Completeness of Sum-Over-Paths for Toffoli-Hadamard and the Clifford Hierarchy

Renaud Vilmart

Completeness of Sum-Over-Paths for Toffoli-Hadamard and the Clifford Hierarchy

Renaud Vilmart
vilmart@lsv.fr

Université Paris-Saclay, CNRS, ENS Paris-Saclay, Inria, Laboratoire Méthodes Formelles, 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.
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 whole Clifford hierarchy.

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 [15,16] 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 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: Provided two circuits $\mathcal{C}_1$ and $\mathcal{C}_2$, the system represents $\mathcal{C}_2^\dagger \circ \mathcal{C}_1$ as a 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 showed $\mathcal{C}_1$ 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. [10,13]) to check precisely for circuit equivalence. It was later extended to account for families of morphisms and used within environment Qbricks [6,7] 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.

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 this fragment is not universal [1], and actually efficiently simulable with a classical computer, so it is a good test for the relevance of an 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 [23] 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 their 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 – [5,12]. A weaker notion of confluence we can ask for is that of completeness: the question here is to know 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).

In this paper, we address the problem of completeness first for arguably the simplest universal fragment of quantum computing, which is *Toffoli-Hadamard*. 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 that the provided rewrite system reaches completeness for the Toffoli-Hadamard fragment in section 5, and at the same time show that it is not confluent. We then show in section 6 how the rewrite strategy can be tweaked to reach completeness for the whole so-called *Clifford hierarchy*, a restriction that encompasses Clifford, Clifford+T and Toffoli-Hadamard.

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 [17,19] denoted **Qubit** where the objects are natural numbers (this makes the category a PROP [14,24]), where morphisms from n to m are linear maps $\mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$, and where $(. \circ .)$ (resp. $(. \otimes .)$) 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 $(.)^\dagger$, that behaves properly with the symmetric braiding and the compact structure. For more information on these structures, see [19].

Definition 1 (SOP). *We define* **SOP** *as the collection of objects* $\mathbb{N}$ *and morphisms between them, of the form:* $f := s \sum_{\boldsymbol{y} \in V^k} e^{2i\pi P(\boldsymbol{y})} |\boldsymbol{O}(\boldsymbol{y})\rangle\langle \boldsymbol{I}(\boldsymbol{y})|$

where $s \in \mathbb{R}$, $P \in \mathbb{R}[X_1, \ldots, X_k]/(1, X_i^2 - X_i)$ *is called the* phase polynomial *of* f, $\boldsymbol{O} \in (\mathbb{F}_2[X_1, \ldots, X_k])^m$ *and* $\boldsymbol{I} \in (\mathbb{F}_2[X_1, \ldots, X_k])^n$.
Compositions are obtained as:

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

We distinguish particular morphisms:

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

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

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

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

We took the liberty of calling the last two maps functors, although **SOP** is not a category. For instance, notice that $id \circ id \neq id$. However, it suffices to quotient the formalism with rewrite rules to turn it into a category [23].

2.2 A Rewrite System

We hence give in Figure 1 a set of rewrite rules denoted $\underset{\text{TH}}{\longrightarrow}$ that induces an equational theory $\underset{\text{TH}}{\sim}$.

$$\sum_{\boldsymbol{y}} e^{2i\pi P}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}| \underset{y_0\notin \mathrm{Var}(P,\boldsymbol{O},\boldsymbol{I})}{\longrightarrow} 2\sum_{\boldsymbol{y}\setminus\{y_0\}} e^{2i\pi P}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}| \tag{Elim}$$

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

$$t = \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q}+\frac{y_0'}{2}\widehat{Q'}+R\right)}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}| \underset{y_0,y_0'\notin \mathrm{Var}(Q,Q',R,\boldsymbol{O},\boldsymbol{I})}{\longrightarrow} 2t[y_0' \leftarrow y_0\oplus y_0Q] \tag{HHnl}$$

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

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

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

Fig. 1. Rewrite system $\underset{\text{TH}}{\longrightarrow}$

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 $y_0 \in \mathrm{Var}(t) \setminus \mathrm{Var}(\boldsymbol{O},\boldsymbol{I})$.

The rules (HHgen), (HHnl) and (Z) all stem from a particular observation: In the morphism $t = \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q}+R\right)}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$ 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.

