oplus Q'}}\right)$	$2\left(1+e^{i\pi Q\oplus\widehat{Q'\oplus QQ'}}\right)$
0	0	4	4
0	1	0	0
1	0	0	0
1	1	0	0

◀

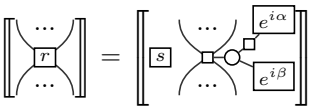
Proof of Lemma 13. . First, thanks to rule (HS1), we have  =  . Then, we have:

 $= \frac{1}{2}\begin{pmatrix}1+r\\1-r\end{pmatrix} = \frac{1+r}{2}\begin{pmatrix}1\\\frac{1-r}{1+r}\end{pmatrix}$

and

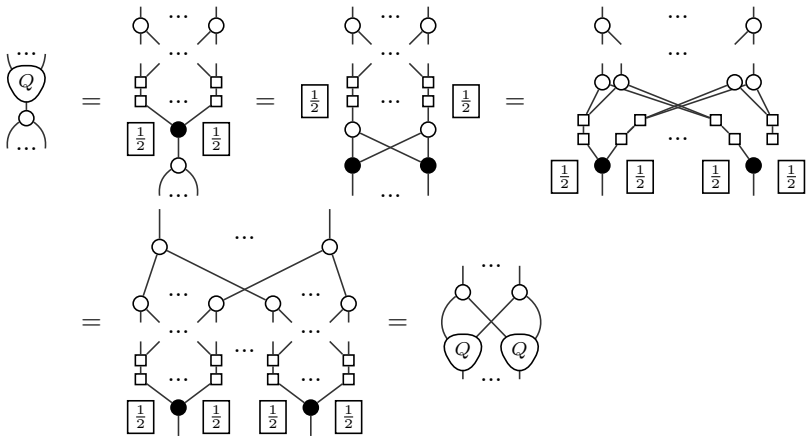
 $= 2se^{i\frac{\alpha}{2}}\begin{pmatrix}\cos\frac{\alpha}{2}\\-ie^{i\beta}\sin\frac{\alpha}{2}\end{pmatrix} = 2se^{i\frac{\alpha}{2}}\cos\frac{\alpha}{2}\begin{pmatrix}1\\e^{i(\beta-\frac{\pi}{2})}\tan\frac{\alpha}{2}\end{pmatrix}$

Hence, when $|r| \notin \{0,1\}$, we have equality between the two with $\alpha := 2\arctan\left(\frac{1-r}{1+r}\right)$, $\beta = \arg\left(\frac{1-r}{1+r}\right) + \frac{\pi}{2}$ and $s := \frac{1+r}{4e^{i\frac{\alpha}{2}}\cos\frac{\alpha}{2}}$ (since $r \neq 1$, α is well defined and $\alpha \neq \pi \mod 2\pi$ so s is also well-defined). From this, we get:



◀

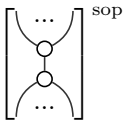
Proof of Lemma 11.



◀

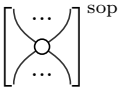
Proof of Proposition 18. We show that all the rules of $\mathrm{ZH}_{\mathrm{TH}}$ hold in $\mathbf{SOP}[\frac{1}{2}]$.

Checking the rules (ZS1), (ZS2), (HS1), (HS2) and (M) is straightforward using the rule (HH). We give for instance a check of the rule (ZS1):



$$= \frac{1}{2}\sum e^{2i\pi\frac{y_0+y_1}{2}y'}\,|y_1,...,y_1\rangle\langle y_0,...,y_0|$$

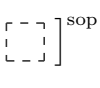
$$\xrightarrow[\mathrm{HH}(y',[y_1\leftarrow y_0])]{} \sum |y_0,...,y_0\rangle\langle y_0,...,y_0| =$$



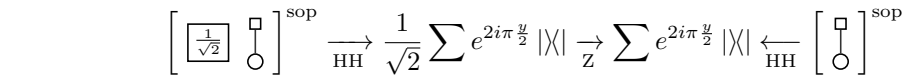
We give derivations to prove the remaining rules of $\mathrm{ZH}_{\mathrm{TH}}$. Recall that equality is up to α-conversion.

