HAL
open science

The rational fragment of the ZX-calculus

Emmanuel Jeandel

To cite this version:

Emmanuel Jeandel. The rational fragment of the ZX-calculus. 2018. hal-01893598

HAL Id: hal-01893598

https://inria.hal.science/hal-01893598v1

Preprint submitted on 11 Oct 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.

The rational fragment of the ZX-calculus

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

October 12, 2018

Abstract

We introduce here a new axiomatisation of the rational fragment of the ZX-calculus, a diagrammatic language for quantum mechanics. Compared to the previous axiomatisation introduced in [8], our axiomatisation does not use any meta-rule, but relies instead on a more natural rule, called the cyclotomic supplementarity rule, that was introduced previously in the literature.

Our axiomatisation is only complete for diagrams using rational angles, and is not complete in the general case. Using results on diophantine geometry, we characterize precisely which diagram equality involving arbitrary angles are provable in our framework without any new axioms, and we show that our axiomatisation is continuous, in the sense that a diagram equality involving arbitrary angles is provable iff it is a limit of diagram equalities involving rational angles.

We use this result to give a complete characterization of all Euler equations that are provable in this axiomatisation.

Introduction

The ZX-calculus is a graphical calculus for quantum computing introduced by Coecke and Duncan [4], which represent quantum evolutions (matrices) by *diagrams*. The language is powerful enough to represent in particular quantum circuits, and is equipped with a set of transformation rules for diagrams so that one may simplify a diagram without changing its interpretation (the matrix it represents).

The initial set of rules as presented in [4] is not complete, in the sense that there exists two diagrams that represent the same matrix but such that one could not be transformed into the other using the set of rules. Thi initial set of rules was studied and refined over the years [2, 3, 17] until some complete axiomatisation were found for the ZX-calculus [10, 9, 7, 8].

The exact set of rules one should use depends on the particular fragment of the ZX-calculus we need, i.e. the set of angles/rotations one may use inside the diagrams. Of particular interest are the $\pi/4$ fragment (an approximatively universal fragment), the rational fragment (where most quantum circuits, e.g.

the Quantum Fourier transform [4, 15], may be expressed exactly), and the general fragment (where every matrix can be represented).

In this article, we deal mainly with the rational fragment, for which a complete axiomatisation was already given in [8]. However, the set of rules the authors found to obtain a complete axiomatisation is arguably not satisfying, as it either relies on using an additional generator (the triangle generator), or on using so-called meta-rules. We solve this problem in this article by proving that one can use instead the generalized cyclotomic rule, that was introduced previously in [11], which is an easier rule to state and to use.

We then compare our axiomatisation with the axiomatisation of the full fragment found in [10]. This full axiomatisation relies on adding only one new nonlinear rule, but this rule, while necessary, is arguably hard to use and understand. To better understand this new rule, we investigate when it is necessary, by characterizing exactly which diagram inequalities can be proven without using this rule. We prove in particular that diagram equalities provable without this rule are exactly the diagram equalities that are "limits" (in some sense) of diagram equalities involving only rational angles. Using this result and classical results on rotations in the three-dimensional space, we will in the last section give a complete list of all so-called Euler equations that can be proven without this rule.

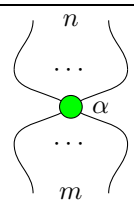
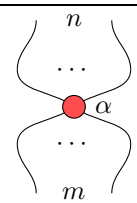
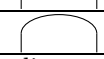
1 Definitions and Statement of the Results

1.1 Syntax and Semantics

Let G be a subgroup of $\mathbb{R}$ that contains 2π. We call G a *fragment*. Of particular interest will be the following fragments:

- $G = \mathbb{Z}\frac{\pi}{4}$. As an abuse of notation, we will call G the $\pi/4$ fragment.
- $G = \{\frac{k\pi}{2^n}, k, n \in \mathbb{Z}\}$. We will call G the $\frac{\pi}{2^\bullet}$ fragment.
- $G = \mathbb{Q}\pi$. This is the *rational* fragment. We will call any angle of G a *rational* angle.
- $G = \mathbb{R}$ This is the *full* fragment (therefore not really a fragment).

Given a fragment G, a ZX diagram $D : k \to l$ with k inputs and l outputs is generated by the following arrows:

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

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

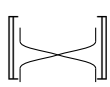
and the two compositions:

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

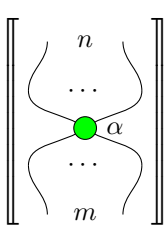
The standard interpretation of the ZX-diagrams associates to any diagram $D : n \to m$ a linear map $[\![D]\!] : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ inductively defined as follows:

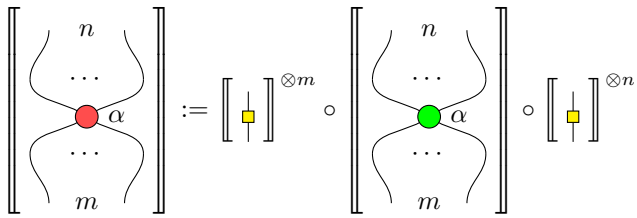
$$[\![D_1 \otimes D_2]\!] := [\![D_1]\!] \otimes [\![D_2]\!] \qquad [\![D_2 \circ D_1]\!] := [\![D_2]\!] \circ [\![D_1]\!]$$

$:= (1)$ $:= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $:= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

 $:= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ $:= \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$ $:= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

For any $\alpha \in G$, $:= \left(1 + e^{i\alpha}\right)$, and for any $n, m \geq 0$ such that $n + m > 0$:

 $:= \overbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \Bigg\} 2^m$



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

In the particular case where we want to emphasize the phase group G in which the angles α live, we will write ZX_G instead of ZX.

1.2 Rules for the $\frac{\pi}{2^\bullet}$ fragments

The set of rules of Figure 1 has been introduced in [9] and has been proven complete for the $\pi/4$ fragment. As subtler distinctions are not needed in this article, we will suppose that all the rules of Figure 1 are given for all possible, real, values of the angles α, β, γ.

Given two diagrams D_1, D_2, we say that $ZX \vdash D_1 = D_2$ if we can prove that the two diagrams are equal using only the axioms of Figure 1, along with some natural topological axioms not presented for simplicity.

The theorem of [9] can be rephrased as follows: If D_1 and D_2 are two diagrams with angles only in the $\pi/4$ fragment, and $[\![D_1]\!] = [\![D_2]\!]$, then $ZX \vdash D_1 = D_2$. The result is actually a bit stronger, as we only to consider the restrictions of the rules of Figure 1 to angles in the $\pi/4$ fragment (said otherwise: to prove that two diagrams of the $\pi/4$ fragment are equal, we do not need e.g. to introduce the angle $\pi/8$ or any other angle). We write this for reference but we stress again that this distinction is not needed in this paper.

Later in [8], it has been proven that the same set of rules is actually complete for the $\pi/2^\bullet$ fragment. In fact, using the proof methods from [10], one can prove an even stronger result:

Theorem 1. *Let $D_1(\alpha)$ and $D_2(\alpha)$ be two ZX-diagrams linear in $\alpha = \alpha_1, \dots \alpha_k$ with constants in $\frac{\pi}{2^\bullet}\mathbb{Z}$.*

If $[\![D_1(\alpha)]\!] = [\![D_2(\alpha)]\!]$ for all values of α, then $ZX \vdash D_1(\alpha) = D_2(\alpha)$ for all values of α.

By a diagram linear in α, we mean that every angle appearing in the diagram is a linear combination with integer coefficients of the angles α_i, possibly with a constant term in $\frac{\pi}{2^\bullet}\mathbb{Z}$. The exact definition may be found in [10]. While the theorem was only proven for the $\pi/4$ fragment in [10], it is easy to see that the same method of proof gives the result for this larger fragment.

1.3 The $\mathbb{Q}\pi$-fragment

The set of axioms of Figure 1 is not enough for completeness of bigger fragments of the ZX-calculus and additional axioms are needed.

In [8], the authors have introduced a "meta-axiom" to obtain a set of rules complete for the $\mathbb{Q}\pi$ fragment.

If one does not want meta-axioms, one can see from the same article that the set of axioms represented in Figure 2 is enough to obtain a complete set of rules: If two diagrams D_1, D_2 with rational angles are equal, then $ZX \cup \{CYC_p, p \geq 3\} \vdash D_1 = D_2$.

