



A Near-Minimal Axiomatisation of ZX-Calculus for Pure Qubit Quantum Mechanics

Renaud Vilmart

► To cite this version:

Renaud Vilmart. A Near-Minimal Axiomatisation of ZX-Calculus for Pure Qubit Quantum Mechanics. LICS 2019 - 34th Annual ACM/IEEE Symposium on Logic in Computer Science, Jun 2019, Vancouver, Canada. 10.1109/LICS.2019.8785765 . hal-01963426

HAL Id: hal-01963426

<https://hal.archives-ouvertes.fr/hal-01963426>

Submitted on 21 Dec 2018

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

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

A Near-Optimal Axiomatisation of ZX-Calculus for Pure Qubit Quantum Mechanics

Renaud Vilmart
 renaud.vilmart@loria.fr

Université de Lorraine, CNRS, Inria, LORIA, F 54000 Nancy, France

Abstract. Recent developments in the ZX-Calculus have resulted in complete axiomatisations first for an approximately universal restriction of the language, and then for the whole language. The main drawbacks were that the axioms that were added to achieve completeness were numerous, tedious to manipulate and lacked a physical interpretation. We present in this paper two complete axiomatisations for the general ZX-Calculus, that we believe are optimal, in that all their equations are necessary and moreover have a nice physical interpretation.

1 Introduction

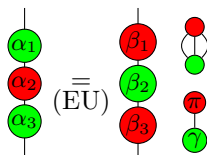
The ZX-Calculus is a powerful graphical language for quantum computing and reasoning [7]. The objects manipulated are open graphs, also called diagrams, that represent quantum evolutions through the standard interpretation. One of the most important features of the language is that the graphs can be considered unoriented, that is, any two isomorphic graphs will yield the same result. Isomorphism between diagrams are not the only transformations that preserve the interpretation though, so the ZX-Calculus comes equipped with a set of axioms: transformations between diagrams that, when applied locally, preserve the interpretation.

The language is universal: any $2^n \times 2^m$ matrix can be represented by a ZX-diagram with respect to the standard interpretation. Hence, it has already been used in numerous applications [8], ranging from measurement-based quantum computing [11,16,22] and quantum codes [5,6,13,14], to protocols [20] and foundations [4,12]. The language itself can be manipulated through tools such as Quantomatic [26] or PYZX [27].

A broader use of the ZX-Calculus was limited though, because of a question that remained open for a while: completeness. The language would be complete if, for any two diagrams that represent the same quantum evolution, they could be transformed into one another by mere application of the axioms. The question has been answered for gradually more expressive restrictions of the language. In 2014, complete axiomatisations were provided for the stabiliser [2] and the real stabiliser [17], then for the one-qubit Clifford+T case [3]. However, none of these restrictions are approximately universal. The first complete axiomatisation for an approximately universal restriction – the many-qubit Clifford+T – was recently provided [23], and soon followed two complete axiomatisations for the general – universal – ZX-Calculus [19,24].

Up to the one-qubit Clifford+T case, all the axioms provided were natural and had a relevant interpretation, however, the axiomatisations for (approximately) universal ZX-Calculus introduced rules that are hard to manipulate, mainly because of their size, and that moreover can not be naturally justified.

We give in this paper a simpler axiomatisation of the general ZX-Calculus, and prove that it is complete for the general ZX-Calculus. It is basically composed of the axioms that make the Clifford – or stabiliser – fragment complete, and of an additional axiom, denoted (EU):



with a side condition that links the angles on the right to those on the left. In ZX-Calculus, the green node with angle α represents a rotation of angle α around the Z axis (denoted $R_Z(\alpha)$),

and the red one a rotation around the orthogonal axis, X (denoted $R_X(\alpha)$). This axiom, which is an application of the Euler angles, essentially gives a normal form for one-qubit unitaries, as a sequences of rotations around the axes X, Z and X again. This equality between diagrams has been used in [30] to prove that the then version of ZX-Calculus was not complete, and is part of the axiomatisation of [10].

To prove that the new axiomatisation is complete, we simply derive the rules of the former axiomatisation [23]. However, since all the power of “beyond-Clifford” is contained in the rule (EU), we will end up using it a lot, which would cause a lot of side computation, for the angles on one side of the rule are not defined from the others in a linear fashion. So to avoid having to go through all this tedious process, we use another kind of normal form for ZX-diagrams, which is the graphical version of the singular-value decomposition of a matrix. Hence, instead of showing that a sound equation is derivable, we will show that we can transform the diagrams on both sides into a particular form, which is essentially unique.

We also provide a second axiomatisation, which is not very far from the other. Indeed, in the first, we may notice a rule (HD) that we call *the Euler decomposition of Hadamard*, which essentially gives the unitary normal form of the Hadamard gate. The second axiomatisation replaces the rules (HD) and (EU) by another single rule that unifies them.

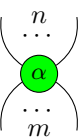
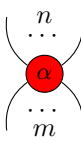






In Section 2, we formally introduce the language ZX-Calculus, as well as the two aforementioned axiomatisations, and we discuss their minimality. In Section 3, we recover a known complete axiomatisation for the Clifford fragment, hence directly giving us access to already proven lemmas from it. In Section 4, we introduce the singular-value decompositions of cycle-free $0 \rightarrow 1$ and $1 \rightarrow 1$ ZX-diagrams, and show they are essentially unique. Finally, in Section 5, we use these decompositions to show the completeness of the axiomatisations for the Clifford+T and for the unrestricted ZX-Calculus.

2 ZX-Calculus

In this section, we introduce the ZX-diagrams together with a new simple axiomatisation that we prove complete in the following sections. The definition of the ZX-diagrams and their interpretation is standard.

2.1 Diagrams and standard interpretation

A ZX-diagram $D : k \rightarrow l$ with k inputs and l outputs is generated by:

$R_Z^{(n,m)}(\alpha) : n \rightarrow m$		$R_X^{(n,m)}(\alpha) : n \rightarrow m$	
$H : 1 \rightarrow 1$		$e : 0 \rightarrow 0$	
$I : 1 \rightarrow 1$		$\sigma : 2 \rightarrow 2$	
$\epsilon : 2 \rightarrow 0$		$\eta : 0 \rightarrow 2$	

where $n, m \in \mathbb{N}$, $\alpha \in \mathbb{R}$, and the generator e is the empty diagram.

and the two compositions:

- Spacial Composition: for any $D_1 : a \rightarrow b$ and $D_2 : c \rightarrow d$, $D_1 \otimes D_2 : a + c \rightarrow b + d$ consists in placing D_1 and D_2 side by side, D_2 on the right of D_1 .
- Sequential Composition: for any $D_1 : a \rightarrow b$ and $D_2 : b \rightarrow c$, $D_2 \circ D_1 : a \rightarrow c$ consists in placing D_1 on the top of D_2 , connecting the outputs of D_1 to the inputs of D_2 .

The standard interpretation of the ZX-diagrams associates to any diagram $D : n \rightarrow m$ a linear map $\llbracket D \rrbracket : \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^m}$ inductively defined as follows:

$$\begin{aligned} \llbracket D_1 \otimes D_2 \rrbracket &:= \llbracket D_1 \rrbracket \otimes \llbracket D_2 \rrbracket & \llbracket D_2 \circ D_1 \rrbracket &:= \llbracket D_2 \rrbracket \circ \llbracket D_1 \rrbracket & \llbracket \text{---} \rrbracket &:= (1) & \llbracket \text{---} \rrbracket &:= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \llbracket \text{---} \rrbracket &:= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & \llbracket \text{---} \rrbracket &:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} & \llbracket \text{---} \rrbracket &:= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} & \llbracket \text{---} \rrbracket &:= (1 \ 0 \ 0 \ 1) \\ \llbracket \text{---} \rrbracket &:= (1 + e^{i\alpha}) & \llbracket \text{---} \rrbracket &:= 2^m \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & e^{i\alpha} \end{pmatrix} \quad (n + m > 0) \end{aligned}$$

For any $n, m \geq 0$ and $\alpha \in \mathbb{R}$:

$$\llbracket \text{---} \rrbracket = \llbracket \text{---} \rrbracket^{\otimes m} \circ \llbracket \text{---} \rrbracket \circ \llbracket \text{---} \rrbracket^{\otimes n}$$

(where $M^{\otimes 0} = (1)$ and $M^{\otimes k} = M \otimes M^{\otimes k-1}$ for any $k \in \mathbb{N}^*$).

To simplify, the red and green nodes will be represented empty when holding a 0 angle:

$$\begin{pmatrix} \dots \\ \bullet \\ \dots \end{pmatrix} := \begin{pmatrix} \dots \\ \emptyset \\ \dots \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \dots \\ \bullet \\ \dots \end{pmatrix} := \begin{pmatrix} \dots \\ \emptyset \\ \dots \end{pmatrix}$$

ZX-Diagrams are universal:

$$\forall A \in \mathbb{C}^{2^n} \times \mathbb{C}^{2^m}, \exists D : n \rightarrow m, \llbracket D \rrbracket = A$$

However, it is customary to restrict the language to a countable or finite set of angles. Some of these restrictions, or fragments, correspond to well-known restrictions of quantum computing: The $\frac{\pi}{2}$ -fragment – the restriction where all the angles are multiples of $\frac{\pi}{2}$ – corresponds to Clifford; while the $\frac{\pi}{4}$ -fragment corresponds to Clifford+T. In the following, we may refer to the $\frac{\pi}{2}$ -fragment using the term Clifford, and similarly for the $\frac{\pi}{4}$ -fragment.