(IV):

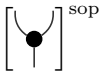
$$= \frac{1}{2}\sum_y |\rangle\langle| \xrightarrow[\mathrm{Elim}]{} 1 =$$



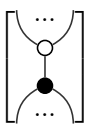
(Z):



$$\xrightarrow[\mathrm{HH}]{} \frac{1}{\sqrt{2}}\sum e^{2i\pi\frac{y}{2}}\,|\rangle\langle| \xrightarrow[\mathrm{Z}]{} \sum e^{2i\pi\frac{y}{2}}\,|\rangle\langle| \xleftarrow[\mathrm{HH}]{}$$

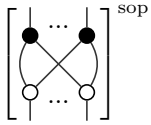
The two rules (BA1) and (BA2) are fairly easy to check, once one realises that 

$\xrightarrow[\mathrm{HH}]{}$ $\sum |y_0\oplus y_1\rangle\langle y_0,y_1|$:

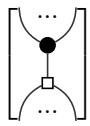


$$\xrightarrow[\mathrm{HH}]{} \frac{1}{2}\sum e^{2i\pi\frac{y_1+...+y_n+y_0}{2}y'}\,|y_1,...,y_n\rangle\langle y_0,...,y_0|$$

$$\xrightarrow[\mathrm{HH}(y',[y_0\leftarrow y_1\oplus...\oplus y_n])]{} \sum |y_1,...,y_n\rangle\langle y_1\oplus...\oplus y_n,...,y_1\oplus...\oplus y_n| \xleftarrow[\mathrm{HH}]{}$$



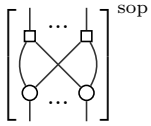
and



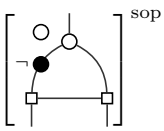
$$\xrightarrow[\mathrm{HH}]{} \frac{1}{2}\sum e^{2i\pi\left(\frac{y_1...y_m y'}{2}+\frac{x_1+...+x_n+y'}{2}y''\right)}\,|y_1,...,y_m\rangle\langle x_1,...x_n|$$

$$\xrightarrow[\mathrm{HH}(y'',[y'\leftarrow x_1\oplus...\oplus x_n])]{} \sum e^{2i\pi\left(\frac{y_1...y_m x_1}{2}+...+\frac{y_1...y_m x_n}{2}\right)}\,|y_1,...,y_m\rangle\langle x_1,...x_n|$$

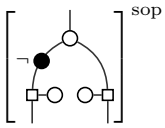
$$\xleftarrow[\mathrm{HH}]{}$$



(O):



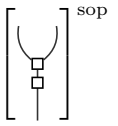
$$\xrightarrow[\mathrm{HH}]{} 2\sum e^{2i\pi\left(\frac{1}{2}y_0y_2y_3+\frac{1}{2}y_0y_3+\frac{1}{2}y_1y_2y_3\right)}\,|y_0,y_1\rangle\langle y_2|$$



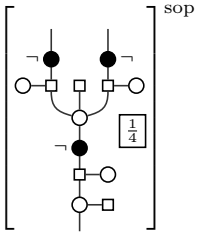
$$\xrightarrow[\text{HH}]{} \sum e^{2i\pi\left(\frac{1}{2}y_0y_1+\frac{1}{2}y_2y_3y_4+\frac{1}{2}y_0y_1y_4\right)}|y_0,y_3\rangle\langle y_4|$$

$$\xrightarrow[\text{HHnl}(y_1,y_2)]{} 2\sum e^{2i\pi\left(\frac{1}{2}y_0y_1+\frac{1}{2}y_0y_1y_4+\frac{1}{2}y_1y_3y_4\right)}|y_0,y_3\rangle\langle y_4|$$

(&):



$$\xrightarrow[\text{HH}]{} \sum e^{2i\pi\left(\frac{1}{2}y_0y_1+\frac{1}{2}y_0y_2y_3\right)}|y_1\rangle\langle y_2,y_3| \xrightarrow[\text{HH}(y_0,[y_1\leftarrow y_2y_3])]{} 2\sum |y_2y_3\rangle\langle y_2,y_3|$$



$$\xrightarrow[\text{HH}]{} \frac{1}{4}\sum e^{2i\pi\left(\frac{1}{2}y_0+\frac{1}{2}y_8y_1y_7+\frac{1}{2}y_1+\frac{1}{2}y_1y_3y_4+\frac{1}{2}y_0y_1y_2+\frac{1}{2}y_0y_2\right)}|y_0\rangle\langle 1\oplus y_4,1\oplus y_7|$$