This set of rules relies on an additional generator, the triangle generator, which is related to the right side of the (BW) rule:

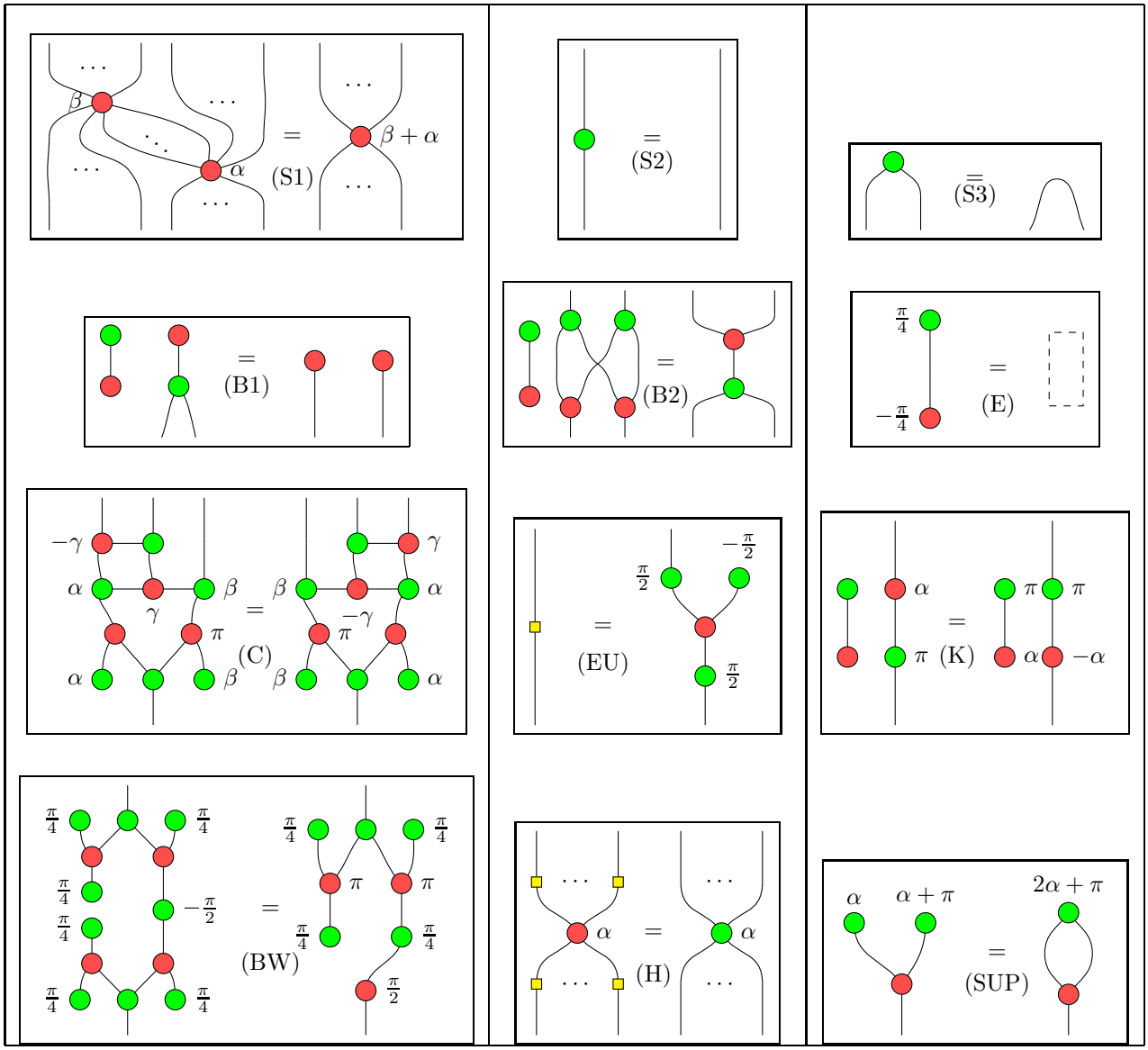


Figure 1: Rules

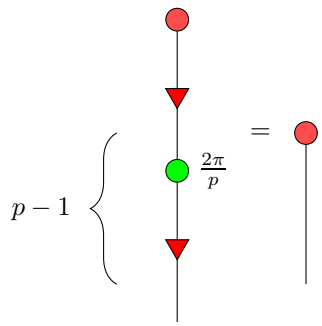
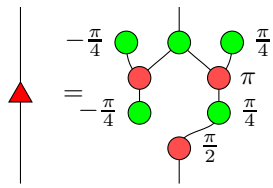


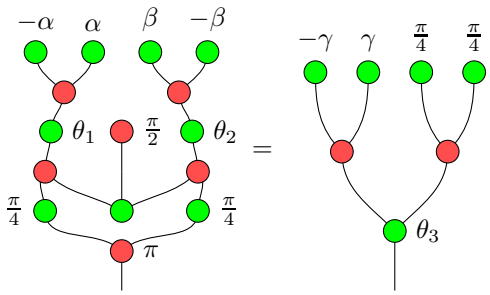
Figure 2: The cyclotomic rules (CYC_p).



The standard interpretation of this new generator is the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

1.4 The general fragment

Adding the cyclotomic axioms is again not enough to obtain completeness for the general fragment. An additional axiom, presented in Figure 3 was introduced in [10], and it is proven that this new axiom is sufficient to obtain a complete axiomatisation (Another axiomatisation, relying on much more axioms, was also given independently in [7]).



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

Figure 3: The general rule (A).

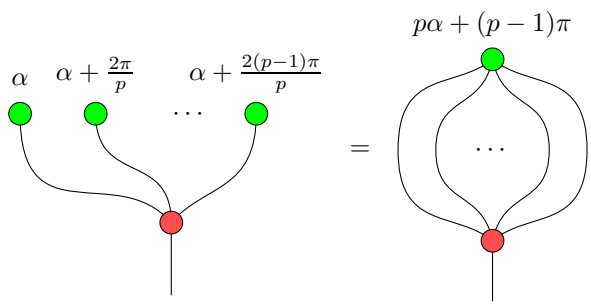
Compared to the other rules, it is important to note that this one cannot be

applied everywhen, but only if the angles satisfy the technical condition stated on the rule.

1.5 Results

We are now ready to state the main results of the paper.

The results are twofold. First, we prove that the ugly rule of Figure 2 can be represented by the well known generalized supplementarity rule. This rule was introduced in [11] and is the content of Figure 4.



(SUP_p)

Figure 4: The generalized supplementarity rules (SUP_p).

The result may be stated as follows: For any prime number p, $ZX \cup \{SUP_p\} \vdash CYC_p$. It is interesting to note that the proof uses complicated angles: To prove CYC_{11} for instance, our proof uses diagrams involving the angle $\pi/32$.

Our second series of results concern the other ugly rule of Figure 3. This rule is the only rule that is nonlinear and involves a precondition to be tested. This rule is known to be necessary, but we are interested here in what can be proved without this rule.

Here are our results:

- An equality $D_1 = D_2$ is provable without rule (A) iff it is a specialization of a more general diagram equality $D'_1(\alpha_1, \alpha_2 \ldots, \alpha_n) = D'_2(\alpha_1, \alpha_2, \ldots \alpha_n)$ with rational angles, that is:
  - For all values of α_i, $ZX \vdash D'_1(\alpha_1, \alpha_2 \ldots, \alpha_n) = D'_2(\alpha_1, \alpha_2, \ldots \alpha_n)$
  - D'_1 and D'_2 use, apart from $\alpha_1 \ldots \alpha_n$, only rational angles.
  - For some value of $\alpha_1 \ldots \alpha_n$, D_1 and D_2 are equal respectively to $D'_1(\alpha_1, \alpha_2 \ldots \alpha_n)$ and $D'_2(\alpha_1, \alpha_2 \ldots \alpha_n)$.
- An equality $D_1 = D_2$ is provable without rule (A) iff it is a "limit" of diagram equalities involving only rational angles: There exists two sequences of diagrams D_1^n and D_2^n with rational angles s.t.

- For all n, $ZX \vdash D_1^n = D_2^n$
- $D_1^n \xrightarrow{n\to\infty} D_1$
- $D_2^n \xrightarrow{n\to\infty} D_2$

Convergence here is to be understood as point-wise convergence of angles: Diagrams D_1^n and D_2^n are structurally identical to D_1 and D_2, but with different angles, that converge to the real angles when n goes to infinity.

- As a consequence of the previous result, we give a complete characterization of all equalities related to the Euler decomposition that are provable without rule (A). This list is not surprising and contains all usual suspects.

2 Cyclotomic Supplementarity as a sufficient rule

In this section, we will prove that the ZX-calculus as presented in Figure 1 together with the supplementarity rules (SUP_p) of Figure 4 is a complete axiomatisation of the rational fragment of the ZX-calculus.

The article [8] introduced a meta-rule to make the ZX-calculus complete for the rational fragment. However, it is also clear from the article that the set of rules CYC_p gives also a complete axiomatisation:

Theorem 2 ([8])**.** *The axioms of ZX, as presented in Figure 1, together with the axioms (CYC_p) for prime numbers p as presented in Figure 4 is a complete axiomatisation of the rational fragment of the ZX-calculus.*

We will prove in this section that we can replace the cyclotomic axioms CYC_p by the supplementarity axioms:

Theorem 3. *Let p be an odd prime number. Then $ZX \cup \{SUP_p\} \vdash CYC_p$.*

We now proceed to the proof of the theorem. In all the following, p is fixed to some odd prime number.

