The Structure of Sum-Over-Paths, its Consequences, and Completeness for Clifford

Renaud Vilmart

The Structure of Sum-Over-Paths, its Consequences, and Completeness for Clifford

Renaud Vilmart
vilmart@lri.fr

Université Paris-Saclay, CNRS, Laboratoire de Recherche en Informatique, 91405, Orsay, France

Abstract. We show that the formalism of "Sum-Over-Path" (SOP), used for symbolically representing linear maps or quantum operators, together with a proper rewrite system, has a structure of dagger-compact PROP. Several consequences arise from this observation:
– Morphisms of SOP are very close to the diagrams of the graphical calculus called ZH-Calculus, so we give a system of interpretation between the two
– A construction, called the discard construction, can be applied to enrich the formalism so that, in particular, it can represent the quantum measurement.
We also enrich the rewrite system so as to get the completeness of the Clifford fragments of both the initial formalism and its enriched version.

1 Introduction

The "Sum-Over-Paths" (SOP) formalism [1] was introduced in order to perform verification on quantum circuits. It is inspired by Feynman's notion of path-integral, and can be conceived as a discrete version of it.

The core idea here is to represent unitary transformations in a symbolic way, so as to be able to simplify the term, which would for instance accelerate its evaluation. To do so, the formalism comes equipped with a rewrite system, which reduces any term into an equivalent one.

As pure quantum circuits (which represent unitary maps) can easily be mapped to an SOP morphism, one can try and perform verification: given a specification $\mathcal{S}$ and another SOP morphism t obtained from a circuit supposed to verify the specification, we can compute the term $\mathcal{S} \circ t^\dagger$ and try to reduce it to the identity. In a very similar way, one can check whether two quantum circuits perform the same unitary map.

The rewrite system is known to be complete for Clifford unitary maps, i.e. in the Clifford fragment of quantum mechanics, the term obtained from $t_1 \circ t_2^\dagger$ will reduce to the identity iff t_1 and t_2 represent the same unitary map. Moreover, this reduction terminates in time polynomial in the size of the SOP term (itself related to the size of the quantum circuit), and still performs well outside the Clifford fragment.

Another use for this formalism is quantum simulation, the problem of evaluating the unitary map represented by a quantum circuit. Doing this is exponential in the number of variables in the SOP term, but the rewrite strategy reduces this number of variables, so each step in the reduction roughly divides the evaluation time by two.

Something that the SOP formalism cannot do for now however is circuit simplification. Indeed, even though we can easily translate an arbitrary quantum circuit to an SOP term, and then reduce it, there is no known way to extract a quantum circuit from the result.

We show in this paper that the formalism, when considered as a category (denoted **SOP**), has the structure of a †-compact PROP. This structure is explained in details in Section 2. This structure is shared by a much larger set of maps than just unitary maps, namely **Qubit**, the category whose morphisms are linear maps of $\mathbb{C}^{2^m} \times \mathbb{C}^{2^n}$. In particular, we show that any morphism of **Qubit** could be expressed as a morphism of **SOP**.

Because the formalism is no longer restricted to unitary maps, we argue that it could benefit from a slight redefinition, which is done in Section 4.

Another "family" of categories that share this structure is the family of graphical languages for quantum computation: ZX-Calculus, ZW-Calculus and ZH-Calculus [3,6,7]. All three formalisms represent morphisms of **Qubit** using diagrams, and come with equational theories, proven to be

complete for the whole category [3,10,18], i.e. whenever two diagrams represent the same morphism of **Qubit**, the first can be turned into the other using only the equational theory.

In Section 5, we show that any diagram of the ZH-Calculus can be interpreted as a morphism of **SOP**, and conversely, that any morphism of **SOP** can be turned into an equivalent ZH-diagram.

This link between the two formalisms was first shown in [12,13]. We give here a slightly different presentation, that in particular uses our redefinition of sums-over-paths.

In Section 6, we realise that the rewrite system of **SOP** is not enough for the completeness of the Clifford fragment of **Qubit**. We define a restriction of **SOP** that captures exactly this fragment, and enrich the set of rules so as to get the completeness in this restriction.

In Section 7, we enrich the whole formalism using the discard construction [5], so as to be able to represent completely positive maps, as well as the operator of partial trace. Again, one can consider the Clifford fragment of this formalism. We give a new set of rewrite rules, and show that it makes the fragment complete.

2 Background

2.1 PROPs and String Diagrams

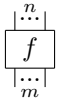
The first kind of category we will be interested in is the *PROP* [11,19]. A PROP **C** is a strict symmetric monoidal category [14,17] generated by a single object, or equivalently, whose objects form $\mathbb{N}$. Hence the morphisms of **C** are of the form $f : n \to m$. They can be composed sequentially $(. \circ .)$ or in parallel $(. \otimes .)$, and they satisfy the following axioms:

$$f \circ (g \circ h) = (f \circ g) \circ h \qquad f \otimes (g \otimes h) = (f \otimes g) \otimes h$$
$$id_m \circ f = f = f \circ id_n \qquad id_0 \otimes f = f = f \otimes id_0$$
$$(f_2 \circ f_1) \otimes (g_2 \circ g_1) = (f_2 \circ g_2) \circ (f_1 \otimes g_1)$$

The category is also equipped with a particular family of morphisms $\sigma_{n,m} : n + m \to m + n$. Intuitively, these allow morphisms to swap places. They satisfy additional axioms:

$$\sigma_{n,m+p} = (id_m \otimes \sigma_{n,p}) \circ (\sigma_{n,m} \otimes id_p) \qquad \sigma_{n+m,p} = (\sigma_{n,p} \otimes id_m) \circ (id_n \otimes \sigma_{m,p})$$
$$\sigma_{m,n} \circ \sigma_{n,m} = id_{n+m} \qquad (id_p \otimes f) \circ \sigma_{n,p} = \sigma_{m,p} \circ (f \otimes id_p)$$

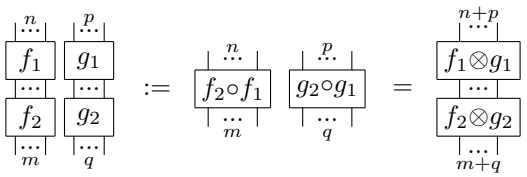
Monoidal categories, and subsequently PROPs, have the benefit of having a nice graphical representation, using string diagrams. The object n and equivalently id_n is represented by n parallel wires: 

; and a morphism $f : n \to m$ as a box with n input wires and m output wires: 

.

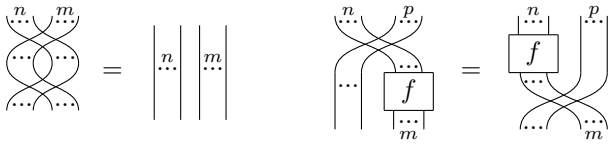
The sequential composition $(. \circ .)$ is obtained by plugging the outputs of the morphism on the right to the inputs of the morphism of the left. The parallel composition $(. \otimes .)$ is obtained by putting the two diagrams side by side.

The first set of axioms is for coherence: the two compositions are associative, so we can forget about the parentheses, and the following string diagram is well defined, as:



The morphism $\sigma_{n,m}$ is represented by 

. The following axioms are satisfied:



2.2 †-Compact PROPs

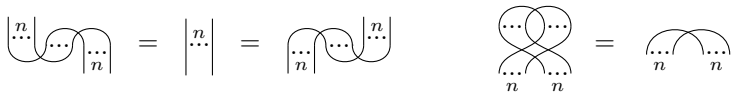
Some PROPs can have additional structure, such as a compact-closed structure, or having a †-functor.

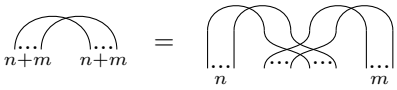
A †-PROP $\mathbf{C}$ is a PROP together with an involutive, identity-on-objects functor $(.)^\dagger : \mathbf{C}^{\mathrm{op}} \to \mathbf{C}$ compatible with $(. \otimes .)$. That is, for every morphism $f : n \to m$, there is a morphism $f^\dagger : m \to n$ such that $f^{\dagger\dagger} = f$. It behaves with the compositions by $(f \circ g)^\dagger = g^\dagger \circ f^\dagger$ and $(f \otimes g)^\dagger = f^\dagger \otimes g^\dagger$. Finally, we have $\sigma^\dagger_{n,m} = \sigma_{m,n}$.

A †-compact PROP as two particular families of morphisms: $\eta_n : 0 \to 2n$ and $\epsilon_n : 2n \to 0$. These are dual by the †-functor: $\eta_n^\dagger = \epsilon_n$. They satisfy the following axioms:

$$(\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n) = id_n = (id_n \otimes \epsilon_n) \circ (\eta_n \otimes id_n)$$
$$\sigma_{n,n} \circ \eta_n = \eta_n \qquad \eta_{n+m} = (id_n \otimes \sigma_{n,m} \otimes id_m) \circ (\eta_n \otimes \eta_m)$$

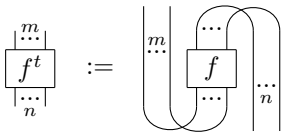
The morphisms η_n and ϵ_n may be denoted  and  . They hence satisfy:





In this context, one can define the transpose operator of a morphism f as:

$$f^t := (\epsilon_m \otimes id_n) \circ (id_m \otimes f \otimes id_n) \circ (id_m \otimes \eta_m) \qquad \text{i.e.}$$



One can check that, thanks to the axioms of †-compact PROP, $(f \circ g)^t = g^t \circ f^t$, $(f \otimes g)^t = f^t \otimes g^t$, and $f^{tt} = f$.

We can then compose $(.)^t$ and $(.)^\dagger$: $\overline{(.)} := (.)^{\dagger t}$. Again using the axioms of †-compact PROP, one can check that $(.)^{\dagger t} = (.)^{t\dagger}$.

2.3 Example: Qubit

The usual example of a strict symmetric †-compact monoidal category is **FHilb**, the category whose objects are finite dimensional Hilbert spaces, and whose morphisms are linear maps between them. It is not, however, a PROP, as it is not generated by a single object.

One subcategory of **FHilb** that *is* a PROP, though, is **Qubit** the subcategory of **FHilb** generated by the object $\mathbb{C}^2$, considered as the object 1. A morphism $f : n \to m$ of **Qubit** is hence a linear map from $\mathbb{C}^{2^n}$ to $\mathbb{C}^{2^m}$. $(. \circ .)$ is then the usual composition of linear maps, and $(. \otimes .)$ is the usual tensor product of linear maps. One can check that the first set of axioms is satisfied.

This is not enough to conclude that **Qubit** is a PROP. We still need to define a family of morphisms $\sigma_{n,m}$. In the Dirac notation, given a basis $\mathcal{B}$ of $\mathbb{C}^2$, we can define $\sigma_{n,m}$ as $\sigma_{n,m} := \sum_{(\boldsymbol{x},\boldsymbol{y}) \in \mathcal{B}^n \times \mathcal{B}^m} |\boldsymbol{y}, \boldsymbol{x}\rangle\langle \boldsymbol{x}, \boldsymbol{y}|$. One can then check that all the axioms of PROPs are satisfied.

Qubit is not only a PROP, but also †-compact. Indeed, first, given a morphism:

$$f = \sum_{(\boldsymbol{x},\boldsymbol{y}) \in \mathcal{B}^n \times \mathcal{B}^m} a_{\boldsymbol{x},\boldsymbol{y}} \, |\boldsymbol{y}\rangle\langle \boldsymbol{x}|$$

we can define its dagger $f^\dagger := \sum_{(\boldsymbol{x},\boldsymbol{y})\in\mathcal{B}^n\times\mathcal{B}^m} \overline{a_{\boldsymbol{x},\boldsymbol{y}}}\,|\boldsymbol{x}\rangle\langle\boldsymbol{y}|$, which is the usual definition of the dagger for linear maps.

Its compact structure can be given by $\eta_n := \sum_{\boldsymbol{x}\in B^n} |\boldsymbol{x},\boldsymbol{x}\rangle$, which implies $\epsilon_n = \eta_n^\dagger = \sum_{\boldsymbol{x}\in B^n} \langle\boldsymbol{x},\boldsymbol{x}|$. One can check that all the axioms of †-compact PROPs are satisfied.

Since **Qubit** is †-compact, we can define the transpose $(.)^t$ which happens to be the usual transpose of linear maps, and the conjugate $\overline{(.)}$, which again is the usual conjugation in linear maps over $\mathbb{C}$.

There is a subcategory of **Qubit** that is of importance: **Stab**. It is the smallest †-compact subcategory of **Qubit** (the compact structure is preserved) that contains:

- $|0\rangle : 0 \to 1$
- $H := \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) : 1 \to 1$
- $S := |0\rangle\langle 0| + i\,|1\rangle\langle 1| : 1 \to 1$
- $CZ := |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| : 2 \to 2$

3 The Category SOP

3.1 SOP as a PROP

The point of the Sum-Over-Paths formalism [1], is to *symbolically* manipulate morphisms written in a form akin to the Dirac notation. Reasoning on symbolic terms allow us to detect where a term can be simplified in a "smaller" one, or to give a specification on a term.

A morphism of the category will be of the form $|\boldsymbol{x}\rangle \mapsto s \sum_{\boldsymbol{y}\in V^k} e^{2i\pi P(\boldsymbol{x},\boldsymbol{y})}\,|\boldsymbol{Q}(\boldsymbol{x},\boldsymbol{y})\rangle$ where:

- $\boldsymbol{x} = x_1,\ldots,x_n$ is the input signature, it is a list of variables
- V is a set of variables (hence $\boldsymbol{y}$ is a collection of these variables)
- P is a multivariate polynomial, instantiated by the variables $\boldsymbol{x}$ and $\boldsymbol{y}$
- $\boldsymbol{Q} = Q_1,\ldots,Q_m$ is the output signature, it is a multivariate, multivalued boolean polynomial
- s is a real scalar

We may denote V_f a subset of the variables V used in f. Then by default, if V_f and V_g are used in the same term, we consider that $V_f \cap V_g = \varnothing$. To distinguish the two sum operators (the one in P and the one in $\boldsymbol{Q}$), we can denote the one in the output signature $\boldsymbol{Q}$ as $\oplus$. Moreover, it will sometimes be necessary to immerse one of the boolean polynomials Q_i in the polynomial P. We hence define $\widehat{Q_i}$ inductively as $\widehat{x} = x$ for a variable x, $\widehat{pq} = \widehat{p}\widehat{q}$ and $\widehat{p\oplus q} = \widehat{p} + \widehat{q} - 2\widehat{p}\widehat{q}$.

Definition 1 (SOP). SOP *is defined as the PROP where, given a set of variables V:*

- *Identity morphisms are $id_n : |\boldsymbol{x}\rangle \mapsto |\boldsymbol{x}\rangle$*
- *Morphisms $f : n \to m$ are of the form $f : |\boldsymbol{x}\rangle \mapsto s \sum_{\boldsymbol{y}\in V^k} e^{2i\pi P(\boldsymbol{x},\boldsymbol{y})}\,|\boldsymbol{Q}(\boldsymbol{x},\boldsymbol{y})\rangle$ where $s \in \mathbb{R}$, $\boldsymbol{x} \in V^n$, $P \in \mathbb{R}[X_1,\ldots,X_{n+k}]/(1, X_i^2 - X_i)$, and $\boldsymbol{Q} \in (\mathbb{F}_2[X_1,\ldots,X_{n+k}])^m$*
- *Composition is obtained as $f \circ g := |\boldsymbol{x}_g\rangle \mapsto s_f s_g \sum_{\substack{\boldsymbol{y}_f\in V_f^{k_f}\\ \boldsymbol{y}_g\in V_g^{k_g}}} e^{2i\pi(P_g + P_f[\boldsymbol{x}_f \leftarrow \widehat{\boldsymbol{Q}_g}])}\,|\boldsymbol{Q}_f[\boldsymbol{x}_f \leftarrow \boldsymbol{Q}_g]\rangle$*
- *Tensor product is obtained as $f \otimes g := |\boldsymbol{x}_f\boldsymbol{x}_g\rangle \mapsto s_f s_g \sum_{\substack{\boldsymbol{y}_f\in V_f^{k_f}\\ \boldsymbol{y}_g\in V_g^{k_g}}} e^{2i\pi(P_g+P_f)}\,|\boldsymbol{Q}_f\boldsymbol{Q}_g\rangle$*
- *The symmetric braiding is $\sigma_{n,m} : |\boldsymbol{x}_1,\boldsymbol{x}_2\rangle \mapsto |\boldsymbol{x}_2,\boldsymbol{x}_1\rangle$*

The polynomial P is called the *phase polynomial*, as it appears in the morphism in $e^{2i\pi\cdot}$. Because of this, we consider the polynomial modulo 1. We also consider the polynomial quotiented by $X^2 - X$ for all its variables X, as these variables are to be evaluated in $\{0,1\}$, so we consider $X^2 = X$.

Notice that the definition of the identities does not directly fit the description of the morphisms. However, we can rewrite it as $|\boldsymbol{x}\rangle \mapsto |\boldsymbol{x}\rangle = |\boldsymbol{x}\rangle \mapsto 1 \sum_{y\in V^0} e^{2i\pi 0}\,|\boldsymbol{x}\rangle$. Hence, when we sum over a single

element, we may forget the sum operator, and when the phase polynomial is 0, we may not write it. Notice by the way that $id_0 = |\rangle \mapsto |\rangle$. Indeed, $|\rangle$ is absolutely valid, it represents an empty register.

Example 1. We can give the **SOP** version of the usual quantum gates:

$$R_Z(\alpha) := |x\rangle \mapsto e^{2i\pi\frac{\alpha x}{2\pi}}|x\rangle \qquad CNot := |x_1, x_2\rangle \mapsto |x_1, x_1 \oplus x_2\rangle$$
$$H := |x\rangle \mapsto \frac{1}{\sqrt{2}}\sum_{y\in V} e^{2i\pi\frac{xy}{2}}|y\rangle \qquad CZ := |x_1, x_2\rangle \mapsto e^{2i\pi\frac{x_1x_2}{2}}|x_1, x_2\rangle$$

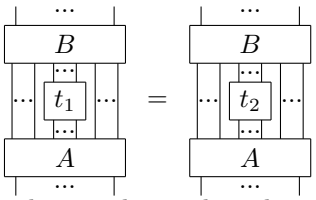
Example 2. Let us derive the operation $(id \otimes H) \circ CNot \circ (id \otimes H)$:

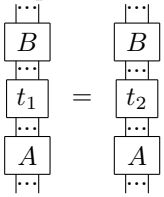
$$\begin{aligned}
&(id \otimes H) \circ CNot \circ (id \otimes H)\\
&= (id \otimes H) \circ \left(|x_1, x_2\rangle \mapsto |x_1, x_1 \oplus x_2\rangle\right) \circ \left(|x_1, x_2\rangle \mapsto \frac{1}{\sqrt{2}}\sum_{y\in V} e^{2i\pi\frac{x_2y}{2}}|x_1, y\rangle\right)\\
&= \left(|x_1, x_2\rangle \mapsto \frac{1}{\sqrt{2}}\sum_{y\in V} e^{2i\pi\frac{x_2y}{2}}|x_1, y\rangle\right) \circ \left(|x_1, x_2\rangle \mapsto \frac{1}{\sqrt{2}}\sum_{y_1\in V} e^{2i\pi\frac{x_2y_1}{2}}|x_1, x_1 \oplus y_1\rangle\right)\\
&= |x_1, x_2\rangle \mapsto \frac{1}{2}\sum_{y_1,y_2\in V} e^{2i\pi\left(\frac{x_2y_1}{2} + \frac{x_1+y_1-2x_1y_1}{2}y_2\right)}|x_1, y_2\rangle
\end{aligned}$$

where $x_1 + y_1 - 2x_1y_1 = \widehat{x_1 \oplus y_1}$.