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 1. 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 $\widehat{(.)} : \mathbb{F}_2[X_1,\ldots,X_k] \to \mathbb{R}[X_1,\ldots,X_k]/(1, X_i^2 - X_i)$, serves this purpose. It is inductively defined as:

$$\widehat{Q_1Q_2} = \widehat{Q_1}\widehat{Q_2} \qquad \widehat{Q_1\oplus Q_2} = \widehat{Q_1} + \widehat{Q_2} - 2\widehat{Q_1}\widehat{Q_2} \qquad \widehat{y_i} = y_i \qquad \widehat{\alpha} = \alpha$$

Remark 2. The rule (HHgen) can be generalised to:

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

However, finding a "minimal" Q' for this rule is a hard problem, as it requires the use of boolean Groebner bases [18]. (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:

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

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 [23]. We can extend this result here thanks to:

Proposition 1.

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

Thanks to this Proposition, and since $\mathbf{SOP}/\underset{\text{HH}}{\sim}$ is a †-compact PROP by [23], we get:

Corollary 1. $\mathbf{SOP}/\underset{\text{TH}}{\sim}$ *is a †-compact PROP.*

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

Proposition 2 (Soundness). *For any two* **SOP** *morphisms* t_1 *and* t_2*, if* $t_1 \xrightarrow[\text{TH}]{*} t_2$*, then* $[\![t_1]\!] = [\![t_2]\!]$.

3 The ZH-Calculus

The graphical calculi ZX, ZW and ZH [4,8,9] are calculi for quantum computing, with a tight link with the Sum-Over-Paths formalism [15,16,23], and whose completeness was proven in particular for the Toffoli-Hadamard fragment [11,21,22].

This fragment of quantum mechanics is approximately universal [2,20], 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 **SOP**. 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 $(. \circ .)$ or in parallel $(. \otimes .)$) 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 $r \in \mathbb{C}$

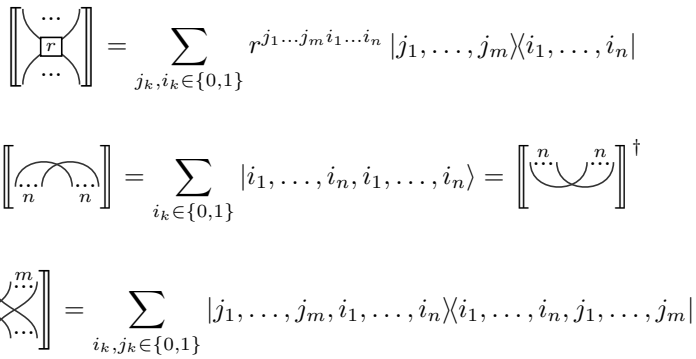
When r is not specified, the parameter in the H-spider is taken to be -1.

ZH is made a †-compact PROP, which means it also has a symmetric structure $\sigma_{n,m} ::$  , a compact structure $\left(\eta_n :: \right.$  $, \epsilon_n ::$  $\left.\right)$, and a †-functor $(.)^\dagger : \mathbf{ZH}^{\text{op}} \to \mathbf{ZH}$. 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:

 $:=$  and  $:=$ 

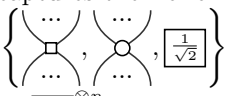
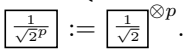
The language comes with a way of interpreting the morphisms as morphisms of **Qubit**. The standard interpretation $[\![.]\!] : \mathbf{ZH} \to \mathbf{Qubit}$ is a †-compact-PROP-functor, defined as:

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



Notice that we used the same symbol for two different functors: the two interpretations $[\![.]\!] : \mathbf{SOP} \to \mathbf{Qubit}$ and $[\![.]\!] : \mathbf{ZH} \to \mathbf{Qubit}$. It should be clear from the context which one is to be used.
The language is universal: $\forall f \in \mathbf{Qubit},\ \exists D_f \in \mathbf{ZH},\quad [\![D_f]\!] = f$. In other words, the interpretation $[\![.]\!]$ is onto.

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 [21], as the language generated by:  . Notice that the two black spiders can still be defined if we also define  . We denote this restriction by $\mathbf{ZH}_{\mathrm{TH}}$.

