



**HAL**  
open science

# Rewriting and Completeness of Sum-Over-Paths in Dyadic Fragments of Quantum Computing

Renaud Vilmart

► **To cite this version:**

Renaud Vilmart. Rewriting and Completeness of Sum-Over-Paths in Dyadic Fragments of Quantum Computing. Logical Methods in Computer Science, 2024, 20 (1), 10.46298/LMCS-20(1:20)2024 . hal-04496100

**HAL Id: hal-04496100**

**<https://hal.science/hal-04496100v1>**

Submitted on 8 Mar 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

## REWRITING AND COMPLETENESS OF SUM-OVER-PATHS IN DYADIC FRAGMENTS OF QUANTUM COMPUTING \*

RENAUD VILMART 

Université Paris-Saclay, CNRS, ENS Paris-Saclay, Inria, LMF, 91190, Gif-sur-Yvette, France  
*e-mail address*: [renaud.vilmart@inria.fr](mailto:renaud.vilmart@inria.fr)

**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. We provide generalisations of the presented rewrite rules, that can prove useful when trying to reduce terms in practice, and we show how to graphically make sense of these new rules.

We show how to enrich the rewrite system to reach completeness for the dyadic fragments of quantum computation, used in particular in the Quantum Fourier Transform, and obtained by adding phase gates with dyadic multiples of  $\pi$  to the Toffoli-Hadamard gate-set.

Finally, we show how to perform sums and concatenation of arbitrary terms, something which is not native in a system designed for analysing gate-based quantum computation, but necessary when considering Hamiltonian-based quantum computation.

### 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 [Amy19]. Its first important feature is its capacity to translate from most common (gate-based) 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.

---

*Key words and phrases:* Quantum Computation, Verification, Sum-Over-Paths, Rewrite Strategy, Toffoli-Hadamard, Completeness.

\* Extended version of the CSL’23 paper [Vil23].

The author acknowledges support from the PEPR integrated project EPiQ ANR-22-PETQ-0007 part of Plan France 2030, the ANR projects TaQC ANR-22-CE47-0012 and HQI ANR-22-PNCQ-0002, as well as the European project HPCQS..

Despite its links [Lem19, LvdWK21] with graphical languages such as the ZH-calculus [BK19] – 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 proves  $\mathcal{C}_1$  and  $\mathcal{C}_2$  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. [dBBW20, KvdW20]) to check precisely for circuit equivalence. It was later extended to account for families of morphisms and used within the Qbricks environment [CBB<sup>+</sup>21, CBL<sup>+</sup>21] 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 [HRA<sup>+</sup>22].

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 [AG04], 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 [Amy19] 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 [Vil21] 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, deciding circuit equivalence would become polynomial, while we know that it is QMA-complete – a quantum variant of NP-complete – [Boo14, JWB05]. 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. This paper extends [Vil23] which was presented at the Computer Science and Logic 2023 (CSL’23). Here we slightly simplify the rewrite system, provide further potential simplification rules, of which we give a graphical treatment, and finally show how to perform two non-trivial operations on SOP terms, namely their sum and their concatenation, both very useful when building arbitrary maps or when considering Hamiltonian-based computation, and which remain in the dyadic fragment at hand. Since the presentation of [Vil23], a complete rewrite system was given to Sum-Over-Paths with arbitrary phases and complex entries [Amy23], although in the “unbalanced” framework, which is noticeably different.

**Structure of the paper.** We first review the Sum-Over-Paths formalism in section 2, providing a rewrite strategy for Toffoli-Hadamard, as well as generalised rules. We then present the ZH-calculus in section 3 and the links between the two in section 4, and we show how to interpret the new rewrite rules of SOP graphically. We then show the completeness result for the Toffoli-Hadamard fragment in section 5. The extension to the dyadic fragments is then handled in section 6. Finally, in section 7, we show a way to “control” arbitrary terms allowing for their sum and their concatenation.

## 2. SUMS-OVER-PATHS

**2.1. The Morphisms.** Sums-Over-Paths [Amy19] 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 [ML13, Sel10] denoted **Qubit** where the objects are natural numbers (this makes the category a PROP [Lac04, Zan15]), where morphisms from  $n$  to  $m$  are linear maps  $\mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^m}$ , 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*  $\sigma_{n,m} : n+m \rightarrow m+n$ , as well as a *compact structure*  $(\eta_n : 0 \rightarrow 2n, \epsilon_n : 2n \rightarrow 0)$ . 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 [Sel10].

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  $|0\rangle = (1 \ 0)^\top$  and  $|1\rangle = (0 \ 1)^\top$ . 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  $|x\rangle\langle y| := |x\rangle \otimes \langle y|$ .

We give in the following the definition of Sum-Over-Paths of [Vil21], which differs from [Amy19] in the way the input qubits are treated, by making them more symmetric with the outputs. This makes some concepts, like the  $\dagger$  or the compact structure, more natural.

**Definition 2.1 (SOP).** We define **SOP** as the collection of objects  $\mathbb{N}$  and morphisms between them that are tuples  $f : n \rightarrow m := (s, \vec{y}, P, \vec{O}, \vec{I})$ , 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,  $P \in \mathbb{R}[X_1, \dots, X_k]/(X_i^2 - X_i)$  is called the *phase polynomial* of  $f$ <sup>1</sup>,  $\vec{O} \in (\mathbb{F}_2[X_1, \dots, X_k])^m$  and  $\vec{I} \in (\mathbb{F}_2[X_1, \dots, X_k])^n - \mathbb{F}_2$  being the binary field, whose only two elements are its additive and multiplicative identities, denoted 0 and 1.

Compositions are obtained as<sup>2</sup>:

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

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  $\eta_m = \sum_{\vec{y}} |\vec{y}, \vec{y}\rangle \langle |$  and  $\epsilon_n = \sum_{\vec{y}} | \rangle \langle \vec{y}, \vec{y}|$

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

- The  $\dagger$ -functor is given by:  $f^\dagger := s \sum_{\vec{y}} e^{-2i\pi P} \left| \vec{I} \right\rangle \left\langle \vec{O} \right|$
- The functor  $\llbracket \cdot \rrbracket : \mathbf{SOP} \rightarrow \mathbf{Qubit}$  is defined as:  $\llbracket f \rrbracket := s \sum_{\vec{y} \in \{0,1\}^k} e^{2i\pi P(\vec{y})} \left| \vec{O}(\vec{y}) \right\rangle \left\langle \vec{I}(\vec{y}) \right|$

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

**Remark 2.2.** In the sequential composition  $(\cdot \circ \cdot)$ , the term  $\widehat{O}_g \cdot \vec{y}$  is to be understood as

$$\widehat{O}_g \cdot \vec{y} = \widehat{O}_{g_1} \cdot y_1 + \dots + \widehat{O}_{g_m} \cdot y_m$$

where  $\vec{O}_g = (O_{g_1}, \dots, O_{g_m})$  and  $\vec{y} = (y_1, \dots, y_m)$ ; and where the map  $\widehat{(\cdot)} : \mathbb{F}_2[X_1, \dots, X_k] \rightarrow \mathbb{R}[X_1, \dots, X_k]/(X_i^2 - X_i)$ , which translates a boolean polynomial into a phase polynomial,

<sup>1</sup>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  $P = P \times 1 = P \times 0 = 0$ .

<sup>2</sup>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...

is inductively defined as:

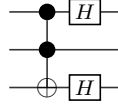
$$\widehat{Q_1 Q_2} = \widehat{Q_1} \widehat{Q_2} \quad \widehat{Q_1 \oplus Q_2} = \widehat{Q_1} + \widehat{Q_2} - 2\widehat{Q_1} \widehat{Q_2} \quad \widehat{y}_i = y_i \quad \widehat{\alpha} = \alpha$$

This translation will also be used in most of the upcoming rewrite rules of the system.

**Example 2.3.** 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:

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

It can be checked that both operators are unitary. To illustrate the compositions of **SOP** terms, we can focus on the following quantum circuit:



which is a graphical representation of  $(H \otimes id \otimes H) \circ \text{Tof}$  (spatial composition represents the tensor product, while sequential composition represents the usual composition). The term  $H \otimes id \otimes H$  can be built as follows (renaming the variables so as to avoid collisions):

$$\begin{aligned} H \otimes id \otimes H &= \left( \frac{1}{\sqrt{2}} \sum_{y_0, y_1} e^{2i\pi \frac{y_0 y_1}{2}} |y_1\rangle\langle y_0| \right) \otimes \left( \sum_{y_2} e^{2i\pi \times 0} |y_2\rangle\langle y_2| \right) \otimes \left( \frac{1}{\sqrt{2}} \sum_{y_3, y_4} e^{2i\pi \frac{y_3 y_4}{2}} |y_4\rangle\langle y_3| \right) \\ &= \frac{1}{2} \sum_{y_0, \dots, y_4} e^{2i\pi \left( \frac{y_0 y_1}{2} + \frac{y_3 y_4}{2} \right)} |y_1, y_2, y_4\rangle\langle y_0, y_2, y_3| \end{aligned}$$

The **SOP** term  $t = (H \otimes id \otimes H) \circ \text{Tof}$  is then computed as:

$$\begin{aligned} t &= \left( \frac{1}{2} \sum_{y_0, \dots, y_4} e^{2i\pi \left( \frac{y_0 y_1}{2} + \frac{y_3 y_4}{2} \right)} |y_1, y_2, y_4\rangle\langle y_0, y_2, y_3| \right) \circ \left( \sum_{y_5, y_6, y_7} |y_5, y_6, y_7 \oplus y_5 y_6\rangle\langle y_5, y_6, y_7| \right) \\ &= \frac{1}{2^4} \sum_{y_0, \dots, y_{10}} e^{2i\pi \left( \frac{y_0 y_1}{2} + \frac{y_3 y_4}{2} + y_8 \frac{y_0 + y_5}{2} + y_9 \frac{y_2 + y_6}{2} + y_{10} \frac{y_3 + y_7 \oplus y_5 y_6}{2} \right)} |y_1, y_2, y_4\rangle\langle y_5, y_6, y_7| \\ &= \frac{1}{2^4} \sum_{y_0, \dots, y_{10}} e^{2i\pi \left( \frac{y_0 y_1}{2} + \frac{y_3 y_4}{2} + y_8 \frac{y_0 + y_5}{2} + y_9 \frac{y_2 + y_6}{2} + y_{10} \frac{y_3 + y_7 + y_5 y_6}{2} \right)} |y_1, y_2, y_4\rangle\langle y_5, y_6, y_7| \end{aligned}$$

where the last equality is obtained thanks to  $y_{10} \frac{y_7 \oplus y_5 y_6}{2} = y_{10} \left( \frac{y_7 + y_5 y_6}{2} - y_5 y_6 y_7 \right) = y_{10} \frac{y_7 + y_5 y_6}{2}$  when taken modulo 1.

As is customary, and as was already done in the previous example, we consider equality of the SOP morphisms up to  $\alpha$ -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  $O_{g_i} = I_{f_i}$  for all  $0 \leq i < m$ . Indeed, when summing over the variable  $y_i$ , we get  $(1 + e^{i\pi(O_{g_i} + I_{f_i})})$  – which is non-null only when  $O_{g_i} = I_{f_i}$  – 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 [Vil21], 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  $\sim_{\text{TH}}$  (the symmetric and transitive closure of  $\xrightarrow{\text{TH}}$ ).

$$\begin{aligned}
& \sum_{\vec{y}} e^{2i\pi P} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| \xrightarrow{y_0 \notin \text{Var}(P, \vec{O}, \vec{I})} 2 \sum_{\vec{y} \setminus \{y_0\}} e^{2i\pi P} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| \quad (\text{Elim}) \\
t = \sum_{\vec{y}} e^{2i\pi \left( \frac{y_0}{2} (y_i \widehat{Q} + \widehat{Q}' + 1) + R \right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| & \xrightarrow{\substack{y_0 \notin \text{Var}(Q, Q', R, \vec{O}, \vec{I}) \\ y_i \notin \text{Var}(Q, Q') \\ QQ' = Q}} t[y_i \leftarrow 1 \oplus Q'] \quad (\text{HHgen}) \\
t = \sum_{\vec{y}} e^{2i\pi(P)} \left| \dots, \overbrace{y_0 \oplus O'_i}^{O_i}, \dots \right\rangle \left\langle \vec{I} \right| & \xrightarrow{\substack{O'_i \neq 0 \\ y_0 \notin \text{Var}(O_1, \dots, O_{i-1}, O'_i)}} t[y_0 \leftarrow O_i] \quad (\text{ket}) \\
t = \sum_{\vec{y}} e^{2i\pi(P)} \left| \vec{O} \right\rangle \left\langle \dots, \overbrace{y_0 \oplus I'_i}^{I_i}, \dots \right| & \xrightarrow{\substack{I'_i \neq 0 \\ y_0 \notin \text{Var}(\vec{O}, I_1, \dots, I_{i-1}, I'_i)}} t[y_0 \leftarrow I_i] \quad (\text{bra}) \\
s \sum_{\vec{y}} e^{2i\pi \left( \frac{y_0}{2} + R \right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| & \xrightarrow{\substack{R \neq 0 \text{ or } \vec{O}, \vec{I} \neq \vec{0} \\ y_0 \notin \text{Var}(R, \vec{O}, \vec{I})}} \sum_{y_0} e^{2i\pi \left( \frac{y_0}{2} \right)} |0, \dots, 0\rangle \langle 0, \dots, 0| \quad (\text{Z})
\end{aligned}$$

Figure 1: Rewrite system  $\xrightarrow{\text{TH}}$

We need in the conditions of all the rules the function  $\text{Var}$ , 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 [Vil21], 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 cornerstone rule of [Amy19] and [Vil21] denoted (HH) was given as:

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

It has been generalised into (HHgen) here ((HH) is the special case where  $Q = 1$ ). It is important to notice that the rule (HHgen) requires that  $QQ' = Q$ . Rule (HH) is so often used that we may, in the following, distinguish it from (HHgen).