2.2 Calculus

The diagrammatic representation of a matrix is not unique in the ZX-Calculus. As a consequence the language comes with a set of axioms. Additionally to the axioms of the language described in Figure 1, one can:

- bend any wire of a ZX-diagram at will, without changing its semantics. This paradigm – the so-called **Only Connectivity Matters** – can be derived from the following axioms:

$$\begin{aligned} \text{---} &= \text{---} = \text{---} & \text{---} &= \text{---} & \text{---} &= \text{---} & \text{---} &= \text{---} \\ \text{---} &= \text{---} & \text{---} &= \text{---} & \text{---} &= \text{---} & \text{---} &= \text{---} \end{aligned}$$

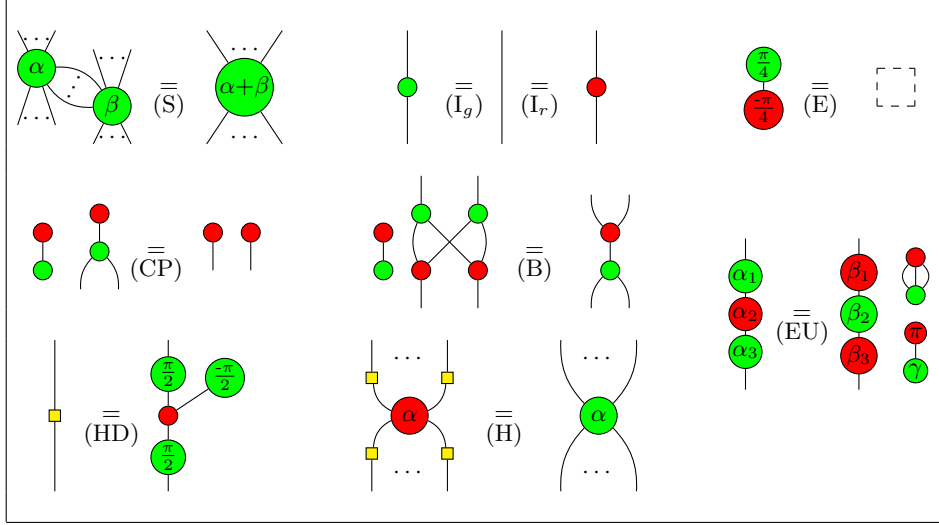


Fig. 1. Set of rules ZX for the ZX-Calculus with scalars. The right-hand side of (E) is an empty diagram. (...) denote zero or more wires, while (..) denote one or more wires. In rule (EU), $\beta_1, \beta_2, \beta_3$ and γ can be determined as follows: $x^+ := \frac{\alpha_1 + \alpha_3}{2}$, $x^- := x^+ - \alpha_3$, $z := \cos\left(\frac{\alpha_2}{2}\right) \cos(x^+) + i \sin\left(\frac{\alpha_2}{2}\right) \cos(x^-)$ and $z' := \cos\left(\frac{\alpha_2}{2}\right) \sin(x^+) - i \sin\left(\frac{\alpha_2}{2}\right) \sin(x^-)$, then $\beta_1 = \arg z + \arg z'$, $\beta_2 = 2 \arg\left(i + \left|\frac{z}{z'}\right|\right)$, $\beta_3 = \arg z - \arg z'$, $\gamma = x^+ - \arg(z) + \frac{\alpha_2 - \beta_2}{2}$ where by convention $\arg(0) := 0$ and $z' = 0 \implies \beta_2 = 0$.

– apply the axioms to sub-diagrams. If $ZX \vdash D_1 = D_2$ then, for any diagram D with the appropriate number of inputs and outputs:

- $ZX \vdash D_1 \circ D = D_2 \circ D$
- $ZX \vdash D \circ D_1 = D \circ D_2$
- $ZX \vdash D_1 \otimes D = D_2 \otimes D$
- $ZX \vdash D \otimes D_1 = D \otimes D_2$

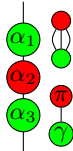
where $ZX \vdash D_1 = D_2$ means that D_1 can be transformed into D_2 using the axioms of the ZX-Calculus.

All the axioms of Figure 1, but (EU), are standard in the ZX-calculus. Roughly speaking: (S) and (I) correspond to the axiomatisation of orthonormal basis [9], each color being associated with an orthonormal basis; (CP) and (B) capture the fact that the two bases are strongly complementary [7]; (H) means that Hadamard can be used to exchange the colours and (HD) means that Hadamard can be decomposed using $\frac{\pi}{2}$ -rotations [15]; (E) states that some particular scalars (ZX-diagram with no input/output) can vanish, which means that their interpretation is one [25]. In the following we investigate the properties of (EU).

2.3 The Euler Angles

The rule (EU) is really all about unitaries. Indeed, we have the following result:

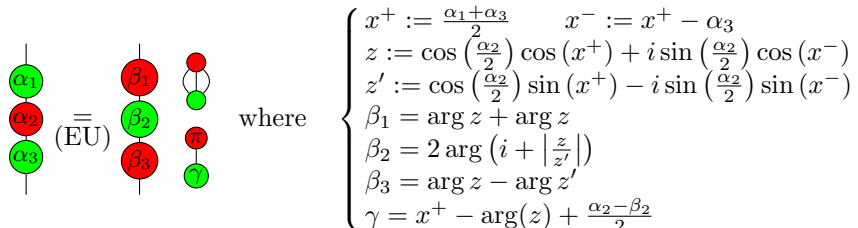
Proposition 1. *Any one-qubit unitary can be decomposed as $e^{i\gamma} R_Z(\alpha_3) R_X(\alpha_2) R_Z(\alpha_1)$, which can be represented in ZX as:*



If the unitary is not diagonal or anti-diagonal (i.e. if $\alpha_2 \neq 0 \pmod{\pi}$), then this decomposition can be made unique if we impose $\alpha_1 \in [0, \pi)$

In 1775, Euler proved what is now called Euler's rotation theorem [18], stating that there are several ways to decompose a rotation into several rotations around elementary axes. In quantum

mechanics, a consequence is that any unitary operator on one qubit can be seen as either a composition of rotations around Z, X, Z; or around X, Z, X. On the one hand, the rule (HD) says – in a distorted, ZX-style way – that the Hadamard gate can be decomposed as a series of rotations, while on the other hand, the rule (EU) gives the equality between two different decompositions of the same unitary:



$$\left\{ \begin{array}{l} x^+ := \frac{\alpha_1 + \alpha_3}{2} \quad x^- := x^+ - \alpha_3 \\ z := \cos\left(\frac{\alpha_2}{2}\right) \cos(x^+) + i \sin\left(\frac{\alpha_2}{2}\right) \cos(x^-) \\ z' := \cos\left(\frac{\alpha_2}{2}\right) \sin(x^+) - i \sin\left(\frac{\alpha_2}{2}\right) \sin(x^-) \\ \beta_1 = \arg z + \arg z \\ \beta_2 = 2 \arg\left(i + \left|\frac{z}{z'}\right|\right) \\ \beta_3 = \arg z - \arg z' \\ \gamma = x^+ - \arg(z) + \frac{\alpha_2 - \beta_2}{2} \end{array} \right.$$

The angles β_i and γ seem to not always be defined. Indeed, \arg is not defined in 0, and β_2 is not defined when $z' = 0$. By convention, we decide that $\arg(0) = 0$ and that $\beta_2 = 0$ when $z' = 0$.

The first proof of incompleteness [30] relied on an euler decomposition, but adding it to the set of ZX axioms has been avoided for a while because of its non-linearity. However, a non-linear axiom is necessary to get the completeness for the general ZX-Calculus [24]. And so, it has been used in [10] to prove the completeness of the 2-qubit $\frac{\pi}{4}$ -fragment of the ZX-Calculus. The rule (EU) is actually much more powerful than this, for, as we will prove in the following:

Theorem 1. *The ZX-Calculus – with axioms in Figure 1 – is complete for pure qubit quantum mechanics. For any two diagrams D_1 and D_2 of the ZX-Calculus:*

$$\llbracket D_1 \rrbracket = \llbracket D_2 \rrbracket \iff \text{ZX} \vdash D_1 = D_2$$

2.4 On Minimality

We call an axiomatisation minimal when there is no redundancy in the axioms. Particularly, we want a proof that none of the axioms are derivable from the others. We conjecture that all the axioms in Figure 1 are necessary. Indeed, in [1], nearly all the rules for Clifford – i.e. all of the axioms in Figure 1 except (E) and (EU)– are proven to be necessary, and all arguments stand here:

- (S): It is the only axiom that can transform a node of degree four or higher into a diagram containing lower-degree nodes
- (I_g) or (I_r): These are the only two axioms that can transform a diagram with nodes connected to a boundary to a node-free diagram
- (CP): It is the only axiom that can transform a diagram with two connected outputs into one with two disconnected outputs
- (HD): The necessity of this axiom requires a non-trivial interpretation given in [15,17], and given again in the Appendix at page 15.
- (H): It is the only axiom that matches red nodes with 4+ degree to green nodes of the same degree

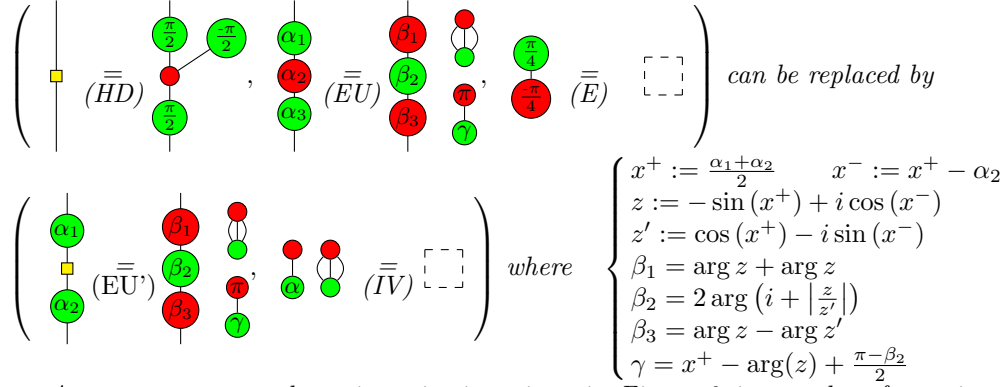
However, (E) and (EU) can also be proven to be necessary:

- (E): It is the only axiom that can transform a non-empty diagram into an empty one
- (EU): It is the only non-linear axiom

In a nutshell, all the axioms are proven to be necessary, except (B) and one of the (I).

Another aspect of minimality, is whether a rule can be made “simpler” thanks to the others, according to some measure, be it arbitrary or well-defined. In the previous axiomatisation, we have two rules that are closely related to how unitaries can be decomposed: (HD) and (EU). It so happens that we can fuse them into one, of the same size as (EU), and doing so allows us to simplify the scalar rule:

Theorem 2.



As a consequence, the axiomatisation given in Figure 2 is complete for universal quantum mechanics.