This restriction is provided with an equational theory, given in Figure 2, that makes it complete:

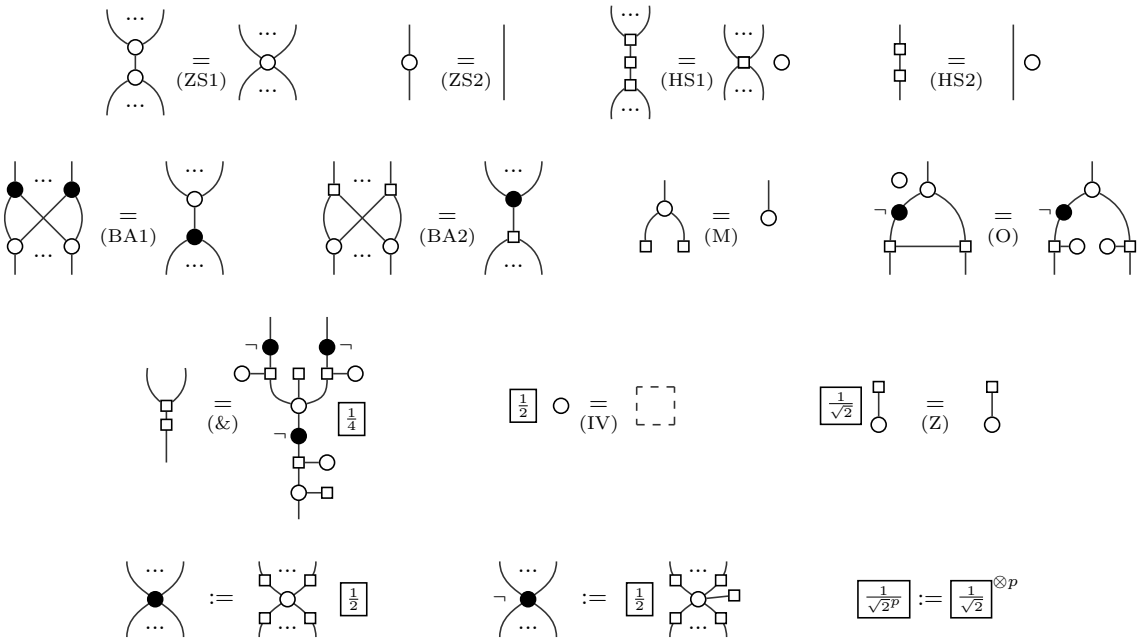


Fig. 2. Set of rules $\mathrm{ZH}_{\mathrm{TH}}$

Theorem 1 ([21] Completeness of $\mathbf{ZH}_{\mathrm{TH}}$/ $\mathrm{ZH}_{\mathrm{TH}}$).

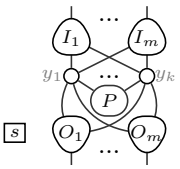
$$\forall D_1, D_2 \in \mathbf{ZH}_{\mathrm{TH}},\quad [\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZH}_{\mathrm{TH}} \vdash D_1 = D_2$$

4 Translations between SOP and ZH

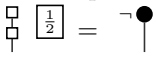
4.1 From SOP to ZH

It is possible to translate **SOP** morphisms to ZH-diagrams using interpretation $[.]^{\mathrm{ZH}} : \mathbf{SOP} \to \mathbf{ZH}$. A description of $[.]^{\mathrm{ZH}} : \mathbf{SOP} \to \mathbf{ZH}$ was defined in [15,16] and in [23]. We choose the latter definition as it fits our definition of **SOP**.

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



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

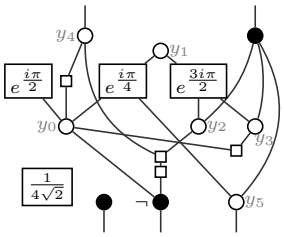
- each monomial $\alpha y_{i_1} \ldots y_{i_s}$ in P gives a single H-spider with parameter $\frac{\alpha}{2\pi}$ and connected to the Z-spiders that represent y_{i_1},...,y_{i_s}
- each monomial $y_{i_1} \ldots y_{i_s}$ in O_i is represented by  where the inputs are connected to the Z-spiders that represent 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 [23].

Example 1. The **SOP** morphism:

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

is mapped to



This translation preserves the semantics:

Proposition 3 ([23]). $[\![[.]^{\mathrm{ZH}}]\!] = [\![.]\!]$.