We will first explain informally the structure of the proof. If terms of interpretation, the supplementarity rule SUP_p is stating that for all α,

$$\begin{pmatrix} P_1(e^{i\alpha}, e^{i\beta}) \\ P_2(e^{i\alpha}, e^{i\beta}) \end{pmatrix} = \begin{pmatrix} P_3(e^{i\alpha}, e^{i\beta}) \\ P_4(e^{i\alpha}, e^{i\beta}) \end{pmatrix}$$

where P, Q, P', Q' are some polynomials, and $\beta = 2\pi/p$.

The cyclotomic rule CYC_p is stating that

$$\begin{pmatrix} 1 \\ R(e^{i\beta}) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

for some polynomial R and $\beta = 2\pi/p$.

To obtain CYC_p from SUP_p, we will proceed in two steps:

- First, rewrite SUP_p in such a way that the new diagram equality can be interpreted, as saying, in terms of interpretation that:

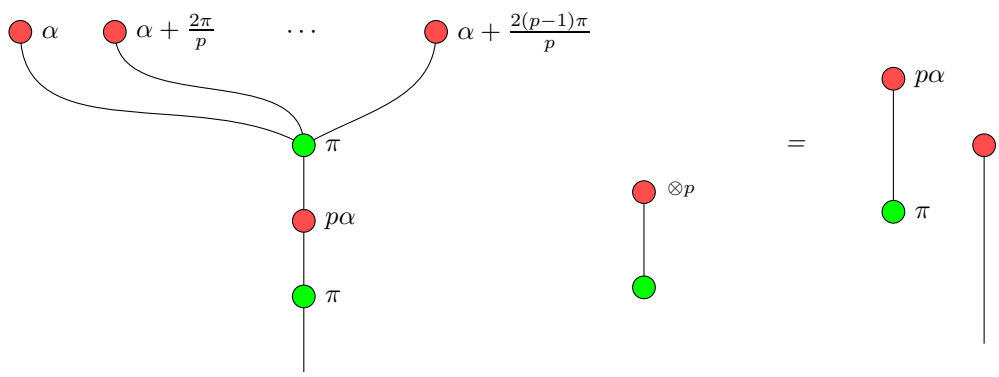
$$\begin{pmatrix} 1 \\ S(e^{i\alpha}, e^{i\beta}) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

  when $\beta = 2\pi/p$.

- It turns out that the polynomial R involved in the cyclotomic rule CYC_p is actually one of the terms of the polynomial S. In the next step, we will explain how this term can be extracted diagrammatically, which will prove the result.

Now, for the first step. Using elementary manipulation, we get to rewrite the supplementarity in the form

Lemma 1. *The following diagram equation is provable in $ZX \cup \{SUP_p\}$:*



In terms of matrices, this can be interpreted as the following equality:

$$\frac{1}{2}\begin{pmatrix} (1+e^{ip\alpha})\prod_k(e^{i\alpha+2k\pi/p}+1)+(1-e^{ip\alpha})\prod_k(e^{i\alpha+2k\pi/p}-1) \\ -(1-e^{ip\alpha})\prod_k(e^{i\alpha+2k\pi/p}+1)-(1+e^{ip\alpha})\prod_k(e^{i\alpha+2k\pi/p}-1) \end{pmatrix} = \begin{pmatrix} 2e^{pi\alpha} \\ 0 \end{pmatrix}$$

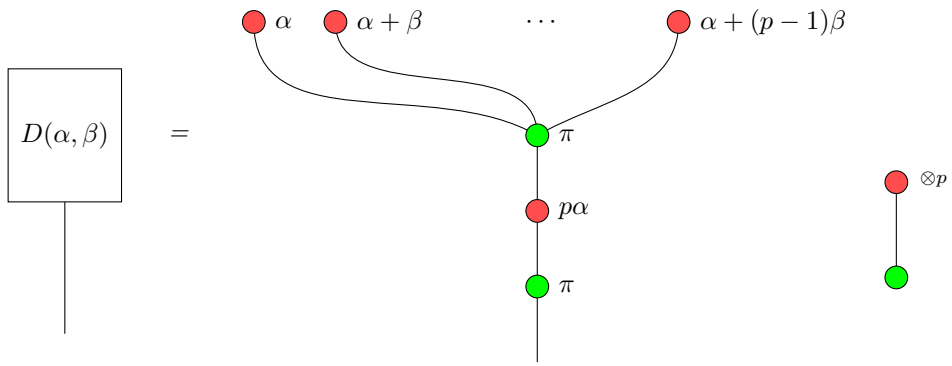
or more simply

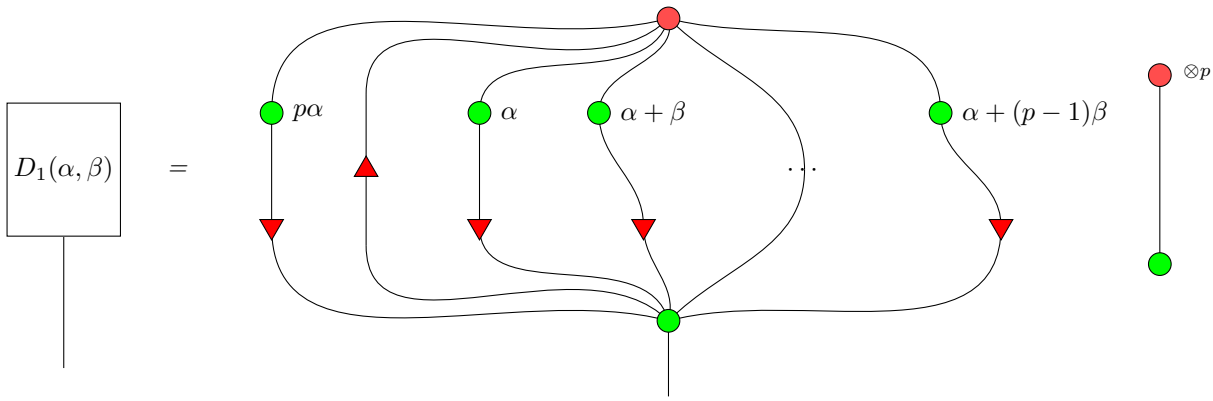
$$\begin{pmatrix} P(e^{i\alpha}) \\ Q(e^{i\alpha}) \end{pmatrix} = \begin{pmatrix} 2e^{pi\alpha} \\ 0 \end{pmatrix}$$

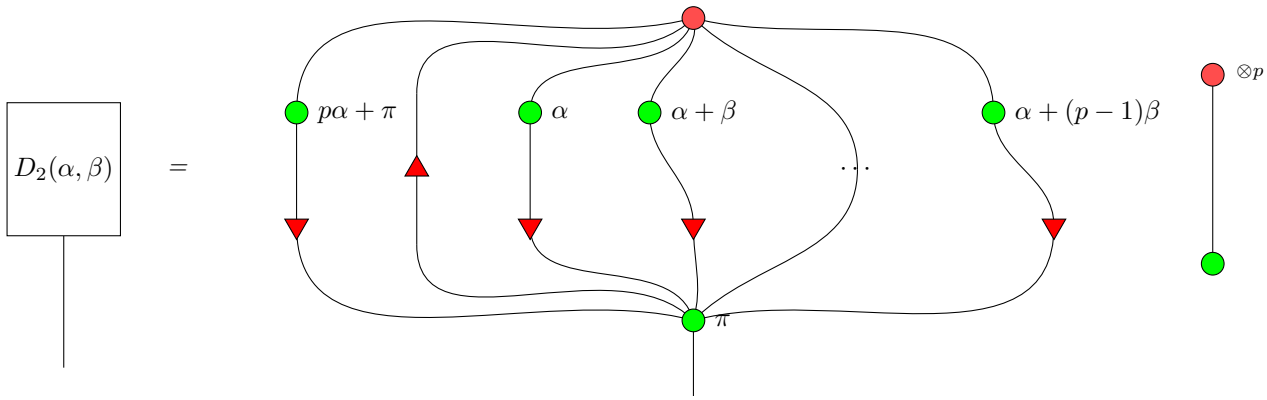
for some polynomials P and Q. The next step is to split this diagram into two diagrams, one that speaks of P, and one that speaks of Q.

For this we introduce three diagrams. D is the generalization of the supplementarity diagrams, and D_1, D_2 somehow corresponds to the two polynomials.