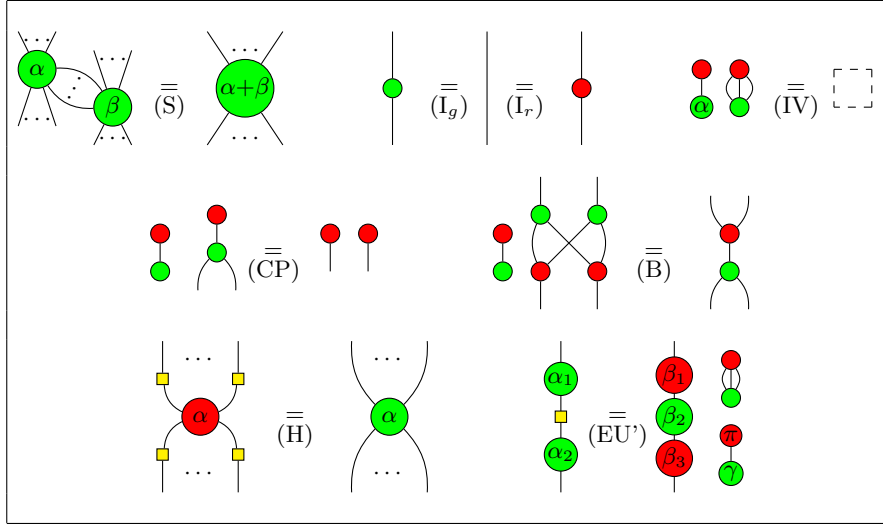
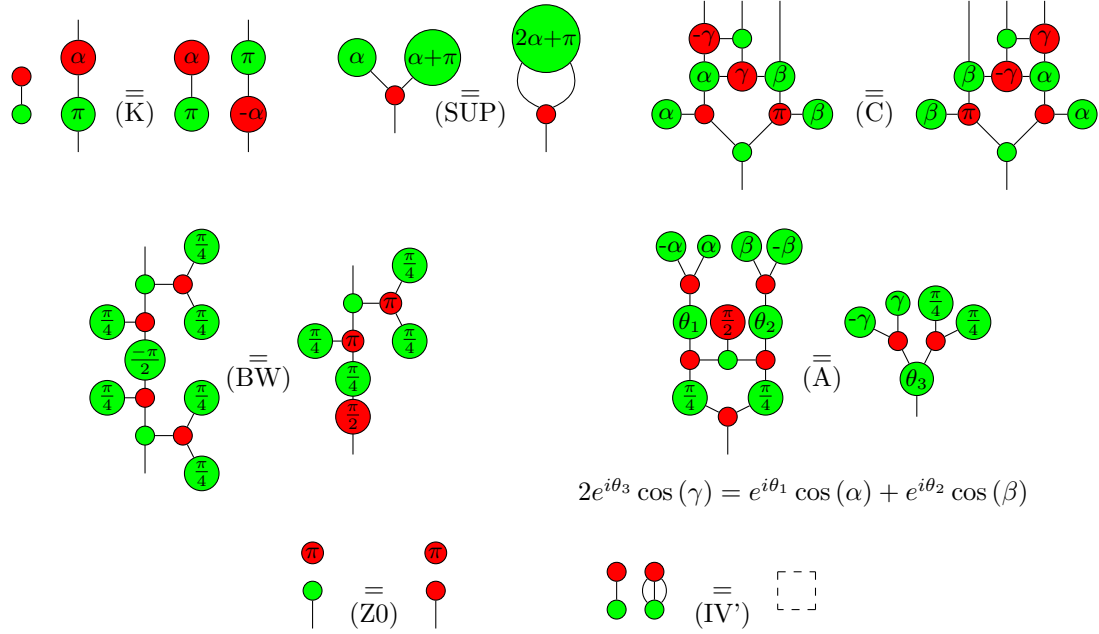


Fig. 2. Set of rules ZX' for the ZX-Calculus with scalars. The right-hand side of (E) is an empty diagram. (...) denote zero or more wires, while $(\cdot \cdot)$ denote one or more wires. In rule (EU'), $\beta_1, \beta_2, \beta_3$ and γ can be determined as follows: $x^+ := \frac{\alpha_1 + \alpha_2}{2}$, $x^- := x^+ - \alpha_2$, $z := -\sin(x^+) + i \cos(x^-)$ and $z' := \cos(x^+) - i \sin(x^-)$, then $\beta_1 = \arg z + \arg z'$, $\beta_2 = 2 \arg \left(i + \left| \frac{z}{z'} \right| \right)$, $\beta_3 = \arg z - \arg z'$, $\gamma = x^+ - \arg(z) + \frac{\pi - \beta_2}{2}$ where by convention $\arg(0) := 0$ and $z' = 0 \implies \beta_2 = 0$.

Proof. The proof, done at the end of the appendix, at page 25, consists in showing that all the rules in Figure 1 are derivable.

On the one hand, this new axiomatisation is one axiom shorter, and (EU') and (IV) can be considered simpler than (EU) and (E). On the other hand, the axiomatisation in Figure 1 has the nice property that it suffices to remove (EU) and (E) to get a complete axiomatisation for the scalar-free Clifford fragment. Moreover, (EU) is arguably more natural, and has already been given for instance in [10].

The following of the paper is dedicated to the proof of Theorem 1. Since [19,24] provided us with two complete axiomatisations for the general ZX-Calculus, all we have to do is prove all the equations used as axioms in either one of these two axiomatisations. As the axiomatisation in [19] requires additional generators and more axioms, we will use the axiomatisation of [24] as a reference which consists in all the axioms of Figure 1 but (EU), together with the following axioms, we call obsolete, as we are proving in the following that they can be derived using the (EU) rule:

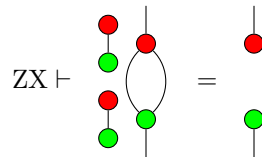


Remark 1. The last two equations, (ZO) and (IV'), are actually derivable from (K), (SUP) and the Clifford axiomatisation [25]. However, they are given here, because together with (S), (I), (CP), (B), (HD) and (H), they make the Clifford fragment complete, which will be our first milestone.

3 Clifford

As we just said, a first and easy step to do is to show that we can recover the rules that are known to make the language complete for Clifford [1]. This will allow us to freely use in the following all the equations of the $\frac{\pi}{2}$ -fragment that are sound. We already have most of these rules that make the ZX-calculus complete for Clifford. We only lack two: the *zero* (ZO) and the *inverse* (IV') rules. A first very well known lemma we will use for both proofs is the Hopf law:

Lemma 1 (Hopf Law).



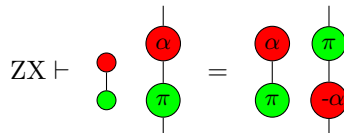
From there, it is fairly easy to recover the inverse rule:

Proposition 2. *The inverse rule is derivable:*



To prove the zero rule, we will use another well known equation, called π -commutation, which is also one of the now obsolete rules.

Proposition 3. *The π -commutation is derivable:*



and, with some effort, the rule (ZO), which only deals with null diagrams, can be recovered:

Proposition 4. *The zero rule is derivable:*

$$\text{ZX} \vdash \begin{array}{c} \bullet \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \end{array}$$

As a result:

Theorem 3. *For any diagrams D_1, D_2 of the $\frac{\pi}{2}$ -fragment:*

$$\llbracket D_1 \rrbracket = \llbracket D_2 \rrbracket \iff \text{ZX} \vdash D_1 = D_2$$

From this first milestone, we get all the sound equations in Clifford, but actually also a bit more. For instance, the following lemmas are known to be derivable from the Clifford axiomatisation (see Appendix):

Lemma 2.

$$\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \end{array}$$

Lemma 3.

$$\begin{array}{c} \bullet \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \end{array}$$

4 Singular Value Decompositions

The next step is logically to get the completeness for Clifford+T quantum mechanics, i.e. the completeness of the $\frac{\pi}{4}$ -fragment of the ZX-calculus. Now that we are seeking to prove equations that are out of Clifford, we will begin to use (EU) to its full potential. However, we would like, as much as possible, to avoid computing the angles, because, since we work on the problem of completeness, we need to *formally* prove the equality between two diagrams, and hence to formally write what the angles resulting from (EU) are, which becomes tedious after a few number of application of the rule.

To simplify this task, instead of showing directly that two diagrams can be turned into one another, we will define a normal form for them, show that it is unique, and show that there is an algorithm to turn them in this normal form.

First, we show another version of the rule (EU) with dangling branches:

Lemma 4.

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array}$$

where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU).

In a particular case, it implies:

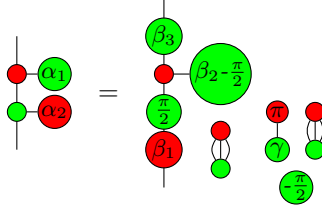
Corollary 1.

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array} = \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array} \begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array}$$

where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU) with $\alpha_2 \leftarrow \frac{\pi}{2}$.

We can also derive a kind of inverse operation:

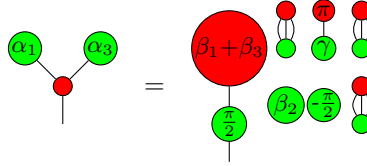
Lemma 5.



where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU) applied with the angles $\alpha_2 \leftarrow \alpha_2 + \frac{\pi}{2}$ and $\alpha_3 \leftarrow \frac{\pi}{2}$.

Then, we show that any diagram in the form of the left hand side of (SUP)– but with arbitrary angles – can be transformed in a state with no branching:

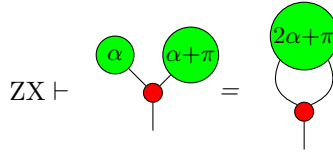
Lemma 6.



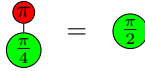
where $\beta_1, \beta_2, \beta_3, \gamma$ can be determined as in rule (EU) with $\alpha_2 \leftarrow \frac{\pi}{2}$.

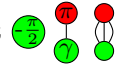

Now, by specialising the angles to α and $\alpha + \pi$, we shall recover (SUP):

Proposition 5. *The supplementarity is derivable:*



Remark 2. The supplementarity allows us to prove:



which, coupled with Lemma 2 , implies that  can be replaced by  in the last three lemmas.

Right now, we have proven all the equations that do not really need a unique normal form. For the rest, we present the singular-value decomposition of a matrix, and introduce it to ZX-diagrams.

Definition 1. *We call a singular value decomposition (SVD) of a matrix a decomposition of the form*

$$M = U \Sigma V^\dagger$$

where U and V are unitary, and Σ is diagonal. Notice that M needs not be square (in this case Σ has the same dimensions as M).

To justify the use of SVDs, we give some of it interesting properties [21]:

Proposition 6. *The SVD $M = U \Sigma V^\dagger$ of a matrix M has the following properties:*

- It exists whatever M
- Σ can be made unique if we impose that its diagonal entries are decreasing non-negative real numbers
- U and V are not unique in general, though:

– If M is square with distinct and non-zero singular values, then U and V are essentially unique:

$$U\Sigma V^\dagger = U'\Sigma V'^\dagger \iff (\exists d, (U' = Ud) \wedge (V' = Vd))$$

where d is diagonal with diagonal entries some roots of unity.

Even though the singular-value decomposition is relevant for any diagram, we are only going to give its derivation for a particular family of diagrams:

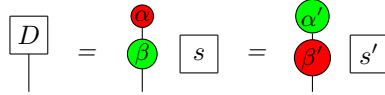
Definition 2. We call a cycle-free diagram a diagram composed only of $|$, \square , $\begin{array}{c} \cdot \\ \vdots \\ \cdot \\ \circ \end{array}$, $\begin{array}{c} \cdot \\ \vdots \\ \cdot \\ \circ \end{array}$ where $n \in \mathbb{N}$ and $\alpha \in \mathbb{R}$.

Remark 3. Some diagrams that do not strictly follow the conditions of the previous definition will still be considered cycle-free if they are equal to a cycle-free diagram by mere application of the “only topology matters” paradigm, i.e. if they are isomorphic to a cycle-free diagram. E.g.:



We can now easily give a normal form for one-qubit states, using the SVD. In this case $\Sigma = s' |0\rangle$, U is a one-qubit unitary, which can be expressed as in Proposition 1, and V is a $0 \rightarrow 0$ unitary, i.e. a global phase.