4.2 From ZH to SOP

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

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

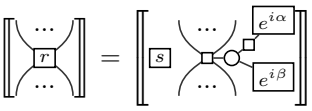
$$[\, s \,]^{\mathrm{sop}} := s \, |\rangle\langle| \qquad \text{for } s \in \mathbb{R}$$

$$\left[\begin{array}{c} \cdots \\ \cdots \end{array} \right]^{\mathrm{sop}} := \sum_{y} |y, \ldots, y\rangle\langle y, \ldots, y| \qquad \left[\begin{array}{c} \cdots \\ 0 \\ \cdots \end{array} \right]^{\mathrm{sop}} := \left[\begin{array}{c} \cdots \\ \frac{1}{2} \\ \cdots \end{array} \right]^{\mathrm{sop}}$$

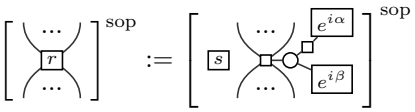
The functor furthermore maps the symmetric braiding (resp. the compact structure) of **ZH** to the symmetric braiding (resp. the compact structure) of **SOP**.

This does not give a full description of $[.]^{\mathrm{sop}}$, 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 1. *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:*



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



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

Proposition 4 ([23]). $[\![[.]^{\mathrm{sop}}]\!] = [\![.]\!]$.

The composition of the two interpretations is close to the identity:

Proposition 5 ([23]). $\left[[.]^{\mathrm{ZH}}\right]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} (.)$

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

Proposition 6. $\mathbf{SOP}[\frac{1}{2}]$ *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, $[\![\mathbf{ZH}_{\mathrm{TH}}]\!] = [\![[\mathbf{ZH}_{\mathrm{TH}}]^{\mathrm{sop}}]\!] \subseteq [\![\mathbf{SOP}[\frac{1}{2}]]\!] = \left[\!\left[\left[\mathbf{SOP}[\frac{1}{2}]\right]^{\mathrm{ZH}}\right]\!\right] \subseteq [\![\mathbf{ZH}_{\mathrm{TH}}]\!]$, so:

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

5 Completeness for Toffoli-Hadamard

The point of this section is 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 7. $\forall D_1, D_2 \in \mathbf{ZH}_{\mathrm{TH}}, \quad \mathrm{ZH}_{\mathrm{TH}} \vdash D_1 = D_2 \implies [D_1]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} [D_2]^{\mathrm{sop}}$

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

Theorem 2. $\mathbf{SOP}[\frac{1}{2}]/\underset{\mathrm{TH}}{\sim}$ *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 3: $[\![[t_1]^{\mathrm{ZH}}]\!] = [\![[t_2]^{\mathrm{ZH}}]\!]$.
By completeness of $\mathbf{ZH}_{\mathrm{TH}}/\,\mathrm{ZH}_{\mathrm{TH}}$ (Theorem 1): $\mathrm{ZH}_{\mathrm{TH}} \vdash [t_1]^{\mathrm{ZH}} = [t_2]^{\mathrm{ZH}}$
Thanks to Proposition 7: $\left[[t_1]^{\mathrm{ZH}}\right]^{\mathrm{sop}} \underset{\mathrm{TH}}{\sim} \left[[t_2]^{\mathrm{ZH}}\right]^{\mathrm{sop}}$. Finally, by Proposition 5:

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

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

Lemma 2 (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:

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

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

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

6 Completeness for the whole Clifford Hierarchy

We show here how we can turn an $\mathbf{SOP}[\frac{1}{2^{n+1}}]$-morphism into an 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 $\mathbf{SOP}[\frac{1}{2^n}]$.

6.1 Ascending the Clifford Hierarchy

These transformations 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 3. *Let* $P = \sum m_i \in \mathbb{R}[X_1,\ldots,X_k]/(1, X_i^2 - X_i)$*, and* $t = s\sum e^{2i\pi P}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$*. Then:*

$$\left(s\sum |\boldsymbol{O}\rangle\langle y_0,...,y_k|\right)\circ \left(\sum e^{2i\pi m_1}\,|y_0,...,y_k\rangle\langle y_0,...,y_k|\right)\circ\ldots\circ\left(\sum e^{2i\pi m_\ell}\,|y_0,...,y_k\rangle\langle y_0,...,y_k|\right)\circ\left(\sum |y_0,...,y_k\rangle\langle\boldsymbol{I}|\right) \underset{\mathrm{HH}}{\overset{*}{\longrightarrow}} t$$

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

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

Lemma 4. $\left[\!\left[\frac{1}{\sqrt{2}}\sum e^{2i\pi\left(\frac{1}{8}+\frac{3}{4}y_0\right)}\right]\!\right] = 1$. *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 $[\![t']\!] = [\![t]\!]$.