Definition 1. *We define three (families of) diagrams as follows:*


$D(\alpha,\beta)$
=
α
$\alpha+\beta$
$\cdots$
$\alpha+(p-1)\beta$
π
$p\alpha$
π
$\otimes p$


$D_1(\alpha,\beta)$
=
$p\alpha$
α
$\alpha+\beta$
$\cdots$
$\alpha+(p-1)\beta$
$\otimes p$


$D_2(\alpha,\beta)$
=
$p\alpha+\pi$
α
$\alpha+\beta$
$\cdots$
$\alpha+(p-1)\beta$
π
$\otimes p$

The three diagrams have the following interpretations:

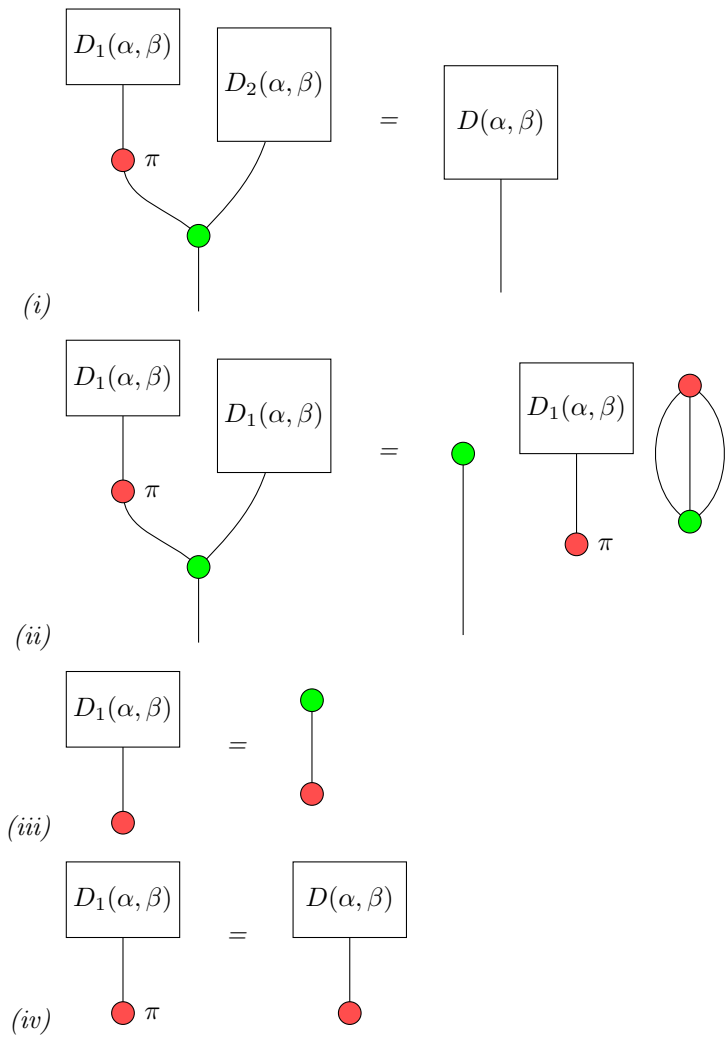
$$[\![D(\alpha,\beta)]\!] = \frac{1}{2}\begin{pmatrix} (1+e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}+1)+(1-e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}-1) \\ -(1-e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}+1)-(1+e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}-1) \end{pmatrix} = \begin{pmatrix} P(e^{i\alpha},e^{i\beta}) \\ Q(e^{i\alpha},e^{i\beta}) \end{pmatrix}$$

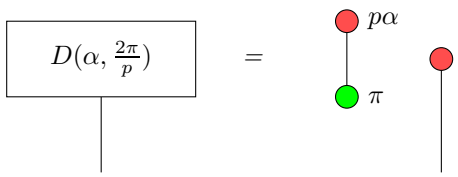
$$[\![D_1(\alpha,\beta)]\!] = \begin{pmatrix} 1 \\ \frac{1}{2}\left[(1+e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}+1)+(1-e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}-1)\right] \end{pmatrix} = \begin{pmatrix} 1 \\ P(e^{i\alpha},e^{i\beta}) \end{pmatrix}$$

$$[\![D_2(\alpha,\beta)]\!] = \begin{pmatrix} 1 \\ \frac{-1}{2}\left[(1-e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}+1)+(1+e^{ip\alpha})\prod_k(e^{i\alpha+k\beta}-1)\right] \end{pmatrix} = \begin{pmatrix} 1 \\ Q(e^{i\alpha},e^{i\beta}) \end{pmatrix}$$

We therefore have the following:

Proposition 1. *The following equations are provable in $ZX \cup \{SUP_p\}$:*

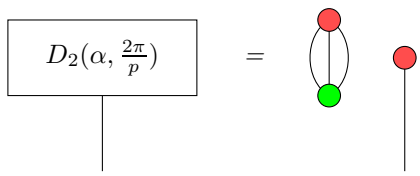


(v) 

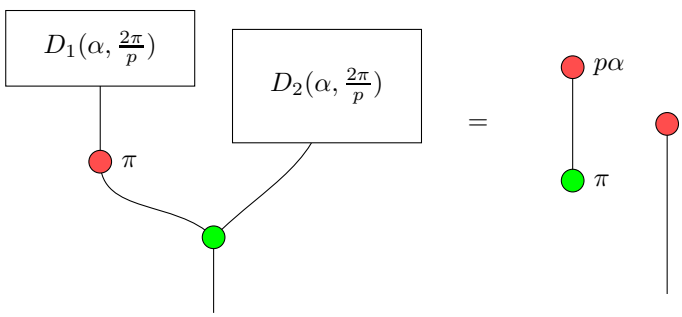
Proof. The first four are true for all α, β and are therefore provable by Theorem 1.

The last one is the supplementary equality in the form provided by the previous lemma. □

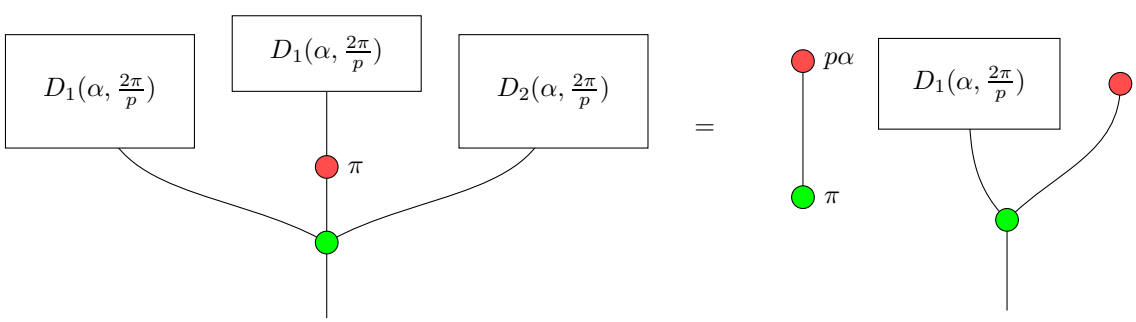
Proposition 2. *The following equation is provable in $ZX \cup \{SUP_p\}$:*



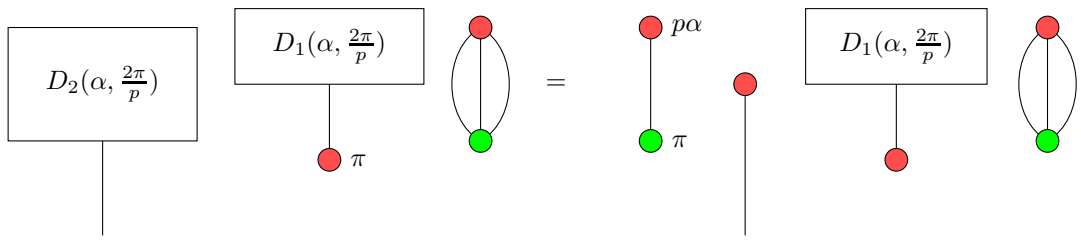
Proof. By putting (i) and (v) together we get:



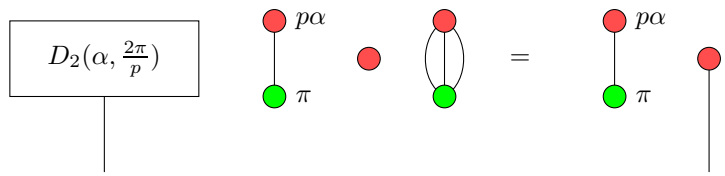
Therefore:



Applying (ii) on the left and simplifying the right term:



Now we apply (iv) then (v) on the left and (iii) on the right:



which gives the result. □

Now the advantage of the diagram D_2 over the original supplementarity equation is that its interpretation is

$$\begin{pmatrix} 1 \\ Q(e^{i\alpha}, e^{i\frac{2\pi}{p}}) \end{pmatrix}$$

That is, at least one term of the matrix is fixed to a value that doesn't depend on $e^{i\alpha}$ (and is nonzero).

Now, the equality of the previous proposition means that $Q(e^{i\alpha}, e^{i\frac{2\pi}{p}})$ is identically 0, which means that each coefficient of the polynomial (in $e^{i\alpha}$) is equal to 0.

It is easy to see that the first coefficient of $Q(e^{i\alpha}, e^{i\beta})$ is 0 (independently of β).

Notice that the term of degree 1 (in $e^{i\alpha}$) of the polynomial $Q(e^{i\alpha}, e^{i\beta})$ is exactly $-1 - e^{i\beta} - e^{i2\beta} - \cdots - e^{i(p-1)\beta}$.

If we find a way to retrieve the term of degree 1 of a polynomial with a diagrammatic construction, we are close to our result.