Proposition 7 (SVD of a State). Any cycle-free state $D : 0 \rightarrow 1$ can be put in the following forms:



where $\beta, \beta' \in [0, \pi)$, and where s and s' are $0 \rightarrow 0$ diagrams, i.e. scalars. We call these two forms respectively SVD_g and SVD_r .

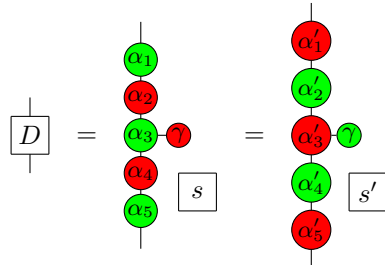
Proposition 8 (SVDs of states are essentially unique). If $D_1 = \begin{array}{c} \alpha_1 \\ \beta_1 \end{array} \square s_1$ and $D_2 = \begin{array}{c} \alpha_2 \\ \beta_2 \end{array} \square s_2$

are in SVD, and if $\llbracket D_1 \rrbracket = \llbracket D_2 \rrbracket \neq 0$, then either:

- $\alpha_1 = \alpha_2 \bmod 2\pi$ and $\alpha_i = 0 \bmod \pi$
- $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$

We can have basically the same results for $1 \rightarrow 1$ operators:

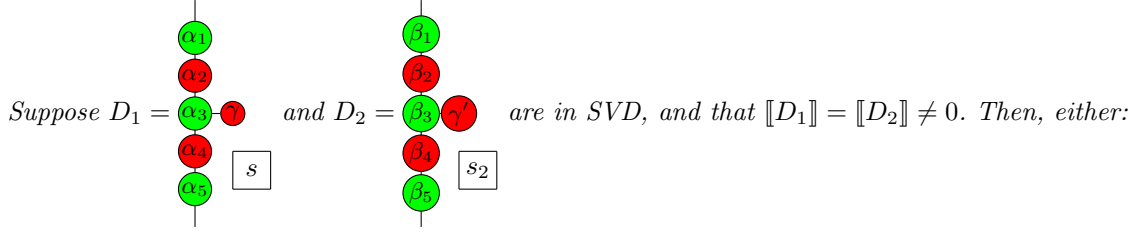
Proposition 9 (SVD of a $1 \rightarrow 1$ diagram). Any cycle-free diagram $D : 1 \rightarrow 1$ can be written in the forms:



where $\gamma \in [0, \frac{\pi}{2}]$, and $\alpha_1, \alpha_5, \alpha'_1, \alpha'_5 \in [0, \pi)$. We denote the two forms respectively SVD_g and SVD_r .

Remark 4. We gave two conventions for the SVDs of $0 \rightarrow 1$ and $1 \rightarrow 1$ diagrams. These two depend on the basis in which we consider the decomposition. SVD_g corresponds to the computational basis, while SVD_r corresponds to the diagonal basis. If $M = U\Sigma V^\dagger$ with Σ diagonal in the computational basis, $M = (UH) \cdot H\Sigma H \cdot (VH)^\dagger$.

Proposition 10 ($1 \rightarrow 1$ SVDs are essentially unique).

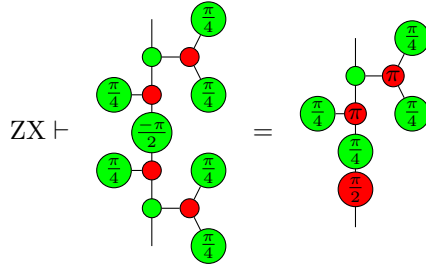


- $\gamma = \gamma' = 0$
- $\gamma = \gamma' = \frac{\pi}{2}$
- $\alpha_i = \beta_i$ and $\gamma = \gamma'$

5 Clifford+T and Beyond

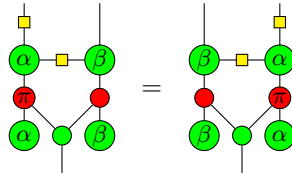
The point now is to exploit the SVD of ZX-diagrams and their uniqueness. A rule that can directly use these results is (BW):

Proposition 11.



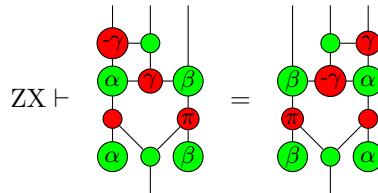
The results on SVDs can not be directly used to prove the equation (C), for its diagrams have 4 inputs/outputs, and have a cycle. However, the SVDs can be used to prove a first intermediary result:

Lemma 7.



From which we can deduce the equation (C) itself:

Proposition 12.



Remark 5. From Lemma 7, (C) can be derived using only the Clifford rules. However, the provided proof requires using half angles. Hence, whenever the considered fragment contains all its half angles, the equation in Lemma 7 should be preferred to (C).

We have derived all the rules necessary for the completeness of the Clifford+T fragment of the ZX-Calculus, which means:

Theorem 4. For any diagrams D_1, D_2 of the $\frac{\pi}{4}$ -fragment:

$$\llbracket D_1 \rrbracket = \llbracket D_2 \rrbracket \iff ZX \vdash D_1 = D_2$$

Finally, it remains to derive the equation (A). Notice that the diagram on the left hand side contains a cycle, which implies we can not use the results on SVDs. However, the cycle can be easily removed, and we are able to prove:

Proposition 13.

$$2e^{i\theta_3} \cos(\gamma) = e^{i\theta_1} \cos(\alpha) + e^{i\theta_2} \cos(\beta)$$

This last proposition ends the proof of Theorem 1. □

6 Discussion and Further Work

We have provided two simple but complete axiomatisations of the ZX-Calculus for universal quantum mechanics. By doing so, we have restored intuitiveness – one of its the first aims – to the language (at least on the structural level, computing the angles in (EU) remains tedious if done formally). This step forward should simplify axiom-related problems such as verification or compilation.

To simplify the task of proving the derivability of equations, we introduced singular-value decomposition of $0 \rightarrow 1$ and $1 \rightarrow 1$ diagrams, and proved that there exists an algorithm to turn any $0 \rightarrow 1$ and $1 \rightarrow 1$ cycle-free diagram into its SVD form. We did not need SVD form for diagrams *with* cycle, and leave as a further development the extension of the algorithm to arbitrary $0 \rightarrow 1$ and $1 \rightarrow 1$ diagrams, which should be possible by completeness and universality.

We did not need to define the SVD form for larger diagrams either. A problem would arise in ZX, for instance for a diagram with 3 inputs/outputs: do we decompose the diagram as a $0 \rightarrow 3$, or a $1 \rightarrow 2$ diagram and then use the map/state duality? This would result in two completely different decompositions. Still, defining SVDs for diagrams of any arity could prove interesting.

Concerning the result itself, we have proven that, in ZX-Calculus:

$$\left. \begin{array}{l} \text{many-qubit Clifford completeness} \\ + \\ \text{completeness for 1-qubit unitaries} \end{array} \right\} = \text{many-qubit completeness}$$

This formulation is a bit excessive, since we actually have several rules that operate beyond the Clifford fragment, namely (S) and (H), where the angles can take any value in \mathbb{R} – and this feature is actually needed for the completeness. Still, since it is not absurd to imagine we can always find similar rules for the considered language, this raises two questions:

- Is it true for fragments of the ZX-Calculus?

The answer in general is no. Indeed, in the case of Clifford+T, the axiomatisation for Clifford is enough to get the 1-qubit completeness [3]. However, it has been proven that rules (SUP) and (E) are necessary [25,28]. Hence, the previous statement does not stand for Clifford+T.

- How far from this statement are we in other languages?

For instance, we know a complete presentation for the many-qubit Clifford fragment of quantum circuits [29]. Moreover, the rule (EU) has an obvious equivalent in circuits, and is the only needed axiom for 1-qubit completeness. So what do we lack to get the universal completeness?

References

1. M. Backens, S. Perdrix & Q. Wang (2017): *Towards a Minimal Stabilizer ZX-calculus*. ArXiv e-prints.
2. Miriam Backens (2014): *The ZX-calculus is complete for stabilizer quantum mechanics*. *New Journal of Physics* 16(9), 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 (2014): *The ZX-calculus is complete for the single-qubit Clifford+T group*. *Electronic Proceedings in Theoretical Computer Science* 172, pp. 293–303, doi:10.4204/eptcs.172.21. Available at <https://doi.org/10.4204%2Feptcs.172.21>.
4. Miriam Backens & Ali Nabi Duman (2014): *A complete graphical calculus for Spekkens' toy bit theory*. *Foundations of Physics*, pp. 1–34, doi:10.1007/s10701-015-9957-7.
5. Niel de Beaudrap & Dominic Horsman (2017): *The ZX calculus is a language for surface code lattice surgery*. CoRR abs/1704.08670. Available at <http://arxiv.org/abs/1704.08670>.
6. Nicholas Chancellor, Aleks Kissinger, Joschka Roffe, Stefan Zohren & Dominic Horsman (2016): *Graphical Structures for Design and Verification of Quantum Error Correction*. Available at <https://arxiv.org/abs/1611.08012>. Last revised Jan. 2018.
7. 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>.
8. Bob Coecke & Aleks Kissinger (2017): *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, doi:10.1017/9781316219317.
9. Bob Coecke, Dusko Pavlovic & Jamie Vicary (2012): *A new description of orthogonal bases*. *Mathematical Structures in Computer Science* 23(03), pp. 555–567, doi:10.1017/s0960129512000047.
10. Bob Coecke & Quanlong Wang (2018): *ZX-Rules for 2-qubit Clifford+T Quantum Circuits*.
11. Ross Duncan (2013): *A Graphical Approach to Measurement-Based Quantum Computing*. In: *Quantum Physics and Linguistics*, Oxford University Press, pp. 50–89, doi:10.1093/acprof:oso/9780199646296.003.0003. Available at <https://doi.org/10.1093%2Facprof%3Aoso%2F9780199646296.003.0003>.
12. Ross Duncan & Kevin Dunne (2016): *Interacting Frobenius Algebras Are Hopf*. In: *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2016*, ACM, New York, NY, USA, pp. 535–544, doi:10.1145/2933575.2934550. Available at <http://doi.acm.org/10.1145/2933575.2934550>.
13. Ross Duncan & Liam Garvie (2017): *Verifying the Smallest Interesting Colour Code with Quantomatic*. Available at <https://arxiv.org/abs/1706.02717>.
14. Ross Duncan & Maxime Lucas (2014): *Verifying the Steane code with Quantomatic*. *Electronic Proceedings in Theoretical Computer Science* 171, pp. 33–49, doi:10.4204/eptcs.171.4. Available at <https://doi.org/10.4204%2Feptcs.171.4>.
15. Ross Duncan & Simon Perdrix (2009): *Graphs States and the necessity of Euler Decomposition*. *Mathematical Theory and Computational Practice* 5635, pp. 167–177, doi:10.1007/978-3-642-03073-4.
16. 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>.
17. Ross Duncan & Simon Perdrix (2013): *Pivoting makes the ZX-calculus complete for real stabilizers*. In: *QPL 2013*, *Electronic Proceedings in Theoretical Computer Science*, pp. 50–62, doi:10.4204/EPTCS.171.5.
18. Leonhard Euler (1776): *Formulae Generales Pro Translatione Quacunque Corporum Rigidorum*. In: *Novi Commentarii academiae scientiarum Petropolitanae* 20, pp. 189–207.
19. Amar Hadzahasanovic, 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>.
20. Anne Hillebrand (2011): *Quantum Protocols involving Multiparticle Entanglement and their Representations*. Master's thesis, University of Oxford. Available at <https://www.cs.ox.ac.uk/people/bob.coecke/Anne.pdf>.
21. Roger A. Horn & Charles R. Johnson (1985): *Positive definite matrices*. In: *Matrix analysis*, Cambridge University Press, pp. 391–486, doi:10.1017/cbo9780511810817.009.
22. Clare Horsman (2011): *Quantum pictorialism for topological cluster-state computing*. *New Journal of Physics* 13(9), p. 095011, doi:10.1088/1367-2630/13/9/095011. Available at <https://doi.org/10.1088%2F1367-2630%2F13%2F9%2F095011>.
23. Emmanuel Jeandel, Simon Perdrix & Renaud Vilmart (2018): *A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics*. In: *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS '18*, ACM, New York, NY, USA, pp. 559–568, doi:10.1145/3209108.3209131. Available at <http://doi.acm.org/10.1145/3209108.3209131>.