The previous definition contains a claim: that **SOP** is a PROP. To be so, one has to check all the axioms of PROPs. One has to be careful when doing so. Indeed, the sequential composition $(. \circ .)$ induces a substitution. Hence, one has to check all the axioms in the presence of a "context", that is, one has to show that the axioms can be applied *locally*.

If an axiom states 

, one should ideally check that 

for any "before" morphism B and any "after" morphism A. However, this can be easily reduced to checking that 

.

In the case of the axioms of PROPs, this can further be reduced to showing the axioms without context, as neither id_n nor $\sigma_{n,m}$ introduce variables or phases. For the other axioms, however, the context will have to be taken into account.

A fairly straightforward but tedious verification gives that, indeed, **SOP** is a PROP. We give as an example the proof of associativity of the sequential composition (without context for simplicity):

$$\begin{aligned}
(f \circ g) \circ h &= \left(|\boldsymbol{x}\rangle \mapsto s_g s_f \sum e^{2i\pi\left(P_g + P_f[\boldsymbol{x}_f \leftarrow \widehat{\boldsymbol{Q}_g}]\right)}|\boldsymbol{Q}_f[\boldsymbol{x}_f \leftarrow \boldsymbol{Q}_g]\rangle\right) \circ h\\
&= |\boldsymbol{x}\rangle \mapsto s_g s_f s_h \sum e^{2i\pi\left(P_h + P_g[\boldsymbol{x}_g \leftarrow \widehat{\boldsymbol{Q}_h}] + P_f[\boldsymbol{x}_f \leftarrow \widehat{\boldsymbol{Q}_g}, \boldsymbol{x}_g \leftarrow \widehat{\boldsymbol{Q}_h}]\right)}|\boldsymbol{Q}_f[\boldsymbol{x}_f \leftarrow \boldsymbol{Q}_g, \boldsymbol{x}_g \leftarrow \boldsymbol{Q}_h]\rangle\\
&= |\boldsymbol{x}\rangle \mapsto s_g s_f s_h \sum e^{2i\pi\left(P_h + P_g[\boldsymbol{x}_g \leftarrow \widehat{\boldsymbol{Q}_h}] + P_f[\boldsymbol{x}_f \leftarrow \widehat{\boldsymbol{Q}_g}[\boldsymbol{x}_g \leftarrow \widehat{\boldsymbol{Q}_h}]]\right)}|\boldsymbol{Q}_f[\boldsymbol{x}_f \leftarrow \boldsymbol{Q}_g[\boldsymbol{x}_g \leftarrow \boldsymbol{Q}_h]]\rangle\\
&= f \circ \left(|\boldsymbol{x}\rangle \mapsto s_g s_h \sum e^{2i\pi\left(P_h + P_g[\boldsymbol{x}_g \leftarrow \widehat{\boldsymbol{Q}_h}]\right)}|\boldsymbol{Q}_g[\boldsymbol{x}_g \leftarrow \boldsymbol{Q}_h]\rangle\right) = f \circ (g \circ h)
\end{aligned}$$

or that σ swaps the places of morphisms:

$$(id_p \otimes f) \circ \sigma_{n,p} = \left(|\boldsymbol{x}_1, \boldsymbol{x}_2\rangle \mapsto s \sum e^{2i\pi P_f}|\boldsymbol{x}_1, \boldsymbol{Q}_f\rangle\right) \circ (|\boldsymbol{x}_1, \boldsymbol{x}_2\rangle \mapsto |\boldsymbol{x}_2, \boldsymbol{x}_1\rangle)$$

$$= |\boldsymbol{x}_1, \boldsymbol{x}_2\rangle \mapsto s \sum e^{2i\pi P_f} |\boldsymbol{Q}_f, \boldsymbol{x}_1\rangle$$
$$= (|\boldsymbol{x}_1, \boldsymbol{x}_2\rangle \mapsto |\boldsymbol{x}_2, \boldsymbol{x}_1\rangle) \circ \left(|\boldsymbol{x}_1, \boldsymbol{x}_2\rangle \mapsto s \sum e^{2i\pi P_f} |\boldsymbol{Q}_f, \boldsymbol{x}_2\rangle\right) = \sigma_{m,p} \circ (f \otimes id_p)$$

3.2 From SOP to Qubit

To check the soundness of what we are going to do in the following, it may be interesting to have a way of interpreting morphisms of **SOP** as morphisms of **Qubit**.

Definition 2. *The functor* $[\![.]\!] : \mathbf{SOP} \to \mathbf{Qubit}$ *is defined as being identity on objects, and such that, for* $f = |\boldsymbol{x}\rangle \mapsto s \sum_{\boldsymbol{y} \in V^k} e^{2i\pi P(\boldsymbol{x},\boldsymbol{y})} |Q(\boldsymbol{x}, \boldsymbol{y})\rangle$*:*

$$[\![f]\!] := \quad s \sum_{(\boldsymbol{x},\boldsymbol{y}) \in \{0,1\}^n \times \{0,1\}^k} e^{2i\pi P(\boldsymbol{x},\boldsymbol{y})} |Q(\boldsymbol{x}, \boldsymbol{y})\rangle\langle \boldsymbol{x}|$$

Example 3. The interpretation of H is as intended the Hadamard gate:

$$[\![H]\!] = \frac{1}{\sqrt{2}} \sum_{x,y \in \{0,1\}} e^{2i\pi \frac{xy}{2}} |y\rangle\langle x| = \frac{1}{\sqrt{2}} \left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right)$$

Proposition 1. *The interpretation* $[\![.]\!]$ *is a* PROP-functor*, meaning:*

- $[\![. \circ .]\!] = [\![.]\!] \circ [\![.]\!]$
- $[\![. \otimes .]\!] = [\![.]\!] \otimes [\![.]\!]$
- $[\![\sigma_{n,m}]\!] = \sigma_{n,m}$

Proof. This is a straightforward verification.

3.3 SOP as a †-Compact PROP

Towards a Compact Structure It is tempting to try and adapt the compact structure of **Qubit** to **SOP**. To do so, we can first define $\eta_n := |\rangle \mapsto \sum_{\boldsymbol{y} \in V^n} |\boldsymbol{y}, \boldsymbol{y}\rangle$. However, we cannot as easily define ϵ_n. What ϵ_1 intuitively does in **Qubit** is: given two inputs x_1 and x_2, it checks if they are equal, if so it returns the scalar 1, if not, the scalar 0.

In **SOP** we can force two variables to be equal, using a third fresh variable y. Indeed, consider the sum $\sum e^{2i\pi(\frac{x_1+x_2}{2}y+P)}$ where y is fresh i.e. not used in P. Then, if the variables x_1 and x_2 are different, then

$$\sum e^{2i\pi(\frac{x_1+x_2}{2}y+P)} = \sum e^{2i\pi(\frac{y}{2}+P)} = \sum e^{2i\pi(0+P)} + \sum e^{2i\pi(\frac{1}{2}+P)} = \sum e^{2i\pi P} - \sum e^{2i\pi P} = 0$$

Hence, we can define ϵ_1 as $\epsilon_1 := |x_1, x_2\rangle \mapsto \frac{1}{2} \sum_{y \in V} e^{2i\pi \frac{x_1+x_2}{2} y} |\rangle$ and even extend it to arbitrary objects: $\epsilon_n := |\boldsymbol{x}_1, \boldsymbol{x}_2\rangle \mapsto \frac{1}{2^n} \sum_{\boldsymbol{y} \in V^n} e^{2i\pi \frac{\boldsymbol{x}_1 \cdot \boldsymbol{y} + \boldsymbol{x}_2 \cdot \boldsymbol{y}}{2}} |\rangle$.

We can check that $[\![\epsilon_1]\!] = \epsilon_1$:

$$[\![\epsilon_1]\!] = \frac{1}{2} \sum_{x_i, y \in \{0,1\}} e^{2i\pi \frac{x_1+x_2}{2} y} |\rangle\langle x_1, x_2| = \frac{1}{2} \sum_{x_i \in \{0,1\}} (1 + e^{i\pi(x_1+x_2)}) \langle x_1, x_2|$$
$$= \langle 00| + \langle 11|$$

Similarly, $[\![\epsilon_n]\!] = \epsilon_n$.

We can now try to check whether the axioms of †-compact PROPs (at least the ones that do not require the †, as we have not defined it yet) are satisfied:

$$\sigma_{n,n} \circ \eta_n = \left(|\boldsymbol{x}_1, \boldsymbol{x}_2\rangle \mapsto |\boldsymbol{x}_2, \boldsymbol{x}_1\rangle\right) \circ \left(|\rangle \mapsto \sum_{\boldsymbol{y} \in V^n} |\boldsymbol{y}, \boldsymbol{y}\rangle\right) = |\rangle \mapsto \sum_{\boldsymbol{y} \in V^n} |\boldsymbol{y}, \boldsymbol{y}\rangle = \eta_n$$

$$
\begin{aligned}
&(id_n \otimes \sigma_{n,m} \otimes id_m) \circ (\eta_n \otimes \eta_m) \\
&\qquad = \left(|\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4\rangle \mapsto |\boldsymbol{x}_1, \boldsymbol{x}_3, \boldsymbol{x}_2, \boldsymbol{x}_4\rangle \right) \circ \left(|\rangle \mapsto \sum_{\boldsymbol{y}_1 \in V^n, \boldsymbol{y}_2 \in V^m} |\boldsymbol{y}_1, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_2\rangle \right) \\
&\qquad = |\rangle \mapsto \sum_{\boldsymbol{y}_1 \in V^n, \boldsymbol{y}_2 \in V^m} |\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_1, \boldsymbol{y}_2\rangle = |\rangle \mapsto \sum_{\boldsymbol{y} \in V^{n+m}} |\boldsymbol{y}, \boldsymbol{y}\rangle = \eta_{n+m}
\end{aligned}
$$

These two equations were shown without a context for simplicity, but still hold with it.

However, the equation:

$$(\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n) = id_n = (id_n \otimes \epsilon_n) \circ (\eta_n \otimes id_n)$$

is not satisfied, as:

$$(\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n) = |\boldsymbol{x}\rangle \mapsto \frac{1}{2} \sum_{\boldsymbol{y}_1, \boldsymbol{y}_2 \in V^n} e^{2i\pi \frac{\boldsymbol{x} \cdot \boldsymbol{y}_2 + \boldsymbol{y}_1 \cdot \boldsymbol{y}_2}{2}} |\boldsymbol{y}_1\rangle \neq id_n$$

The fact that we have $(\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n) \neq id_n$ in **SOP** but $[\![(\epsilon_n \otimes id_n) \circ (id_n \otimes \eta_n)]\!] = [\![id_n]\!]$ in **Qubit** hints at a way to *rewrite* the first term as the second in **SOP**.

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

$$\sum_{\boldsymbol{y}} e^{2i\pi \left(\frac{y_0}{2}(y_0' + \widehat{Q_2}) + R \right)} |\boldsymbol{Q}\rangle \underset{\substack{y_0 \notin \mathrm{Var}(R, Q_2, \boldsymbol{Q}) \\ y_0' \notin \mathrm{Var}(Q_2)}}{\longrightarrow} 2 \sum_{\boldsymbol{y} \setminus \{y_0, y_0'\}} e^{2i\pi \left(R[y_0' \leftarrow \widehat{Q_2}] \right)} |\boldsymbol{Q}\left[y_0' \leftarrow Q_2\right]\rangle \tag{HH}$$

$$\sum_{\boldsymbol{y}} e^{2i\pi \left(\frac{y_0}{4} + \frac{y_0}{2} \widehat{Q_2} + R \right)} |\boldsymbol{Q}\rangle \underset{y_0 \notin \mathrm{Var}(Q_2, R, \boldsymbol{Q})}{\longrightarrow} \sqrt{2} \sum_{\boldsymbol{y} \setminus \{y_0\}} e^{2i\pi \left(\frac{1}{8} - \frac{1}{4} \widehat{Q_2} + R \right)} |\boldsymbol{Q}\rangle \tag{ω}$$

Fig. 1. Rewrite strategy $\underset{\text{Clif}}{\longrightarrow}$.

An Equational Theory A rewrite strategy is given in [1], and we show in Figure 1 the ones we are going to use in the paper. Each rewrite rule contains a condition, which usually ensures that a variable (the one we want to get rid of) does not appear in some polynomials. We hence use Var as the operator that gets all the variables from a sequence of polynomials:

$$\begin{cases}
\mathrm{Var}(Q_1, Q_2, \ldots) = \mathrm{Var}(Q_1) \cup \mathrm{Var}(Q_2) \cup \ldots \\
\mathrm{Var}(Q_1 \oplus Q_2) = \mathrm{Var}(Q_1) \cup \mathrm{Var}(Q_2) \\
\mathrm{Var}(Q_1 Q_2) = \mathrm{Var}(Q_1) \cup \mathrm{Var}(Q_2) \\
\mathrm{Var}(y) = \{y\} \text{ if } y \in V \\
\mathrm{Var}(0) = \mathrm{Var}(1) = \varnothing
\end{cases}$$

For simplicity, the input signature is omitted, as well as the parameters in the polynomials.

$\underset{\text{Clif}}{\longrightarrow}$ denotes the rewrite system formed by the three rules (Elim), (HH) and (ω). $\overset{*}{\underset{\text{Clif}}{\longrightarrow}}$ is the transitive closure of the rewrite system. Notice that all the rules remove at least one variable from the morphism, so we know $\underset{\text{Clif}}{\longrightarrow}$ terminates.

When the rules are not oriented, we get an equivalence relation on the morphisms of **SOP**. We denote this equivalence $\underset{\text{Clif}}{\sim}$.

We denote $\mathbf{SOP}/\underset{\text{Clif}}{\sim}$ the category **SOP** quotiented by the equivalence relation $\underset{\text{Clif}}{\sim}$.

It is to be noticed that:

Proposition 2. *For any rule r of $\underset{\text{Clif}}{\sim}$:*

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

Proof. This is an easy check.

This obviously implies that:

Corollary 1.

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

This result allows us to forget about the context in the rewriting process.

The newly obtained category $\mathbf{SOP}/\underset{\text{Clif}}{\sim}$ is still a PROP. It even has a compact structure, as the last necessary axiom is now derivable:

$$(\epsilon \otimes id) \circ (id \otimes \eta) = |x\rangle \mapsto \frac{1}{2} \sum_{y_1, y_2 \in V} e^{2i\pi(\frac{y_1 y_2}{2} + \frac{x y_2}{2})} |y_1\rangle \underset{\text{(HH)}}{\longrightarrow} |x\rangle \mapsto |x\rangle = id$$

and similarly for $(id \otimes \epsilon) \circ (\eta \otimes id) = id$.

†-Functor for SOP To show that $\mathbf{SOP}/\underset{\text{Clif}}{\sim}$ is †-compact, we lack a notion of †-functor **SOP**.

Remember that we defined $\overline{(.)}$ as $(.)^{\dagger t}$. Since we have a compact structure, we can already define the functor $(.)^t$. Thanks to the new equivalence relation $\underset{\text{Clif}}{\sim}$, this functor is involutive. Hence, we have $(.)^\dagger = \overline{(.)}^t$. An appropriate definition of the conjugation can be given:

Definition 3. *The conjugation is defined on morphisms $f = |\boldsymbol{x}\rangle \mapsto s_f \sum e^{2i\pi P_f} |\boldsymbol{Q}_f\rangle$ as:*

$$\overline{f} := |\boldsymbol{x}\rangle \mapsto s_f \sum e^{-2i\pi P_f} |\boldsymbol{Q}_f\rangle$$

This gives a definition of the †. For the record, if f is of the above form:

$$f^t = |\boldsymbol{x}\rangle \mapsto \frac{s_f}{2^m} \sum e^{2i\pi\left(P_f + \frac{\widehat{\boldsymbol{Q_f}[\boldsymbol{x}_f \leftarrow \boldsymbol{y}]} \cdot \boldsymbol{y}' + \boldsymbol{x} \cdot \boldsymbol{y}'}{2}\right)} |\boldsymbol{y}\rangle$$

$$f^\dagger = |\boldsymbol{x}\rangle \mapsto \frac{s_f}{2^m} \sum e^{2i\pi\left(-P_f + \frac{\widehat{\boldsymbol{Q_f}[\boldsymbol{x}_f \leftarrow \boldsymbol{y}]} \cdot \boldsymbol{y}' + \boldsymbol{x} \cdot \boldsymbol{y}'}{2}\right)} |\boldsymbol{y}\rangle$$

These three functors are the expected ones:

Proposition 3. $[\![(.)^t]\!] = [\![.]\!]^t$, $\left[\!\left[\overline{(.)}\right]\!\right] = \overline{[\![.]\!]}$, $[\![(.)^\dagger]\!] = [\![.]\!]^\dagger$

Proof. In appendix at page 23.

We can finally prove the wanted result:

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

Proof. In appendix, at page 23.

4 Redefinition of SOP

In **Qubit**, and hence in **SOP**, it may feel unnatural to have asymmetrical input and outputs. Why not have morphisms of the form $f = s\sum_{\boldsymbol{y}} e^{2i\pi P}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$? In this case, we have to change the definition of the composition, and, because of this, the **SOP** morphisms do not form a category. However, it is a category when quotiented by $\underset{\text{Clif}}{\sim}$. This is the reason why we did not define **SOP** like this at first, although it greatly simplifies the notions of compact structure and †-functor.