This is done with the following result:

Proposition 3. *Let $P(X) = \sum_{r \leq d} a_r X^r$ be a polynomial of degree d. Choose n such that $2^n > d$.*

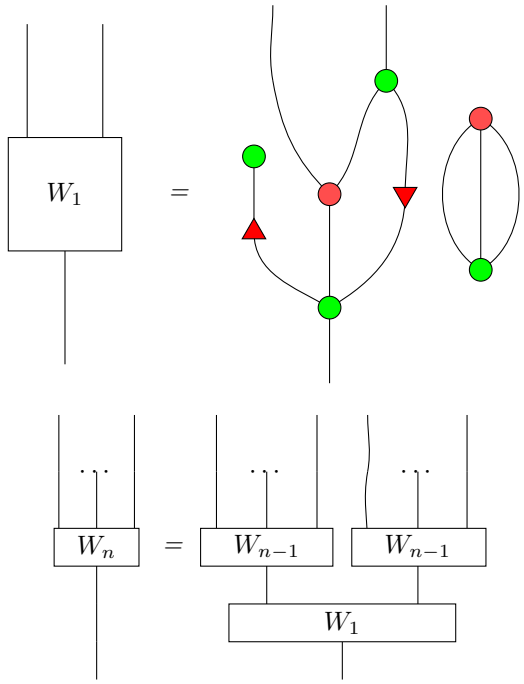
Then

$$\sum_{k=0}^{2^n-1} \frac{P(e^{2ki\pi/2^n})}{e^{2ki\pi/2^n}} = 2^n a_1$$

Proof. Indeed $\sum_k e^{2irk\pi/2^n} = 0$ if $r \neq 0 \mod 2^n$ and $\sum_k e^{2irk\pi/2^n} = 2^n$ otherwise. □

We will use this idea to extract diagrammatically the first coefficient of our polynomial.

Definition 2. *We define recursively a family of diagrams W_n as follows:*



For reference, here are the interpretations of W_1 and W_2:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/4 & 1/4 & 0 & 1/4 & 0 & 0 & 0 & 1/4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

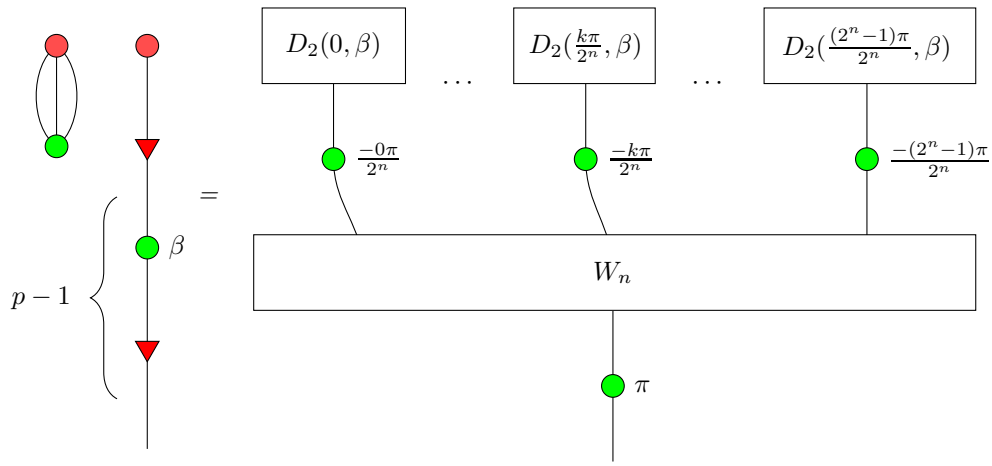
It is easy to see by induction that W_n is the matrix whose first row contains a 1 in position 0 and whose second row contains 2^{-n} in position 2^i for all i.

The astute reader may remark that W_n is a slight variant of the W-state presented e.g. in the ZW calculus [6].

The previous proposition then gives us immediately the following:

Proposition 4. *Let n be big enough s.t. $2^n > 2p$.*

The following equality is provable in ZX:

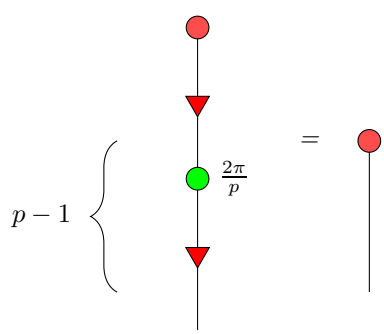


(the brace means this part of the diagram should be repeated $p-1$ times).

Proof. By the previous proposition, the two diagrams have the same interpretations (the interpretation of D_2 is a polynomial of degree $2p < 2^n$ in $e^{i\alpha}$).

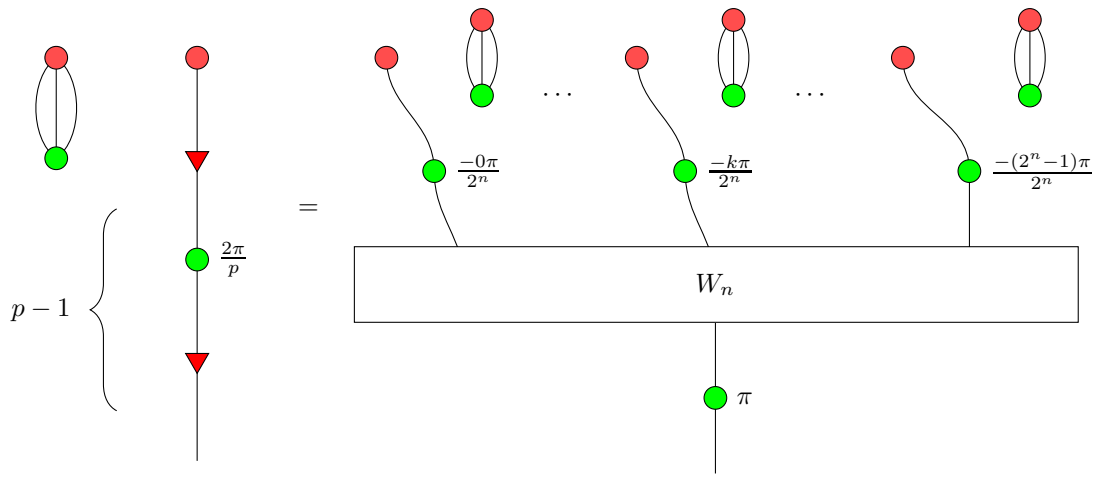
Now these two diagrams are (apart from β) diagrams where all angles are of the form $k\pi/2^n$ and the two diagrams have the same interpretations for all possible values of β. Therefore the equality is provable by Theorem 1. □

Proposition 5. *The following is provable in $ZX \cup \{SUP_p\}$.*

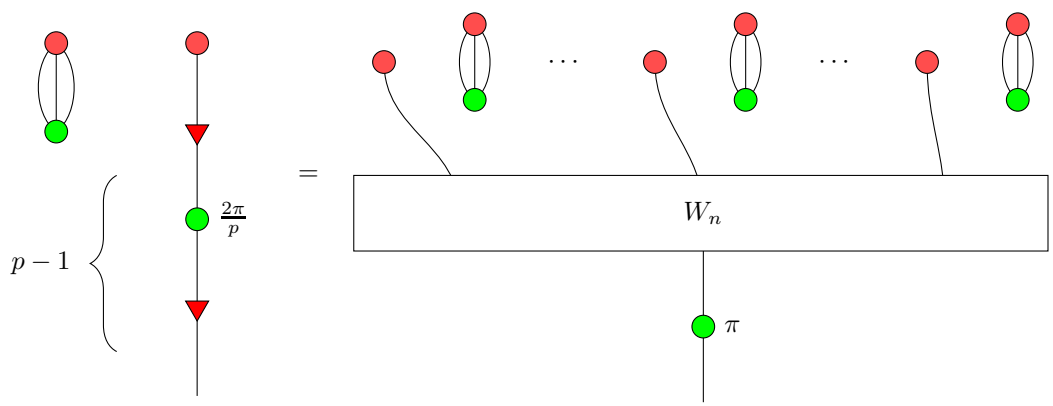


That is, $ZX \cup \{SUP_p\} \vdash CYC_p$.

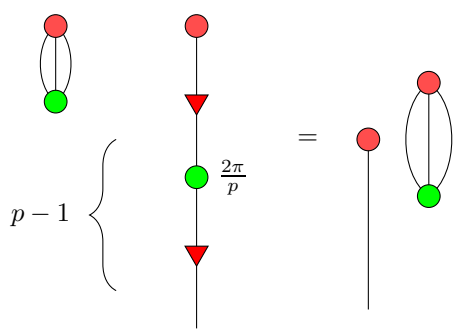
Proof. By the previous proposition and Proposition 2:



Therefore:



And therefore:



where the last equality comes from the fact the two right terms have the same interpretations and are in the fragment $\pi/4$ and therefore are provably equal by completeness. $\square$

3 Equalities provable without rule (A)

In this section we characterize which diagram equalities $D_1 = D_2$ can be proven without rule (A).

This section will primarily deal with vectors of variables. The notation $\overline{a}$ in this section will denote the vector $a_1 \dots a_n$. The size of the vector is usually either irrelevant or obvious from the context. On some occasions, we will use the notation $(\overline{a}_i)_{i \in I}$ which is not a typo, but refers to a tuple of vectors.