Definition 4. *For any $k \geq 1$, we define the functor $\lfloor . \rfloor_k : \mathbf{SOP}[\frac{1}{2^{k+1}}]' \to \mathbf{SOP}[\frac{1}{2^k}]'$, first for morphisms $t = s\sum e^{2i\pi\frac{\ell}{2^{k+1}}y_{i_1}\cdots y_{i_q}}|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$ with phase polynomial of size 0 or 1:*

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

The functor is then extended to any $\mathbf{SOP}[\frac{1}{2^{k+1}}]'$-morphism by the decomposition of Lemma 3 (and given a particular ordering on the monomials of the phase polynomial).

Since $\lfloor . \rfloor_k$ is defined to be a functor, we have $\lfloor . \circ . \rfloor_k = \lfloor . \rfloor_k \circ \lfloor . \rfloor_k$. We can show that the ordering of the monomials has no real importance. Indeed, suppose $t_1 = \sum e^{2i\pi\frac{\ell_1}{2^{k+1}}y_{i_1}\cdots y_{i_q}}|\boldsymbol{y}\rangle\langle\boldsymbol{y}|$ and $t_2 = \sum e^{2i\pi\frac{\ell_2}{2^{k+1}}y_{j_1}\cdots y_{j_r}}|\boldsymbol{y}\rangle\langle\boldsymbol{y}|$. Then: $\lfloor t_1 \circ t_2 \rfloor_k = \lfloor t_2 \circ t_1 \rfloor_k$ quite obviously when either $l_1 \bmod 2 = 0$ or $l_2 \bmod 2 = 0$, but also when $l_1 \bmod 2 = l_2 \bmod 2 = 1$:

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

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

Proposition 8. $\forall t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]',\quad [\![t_1]\!] = [\![t_2]\!] \implies [\![\lfloor t_1 \rfloor_k]\!] = [\![\lfloor t_2 \rfloor_k]\!]$

6.2 Going Back

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

Definition 5. *We define the (partial) functor $\lceil . \rceil_k : \mathbf{SOP}[\frac{1}{2^k}]' \to \mathbf{SOP}[\frac{1}{2^{k+1}}]'$ 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 $\lceil . \rceil_k$ can only be applied on morphisms that have at least one input and one output.

Proposition 9. $\lceil \lfloor . \rfloor_k \rceil_k \underset{\text{TH}}{\sim} (.)$

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 3 (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 8:

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

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

$$\lfloor ... \lfloor t_1 \rfloor_k ... \rfloor_1 \underset{\mathrm{TH}}{\sim} \lfloor ... \lfloor t_2 \rfloor_k ... \rfloor_1$$

Finally, by Proposition 9: $t_1 \underset{\mathrm{TH}}{\sim} \lceil ... \lceil \lfloor ... \lfloor t_1 \rfloor_k ... \rfloor_1 \rceil_1 ... \rceil_k \underset{\mathrm{TH}}{\sim} \lceil ... \lceil \lfloor ... \lfloor t_2 \rfloor_k ... \rfloor_1 \rceil_1 ... \rceil_k \underset{\mathrm{TH}}{\sim} t_2$.

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

Lemma 5. *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:

$$\sum_{\boldsymbol{y}} e^{2i\pi\left(\frac{1}{8}+\frac{3}{4}y_0+R\right)} |\boldsymbol{O}\rangle\langle\boldsymbol{I}| \underset{y_0 \notin \mathrm{Var}(R,\boldsymbol{O},\boldsymbol{I})}{\longrightarrow} \sqrt{2} \sum_{\boldsymbol{y}\setminus\{y_0\}} e^{2i\pi R} |\boldsymbol{O}\rangle\langle\boldsymbol{I}| \qquad (\sqrt{2})$$

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

$$\sum_{\boldsymbol{y}} e^{2i\pi\left(\frac{y_0}{4}+\frac{y_0}{2}\widehat{Q}+R\right)} |\boldsymbol{O}\rangle\langle\boldsymbol{I}| \underset{y_0 \notin \mathrm{Var}(Q,R,\boldsymbol{O},\boldsymbol{I})}{\longrightarrow} \sqrt{2} \sum_{\boldsymbol{y}\setminus\{y_0\}} e^{2i\pi\left(\frac{1}{8}-\frac{1}{4}\widehat{Q}+R\right)} |\boldsymbol{O}\rangle\langle\boldsymbol{I}| \qquad (\omega)$$

which was already used in [3,16,23] to deal with the Clifford fragment of quantum mechanics.

Theorem 4 (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: $t_i' := \begin{cases} t_i & \text{if } t_i \in \mathbf{SOP}[\frac{1}{2^{k+1}}]' \\ t_i \otimes t_{\sqrt{2}} & \text{if } t_i \notin \mathbf{SOP}[\frac{1}{2^{k+1}}]' \end{cases}$.