We now redefine **SOP**, and will use this new definition in the rest of the paper:

Definition 4 (SOP). *We redefine* **SOP** *as the collection of objects* $\mathbb{N}$ *and morphisms between them:*

- *Identity morphisms are* $id_n : \sum_{\boldsymbol{y}\in V^n} |\boldsymbol{y}\rangle\langle\boldsymbol{y}|$
- *Morphisms* $f : n \to m$ *are of the form* $f : s\sum_{\boldsymbol{y}\in V^k} e^{2i\pi P(\boldsymbol{y})}\,|\boldsymbol{O}(\boldsymbol{y})\rangle\langle\boldsymbol{I}(\boldsymbol{y})|$ *where* $s \in \mathbb{R}$, $P \in \mathbb{R}[X_1,\dots,X_k]/(1, X_i^2 - X_i)$, $\boldsymbol{O} \in (\mathbb{F}_2[X_1,\dots,X_k])^m$ *and* $\boldsymbol{I} \in (\mathbb{F}_2[X_1,\dots,X_k])^n$
- *Composition is obtained as* $f \circ g := \frac{s_f s_g}{2^{|I_f|}} \sum_{\substack{\boldsymbol{y}_f,\boldsymbol{y}_g\\ \boldsymbol{y}\in V^m}} e^{2i\pi\left(P_g + P_f + \frac{\boldsymbol{O}_g\cdot\boldsymbol{y}+\boldsymbol{I}_f\cdot\boldsymbol{y}}{2}\right)}\,|\boldsymbol{O}_f\rangle\langle\boldsymbol{I}_g|$
- *Tensor product is obtained as* $f \otimes g := s_f s_g \sum_{\boldsymbol{y}_f,\boldsymbol{y}_g} e^{2i\pi(P_g+P_f)}\,|\boldsymbol{O}_f\boldsymbol{O}_g\rangle\langle\boldsymbol{I}_f\boldsymbol{I}_g|$
- *The symmetric braiding is* $\sigma_{n,m} = \sum_{\boldsymbol{y}_1,\boldsymbol{y}_2} |\boldsymbol{y}_2,\boldsymbol{y}_1\rangle\langle\boldsymbol{y}_1,\boldsymbol{y}_2|$
- *The compact structure is* $\eta_n = \sum_{\boldsymbol{y}} |\boldsymbol{y},\boldsymbol{y}\rangle\langle|$ *and* $\epsilon_n = \sum_{\boldsymbol{y}} |\rangle\langle\boldsymbol{y},\boldsymbol{y}|$
- *The †-functor is given by:* $f^\dagger := s\sum_{\boldsymbol{y}} e^{-2i\pi P}\,|\boldsymbol{I}\rangle\langle\boldsymbol{O}|$
- *The functor* $[\![.]\!]$ *is defined as:* $[\![f]\!] := s\sum_{\boldsymbol{y}\in\{0,1\}^k} e^{2i\pi P(\boldsymbol{y})}\,|\boldsymbol{O}(\boldsymbol{y})\rangle\langle\boldsymbol{I}(\boldsymbol{y})|$

As announced, this is not a category, as $id \circ id = \frac{1}{2}\sum_{\boldsymbol{y}} e^{2i\pi\frac{y_1+y_2}{2}y_3}\,|y_2\rangle\langle y_1| \neq \sum_y |y\rangle\langle y| = id$. This problem is solved by reintroducing the rewrite rules, that we adapt to the new formalism in Figure 2.

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

$$\sum_{\boldsymbol{y}} e^{2i\pi\left(\frac{y_0}{2}(y_0'+\widehat{Q})+R\right)}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}| \underset{\substack{y_0\notin \mathrm{Var}(R,Q,\boldsymbol{O},\boldsymbol{I})\\ y_0'\notin\mathrm{Var}(Q)}}{\longrightarrow} 2\sum_{\boldsymbol{y}\setminus\{y_0,y_0'\}} e^{2i\pi\left(R\left[y_0'\leftarrow\widehat{Q}\right]\right)}\,(|\boldsymbol{O}\rangle\langle\boldsymbol{I}|)\,[y_0'\leftarrow Q] \tag{HH}$$

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

Fig. 2. Rewrite strategy $\underset{\text{Clif}}{\longrightarrow}$.

Again, we give the same name to the rewrite system, but this last one is the one we will use in the rest of the paper.

The results given for the previous formalisation can easily be adapted. In particular:

Proposition 4. **SOP**$/\underset{\text{Clif}}{\sim}$ *is a †-compact PROP, and* $[\![.]\!]$ *is a †-compact PROP-functor.*

Remark 1. In this new formalism, it is fairly easy to perform *weak simulation*: given a quantum circuit $\mathcal{C}$ and two quantum states $|\psi_i\rangle$ and $|\psi_o\rangle$, what is the probability of outputting $|\psi_o\rangle$ when the circuit $\mathcal{C}$ is applied to the input $|\psi_i\rangle$?

Given **SOP**-morphisms $t_{\mathcal{C}}$ for the circuit and t_i and t_o for the states $|\psi_i\rangle$ and $|\psi_o\rangle$, one simply needs to compute $t_o^\dagger \circ t_{\mathcal{C}} \circ t_i$ and simplify the term (which represents a scalar), before evaluating it.

Obviously, the efficiency of this method is conditioned by the simplification strategy used before evaluation.

Remark 2. When building a **SOP**-morphism t from a circuit (or a diagram as we will show in the following) in this formalism, the resulting t is always of size $O(d \times n)$ where n is the size of the register, and d the *depth* of the circuit (and for a diagram in $O(G \times a)$ where G is the number of generators and a the maximum arity of these generators).

This contrasts with the first definition of **SOP**, where the size of the constructed **SOP** term is polynomial for fixed restrictions of quantum mechanics (where the gates R_Z are restricted to parameters that are multiples of $\frac{\pi}{2^{p-1}}$ for a fixed p), but exponential in general. This is due to the substitution $[x \leftarrow \widehat{Q}]$ in the composition. Indeed, if Q contains ℓ monomials, $\widehat{Q}$ contains in the worst case $2^\ell - 1$ monomials. In the considered fragment, the size is constrained as $\frac{1}{2^p}\widehat{Q} \bmod 1$ has at most $\sum_{k=1}^{p} \binom{\ell}{k} \leq p\ell^p$ monomials.

5 SOP and Graphical Languages

The sum-over-paths formalism was initially intended to be used for isometries. As such, it was given a weak form of completeness – as we will discuss in the next section. However, if transforming a quantum circuit – that describes an isometry – into an **SOP** morphism is easy, the converse, transforming a **SOP** morphism into a circuit is not. And actually, all **SOP** morphisms do not represent an isometry. For instance, the morphism ϵ_1 described above is not an isometry. An even smaller example is $\sum_y |\rangle\langle y|$ which is a valid **SOP** morphism, but clearly does not represent an isometry.

The fact that **SOP** is †-compact hints at another (family) of language(s) more suited for representing it: the Z∗-Calculi: ZX, ZW and ZH. These are all †-compact graphical languages, that have an interpretation in **Qubit**, and are universal for **Qubit**. This means that any morphism of **Qubit** can be represented as a morphism of either of these 3 languages.

The language that happens to be the closest to **SOP** is the ZH-Calculus. This is the one we are going to present in the following. However, bear in mind that, as we have semantics-preserving functors between any two of these three languages, one can do the same work with ZX and ZW-Calculi.

The link between the sum-over-paths formalism and the ZH-Calculus was first shown in [12,13]. We give here a slightly different but equivalent presentation, that in particular uses the fact that we altered the formalism of **SOP**.

5.1 The ZH-Calculus

ZH is a PROP whose morphisms are composed (sequentially $(. \circ .)$ or in parallel $(. \otimes .)$) from Z-spiders and H-spiders:

– $Z^n_m : n \to m ::$  , called Z-spider

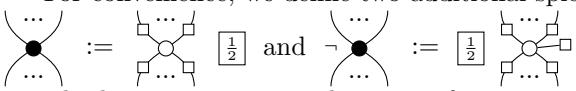
– $H^n_m(r) : n \to m ::$  , called H-spider, with a parameter $r \in \mathbb{C}$

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

ZH is made a †-compact PROP, which means it also has the symmetric structure σ, the compact structure (η, ϵ), and a †-functor $(.)^\dagger : \mathbf{ZH}^{\mathrm{op}} \to \mathbf{ZH}$. It is defined by:

$$(Z^n_m)^\dagger := Z^m_n \qquad \text{and} \qquad (H^n_m(r))^\dagger := H^m_n(\overline{r})$$

For convenience, we define two additional spiders:



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

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


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

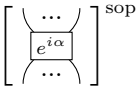
Notice that we used the same symbol for two different functors: the two interpretations $[\![.]\!] : \mathbf{SOP} \to \mathbf{Qubit}$ and $[\![.]\!] : \mathbf{ZH} \to \mathbf{Qubit}$. It should be clear from the context which one is to be used.

The language is universal: $\forall f \in \mathbf{Qubit},\ \exists D_f \in \mathbf{ZH},\quad [\![D_f]\!] = f$. In other words, the interpretation $[\![.]\!]$ is onto. This is shown using a notion of normal form. This means there is a functor $\mathcal{N} : \mathbf{Qubit} \to \mathbf{ZH}$.

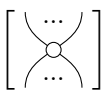
The language comes with an equational theory, which in particular gives the axioms for a †-compact PROP. We will not present it here.

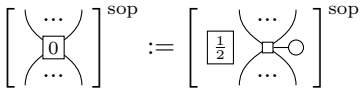
5.2 From ZH to SOP

We show in this section how any **ZH** morphism can be turned into a **SOP** morphism in a way that preserves the semantics. We define $[.]^{\mathrm{sop}} : \mathbf{ZH} \to \mathbf{SOP}$ as the †-compact PROP-functor such that:


$$:= \sum e^{2i\pi \frac{\alpha}{2\pi} x_1 \dots x_n y_1 \dots y_m} \, |y_1, \dots, y_m\rangle\langle x_1, \dots, x_n|$$

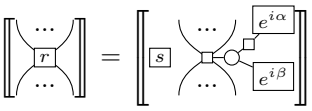
$$[\,\boxed{s}\,]^{\mathrm{sop}} := s\,|\rangle\langle| \qquad \text{for } s \in \mathbb{R}$$


$$:= \sum_y |y, \dots, y\rangle\langle y, \dots, y|$$



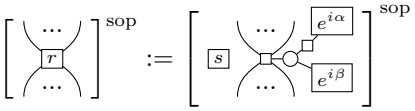
This does not give a full description of $[.]^{\mathrm{sop}}$, as we did not describe the interpretation of the H-spider for all parameters, but only for phases and 0. However, any H-spider can be decomposed using the previous ones:

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



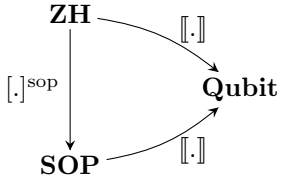
Proof. In appendix at page 24.

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



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

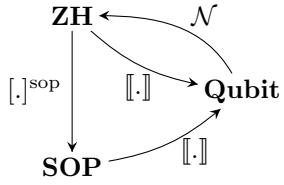
Proposition 5. $[\![[.]^{\mathrm{sop}}]\!] = [\![.]\!]$. *In other words, the following diagram commutes:*



Proof. This is a straightforward verification.

5.3 From SOP to ZH

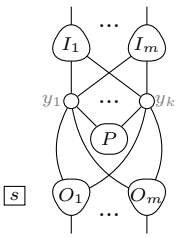
As we explained previously, there exists a functor from **Qubit** to **ZH**. Hence, we have the following (non commutative) diagram:



We could hence define the interpretation from **SOP** to **ZH** as $\mathcal{N}([\![.]\!])$. This would preserve the semantics, as $\mathcal{N}$ does. However, this would yield in general a diagram of exponential size in the size of the **SOP** morphism. Instead, we define in the following an interpretation of **SOP** morphisms as **ZH**-diagrams of roughly the same size.

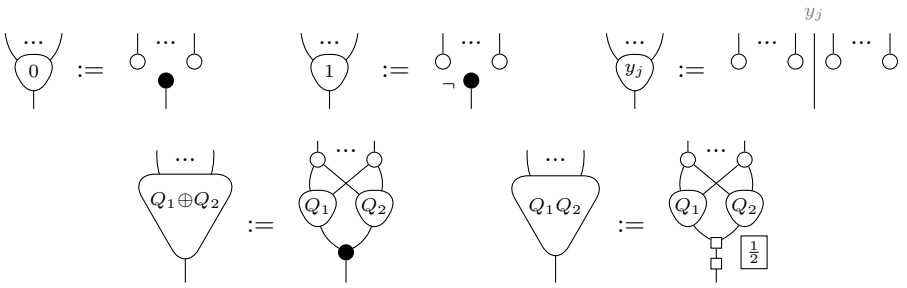
We define $[.]^{\text{ZH}} : \mathbf{SOP} \to \mathbf{ZH}$ on arbitrary **SOP** morphisms as:

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



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

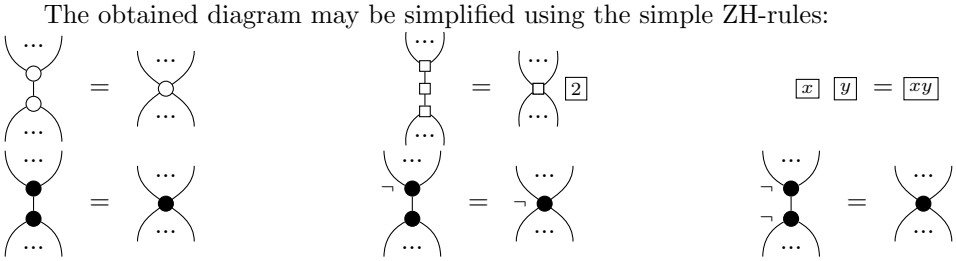
The inputs of O_i are linked to $y_1, \ldots, y_k$. The nodes O_i can be inductively defined as:



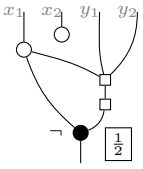
The nodes I_i are defined similarly, but upside-down.

The node P can be inductively defined as:

The obtained diagram may be simplified using the simple ZH-rules:



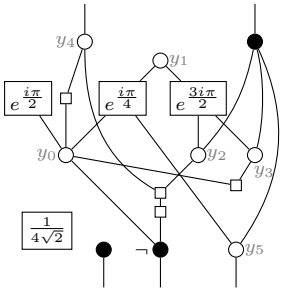
For instance, the polynomial $1 \oplus x_1 \oplus x_1 y_1 y_2$ in a diagram that contains variables x_1, x_2, y_1, y_2 will be represented after simplification as:



Example 4. The **SOP** morphism:

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

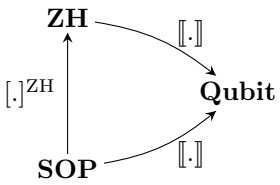
is mapped to



Proposition 6. $\left[[.]^{\mathrm{ZH}}\right]^{\mathrm{sop}} \underset{\mathrm{Clif}}{\sim} (.)$

Proof. In appendix at page 24.

Corollary 2. $[\![[.]^{\mathrm{ZH}}]\!] = [\![.]\!]$. *In other words, the following diagram commutes:*



Proof. Since $\underset{\mathrm{Clif}}{\sim}$ preserves the semantics, we have $[\![.]\!] = [\![\left[[.]^{\mathrm{ZH}}\right]^{\mathrm{sop}}]\!] = [\![[.]^{\mathrm{ZH}}]\!]$ by Propositions 6 and 5.

6 SOP for Clifford

The *Clifford* fragment of Quantum Mechanics is the one that represents **Stab**. We would like to have a characterisation of this fragment for **SOP**. Thankfully, this fragment is well known in **ZH**. It can hence be inferred in **SOP** thanks to $[.]^{\mathrm{sop}}$.

6.1 The Subcategories of ZH and SOP for Clifford

Definition 5. $\mathbf{ZH}_{\mathrm{Clif}}$ *is the* †*-compact subPROP of* **ZH** *with the same objects, and generated by:*


, 
, 
($\alpha \in \{0, \frac{\pi}{2}, \pi, -\frac{\pi}{2}\}$*)*, 
, 
.

Defining  :=  , we can still define the black spiders in this fragment.

Proposition 7. $[\![.]\!] : \mathbf{ZH}_{\mathrm{Clif}} \to \mathbf{Stab}$*, the standard interpretation of* **ZH***-diagrams restricted to the Clifford fragment in* **Stab** *is onto.*

Proof. In appendix at page 25.

We hence propose a restriction of **SOP** for the Clifford fragment, and show afterwards that it does indeed capture exactly **Stab**.

Definition 6. $\mathbf{SOP}_{\mathrm{Clif}}$ *is the subPROP of* **SOP** *with the same objects, and whose morphisms are of the form:*

$$\frac{1}{\sqrt{2}^p} \sum e^{2i\pi\left(\frac{1}{8}P^{(0)}+\frac{1}{4}P^{(1)}+\frac{1}{2}P^{(2)}\right)} |\boldsymbol{O}\rangle\langle\boldsymbol{I}|$$

where $P^{(i)}$ *is a polynomial with integer coefficients of degree at most* i *(hence* $P^{(0)}$ *is in fact merely an integer); and where all the* O_i *and* I_i *are linear.*

Proposition 8. $[\![.]\!] : \mathbf{SOP}_{\mathrm{Clif}} \to \mathbf{Stab}$, *the restriction of the standard interpretation to* $\mathbf{SOP}_{\mathrm{Clif}}$ *is onto* **Stab**.

Proof. In appendix at page 26.

Hence, $\mathbf{SOP}_{\mathrm{Clif}}$ does capture the Clifford fragment of quantum mechanics.

6.2 A Complete Rewrite System for Clifford

In [1], where the rewrite rules are introduced, the author gives a notion of completeness for Clifford *unitaries*, that we will refer to in the following as "weak completeness":

Proposition 9 (Weak Completeness for Clifford Unitaries). *Given two terms* t_1, t_2 *of* $\mathbf{SOP}_{\mathrm{Clif}}$ *such that* $[\![t_i]\!] \circ [\![t_i]\!]^\dagger = id = [\![t_i]\!]^\dagger \circ [\![t_i]\!]$, *we have:*

$$t_1 \circ t_2^\dagger \xrightarrow[\mathrm{Clif}]{*} id \quad \Longleftrightarrow \quad [\![t_1]\!] = [\![t_2]\!]$$

In practice, this is sufficient for deciding the equivalence of two Clifford quantum circuits, as they are represented as unitary morphisms of $\mathbf{SOP}_{\mathrm{Clif}}$. However, in our case, where we deal with more than unitaries, we cannot use this trick. Instead, we aim at a result like "$t_1 \xrightarrow{*} t \xleftarrow{*} t_2 \iff [\![t_1]\!] = [\![t_2]\!]$". In other words, we want a rewrite system that will transform any term of $\mathbf{SOP}_{\mathrm{Clif}}$ into a unique normal form.