**Example 2.4.** Recall the term:

$$t = \frac{1}{2^4} \sum_{y_0, \dots, y_{10}} e^{2i\pi(\frac{y_0 y_1}{2} + \frac{y_3 y_4}{2} + y_8 \frac{y_0 + y_5}{2} + y_9 \frac{y_2 + y_6}{2} + y_{10} \frac{y_3 + y_7 + y_5 y_6}{2})} |y_1, y_2, y_4\rangle\langle y_5, y_6, y_7|$$

we got from Example 2.3. Its internal variables are  $y_0, y_3, y_8, y_9, y_{10}$ . It is often the case that the variables created by the sequential composition ( $y_8, y_9$  and  $y_{10}$  here), can be used right away to rewrite the term using (HH). For instance, the term  $\frac{y_8}{2}(y_0 + y_5)$  where  $y_8$  appears nowhere else in the morphism, allows for an application of the rule, that will replace  $y_0$  by  $y_5$  (or vice-versa). We get:

$$t \xrightarrow{\text{HH}} \frac{1}{2^4} \sum_{y_1, \dots, y_{10}} e^{2i\pi(\frac{y_5 y_1}{2} + \frac{y_3 y_4}{2} + y_9 \frac{y_2 + y_6}{2} + y_{10} \frac{y_3 + y_7 + y_5 y_6}{2})} |y_1, y_2, y_4\rangle\langle y_5, y_6, y_7|$$

The rule (HH) can always be followed by (Elim): here  $y_8$  remains in the variables, but isn't used anywhere anymore.  $t$  can then be further reduced to:

$$\frac{1}{2^3} \sum_{\substack{y_i \\ i \in \{1, 2, 3, 4, 5, 6, 7, 9, 10\}}} e^{2i\pi(\frac{y_5 y_1}{2} + \frac{y_3 y_4}{2} + y_9 \frac{y_2 + y_6}{2} + y_{10} \frac{y_3 + y_7 + y_5 y_6}{2})} |y_1, y_2, y_4\rangle\langle y_5, y_6, y_7|$$

Proceeding similarly for  $y_9$  and  $y_{10}$ , we get:

$$\begin{aligned} t &\rightarrow^* \frac{1}{2^2} \sum_{\substack{y_i \\ i \in \{1, 3, 4, 5, 6, 7, 10\}}} e^{2i\pi(\frac{y_5 y_1}{2} + \frac{y_3 y_4}{2} + y_{10} \frac{y_3 + y_7 + y_5 y_6}{2})} |y_1, y_6, y_4\rangle\langle y_5, y_6, y_7| \\ &\rightarrow^* \frac{1}{2} \sum_{\substack{y_i \\ i \in \{1, 4, 5, 6, 7\}}} e^{2i\pi(\frac{y_5 y_1}{2} + \frac{y_4 y_7}{2} + \frac{y_4 y_5 y_6}{2})} |y_1, y_6, y_4\rangle\langle y_5, y_6, y_7| \end{aligned}$$

The term cannot be reduced further with the rewrite system  $\xrightarrow{\text{TH}}$ .

In the following, we assume that (Elim) is always applied after (HH), without necessarily mentioning it.

The rules (HH), (HHgen) and (Z) all stem from a particular observation: In the morphism  $t = \sum e^{2i\pi(\frac{y_0}{2}\hat{Q}+R)} |\vec{O}\rangle\langle \vec{I}|$  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 – and the conditions on  $R$ ,  $\vec{O}$  and  $\vec{I}$  are simply here to avoid applying the rule indefinitely.

The rule (HH) deals with a case where the polynomial  $Q$  can be forced to 0, whilst the rule (HHgen) more generally deals with a case where one of the variables in the polynomial  $Q$  is forced to get a precise value due to the form of the polynomial.

The rule (HH) is of particular interest. It was introduced in [Amy19] and gives enough power to the formalism to become a †-compact PROP [Vil21]. We can extend this result here thanks to:

**Proposition 2.5.**

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



*Proof.* The result is obvious for the tensor product  $(\cdot \otimes \cdot)$ . For the composition, we show that if  $t_1 \xrightarrow{\text{TH}} t_2$  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  $\xrightarrow{\text{TH}}$ :

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

$$\begin{aligned} A \circ t_1 \circ B &= \sum e^{2i\pi \left( P_A + P_B + \frac{y_0}{2} (y_i \widehat{Q} + \widehat{Q}') + 1 \right) + R + \frac{\vec{O} \cdot \vec{x} + \vec{I}_A \cdot \vec{x} + \vec{I} \cdot \vec{x}' + \vec{O}_B \cdot \vec{x}'}{2}} \left| \vec{O}_A \right\rangle \left\langle \vec{I}_B \right| \\ \xrightarrow{\text{HHgen}} \sum e^{2i\pi \left( P_A + P_B + \frac{y_0}{2} (\widehat{Q} + 1) + R [y_i \leftarrow 1 \oplus \widehat{Q}'] + \frac{\vec{O} [y_i \leftarrow 1 \oplus \widehat{Q}'] \cdot \vec{x} + \vec{I}_A \cdot \vec{x} + \vec{I} [y_i \leftarrow 1 \oplus \widehat{Q}'] \cdot \vec{x}' + \vec{O}_B \cdot \vec{x}'}{2}} \right)} \left| \vec{O}_A \right\rangle \left\langle \vec{I}_B \right| \\ &= A \circ t_1 [y_i \leftarrow 1 \oplus \widehat{Q}'] \circ B = A \circ t_2 \circ B \end{aligned}$$

- (ket):

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

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

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

Thanks to this Proposition, and since  $\mathbf{SOP} / \underset{\text{HH}}{\sim}$  is a  $\dagger$ -compact PROP by [Vil21], we get:

**Corollary 2.6.**  $\mathbf{SOP} / \underset{\text{TH}}{\sim}$  is a  $\dagger$ -compact PROP.

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

**Proposition 2.7** (Soundness). *For any two SOP morphisms  $t_1$  and  $t_2$ , if  $t_1 \xrightarrow{\text{TH}}^* t_2$ , then  $\llbracket t_1 \rrbracket = \llbracket t_2 \rrbracket$ .*

*Proof.* We mean to show that for any single step rewrite, the interpretation is preserved. As most of the rules were present in [Amy19] or [Vil21], this was proven for them. It remains to show the result for (HHgen). The soundness of a stronger version of (HHgen) is proven in upcoming Lemma 2.11. The result is then a direct consequence of this.  $\square$

The addition of the rule (HHgen) allows for further reductions:

**Example 2.8.** The following morphism:

$$\sum_{\vec{y}} e^{2i\pi\left(\frac{y_0 y_1 y_2}{2} + \frac{y_2}{2} + \frac{y_1 y_2 y_3}{2} + \frac{y_0 y_1 y_2 y_3}{2}\right)} |y_3\rangle\langle y_0|$$

is irreducible using the rules of [Amy19] and [Vil21]. However, here it can be reduced to:

$$\sum_{\vec{y}} e^{2i\pi\left(\frac{y_0 y_1 y_2}{2} + \frac{y_2}{2} + \frac{y_1 y_2 y_3}{2} + \frac{y_0 y_1 y_2 y_3}{2}\right)} |y_3\rangle\langle y_0| \xrightarrow[y_1 \leftarrow 1]{\text{HHgen}} \sum_{y_0, y_2, y_3} e^{2i\pi\left(\frac{y_0 y_2}{2} + \frac{y_2}{2} + \frac{y_2 y_3}{2} + \frac{y_0 y_2 y_3}{2}\right)} |y_3\rangle\langle y_0|$$

where the rewrite can be made clearer by writing the phase polynomial as  $\frac{y_2}{2}(y_1(y_0 + y_3 + y_2 y_3) + 0 + 1)$  and checking that (obviously)  $(y_0 + y_3 + y_2 y_3) \times 0 = 0$ .

**2.3. Generalising Rules.** In [Vil23] another rule was introduced to allow for the proof of completeness:

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

This rule was only used when proving that one of the axioms of  $\text{ZH}_{\text{TH}}$  from [vdWW19] was provable with  $\widetilde{\cdot}_{\text{TH}}$ . However, it was proven in [BKMB<sup>+</sup>23] that this axiom could be replaced by two simpler ones and otherwise provable, hence making (HHnl) unnecessary for completeness, as will be shown in the following of the paper.

Completeness however assumes rules can be used both ways, while we ideally only want to reduce a term when analysing it. With this in mind, it is relevant to look for rules that allow for further reduction, and (HHnl) is one of them.

**Example 2.9.** The following term, while irreducible with  $\xrightarrow{\text{TH}}$ , can be reduced using (HHnl):

$$\begin{aligned} & \sum_{y_0, y_1, y_2, y_3, y_4} e^{2i\pi\left(\frac{y_0 y_1 y_2}{2} + \frac{y_2}{2} + \frac{y_2 y_3 y_4}{2}\right)} |y_4\rangle\langle y_0| \\ & \xrightarrow[\text{HHnl}]{} 2 \sum_{y_3 \leftarrow y_1 \oplus y_0 y_1 y_2} e^{2i\pi\left(\frac{y_0 y_1 y_2}{2} + \frac{y_2}{2} + \frac{y_1 y_2 y_4}{2} + \frac{y_0 y_1 y_2 y_4}{2}\right)} |y_4\rangle\langle y_0| \end{aligned}$$

As (HHnl) is not necessary for completeness, it should be possible to derive it from the rules of  $\xrightarrow{\text{TH}}$ :

**Lemma 2.10.** (HHnl) can be derived from  $\xrightarrow{\text{TH}}$ .

*Proof.* Consider the term:

$$\sum e^{2i\pi\left(\frac{y_0}{2} + \frac{y_0 y_1 (\widehat{Q}+1)}{2} + \frac{y_1 y'_0}{2} + \frac{y'_0 (\widehat{Q}'+1)}{2} + R\right)} \left| \vec{O} \right\rangle\left\langle \vec{I} \right|$$

We can rewrite it in two different ways, which give both sides of the (HHnl) rule:

$$\begin{aligned} & \sum e^{2i\pi\left(\frac{y_0}{2} + \frac{y_0 y_1 (\widehat{Q}+1)}{2} + \frac{y_1 y'_0}{2} + \frac{y'_0 (\widehat{Q}'+1)}{2} + R\right)} \left| \vec{O} \right\rangle\left\langle \vec{I} \right| \\ & \quad \downarrow \text{HHgen}(y_1 \leftarrow 1) \qquad \qquad \qquad \downarrow \text{HH}(y_1 \leftarrow Q' \oplus 1) \\ & \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q} + \frac{y'_0}{2}\widehat{Q}' + R\right)} \left| \vec{O} \right\rangle\left\langle \vec{I} \right| \qquad \qquad \qquad 2 \sum e^{2i\pi\left(\frac{y_0}{2}(\widehat{Q} + \widehat{Q}' + \widehat{Q}\widehat{Q}') + R\right)} \left| \vec{O} \right\rangle\left\langle \vec{I} \right| \quad \square \end{aligned}$$

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) itself can be generalised to:

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

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 [SIS<sup>+</sup>11], while instances (HHgen) can easily be found. (HHgen) can be seen as a particular case of (HHgen'), where  $Q' \leftarrow QQ'$ , as  $Q \times QQ' = QQ'$ .