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 3:

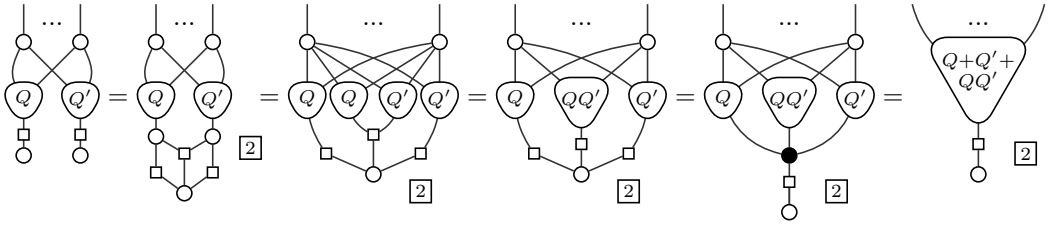
$$t_1 \underset{\mathrm{TH}'}{\sim} t_1' \underset{\mathrm{TH}'}{\sim} t_2' \underset{\mathrm{TH}'}{\sim} t_2$$

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 Clifford Hierarchy. As expected from the universality of the fragments at hand, the rewrite strategies given here are not confluent.

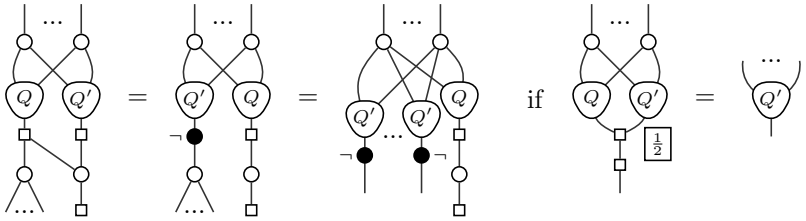
Using the translation from **SOP** to **ZH**, this time, we can make sense of the **SOP** rewrite rules as graphical ones. We will focus on the two rules that were not present in the previous works on **SOP**, namely (HHgen) and (HHnl). Let us start with the latter.

(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:



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 transformation, 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. 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.
6. 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.
7. 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.

8. 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.
9. 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.
10. Niel de Beaudrap, Xiaoning Bian, and Quanlong Wang. Fast and effective techniques for T-count reduction via spider nest identities, 2020. arXiv:2004.05164.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. Louis Lemonnier, John van de Wetering, and Aleks Kissinger. Hypergraph simplification: Linking the path-sum approach to the ZH-calculus, 2020. arXiv:2003.13564. arXiv:2003.13564.
17. Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5. Springer Science & Business Media, 2013.
18. 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.
19. Peter Selinger. A survey of graphical languages for monoidal categories. In *New Structures for Physics*, pages 289–355. Springer, 2010.
20. 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.
21. John van de Wetering and Sal Wolffs. Completeness of the Phase-free ZH-calculus, April 2019. arXiv:1904.07545. arXiv:1904.07545.
22. 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.
23. 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.
24. 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 (Proof of Proposition 1). 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):

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

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

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

- (HHnl):

$$A \circ t_1 \circ B = \sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}\widehat{Q}+\frac{y_0'}{2}\widehat{Q'}+R+\frac{\boldsymbol{O}\cdot\boldsymbol{x}+\boldsymbol{I}_A\cdot\boldsymbol{x}+\boldsymbol{I}\cdot\boldsymbol{x}'+\boldsymbol{O}_B\cdot\boldsymbol{x}'}{2}\right)} |\boldsymbol{O}_A\rangle\langle\boldsymbol{I}_B|$$
$$\xrightarrow[\text{HHnl}]{} 2\sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}(\widehat{Q}+\widehat{Q'}+\widehat{QQ'})+R+\frac{\boldsymbol{O}\cdot\boldsymbol{x}+\boldsymbol{I}_A\cdot\boldsymbol{x}+\boldsymbol{I}\cdot\boldsymbol{x}'+\boldsymbol{O}_B\cdot\boldsymbol{x}'}{2}\right)} |\boldsymbol{O}_A\rangle\langle\boldsymbol{I}_B|$$
$$= A \circ (2t_1[y_0' \leftarrow y_0 \oplus y_0 Q]) \circ B = A \circ t_2 \circ B$$