$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{3}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(I)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(CP)_2}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (2)$$

$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{1}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{3}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{1/2}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (3)$$

$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \end{array} \stackrel{(3)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \end{array} \stackrel{(2)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \end{array} \stackrel{2}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (4)$$

Now, if $\alpha \in \mathbb{D}\pi$ (where $\mathbb{D} := \mathbb{Z}[\frac{1}{2}]$), then there exists n such that $2^n\alpha = 0 \pmod{2\pi}$. Hence, in this case the scalar on the right hand side of (3) can be removed by applying (4) from right to left $n+1$ times then using (2) and 2 to remove it. Hence:

$$\forall \alpha \in \mathbb{D}\pi, \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} = \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (5)$$

$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(5)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(E)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (6)$$

$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(H)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(HD)_{(S)_2}}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(CP)_{(S)}}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (7)$$

$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(5)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(7)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(5)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(1)_2}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(6)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (8)$$

Proof (Lem. 2). We are going to use the following equation we get from the Clifford completeness:

$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} = \begin{array}{c} \text{Red node} \\ / \quad \backslash \\ \text{Green node} \quad \text{Green node} \end{array} \quad (8)$$

so:

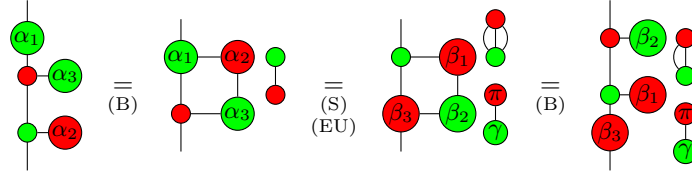
$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)_{(CP)}}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{8}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (9)$$

Proof (Lem. 3).

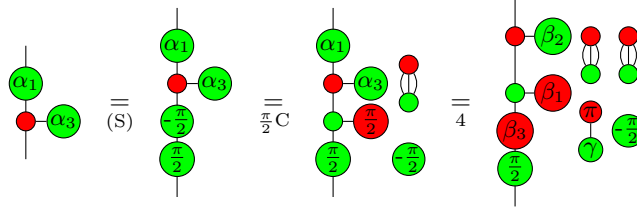
$$\begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{3}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(CP)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{2}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(CP)}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Red node} \\ | \\ \text{Green node} \end{array} \stackrel{(S)_2}{=} \begin{array}{c} \text{Red node} \\ | \\ \text{Green node} \end{array} \quad (10)$$

A.2 Proofs for Singular-Value Decompositions

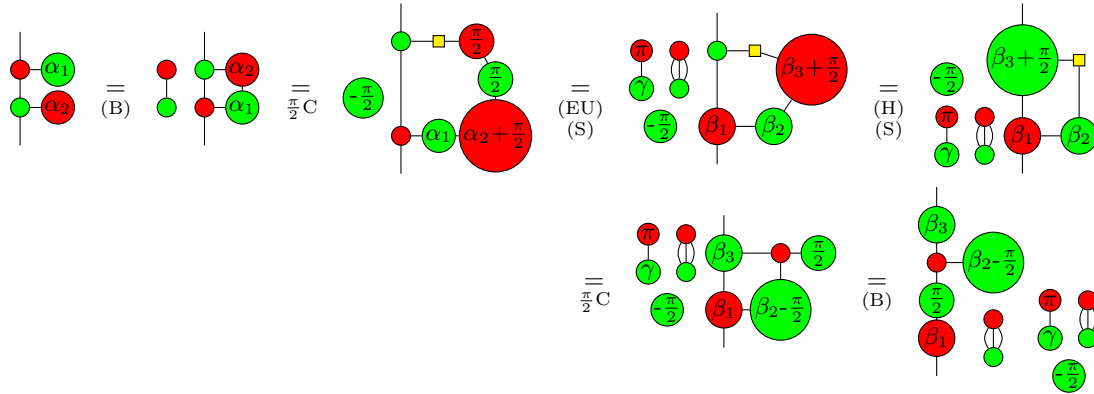
Proof (Lem. 4).



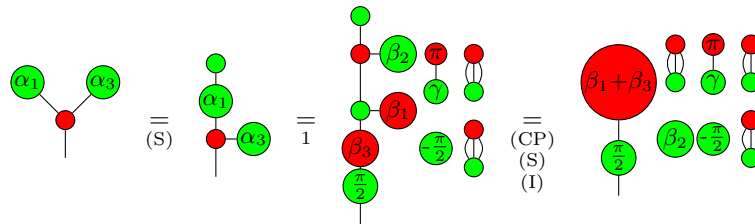
Proof (Cor. 1).



Proof (Lem. 5).



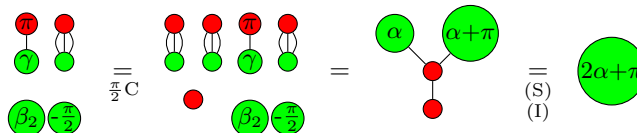
Proof (Lem. 6).



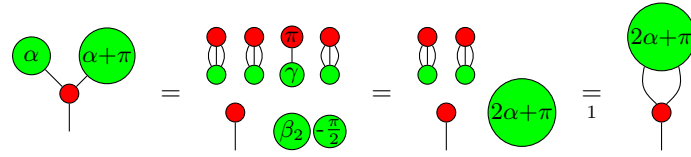
Proof (Prop. 5). We first use Lemma 6, where $\alpha_3 = \alpha_1 + \pi$. In this case, it can be computed that

$\beta_1 + \beta_3 = 0$, so we end up with: . From this, we can easily specify the

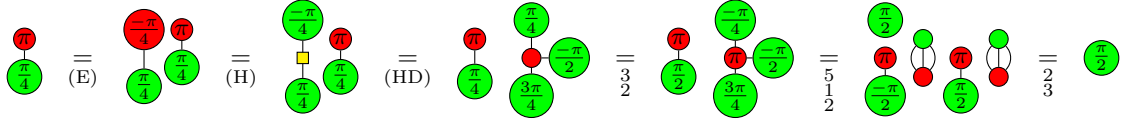
scalar on the right part:



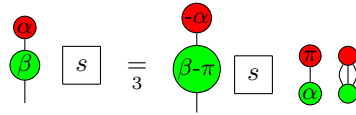
So finally:



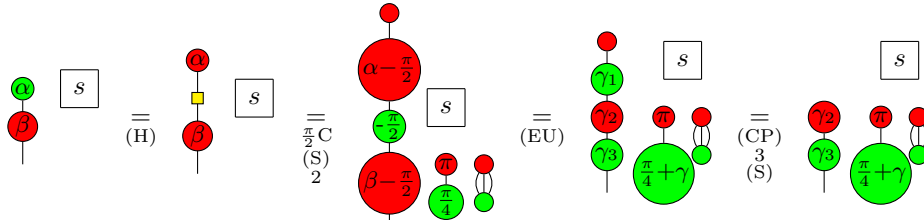
Proof (Rem. 2).



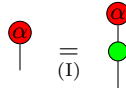
Proof (Prop. 7). First, notice that a state in the previous form can easily be transformed into an SVD. Indeed, if $\beta \in [\pi, 2\pi)$:



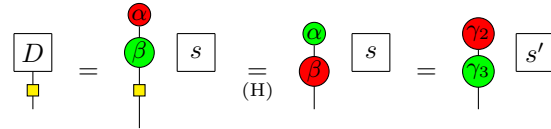
and similarly for the SVD_r . We can show that we can transform an SVD_r into an SVD_g and vice-versa :



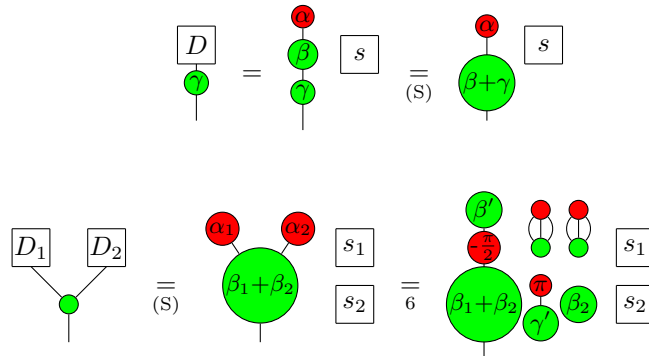
Then, we prove the result by induction.

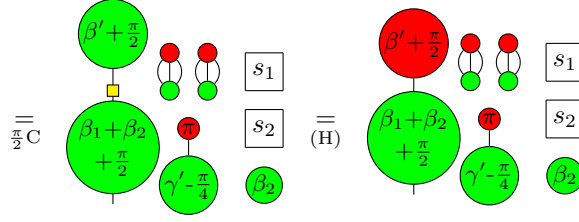


Then :



Notice that the generator $R_Z^{(0,1)}(\alpha)$ can be obtained as a combination of the last two. Then :





Finally, the generator $R_Z^{(n,1)}(\alpha)$ can be obtained by composition of $R_Z(\alpha)$ and $R_Z^{(2,1)}(\alpha)$; and $R_X^{(n,1)}(\alpha)$ can be obtained by composition of $R_Z^{(n,1)}(\alpha)$ and H .