The previous observation can be made into another rule, which again uses the fact that when a term has a phase polynomial of the form  $\frac{y_0}{2}\widehat{Q} + R$  with  $y_0$  internal, then we can force  $Q$  to be 0. This means we can replace  $R$  by a remainder in the euclidean division of  $R$  by  $Q$ :

$$\sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q}+\widehat{S}\widehat{Q}+\widehat{R}\right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| \xrightarrow[\substack{y_0 \notin \text{Var}(Q, S, R, \vec{O}, \vec{I})}]{} \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q}+\widehat{R}\right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| \quad (\text{Rem})$$

Notice that, in contrast with the (HH), (HHgen) and (HHgen'), this rule does not reduce the number of variables, but instead equates polynomials that are equivalent “modulo  $Q$ ”. In practice, this rule is also hard to use as it again uses Groebner bases to properly implement. The proximity between the last two aforementioned rules is not surprising once we realise that (Rem) can be deduced from (HHgen) and (HHgen'):

$$\begin{array}{ccc} \sum e^{2i\pi\left(\frac{y_0}{2}(y_i(1+\widehat{Q})+(1+\widehat{Q})\widehat{S}+1)+\frac{\widehat{S}}{2}+\frac{y_i}{2}+\frac{1}{2}+R\right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| & & \\ \text{HHgen}(y_i \leftarrow (1 \oplus Q)S \oplus 1) \downarrow & & \downarrow \text{HHgen}'(y_i \leftarrow S \oplus 1) \\ \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q}+\widehat{S}\widehat{Q}+R\right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| & & \sum e^{2i\pi\left(\frac{y_0}{2}\widehat{Q}+R\right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right| \end{array}$$

We can show that (HHgen') is sound, which implies that (HHgen) – as a particular case – and both (HHnl) and (Rem) – as a compositions of particular cases of (HHgen') – are also sound:

**Lemma 2.11.** *(HHgen') is sound.*

*Proof.* If  $t = \sum_{\vec{y} \in V^k} e^{2i\pi\left(\frac{y_0}{2}(y_i\widehat{Q}+\widehat{Q}\widehat{Q}'+1)+R\right)} \left| \vec{O} \right\rangle \left\langle \vec{I} \right|$ , then:

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

$$= \llbracket t[y_i \leftarrow 1 \oplus Q'] \rrbracket \quad \square$$

While we have identified stronger rewrite rules than the ones in  $\widetilde{\text{TH}}$ , as the rest of the paper is mainly focussed on completeness, we stick to the rules of  $\widetilde{\text{TH}}$ , since, as we shall see later, they are enough for that particular problem.

### 3. THE ZH-CALCULUS

As a foundation towards completeness of the Toffoli-Hadamard fragment of **SOP**, we will use a similar result on another formalism: the graphical calculus ZH.

The graphical calculi ZX, ZW and ZH [BK19, CD11, CK10] are calculi for quantum computing, with a tight link with the Sum-Over-Paths formalism [Lem19, LvdWK21, Vil21], and whose completeness was proven in particular for the Toffoli-Hadamard fragment [BKMB<sup>+</sup>23, Had15, vdWW19, Vil19].

This fragment of quantum mechanics is approximately universal [Aha03, Shi03], 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.

**3.1. The Diagrams and their Interpretation.** 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:

- $Z_m^n : n \rightarrow m :: \begin{array}{c} \cdots \\ \circ \\ \cdots \end{array}$ , called Z-spider
- $H_m^n(r) : n \rightarrow m :: \begin{array}{c} \cdots \\ \boxed{r} \\ \cdots \end{array}$ , 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  $\dagger$ -compact PROP, which means it also has a symmetric structure  $\sigma_{n,m} :: \begin{array}{c} \cdots \quad \cdots \\ \times \\ \cdots \quad \cdots \end{array}$ , a compact structure  $(\eta_n :: \begin{array}{c} \cdots \quad \cdots \\ \curvearrowright \\ \cdots \quad \cdots \end{array}, \epsilon_n :: \begin{array}{c} \cdots \quad \cdots \\ \curvearrowleft \\ \cdots \quad \cdots \end{array})$ , and a  $\dagger$ -functor  $(\cdot)^\dagger : \mathbf{ZH}^{\text{op}} \rightarrow \mathbf{ZH}$ . It is defined by:  $(Z_m^n)^\dagger := Z_n^m$  and  $(H_m^n(r))^\dagger := H_n^m(\bar{r})$  where  $\bar{r}$  is the complex conjugate of  $r$ . For convenience, we define two additional spiders:

$$\begin{array}{c} \cdots \\ \bullet \\ \cdots \end{array} := \begin{array}{c} \cdots \\ \circ \\ \cdots \end{array} \begin{array}{c} \cdots \\ \square \\ \cdots \end{array} \begin{array}{c} \frac{1}{2} \end{array} \quad \text{and} \quad \begin{array}{c} \cdots \\ \bullet \\ \cdots \end{array} := \begin{array}{c} \cdots \\ \circ \\ \cdots \end{array} \begin{array}{c} \cdots \\ \square \\ \cdots \end{array} \begin{array}{c} \frac{1}{2} \end{array}$$

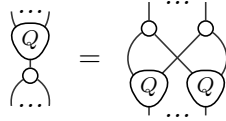
The language comes with a way of interpreting the morphisms as morphisms of **Qubit**. The standard interpretation  $\llbracket \cdot \rrbracket : \mathbf{ZH} \rightarrow \mathbf{Qubit}$  is a  $\dagger$ -compact-PROP-functor, defined as:

$$\begin{aligned} \llbracket \begin{array}{c} \cdots \\ \circ \\ \cdots \end{array} \rrbracket &= |0^m\rangle\langle 0^n| + |1^m\rangle\langle 1^n| & \llbracket \begin{array}{c} | \\ | \end{array} \rrbracket &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ \llbracket \begin{array}{c} \cdots \\ \boxed{r} \\ \cdots \end{array} \rrbracket &= \sum_{j_k, i_k \in \{0,1\}} r^{j_1 \dots j_m i_1 \dots i_n} |j_1, \dots, j_m\rangle\langle i_1, \dots, i_n| \end{aligned}$$

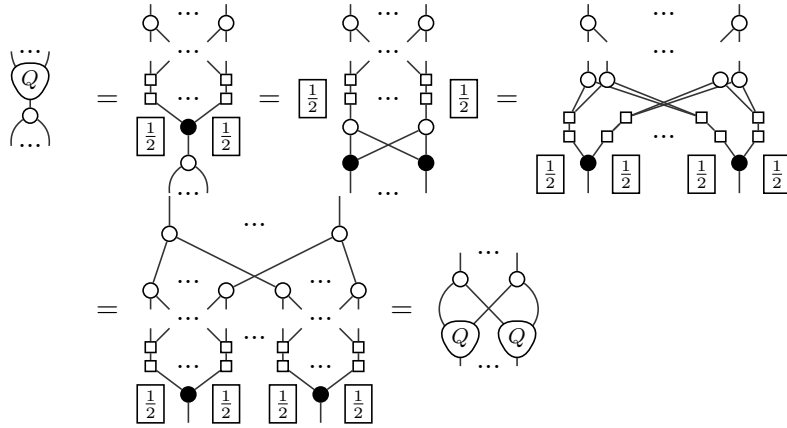




**Lemma 4.2.**



*Proof.* We prove the result where  $Q$ 's constant is 0. The proof where  $Q$ 's constant is 1 is very similar, and simply uses the fact that  $\neg \bullet$  is copied through the white node [BKMB<sup>+</sup>23]:



□

The above translation preserves the semantics:

**Proposition 4.3** [Vil21].  $\llbracket [\cdot]^{ZH} \rrbracket = \llbracket \cdot \rrbracket$ .

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

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

$$[\mathbf{s}]^{SOP} := s | \rangle \langle | \quad \text{for } s \in \mathbb{R}$$

$$\left[ \begin{array}{c} \dots \\ \circ \\ \dots \end{array} \right]^{SOP} := \sum_y |y, \dots, y\rangle \langle y, \dots, y| \quad \left[ \begin{array}{c} \dots \\ \boxed{0} \\ \dots \end{array} \right]^{SOP} := \left[ \begin{array}{c} \dots \\ \boxed{\frac{1}{2}} \\ \dots \end{array} \right]^{SOP}$$

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  $[\cdot]^{SOP}$ , 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 4.4.** 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:

$$\left[ \begin{array}{c} \dots \\ \boxed{r} \\ \dots \end{array} \right] = \left[ \begin{array}{c} \dots \\ \boxed{s} \\ \dots \end{array} \right] \left[ \begin{array}{c} \dots \\ \circ \\ \dots \end{array} \right] \left[ \begin{array}{c} \dots \\ \boxed{e^{i\alpha}} \\ \dots \end{array} \right] \left[ \begin{array}{c} \dots \\ \circ \\ \dots \end{array} \right] \left[ \begin{array}{c} \dots \\ \boxed{e^{i\beta}} \\ \dots \end{array} \right]$$

*Proof.* First, thanks to rule (HS1), we have  $\left( \begin{array}{c} \dots \\ r \\ \dots \end{array} \right) = \left[ \frac{1}{2} \right] \left( \begin{array}{c} \dots \\ \square \\ \dots \end{array} \right) \square r$ . Then, we have:

$$\left[ \left[ \frac{1}{2} \right] \square r \right] = \frac{1}{2} \begin{pmatrix} 1+r \\ 1-r \end{pmatrix} = \frac{1+r}{2} \begin{pmatrix} 1 \\ \frac{1-r}{1+r} \end{pmatrix}$$

and

$$\left[ \left[ s \right] \begin{array}{c} \square e^{i\alpha} \\ \square \\ \circ \\ \square e^{i\beta} \end{array} \right] = 2s e^{i\frac{\alpha}{2}} \begin{pmatrix} \cos \frac{\alpha}{2} \\ -i e^{i\beta} \sin \frac{\alpha}{2} \end{pmatrix} = 2s e^{i\frac{\alpha}{2}} \cos \frac{\alpha}{2} \begin{pmatrix} 1 \\ e^{i(\beta - \frac{\pi}{2})} \tan \frac{\alpha}{2} \end{pmatrix}$$

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  $r \neq 1$ ,  $\alpha$  is well defined and  $\alpha \neq \pi \pmod{2\pi}$  so  $s$  is also well-defined). From this, we get:

$$\left[ \left( \begin{array}{c} \dots \\ r \\ \dots \end{array} \right) \right] = \left[ \left[ s \right] \left( \begin{array}{c} \dots \\ \square \\ \circ \\ \square \end{array} \right) \begin{array}{c} \square e^{i\alpha} \\ \square e^{i\beta} \end{array} \right]$$

□

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

$$\left[ \left( \begin{array}{c} \dots \\ r \\ \dots \end{array} \right) \right]^{\text{SOP}} := \left[ \left[ s \right] \left( \begin{array}{c} \dots \\ \square \\ \circ \\ \square \end{array} \right) \begin{array}{c} \square e^{i\alpha} \\ \square e^{i\beta} \end{array} \right]^{\text{SOP}}$$

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

**Proposition 4.5** [Vil21].  $[[\cdot]^{\text{SOP}}] = [\cdot]$ . In other words, the following diagram commutes:

$$\begin{array}{ccc} \mathbf{ZH} & \xrightarrow{[\cdot]} & \mathbf{Qubit} \\ \downarrow [\cdot]^{\text{SOP}} & & \uparrow [\cdot] \\ \mathbf{SOP} & & \end{array}$$

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

**Proposition 4.6** [Vil21].  $[[\cdot]^{\text{ZH}}]^{\text{SOP}} \underset{\text{TH}}{\sim} (\cdot)$

**4.3. Restrictions of SOP.** Recall that  $\mathbf{ZH}_{\text{TH}}$  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 4.7** ( $\mathbf{SOP}_{[\frac{1}{2^n}]}$ ). We define  $\mathbf{SOP}_{[\frac{1}{2^n}]}$  as the restriction of **SOP** to morphisms of the form:  $t = \frac{1}{\sqrt{2^p}} \sum e^{2i\pi \frac{P}{2^n}} |\vec{O}\rangle \langle \vec{I}|$  where  $p \in \mathbb{Z}$  and  $P$  has integer coefficients.