$$\xrightarrow[\text{HHnl}(y_8,y_2)]{} \frac{1}{2}\sum e^{2i\pi\left(\frac{1}{2}y_0y_1y_8+\frac{1}{2}y_0+\frac{1}{2}y_8y_1y_7+\frac{1}{2}y_1+\frac{1}{2}y_1y_3y_4+\frac{1}{2}y_0y_8\right)}|y_0\rangle\langle 1\oplus y_4,1\oplus y_7|$$

$$\xrightarrow[\substack{\text{ket/bra}([y_4\leftarrow y_4\oplus 1])\\ \text{ket/bra}([y_7\leftarrow y_7\oplus 1])}]{} \frac{1}{2}\sum e^{2i\pi\left(\frac{1}{2}y_0y_1y_8+\frac{1}{2}y_0+\frac{1}{2}y_8y_1y_7+\frac{1}{2}y_8y_1+\frac{1}{2}y_1+\frac{1}{2}y_1y_3y_4+\frac{1}{2}y_1y_3+\frac{1}{2}y_0y_8\right)}|y_0\rangle\langle y_4,y_7|$$

$$\xrightarrow[\text{HHnl}(y_8,y_3)]{} \sum e^{2i\pi\left(\frac{1}{2}y_0y_1y_8+\frac{1}{2}y_0+\frac{1}{2}y_8y_1y_4y_7+\frac{1}{2}y_1+\frac{1}{2}y_8y_1+\frac{1}{2}y_0y_8\right)}|y_0\rangle\langle y_4,y_7|$$

$$\xrightarrow[\text{HHgen}(y_1,[y_0\leftarrow y_4y_7y_8\oplus y_8\oplus 1])]{} \sum e^{2i\pi\left(\frac{1}{2}y_1+\frac{1}{2}y_8y_1+\frac{1}{2}y_8+\frac{1}{2}\right)}|y_4y_7y_8\oplus y_8\oplus 1\rangle\langle y_4,y_7|$$

$$\xrightarrow[\text{HH}(y_1,[y_8\leftarrow 1])]{} 2\sum |y_4y_7\rangle\langle y_4,y_7|$$

◀

Proof of Proposition 26. We demonstrate this proposition by showing that:

1. $[\![\mathbf{SOP}[\frac{1}{2^{k+1}}]']\!] \subseteq \mathcal{M}(\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^k}}])$
2. For each element $x \in \mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^k}}]$, there exists a unique decomposition as $x = x_1 + e^{i\frac{\pi}{2^k}}x_2$ where $x_1, x_2 \in \mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^{k-1}}}]$
3. There exists a map $\psi_k : \mathcal{M}(\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^k}}]) \to \mathcal{M}(\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^{k-1}}}])$, based on the decomposition, and such that $[\![\lfloor t \rfloor_k]\!] = \psi_k([\![t]\!])$

In this case, given $t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]'$ such that $[\![t_1]\!] = [\![t_2]\!]$, by 1. we can apply ψ_k to their interpretation. By uniqueness of the decomposition 2., $\psi_k([\![t_1]\!]) = \psi_k([\![t_2]\!])$. Finally, by 3., $[\![\lfloor t_1 \rfloor_k]\!] = [\![\lfloor t_2 \rfloor_k]\!]$. Let us now prove the previous claims:

1. This point is a simple verification.
2. Let $x = \sum_{\ell=0}^{2^k-1} \alpha_\ell e^{i\frac{\ell\pi}{2^k}} \in \mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^k}}]$. Obviously, x can be decomposed as

$$x = \sum_{\ell=0}^{2^{k-1}-1} \alpha_{2\ell} e^{i\frac{\ell\pi}{2^{k-1}}} + e^{i\frac{\pi}{2^k}} \sum_{\ell=0}^{2^{k-1}-1} \alpha_{2\ell+1} e^{i\frac{\ell\pi}{2^{k-1}}} = x_1 + e^{i\frac{\pi}{2^k}} x_2$$

where $x_1, x_2 \in \mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^{k-1}}}]$. We now need to show that this decomposition is unique. To do so, let us consider $\mathbb{Q}[e^{i\frac{\pi}{2^k}}]$ and $\mathbb{Q}[e^{i\frac{\pi}{2^{k-1}}}]$. These are two fields such that $\mathbb{Q}[e^{i\frac{\pi}{2^{k-1}}}] \subset \mathbb{Q}[e^{i\frac{\pi}{2^k}}]$. $\mathbb{Q}[e^{i\frac{\pi}{2^k}}]$ can hence be seen as a vector space over $\mathbb{Q}[e^{i\frac{\pi}{2^{k-1}}}]$. This vector space is of dimension:

$$\left[\mathbb{Q}[e^{i\frac{\pi}{2^k}}] : \mathbb{Q}[e^{i\frac{\pi}{2^{k-1}}}]\right] = \left[\mathbb{Q}[e^{i\frac{2\pi}{2^{k+1}}}] : \mathbb{Q}[e^{i\frac{2\pi}{2^k}}]\right] = \frac{\left[\mathbb{Q}[e^{i\frac{2\pi}{2^{k+1}}}] : \mathbb{Q}\right]}{\left[\mathbb{Q}[e^{i\frac{2\pi}{2^k}}] : \mathbb{Q}\right]} = \frac{\varphi(2^{k+1})}{\varphi(2^k)} = \frac{2^k}{2^{k-1}} = 2$$

where φ is Euler's totient function. The vector space has $(1, e^{i\frac{\pi}{2^k}})$ as a basis. Hence, the above decomposition is unique.

3. We now need to define ψ_k. We are going to define it first on scalars, and on the basis $(1, e^{i\frac{\pi}{2^k}})$:

$$\psi_k(1) := I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \psi_k(e^{i\frac{\pi}{2^k}}) := X_k = \begin{pmatrix} 0 & 1 \\ e^{i\frac{\pi}{2^{k-1}}} & 0 \end{pmatrix}$$

By linearity, ψ_k is defined on all elements of $\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^k}}]$. We then naturally extend this definition to any matrix over these elements. Formally: $\psi_k : A + Be^{i\frac{\pi}{2^k}} \mapsto A \otimes I_2 + B \otimes X_k$ where $A + Be^{i\frac{\pi}{2^k}}$ is the aforementioned decomposition extended to matrices. One can check that ψ_k is a homomorphism, i.e. $\psi_k(. + .) = \psi_k(.) + \psi_k(.)$ and $\psi_k(. \circ .) = \psi_k(.) \circ \psi_k(.)$. It remains to show that $[\![\lfloor . \rfloor_k]\!] = \psi_k([\![.]\!])$. Since ψ_k is a homomorphism, it is enough to show the result on the terms in the decomposed form of Lemma 22. Let $t = s \sum e^{2i\pi \frac{\ell}{2^{k+1}} y_{i_1} \dots y_{i_q}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$ be such a term.

If $\ell \bmod 2 = 0$, then $[\![t]\!] \in \mathcal{M}(\mathbb{Z}[\frac{1}{2}, e^{i\frac{\pi}{2^{k-1}}}])$ so $\psi_k([\![t]\!]) = [\![t]\!] \otimes I_2$ and:

$$[\![\lfloor t \rfloor_k]\!] = \left[\!\!\left[s \sum e^{2i\pi \frac{\ell/2}{2^k} y_{i_1} \dots y_{i_q}} \left|\vec{O}, y'\right\rangle\!\left\langle\vec{I}, y'\right| \right]\!\!\right] = [\![t]\!] \otimes I_2.$$

If $\ell \bmod 2 = 1$, then:

$$[\![t]\!] = s e^{i\frac{\pi}{2^k}} \sum_{y_{i_1} \dots y_{i_q} = 1} e^{2i\pi \frac{(\ell-1)/2}{2^k}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| + s \sum_{y_{i_1} \dots y_{i_q} = 0} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$$

so:

$$\psi_k([\![t]\!]) = \left(s \sum_{y_{i_1} \dots y_{i_q} = 1} e^{2i\pi \frac{(\ell-1)/2}{2^k}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \right) \otimes X_k + \left(s \sum_{y_{i_1} \dots y_{i_q} = 0} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \right) \otimes I_2$$

and

$$\begin{aligned}
[\![\lfloor t \rfloor_k]\!] &= s \sum e^{2i\pi \frac{y_{i_1} \dots y_{i_q}}{2^k} ((\ell-1)/2 + y')} \left|\vec{O}, y'\right\rangle\!\left\langle\vec{I}, y' \oplus y_{i_1} \dots y_{i_q}\right| \\
&= s \sum_{y_{i_1} \dots y_{i_q} = 1} e^{2i\pi \frac{(\ell-1)/2 + y'}{2^k}} \left|\vec{O}, y'\right\rangle\!\left\langle\vec{I}, y' \oplus 1\right| + s \sum_{y_{i_1} \dots y_{i_q} = 0} \left|\vec{O}, y'\right\rangle\!\left\langle\vec{I}, y'\right| \\
&= \left(s \sum_{y_{i_1} \dots y_{i_q} = 1} e^{2i\pi \frac{(\ell-1)/2}{2^k}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \right) \otimes X_k + \left(s \sum_{y_{i_1} \dots y_{i_q} = 0} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right| \right) \otimes I_2 = \psi_k([\![t]\!])
\end{aligned}$$ ◀