Greek letters will represent variables. By an abstract diagram $D_1(\overline{\alpha})$ we mean a diagram of the ZX-calculus where some of the angles inside the green and red nodes are replaced by some of the variables α_i. We say the diagram is rational if the other angles are in $\mathbb{Q}\pi$. If $\overline{x}$ is a vector of real numbers of the same size as $\overline{\alpha}$, we denote by $D_1(\overline{x})$ the diagram where the variable α_i is replaced by the real number x_i.

Many of the results of this section are based on the following remark. Consider two abstract diagrams $D_1(\overline{\alpha})$ and $D_2(\overline{\alpha})$. Then the set

$$S = \{\overline{x} \in \mathbb{R}^l | \, [\![D_1(\overline{x})]\!] = [\![D_2(\overline{x})]\!]\}$$

has a special structure that can be exploited. This special structure is best evidenced by not seeing S as a subset of (vectors of) reals, but as points of the unit circle, i.e. by investigating:

$$S' = \{e^{i\overline{x}} | \, [\![D_1(\overline{x})]\!] = [\![D_2(\overline{x})]\!]\}$$

We will then rely on classical results from algebraic group theory and diophantine geometry. The two main results we will use is the fact that any linear commutative compact groups is a quasi-torus [16] (which is well-known in linear algebraic group theory, or in Lie theory, and easy to prove once all relevant definitions are given), and the Mordell-Lang conjecture on rational points on algebraic varieties (which is lesser known and whose proof is much harder, even in our context [12]).

To simplify the exposition, we will state these classical results only when necessary, and only in terms of real numbers (or in terms of numbers in the quotient space $\mathbb{R}/2\pi\mathbb{Z}$ which is compact), but the reader should be aware that the results in the cited litterature are usually expressed in terms of points of the unit circle.

To begin our investigation, we note that we can do the same trick as in the beginning of the paper: From the fact $ZX \cup \{SUP_p, p \geq 3\}$ is complete for the rational fragment, we deduce that all *linear* equalities are also provable.

It will be useful in what follows to state this theorem precisely, which needs a few notations.

By an affine form, we mean a function of the form $f(\overline{\alpha}) = f(\alpha_1, \ldots, \alpha_k) = p_0 + \sum p_i \alpha_i$ where all coefficients p_i are integer. The form is *rational* if p_0 is a rational angle. It is linear if $p_0 = 0$. By a (rational) affine transformation F, we mean a finite sequence of (rational) affine forms $f_1 \ldots f_n$, and we will write $F(\overline{\alpha})$ for $f_1(\overline{\alpha}), \ldots f_n(\overline{\alpha})$. Notice that a linear affine transformation is essentially a matrix with integer coefficients.

Theorem 4. *Let $D_1(\overline{\alpha})$ and $D_2(\overline{\beta})$ be two abstract rational ZX-diagrams.*

Let F, G be two rational transformations s.t. for all (vector of) angles $\overline{x}$,

$$[\![D_1(F(\overline{x}))]\!] = [\![D_2(G(\overline{x}))]\!]$$

Then for all angles $\overline{x}$,

$$ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(F(\overline{x})) = D_2(G(\overline{x}))$$

This theorem follows mutatis mutandis from the similar theorem in [10].

Our first result in this section is that this previous theorem is somehow an if and only if:

Theorem 5. *Let $D_1(\overline{\alpha})$ and $D_2(\overline{\beta})$ be two abstract rational diagrams of the ZX-calculus*

Let $\overline{x}$ and $\overline{y}$ be two (vectors of) angles.

Then the following are equivalent:

(i) $ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x}) = D_2(\overline{y})$

(ii) There exists n s.t. for all positive integers $k \equiv 1 \mod n$:

$$[\![D_1(k\overline{x})]\!] = [\![D_2(k\overline{y})]\!]$$

(iii) There exist rational affine transformations F, G s.t.

- *For all values of $\overline{z}$, we have*

$$[\![D_1(F(\overline{z}))]\!] = [\![D_2(G(\overline{z}))]\!]$$

- *There exist some value of $\overline{z}$ s.t. $\overline{x} = F(\overline{z})$ and $\overline{y} = G(\overline{z})$*

What this theorem means is that there is no coincidence: If a diagram equality is provable without the rule (A), then the diagram equality is not provable only for the angles that appear in it, but (ii) is also provable if all angles are multiplied by some constants and (iii) the diagram equality is actually an instance of a much more general diagram equality.

We note that it is likely that *(i)* $\rightarrow$ *(iii)* could be proven directly by a cumbersome induction on the structure of the proof. However, we will adopt here an algebraic approach that will be useful for the next theorem.

Proof. $(iii) \to (i)$ is exactly the statement of the previous theorem.

Now let's prove $(i) \to (ii)$.

First, as a diagram with variables $\overline{\alpha}$ is a fortiori a diagram with variables $\overline{\alpha}$ and $\overline{\beta}$, we may suppose wlog that D_1 and D_2 are two diagrams with the same set of variables $\overline{\alpha}$ and that $\overline{x} = \overline{y}$.

Now suppose that $ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x}) = D_2(\overline{x})$. As a proof is finite, only finitely many axioms of the form SUP_p are used. Let q be an upper bound of the denominators p of the rational angles $k\pi/p$ that are involved in the diagrams D_1 and D_2 and on the numbers p s.t. SUP_p is used in the proof.

In particular, we have $ZX \cup \{SUP_p, p < q\} \vdash D_1(\overline{x}) = D_2(\overline{x})$.

Let $n = 8q!$ and let k be an integer.Consider the two diagrams $D_1(\overline{x})$ and $D_2(\overline{x})$ where all angles are multiplied by $kn + 1$.

By our choice of q, it is easy to see that all rational coefficients inside D_1 and D_2 do not change. Therefore the two new diagrams we obtain are actually equal to $D_1((kn+1)\overline{x})$ and $D_2((kn+1)\overline{x})$

Furthermore, by our choice of q, all axioms of ZX and $SUP_p, p < q$ remain valid where their angles are multiplied by $kn + 1$. As a consequence, we have for all k,

$$ZX \cup \{SUP_p, p < q\} \vdash D_1((kn+1)\overline{x}) = D_2((kn+1)\overline{x})$$

In particular for all positive values of k, $[\![D_1((kn+1)\overline{x})]\!] = [\![D_2((kn+1)\overline{x})]\!]$.

Now let's prove $(ii) \to (iii)$. As before we may suppose wlog that D_1 and D_2 are two diagrams with the same set of variables $\overline{\alpha}$ and that $\overline{x} = \overline{y}$. Let m be the size of $\overline{x}$.

Let $S = \{(kn+1)\overline{x}, k \geq 0\}$, seen as a subset of $(\mathbb{R}/2\pi\mathbb{Z})^m$ and X be its topological closure. Each individual coefficient of the interpretation of $D_1(\overline{\alpha})$ and $D_2(\overline{\alpha})$ is an exponential polynomial in $\overline{\alpha}$, and therefore is continuous. As a consequence, for all $\overline{z} \in X$, we have $[\![D_1(\overline{z})]\!] = [\![D_2(\overline{z})]\!]$.

It remains to know what X looks like. Such sets have been extensively studied in the context of algebraic groups. To be more exact, $\{kn\overline{x}, k \geq 0\}$ is a monoid, and its closure Y is a compact subgroup of $(\mathbb{R}/2\pi\mathbb{Z})^m$, and each such group is a linear quasi-torus[16], which means that there exists a rational linear transformation F and finitely many (vectors of) rational numbers $(\overline{l}_i)_{i\in I}$ s.t.

$$Y = \bigcup_{i\in I} \{F(\overline{z}) + \overline{l}_i, \overline{z} \in (\mathbb{R}/2\pi\mathbb{Z})^m\}$$

It is a routine exercise[1] to show that this implies the same result for $X = x + Y$:

$$X = \bigcup_{i\in I} \{F(\overline{z}) + l'_i, \overline{z} \in (\mathbb{R}/2\pi\mathbb{Z})^m\} = \bigcup_{i\in I} \{F_i(\overline{z}), \overline{z} \in (\mathbb{R}/2\pi\mathbb{Z})^m\}$$

for some rational forms F_i.

[1] Notice that $nx \in Y$ therefore $nx = F(\overline{w}) + \overline{l}_i$ for some $\overline{w}$ and some i thus $x = F(\overline{w}/n) + \overline{\ell}$ for some (vector of) rational angles $\overline{\ell}$. The result follows by a change of variables

As a nontrivial example, let $\overline{x} = (\sqrt{2}, 2\sqrt{3}, \pi/3 + \sqrt{2}, \sqrt{2} + \sqrt{3})$ and $n = 3$. Then one can prove with some work (using linear independence of $\sqrt{2}$, $\sqrt{3}$ and π) that the topological closure Y of $\{kn\overline{x}, k \geq 0\}$ can be defined by $Y = \{(t, 2u, t, u + t), (t, u) \in (\mathbb{R}/2\pi\mathbb{Z})^m\} \cup \{(t, 2u, \pi + t, t + u), (t, u) \in (\mathbb{R}/2\pi\mathbb{Z})^m\}$. Similarly, one can prove that the topological closure X of $S = \{kn\overline{x}+1, k \geq 0\}$ is $X = \{(t, 2u, \pi/3 + t, u + t), (t, u) \in (\mathbb{R}/2\pi\mathbb{Z})^m\} \cup \{(t, 2u, 4\pi/3 + t, t + u), (t, u) \in (\mathbb{R}/2\pi\mathbb{Z})^m\}$.