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



**Proposition 4.8.**  $\mathbf{SOP}[\frac{1}{2}]$  captures exactly the Toffoli-Hadamard fragment of quantum mechanics.

*Proof.* We can prove this by showing that  $[\mathbf{ZH}_{\text{TH}}]^{\text{SOP}} \subseteq \mathbf{SOP}[\frac{1}{2}]$  and that  $[\mathbf{SOP}[\frac{1}{2}]]^{\text{ZH}} \subseteq \mathbf{ZH}_{\text{TH}}$ . 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,  $\llbracket \mathbf{ZH}_{\text{TH}} \rrbracket = \llbracket [\mathbf{ZH}_{\text{TH}}]^{\text{SOP}} \rrbracket \subseteq \llbracket \mathbf{SOP}[\frac{1}{2}] \rrbracket = \llbracket [\mathbf{SOP}[\frac{1}{2}]]^{\text{ZH}} \rrbracket \subseteq \llbracket \mathbf{ZH}_{\text{TH}} \rrbracket$ , so:

$$\llbracket \mathbf{SOP}[\frac{1}{2}] \rrbracket = \llbracket \mathbf{ZH}_{\text{TH}} \rrbracket \quad \square$$

Notice in particular that the Hadamard and Toffoli gates given in Example 2.3 lie in this fragment; and that compositions of elements of this fragment remain in the fragment. Not all of  $\mathbf{SOP}[\frac{1}{2}]$  can be generated by the two gates  $H$  and Tof, however, as  $\mathbf{SOP}[\frac{1}{2}]$  comprises linear maps that are not unitary, i.e. such that  $\llbracket t^\dagger \circ t \rrbracket \neq id$ .

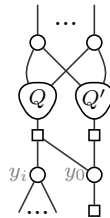
**4.4. The Rewrite System  $\xrightarrow{\text{TH}}$ , Graphically.** Before moving on to show the result of completeness the Toffoli-Hadamard fragment of  $\mathbf{SOP}$ , it is worth checking how the rules of  $\xrightarrow{\text{TH}}$  translate in  $\mathbf{ZH}$ . We will focus on the rules mentioned above, that were not present in the previous works on  $\mathbf{SOP}$ , namely (HHgen), (HHgen'), (HHnl) and (Rem).

Rule (HHgen) uses a side condition, that is  $QQ' = Q$ , which translates to

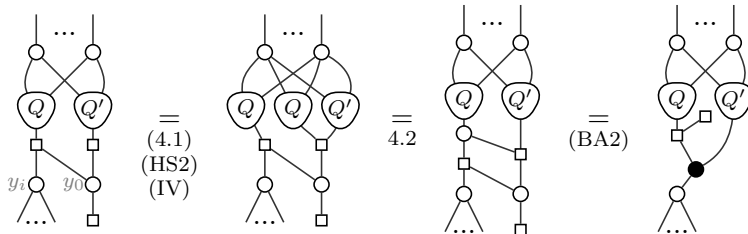


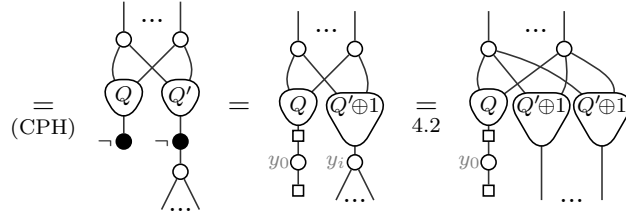
$$(4.1)$$

The pattern  $\frac{y_0}{2}(y_i \widehat{Q} + \widehat{Q}' + 1)$  is represented by:



and can be rewritten into:

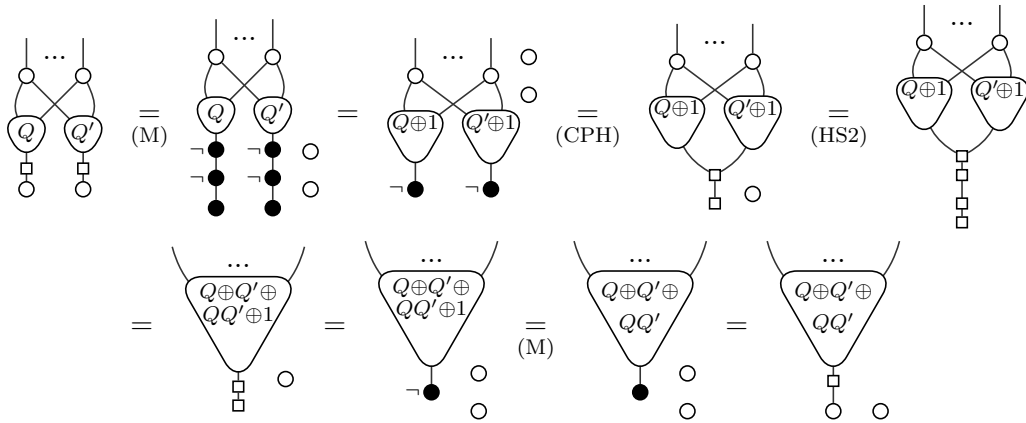




where the last equality (that uses Lemma 4.2) is the substitution  $[y_i \leftarrow Q' \oplus 1]$ .

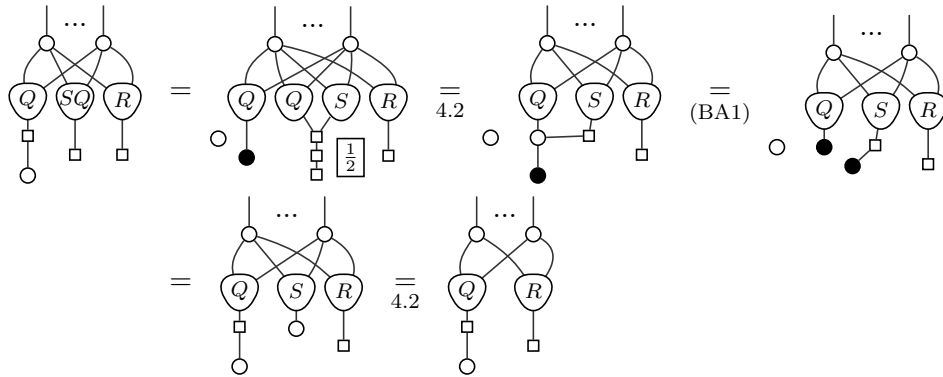
Rule (HHgen') can be proven graphically exactly in the same way, except we start from the second diagram in the derivation above.

Rule (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.

Finally, Rule (Rem) turns the phase polynomial  $\frac{y_0}{2} \widehat{Q} + \widehat{S}\widehat{Q} + \widehat{R}$  into  $\frac{y_0}{2} \widehat{Q} + \widehat{R}$ , which can be derived graphically as:



### 5. COMPLETENESS FOR TOFFOLI-HADAMARD

In this section, we aim to show that the set of rules  $\xrightarrow{\text{TH}}$  captures the whole Toffoli-Hadamard fragment of quantum mechanics. We do so by transporting the similar result from **ZH**<sub>TH</sub> to **SOP** $[\frac{1}{2}]$ . First, we show:

**Proposition 5.1.**  $\forall D_1, D_2 \in \mathbf{ZH}_{\text{TH}}, \mathbf{ZH}_{\text{TH}} \vdash D_1 = D_2 \implies [D_1]^{\text{sop}}_{\text{TH}} \sim [D_2]^{\text{sop}}_{\text{TH}}$

*Proof.* We show that all the rules of  $\mathbf{ZH}_{\text{TH}}$  hold in  $\mathbf{SOP}[\frac{1}{2}]$ , which together with Proposition 2.5 proves the result.

The translation of rule (IP) is implicit in  $\mathbf{SOP}$ : it essentially states that  $y_i \cdot y_i = y_i$  for boolean variable  $y_i$ . 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):

$$\begin{aligned} \left[ \begin{array}{c} \dots \\ \circ \\ \circ \\ \dots \end{array} \right]^{\text{sop}} &= \frac{1}{2} \sum e^{2i\pi \frac{y_0 + y_1}{2} y'} |y_1, \dots, y_1 \rangle \langle y_0, \dots, y_0| \\ &\xrightarrow{\text{HH}(y', [y_1 \leftarrow y_0])} \sum |y_0, \dots, y_0 \rangle \langle y_0, \dots, y_0| = \left[ \begin{array}{c} \dots \\ \circ \\ \circ \\ \dots \end{array} \right]^{\text{sop}} \end{aligned}$$

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

(IV):

$$\left[ \begin{array}{c} \square \\ \circ \end{array} \right]^{\text{sop}} = \frac{1}{2} \sum_y |\chi| \xrightarrow{\text{Elim}} 1 = \left[ \begin{array}{c} \square \\ \square \end{array} \right]^{\text{sop}}$$

(Z):

$$\left[ \begin{array}{c} \square \\ \square \\ \circ \end{array} \right]^{\text{sop}} \xrightarrow{\text{HH}} \frac{1}{\sqrt{2}} \sum e^{2i\pi \frac{y}{2}} |\chi| \xrightarrow{Z} \sum e^{2i\pi \frac{y}{2}} |\chi| \xleftarrow{\text{HH}} \left[ \begin{array}{c} \square \\ \circ \end{array} \right]^{\text{sop}}$$

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

$$\left[ \begin{array}{c} \bullet \\ \circ \end{array} \right]^{\text{sop}} \xrightarrow{\text{HH}} \sum |y_0 \oplus y_1 \rangle \langle y_0, y_1|$$

$$\begin{aligned} \left[ \begin{array}{c} \dots \\ \circ \\ \bullet \\ \dots \end{array} \right]^{\text{sop}} &\xrightarrow{\text{HH}} \frac{1}{2} \sum e^{2i\pi \frac{y_1 + \dots + y_n + y_0}{2} y'} |y_1, \dots, y_n \rangle \langle y_0, \dots, y_0| \\ &\xrightarrow{\text{HH}(y', [y_0 \leftarrow y_1 \oplus \dots \oplus y_n])} \sum |y_1, \dots, y_n \rangle \langle y_1 \oplus \dots \oplus y_n, \dots, y_1 \oplus \dots \oplus y_n| \xleftarrow{\text{HH}} \left[ \begin{array}{c} \bullet \dots \bullet \\ \circ \dots \circ \end{array} \right]^{\text{sop}} \end{aligned}$$

and

$$\begin{aligned} \left[ \begin{array}{c} \dots \\ \bullet \\ \circ \\ \dots \end{array} \right]^{\text{sop}} &\xrightarrow{\text{HH}} \frac{1}{2} \sum e^{2i\pi \left( \frac{y_1 \dots y_m y' + x_1 + \dots + x_n + y'}{2} \right)} |y_1, \dots, y_m \rangle \langle x_1, \dots, x_n| \\ &\xrightarrow{\text{HH}(y'', [y' \leftarrow x_1 \oplus \dots \oplus x_n])} \sum e^{2i\pi \left( \frac{y_1 \dots y_m x_1 + \dots + y_1 \dots y_m x_n}{2} \right)} |y_1, \dots, y_m \rangle \langle x_1, \dots, x_n| \\ &\xleftarrow{\text{HH}} \left[ \begin{array}{c} \dots \\ \circ \dots \circ \end{array} \right]^{\text{sop}} \end{aligned}$$



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

$$t_k := \sum e^{2i\pi \left( y_1 \dots y_k + \sum_{i=1}^k \frac{y'_i}{2} (y_i + x_i + x'_i) \right)}$$

on which we can apply (HH)  $k$  times in a row with  $[y_i \leftarrow x_i \oplus x'_i]$ . In that case we end up with:

$$t_k \xrightarrow{k} 2^k \sum e^{2i\pi \left( \prod_{i=1}^k (x_i + x'_i) \right)}$$

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

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  $\pi$ , used in particular in the quantum Fourier transform, belong in these fragments:

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

**Remark 6.1.** The construction we are about to define to relate the different dyadic levels together can be seen as a (non-unitary) instance of “catalysis”, defined and studied at length in the recent paper [ACG<sup>+</sup>23], where the complexity of applying gate (or piece of circuit)  $U$  several times in the overall circuit is offset to a particular state  $|\chi_U\rangle$  and several occurrences of a “simpler” piece of circuit  $\phi_U$  such that  $\phi_U \circ (id \otimes |\chi_U\rangle) = U \otimes |\chi_U\rangle$ . In our case,  $U$  is an occurrence of the  $\frac{\pi}{2^{n+1}}$  phase, and  $|\chi_U\rangle$  encodes that phase. Both  $U$  and  $|\chi_U\rangle$  live in  $\mathbf{SOP}[\frac{1}{2^{n+1}}]$ , while  $\phi_U$  lives in  $\mathbf{SOP}[\frac{1}{2^n}]$ .