The rewrite system $\xrightarrow[\mathrm{Clif}]{}$ is not enough for this:

Lemma 2. *There exist* t_1 *and* t_2 *two morphisms of* $\mathbf{SOP}_{\mathrm{Clif}}$ *such that:*

- $[\![t_1]\!] = [\![t_2]\!]$
- *there is no* t_i' *such that* $t_i \xrightarrow[\mathrm{Clif}]{} t_i'$
- $t_1 \neq t_2$

Proof. An example of such behaviour can be obtained with:

$$t_1 := \sum e^{2i\pi\left(\frac{y_1 y_2}{2} + \frac{y_2 y}{2}\right)} |y\rangle\langle y_1, y_2| \qquad t_2 := \sum e^{2i\pi \frac{y_2 y}{2}} |y_1 \oplus y\rangle\langle y_1, y_2|$$

To palliate this problem, we propose to add three rewrite rules to the previously presented ones. These new rewrite rules are shown in Figure 3.

$$\sum_{\boldsymbol{y}} e^{2i\pi(P)} |O_1, \cdots, \overbrace{y_0 \oplus O_i'}^{O_i}, \cdots, O_m\rangle\langle \boldsymbol{I}| \xrightarrow[\substack{y_0 \notin \mathrm{Var}(O_1,\ldots,O_{i-1},O_i') \\ O_i' \neq 0}]{} \sum_{\boldsymbol{y}} e^{2i\pi\left(P[y_0 \leftarrow \widehat{O_i}]\right)} \left(|\boldsymbol{O}\rangle\langle \boldsymbol{I}|\right)[y_0 \leftarrow O_i] \quad \text{(ket)}$$

$$\sum_{\boldsymbol{y}} e^{2i\pi(P)} |\boldsymbol{O}\rangle\langle I_1, \cdots, \overbrace{y_0 \oplus I_i'}^{I_i}, \cdots, I_m| \xrightarrow[\substack{y_0 \notin \mathrm{Var}(\boldsymbol{O},I_1,\ldots,I_{i-1},I_i') \\ I_i' \neq 0}]{} \sum_{\boldsymbol{y}} e^{2i\pi\left(P[y_0 \leftarrow \widehat{I_i}]\right)} \left(|\boldsymbol{O}\rangle\langle \boldsymbol{I}|\right)[y_0 \leftarrow I_i] \quad \text{(bra)}$$

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

Fig. 3. Additional rewrite rules. Together with those of $\xrightarrow[\mathrm{Clif}]{}$, they constitute the rewrite system $\xrightarrow[\mathrm{Clif+}]{}$.

The last rule (Z) describes what happens for a term that represents the linear map 0. Rule (bra) is simply the continuation of (ket). They explain how to operate suitable changes of variables.

Proposition 10. *The rewrite system* $\xrightarrow[\mathrm{Clif+}]{}$ *terminates.*

Proof. In appendix at page 26.

Not only does this rewrite system terminate, it is confluent in $\mathbf{SOP}_{\mathrm{Clif}}$ and the induced equivalence relation $\underset{\mathrm{Clif+}}{\sim}$ is complete for Clifford. We prove this by showing that any morphism of $\mathbf{SOP}_{\mathrm{Clif}}$ reduces to a normal form that is unique.

Lemma 3. *Any morphism of* $\mathbf{SOP}_{\mathrm{Clif}}$ *reduces by* $\underset{\mathrm{Clif+}}{\longrightarrow}$ *to a morphism of the form*

$$\frac{1}{\sqrt{2^p}} \sum e^{2i\pi P} \, |\boldsymbol{O}\rangle\langle \boldsymbol{I}|$$

where:

- $\mathrm{Var}(P) \subseteq \mathrm{Var}(\boldsymbol{O}, \boldsymbol{I})$ *or* $P = \frac{y_0}{2}$ *where* $y_0 \notin \mathrm{Var}(\boldsymbol{O}, \boldsymbol{I})$
- $O_i = \begin{cases} y_k \\ \quad or \\ c \oplus \bigoplus\limits_{y \in \mathrm{Var}(O_1, \ldots, O_{i-1})} c_y y \end{cases}$ *where* $c, c_y \in \{0, 1\}$
- $I_i = \begin{cases} y_k \\ \quad or \\ c \oplus \bigoplus\limits_{y \in \mathrm{Var}(\boldsymbol{O}, I_1, \ldots, I_{i-1})} c_y y \end{cases}$ *where* $c, c_y \in \{0, 1\}$

Proof. In appendix at page 26.

To start with, we deal with the case where the term represents the null map.

Proposition 11. *Let* t *be a morphism of* $\mathbf{SOP}_{\mathrm{Clif}}$ *such that* $[\![t]\!] = 0$*. Then:*

$$t \underset{\mathrm{Clif+}}{\overset{*}{\longrightarrow}} \sum_{y_0} e^{2i\pi \frac{y_0}{2}} \, |0, \ldots, 0\rangle\langle 0, \ldots, 0|$$

Proof. In appendix at page 26.

Corollary 3. *If a morphism* $t = \frac{1}{\sqrt{2^p}} \sum e^{2i\pi P} \, |\boldsymbol{O}\rangle\langle \boldsymbol{I}|$ *of* $\mathbf{SOP}_{\mathrm{Clif}}$ *is irreducible such that* $\mathrm{Var}(P) \subseteq \mathrm{Var}(\boldsymbol{O}, \boldsymbol{I})$*, then* $[\![t]\!] \neq 0$*.*

Before moving on to the completeness by normal forms theorem, we need a result for the uniqueness of the phase polynomial:

Lemma 4. *Let* P_1 *and* P_2 *be two polynomials of* $\mathbb{R}[X_1, \ldots, X_k]/(1, X^2 - X)$*, such that:*

$$\forall \boldsymbol{x} \in \{0, 1\}^k, \;\; P_1(\boldsymbol{x}) = P_2(\boldsymbol{x})$$

Then, $P_1 = P_2$*.*

Proof. In appendix at page 27.

Theorem 2. *Let* t_1*, and* t_2 *be two morphisms of* $\mathbf{SOP}_{\mathrm{Clif}}$ *such that* $[\![t_1]\!] = [\![t_2]\!]$*. Then, there exists* t *in* $\mathbf{SOP}_{\mathrm{Clif}}$ *such that* $t_1 \underset{\mathrm{Clif+}}{\overset{*}{\longrightarrow}} t \underset{\mathrm{Clif+}}{\overset{*}{\longleftarrow}} t_2$*, up to* α*-conversion.*

Proof. In appendix at page 27.

Corollary 4. *The equality of morphisms in* $\mathbf{SOP}_{\mathrm{Clif}}/\underset{\mathrm{Clif+}}{\sim}$ *is decidable in time polynomial in the size of the phase polynomial and in the combined size of the ket/bra polynomials.*

Although the set of rules is confluent in $\mathbf{SOP}_{\mathrm{Clif}}$, it is not in $\mathbf{SOP}$:

Lemma 5 (Non-confluence). *The rewrite systems* $\underset{\mathrm{Clif}}{\longrightarrow}$ *and* $\underset{\mathrm{Clif+}}{\longrightarrow}$ *are not confluent in* $\mathbf{SOP}$*.*

Proof. Consider the morphism $\sum e^{2i\pi\left(\frac{y_0}{4}+\frac{y_0y_1y_2}{2}+\frac{y_1y_3}{2}\right)}|y_3\rangle$:

$$\sum e^{2i\pi\left(\frac{y_0}{4}+\frac{y_0y_1y_2}{2}+\frac{y_1y_3}{2}\right)}|y_3\rangle \underset{\text{(HH)}}{\longrightarrow} 2\sum e^{2i\pi\left(\frac{y_0}{4}\right)}|y_0y_2\rangle$$

However

$$\sum e^{2i\pi\left(\frac{y_0}{4}+\frac{y_0y_1y_2}{2}+\frac{y_1y_3}{2}\right)}|y_3\rangle \underset{(\omega)}{\longrightarrow} \sqrt{2}\sum e^{2i\pi\left(\frac{1}{8}-\frac{y_1y_2}{4}+\frac{y_1y_3}{2}\right)}|y_3\rangle$$

The two resulting morphisms are not reducible, be it with $\underset{\text{Clif}}{\longrightarrow}$ or with $\underset{\text{Clif+}}{\longrightarrow}$.

6.3 Pivoting and Local Complementation

We show here how, in the Clifford case, the rule (HH) corresponds to the operation of *pivoting* [9], and the rule (ω) to that of *local complementation* [2,15]. To do so, we realise that graph states are easily representable in **SOP**, for instance by interpreting the ZH-version of the graph state as a **SOP** morphism.

Let $G = (V, E)$ be a graph, with vertices V and edges $E \subseteq V \times V$. The associated **SOP** morphism is:

$$\sum_{\boldsymbol{y}\in V} e^{2i\pi\left(\sum\limits_{(y_i,y_j)\in E}\frac{y_iy_j}{2}\right)}|\boldsymbol{y}\rangle$$

Pivoting The operation of pivoting can be used to simplify a diagram of $\mathbf{ZH}_{\text{Clif}}$ (or equivalently a Clifford diagram of the ZX-Calculus, as described in [9]). Informally, pivoting can be applied on any neighbouring pair of white nodes (where at least one of them is *internal* i.e. not linked to an input/output, for it to actually simplify the diagram). In the process, we complement the exclusive neighbours of both nodes with the other neighbours. Moreover, the common neighbours get an additional phase of π.

Let us see how it translates in **SOP**. Let $t = s\sum e^{2i\pi\left(\frac{y_0y_i}{2}+\frac{y_0}{2}\widehat{Q_0}+\frac{y_i}{2}\widehat{Q_i}+\frac{y_0+y_i}{2}\widehat{Q_{0i}}+R\right)}|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$ be a Clifford term, where the phase polynomial is already factorised by y_0 and y_i, the pair of variables/white dots on which to apply the pivoting. We consider that y_0 is internal $y_0 \notin \text{Var}(\boldsymbol{O}, \boldsymbol{I})$. The fact that y_0 and y_i are neighbours is captured by the term $\frac{y_0y_i}{2}$ in the phase polynomial. We can distinguish the exclusive neighbours of y_0 (resp. y_i) by Q_0 (resp. Q_i), and their common neighbours by Q_{0i}.

The rule (HH) can be applied, with the substitution $[y_i \leftarrow Q_0 \oplus Q_{0i}]$. The result is

$$t' = 2s\sum e^{2i\pi\left(\frac{1}{2}\widehat{Q_0Q_i}+\frac{1}{2}\widehat{Q_{0i}Q_i}+\frac{1}{2}\widehat{Q_0Q_{0i}}+\frac{1}{2}\widehat{Q_{0i}}+R\right)}(|\boldsymbol{O}\rangle\langle\boldsymbol{I}|)\,[y_i \leftarrow Q_0 \oplus Q_{0i}]$$

The term $\frac{1}{2}\widehat{Q_0Q_i}$ creates the monomial $\frac{y_ky_\ell}{2}$ for all $y_k \in \text{Var}(Q_0)$ and $y_\ell \in \text{Var}(Q_i)$. If this monomial was already in R, it gets cancelled. This performs the complementation between the groups of variables in Q_0 and those in Q_i, and similarly for $\frac{1}{2}\widehat{Q_{0i}Q_i}$ and $\frac{1}{2}\widehat{Q_0Q_{0i}}$. On the other hand, the term $\frac{1}{2}\widehat{Q_{0i}}$ creates a π phase for all the common neighbours of y_0 and y_i.

Local Complementation The operation of local complementation is another operation that can be used to simplify the Clifford term at hand. Consider an internal white node in a Clifford diagram. If this node has a phase of $\pm\frac{\pi}{2}$, it can be removed. Doing so will add a phase of $\mp\frac{\pi}{2}$ to all the neighbours of the node, and at the same time, will perform a local complementation on them (all the nodes connected through an H will get disconnected, and vice-versa). A global phase is also created.

A **SOP** morphism in this situation is of the form $t = s\sum e^{2i\pi\left(\frac{y_0}{4}+\frac{y_0}{2}(\sum x_i)+R\right)}|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$ with y_0 an internal variable and x_i its neighbours. The rule (ω) can hence be applied, and the resulted term is:

$$t' = \sqrt{2}s\sum e^{2i\pi\left(\frac{1}{8}-\frac{1}{4}(\sum x_i)+\frac{1}{2}(\sum\limits_{i\neq j}x_ix_j)+R\right)}|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$$

as $-\frac{1}{4}\widehat{\bigoplus x_i} = -\frac{1}{4}(\sum x_i) + \frac{1}{2}(\sum_{i\neq j} x_i x_j) \bmod 1$.

The constant $\frac{1}{8}$ corresponds to the global phase, the term $-\frac{1}{4}(\sum x_i)$ represents an additional $-\frac{\pi}{2}$ phase to all the neighbours of y_0, and term $\frac{1}{2}(\sum_{i\neq j} x_i x_j)$ performs the local complementation on them.

In the case where y_0 holds a $-\frac{\pi}{2}$ phase, the term can also be simplified like this.

7 SOP with Discards

7.1 The Discard Construction on SOP

In [5], a construction is given to extend any †-compact PROP for *pure* quantum mechanics to another †-compact PROP for quantum mechanics with environment. This new formalism can also be understood as the previous one, but where on top of it, one can discard the qubits. Because **SOP** fits the requirements, the construction can be applied to it.

First, we have to create the subcategory $\mathbf{SOP}_{\text{iso}}$ of **SOP** that contains all its isometries. The objects of the new category are the same, and its morphisms are $\{f \in \mathbf{SOP} \mid [\![f^\dagger \circ f]\!] = id\}$.

These are important, as the isometries are exactly the pure quantum operators that can be discarded. The next step in the construction does just that. We perform the affine completion of $\mathbf{SOP}_{\text{iso}}$, that is, for every object n, we add a new morphism $!_n : n \to 0$, and we impose that $! \circ f = !$ for any f in the new category, that we denote $\mathbf{SOP}^!_{\text{iso}}$. We also need to impose that $!_n \otimes !_m = !_{n+m}$ and $!_0 = id_0$.

Finally, the category $\mathbf{SOP}^{\doteq}$ is obtained as the pushout:

$$\begin{array}{ccc} \mathbf{SOP}_{\text{iso}} & \longrightarrow & \mathbf{SOP} \\ \downarrow & & \downarrow \\ \mathbf{SOP}^!_{\text{iso}} & \longrightarrow & \mathbf{SOP}^{\doteq} \end{array}$$

where the arrows are the inclusion functors.

We write morphisms in the new category in the form:

$$s \sum_{\boldsymbol{y}\in V^k} e^{2i\pi P(\boldsymbol{y})} |\boldsymbol{O}(\boldsymbol{y})\rangle !\boldsymbol{D}(\boldsymbol{y}) \langle \boldsymbol{I}(\boldsymbol{y})|$$

where the additional D is a set of multivariate polynomials of $\mathbb{F}_2$. The fact that it is a set, and not a list, already captures some rules on the discard: first permuting qubits and then discarding them is equivalent to discarding them right away. Similarly, copying data and discarding the copies is equivalent to discarding the data right away.

Pure morphisms are those such that $\boldsymbol{D} = \{\}$. In those, no qubits are discarded. We hence easily induce usual morphisms such as H and CZ in the new formalism.

The new morphisms $!_n$ are given by:

$$!_n := \sum_{\boldsymbol{y}\in V^n} |\rangle !\{y_1, \ldots, y_n\} \langle y_1, \ldots, y_n|$$

In the new formalism, the compositions are obtained by:

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

$$f \otimes g := s_f s_g \sum_{\boldsymbol{y}_f, \boldsymbol{y}_g} e^{2i\pi(P_g + P_f)} |\boldsymbol{O}_f \boldsymbol{O}_g\rangle !D_f \cup D_g \langle \boldsymbol{I}_f \boldsymbol{I}_g|$$

It might be useful to be able to give an interpretation to the morphisms of the new formalism. To do so, we use the CPM construction [16] to map morphisms of $\mathbf{SOP}^{\doteq}$ to morphisms of **SOP**.

Definition 7. *The functor* $\mathrm{CPM} : \mathbf{SOP}^{\doteq}/\underset{\text{Clif}\ \doteq}{\sim} \to \mathbf{SOP}/\underset{\text{Clif+}}{\sim}$ *is defined as:*

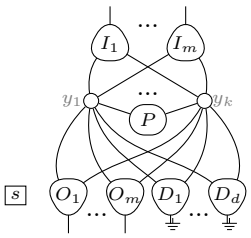
$$s\sum_{\boldsymbol{y}} e^{2i\pi P}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\,\langle\boldsymbol{I}| \;\mapsto\; \frac{s^2}{2^{|\boldsymbol{D}|}}\sum_{\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}} e^{2i\pi\left(P(\boldsymbol{y}_1)-P(\boldsymbol{y}_2)+\frac{\boldsymbol{D}(\boldsymbol{y}_1)\cdot\boldsymbol{y}+\boldsymbol{D}(\boldsymbol{y}_2)\cdot\boldsymbol{y}}{2}\right)}\,|\boldsymbol{O}(\boldsymbol{y}_1),\boldsymbol{O}(\boldsymbol{y}_2)\rangle\langle\boldsymbol{I}(\boldsymbol{y}_1),\boldsymbol{I}(\boldsymbol{y}_2)|$$

We can now define a standard interpretation of $\mathbf{SOP}^{\doteq}$-morphisms as:

Definition 8. *The standard interpretation* $[\![.]\!]$ *of* $\mathbf{SOP}^{\doteq}$ *is defined as* $[\![.]\!] := [\![\mathrm{CPM}(.)]\!]$.

Again, it is easy to transform any morphism of $\mathbf{SOP}^{\doteq}$ in $\mathbf{ZH}^{\doteq}$ and vice-versa:

$$\left[s\sum_{\boldsymbol{y}\in V^k} e^{2i\pi P(\boldsymbol{y})}\,|\boldsymbol{O}(\boldsymbol{y})\rangle!\boldsymbol{D}(\boldsymbol{y})\,\langle\boldsymbol{I}(\boldsymbol{y})|\right]^{\mathrm{ZH}} :=$$



and $[\frac{\perp}{\doteq}]^{\mathrm{sop}} = !_1$.