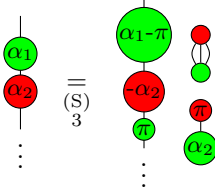
Proof (Prop. 8). The equality reads $s_1 \left(\frac{1 + e^{i\alpha_1}}{e^{i\beta_1}(1 - e^{i\alpha_1})} \right) = s_2 \left(\frac{1 + e^{i\alpha_2}}{e^{i\beta_2}(1 - e^{i\alpha_2})} \right)$. If $\alpha_1 = \pi$, then it is easy to see that $\alpha_2 = \pi$ and $s_1 e^{i\beta_1} = s_2 e^{i\beta_2}$. If $\alpha_i \neq \pi$, then the upper coefficient is non-null, hence we can divide the lower coefficient by the upper one, which yields:

$$e^{i\beta_1} \frac{1 - e^{i\alpha_1}}{1 + e^{i\alpha_1}} = e^{i\beta_2} \frac{1 - e^{i\alpha_2}}{1 + e^{i\alpha_2}} \quad \Leftrightarrow \quad e^{i\beta_1} \tan\left(\frac{\alpha_1}{2}\right) = e^{i\beta_2} \tan\left(\frac{\alpha_2}{2}\right)$$

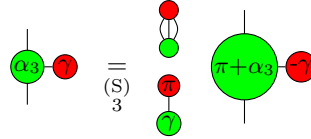
If $\alpha_1 = 0 \bmod 2\pi$ then $\alpha_2 = 0 \bmod 2\pi$. Otherwise, since $\beta_1, \beta_2 \in [0, \pi)$, $\beta_1 = \beta_2$ and $\alpha_1 = \alpha_2 \bmod 2\pi$.

Proof (Prop. 9). First, if D is in the form SVD_g , but where the constraints on the angles are not met, we can transform it into an actual SVD_g :

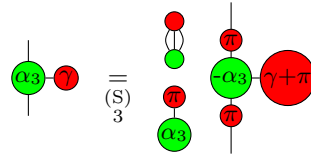
– If $\alpha_1 \in [\pi, 2\pi)$ (and similarly for α_5):



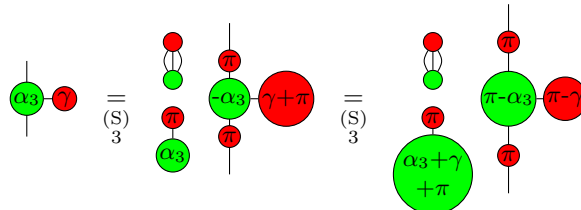
– If $\gamma \in [-\frac{\pi}{2}, 0[$:



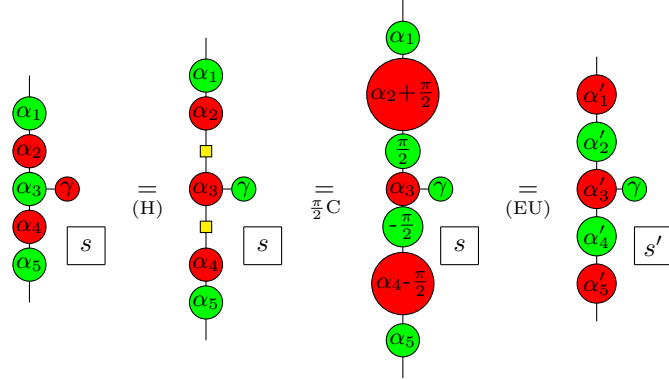
– If $\gamma \in [-\pi, -\frac{\pi}{2}[$:



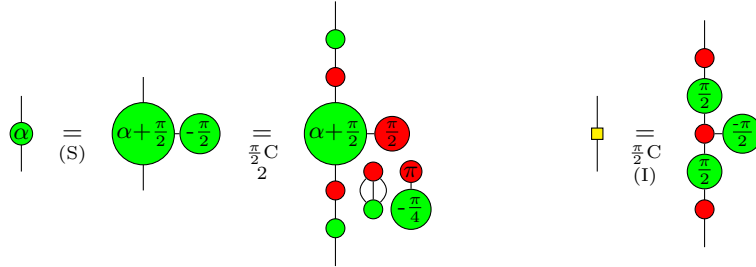
– If $\gamma \in [\frac{\pi}{2}, \pi)$:



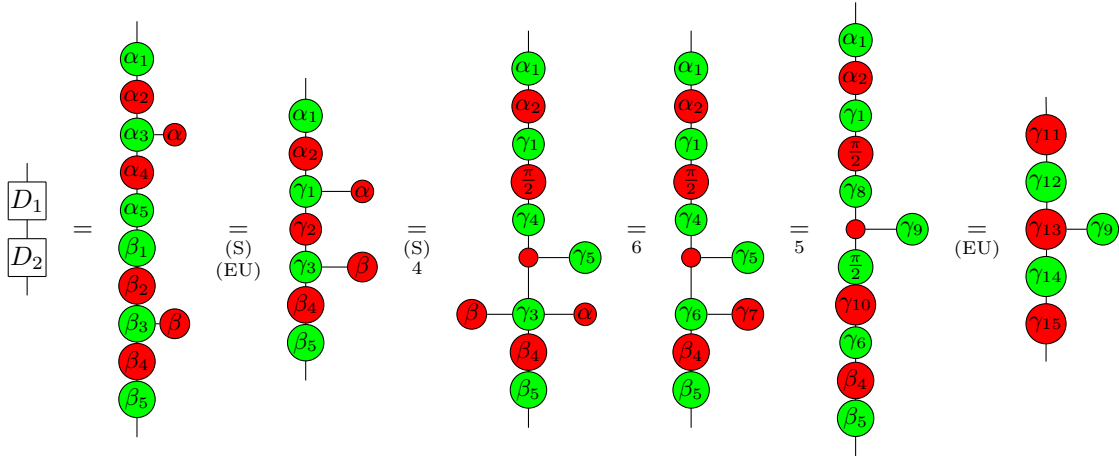
Then, we show that the two decompositions are equivalent:



The two $1 \rightarrow 1$ generators $R_Z^{(1,1)}(\alpha)$ and H can be put in SVD:

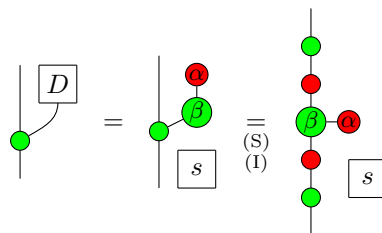


The composition of two SVDs can be put in SVD (here, ignoring the scalars):



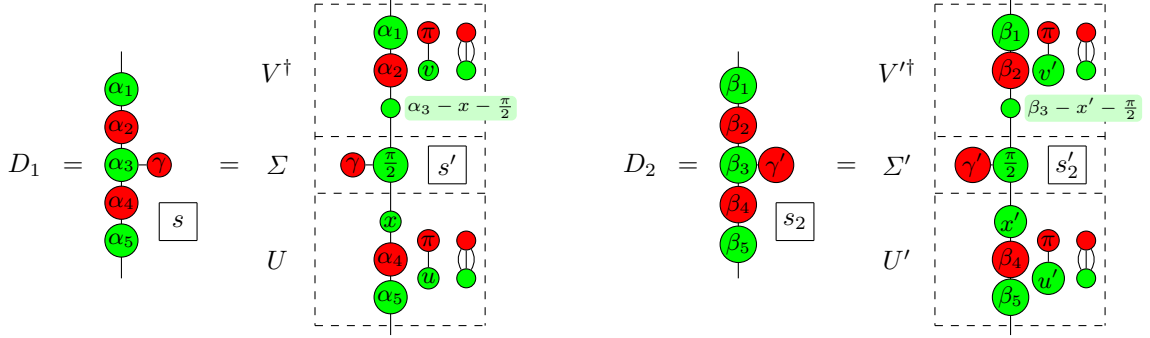
Notice that, by composition, the $1 \rightarrow 1$ generator $R_X^{(1,1)}(\alpha)$ can be put in SVD.

If the $1 \rightarrow 1$ diagram has no cycle, there can still be branching. Hence, there can be a state $D : 0 \rightarrow 1$ in tree-like form attached to the “main wire” by a node, say green, as follows:



Branching made by a red node can be deduced by composing the green one and Hadamard nodes.

Proof (Prop. 10). First we decompose D_1 and D_2 as:



where u, v, u' and v' have been chosen so that $[\Sigma]$ and $[\Sigma']$ are real matrices. Notice that $[U]$, $[V^\dagger]$, $[U']$, $[V'^\dagger]$ are unitaries. We have two SVDs that represent the same matrix:

$$[U] \circ [\Sigma] \circ [V^\dagger] = [D_1] = [D_2] = [U'] \circ [\Sigma'] \circ [V'^\dagger]$$

First off, let us show that Σ and Σ' are essentially the same. One could compute $[\Sigma] = [s'] (1 + e^{i\gamma}) \begin{pmatrix} 1 & 0 \\ 0 & \tan(\frac{\gamma}{2}) \end{pmatrix}$ and $[\Sigma'] = [s'_2] (1 + e^{i\gamma'}) \begin{pmatrix} 1 & 0 \\ 0 & \tan(\frac{\gamma'}{2}) \end{pmatrix}$. Since $\gamma, \gamma' \in [0, \frac{\pi}{2}]$, $\tan(\frac{\gamma}{2})$ and $\tan(\frac{\gamma'}{2})$ are smaller than 1, and since the diagrams are non-null, we get $[\Sigma] = [\Sigma']$ by Proposition 6, which implies $\gamma = \gamma'$.

If $\gamma = \gamma' \neq 0$, then $[\Sigma]$ and $[\Sigma']$ have full rank. Moreover, if $\gamma = \gamma' \neq \frac{\pi}{2}$, then $[\Sigma]$ and $[\Sigma']$ are not colinear to the identity. Hence, if $\gamma = \gamma' \in]0, \frac{\pi}{2}[$, then we can apply Proposition 6.

By Proposition 6, there exists $d = \begin{pmatrix} e^{i\varphi_0} & 0 \\ 0 & e^{i\varphi_1} \end{pmatrix}$ such that $[U'] = [U] \circ d$ and $[V'^\dagger] = d^\dagger \circ [V^\dagger]$.