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

**Lemma 6.2.** *Let  $P = \sum m_i \in \mathbb{R}[X_1, \dots, X_k]/(X_i^2 - X_i)$ , and  $t = s \sum e^{2i\pi P} |\vec{O}\rangle\langle \vec{I}|$ . Then:*

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

*Proof.* Let us start by composing the two first diagonal terms:

$$\begin{aligned} & \left( \sum e^{2i\pi m_1} |y_0, \dots, y_k\rangle\langle y_0, \dots, y_k| \right) \circ \left( \sum e^{2i\pi m_\ell} |y_0, \dots, y_k\rangle\langle y_0, \dots, y_k| \right) \\ &= \frac{1}{2^{k+1}} \sum e^{2i\pi(m_1+m_2[y_i \leftarrow y'_i] + \frac{y_0 y'_0 + y'_0 y_0}{2} + \dots + \frac{y_k y'_k + y'_k y_k}{2})} |y_0, \dots, y_k\rangle\langle y'_0, \dots, y'_k| \\ & \xrightarrow{\text{HH}(y'_i \leftarrow y_i)} \sum e^{2i\pi(m_1+m_2)} |y_0, \dots, y_k\rangle\langle y_0, \dots, y_k| \end{aligned}$$

Doing so repeatedly with all the diagonal terms gives

$$\sum e^{2i\pi P} |y_0, \dots, y_k\rangle\langle y_0, \dots, y_k|$$

Finally, applying the extremal terms (one at a time) and removing the newly created variables with (HH), just as we did for the diagonal terms, yields  $t$ .  $\square$

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 6.3** ( $\mathbf{SOP}[\frac{1}{2^n}]'$ ). We define  $\mathbf{SOP}[\frac{1}{2^n}]'$  as the restriction of **SOP** to morphisms of the form:  $t = \frac{1}{2^p} \sum e^{2i\pi \frac{P}{2^n}} |\vec{O}\rangle\langle \vec{I}|$  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 6.4.**  $\left[ \frac{1}{\sqrt{2}} \sum_{y_0 \in V} e^{2i\pi(\frac{1}{8} + \frac{3}{4}y_0)} \right] = 1$ . Hence:

$$\forall t \in \mathbf{SOP}[\frac{1}{2^n}], \exists t' \in \mathbf{SOP}[\frac{1}{2^{\max(3,n)}}]', \llbracket t \rrbracket = \llbracket t' \rrbracket$$

*Proof.* If  $t \in \mathbf{SOP}[\frac{1}{2^n}]$  and  $t \notin \mathbf{SOP}[\frac{1}{2^n}]'$ , then:

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

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

**Definition 6.5.** For any  $k \geq 1$ , we define the functor  $[\cdot]_k : \mathbf{SOP}[\frac{1}{2^{k+1}}]' \rightarrow \mathbf{SOP}[\frac{1}{2^k}]'$ , first for morphisms  $t = s \sum e^{2i\pi \frac{\ell}{2^{k+1}} y_{i_1} \dots y_{i_q}} |\vec{O}\rangle\langle \vec{I}|$  with phase polynomial of size 0 or 1:

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

The functor is then extended to any  $\mathbf{SOP}[\frac{1}{2^{k+1}}]'$ -morphism by the decomposition of Lemma 6.2 (and given a particular ordering on the monomials of the phase polynomial).

Since  $[\cdot]_k$  is defined to be a functor, we have  $[\cdot \circ \cdot]_k = [\cdot]_k \circ [\cdot]_k$ . 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:  $[t_1 \circ t_2]_k = [t_2 \circ t_1]_k$  quite obviously when either  $\ell_1 \bmod 2 = 0$  or  $\ell_2 \bmod 2 = 0$ , but also when  $\ell_1 \bmod 2 = \ell_2 \bmod 2 = 1$ :

$$[t_1 \circ t_2]_k \xrightarrow{\text{HH}} \sum e^{2i\pi \left( \frac{y_{i_1} \dots y_{i_q} ((\ell_1 - 1)/2 + y') + y_{j_1} \dots y_{j_r} ((\ell_2 - 1)/2 + y')}{2^k} + \frac{y_{i_1} \dots y_{i_q} y_{j_1} \dots y_{j_r} (1 - 2y')}{2^k} \right)} |\vec{y}, y'\rangle\langle \vec{y}, y' \oplus y_{i_1} \dots y_{i_q} \oplus y_{j_1} \dots y_{j_r} |$$

$$\xleftarrow{\text{HH}} [t_2 \circ t_1]_k$$

Notice however that  $[\cdot]_k$  adds an input and an output, so necessarily  $[\cdot \otimes \cdot]_k \neq [\cdot]_k \otimes [\cdot]_k$ .

The functors  $[\cdot]_k$  map terms with the same semantics to terms with the same semantics:

**Proposition 6.6.**  $\forall t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]'$ ,  $\llbracket t_1 \rrbracket = \llbracket t_2 \rrbracket \implies \llbracket [t_1]_k \rrbracket = \llbracket [t_2]_k \rrbracket$

*Proof.* We prove this proposition by showing that:

- (1)  $\llbracket \mathbf{SOP}[\frac{1}{2^{k+1}}] \rrbracket \subseteq \mathcal{M}(\mathbb{Z}[\frac{1}{2}], e^{i\frac{\pi}{2^k}})$
- (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  $\psi_k : \mathcal{M}(\mathbb{Z}[\frac{1}{2}], e^{i\frac{\pi}{2^k}}) \rightarrow \mathcal{M}(\mathbb{Z}[\frac{1}{2}], e^{i\frac{\pi}{2^{k-1}}})$ , based on the decomposition, and such that  $\llbracket [t]_k \rrbracket = \psi_k(\llbracket t \rrbracket)$

In this case, given  $t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]'$  such that  $\llbracket t_1 \rrbracket = \llbracket t_2 \rrbracket$ , by (1) we can apply  $\psi_k$  to their interpretation. By uniqueness of the decomposition (2),  $\psi_k(\llbracket t_1 \rrbracket) = \psi_k(\llbracket t_2 \rrbracket)$ . Finally, by (3),  $\llbracket [t_1]_k \rrbracket = \llbracket [t_2]_k \rrbracket$ . 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:

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

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

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

By linearity,  $\psi_k$  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  $\psi_k$  is a homomorphism, i.e.  $\psi_k(\cdot + \cdot) = \psi_k(\cdot) + \psi_k(\cdot)$  and  $\psi_k(\cdot \circ \cdot) = \psi_k(\cdot) \circ \psi_k(\cdot)$ .

It remains to show that  $\llbracket [\cdot]_k \rrbracket = \psi_k(\llbracket \cdot \rrbracket)$ . Since  $\psi_k$  is a homomorphism, it is enough to show the result on the terms in the decomposed form of Lemma 6.2. Let  $t = s \sum e^{2i\pi \frac{\ell}{2^{k+1}} y_{i_1} \dots y_{i_q}} |\vec{0}\rangle\langle \vec{1}|$  be such a term.

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

$$\llbracket [t]_k \rrbracket = \left\| s \sum e^{2i\pi \frac{\ell/2}{2^k} y_{i_1} \dots y_{i_q}} |\vec{0}, y'\rangle\langle \vec{1}, y'| \right\| = \llbracket t \rrbracket \otimes I_2.$$

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

$$\llbracket t \rrbracket = s e^{i\frac{\pi}{2^k}} \sum_{y_{i_1} \dots y_{i_q}=1} e^{2i\pi \frac{(\ell-1)/2}{2^k}} |\vec{0}\rangle\langle \vec{1}| + s \sum_{y_{i_1} \dots y_{i_q}=0} |\vec{0}\rangle\langle \vec{1}|$$

so:

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

and

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

**6.2. Going Back.** We now show how to reverse the functors  $\llbracket \cdot \rrbracket_k$ .

**Definition 6.7.** For any  $k \geq 1$ , we define the (partial) map  $\llbracket \cdot \rrbracket_k : \mathbf{SOP}[\frac{1}{2^k}]' \rightarrow \mathbf{SOP}[\frac{1}{2^{k+1}}]'$  as:

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

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

$\llbracket \cdot \rrbracket_k$  reverses the action of  $\llbracket \cdot \rrbracket_k$  (up to some rewrites):

**Proposition 6.8.**  $\llbracket \llbracket \cdot \rrbracket_k \rrbracket_k \underset{\text{TH}}{\sim} (\cdot)$  and  $t_1 \underset{\text{TH}}{\sim} t_2 \implies \llbracket t_1 \rrbracket \underset{\text{TH}}{\sim} \llbracket t_2 \rrbracket$  for any two terms  $t_1, t_2$ .



*Proof.* Again, we can use the decomposition given in Lemma 6.2. 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  $[t]_k \circ (id_n \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}} |y_0\rangle}) \underset{\text{TH}}{\sim} t \otimes \sum e^{2i\pi \frac{y_0}{2^{k+1}} |y_0\rangle}$ :

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

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

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

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

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

The second result in the Proposition simply comes from the fact that  $[t_i]$  is built by composition from  $t_i$ , so Proposition 2.5 gives the desired result.  $\square$

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

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

*Proof.* Let  $t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}]'$  such that  $\llbracket t_1 \rrbracket = \llbracket t_2 \rrbracket$ . By Proposition 6.6:

$$\llbracket [\dots [t_1]_k \dots]_1 \rrbracket = \llbracket [\dots [t_2]_k \dots]_1 \rrbracket$$

Since  $[\dots [t_i]_k \dots]_1 \in \mathbf{SOP}[\frac{1}{2}]' \subset \mathbf{SOP}[\frac{1}{2}]$ , by completeness of this fragment (Theorem 5.3):

$$[\dots [t_1]_k \dots]_1 \underset{\text{TH}}{\sim} [\dots [t_2]_k \dots]_1$$

Finally, by Proposition 6.8:

$$t_1 \underset{\text{TH}}{\sim} \left[ \dots \left[ [\dots [t_1]_k \dots]_1 \right]_1 \dots \right]_k \underset{\text{TH}}{\sim} \left[ \dots \left[ [\dots [t_2]_k \dots]_1 \right]_1 \dots \right]_k \underset{\text{TH}}{\sim} t_2. \quad \square$$

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

**Lemma 6.10.** *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  $t_1 \underset{\text{TH}}{\not\sim} t_2$ .*

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

However, adding a single rule:

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

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

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

which was already used in [Amy19, LvdWK21, Vil21] to deal with the Clifford fragment of quantum mechanics.

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

**Theorem 6.11** (Completeness of  $\mathbf{SOP}[\frac{1}{2^{k+1}}]/\sim_{\text{TH}}$ ). *Let us write  $\xrightarrow{\text{TH}} := \xrightarrow{\text{TH}} + \{(\sqrt{2})\}$ .*

*Then:  $\forall t_1, t_2 \in \mathbf{SOP}[\frac{1}{2^{k+1}}], \llbracket t_1 \rrbracket = \llbracket t_2 \rrbracket \iff t_1 \sim_{\text{TH}} t_2$*

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

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

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  $t_i \sim_{\text{TH}} t'_i$ . By Theorem 6.9:

$$t_1 \sim_{\text{TH}} t'_1 \sim_{\text{TH}} t'_2 \sim_{\text{TH}} t_2 \quad \square$$

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

**Corollary 6.13** (Completeness of  $\mathbf{SOP}[\mathbb{D}]/\sim_{\text{TH}}$ ).

$$\forall t_1, t_2 \in \mathbf{SOP}[\mathbb{D}], \llbracket t_1 \rrbracket = \llbracket t_2 \rrbracket \iff t_1 \sim_{\text{TH}} t_2$$

## 7. SUMMING AND CONCATENATING SOP-MORPHISMS

We show in this section two interesting constructions that allow us to perform operations on **SOP**-morphisms that are not primitively doable in **SOP** or more generally in gate-based quantum computation, but necessary when considering Hamiltonian-based computation [SWY22], namely their sum and concatenation. Specifically, for any two **SOP**-morphisms  $t_0, t_1 : n \rightarrow m$ , we want to be able to build terms  $t_{\text{sum}}$  and  $t_{\text{concat}}$  such that:

$$\begin{aligned} \llbracket t_{\text{sum}} \rrbracket &= \llbracket t_0 \rrbracket + \llbracket t_1 \rrbracket \\ \llbracket t_{\text{concat}} \rrbracket &= |0\rangle \otimes \llbracket t_0 \rrbracket + |1\rangle \otimes \llbracket t_1 \rrbracket \end{aligned}$$

As we will see, these constructions are well suited to the dyadic fragments, as they can be performed entirely inside them.

To do so, we need a notion of controlled **SOP**-morphism, inferred from [JPV19] and made systematic in the graphical framework in [JPV22].

**Definition 7.1.** A **SOP**-morphism  $t : n + 1 \rightarrow m$  is called a *controlled morphism* if:

$$\llbracket t \circ (|0\rangle \otimes id_n) \rrbracket = \sum_{\vec{y} \in \{0,1\}^{n+m}} |y_0, \dots, y_m\rangle \langle y_{m+1}, \dots, y_{m+n}| = \llbracket H_m^n(1) \rrbracket$$

where  $H_m^n(1)$  is the H-spider from **ZH** with parameter 1. It will be used as a shortcut notation to represent the linear map  $\sum_{\vec{y} \in \{0,1\}^{n+m}} |y_0, \dots, y_m\rangle \langle y_{m+1}, \dots, y_{m+n}|$  or equivalently the **SOP**-morphism  $\sum_{\vec{y}} |y_0, \dots, y_m\rangle \langle y_{m+1}, \dots, y_{m+n}|$ .