7.2 SOP with Discards for Clifford

The discard construction can be applied to the subcategory $\mathbf{SOP}_{\mathrm{Clif}}$. We end up with a new category $\mathbf{SOP}^{\doteq}_{\mathrm{Clif}}$, such that the following diagram, whose arrows are inclusions, commutes:

$$\begin{array}{ccc} \mathbf{SOP}_{\mathrm{Clif}} & \longrightarrow & \mathbf{SOP} \\ \downarrow & & \downarrow \\ \mathbf{SOP}^{\doteq}_{\mathrm{Clif}} & \longrightarrow & \mathbf{SOP}^{\doteq} \end{array}$$

Following the characterisation of $\mathbf{SOP}_{\mathrm{Clif}}$ morphisms, we can determine that all the morphisms of $\mathbf{SOP}^{\doteq}_{\mathrm{Clif}}$ are of the form:

$$\frac{1}{\sqrt{2}^p}\sum e^{2i\pi\left(\frac{1}{8}P^{(0)}+\frac{1}{4}P^{(1)}+\frac{1}{2}P^{(2)}\right)}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\,\langle\boldsymbol{I}|$$

where $p\in\mathbb{Z}$, where $P^{(i)}$ is a polynomial with integer coefficients and of degree at most i, and where the polynomials of $\boldsymbol{O},\boldsymbol{D}$ and $\boldsymbol{I}$ are linear.

The rewrite system presented previously can obviously be adapted to the new formalism (when there is a substitution, it has to be applied in $!\boldsymbol{D}$ as well). On top of that, the condition that makes $\mathbf{SOP}^{!}_{\mathrm{iso}}$ terminal can be translated as the meta rule:

$$\left[\!\!\left[\frac{s_f\overline{s_f}}{2^{|O_f|}}\sum e^{2i\pi\left(P_f(\boldsymbol{y})-P_f(\boldsymbol{y}')+\frac{\boldsymbol{O}_f(\boldsymbol{y})\cdot\boldsymbol{y}''+\boldsymbol{O}_f(\boldsymbol{y}')\cdot\boldsymbol{y}''}{2}\right)}\,|\boldsymbol{I}(\boldsymbol{y}')\rangle\langle\boldsymbol{I}(\boldsymbol{y})|\right]\!\!\right] = id$$

$$\implies \frac{s_f s_B}{2^{|\boldsymbol{O}_B|}}\sum e^{2i\pi\left(P_B+P_f+\frac{\boldsymbol{I}_f\cdot\boldsymbol{y}+\boldsymbol{O}_B\cdot\boldsymbol{y}}{2}\right)}\,|\boldsymbol{O}\rangle!\{\boldsymbol{O}_f,\ldots\}\,\langle\boldsymbol{I}_B| = s_B\sum e^{2i\pi P_B}\,|\boldsymbol{O}\rangle!\{\boldsymbol{O}_B,\ldots\}\,\langle\boldsymbol{I}_B|$$

As you can see, this rule is not easy to apply. Thankfully, the last part of [5] is devoted to showing that the big meta rule can sometimes be replaced by a few small ones. The idea is that, in some cases (in particular in the Clifford fragment), all the isometries can be generated from a finite set of generators. In particular, it is enough to impose that:

- $e^{i\alpha} = 1$
- $! \circ |0\rangle = 1$

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

$$\sum_{\boldsymbol{y}} e^{2i\pi\left(\frac{y_0}{2}(y_0'+\widehat{Q})+R\right)}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\,\langle \boldsymbol{I}| \underset{\substack{y_0\notin \mathrm{Var}(R,Q,\boldsymbol{D},\boldsymbol{O},\boldsymbol{I})\\ y_0'\notin \mathrm{Var}(Q)}}{\longrightarrow} 2\sum_{\boldsymbol{y}\setminus\{y_0,y_0'\}} e^{2i\pi\left(R\left[y_0'\leftarrow\widehat{Q}\right]\right)}\,(|\boldsymbol{O}\rangle!\boldsymbol{D}\,\langle \boldsymbol{I}|)\left[y_0'\leftarrow Q\right] \tag{HH}$$

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

$$\sum e^{2i\pi\left(P+\alpha\widehat{D_1\ldots D_p}\right)}\,|\boldsymbol{O}\rangle!\{D_1,\ldots,D_p,\ldots\}\,\langle \boldsymbol{I}| \longrightarrow \sum e^{2i\pi P}\,|\boldsymbol{O}\rangle!\{D_1,\ldots,D_p,\ldots\}\,\langle \boldsymbol{I}| \tag{Z$_{\doteq}$}$$

$$\sum_{\boldsymbol{y}} e^{2i\pi\left(P+\frac{y_0}{2}\widehat{Q}\right)}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\cup\{y_0\}\,\langle \boldsymbol{I}| \underset{y_0\notin \mathrm{Var}(P,\boldsymbol{O},\boldsymbol{I},\boldsymbol{D})}{\longrightarrow} \sqrt{2}\sum_{\boldsymbol{y}\setminus\{y_0\}} e^{2i\pi P}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\cup\{Q\}\,\langle \boldsymbol{I}| \tag{H$_{\doteq}$}$$

$$\sum e^{2i\pi P}\,|\boldsymbol{O}\rangle!\{D_1,\ldots,D_p,D_1\ldots D_p\oplus D_{p+1},\ldots\}\,\langle \boldsymbol{I}| \longrightarrow \sum e^{2i\pi P}\,|\boldsymbol{O}\rangle!\{D_1,\ldots,D_p,D_{p+1},\ldots\}\,\langle \boldsymbol{I}| \tag{$\oplus_{\doteq}$}$$

$$\sum e^{2i\pi P}\,|\boldsymbol{O}\rangle!\{c,\ldots\}\,\langle \boldsymbol{I}| \underset{c\in\{0,1\}}{\longrightarrow} \sum e^{2i\pi P}\,|\boldsymbol{O}\rangle!\{\ldots\}\,\langle \boldsymbol{I}| \tag{Cst$_{\doteq}$}$$

$$\begin{array}{l}\displaystyle\sum_{\boldsymbol{y}} e^{2i\pi(P)}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\cup\{\overbrace{y_0\oplus D_i'}^{D_i}\}\,\langle \boldsymbol{I}|\\ \qquad\qquad \Big\downarrow {\scriptstyle y_0\notin\mathrm{Var}(D_i')\ \ |\{D_k\in\boldsymbol{D}\ |\,\mathrm{mon}(D_k)\geq 2\}|\geqslant|\{D_k\in\boldsymbol{D}[y_0\leftarrow D_i]\ \ |\,\mathrm{mon}(D_k)\geq 2\}|}\\ \displaystyle\sum_{\boldsymbol{y}} e^{2i\pi\left(P[y_0\leftarrow\widehat{D_i}]\right)}\,(|\boldsymbol{O}\rangle!\boldsymbol{D}\cup\{D_i\}\,\langle \boldsymbol{I}|)\,[y_0\leftarrow D_i]\end{array} \tag{disc}$$

$$\sum_{\boldsymbol{y}} e^{2i\pi(P)}|\cdots,\overbrace{y_0\oplus O_i'}^{O_i}\oplus O_i'',\cdots\rangle!\boldsymbol{D}\,\langle \boldsymbol{I}| \underset{\substack{O_i'\neq 0\\ y_0\notin\mathrm{Var}(O_1,\ldots,O_{i-1},O_i',O_i'')\\ y_0\notin\mathrm{Var}(\boldsymbol{D})\text{ or }\{y_0,O_i'\}\subseteq\boldsymbol{D}\cup\{1\}}}{\longrightarrow} \sum_{\boldsymbol{y}} e^{2i\pi\left(P[y_0\leftarrow\widehat{O_i}]\right)}\,|\boldsymbol{O}[y_0\leftarrow O_i]\rangle!\boldsymbol{D}\,\langle \boldsymbol{I}[y_0\leftarrow O_i]| \tag{ket}$$

$$\sum_{\boldsymbol{y}} e^{2i\pi(P)}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\langle\cdots,\overbrace{y_0\oplus I_i'}^{I_i}\oplus I_i'',\cdots| \underset{\substack{I_i'\neq 0\\ y_0\notin\mathrm{Var}(\boldsymbol{O},I_1,\ldots,I_{i-1},I_i',I_i'')\\ y_0\notin\mathrm{Var}(\boldsymbol{D})\text{ or }\{y_0,I_i'\}\subseteq\boldsymbol{D}\cup\{1\}}}{\longrightarrow} \sum_{\boldsymbol{y}} e^{2i\pi\left(P[y_0\leftarrow\widehat{I_i}]\right)}\,|\boldsymbol{O}\rangle!\boldsymbol{D}\,\langle \boldsymbol{I}[y_0\leftarrow I_i]| \tag{bra}$$

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

Fig. 4. Rewrite system $\underset{\text{Clif}\ \doteq}{\longrightarrow}$ for $\mathbf{SOP}^{\doteq}$.

- $!\circ H = !$ (test)
- $!\circ S = !$
- $!_2\circ CZ = !_2$

We give in Figure 4 the updated set of rewrite rules.

Notice that we have made the choice to simplify the discarded polynomials before those in kets and bras. This is motivated by the example:

Example 5. Consider $t := |y_1,y_2,y_3\rangle!\{y_1\oplus y_2, y_2\oplus y_3, y_1\oplus y_3\}$. If (ket) had priority over (disc), the term could not be reduced. Instead, we reduce t as:

$$\begin{aligned}|y_1,y_2,y_3\rangle!\{y_1\oplus y_2,y_2\oplus y_3,y_1\oplus y_3\} &\underset{\text{(disc)}}{\longrightarrow} |y_1\oplus y_2,y_2,y_3\rangle!\{y_1,y_2\oplus y_3,y_1\oplus y_2\oplus y_3\}\\ &\underset{\oplus_{\doteq}}{\longrightarrow} |y_1\oplus y_2,y_2,y_3\rangle!\{y_1,y_2\oplus y_3\} \underset{\text{(disc)}}{\longrightarrow} |y_1\oplus y_2,y_2,y_2\oplus y_3\rangle!\{y_1,y_3\}\\ &\underset{\text{ket}}{\longrightarrow} |y_2,y_1\oplus y_2,y_1\oplus y_2\oplus y_3\rangle!\{y_1,y_3\} \underset{\text{ket}}{\longrightarrow} |y_2,y_1\oplus y_2,y_2\oplus y_3\rangle!\{y_1,y_3\}\end{aligned}$$

Hence, by giving priority to (disc) over (ket) and (bra), one can hope to reduce the number of discarded polynomials.

Proposition 12. *The rewrite system* $\underset{\text{Clif}\ \div}{\longrightarrow}$ *terminates.*

Proof. In appendix at page 28.

Lemma 6. *Any non-null morphism of* $\mathbf{SOP}^{\div}_{\text{Clif}}$ *can be reduced to:*

$$\frac{1}{\sqrt{2^p}} \sum_{\boldsymbol{y},\boldsymbol{y}_d} e^{2i\pi\left(\frac{1}{4}P^{(1)}(\boldsymbol{y})+\frac{1}{2}P^{(2)}(\boldsymbol{y},\boldsymbol{y}_d)\right)} |\boldsymbol{O}(\boldsymbol{y},\boldsymbol{y}_d)\rangle!\{\boldsymbol{y}_d\}\langle \boldsymbol{I}(\boldsymbol{y},\boldsymbol{y}_d)|$$

where:

- *polynomials of* $\boldsymbol{O}$ *and* $\boldsymbol{I}$ *are linear*
- *the set of discarded polynomials is reduced to a set of variables* $\{\boldsymbol{y}_d\}$
- $P^{(1)}$ *and* $P^{(2)}$ *have no constants*
- *no monomial of* $P^{(2)}$ *uses only variables of* $\boldsymbol{y}_d$
- $\{\boldsymbol{y}_d\} \subseteq \mathrm{Var}(\boldsymbol{O},\boldsymbol{I})$ *i.e. discarded variables have to appear somewhere in the ket or bra*
- $\mathrm{Var}(P^{(1)},P^{(2)}) \subseteq \mathrm{Var}(\boldsymbol{O},\boldsymbol{I},\boldsymbol{D})$ *or* $P = \frac{y_0}{2}$ *with* $y_0 \notin \mathrm{Var}(\boldsymbol{O},\boldsymbol{I},\boldsymbol{D})$.

Proof. In appendix at page 28.

Corollary 5. *Any morphism of* $\mathbf{SOP}^{\div}_{\text{Clif}}$ *eventually reduces to a morphism of the form given in Lemma 6.*

Proof. As the rewrite system terminates, and since every morphism of $\mathbf{SOP}^{\div}_{\text{Clif}}$ can be reduced into the form of Lemma 6, the rewrite system terminates in a term of the form of Lemma 6.

Lemma 7. *Any morphism* t *of* $\mathbf{SOP}^{\div}_{\text{Clif}}$ *such that* $[\![t]\!] = 0$ *reduces to:*

$$\sum_{y_0} e^{2i\pi\left(\frac{y_0}{2}\right)} |0,\cdots,0\rangle!\{\}\langle 0,\cdots,0|$$

Proof. In appendix at page 29.

Corollary 6. *If a morphism* t *of* $\mathbf{SOP}^{\div}_{\text{Clif}}$ *is terminal with* $\mathrm{Var}(P) \subseteq \mathrm{Var}(\boldsymbol{O},\boldsymbol{D},\boldsymbol{I})$, *then* $[\![t]\!] \neq 0$.

Theorem 3 (Completeness for Clifford). *Let* t_1 *and* t_2 *be two morphisms of* $\mathbf{SOP}^{\div}_{\text{Clif}}$ *such that* $[\![t_1]\!] = [\![t_2]\!]$. *If* t_1' *and* t_2' *are terminal such that* $t_1 \underset{\text{Clif}\ \div}{\overset{*}{\longrightarrow}} t_1'$ *and* $t_2 \underset{\text{Clif}\ \div}{\overset{*}{\longrightarrow}} t_2'$, *then* $t_1' = t_2'$ *up to* α*-conversion.*

To prove this theorem, we suggest to use the similar result in $\mathbf{SOP}_{\text{Clif}}$, and transport it to our case. To do so, we need some additional constructions.

Definition 9. *We define* $\overline{\mathbf{SOP}^{\div}_{\text{Clif}}}$ *as the set of morphisms of* $\mathbf{SOP}^{\div}_{\text{Clif}}$ *in the form given in Lemma 6. We define the function* F *on* $\overline{\mathbf{SOP}^{\div}_{\text{Clif}}}$ *such that, for any morphism*

$$t = \frac{1}{\sqrt{2^p}} \sum_{\boldsymbol{y},\boldsymbol{y}_d} e^{2i\pi P(\boldsymbol{y},\boldsymbol{y}_d)} |\boldsymbol{O}(\boldsymbol{y},\boldsymbol{y}_d)\rangle!\{\boldsymbol{y}_d\}\langle \boldsymbol{I}(\boldsymbol{y},\boldsymbol{y}_d)|$$

of $\overline{\mathbf{SOP}^{\div}_{\text{Clif}}}$:

$$F(t) := \frac{1}{\sqrt{2^{2p}}} \sum_{\boldsymbol{y},\boldsymbol{y}',\boldsymbol{y}_d} e^{2i\pi\left(P(\boldsymbol{y},\boldsymbol{y}_d)-P(\boldsymbol{y}',\boldsymbol{y}_d)\right)} |\boldsymbol{O}(\boldsymbol{y},\boldsymbol{y}_d),\boldsymbol{O}(\boldsymbol{y}',\boldsymbol{y}_d)\rangle\langle \boldsymbol{I}(\boldsymbol{y},\boldsymbol{y}_d),\boldsymbol{I}(\boldsymbol{y}',\boldsymbol{y}_d)|$$

This new functor F can be seen as a simplified CPM construction, in the case where the term is already simplified.

Proposition 13. *For any* $t \in \overline{\mathbf{SOP}^{\div}_{\text{Clif}}}$, $F(t) \underset{\text{Clif+}}{\sim} \mathrm{CPM}(t)$. *This implies* $[\![F(.)]\!] = [\![\mathrm{CPM}(.)]\!]$.

Proof.

$$\mathrm{CPM}(t) = \frac{1}{2^{p+|\boldsymbol{y}_{d_1}|}} \sum_{\boldsymbol{y}_1,\boldsymbol{y}_{d_1},\boldsymbol{y}_2,\boldsymbol{y}_{d_2},\boldsymbol{y}} e^{2i\pi\left(P(\boldsymbol{y}_1,\boldsymbol{y}_{d_1})-P(\boldsymbol{y}_2,\boldsymbol{y}_{d_2})+\frac{\boldsymbol{y}_{d_1}\cdot\boldsymbol{y}+\boldsymbol{y}_{d_2}\cdot\boldsymbol{y}}{2}\right)} |\boldsymbol{O}(\boldsymbol{y}_1,\boldsymbol{y}_{d_1}),\boldsymbol{O}(\boldsymbol{y}_2,\boldsymbol{y}_{d_2})\rangle\langle\boldsymbol{I}(\boldsymbol{y}_1,\boldsymbol{y}_{d_1}),\boldsymbol{I}(\boldsymbol{y}_2,\boldsymbol{y}_{d_2})|$$

$$\xrightarrow[\text{(HH)}]{*} \frac{1}{\sqrt{2}^{2p}} \sum_{\boldsymbol{y}_1,\boldsymbol{y}_2,\boldsymbol{y}_{d_1}} e^{2i\pi\left(P(\boldsymbol{y}_1,\boldsymbol{y}_{d_1})-P(\boldsymbol{y}_2,\boldsymbol{y}_{d_1})\right)} |\boldsymbol{O}(\boldsymbol{y}_1,\boldsymbol{y}_{d_1}),\boldsymbol{O}(\boldsymbol{y}_2,\boldsymbol{y}_{d_1})\rangle\langle\boldsymbol{I}(\boldsymbol{y}_1,\boldsymbol{y}_{d_1}),\boldsymbol{I}(\boldsymbol{y}_2,\boldsymbol{y}_{d_1})| = F(t)$$

Definition 10. *We define the function G on some morphisms of* $\mathbf{SOP}_{\mathrm{Clif}}$*.*
Let $t = \frac{1}{\sqrt{2}^p}\sum_{\boldsymbol{y}} e^{2i\pi P}\,|\boldsymbol{O}_1,\boldsymbol{O}_2\rangle\langle\boldsymbol{I}_1,\boldsymbol{I}_2|$ such that:

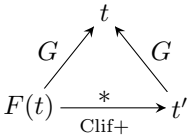
- $p = 2p'$
- $|\boldsymbol{O}_1| = |\boldsymbol{O}_2|$ *and* $|\boldsymbol{I}_1| = |\boldsymbol{I}_2|$
- $\{\boldsymbol{y}_d\} := \{\boldsymbol{y}\} \setminus \mathrm{Var}(\boldsymbol{O}_1 \oplus \boldsymbol{O}_2, \boldsymbol{I}_1 \oplus \boldsymbol{I}_2)$
- $\{\boldsymbol{y}_1\} := \mathrm{Var}(\boldsymbol{O}_1, \boldsymbol{I}_1) \setminus \{\boldsymbol{y}_d\}$
- $\{\boldsymbol{y}_2\} := (\{\boldsymbol{y}\} \setminus \{\boldsymbol{y}_1\}) \setminus \{\boldsymbol{y}_d\}$
- $|\boldsymbol{y}_1| = |\boldsymbol{y}_2|$
- *there exists a unique bijection* $\delta : \{\boldsymbol{y}_2\} \to \{\boldsymbol{y}_1\}$ *such that* $(\boldsymbol{O}_1 \oplus \boldsymbol{O}_2, \boldsymbol{I}_1 \oplus \boldsymbol{I}_2)[\boldsymbol{y}_2 \leftarrow \delta(\boldsymbol{y}_2)] = \mathbf{0}$

then $G(t)$ is defined, and:

$$G(t) := \frac{1}{\sqrt{2}^{p'}} \sum_{\boldsymbol{y}_1,\boldsymbol{y}_d} e^{-2i\pi P[\boldsymbol{y}_1\leftarrow\mathbf{0}][\boldsymbol{y}_2\leftarrow\delta(\boldsymbol{y}_2)]}\, |\boldsymbol{O}_2[\boldsymbol{y}_1\leftarrow\mathbf{0}][\boldsymbol{y}_2\leftarrow\delta(\boldsymbol{y}_2)]\rangle!\{\boldsymbol{y}_d\}\,\langle\boldsymbol{I}_2[\boldsymbol{y}_1\leftarrow\mathbf{0}][\boldsymbol{y}_2\leftarrow\delta(\boldsymbol{y}_2)]|$$

The function G is designed to be an inverse of F for some morphisms, while at the same being impervious to some rewrite rules.