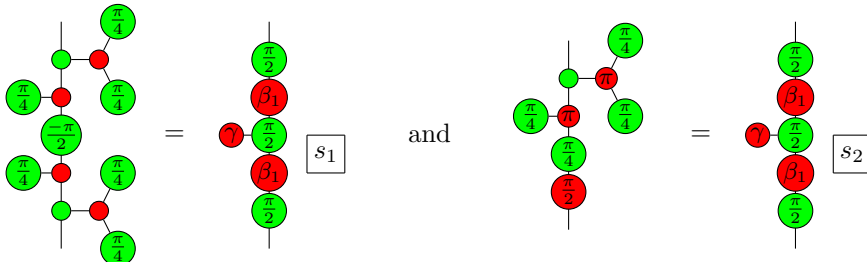
Notice that $\left[\begin{array}{c} \varphi_1 - \varphi_0 \\ \varphi_0 \end{array} \right] = d$ and $\left[\begin{array}{c} \varphi_0 - \varphi_1 \\ \varphi_1 \end{array} \right] = d^\dagger$. Hence:

$$[U'] = \left[\begin{array}{c} x' \\ \beta_4 \\ \beta_5 \end{array} \right] = [U] \circ d = \left[\begin{array}{c} x + \varphi_1 - \varphi_0 \\ \alpha_4 \\ \alpha_5 \\ u + \varphi_0 \end{array} \right]$$

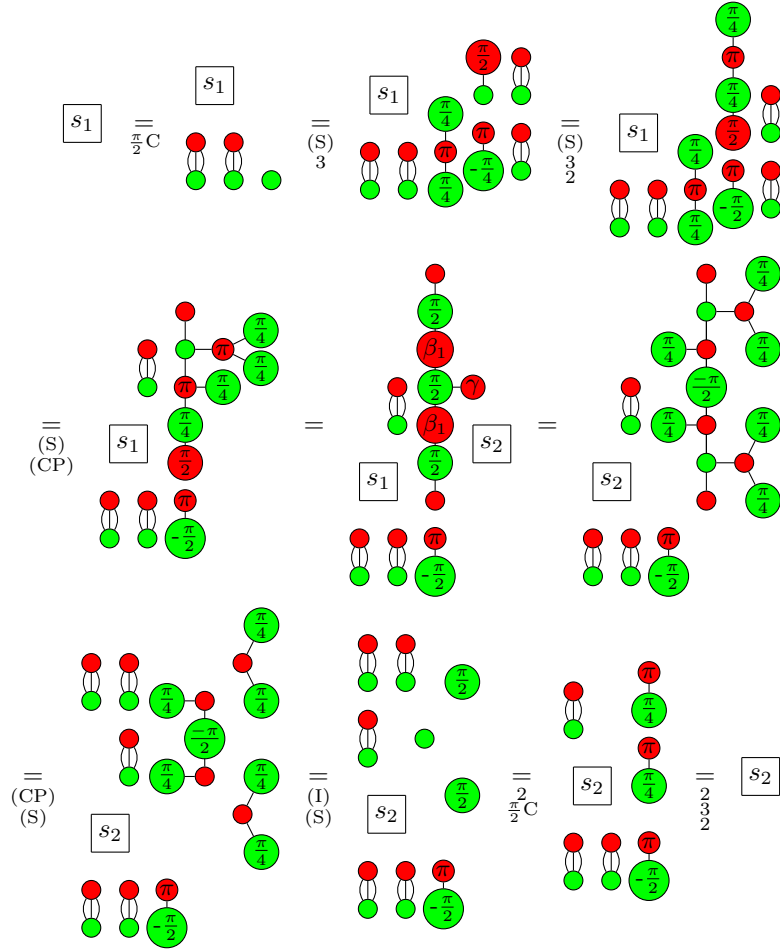
Since β_5 and α_5 are in $[0, \pi)$, the representation of the unitary is unique by Proposition 1, so $\beta_5 = \alpha_5$, $\beta_4 = \alpha_4$, and $x' = x + \varphi_1 - \varphi_0$. Similarly, the second equation yields $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$ and $\beta_3 - x' - \frac{\pi}{2} = \alpha_3 - x - \frac{\pi}{2} + \varphi_0 - \varphi_1$. Together, the equations on x and x' imply that $\alpha_3 = \beta_3$.

A.3 Proofs for Clifford+T and Beyond

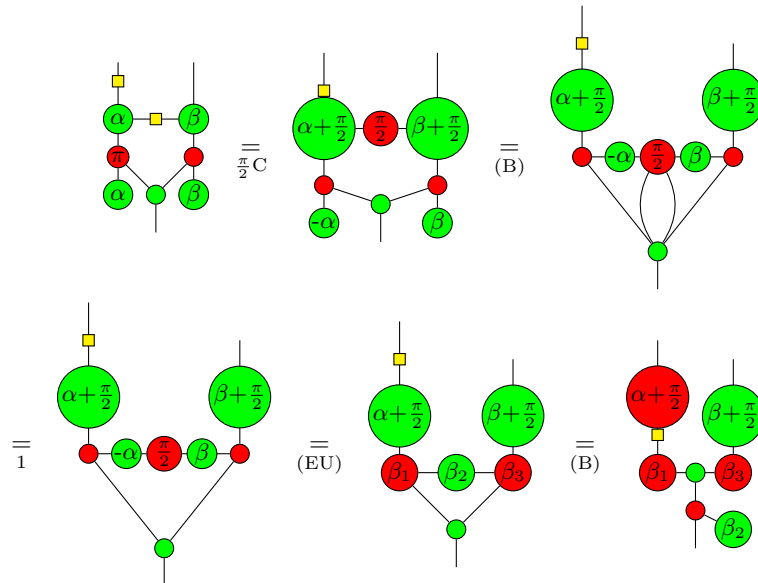
Proof (Prop. 11). Using Proposition 9, we can put both sides of the equation in SVD, and thanks to Proposition 10, the two forms have the same angles. We can even compute:

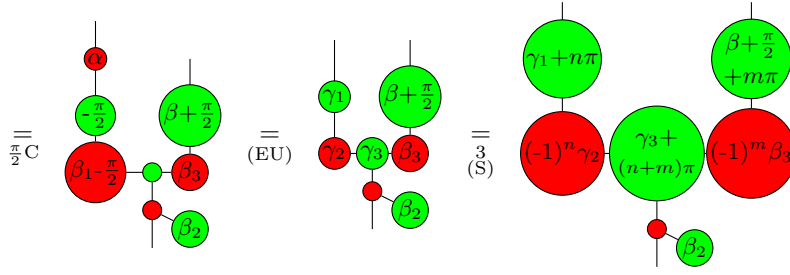


with $\gamma = \frac{\pi}{2} - 2 \arctan \frac{1}{\sqrt{5}}$ and $\beta_1 = \arctan 2$. It remains to prove that the two scalar diagrams are equal:

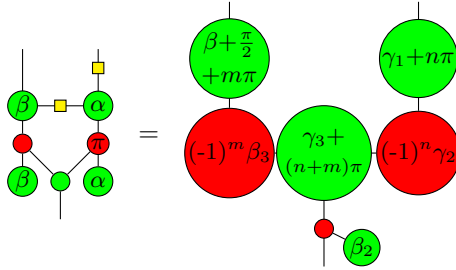


Proof (Lem. 7). We prove the equality by simplifying both sides of the equation. The left hand side yields, when ignoring the scalars:



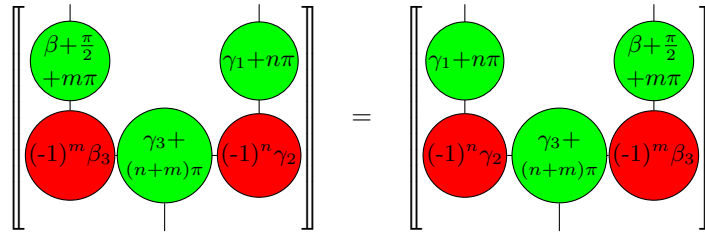


where n and m are chosen in $\{0, 1\}$ so that $\gamma_1 + n\pi$ and $\beta + \frac{\pi}{2} + m\pi$ are in $[0, \pi)$. Similarly, the right hand side yields:



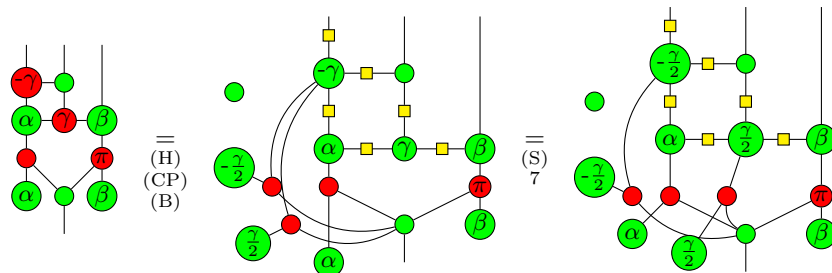
Notice that, due to the symmetry of the two diagrams, the resulting scalars (that we ignored) are equal (and non null). If $\beta_2 = 0 \pmod{\pi}$, then we can compute that both α and β are multiples of π , and in this case the equation is trivially derivable. Else, notice that $\left[\begin{array}{c} \bullet \\ \beta_2 \end{array} \right]$ is invertible,

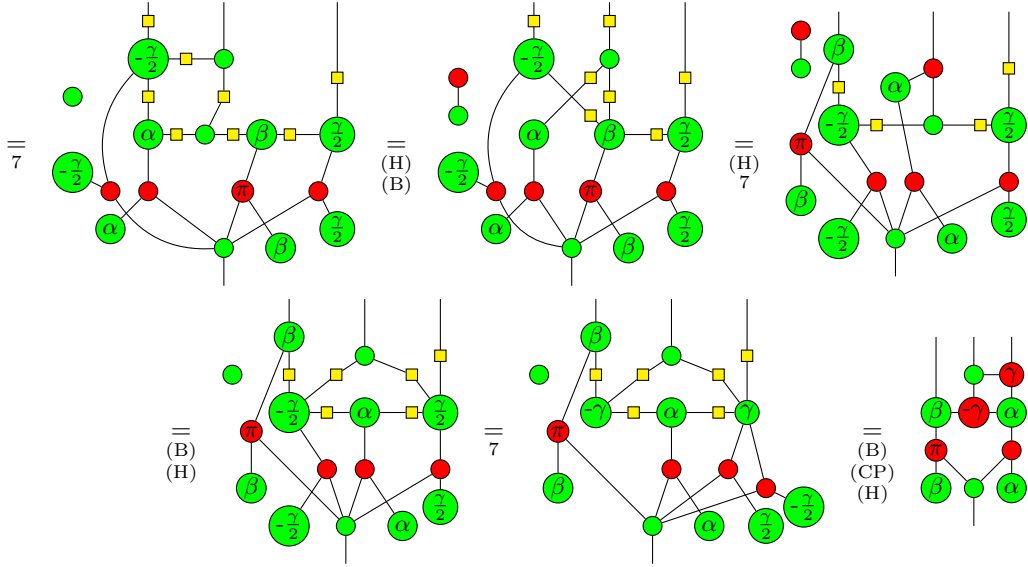
(its inverse is $\frac{1}{1-e^{2i\beta_2}} \begin{pmatrix} 1 & -e^{i\beta_2} \\ -e^{i\beta_2} & 1 \end{pmatrix}$). Hence, we get:



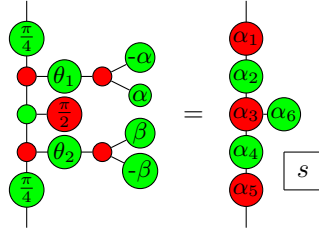
We can then plug any red dot with angle $\in]0, \frac{\pi}{2}[$, say $\frac{\pi}{4}$, on the lower branch. We can now use Proposition 10, match the angles $\gamma_1 + n\pi = \beta + \frac{\pi}{2} + m\pi$ and $(-1)^n \gamma_2 = (-1)^m \beta_3$, so the two initial diagrams are equal.