In a controlled morphism, the rightmost input is called the *control input*. We also call the morphism  $t \circ (|1\rangle \otimes id_n)$  the *controlee*.

**Example 7.2.**  $t := \frac{1}{2} \sum e^{2i\pi(\frac{1}{2}y_0y_1y_6 + \frac{1}{2}y_1y_2y_6)} |y_0\rangle \langle y_1, y_2|$  is a controlled morphism, as  $\llbracket t \rrbracket = \langle 0| \otimes \llbracket H_1^1(1) \rrbracket + \langle 1| \otimes id_1$ .

In the following, we show how given two controlled morphisms, we can build a third controlled morphism whose controlee is the sum (resp. the concatenation) of the controlees of the first two terms. Finally, we show how to turns any term  $t$  into a controlled morphism whose controlee is precisely  $t$ . Since recovering the controlee out of a controlled term is easy (it suffices to apply  $|1\rangle$  to the control input), the process towards building e.g. the sum of two terms  $t_0$  and  $t_1$  would then be:

- build controlled terms  $\Lambda t_0$  and  $\Lambda t_1$  controlling  $t_0$  and  $t_1$  respectively
- use the construction to build  $\Lambda(t_0 + t_1)$ , a term controlling  $t_0 + t_1$
- apply  $|1\rangle$  to the control inputs to get  $t_0 + t_1$

**7.1. The Constructions.** Using this notion of controlled morphism, there exists a construction that will allow us to perform a sum of terms. In this construction, we need in particular:

$$t_+ := \frac{1}{2} \sum e^{2i\pi(\frac{1}{2}y_0y_1y_3)} |y_0, y_1\rangle \langle y_0 \oplus y_1|$$

and the family of morphisms:

$$cp_n : n \rightarrow 2n := \sum_{\vec{y}} |\vec{y}, \vec{y}\rangle \langle \vec{y}|$$

We also need the following identities:

**Lemma 7.3.**  $\llbracket H_{m_1}^{n_1}(1) \rrbracket \otimes \llbracket H_{m_2}^{n_2}(1) \rrbracket = \llbracket H_{m_1+m_2}^{n_1+n_2}(1) \rrbracket$

*Proof.* This is obvious from the fact that:

$$\llbracket H_m^n(1) \rrbracket = \sum_{\vec{y} \in \{0,1\}^{n+m}} |y_0, \dots, y_m\rangle \langle y_{m+1}, \dots, y_{m+n}| \quad \square$$

**Lemma 7.4.**  $(\llbracket H_0^n(1) \rrbracket \otimes \cdot) \circ \llbracket cp_n \rrbracket = (\cdot)$        $(\cdot \otimes \llbracket H_0^n(1) \rrbracket) \circ \llbracket cp_n \rrbracket = (\cdot)$   
 $\llbracket cp_m \rrbracket^\dagger \circ (\llbracket H_m^0(1) \rrbracket \otimes \cdot) = (\cdot)$        $\llbracket cp_m \rrbracket^\dagger \circ (\cdot \otimes \llbracket H_m^0(1) \rrbracket) = (\cdot)$

*Proof.* The first equation is obtained by:

$$(\llbracket H_0^n(1) \rrbracket \otimes .) \circ \llbracket \text{cp}_n \rrbracket = \left( \sum_{\vec{y}_1, \vec{y}_2} |\vec{y}_2\rangle\langle\vec{y}_1, \vec{y}_2| \right) \circ \left( \sum_{\vec{y}} |\vec{y}, \vec{y}\rangle\langle\vec{y}| \right) = \sum_{\vec{y}} |\vec{y}\rangle\langle\vec{y}| = id_n$$

The other three equations can be obtained similarly.  $\square$

We may now build, from two controlled morphisms, a third controlled morphism whose controllee is the sum of the two first controllees:

**Proposition 7.5.** *Let  $t_1, t_2 : n + 1 \rightarrow m$  be two controlled morphisms. We define:*

$$t := \text{cp}_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ (t_+ \otimes \text{cp}_n)$$

*Then:*

$$\llbracket t \rrbracket = \langle 0| \otimes \llbracket H_m^n(1) \rrbracket + \langle 1| \otimes \left( \llbracket t_1 \circ (|1\rangle \otimes id_n) \rrbracket + \llbracket t_2 \circ (|1\rangle \otimes id_n) \rrbracket \right)$$

*Proof.* First, notice that  $t_+ \circ |0\rangle \xrightarrow{\text{HH}} |0, 0\rangle$  and  $t_+ \circ |1\rangle \xrightarrow{\text{HH}} \sum |y_0, y_0 \oplus 1\rangle$ .

Then:

$$\begin{aligned} \llbracket t \circ (|0\rangle \otimes id_n) \rrbracket &= \llbracket \text{cp}_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ ((t_+ \circ |0\rangle) \otimes \text{cp}_n) \rrbracket \\ &= \llbracket \text{cp}_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ (|0, 0\rangle \otimes \text{cp}_n) \rrbracket \\ &= \llbracket \text{cp}_m \rrbracket^\dagger \circ (\llbracket t_1 \circ (|0\rangle \otimes id_n) \rrbracket \otimes \llbracket t_2 \circ (|0\rangle \otimes id_n) \rrbracket) \circ \llbracket \text{cp}_n \rrbracket \\ &= \llbracket \text{cp}_m \rrbracket^\dagger \circ (\llbracket H_m^n(1) \rrbracket \otimes \llbracket H_m^n(1) \rrbracket) \circ \llbracket \text{cp}_n \rrbracket = \llbracket H_m^n(1) \rrbracket \end{aligned}$$

and:

$$\begin{aligned} \llbracket t \circ (|1\rangle \otimes id_n) \rrbracket &= \llbracket \text{cp}_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ ((t_+ \circ |1\rangle) \otimes \text{cp}_n) \rrbracket \\ &= \llbracket \text{cp}_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ \left( \left( \sum |y_0, y_0 \oplus 1\rangle \right) \otimes \text{cp}_n \right) \rrbracket \\ &= \llbracket \text{cp}_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ (|0, 1\rangle \otimes \text{cp}_n) \rrbracket \\ &\quad + \llbracket \text{cp}_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ (|1, 0\rangle \otimes \text{cp}_n) \rrbracket \\ &= \llbracket \text{cp}_m \rrbracket^\dagger \circ (\llbracket t_1 \circ (|0\rangle \otimes id_n) \rrbracket \otimes \llbracket t_2 \circ (|1\rangle \otimes id_n) \rrbracket) \circ \llbracket \text{cp}_n \rrbracket \\ &\quad + \llbracket \text{cp}_m \rrbracket^\dagger \circ (\llbracket t_1 \circ (|1\rangle \otimes id_n) \rrbracket \otimes \llbracket t_2 \circ (|0\rangle \otimes id_n) \rrbracket) \circ \llbracket \text{cp}_n \rrbracket \\ &= \llbracket t_2 \circ (|1\rangle \otimes id_n) \rrbracket + \llbracket t_1 \circ (|1\rangle \otimes id_n) \rrbracket \quad \square \end{aligned}$$

**Example 7.6.**  $t_1 = \frac{1}{2} \sum e^{2i\pi(\frac{1}{2}y_0y_1y_6 + \frac{1}{2}y_1y_2y_6)} |y_0\rangle\langle y_1, y_2|$  is a controlled morphism by Example 7.2. The morphism  $t_2 = \sum |y_0\rangle\langle y_1, y_2|$  is also obviously a controlled morphism.  $t_1$  controls  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  and  $t_2$  controls  $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ . The above construction on  $t_1$  and  $t_2$  yields

$$t \xrightarrow{\text{HH}} \frac{1}{4} \sum e^{2i\pi(\frac{1}{2}y_2y_1y_6 + \frac{1}{2}y_2y_3y_4 + \frac{1}{2}y_0y_2y_4)} |y_0\rangle\langle y_2 \oplus y_6, y_3| \quad \text{which controls } \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

To get the controllee, it then suffices to apply  $|1\rangle$  on the first input of  $t$ :

$$t \circ (|1\rangle \otimes id) \xrightarrow{\text{HH}} \frac{1}{2} \sum e^{2i\pi(\frac{1}{2}y_3y_4y_6 + \frac{1}{2}y_0y_4 + \frac{1}{2}y_3y_4 + \frac{1}{2}y_0y_4y_6)} |y_0\rangle\langle y_3|$$

The notion of controlled morphism also allows us to define a construction that will perform the concatenation of the controlees. Here again, we need a new building block:

$$t_c := \sum |y_0, y_0 y_1 \oplus y_1, y_0 y_1 \rangle \langle y_1|$$

**Proposition 7.7.** *Let  $t_1, t_2 : n + 1 \rightarrow m$  be two controlled morphisms. We define:*

$$t := (id_1 \otimes cp_m^\dagger) \circ (id_1 \otimes t_1 \otimes t_2) \circ (id_2 \otimes \sigma_{1,n} \otimes id_n) \circ (t_c \otimes cp_n)$$

Then:

$$\llbracket t \rrbracket = \langle 0| \otimes \llbracket H_{m+1}^n(1) \rrbracket + \langle 1| \otimes \left( |0\rangle \otimes \llbracket t_1 \circ (|1\rangle \otimes id_n) \rrbracket + |1\rangle \otimes \llbracket t_2 \circ (|1\rangle \otimes id_n) \rrbracket \right)$$

i.e.  $t$  controls the concatenation of  $t_1$  and  $t_2$ 's controlees.

*Proof.* Notice first that  $t_c \circ |0\rangle \xrightarrow{\text{HH}} \sum |y_0, 0, 0\rangle$ ,  $(\langle 0| \otimes id_2) \circ t_c |1\rangle \xrightarrow{\text{HH}} |1, 0\rangle$  and  $(\langle 1| \otimes id_2) \circ t_c |1\rangle \xrightarrow{\text{HH}} |0, 1\rangle$ .

Let  $t$  be defined as above. First, we have:

$$\begin{aligned} & \llbracket t \circ (|0\rangle \otimes id_n) \rrbracket \\ &= \llbracket (id_1 \otimes cp_m^\dagger) \circ (id_1 \otimes t_1 \otimes t_2) \circ (id_2 \otimes \sigma_{1,n} \otimes id_n) \circ \left( \left( \sum |y_0, 0, 0\rangle \right) \otimes cp_n \right) \rrbracket \\ &= \llbracket \left( \sum |y_0\rangle \right) \otimes \left( cp_m^\dagger \circ ((t_1 \circ (|0\rangle \otimes id_n)) \otimes (t_2 \circ (|0\rangle \otimes id_n))) \circ cp_n \right) \rrbracket \\ &= \llbracket H_1^0(1) \rrbracket \otimes \left( \llbracket cp_m \rrbracket^\dagger \circ (\llbracket t_1 \circ (|0\rangle \otimes id_n) \rrbracket \otimes \llbracket t_2 \circ (|0\rangle \otimes id_n) \rrbracket) \circ \llbracket cp_n \rrbracket \right) \\ &= \llbracket H_1^0(1) \rrbracket \otimes \left( \llbracket cp_m \rrbracket^\dagger \circ (\llbracket H_m^n(1) \rrbracket \otimes \llbracket H_m^n(1) \rrbracket) \circ \llbracket cp_n \rrbracket \right) = \llbracket H_1^0(1) \rrbracket \otimes \llbracket H_m^n(1) \rrbracket \\ &= \llbracket H_{m+1}^n(1) \rrbracket \end{aligned}$$

Then:

$$\begin{aligned} & \llbracket (\langle 0| \otimes id_m) \circ t \circ (|0\rangle \otimes id_n) \rrbracket \\ &= \llbracket cp_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ ((\langle 0| \otimes id_2) \circ t_c |1\rangle) \otimes cp_n \rrbracket \\ &= \llbracket cp_m^\dagger \circ (t_1 \otimes t_2) \circ (id_1 \otimes \sigma_{1,n} \otimes id_n) \circ (|1, 0\rangle \otimes cp_n) \rrbracket \\ &= \llbracket cp_m \rrbracket^\dagger \circ (\llbracket t_1 \circ (|1\rangle \otimes id_n) \rrbracket \otimes \llbracket t_2 \circ (|0\rangle \otimes id_n) \rrbracket) \circ \llbracket cp_n \rrbracket \\ &= \llbracket cp_m \rrbracket^\dagger \circ (\llbracket t_1 \circ (|1\rangle \otimes id_n) \rrbracket \otimes \llbracket H_m^n(1) \rrbracket) \circ \llbracket cp_n \rrbracket \\ &= \llbracket t_1 \circ (|1\rangle \otimes id_n) \rrbracket \end{aligned}$$

and similarly:

$$\llbracket (\langle 1| \otimes id_m) \circ t \circ (|0\rangle \otimes id_n) \rrbracket = \llbracket t_2 \circ (|1\rangle \otimes id_n) \rrbracket \quad \square$$

**7.2. Controlling SOP-Morphisms.** Critical to the previous two constructions is the existence, for every morphism  $t$  of another morphism that controls it.