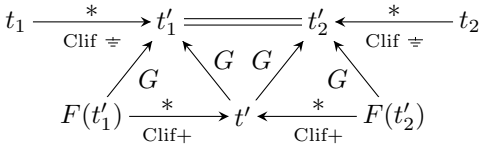
Proposition 14. *Let t be terminal with $\xrightarrow[\mathrm{Clif}\ \doteq]{}$. Then, the following diagram commutes up to α-conversion:*



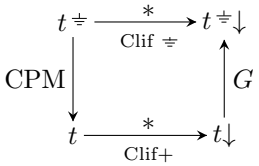
for any t' obtained by reducing $F(t)$.

Proof. In appendix at page 29.

Proof (Theorem 3). Let t_1 and t_2 be two morphisms of $\mathbf{SOP}^{\doteq}_{\mathrm{Clif}}$ such that $[\![t_1]\!] = [\![t_2]\!]$. Since $\xrightarrow[\mathrm{Clif}\ \doteq]{}$ terminates by Proposition 14, both t_1 and t_2 reduce to respectively t_1' and t_2', two terminal morphisms of $\overline{\mathbf{SOP}^{\doteq}_{\mathrm{Clif}}}$. By soundness, $[\![t_1']\!] = [\![t_2']\!]$, so, by Proposition 13, $[\![F(t_1')]\!] = [\![F(t_2')]\!]$. By completeness of $\xrightarrow[\mathrm{Clif+}]{}$, we have $F(t_1') \xrightarrow[\mathrm{Clif+}]{*} t' \xleftarrow[\mathrm{Clif+}]{*} F(t_2')$ up to α-conversion. Finally, by Proposition 14, $t_1' = G(t') = t_2'$ up to α-conversion:



Remark 3. Interestingly, the previous proposition and theorem show that the simplification of a term of $\mathbf{SOP}^{\doteq}_{\mathrm{Clif}}$ can be operated in the "pure" setting, and then G can be used to retrieve the normal form. More precisely:



Corollary 7. *The equality of morphisms in $\mathbf{SOP}^{\doteq}_{\mathrm{Clif}}/\underset{\mathrm{Clif}\ \doteq}{\sim}$ is decidable in time polynomial in the size of the phase polynomial and in the combined size of the ket/bra/discarded polynomials.*

Conclusion and Further Work

We have shown that **SOP** could represent any morphism of **Qubit**, and that it could be enriched using the discard construction to include measurements. We have shown a correspondence between this formalism and graphical languages such as the ZH-Calculus, and we have provided two rewrite strategies for simplifying terms. We have shown that these are complete in the Clifford case.

This framework can be used to simplify Z*-diagrams: one simply needs to translate the diagram as a **SOP**-morphism, simplify it, then translate the result as a diagram in the target language.

By applying the discard construction, we have extended the domain of use of **SOP** to programs that contain measurements. For instance, schemes for error detection/correction can now be studied/verified/simplified in the framework.

One of the obvious further developments of the framework is to use the completeness of (fragments of) Z*-Calculi and their interpretation to generate rewrite strategies complete for fragments larger than Clifford. On can also transport constructions that are known in the Z*-Calculi to perform non trivial operations on **SOP** morphisms.

Another important development of the framework would be to more easily represent families of processes. The recent enrichment SZX [4] could be of help for this topic.

Finally, it could be interesting to see how graph-theoretic notions like the gflow [8] translate to **SOP**. This particular notion could for instance allow to extract a quantum circuit from an arbitrary (isometry) **SOP**-morphism.

Acknowledgements

The author acknowledges support from the project PIA-GDN/Quantex. The author would like to thank Simon Perdrix, Emmanuel Jeandel and Benoît Valiron for fruitful discussions.

References

1. Matthew Amy (2019): *Towards Large-scale Functional Verification of Universal Quantum Circuits*. In Peter Selinger & Giulio Chiribella, editors: *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, *Electronic Proceedings in Theoretical Computer Science* 287, pp. 1–21, doi:10.4204/EPTCS.287.1.
2. Miriam Backens (2014): *The ZX-Calculus is Complete for Stabilizer Quantum Mechanics*. In: *New Journal of Physics*, 16, IOP Publishing, p. 093021, doi:10.1088/1367-2630/16/9/093021. Available at https://doi.org/10.1088%2F1367-2630%2F16%2F9%2F093021.
3. Miriam Backens & Aleks Kissinger (2019): *ZH: A Complete Graphical Calculus for Quantum Computations Involving Classical Non-linearity*. In Peter Selinger & Giulio Chiribella, editors: *Proceedings of the 15th International Conference on Quantum Physics and Logic, Halifax, Canada, 3-7th June 2018*, *Electronic Proceedings in Theoretical Computer Science* 287, pp. 23–42, doi:10.4204/EPTCS.287.2.
4. Titouan Carette, Dominic Horsman & Simon Perdrix (2019): *SZX-Calculus: Scalable Graphical Quantum Reasoning*. In Peter Rossmanith, Pinar Heggernes & Joost-Pieter Katoen, editors: *44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019)*, *Leibniz International Proceedings in Informatics (LIPIcs)* 138, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, pp. 55:1–55:15, doi:10.4230/LIPIcs.MFCS.2019.55. Available at http://drops.dagstuhl.de/opus/volltexte/2019/10999.
5. Titouan Carette, Emmanuel Jeandel, Simon Perdrix & Renaud Vilmart (2019): *Completeness of Graphical Languages for Mixed States Quantum Mechanics*. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini & Stefano Leonardi, editors: *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, *Leibniz International Proceedings in Informatics (LIPIcs)* 132, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, pp. 108:1–108:15, doi:10.4230/LIPIcs.ICALP.2019.108. Available at http://drops.dagstuhl.de/opus/volltexte/2019/10684.
6. Bob Coecke & Ross Duncan (2011): *Interacting Quantum Observables: Categorical Algebra and Diagrammatics*. *New Journal of Physics* 13(4), p. 043016, doi:10.1088/1367-2630/13/4/043016. Available at https://doi.org/10.1088%2F1367-2630%2F13%2F4%2F043016.
7. Bob Coecke & Aleks Kissinger (2010): *The Compositional Structure of Multipartite Quantum Entanglement*. In: *Automata, Languages and Programming*, Springer Berlin Heidelberg, pp. 297–308, doi:10.1007/978-3-642-14162-1_25. Available at https://doi.org/10.1007%2F978-3-642-14162-1_25.

8. Ross Duncan & Simon Perdrix (2010): *Rewriting Measurement-Based Quantum Computations with Generalised Flow*. *Lecture Notes in Computer Science* 6199, pp. 285–296, doi:10.1007/978-3-642-14162-1_24. Available at http://personal.strath.ac.uk/ross.duncan/papers/gflow.pdf.
9. Ross Duncan & Simon Perdrix (2014): *Pivoting makes the ZX-calculus complete for real stabilizers*. In Bob Coecke & Matty Hoban, editors: *Proceedings of the 10th International Workshop on Quantum Physics and Logic, Castelldefels (Barcelona), Spain, 17th to 19th July 2013*, *Electronic Proceedings in Theoretical Computer Science* 171, pp. 50–62, doi:10.4204/EPTCS.171.5.
10. Amar Hadzihasanovic, Kang Feng Ng & Quanlong Wang (2018): *Two Complete Axiomatisations of Pure-state Qubit Quantum Computing*. In: *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, ACM, New York, NY, USA, pp. 502–511, doi:10.1145/3209108.3209128. Available at http://doi.acm.org/10.1145/3209108.3209128.
11. Stephen Lack (2004): *Composing PROPs*. In: *Theory and Applications of Categories*, 13, pp. 147–163. Available at http://www.tac.mta.ca/tac/volumes/13/9/13-09abs.html.
12. Louis Lemonnier (2019): *Relating high-level frameworks for quantum circuits*. Master's thesis, Radbound University. Available at https://www.cs.ox.ac.uk/people/aleks.kissinger/papers/lemonnier-high-level.pdf.
13. Louis Lemonnier, John van de Wetering & Aleks Kissinger (2020): *Hypergraph simplification: Linking the path-sum approach to the ZH-calculus*. arXiv:2003.13564.
14. Saunders Mac Lane (2013): *Categories for the Working Mathematician*. 5, Springer Science & Business Media.
15. Maarten Van den Nest, Jeroen Dehaene & Bart De Moor (2004): *Graphical description of the action of local Clifford transformations on graph states*. *Phys. Rev. A* 69, p. 022316, doi:10.1103/PhysRevA.69.022316. Available at https://link.aps.org/doi/10.1103/PhysRevA.69.022316.
16. Peter Selinger (2007): *Dagger Compact Closed Categories and Completely Positive Maps*. *Electronic Notes in Theoretical Computer Science* 170, pp. 139–163, doi:10.1016/j.entcs.2006.12.018. Available at https://doi.org/10.1016%2Fj.entcs.2006.12.018.
17. Peter Selinger (2010): *A Survey of Graphical Languages for Monoidal Categories*. In: *New Structures for Physics*, Springer, pp. 289–355.
18. Renaud Vilmart (2019): *A Near-Minimal Axiomatisation of ZX-Calculus for Pure Qubit Quantum Mechanics*. In: *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pp. 1–10, doi:10.1109/LICS.2019.8785765.
19. Fabio Zanasi (2015): *Interacting Hopf Algebras – the theory of linear systems*. Ph.D. thesis, Université de Lyon. Available at http://www.zanasi.com/fabio/#/publications.html.

A Appendix

Proof (Proposition 3).

- $[\![(.)^t]\!] = [\![(\epsilon_m \otimes id_n) \circ (id_m \otimes . \otimes id_n) \circ (id_m \otimes \eta_m)]\!] = (\epsilon_m \otimes id_n) \circ (id_m \otimes [\![.]\!] \otimes id_n) \circ (id_m \otimes \eta_m)$
  $= [\![.]\!]^t$
- $[\![\overline{f}]\!] = s_f \sum_{\boldsymbol{y},\boldsymbol{x} \in \{0,1\}} e^{-2i\pi P_f} |\boldsymbol{Q}_f\rangle\langle\boldsymbol{x}| = \overline{s_f \sum_{\boldsymbol{y},\boldsymbol{x} \in \{0,1\}} e^{2i\pi P_f} |\boldsymbol{Q}_f\rangle\langle\boldsymbol{x}|} = \overline{[\![f]\!]}$
- $[\![(.)^\dagger]\!] = \left[\!\!\left[\overline{(.)}^t\right]\!\!\right] = \overline{[\![.]\!]}^t = [\![.]\!]^\dagger$

Proof (Theorem 1). As we already mentioned, **SOP** is a PROP. Quotienting it with the equivalence relation $\underset{\text{Clif}}{\sim}$ does not change this property. We already saw that all the axioms for a compact structure are satisfied. It remains to show that $(.)^\dagger$ is involutive.

First, for any morphism $f \in \mathbf{SOP}$, we have:

$$\overline{\overline{f}} = \overline{|\boldsymbol{x}\rangle \mapsto s_f \sum e^{-2i\pi P_f} |\boldsymbol{Q}_f\rangle} = |\boldsymbol{x}\rangle \mapsto s_f \sum e^{2i\pi P_f} |\boldsymbol{Q}_f\rangle = f$$

so $\overline{\overline{(.)}} = (.)$.

Moreover:

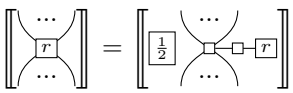
$$\overline{f}^t = |\boldsymbol{x}\rangle \mapsto \frac{s_f}{2^m} \sum e^{2i\pi\left(-P_f + \frac{\widehat{\boldsymbol{Q_f}}[\boldsymbol{x}_f \leftarrow \boldsymbol{y}] \cdot \boldsymbol{y}' + \boldsymbol{x} \cdot \boldsymbol{y}'}{2}\right)} |\boldsymbol{y}\rangle$$

$$= |\boldsymbol{x}\rangle \mapsto \frac{s_f}{2^m} \sum e^{2i\pi\left(-P_f - \frac{\widehat{\boldsymbol{Q_f}}[\boldsymbol{x}_f \leftarrow \boldsymbol{y}]\cdot \boldsymbol{y}' + \boldsymbol{x}\cdot\boldsymbol{y}'}{2}\right)} |\boldsymbol{y}\rangle = \overline{f^t}$$

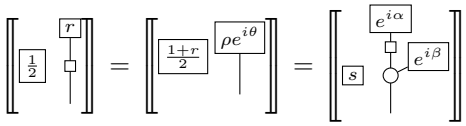
Indeed, $\widehat{\boldsymbol{Q_f}}[\boldsymbol{x}_f \leftarrow \boldsymbol{y}] \cdot \boldsymbol{y}' + \boldsymbol{x} \cdot \boldsymbol{y}'$ is integer-valued, and $e^{i\pi n} = e^{-i\pi n}$ for any $n \in \mathbb{Z}$.

Finally: $(.)^{\dagger\dagger} = \overline{\overline{(.)}^t}^t = \overline{\overline{(.)}^{tt}} = (.)$

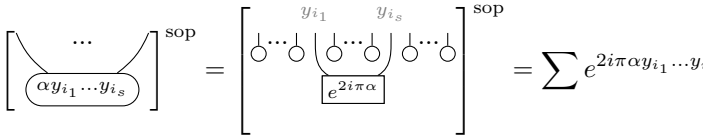
Proof (Lemma 1). First, one of the (sound) rules of the ZH-Calculus tells us that:



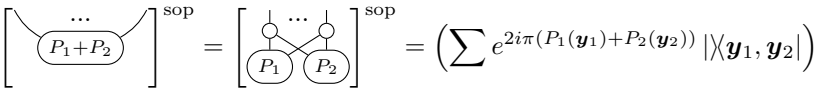
Then, let $\rho e^{i\theta} := \frac{1-r}{1+r}$ with $\rho > 0$, which is well defined and unique since $r \neq -1$ and $r \neq 1$. Let also $\alpha := 2 \arctan \frac{\rho}{2}$, $\beta := \theta + \frac{\pi}{2}$ and $s := \frac{1+r}{2(1+e^{i\alpha})}$. Then, one can check that:



Proof (Proposition 6). First, we can show inductively that $\left[\begin{smallmatrix}\cdots\\ P\end{smallmatrix}\right]^{\mathrm{sop}} \underset{\mathrm{Clif}}{\sim} \sum_{\boldsymbol{y}} e^{2i\pi P(\boldsymbol{y})} |\rangle\langle \boldsymbol{y}|$. Indeed, we have:



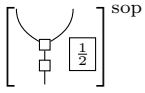
and



$$\underset{\mathrm{Clif}}{\sim} \sum e^{2i\pi(P_1(\boldsymbol{y})+P_2(\boldsymbol{y}))} |\rangle\langle \boldsymbol{y}| = \sum e^{2i\pi(P_1+P_2)(\boldsymbol{y})} |\rangle\langle \boldsymbol{y}|$$

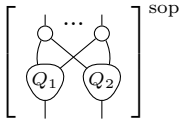
Similarly, we can prove that $\left[\begin{smallmatrix}\cdots\\ O_i\end{smallmatrix}\right]^{\mathrm{sop}} \underset{\mathrm{Clif}}{\sim} \sum_{\boldsymbol{y}} |O_i(\boldsymbol{y})\rangle\langle \boldsymbol{y}|$. The base cases are straightforward, so we show the sum and product. Notice that:

$$\left[\begin{smallmatrix}\\ \bullet\end{smallmatrix}\right]^{\mathrm{sop}} = \frac{1}{4} \sum e^{2i\pi\left(\frac{y_5 y_1}{2} + \frac{y_6 y_2}{2} + \frac{y_1 y_3}{2} + \frac{y_2 y_3}{2} + \frac{y_1 y_4}{2}\right)} |y_4\rangle\langle y_5, y_6| \xrightarrow[\mathrm{Elim}]{*} \sum |y_1 \oplus y_2\rangle\langle y_1, y_2|$$

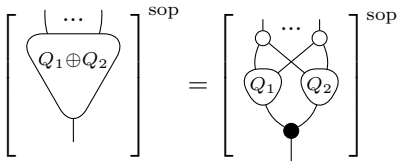


$$= \frac{1}{2} \sum e^{2i\pi\left(\frac{y_3 y_4 y_1}{2} + \frac{y_1 y_2}{2}\right)} |y_2\rangle\langle y_3, y_4| \xrightarrow[\mathrm{Elim}]{} \sum |y_1 y_2\rangle\langle y_1, y_2|$$

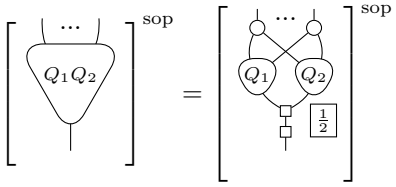
and



so we directly get:

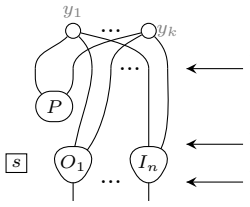


and



$\underset{\text{Clif}}{\sim} \sum |(Q_1Q_2)(\boldsymbol{y})\rangle\langle\boldsymbol{y}|$