Now $\overline{x} \in X$. Therefore there exists i s.t. $\overline{x} \in \{F_i(\overline{z}), \overline{z} \in (\mathbb{R}/2\pi\mathbb{Z})^m\}$. Then

- $\{F_i(\overline{z}), \overline{z} \in (\mathbb{R}/2\pi\mathbb{Z})^m\} \subseteq X$ and therefore $[\![D_1(F(\overline{z}))]\!] = [\![D_2(F(\overline{z}))]\!]$ for all values of $\overline{z}$.
- $x \in \{F_i(\overline{z}), \overline{z} \in (\mathbb{R}/2\pi\mathbb{Z})^m\}$, therefore there exists $\overline{z}$ s.t $x = F_i(\overline{z})$.

$\square$

Corollary 1. *Let $D_1(\overline{\alpha})$ and $D_2(\overline{\beta})$ be two rational diagrams of the ZX-calculus*

Suppose that $ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x}) = D_2(\overline{y})$ for some angles $\overline{x}, \overline{y}$.

Then there exist two sequences of (vectors of) rational angles $\overline{x^i}, \overline{y^i}$ that converges respectively to $\overline{x}$ and $\overline{y}$ s.t. for all values of i,

$$ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x^i}) = D_2(\overline{x^i})$$

Proof. Use *(i)* $\rightarrow$ *(iii)* in the previous theorem, and choose a sequence of rational angles $\overline{z}^i$ that converges to $\overline{z}$ and take $\overline{x}^i = F(\overline{z}^i)$ and $\overline{y}^i = G(\overline{z}^i)$. □

This is actually a characterization:

Theorem 6. *Let $D_1(\overline{\alpha})$ and $D_2(\overline{\beta})$ be two rational diagrams of the ZX-calculus.*

Let $\overline{x^i}, \overline{y^i}$ be two sequences of rational angles that converge respectively to $\overline{x}$ and $\overline{y}$ and s.t. for all values of i,

$$\left[\!\left[D_1(\overline{x^i})\right]\!\right] = \left[\!\left[D_2(\overline{y^i})\right]\!\right]$$

Then

$$ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x}) = D_2(\overline{y})$$

Corollary 2. *A limit of provable equalities is again a provable equality.*

Proof ot the Corollary. Let $\overline{x^i}, \overline{y^i}$ be two sequences of angles that converge respectively to $\overline{x}$ and $\overline{y}$ and s.t. for all values of i,

$$ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x^i}) = D_2(\overline{y^i})$$

By the previous corollary, we may find, for each i, *rational* angles arbitrarily close to $\overline{x^i}$ and $\overline{y^i}$ s.t. the equality remains provable for these angles.

But this implies that we can find rational angles arbitrarility close to $\overline{x}$ and $\overline{y}$ s.t. the equality remains provable for these angles. Which implies by the previous theorem that $ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x}) = D_2(\overline{y})$ □

Proof of the Theorem. As before, by seeing D_1 and D_2 as diagrams over a bigger set of variables, we may suppose wlog that $\overline{x^i} = \overline{y^i}$.

Now, the key idea is to consider

$$X = \{\overline{z} \in (2\pi\mathbb{Q}/2\pi\mathbb{Z})^m \,|\, [\![D_1(\overline{z})]\!] = [\![D_2(\overline{z})]\!]\}$$

X is therefore the set of (vectors of) rational angles for which the diagram equality is true. We note that all $\overline{x^i}$ are in X.

Now take

$$Y = \{e^{i\overline{z}}, z \in X\}$$

Each individual coefficient of D_1 and D_2 are polynomials in $e^{iz_1} \dots e^{iz_l}$. The set Y itself can therefore be seen as the intersection between the set of zeroes of some polynomials, and the set of (vectors consisting of) roots of unity.

Such sets have been widely used in the context of the Mordell-Lang conjecture, and it is known that each of them is the finite union of translates of algebraic groups, which is in our particular case a result of Laurent [12]. In our formalism, this can be rewritten as follows: There exists finitely many rational affine transformations $(F_j)_{j\in J}$ s.t. (as before)

$$X = \bigcup_{j\in J} \{F_j(\overline{z}), \overline{z} \in (2\pi\mathbb{Q}/2\pi\mathbb{Z})^m\}$$

Now as J is finite, infinitely many of the $\overline{x^i}$ are in the same set, say F_j. Write $S = \{F_j(\overline{z}), \overline{z} \in (2\pi\mathbb{Q}/2\pi\mathbb{Z})^m\}$. By taking a subsequence, we may suppose that all of the $\overline{x}^i$ are in S.

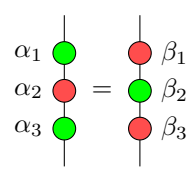
- $S \subseteq X$. Therefore for all $\overline{w} \in S$, $[\![D_1(\overline{w})]\!] = [\![D_2(\overline{w})]\!]$.
- Therefore for all $\overline{z} \in (2\pi\mathbb{Q}/2\pi\mathbb{Z})^m$, $[\![D_1(F_j(\overline{z}))]\!] = [\![D_2(F_j(\overline{z}))]\!]$. By continuity this is also true for any $\overline{z} \in (\mathbb{R}/2\pi\mathbb{Z})^m$.
- Therefore by Theorem 4, the equality is not only true but provable: For all $\overline{z}$, we have $ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(F_j(\overline{z})) = D_2(F_j(\overline{z}))$
- Now it remains to show that there exists some $\overline{z}$ s.t. $F_j(\overline{z}) = \overline{x}$ which will prove that $ZX \cup \{SUP_p, p \geq 3\} \vdash D_1(\overline{x})) = D_2(\overline{x})$. But this is obvious: For each i, as $\overline{x^i} \in S$, we may find $\overline{z^i} \in (\mathbb{R}/2\pi\mathbb{Z})^m$ s.t. $F_j(\overline{z}^i) = \overline{x}^i$ and we may suppose (upto a converging subsequence) that $\overline{z}^i$ converges to some $\overline{z}$. And for this particular $\overline{z}$ we have $F_j(\overline{z}) = \overline{x}$.

□

4 Applications to Euler transforms

As an application of the previous result, we will characterize in this section the set of Euler equalities that are provable without rule (A).

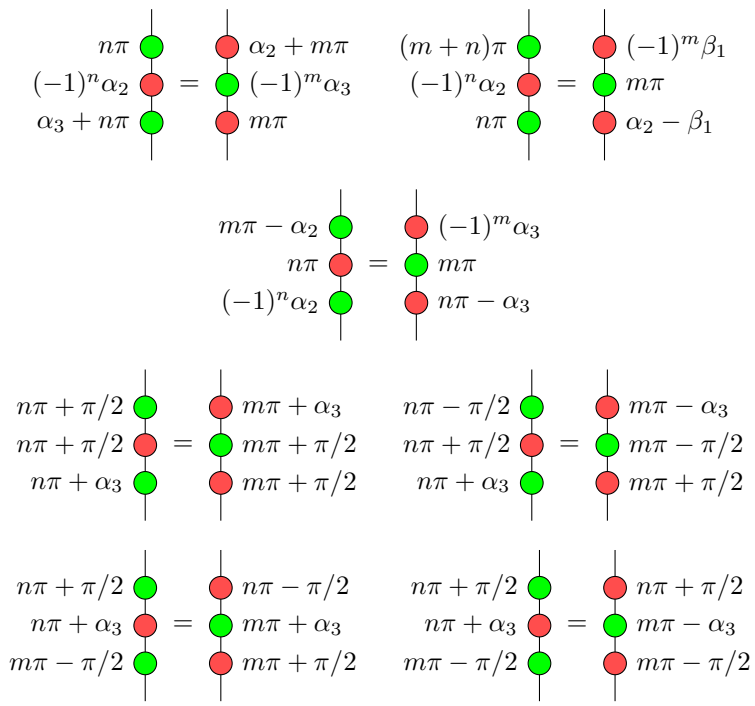
By a Euler equality, we mean an equality of the form:



possibly also involving (nonzero) scalars. For simplicity of the presentation, we will not represent the scalars in the proofs.

Our main result is the following:

Theorem 7. *The only Euler equalities that are provable in $ZX \cup \{SUP_p, p \geq 3\}$ are:*

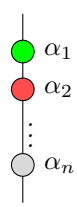


and their color-swapped variants.

Our method to prove the result is obvious from the previous sections: We only have to find the Euler equalities satisfied by rational angles to deduce the equalities satisfied by arbitrary angles.