First, we need to be able, in all generality, to control arbitrary complex scalars.

**Definition 7.8.** Let  $s \in \mathbb{C}$ . If  $s \neq 0$ , let  $n := \lceil \log_2(|s| + 1) \rceil$ ,  $\alpha := \arccos\left(\frac{|s|}{2^n - 1}\right)$  and  $\theta = \arg(s)$ . Then  $s = (2^n - 1) \cos \alpha e^{i\theta}$ . We hence define:

$$\Lambda' s := \begin{cases} \langle 0 | & \text{if } s = 0 \\ \frac{1}{4} \sum e^{2i\pi \left( \frac{y_1 \dots y_n y''}{2} + \frac{y''(1+y_0)}{2} + \frac{2\alpha}{2\pi} y_0 y' + \frac{\theta - \alpha}{2\pi} y_0 \right)} \langle y_0 | & \text{if } s \neq 0 \end{cases}$$

**Proposition 7.9.** For any  $s \in \mathbb{C}$ ,  $[\Lambda' s] = \langle 0 | + s \langle 1 |$ .

*Proof.* If  $s = 0$ , the result is obvious. Otherwise, notice that  $\sum_{\vec{y} \in \{0,1\}^n} e^{2i\pi \frac{y_1 \dots y_n}{2}} = 2^n - 2$ .

Then:

$$\begin{aligned} [\Lambda' s \circ |0\rangle] &= \left[ \frac{1}{4} \sum_{\vec{y} \setminus \{y_0\}} e^{2i\pi \left( \frac{y_1 \dots y_n y''}{2} + \frac{y''}{2} \right)} \right] = \left[ \frac{1}{2} \sum_{\vec{y} \setminus \{y_0, y'\}} e^{2i\pi \left( \frac{y_1 \dots y_n y''}{2} + \frac{y''}{2} \right)} \right] \\ &= \left[ \frac{1}{2} \sum_{\vec{y} \setminus \{y_0, y', y''\}} e^{2i\pi(0)} \right] - \left[ \frac{1}{2} \sum_{\vec{y} \setminus \{y_0, y', y''\}} e^{2i\pi \left( \frac{y_1 \dots y_n}{2} \right)} \right] = \frac{1}{2} (2^n - (2^n - 2)) = 1 \\ [\Lambda' s \circ |1\rangle] &= \left[ \frac{1}{4} \sum_{\vec{y} \setminus \{y_0\}} e^{2i\pi \left( \frac{y_1 \dots y_n y''}{2} + \frac{2\alpha}{2\pi} y' + \frac{\theta - \alpha}{2\pi} \right)} \right] \\ &= \frac{1}{4} \left[ \sum_{\vec{y} \setminus \{y_0, y'\}} e^{2i\pi \left( \frac{y_1 \dots y_n y''}{2} \right)} \right] \left[ \sum_{y'} e^{2i\pi \left( \frac{2\alpha}{2\pi} y' + \frac{\theta - \alpha}{2\pi} \right)} \right] \\ &= \frac{1}{4} (2^{n+1} - 2) e^{i(\theta - \alpha)} (1 + e^{2i\alpha}) = (2^n - 1) \cos \alpha e^{i\theta} = s \quad \square \end{aligned}$$

This construction is interesting as it requires a fairly small number of variables. However, scalars that we can find in the dyadic fragments ( $\mathbf{SOP}_{\lfloor \frac{1}{2^n} \rfloor}$ ) may require their control to be outside them. For instance, in  $\Lambda^{\frac{1}{2}}$ , we need  $\alpha = \frac{\pi}{3}$ , which is not a dyadic multiple of  $\pi$ . We hence give another definition for the controlled scalar:

**Definition 7.10.** Let  $s \in \mathbb{C}$ . If  $s \neq 0$ , let  $n := \lceil \log_2(|s|) \rceil$ ,  $\alpha := \arccos\left(\frac{|s|}{2^n}\right)$  and  $\theta = \arg(s)$ . Then  $s = 2^n \cos \alpha e^{i\theta}$ . We define:

$$\Lambda s := \begin{cases} \langle 0 | & \text{if } s = 0 \\ \frac{1}{2^{n+1}} \sum e^{2i\pi \left( \sum_{i=1}^n \frac{y_i y'_i (1+y_0)}{2} + \frac{2\alpha}{2\pi} y_0 y' + \frac{\theta - \alpha}{2\pi} y_0 \right)} \langle y_0 | & \text{if } n \geq 0 \\ 2^{2n-1} \sum e^{2i\pi \left( \sum_{i=1}^{|n|} \frac{y_i y'_i y_0}{2} + \frac{2\alpha}{2\pi} y_0 y' + \frac{\theta - \alpha}{2\pi} y_0 \right)} \langle y_0 | & \text{if } n < 0 \end{cases}$$

**Proposition 7.11.** For any  $s \in \mathbb{C}$ ,  $[\Lambda s] = \langle 0 | + s \langle 1 |$ .

*Proof.* If  $s = 0$ , the result is obvious.

Then, if  $n \geq 0$ :

$$\Lambda s \circ |0\rangle \xrightarrow{\text{HH}} \frac{1}{2^{n+1}} \sum e^{2i\pi \left( \sum_{i=1}^n \frac{y_i y'_i}{2} \right)} \xrightarrow{\text{Elim}} \frac{1}{2^n} \sum e^{2i\pi \left( \sum_{i=1}^n \frac{y_i y'_i}{2} \right)} \xrightarrow{\text{HH}^n} 1$$

and:

$$\Lambda s \circ |1\rangle \xrightarrow{\text{HH}} \frac{1}{2^{n+1}} \sum e^{2i\pi \left( \sum_{i=1}^n 0 + \frac{2\alpha}{2\pi} y' + \frac{\theta - \alpha}{2\pi} \right)} \xrightarrow{\text{Elim}^{2n}} 2^{n-1} \sum e^{2i\pi \left( \frac{2\alpha}{2\pi} y' + \frac{\theta - \alpha}{2\pi} \right)}$$

So  $[\Lambda s \circ |1\rangle] = 2^{n-1} e^{i(\theta - \alpha)} (1 + e^{2i\alpha}) = 2^n \cos \alpha e^{i\theta} = s$ .

Now, if  $n < 0$ :

$$\Lambda s \circ |0\rangle \xrightarrow{\text{HH}} 2^{2n-1} \sum e^{2i\pi(0)} \xrightarrow{\text{Elim}^{2|n|+1}} 1$$

and

$$\Lambda s \circ |1\rangle \xrightarrow{\text{HH}} 2^{2n-1} \sum e^{2i\pi \left( \sum_{i=1}^{|n|} \frac{y_i y'_i}{2} + \frac{2\alpha}{2\pi} y' + \frac{\theta - \alpha}{2\pi} \right)} \xrightarrow{\text{HH}^{|n|}} 2^{n-1} \sum e^{2i\pi \left( \frac{2\alpha}{2\pi} y' + \frac{\theta - \alpha}{2\pi} \right)}$$

so again  $[\Lambda s \circ |1\rangle] = s$ . □

This time, if  $s = \frac{1}{\sqrt{2^p}} = 2^{\lceil \frac{p}{2} \rceil} \cos \frac{\pi}{4} (p \bmod 2)$ , controlling  $s$  gives a morphism in a dyadic fragment of **SOP**.

We now give a general construction for controlling an arbitrary **SOP**-term.

**Definition 7.12.** Let  $t = s \sum_{\vec{y}} e^{2i\pi P} |\vec{O}\rangle\langle\vec{I}| \in \mathbf{SOP}$ . We define:

$$\tilde{\Lambda} t := \frac{1}{2^{|\vec{y}|}} \sum_{\substack{\vec{y}, x_0, \\ \vec{x}_1, \vec{x}_2}} e^{2i\pi x_0 P} |x_0 \vec{O} \oplus \vec{x}_1 \oplus x_0 \vec{x}_1\rangle\langle x_0, x_0 \vec{I} \oplus \vec{x}_2 \oplus x_0 \vec{x}_2|$$

where

$$x_0 \vec{O} \oplus \vec{x}_1 \oplus x_0 \vec{x}_1 := (x_0 O_1 \oplus x_{11} \oplus x_0 x_{11}, \dots, x_0 O_m \oplus x_{1m} \oplus x_0 x_{1m}),$$

and similarly

$$x_0 \vec{I} \oplus \vec{x}_2 \oplus x_0 \vec{x}_2 := (x_0 I_1 \oplus x_{21} \oplus x_0 x_{21}, \dots, x_0 I_{m+n} \oplus x_{2n} \oplus x_0 x_{2n}).$$

We finally define:

$$\Lambda t := \left( \Lambda(s 2^{|\vec{y}| - n - m}) \otimes \tilde{\Lambda} t \right) \circ (\text{cp}_1 \otimes id_n)$$

**Proposition 7.13.**  $\Lambda t$  is a controlled morphism, that controls  $t$ , i.e.:

$$[\Lambda t] = \langle 0 | \otimes [H_m^n(1)] + \langle 1 | \otimes [t]$$

*Proof.* We have

$$\begin{aligned} [\Lambda t] \circ (|0\rangle \otimes id_n) &= \left[ \Lambda(s 2^{|\vec{y}| - n - m}) \circ |0\rangle \right] \otimes \left[ \tilde{\Lambda} t \circ (|0\rangle \otimes id_n) \right] = 1 \otimes \frac{1}{2^{|\vec{y}|}} \sum_{\vec{y}, \vec{x}_1, \vec{x}_2} e^{2i\pi 0} |\vec{x}_1\rangle\langle\vec{x}_2| \\ &= \sum_{\vec{x}_1, \vec{x}_2} |\vec{x}_1\rangle\langle\vec{x}_2| = [H_m^n(1)] \end{aligned}$$

and

$$\begin{aligned} [\Lambda t] \circ (|1\rangle \otimes id_n) &= \left[ \Lambda(s 2^{|\vec{y}| - n - m}) \circ |1\rangle \right] \otimes \left[ \tilde{\Lambda} t \circ (|1\rangle \otimes id_n) \right] \\ &= \frac{s 2^{|\vec{y}|}}{2^{n+m}} \otimes \frac{1}{2^{|\vec{y}|}} \sum_{\vec{y}, \vec{x}_1, \vec{x}_2} e^{2i\pi P} |\vec{O}\rangle\langle\vec{I}| \end{aligned}$$

$$= \frac{s}{2^{n+m}} \sum_{\vec{y}, \vec{x}_1, \vec{x}_2} e^{2i\pi P} |\vec{O}\rangle\langle\vec{I}| = s \sum_{\vec{y}} e^{2i\pi P} |\vec{O}\rangle\langle\vec{I}| = t \quad \square$$

Notice that if  $t \in \mathbf{SOP}[\frac{1}{2^n}]$ , then  $\Lambda t \in \mathbf{SOP}[\frac{1}{2^{\max(3,n)}}]$ . Notice also that, for  $t : n \rightarrow m$ , only  $n + m + 1$  additional variables are needed in  $\tilde{\Lambda}t$ . However, the controlled scalar will require around  $2(|\vec{y}| - n - m + \log_2(|s|))$  variables, and the phase polynomial gets one degree higher. Hence, it may be useful to put additional information to use if we are provided some.