Finally:

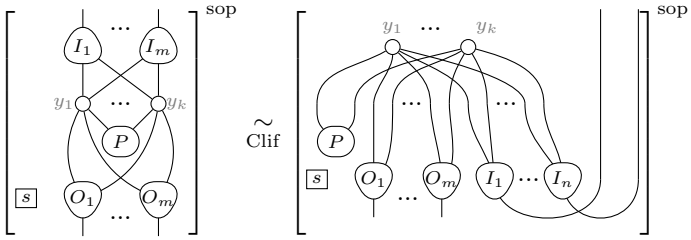


$\longleftarrow \sum |\boldsymbol{y}^{m+n+1}\rangle\langle|$

$\longleftarrow \sum e^{2i\pi P(\boldsymbol{y})} |\boldsymbol{y}^{m+n}\rangle\langle|$

$\longleftarrow \sum e^{2i\pi P(\boldsymbol{y})} |\boldsymbol{O}_1(\boldsymbol{y}), \ldots, \boldsymbol{O}_m(\boldsymbol{y}), \boldsymbol{I}_1(\boldsymbol{y}), \ldots, \boldsymbol{I}_n(\boldsymbol{y})\rangle\langle|$

Hence:



$\underset{\text{Clif}}{\sim} \sum e^{2i\pi P(\boldsymbol{y})} |\boldsymbol{O}(\boldsymbol{y})\rangle\langle\boldsymbol{I}(\boldsymbol{y})|$

Proof (Proposition 7). First, we shall show that $[\![\mathbf{ZH}_{\text{Clif}}]\!] \subseteq \mathbf{Stab}$. To do so, it suffices to show that all the generators of $\mathbf{ZH}_{\text{Clif}}$ are mapped to morphisms of **Stab**:

$$[\![\boxed{\tfrac{1}{\sqrt{2}}}]\!] = \frac{1}{\sqrt{2}} = \epsilon \circ (|0\rangle \otimes (H \circ |0\rangle)) \in \mathbf{Stab}$$

$$2 = \epsilon \circ \eta \in \mathbf{Stab}$$

$$[\![\text{—}\boxed{\ }\text{—}]\!] = H \times \frac{2}{\sqrt{2}} \in \mathbf{Stab}$$

$$[\![\boxed{1}]\!] = |0\rangle + |1\rangle = \frac{2}{\sqrt{2}} H |0\rangle \in \mathbf{Stab}$$

$$[\![\boxed{e^{ik\frac{\pi}{2}}}]\!] = |0\rangle + i^k |1\rangle = S^k(|0\rangle + |1\rangle) \in \mathbf{Stab}$$

$$[\![\cap]\!] = (id \otimes H) \circ CZ \circ (id \otimes (H \circ |0\rangle)) \in \mathbf{Stab}$$

$$[\![\curlyvee]\!] = (id \otimes \epsilon) \circ \left([\![\cap]\!] \otimes id \right) \in \mathbf{Stab}$$

$$[\![\text{—}\circ]\!] = \epsilon \circ [\![\cap]\!] \in \mathbf{Stab}$$

$$[\![\circ\text{—}]\!] = [\![\curlyvee]\!] \circ \eta \in \mathbf{Stab}$$

$$[\![\boxed{e^{i\frac{\pi}{4}}}]\!] = [\![\boxed{\tfrac{1}{\sqrt{2}}}\ \boxed{i}\ \circ]\!] \in \mathbf{Stab}$$

and $[\![\cdots]\!]$ can be obtained as a composition of $[\![\cap]\!]$, $[\![\curlyvee]\!]$, $[\![\text{—}\circ]\!]$ and $[\![\circ\text{—}]\!]$.

Then, we can show that all the generators of **Stab** have a preimage by $[\![.]\!]_{\text{Clif}}$ in $\mathbf{ZH}_{\text{Clif}}$:

$$[\![\boxed{\tfrac{1}{2}}\ \circ]\!] = |0\rangle$$

$$[\![\text{—}\boxed{\ }\ \boxed{\tfrac{1}{\sqrt{2}}}]\!] = H$$

$$\left[\!\left[\ \right]\!\right] = CZ$$

$$\left[\!\left[\ \right]\!\right] = S$$

Proof (Proposition 8). First, we show that $[\![\mathbf{SOP}_{\mathrm{Clif}}]\!] \subseteq \mathbf{Stab}$. To do so, it can be seen that $[\mathbf{SOP}_{\mathrm{Clif}}]^{\mathrm{ZH}} \subseteq \mathbf{ZH}_{\mathrm{Clif}}$: $\frac{1}{\sqrt{2^p}}$ is mapped to $\boxed{\frac{1}{\sqrt{2}}}^p$, $\frac{1}{8}P^{(0)}$ contributes for $\boxed{e^{i\frac{\pi}{4}}}^{P^{(0)}}$, $\frac{1}{4}P^{(1)}$ contributes to $\boxed{e^{i\alpha}}$ linked to the associated variable (where $\alpha \in \{0, \frac{\pi}{2}, \pi, -\frac{\pi}{2}\}$), and $\frac{1}{2}P^{(2)}$ contributes to $\sqcup$ linked to the associated pair of variables; and O_i and I_i being linear, they are mapped to black spiders (with or without $\neg$).
Hence, $[\![\mathbf{SOP}_{\mathrm{Clif}}]\!] = [\![[\mathbf{SOP}_{\mathrm{Clif}}]^{\mathrm{ZH}}]\!] \subseteq [\![\mathbf{ZH}_{\mathrm{Clif}}]\!] \subseteq \mathbf{Stab}$.

Next, it suffices to show that all the generators of **Stab** have a preimage by $[\![.]\!]$ in $\mathbf{SOP}_{\mathrm{Clif}}$:

$$\left[\!\left[\frac{1}{\sqrt{2}}\sum e^{2i\pi\frac{y_1y_2}{2}}\,|y_2\rangle\langle y_1|\right]\!\right] = H$$

$$\left[\!\left[\sum e^{2i\pi\frac{y}{4}}\,|y\rangle\langle y|\right]\!\right] = S$$

$$\left[\!\left[\sum e^{2i\pi\frac{y_1y_2}{2}}\,|y_1,y_2\rangle\langle y_1,y_2|\right]\!\right] = CZ$$

$$[\![|0\rangle\langle|]\!] = |0\rangle$$

Proof (Proposition 10). For a morphism $s\sum_{\boldsymbol{y}} e^{2i\pi P}\,|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$ of **SOP**, consider the tuple:

$$\Big(\,|\boldsymbol{y}|\,,\ \mathrm{mon}(O_1),\ \ldots,\ \mathrm{mon}(O_m),\ \mathrm{mon}(I_1),\ \ldots,\ \mathrm{mon}(I_n), \mathrm{mon}(P)\Big)$$

where:

- $|.|$ denotes the cardinality
- $\mathrm{mon}(Q)$ counts the number of monomials in the expanded simplified polynomial Q

We can define an order on these tuples, as their lexicographic order. Notice that all the components of the tuple are natural integers. Hence, if we can show that every rewrite rule in $\underset{\text{Clif+}}{\longrightarrow}$ strictly reduces the tuple, then it means $\underset{\text{Clif+}}{\longrightarrow}$ terminates.

It is easy to check that the three rules of $\underset{\text{Clif}}{\longrightarrow}$ reduce the size of $\boldsymbol{y}$, hence reducing the tuple.

When the rule (ket) is applied on O_i, we necessarily have $\mathrm{mon}(O_i) \geq 2$. Indeed, $O_i = y_0 \oplus O_i'$ where $O_i' \neq 0$. After application of the rule, this quantity is reduced to 1. Moreover, neither $|\boldsymbol{y}|$, $\mathrm{mon}(O_1)$, ..., nor $\mathrm{mon}(O_{i-1})$ is changed, as there is no creation or removal of variables, and y_0 does not appear in $O_1, \ldots, O_{i-1}$. The rule (bra) works exactly in the same fashion.

Finally, the rule (Z) reduces the morphism to one whose tuple is $(1, 0, \ldots, 0, 0, \ldots, 0, 1)$, and only from a morphism with a larger associated tuple.

Proof (Lemma 3). The rules (ket) and (bra) quite obviously enforce the form of $\boldsymbol{O}$ and $\boldsymbol{I}$. Then, suppose y_0 is an internal variable. Then either:

- the monomial $\frac{1}{4}y_0$ appears in the phase polynomial, in which case the rule (ω) can be applied
- the monomial $\frac{1}{2}y_0y_i$ appears in the phase polynomial, with some arbitrary y_i, in which case the rule (HH) can be applied
- the monomial $\frac{1}{2}y_0$ appears in the phase polynomial, as the only occurrence of y_0, in which case the rule (Z) can be applied

Proof (Proposition 11). By reductio ad absurdum, suppose that t reduces to $t' = \frac{1}{\sqrt{2^p}}\sum e^{2i\pi P}|\boldsymbol{O}\rangle\langle\boldsymbol{I}|$ different from $\sum_{y_0} e^{2i\pi\frac{y_0}{2}}\,|0,...,0\rangle\langle 0,...,0|$, but irreducible. By Lemma 3, this implies $\mathrm{Var}(P) \subseteq \mathrm{Var}(\boldsymbol{O}, \boldsymbol{I})$. We show that we can build $\boldsymbol{x}_1, \boldsymbol{x}_2 \in \{0,1\}^{n+m}$ such that $\langle \boldsymbol{x}_1|\,[\![t']\!]\,|\boldsymbol{x}_2\rangle \neq 0$.

To do so, consider O_1. By Lemma 3, either it is a constant c, or a "fresh" variable y_k. In the first case, build

$$t^{(1)} := \frac{1}{\sqrt{2^p}} \sum e^{2i\pi P} \left|O_2, ..., O_m\right\rangle\!\left\langle \boldsymbol{I}\right|,$$

in the second case, build

$$t^{(1)} := \left(\frac{1}{\sqrt{2^p}} \sum e^{2i\pi P} \left|O_2, ..., O_m\right\rangle\!\left\langle \boldsymbol{I}\right|\right)[y_k \leftarrow 0].$$

Notice that:

- $t^{(1)}$ is irreducible
- $\mathrm{Var}(P^{(1)}) \subseteq \mathrm{Var}(\boldsymbol{O}^{(1)}, \boldsymbol{I}^{(1)})$
- $[\![t^{(1)}]\!] = (\langle c| \otimes id_{m-1}) \circ [\![t']\!]$ if $O_1 = c$
- $[\![t^{(1)}]\!] = (\langle 0| \otimes id_{m-1}) \circ [\![t']\!]$ if $O_1 = y_k$

c (resp. 0) will be the first term of $\boldsymbol{x}_1$.

Doing so repeatedly (building $t^{(i+1)}$ from $t^{(i)}$) first for the whole ket, and then for the whole bra, we end up with a term $t^{(n+m)}$ of the form $t^{(n+m)} = \frac{1}{\sqrt{2^p}} \sum e^{2i\pi c}$ with c a constant. In the process, we build $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$.

Clearly, $[\![t^{(n+m)}]\!] \neq 0$, and yet, $[\![t^{(n+m)}]\!] = \langle \boldsymbol{x}_1| [\![t']\!] |\boldsymbol{x}_2\rangle$. Hence, $[\![t']\!] \neq 0$. We end up with a contradiction, so t actually reduces to $\sum_{y_0} e^{2i\pi \frac{y_0}{2}} |0, ..., 0\rangle\!\langle 0, ..., 0|$.

Proof (Lemma 4). Let us prove the result by induction on k:

- If $k = 0$, the result is obvious
- Suppose the result is true for k. Let $P_i \in \mathbb{R}[X_1, ..., X_{k+1}]/(1, X^2 - X)$. Then $P_i(\boldsymbol{x}, x_0) = P_i'(\boldsymbol{x}) + x_0 P_i''(\boldsymbol{x})$ with $P_i', P_i'' \in \mathbb{R}[X_1, ..., X_k]/(1, X^2 - X)$. By hypothesis, we have $\forall \boldsymbol{x} \in \{0,1\}^k$, $P_1(\boldsymbol{x}, 0) = P_2(\boldsymbol{x}, 0)$, so by induction hypothesis, $P_1' = P_2'$. Similarly, we get $P_1'' = P_2''$. Hence, $P_1 = P_2$.

Proof (Theorem 2). If $[\![t_1]\!] = 0 = [\![t_2]\!]$, by Proposition 11, the two terms reduce to the same normal form.

Suppose now that $[\![t_i]\!] \neq 0$, and that t_i reduce to $t_i' = \frac{1}{\sqrt{2^{p_i}}} \sum e^{2i\pi P_i} \left|\boldsymbol{O}^{(i)}\right\rangle\!\left\langle \boldsymbol{I}^{(i)}\right|$, irreducible. By Corollary 3, $\mathrm{Var}(P_i) \subseteq \mathrm{Var}(\boldsymbol{O}^{(i)}, \boldsymbol{I}^{(i)})$.

We first show that $\boldsymbol{O}^{(1)} = \boldsymbol{O}^{(2)}$ and $\boldsymbol{I}^{(1)} = \boldsymbol{I}^{(2)}$ while at the same time building the α-conversion. Consider $O_1^{(i)}$. By Lemma 3, either $O_1^{(i)} = c$ constant or $O_1^{(i)} = y_{k_i}$. We can show that $O^{(1)}$ and $O^{(2)}$ are in the form. Indeed, suppose $O_1^{(1)} = c$ and $O_1^{(2)} = y_k$. Then, $(\langle c \oplus 1| \otimes id) \circ [\![t_1']\!] = 0$, however $(\langle c \oplus 1| \otimes id) \circ [\![t_2']\!] = \left[\!\!\left[\left(\frac{1}{\sqrt{2^{p_i}}} \sum e^{2i\pi P_i} \left|O_2^{(2)}, ..., O_m^{(2)}\right\rangle\!\left\langle \boldsymbol{I}^{(i)}\right|\right)[y_k \leftarrow c \oplus 1]\right]\!\!\right] \neq 0$ by Corollary 3, since the last term is irreducible with no internal variable.

Hence, either $O_1^{(1)} = c = O_1^{(2)}$ or $O_1^{(1)} = y_{k_1}$ and $O_1^{(2)} = y_{k_2}$. In the first case, build

$$t_i^{(1)} := \frac{1}{\sqrt{2^{p_i}}} \sum e^{2i\pi P_i} \left|O_2^{(i)}, ..., O_m^{(i)}\right\rangle\!\left\langle \boldsymbol{I}^{(i)}\right|.$$

In the second case, build

$$t_i^{(1)} := \left(\frac{1}{\sqrt{2^{p_i}}} \sum e^{2i\pi P_i} \left|O_2^{(i)}, ..., O_m^{(i)}\right\rangle\!\left\langle \boldsymbol{I}^{(i)}\right|\right)[y_{k_i} \leftarrow 0],$$

and the α-conversion $y_{k_1} \leftrightarrow y_{k_2}$.

In parallel, we start building a particular operator that will be of use in the following. In the first case, the operator is built from $\mathrm{op} := \langle +|$, in the second case, from $\mathrm{op} := id$.

We may notice that:

- $t_i^{(1)}$ is irreducible
- $t_i^{(1)}$ has no internal variable

– by Corollary 3, $\left[\!\left[t_i^{(1)}\right]\!\right] \neq 0$
– $\left[\!\left[t_i^{(1)}\right]\!\right] = (\langle c| \otimes id) \circ [\![t_i']\!]$ if $O_1^{(i)} = c$
– $\left[\!\left[t_i^{(1)}\right]\!\right] = (\langle 0| \otimes id) \circ [\![t_i']\!]$ if $O_1^{(i)} = y_{k_i}$
– $(\mathrm{op} \otimes id) \circ [\![t_i']\!] = \left[\!\left[\frac{1}{\sqrt{2^{p_i}}} \sum e^{2i\pi P_i} \left|O_2^{(i)}, ..., O_m^{(i)}\right\rangle\!\left\langle \boldsymbol{I}^{(i)}\right|\right]\!\right]$ if $O_1^{(i)} = c$
– $(\mathrm{op} \otimes id) \circ [\![t_i']\!] = \left[\!\left[\frac{1}{\sqrt{2^{p_i}}} \sum e^{2i\pi P_i} \left|y_{k_i}, O_2^{(i)}, ..., O_m^{(i)}\right\rangle\!\left\langle \boldsymbol{I}^{(i)}\right|\right]\!\right]$ if $O_1^{(i)} = y_{k_i}$

Doing so inductively first for the whole ket, then for the whole bra, we get:

– a matching of variables of t_2' with variables of t_1'. We may call δ the bijection that maps a variable of t_2' to a variable of t_1'.
– the equalities $\boldsymbol{O}^{(1)} = \boldsymbol{O}^{(2)}[\boldsymbol{y}_2 \leftarrow \delta(\boldsymbol{y}_2)]$ and $\boldsymbol{I}^{(1)} = \boldsymbol{I}^{(2)}[\boldsymbol{y}_2 \leftarrow \delta(\boldsymbol{y}_2)]$
– the equality $\frac{1}{\sqrt{2^{p_1}}} e^{2i\pi P_1[\boldsymbol{y}_1 \leftarrow \boldsymbol{0}]} = \left[\!\left[t_1^{(n+m)}\right]\!\right] = \left[\!\left[t_2^{(n+m)}\right]\!\right] = \frac{1}{\sqrt{2^{p_2}}} e^{2i\pi P_2[\boldsymbol{y}_2 \leftarrow \boldsymbol{0}]}$ which implies equality for the p_i and the constants in the phase polynomials.
– two operators op_1 (for the ket) and op_2 (for the bra), such that

$$\mathrm{op}_1 \circ [\![t_i']\!] \circ \mathrm{op}_2 = \left[\!\left[\frac{1}{\sqrt{2^{p_i}}} \sum e^{2i\pi P_i} \left|y_1^{(i)}, ...\right\rangle\!\left\langle ..., y_k^{(i)}\right|\right]\!\right]$$

It remains to show that $P_1 = P_2[\boldsymbol{y}_2 \leftarrow \delta(\boldsymbol{y}_2)]$. We have:

$$\begin{aligned}\sum_{\boldsymbol{y} \in \{0,1\}^k} e^{2i\pi P_1(\boldsymbol{y})} |y_1, ...\rangle\!\langle ..., y_k| &= \left[\!\left[\sum e^{2i\pi P_1} |y_1, ...\rangle\!\langle ..., y_k|\right]\!\right] \\ &= \mathrm{op}_1 \circ [\![t_1']\!] \circ \mathrm{op}_2 = \mathrm{op}_1 \circ [\![t_2'[\boldsymbol{y}_2 \leftarrow \delta(\boldsymbol{y}_2)]]\!] \circ \mathrm{op}_2 \\ &= \left[\!\left[\sum e^{2i\pi P_2} |y_1, ...\rangle\!\langle ..., y_k|\right]\!\right] = \sum_{\boldsymbol{y} \in \{0,1\}^k} e^{2i\pi P_2(\boldsymbol{y})} |y_1, ...\rangle\!\langle ..., y_k|\end{aligned}$$

By linear independence of the family $(|y_1, ...\rangle\!\langle ..., y_k|)_{\boldsymbol{y} \in \{0,1\}^k}$, we have:

$$\forall \boldsymbol{y} \in \{0,1\}^k,\ e^{2i\pi P_1(\boldsymbol{y})} = e^{2i\pi P_2(\boldsymbol{y})}$$

Since the P_i are considered modulo 1, we have $\forall \boldsymbol{y} \in \{0,1\}^k,\ P_1(\boldsymbol{y}) = P_2(\boldsymbol{y})$. By Lemma 4, we finally get $P_1 = P_2$.