To find Euler equalities for rational angles, we will use the following result, original formulated in the context of tilings[2]:

Theorem 8 ([18])**.** *Let $\alpha_1 \dots \alpha_n \in \mathbb{Q}\pi$ s.t. the diagram*[3]



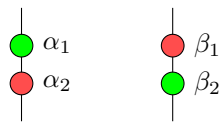
represents the identity matrix up to a scalar. Then either there exists i s.t. $\alpha_i \in \{0, \pi\}$ or there exists i s.t. $\{\alpha_i, \alpha_{i+1}\} \subseteq \{\pi/2, -\pi/2\}$.

Now we can begin the proof of the theorem. We first investigate the case of equalities involving only four nodes:

[2]The astute reader should remark that this theorem subsumes most of the results of Backens [1] and Mastumoto-Amano [14].

[3]the last node is green if n is even, and red otherwise.

Proposition 6. *Suppose that the two diagrams*



represents the same matrix up to a scalar.

Then either ($\alpha_1 = \beta_2 = n\pi$ and $\beta_1 = (-1)^n\alpha_2$) or ($\alpha_2 = \beta_1 = n\pi$ and $\beta_2 = (-1)^n\alpha_1$).

Proof. The two diagrams represents respectively the matrices:

$$\frac{1}{2}\begin{pmatrix} e^{i\alpha_2}+1 & (1-e^{i\alpha_2})e^{i\alpha_1} \\ 1-e^{i\alpha_2} & (1+e^{i\alpha_2})e^{i\alpha_1} \end{pmatrix}$$

and

$$\frac{1}{2}\begin{pmatrix} e^{i\beta_1}+1 & 1-e^{i\beta_1} \\ (1-e^{i\beta_1})e^{i\beta_2} & (1+e^{i\beta_1})e^{i\beta_2} \end{pmatrix}$$

- Suppose that $\alpha_2 = \pi$. Then we get immediately $\beta_1 = \pi$ so that the top-left coefficients are equal.

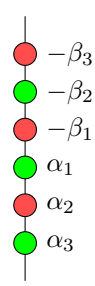
  The quotient of the bottom-left value by the top-right value should be equal in the two matrices, and we get $\beta_2 = -\alpha_1$.

- If $\alpha_2 = 0$, we get by a similar argument that $\beta_1 = 0$ and $\beta_2 = \alpha_1$.

- If $\alpha_2 \notin \{0, \pi\}$, we can look again at the two quotients (as the denominators are nonzero) and we get simultaneously $\beta_2 = \alpha_1$ and $\beta_2 = -\alpha_1$, and therefore $\beta_2 = \alpha_1 = 0$ or $\beta_2 = \alpha_1 = \pi$ from which we get the same conclusions as before by the red-green symmetry.

□

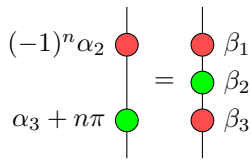
Proof ot the theorem. It is enough to find all equalities relating rational angles. Take such an equality. By slightly rewriting it, we see that the diagram



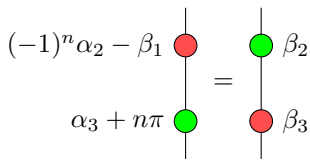
represents the identity matrix upto a scalar. By Theorem 8, one of the coefficient should be in $\{0, \pi\}$ or two consecutive coefficients are equal to $\pm\pi/2$.

The rest of the proof is just an enumeration of all possible cases.

- $\alpha_1 = n\pi$. Then the equation can be rewritten:



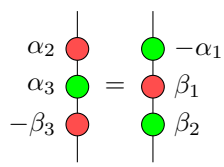
  and therefore



  upto a scalar. We therefore get the first two cases of the theorem by the previous proposition.

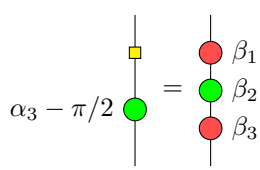
- The cases $\alpha_3 = n\pi, \beta_1 = n\pi, \beta_3 = n\pi$ are treated in the same way and give symmetric conditions.

- The cases $\alpha_2 = n\pi, \beta_2 = n\pi$ can be treated by rewriting the equality in the form

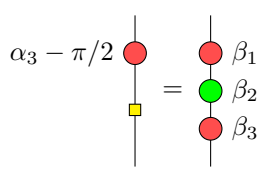


  and we recover one of the previous cases.

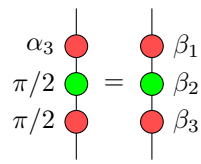
- $\alpha_1 = \pi/2$ and $\alpha_2 = \pi/2$. Then the equation can be rewritten:



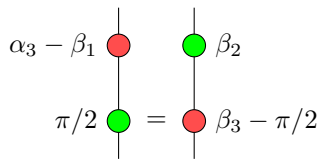
  and therefore



which gives

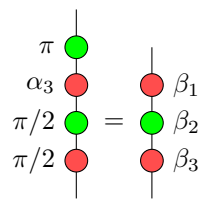


Finally:

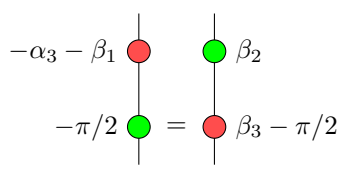


and we can apply the previous proposition. We obtain the fourth case of the theorem for $n = 0$ (notice that $(-1)^m \pi/2 = m\pi + \pi/2$).

- $\alpha_1 = -\pi/2$ and $\alpha_2 = -\pi/2$ is treated in a similar way and gives use the fourth case with $n = 1$.
- $\alpha_1 = -\pi/2$ and $\alpha_2 = \pi/2$. The same computation gives us:



and finally:



And we apply again the proposition.

- The case $\{\alpha_2, \alpha_3\} \subseteq \{\pi/2, -\pi/2\}$ is done in the same way. The case $\{\alpha_1, \beta_1\} \subseteq \{\pi/2, -\pi/2\}$ is done by rewriting the equality as before.

$\square$

5 Further work

The work that has been done for the Euler equalities can be also done for the rule (A) itself, to find for which angles rule (A) is actually provable without rule (A). The technical condition below rule (A) can be rewritten as a sum of 6 exponential terms, and has been investigated previously by Mann [13] and Conway and Jones[5] (see in particular Theorem 6). The most complicated equality with rational angles uses angles of the form $\pi/3$ and $\pi/5$.

Replacing the rule CYC_p (or the metarule) by the rule SUP_p gives a nicer set of rules for the rational fragment of the ZX-calculus. What remains is to find a nicer replacement for rule (A) for the full fragment. The obvious candidate is of course Euler equalities, but we do not know if adding Euler equalities to the rule of ZX is sufficient to prove rule (A) in its full generality.

References

[1] Miriam Backens. The ZX-calculus is complete for the single qubit Clifford+T fragment. In *Quantum Physics and Logic (QPL)*, pages 293–303, 2014.

[2] Miriam Backens. Making the stabilizer ZX-calculus complete for scalars. *Electronic Proceedings in Theoretical Computer Science*, 2015.

[3] Miriam Backens, Simon Perdrix, and Quanlong Wang. A simplified stabilizer ZX-calculus. In *QPL 2016*, 2016.

[4] Bob Coecke and Ross Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, 2011.

[5] J.H. Conway and A.J. Jones. Trigonometric diophantine equations. *Acta Arithmetica*, 1976.

[6] Amar Hadzihasanovic. A diagrammatic axiomatisation for qubit entanglement. In *Symposium on Logic in Computer Science (LiCS)*, pages 573–584, July 2015.

[7] Amar Hadzihasanovic, Kang Feng Ng, and Quanlong Wang. Two complete axiomatisations of pure-state qubit quantum computing. In *Logic in Computer Science (LICS)*, 2018.

[8] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A generic normal form for zx-diagrams and application to the rational angle completeness. arXiv:1805.05296 [quant-ph].

[9] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In *ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2018.

[10] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond clifford+t quantum mechanics. In *ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2018.

[11] Emmanuel Jeandel, Simon Perdrix, Renaud Vilmart, and Quanlong Wang. ZX-calculus: Cyclotomic supplementarity and incompleteness for Clifford+T quantum mechanics. In *Mathematical Foundations of Computer Science (MFCS)*, number 83 in LIPIcs, pages 11:1 – 11:13, 2017.

[12] Michel Laurent. Equations diophantiennes exponentielles. *Inventiones Mathematicae*, 78:299–327, 1984.

[13] Henry B. Mann. On linear relations between roots of unity. *Mathematika*, 1965.

[14] K. Matsumoto and K. Amano. Representations of quantum circuits with Clifford and $\pi/8$ gates. arXiv:0806.3834, 2008.

[15] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[16] A.L. Onishchik and E.B. Vinberg. *Lie groups and algebraic groups*. Springer, 1988.

[17] Simon Perdrix and Quanlong Wang. Supplementarity is necessary for quantum diagram reasoning. In *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016)*, volume 58 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 76:1–76:14, Krakow, Poland, August 2016.

[18] Charles Radin and Lorenzo Sadun. On 2-generator subgroups of $SO(3)$. *Transactions of the American Mathematical Society*, 351(11):4469–4480, 1999.