**Definition 7.14.** Let  $t = s \sum_{\vec{y}} e^{2i\pi P} |\vec{O}\rangle\langle\vec{I}| \in \mathbf{SOP}$ . For any  $\vec{v}_1 \in \{0, 1\}^m, \vec{v}_2 \in \{0, 1\}^n$  and  $\rho e^{i\theta} \neq 0$ , we define:

$$\tilde{\Lambda}_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) := \frac{1}{\rho 2^{n+m}} \sum e^{2i\pi \left( -\frac{\theta}{2\pi} + P + \frac{1}{2} \left( \vec{O} + \vec{x}_1 + x_0 \vec{x}_1 + x_0 \vec{v}_1 \right) \cdot \vec{x}'_1 + \frac{1}{2} \left( \vec{I} + \vec{x}_2 + x_0 \vec{x}_2 + x_0 \vec{v}_2 \right) \cdot \vec{x}'_2 \right)} |\vec{x}_1\rangle\langle x_0 \oplus 1, \vec{x}_2|$$

and:

$$\Lambda_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) := \left( \Lambda(s\rho e^{i\theta}) \otimes \tilde{\Lambda}_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) \right) \circ (\text{cp}_1 \otimes \text{id}_n)$$

**Proposition 7.15.** For any  $\vec{v}_1 \in \{0, 1\}^m, \vec{v}_2 \in \{0, 1\}^n$  and  $\rho e^{i\theta} \neq 0$  such that  $\langle \vec{v}_1 | \llbracket t \rrbracket | \vec{v}_2 \rangle = \rho e^{i\theta}$ ,  $\Lambda_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta)$  is a controlled morphism, that controls  $t$ , i.e.:

$$\llbracket \Lambda_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) \rrbracket = \langle 0 | \otimes \llbracket H_m^n(1) \rrbracket + \langle 1 | \otimes \llbracket t \rrbracket$$

*Proof.* Let  $t = s \sum_{\vec{y}} e^{2i\pi P} |\vec{O}\rangle\langle\vec{I}| \in \mathbf{SOP}$ ,  $\vec{v}_1 \in \{0, 1\}^m, \vec{v}_2 \in \{0, 1\}^n$  and  $\rho e^{i\theta} \neq 0$  such that  $\langle \vec{v}_1 | \llbracket t \rrbracket | \vec{v}_2 \rangle = \rho e^{i\theta}$ . We have:

$$\begin{aligned} & \left[ \tilde{\Lambda}_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) \circ (|0\rangle \otimes \text{id}_n) \right] \\ &= \left[ \frac{1}{\rho 2^{n+m}} \sum_{\substack{\vec{y}, \vec{x}_1, \vec{x}_2 \\ \vec{x}'_1, \vec{x}'_2}} e^{2i\pi \left( -\frac{\theta}{2\pi} + P + \frac{1}{2} \left( \vec{O} + \vec{v}_1 \right) \cdot \vec{x}'_1 + \frac{1}{2} \left( \vec{I} + \vec{v}_2 \right) \cdot \vec{x}'_2 \right)} |\vec{x}_1\rangle\langle\vec{x}_2| \right] \\ &= \frac{1}{\rho e^{i\theta}} \left[ \frac{1}{2^{n+m}} \sum_{\vec{y}, \vec{x}'_1, \vec{x}'_2} e^{2i\pi \left( P + \frac{1}{2} \left( \vec{O} + \vec{v}_1 \right) \cdot \vec{x}'_1 + \frac{1}{2} \left( \vec{I} + \vec{v}_2 \right) \cdot \vec{x}'_2 \right)} \right] \left[ \sum_{\vec{x}_1, \vec{x}_2} |\vec{x}_1\rangle\langle\vec{x}_2| \right] \\ &= \frac{1}{\rho e^{i\theta}} \llbracket \langle \vec{v}_1 | t | \vec{v}_2 \rangle \rrbracket \llbracket H_m^n(1) \rrbracket = \llbracket H_m^n(1) \rrbracket \end{aligned}$$

so

$$\begin{aligned} \llbracket \Lambda_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) \rrbracket \circ (|0\rangle \otimes \text{id}_n) &= \left[ \Lambda(s\rho e^{i\theta}) \circ |0\rangle \right] \otimes \left[ \tilde{\Lambda}_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) \circ (|0\rangle \otimes \text{id}_n) \right] \\ &= \llbracket H_m^n(1) \rrbracket \end{aligned}$$

And:

$$\tilde{\Lambda}_2(t | \vec{v}_1, \vec{v}_2, \rho, \theta) \circ (|0\rangle \otimes \text{id}_n) \xrightarrow{\text{HH}} \frac{1}{\rho 2^{n+m}} \sum e^{2i\pi \left( -\frac{\theta}{2\pi} + P + \frac{1}{2} \left( \vec{O} + \vec{x}_1 \right) \cdot \vec{x}'_1 + \frac{1}{2} \left( \vec{I} + \vec{x}_2 \right) \cdot \vec{x}'_2 \right)} |\vec{x}_1\rangle\langle\vec{x}_2|$$



$$\xrightarrow{\text{HH}^{n+m}} \frac{1}{\rho} \sum e^{2i\pi(-\frac{\theta}{2\pi}+P)} |\vec{O}\rangle\langle\vec{I}|$$

so

$$\begin{aligned} \llbracket \Lambda_2(t|\vec{v}_1, \vec{v}_2, \rho, \theta) \rrbracket \circ (|1\rangle \otimes id_n) &= \llbracket \Lambda(s\rho e^{i\theta}) \circ |1\rangle \rrbracket \otimes \llbracket \tilde{\Lambda}_2(t|\vec{v}_1, \vec{v}_2, \rho, \theta) \circ (|1\rangle \otimes id_n) \rrbracket \\ &= s\rho e^{i\theta} \llbracket \frac{1}{\rho} \sum e^{2i\pi(-\frac{\theta}{2\pi}+P)} |\vec{O}\rangle\langle\vec{I}| \rrbracket \\ &= \llbracket s \sum e^{2i\pi P} |\vec{O}\rangle\langle\vec{I}| \rrbracket = \llbracket t \rrbracket \end{aligned}$$

This proves  $\llbracket \Lambda_2(t|\vec{v}_1, \vec{v}_2, \rho, \theta) \rrbracket = \langle 0| \otimes \llbracket H_m^n(1) \rrbracket + \langle 1| \otimes \llbracket t \rrbracket$ . □

In order to control  $t : n \rightarrow m$  in this version, we only need around  $2(n+m+\log_2(|s\rho e^{i\theta}|))$  additional variables, and the initial phase polynomial is simply added another polynomial. However, it requires some prior knowledge on the linear map that is represented by  $t$ , namely, one of its coefficients. Another caveat of importance is that  $\frac{1}{\rho e^{i\theta}}$ , which is needed in the definition of the control, will in general get us out of the dyadic fragments.

**Remark 7.16.** In the definitions of  $\Lambda$  and  $\Lambda_2$  for **SOP**-terms, we used the control of scalars denoted  $\Lambda$ . However, any other notion of control of scalars (like  $\Lambda'$  for instance) would work.

## 8. CONCLUSION AND DISCUSSION

We have given a new rewrite system for the (balanced) 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 any dyadic fragment of quantum computation. 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. In particular, we have exhibited two rules that, in order to be applied properly, require solving a hard but well studied problem, i.e. that of building Groebner bases. We wonder if this is a sufficient price to pay to get confluence. If not, it would be interesting to see if a completion of the rewrite strategy à la Knuth-Bendix is possible in this framework, and if such completion would eventually yield a finite set of rules (note that this would not necessarily make problems like circuit equivalence classically tractable, as the size of the phase polynomial may still grow exponentially quickly, and application of some rules may require solving hard problems).

On a more foundational note, we conjecture that the rewrite strategy  $\xrightarrow{\text{TH}}$  is minimal, i.e. that none of the rewrites can be derived from the others. The same question can be asked in **ZH**, but no proof (confirming or refuting it) has been provided yet. The graphical study of the rewrite rules of subsection 4.4 hint at directions to simplify the rules of **ZH** thanks to their interpretation in **SOP**, or to transport potential proofs of minimality between the two. The completeness result derived from that of the **ZH**, and this small study of how the rewrites translate as **ZH** transformations, really show how the two formalisms give different and complementary approaches to rewriting and simplifying representations of quantum processes.

Thanks to the proximity of **SOP** with the **ZH**-calculus and to the theory developed in the graphical setting to perform sums and concatenations of terms, we were able to transport these constructions in the **SOP** formalism. This proves very useful when analysing Hamiltonian-based quantum computation, which heavily relies on building large Hamiltonians by sums of smaller terms.

All the work presented here was in the case of *balanced* sum-over-paths. Adding unbalancedness as in [Amy23] allows for reductions of equivalent terms with fewer variables, at the cost of a larger space in which the morphisms live. While having fewer variables is crucial when performing simulation (which implies actually computing the term), the extra degree of freedom that amplitude polynomials offer also makes issues like confluence potentially harder to tackle. We wonder if a proper unbalanced Sum-Over-Paths formalism can be stated for the Toffoli-Hadamard fragment and the dyadic fragments.

## REFERENCES

- [ACG<sup>+</sup>23] M. Amy, M. Crawford, A. N. Glauzell, M. L. Macasieb, S. S. Mendelson, and N. J. Ross. Catalytic embeddings of quantum circuits, 2023.
- [AG04] 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.
- [Aha03] Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. *eprint arXiv:quant-ph/0301040*, Jan 2003.
- [Amy19] 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.
- [Amy23] Matthew Amy. Complete equational theories for the sum-over-paths with unbalanced amplitudes. *Electronic Proceedings in Theoretical Computer Science*, 384:127–141, August 2023. URL: <http://dx.doi.org/10.4204/EPTCS.384.8>, doi:10.4204/eptcs.384.8.
- [BK19] 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.
- [BKMB<sup>+</sup>23] Miriam Backens, Aleks Kissinger, Hector Miller-Bakewell, John van de Wetering, and Sal Wolfs. Completeness of the ZH-calculus. *Compositionality*, 5, July 2023. doi:10.32408/compositionality-5-5.
- [Boo14] Adam D. Bookatz. QMA-complete problems. *Quantum Information and Computation*, 14(5&6):361–383, may 2014. URL: <https://doi.org/10.26421/qic14.5-6-1>, doi:10.26421/qic14.5-6-1.
- [CBB<sup>+</sup>21] Christophe Charetton, 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.
- [CBL<sup>+</sup>21] Christophe Charetton, 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.
- [CD11] 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/10.1088/1367-2630/13/4/043016>, doi:10.1088/1367-2630/13/4/043016.
- [CK10] 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/10.1007/978-3-642-14162-1\\_25](https://doi.org/10.1007/978-3-642-14162-1_25), doi:10.1007/978-3-642-14162-1\_25.
- [dBBW20] 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.
- [Had15] 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.
- [HRA<sup>+</sup>22] Mohammad Haidar, Marko J. Rančić, Thomas Ayril, 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.
- [JPV18] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '18*, pages 559–568, New York, NY, USA, 2018. ACM. URL: <http://doi.acm.org/10.1145/3209108.3209131>, doi:10.1145/3209108.3209131.
- [JPV19] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A Generic Normal Form for ZX-Diagrams and Application to the Rational Angle Completeness. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–10, June 2019. doi:10.1109/LICS.2019.8785754.
- [JPV22] Emmanuel Jeandel, Simon Perdrix, and Margarita Veshchezerova. Addition and Differentiation of ZX-Diagrams. In Amy P. Felty, editor, *7th International Conference on Formal Structures for Computation and Deduction (FSCD 2022)*, volume 228 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 13:1–13:19, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2022/16294>, doi:10.4230/LIPIcs.FSCD.2022.13.
- [JWB05] 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.
- [KvdW20] 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.
- [Lac04] 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>.
- [Lem19] 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>.
- [LvdWK21] 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.
- [ML13] Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5. Springer Science & Business Media, 2013.
- [Sel10] Peter Selinger. A survey of graphical languages for monoidal categories. In *New Structures for Physics*, pages 289–355. Springer, 2010.
- [Shi03] 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>.

- [SIS<sup>+</sup>11] Yosuke Sato, Shutaro Inoue, Akira Suzuki, Katsusuke Nabeshima, and Ko Sakai. Boolean gröbner bases. *J. Symb. Comput.*, 46(5):622–632, May 2011. doi:10.1016/j.jsc.2010.10.011.
- [SWY22] Razin A. Shaikh, Quanlong Wang, and Richie Yeung. How to sum and exponentiate hamiltonians in ZXW calculus, 2022. QPL 2022.
- [vdWW19] John van de Wetering and Sal Wolffs. Completeness of the Phase-free ZH-calculus, April 2019. arXiv:1904.07545.
- [Vil19] 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.
- [Vil21] 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.
- [Vil23] Renaud Vilmart. Completeness of Sum-Over-Paths for Toffoli-Hadamard and the Dyadic Fragments of Quantum Computation. In Bartek Klin and Elaine Pimentel, editors, *31st EACSL Annual Conference on Computer Science Logic (CSL 2023)*, volume 252 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:17, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: <https://drops.dagstuhl.de/opus/volltexte/2023/17497>, doi:10.4230/LIPIcs.CSL.2023.36.
- [Zan15] Fabio Zanasi. *Interacting Hopf Algebras – the theory of linear systems*. PhD thesis, Université de Lyon, 2015. URL: <http://www.zanasi.com/fabio/#/publications.html>.