Proof of Proposition 28. Again, we can use the decomposition given in Lemma 22. We can show that if $t = s \sum e^{2i\pi \frac{\ell}{2^{k+1}} y_{i_1} \dots y_{i_q}} \left|\vec{O}\right\rangle\!\left\langle\vec{I}\right|$, then $\lfloor t \rfloor_k \circ (id_n \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle) \underset{\text{TH}}{\sim} t \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle$:

If $\ell \bmod 2 = 0$, then $\lfloor t \rfloor_k = t \otimes id$ so $\lfloor t \rfloor_k \circ (id_n \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle) \underset{\text{TH}}{\sim} t \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle$.
If $\ell \bmod 2 = 1$, then:

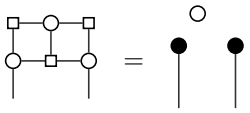
$$\begin{aligned}
&\lfloor t \rfloor_k \circ (id_n \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle) \\
&\qquad = \frac{s}{2} \sum e^{2i\pi \left(\frac{y_{i_1} \cdots y_{i_q}}{2^k} \left((\ell-1)/2 + y' \right) + \frac{y' + y_{i_1} \cdots y_{i_q} + y_0}{2} y'' + \frac{y_0}{2^{k+1}} \right)} \left| \vec{O}, y' \right\rangle \left\langle \vec{I} \right| \\
&\xrightarrow[\text{HH}(y'', [y_0 \leftarrow y' \oplus y_{i_1} \cdots y_{i_q}])]{} s \sum e^{2i\pi \left(\frac{y_{i_1} \cdots y_{i_q}}{2^k} \left((\ell-1)/2 + y' \right) + \frac{y' + y_{i_1} \cdots y_{i_q} - 2y' y_{i_1} \cdots y_{i_q}}{2^{k+1}} \right)} \left| \vec{O}, y' \right\rangle \left\langle \vec{I} \right| \\
&\qquad = s \sum e^{2i\pi \left(\ell \frac{y_{i_1} \cdots y_{i_q}}{2^k} + \frac{y'}{2^{k+1}} \right)} \left| \vec{O}, y' \right\rangle \left\langle \vec{I} \right| = t \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle
\end{aligned}$$

Now, for an arbitrary $t \in \mathbf{SOP}[\frac{1}{2^{k+1}}]'$, we can do the above inductively on each term in its decomposition, resulting in $\lfloor t \rfloor_k \circ (id_n \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle) \underset{\text{TH}}{\sim} t \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle$. Finally:

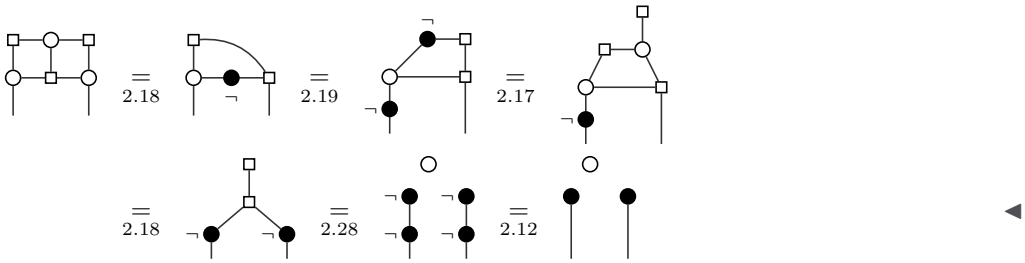
$$\begin{aligned}
\lceil \lfloor t \rfloor_k \rceil_k &= (id_m \otimes \langle 0|) \circ \lfloor t \rfloor_k \circ (id_n \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle) \\
&\underset{\text{TH}}{\sim} (id_m \otimes \langle 0|) \circ \left(t \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}}} |y_0\rangle \right) \underset{\text{TH}}{\sim} t
\end{aligned}$$

The second result in the Proposition simply comes from the fact that $\lceil t_i \rfloor$ is built by composition from t_i, so Proposition 5 gives the desired result. ◀

▶ **Lemma 34.**



Proof. We have the following, where the numbering refers to lemmas in [5]:



◀