- (ket):

$$A \circ t_1 \circ B =$$
$$\sum e^{2i\pi\left(P_A+P_B+P+\frac{(\hat{O}_1+\hat{I}_{A1})x_1+\ldots+(y_0+\hat{O}_i'+\hat{I}_{Ai})x_i+\ldots+(\hat{O}_m+\hat{I}_{Am})x_m+\boldsymbol{I}\cdot\boldsymbol{x}'+\boldsymbol{O}_B\cdot\boldsymbol{x}'}{2}\right)} |\boldsymbol{O}_A\rangle\langle\boldsymbol{I}_B|$$
$$\xrightarrow[\text{HH}]{} 2\sum e^{2i\pi\left(P_A+P_B+P[y_0\leftarrow\widehat{O_i'\oplus I_{Ai}}]+\frac{\boldsymbol{O}[y_0\leftarrow\widehat{O_i'\oplus I_{Ai}}]\cdot\boldsymbol{x}+\boldsymbol{I}_A\cdot\boldsymbol{x}+\boldsymbol{I}[y_0\leftarrow\widehat{O_i'\oplus I_{Ai}}]\cdot\boldsymbol{x}'+\boldsymbol{O}_B\cdot\boldsymbol{x}'}{2}\right)} |\boldsymbol{O}_A\rangle\langle\boldsymbol{I}_B|$$
$$\xleftarrow[\text{HH}]{} \sum e^{2i\pi\left(P_A+P_B+P[y_0\leftarrow\widehat{y_0\oplus O_i'}]+\frac{\boldsymbol{O}[y_0\leftarrow\widehat{y_0\oplus O_i'}]\cdot\boldsymbol{x}+\boldsymbol{I}_A\cdot\boldsymbol{x}+\boldsymbol{I}[y_0\leftarrow\widehat{y_0\oplus O_i'}]\cdot\boldsymbol{x}'+\boldsymbol{O}_B\cdot\boldsymbol{x}'}{2}\right)} |\boldsymbol{O}_A\rangle\langle\boldsymbol{I}_B|$$
$$= A \circ t_1[y_0 \leftarrow y_0 \oplus O_i'] \circ B = A \circ t_2 \circ B$$

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

$$A \circ t_1 \circ B = \sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}+R+\frac{\boldsymbol{O}\cdot\boldsymbol{x}+\boldsymbol{I}_A\cdot\boldsymbol{x}+\boldsymbol{I}\cdot\boldsymbol{x}'+\boldsymbol{O}_B\cdot\boldsymbol{x}'}{2}\right)} |\boldsymbol{O}_A\rangle\langle\boldsymbol{I}_B| \xrightarrow[\text{Z}]{} \sum e^{2i\pi\left(\frac{y_0}{2}\right)} |\boldsymbol{0}\rangle\langle\boldsymbol{0}|$$
$$\xleftarrow[\text{Z}]{} \sum e^{2i\pi\left(P_A+P_B+\frac{y_0}{2}+\frac{\boldsymbol{0}\cdot\boldsymbol{x}+\boldsymbol{I}_A\cdot\boldsymbol{x}+\boldsymbol{0}\cdot\boldsymbol{x}'+\boldsymbol{O}_B\cdot\boldsymbol{x}'}{2}\right)} |\boldsymbol{O}_A\rangle\langle\boldsymbol{I}_B| = A \circ t_2 \circ B$$

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

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

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

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

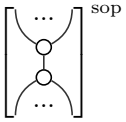
$$= 2 \sum_{\boldsymbol{y} \in \{0,1\}^{k-1}} e^{2i\pi\left(\frac{y_0}{2}(\widehat{Q}+\widehat{Q'}+\widehat{QQ'})+R\right)} |\boldsymbol{O}\rangle\langle\boldsymbol{I}|$$
$$= [\![2t[y'_0 \leftarrow y_0 \oplus y_0 Q]]\!]$$

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

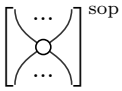
Proof (Proof of Proposition 7). We show that all the rules of $\underset{\text{TH}}{\longrightarrow}$ hold in $\mathbf{SOP}[\frac{1}{2}]$.