Proof (Prop. 12).

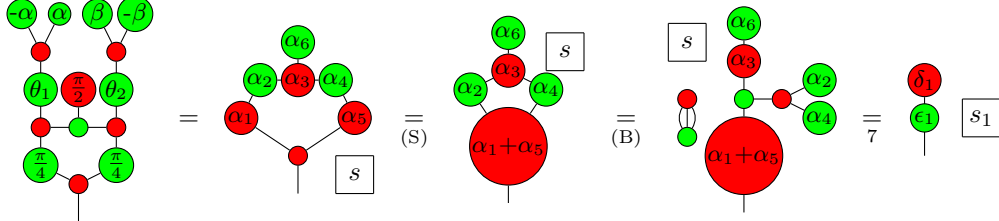




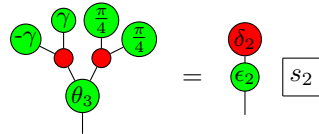
Proof (Prop. 13). The idea of the proof is here again to use the SVD, but this time of a state, the equation being between two states. The diagram on the right hand side has an SVD by direct use of Proposition 7. However, the one on the left hand side has a cycle, so we have to work a bit more. Notice that, using Proposition 9:



Hence:



From a direct use of Proposition 7:



Since the initial equation is sound under the constraint $2e^{i\theta_3} \cos(\gamma) = e^{i\theta_1} \cos(\alpha) + e^{i\theta_2} \cos(\beta)$, we have:

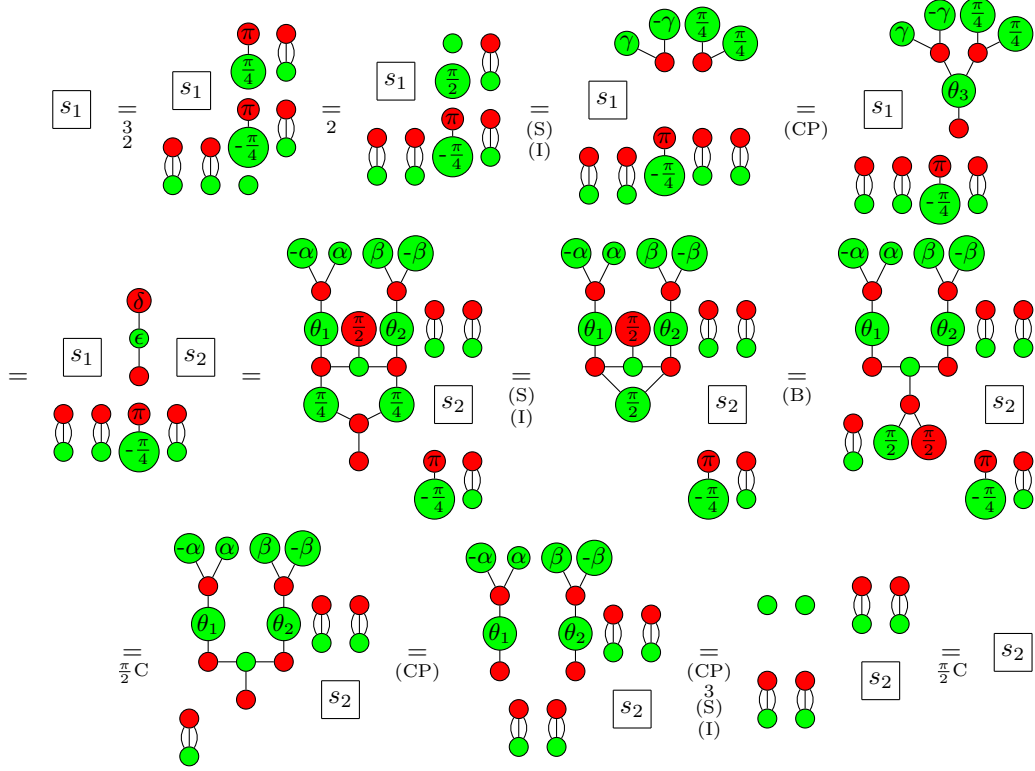
$$\left\| \begin{array}{c} \delta_1 \\ \epsilon_1 \end{array} \right\|_{s_1} = \left\| \begin{array}{c} \delta_2 \\ \epsilon_2 \end{array} \right\|_{s_2}$$

By Proposition 8, either $\delta_1 = \delta_2 = 0$, or $\delta_1 = \delta_2 = \pi$, or $\delta_1 = \delta_2 \neq 0 \pmod{\pi}$ and $\epsilon_1 = \epsilon_2$. Notice

however that in our case, δ_1 and δ_2 cannot be π because $\left\| \begin{array}{c} \gamma \\ \theta_3 \end{array} \right\| = (1+i) \left(\sqrt{2} e^{i\theta_3} \cos(\gamma) \right)$

and $\left[\begin{array}{c} \pi \\ \bullet \\ \square \\ \bullet \\ \square \end{array} \right] = \begin{pmatrix} 0 \\ \sqrt{2}se^{i\epsilon} \end{pmatrix}.$

If $\delta_1 = \delta_2 = 0$, then ϵ_1 and ϵ_2 can be discarded: $\begin{array}{c} \bullet \\ \square \\ \bullet \end{array} = \begin{array}{c} \bullet \\ \square \\ \bullet \end{array}.$ Hence, in any case, it only remains to prove that the two scalar diagrams s_1 and s_2 can be transformed into one another.



Proof (Thm. 2). We are going to prove here that all the equations in Figure 1 can be recovered from the ones in 2. First of all, we try to recover a complete axiomatisation for Clifford. To do so, we simply need to show that the Hadamard gate can be decomposed.

(12)

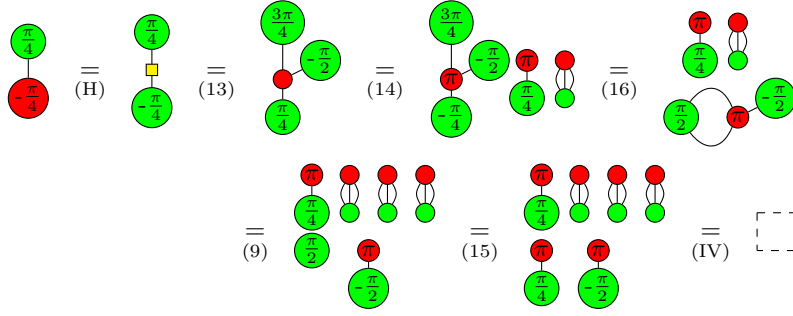
(13)

We have recovered a complete axiomatisation for Clifford. We now have access to all the lemmas deriving from this axiomatisation. The next step is to prove the equation (E) is derivable.

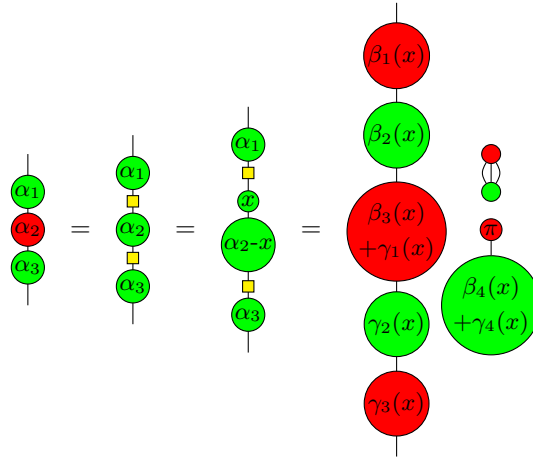
(14)

(15)

(16)



It now remains to prove the rule (EU) can be derived. We decompose the left hand side diagram as such:



where x is considered as a variable, and hence, all the computed angles depend on it, while the angles α_i are fixed. We want to find x_0 such that $\beta_3(x_0) + \gamma_1(x_0) = 0 \pmod{\pi}$. Let the functions f and g be defined as:

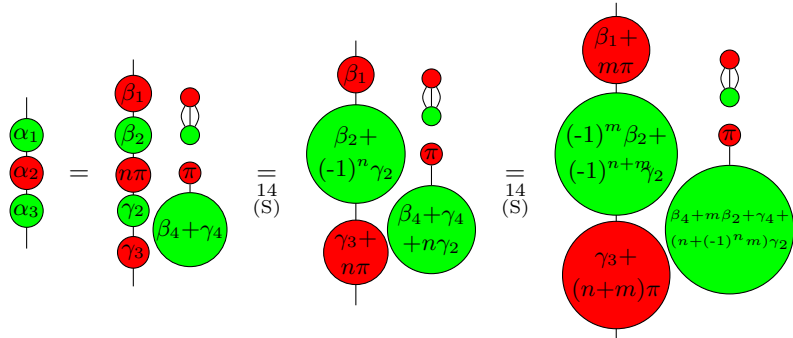
$$f : x \mapsto \arctan \left(\frac{\tan(\alpha_1) \cos(x) + \tan(\alpha_3) \cos(\alpha_2 - x)}{1 - \tan(\alpha_1) \cos(x) \tan(\alpha_3) \cos(\alpha_2 - x)} \right)$$

$$g : x \mapsto \tan(\alpha_1) \cos(x) + \tan(\alpha_3) \cos(\alpha_2 - x)$$

Notice that

$$g\left(-\frac{\pi}{2}\right) = \tan(\alpha_3) \cos\left(\alpha_2 + \frac{\pi}{2}\right) \quad \text{and} \quad g\left(\frac{\pi}{2}\right) = \tan(\alpha_1) \cos\left(\alpha_2 - \frac{\pi}{2}\right)$$

Hence, $g\left(-\frac{\pi}{2}\right)g\left(\frac{\pi}{2}\right) \leq 0$. Since g is continuous, by the intermediate value theorem, there exists $x_0 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ such that $g(x_0) = 0$. Notice now that $f(x_0) = \arctan\left(\frac{0}{1 + \tan(\alpha_1)^2 \cos(\alpha_2 - x_0)^2}\right) = 0$. Also, it can be computed that $f = \beta_3 + \gamma_1 \pmod{\pi}$. Hence, $\beta_3(x_0) + \gamma_1(x_0) = 0 \pmod{\pi}$ i.e. $\beta_3(x_0) + \gamma_1(x_0) = n\pi$. Hence, denoting $\beta_i \leftarrow \beta_i(x_0)$ and $\gamma_i \leftarrow \gamma_i(x_0)$:



Since, thank to Proposition 1, the unitary representation is unique if $\beta_1 + m\pi \in [0, \pi[$ (m has been chosen for this purpose), then the previous diagram is provably equivalent to the one resulting directly from (EU).