Proof (Proposition 12). For a morphism $s \sum_{\boldsymbol{y}} e^{2i\pi P} |\boldsymbol{O}\rangle ! \boldsymbol{D} \langle \boldsymbol{I}|$ of $\mathbf{SOP}^{\doteq}$, consider the tuple:

$$\left(|\boldsymbol{y}|, |\{D_i \in \boldsymbol{D} \mid \mathrm{mon}(D_i) \geq 2\}|, \sum_i \mathrm{mon}(D_i), \mathrm{mon}(O_1), \ldots, \mathrm{mon}(O_m), \mathrm{mon}(I_1), \ldots, \mathrm{mon}(I_n), \mathrm{mon}(P)\right)$$

Again, we define an order on these, as their lexicographic order. We can show that all the rules of $\underset{\text{Clif}^{\doteq}}{\longrightarrow}$ reduce the tuple:

– (Elim), (HH), (ω) and $(\mathrm{H}_{\doteq})$ all reduce $|\boldsymbol{y}|$
– (disc) reduces $|\{D_i \in \boldsymbol{D} \mid \mathrm{mon}(D_i) \geq 2\}|$
– $(\oplus_{\doteq})$ reduces $\sum_i \mathrm{mon}(D_i)$ and sometimes even $|\{D_i \in \boldsymbol{D} \mid \mathrm{mon}(D_i) \geq 2\}|$
– $(\mathrm{Cst}_{\doteq})$ reduces $\sum_i \mathrm{mon}(D_i)$
– (ket) reduces $\mathrm{mon}(O_i)$ and none of the previous quantities in the tuple
– (bra) reduces $\mathrm{mon}(I_i)$ and none of the previous quantities in the tuple
– $(\mathrm{Z}_{\doteq})$ reduces $\mathrm{mon}(P)$ and none of the previous quantities
– (Z) reduces any tuple with $|\boldsymbol{y}| \geq 1$ and $\mathrm{mon}(P) \geq 1$ to $(1, 0, \ldots, 0, 1)$

Proof (Lemma 6). The first and last conditions are verified just as in the pure case. Then, all the constants in the phase polynomial can be removed using rule $(\mathrm{Z}_{\doteq})$.

Then for the form of $\boldsymbol{D}$, let us decompose it as $\boldsymbol{D} = \{y_1, \ldots, y_k\} \cup \{D_{i_1}, \ldots, D_{i_s}\}$ where all the polynomials in the right hand side have $\mathrm{mon}(.) \geq 2$ (if 0 or 1 appears as a polynomial in $\boldsymbol{D}$, it is removed using $(\mathrm{Cst}_{\doteq})$). Consider D_{i_1}. Either

– D_{i_1} contains at least one variable $y_{k+1} \notin \{y_1, \dots, y_k\}$, in which case (disc) can be used so $\boldsymbol{D}' = \{y_1, \dots, y_{k+1}\} \cup \{D_{i_2}, \dots, D_{i_s}\}[y_{k+1} \leftarrow D_{i_1}]$
– or D_{i_1} contains only variables of $\{y_1, \dots, y_k\}$, in which case, using $(\oplus_{\div})$ repeatedly, it can be reduced to a constant that can then be removed using $(\mathrm{Cst}_{\div})$, so $\boldsymbol{D}' = \{y_1, \dots, y_k\} \cup \{D_{i_2}, \dots, D_{i_s}\}$

Hence, in any case, $\boldsymbol{D}$ can be reduced to the form $\boldsymbol{D} = \{y_1, \dots, y_k\}$.

We then have to show that P can be reduced to the form above. Suppose y_0 appears both in $!\{\boldsymbol{y}_d\}$ and in $P^{(1)}$, then $(\mathrm{Z}_{\div})$ can be used to remove it from P. The same goes for monomials of the form $y_0 y_0'$ in $P^{(2)}$ when $\{y_0, y_0'\} \subseteq \{\boldsymbol{y}_d\}$.

Finally, if a variable of $\boldsymbol{y}_d$ appears only in $!\{\boldsymbol{y}_d\}$ and in P, then the rule $(\mathrm{H}_{\div})$ can be applied to remove the variable.

Proof (Lemma 7). The proof is similar to that of Proposition 11, except now we have a set of discarded variables $\{\boldsymbol{y}_d\}$. However, since $\{\boldsymbol{y}_d\} \subseteq \mathrm{Var}(\boldsymbol{O}, \boldsymbol{I})$, the set of discarded variables will deplete as the $t^{(i)}$ are built. The conclusion remains unchanged.

Proof (Proposition 14). First, let us prove that, if $t \in \overline{\mathbf{SOP}^{\div}}$ is terminal, $G(F(t))$ is defined and $G(F(t)) = t$. By definition:

$$t = \frac{1}{\sqrt{2}^p} \sum_{\boldsymbol{y}, \boldsymbol{y}_d} e^{2i\pi P(\boldsymbol{y}, \boldsymbol{y}_d)} \, |\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d)\rangle !\{\boldsymbol{y}_d\} \, \langle \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d)|$$

where P has no constant, all its monomials contain a variable of $\boldsymbol{y}$, $\{\boldsymbol{y}\} \subseteq \mathrm{Var}(\boldsymbol{O}, \boldsymbol{I})$ and $\{\boldsymbol{y}_d\} \subseteq \mathrm{Var}(\boldsymbol{O}, \boldsymbol{I}, P)$. Hence, again by definition:

$$F(t) := \frac{1}{\sqrt{2}^{2p}} \sum_{\boldsymbol{y}, \boldsymbol{y}', \boldsymbol{y}_d} e^{2i\pi \left(P(\boldsymbol{y}, \boldsymbol{y}_d) - P(\boldsymbol{y}', \boldsymbol{y}_d)\right)} \, |\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d), \boldsymbol{O}(\boldsymbol{y}', \boldsymbol{y}_d)\rangle\langle \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}', \boldsymbol{y}_d)|$$

Notice that:

– obviously $|\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d)| = |\boldsymbol{O}(\boldsymbol{y}', \boldsymbol{y}_d)|$ and $|\boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d)| = |\boldsymbol{I}(\boldsymbol{y}', \boldsymbol{y}_d)|$
– $\{\boldsymbol{y}_d\} = \{\boldsymbol{y}, \boldsymbol{y}', \boldsymbol{y}_d\} \setminus \mathrm{Var}(\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{O}(\boldsymbol{y}', \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{I}(\boldsymbol{y}', \boldsymbol{y}_d))$.
Indeed, if $O_i(\boldsymbol{y}, \boldsymbol{y}_d) = y_{i_1} \oplus \ldots \oplus y_{i_k} \oplus y_{d_{j_1}} \oplus \ldots \oplus y_{d_{j_\ell}}$, then $O_i(\boldsymbol{y}, \boldsymbol{y}_d) \oplus O_i(\boldsymbol{y}', \boldsymbol{y}_d) = y_{i_1} \oplus \ldots \oplus y_{i_k} \oplus y'_{i_1} \oplus \ldots \oplus y'_{i_k}$, so $\{\boldsymbol{y}_d\} \cap \mathrm{Var}(\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{O}(\boldsymbol{y}', \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{I}(\boldsymbol{y}', \boldsymbol{y}_d)) = \varnothing$. Moreover, all the variables of $\boldsymbol{y}$ and $\boldsymbol{y}'$ appear somewhere in $\mathrm{Var}(\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{O}(\boldsymbol{y}', \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{I}(\boldsymbol{y}', \boldsymbol{y}_d))$, since $\{\boldsymbol{y}\} \subseteq \mathrm{Var}(\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d))$.
– $\{\boldsymbol{y}\} := \mathrm{Var}(\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d)) \setminus \{\boldsymbol{y}_d\}$ for roughly the same reasons
– $\{\boldsymbol{y}'\} := (\{\boldsymbol{y}, \boldsymbol{y}', \boldsymbol{y}_d\} \setminus \{\boldsymbol{y}\}) \setminus \{\boldsymbol{y}_d\}$
– by construction of F, $|\boldsymbol{y}| = |\boldsymbol{y}'|$
– whenever $\boldsymbol{O}_i(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{O}_i(\boldsymbol{y}', \boldsymbol{y}_d) = y_{i_1} \oplus y'_{i_2}$ we define $\delta(y'_{i_2}) := y_{i_1}$. We need to show that it completely and uniquely defines δ as a bijection. Consider the variable y_i. Let K_i be the first (from left to right) polynomial of $(\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d))$ where y_i appears. Then $K_i(\boldsymbol{y}, \boldsymbol{y}_d) = y_i$, otherwise, either (ket) or (bra) could be applied on t, which means t is not terminal. Hence $K_i(\boldsymbol{y}, \boldsymbol{y}_d) \oplus K_i(\boldsymbol{y}', \boldsymbol{y}_d) = y_i \oplus y'_i$, so $\delta(y'_i) = y_i$, and y'_i is the only possible preimage of y_i by δ. Notice that $\delta(\boldsymbol{y}') = \boldsymbol{y}$ with no permutation on the indexes, so we obviously get $(\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{O}(\boldsymbol{y}', \boldsymbol{y}_d), \boldsymbol{I}(\boldsymbol{y}, \boldsymbol{y}_d) \oplus \boldsymbol{I}(\boldsymbol{y}', \boldsymbol{y}_d))[\boldsymbol{y}' \leftarrow \delta(\boldsymbol{y}')] = \boldsymbol{0}$.

Hence, $G(F(t))$ is well defined, and:

$$\begin{aligned} G(F(t)) &= \frac{1}{\sqrt{2}^p} \sum_{\boldsymbol{y}, \boldsymbol{y}_d} e^{-2i\pi \left(P(\boldsymbol{y}, \boldsymbol{y}_d) - P(\boldsymbol{y}', \boldsymbol{y}_d)\right)[\boldsymbol{y} \leftarrow \boldsymbol{0}][\boldsymbol{y}' \leftarrow \boldsymbol{y}]} \left(|\boldsymbol{O}(\boldsymbol{y}', \boldsymbol{y}_d)\rangle !\{\boldsymbol{y}_d\} \, \langle I(\boldsymbol{y}', \boldsymbol{y}_d)|\right)[\boldsymbol{y} \leftarrow \boldsymbol{0}][\boldsymbol{y}' \leftarrow \boldsymbol{y}] \\ &= \frac{1}{\sqrt{2}^p} \sum_{\boldsymbol{y}, \boldsymbol{y}_d} e^{-2i\pi (0 - P(\boldsymbol{y}, \boldsymbol{y}_d))} \, |\boldsymbol{O}(\boldsymbol{y}, \boldsymbol{y}_d)\rangle !\{\boldsymbol{y}_d\} \, \langle I(\boldsymbol{y}, \boldsymbol{y}_d)| = t \end{aligned}$$

We now need to show that for all the terms t' that are reduced from $F(t)$, $G(t')$ is defined, and $G(t') = G(F(t)) = t$. To do so, we show by induction that along any reduction path from $F(t)$, some properties are preserved.

Let $t' = \frac{1}{\sqrt{2}^{p'}} \sum_{\boldsymbol{y}^{(t')}} e^{2i\pi P} \, |\boldsymbol{O}_1, \boldsymbol{O}_2\rangle\langle \boldsymbol{I}_1, \boldsymbol{I}_2|$ such that $F(t) \xrightarrow[\text{Clif+}]{*} t'$. We claim that:

- $p' = 2p$
- $\boldsymbol{y}^{(t')} = \boldsymbol{y}, \boldsymbol{y}', \boldsymbol{y}_d$, i.e. no variable is removed, and the partitioning by G does not change
- $\mathrm{Var}(\boldsymbol{O}_1, \boldsymbol{O}_2, \boldsymbol{I}_1, \boldsymbol{I}_2) = \{\boldsymbol{y}, \boldsymbol{y}', \boldsymbol{y}_d\}$, i.e. no variable becomes internal
- $\forall k,\ \left|\mathrm{Var}(O_i^{(k)}) \cap \{\boldsymbol{y}_d\}\right| \leq 1$ and $\begin{cases} \mathrm{Var}(O_1^{(k)}) \setminus \{\boldsymbol{y}_d\} \subseteq \mathrm{Var}(O_1^{(1)}, ..., O_1^{(k-1)}) \\ \mathrm{Var}(O_2^{(k)}) \subseteq \mathrm{Var}(\boldsymbol{O}_1, O_2^{(1)}, ..., O_2^{(k-1)}) \\ \text{or} \\ O_i^{(k)} = y_{k'} \end{cases}$
- $\forall k,\ \left|\mathrm{Var}(I_i^{(k)}) \cap \{\boldsymbol{y}_d\}\right| \leq 1$ and $\begin{cases} \mathrm{Var}(I_1^{(k)}) \setminus \{\boldsymbol{y}_d\} \subseteq \mathrm{Var}(\boldsymbol{O}_1, \boldsymbol{O}_2, I_1^{(1)}, ..., I_1^{(k-1)}) \\ \mathrm{Var}(I_2^{(k)}) \subseteq \mathrm{Var}(\boldsymbol{O}_1, \boldsymbol{O}_2, \boldsymbol{I}_1, I_2^{(1)}, ..., I_2^{(k-1)}) \\ \text{or} \\ I_i^{(k)} = y_{k'} \end{cases}$
- $G(t')$ is well defined and $G(t') = t$

It is the case for $F(t)$. Indeed, t is terminal with $\underset{\text{Clif} \div}{\longrightarrow}$, so since the rule (ket) cannot be applied to t, it in particular implies the above properties on $F(t)$.

Let us consider one such t'. Notice that since there are no internal variables, none of the rules (Elim), (HH), (ω) or (Z) can be applied. Suppose $t' \underset{\text{Clif+}}{\longrightarrow} t''$ in one step. Only (ket) or (bra) can be applied from t' to t'', and only on either $\boldsymbol{O}_1$ or $\boldsymbol{I}_1$. Without loss of generality, suppose (ket) is applied on, in the polynomial $O_1^{(k)}$ of t'. Notice that $O_1^{(k)}$ is necessarily of the form $O_1^{(k)} = y_{d_k} \oplus O'$ where $y_{d_k} \in \{\boldsymbol{y}_d\} \setminus \mathrm{Var}(O_1^{(1)}, ..., O_1^{(k-1)})$ and $\mathrm{Var}(O') \subseteq \mathrm{Var}(O_1^{(1)}, ..., O_1^{(k-1)})$, otherwise the rule cannot be applied.

By application of the rule, $t'' = t'[y_{d_k} \leftarrow y_{d_k} \oplus O']$. Since $y_{d_k} \notin \mathrm{Var}(O_1^{(1)}, ..., O_1^{(k-1)})$, the first $k-1$ polynomials in the ket are left unchanged, so the variables $\mathrm{Var}(O_1^{(1)}, ..., O_1^{(k-1)})$ are still in the ket. In particular, the variables $\mathrm{Var}(O') \subseteq \mathrm{Var}(O_1^{(1)}, ..., O_1^{(k-1)})$ are also still present in the ket. The substitution cannot remove other variables from the ket, so $\mathrm{Var}\left(\boldsymbol{O}_i[y_{d_k} \leftarrow y_{d_k} \oplus O'], \boldsymbol{I}_i[y_{d_k} \leftarrow y_{d_k} \oplus O']\right) = \{\boldsymbol{y}, \boldsymbol{y}', \boldsymbol{y}_d\}$. The overall scalar is obviously unchanged. It is fairly easy to check the property of the ket for t''. Finally, we can show that the partitioning of variables by G is unchanged.

We assume that $G(t')$ is well defined. $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ are hence of the same size. $\{\boldsymbol{y}_d\}$ is defined for t' as $\{\boldsymbol{y}_d\} = \{\boldsymbol{y}^{(t')}\} \setminus \mathrm{Var}(\boldsymbol{O}_1 \oplus \boldsymbol{O}_2)$. Notice that $y_{d_k} \in \{\boldsymbol{y}_d\}$ so $y_{d_k} \notin \mathrm{Var}(\boldsymbol{O}_1 \oplus \boldsymbol{O}_2)$. Hence, if it appears somewhere in $\boldsymbol{O}_1$, say in $O_1^{(j)}$, it also appears in $O_2^{(j)}$ so that $y_{d_k} \notin \mathrm{Var}(O_1^{(j)} \oplus O_2^{(j)})$. So, the substitution will not change:

$$\{\boldsymbol{y}_d\} = \{\boldsymbol{y}^{(t')}\} \setminus \mathrm{Var}(\boldsymbol{O}_1 \oplus \boldsymbol{O}_2) = \{\boldsymbol{y}^{(t')}\} \setminus \mathrm{Var}(\boldsymbol{O}_1[y_{d_k} \leftarrow y_{d_k} \oplus O'] \oplus \boldsymbol{O}_2[y_{d_k} \leftarrow y_{d_k} \oplus O'])$$

Similarly, $\{\boldsymbol{y}_1\}$ and $\{\boldsymbol{y}_2\}$ are left unchanged, as well as the bijection δ.
Since $\mathrm{Var}(O') \subseteq \mathrm{Var}(O_1^{(1)}, ..., O_1^{(k-1)}) \subseteq \{\boldsymbol{y}_1\}$, the substitution $[y_{d_k} \leftarrow y_{d_k} \oplus O'][\boldsymbol{y}_1 \leftarrow \boldsymbol{0}][\boldsymbol{y}_2 \leftarrow \delta(\boldsymbol{y}_2)]$ is the same as the substitution $[\boldsymbol{y}_1 \leftarrow \boldsymbol{0}][\boldsymbol{y}_2 \leftarrow \delta(\boldsymbol{y}_2)]$. Hence, $G(t'') = G(t') = t$.

The whole reasoning is similar when the rule (bra) is applied instead of (ket). This concludes the proof.