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):

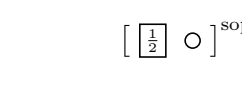


$$= \frac{1}{2} \sum e^{2i\pi \frac{y_0+y_1}{2} y'} |y_1, ..., y_1\rangle\langle y_0, ..., y_0|$$

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

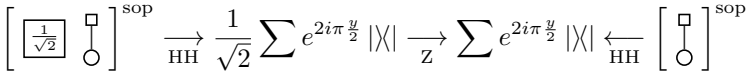


(IV):

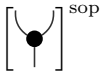


$$\underset{\text{Elim}}{\longrightarrow} 1 =$$

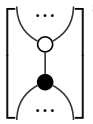
(Z):



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

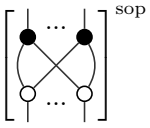


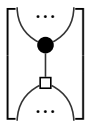
$\underset{\text{HH}}{\longrightarrow} \sum |y_0 \oplus y_1\rangle\langle y_0, y_1|$:



$$\underset{\text{HH}}{\longrightarrow} \frac{1}{2} \sum e^{2i\pi \frac{y_1+...+y_n+y_0}{2} y'} |y_1, ..., y_n\rangle\langle y_0, ..., y_0|$$

$$\underset{\text{HH}(y', [y_0 \leftarrow y_1 \oplus ... \oplus y_n])}{\longrightarrow} \sum |y_1, ..., y_n\rangle\langle y_1 \oplus ... \oplus y_n, ..., y_1 \oplus ... \oplus y_n| \underset{\text{HH}}{\longleftarrow}$$

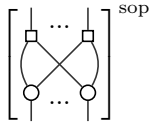




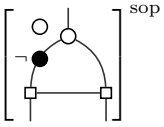
$$\underset{\text{HH}}{\longrightarrow} \frac{1}{2} \sum e^{2i\pi\left(\frac{y_1 ... y_m y'}{2} + \frac{x_1+...+x_n+y'}{2} y''\right)} |y_1, ..., y_m\rangle\langle x_1, ...x_n|$$

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

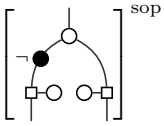
$$\underset{\text{HH}}{\longleftarrow}$$



(O):



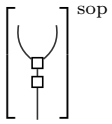
$$\xrightarrow[\text{HH}]{} 2\sum e^{2i\pi\left(\frac{1}{2}y_0y_2y_3+\frac{1}{2}y_0y_3+\frac{1}{2}y_1y_2y_3\right)}|y_0,y_1\rangle\langle y_2|$$



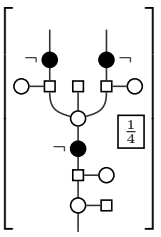
$$\xrightarrow[\text{HH}]{} \sum e^{2i\pi\left(\frac{1}{2}y_0y_1+\frac{1}{2}y_2y_3y_4+\frac{1}{2}y_0y_1y_4\right)}|y_0,y_3\rangle\langle y_4|$$

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

(&):



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



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

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

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

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

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

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

Proof (Proof of Proposition 8). 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 3. Let $t = s \sum e^{2i\pi \frac{\ell}{2^{k+1}} y_{i_1} \dots y_{i_q}} |\boldsymbol{O}\rangle\langle \boldsymbol{I}|$ 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:

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

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

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

so:

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

and

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

Proof (Proof of Proposition 9). Again, we can use the decomposition given in Lemma 3. We can show that if $t = s \sum e^{2i\pi \frac{\ell}{2^{k+1}} y_{i_1} \dots y_{i_q}} |\boldsymbol{O}\rangle\langle \boldsymbol{I}|$, 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:

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

$$\xrightarrow[\mathrm{HH}(y'',[y_0\leftarrow y'\oplus y_{i_1}\ldots y_{i_q}])]{} s\sum e^{2i\pi\left(\frac{y_{i_1}\cdots y_{i_q}}{2^k}\left((\ell-1)/2+y'\right)+\frac{y'+y_{i_1}\cdots y_{i_q}-2y'y_{i_1}\cdots y_{i_q}}{2^{k+1}}\right)}|\boldsymbol{O},y'\rangle\langle\boldsymbol{I}|$$
$$= s\sum e^{2i\pi\left(\ell\frac{y_{i_1}\cdots y_{i_q}}{2^k}+\frac{y'}{2^{k+1}}\right)}|\boldsymbol{O},y'\rangle\langle\boldsymbol{I}| = t\otimes\sum e^{2i\pi\frac{y_0}{2^{k+1}}}|y_0\rangle$$

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 $\lfloor t\rfloor_k\circ(id_n\otimes\sum e^{2i\pi\frac{y_0}{2^{k+1}}}|y_0\rangle)\underset{\mathrm{TH}}{\sim}t\otimes\sum e^{2i\pi\frac{y_0}{2^{k+1}}}|y_0\rangle$. Finally:

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