

Finite Verification of Infinite Families of Diagram Equations

Hector Miller-Bakewell

Department of Computer Science, University of Oxford, Parks Road, Oxford, OX1 3QD

hector.miller-bakewell@cs.ox.ac.uk

The ZX, ZW and ZH calculi are all graphical calculi for reasoning about pure state qubit quantum mechanics. All of these languages use certain diagrammatic decorations, called !-boxes and phase variables, to indicate not just one diagram but an infinite family of diagrams. These decorations are powerful enough to allow complete rulesets for these calculi to be expressed in around fifteen rules. Historically rules involving !-boxes have not been verifiable by computer. We present the first algorithm for reducing infinite families of equations involving !-boxes into finite verifying subsets. The only requirement for this method is a mild property on the connectivity of the !-boxes. Previous results had focussed on finite case analysis of phase variables in ZX, a result we also extend for ZW and ZH, as well as providing a general framework for further languages. The results presented here allow proof assistants to reduce infinite families of problems (involving combinations of phase variables and !-boxes) down to undecorated, case-by-case verification, in a way not previously possible. In particular we note the removal of the need to reason directly with !-boxes in verification tasks as something entirely new. This forms part of larger work in automated verification of quantum circuitry, conjecture synthesis, and diagrammatic languages in general. The methods described here extend to any diagrammatic languages that meet certain simple conditions.

1 Introduction

The investigation of qubit graphical calculi began with Coecke and Duncan in [4], where they created the ZX calculus: A sound, universal calculus that was shown to be complete in [13]. Since then ZX has been used for such things as reasoning about quantum error correction via lattice surgery ([2] and [5],) through to being the basis for taught courses in quantum computing [3]. The $ZW_{\mathbb{C}}$ calculus, invented by Hadzihasanovic [6], presents a different point of view; rather than focus on the Z and X rotations of the Bloch sphere as ZX does, it focusses on the GHZ and W entanglement states. The ZH calculus (Kissinger and Backens, [1]) has another viewpoint again; that of extending the notion of Hadamard and CCZ gates.

Each of these calculi has strength in different areas, and all of them are complete and universal for pure state qubit quantum mechanics. Our interest is that, with one exception, the rules of these calculi are expressed in a finite manner; that is to say a finite collection of parameterised families of equations. This parameterisation is an expression of two types of regular structure:

- Phase variables: e.g. “This X can be any complex number”
- !-boxes: e.g. “This part of the diagram can be repeated 0 or more times”

The one exception to this being the (EU) rule of the ZX calculus (see [14]) which use what we call *side conditions*, a case we shall not be considering in this paper.

The aim of this paper is to show when these parameterisations admit themselves to finite verification: A process by which a computer can verify an entire infinite family by checking a finite number of cases. For phase variables we exploit the properties of the polynomial functions they represent (theorem 18), and for !-boxes we exploit the finite dimensionality of the space in which their repeated structure resides

(theorem 30). We show how these two types of parameterisation interact in theorem 32 before finally giving a constructive method for finding a verifying subset in theorem 33.

In essence finite verification allows us to start with an infinite family of equations (indicated by a pair of diagrams decorated with phase variables and !-boxes,) and show that this entire family of equations are sound by only checking a finite number of individual equations, none of which are decorated.

2 Parameterised families of diagrams

In this chapter we define the language with which we discuss decorations, infinite families and so on. We then give a few examples of the way we use this language.

Definition 1. A **diagram** is a morphism in a PROP (see e.g. [10, p 97]); it has $n \in \mathbb{N}$ inputs (at the top) and $m \in \mathbb{N}$ outputs (at the bottom.) Morphisms in the PROP are constructed from a set of generators using horizontal composition (given the symbol \otimes) and vertical composition (given the symbol \circ .)

Definition 2. A **complex matrix interpretation** for a PROP of diagrams \mathbb{L} , written $\llbracket \cdot \rrbracket$, is a monoidal functor from \mathbb{L} to $\text{Mat}_{\mathbb{C}}$. I.e. a functor that preserves the \otimes and \circ products of diagrams:

$$\llbracket \cdot \rrbracket : \mathbb{L} \rightarrow \text{Mat}_{\mathbb{C}} \tag{1}$$

$$\llbracket \mathbb{D}_1 \otimes \mathbb{D}_2 \rrbracket = \llbracket \mathbb{D}_1 \rrbracket \otimes \llbracket \mathbb{D}_2 \rrbracket \tag{2}$$

$$\llbracket \mathbb{D}_1 \circ \mathbb{D}_2 \rrbracket = \llbracket \mathbb{D}_1 \rrbracket \circ \llbracket \mathbb{D}_2 \rrbracket \tag{3}$$

(We are using \otimes to represent the Kronecker product of matrices, and \circ to represent standard matrix multiplication.)

We include a list of the generators of ZX, ZH, and $\text{ZW}_{\mathbb{C}}$, as well as their interpretations into $\text{Mat}_{\mathbb{C}}$, in appendix B.1.

Definition 3. An equation of diagrams $\mathbb{D}_1 = \mathbb{D}_2$ is **sound** if $\llbracket \mathbb{D}_1 \rrbracket = \llbracket \mathbb{D}_2 \rrbracket$

Definition 4. A **phase algebra** describes additional structure used in presenting infinite families of rules. Diagram generators are decorated with terms from the phase algebra. Elements of this algebra are called **phases** (introduced in [4]), and a **phase variable** is a formal variable adjoined to the phase algebra. For universal ZX the phase group is $([0, 2\pi), +_{2\pi})$, and for ZH and $\text{ZW}_{\mathbb{C}}$ the phase ring is the complex numbers.

Example 5. A ZH diagram that has no phase variables has every phase an element of \mathbb{C} . A ZH diagram that has a single phase variable α has every phase an element of $\mathbb{C}[\alpha]$. Unused phase variables (and later, unused !-boxes) are ignored.

Definition 6. A **!-box** (introduced in [8], discussed in more detail in [12]) is a special vertex δ added to the diagram. A vertex v is described as “in” a particular !-box if there is a directed edge from δ to v . Instantiating the !-box δ with n copies is performed by:

- Making n copies of every vertex in δ , maintaining any connections to other vertices.
- Deleting the vertex δ

Definition 7. A diagram that does not contain any phase variables or !-boxes is called **simple**, or otherwise called **decorated**.

Definition 8. We will use the term **instantiation** to refer to both the evaluation of a phase variable and the copying procedure of !-boxes. We use the notation $\alpha|a = a$ to indicate that α has been instantiated at the value a .

An explicit instantiation is given in Example 11.

Definition 9. We write

$$\{ \mathbb{D}_1 = \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m} \quad (4)$$

for the family of simple equations between diagrams parameterised by the α_j and δ_k .

Definition 10. The parameterised equation \mathbb{E} (between diagrams \mathbb{D}_1 and \mathbb{D}_2) is **sound** if for any choice of parameter values the resulting equation between simple diagrams is sound. (See Definition 3)

We show restrictions of the parameter values by expressing the instantiated value as belonging to some subset. For example if the family \mathbb{E} is sound for $\alpha_2 = a_2$ whenever $a_2 \in A_2$ we will just write:

$$\{ \mathbb{E} \}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \alpha_2 \in A_2} \text{ is sound} \quad (5)$$

Example 11. The (slightly simplified) spider law in universal ZX is parameterised over

- $\delta_1 \in \mathbb{N}$ inputs and $\delta_2 \in \mathbb{N}$ outputs
- $\alpha_1, \alpha_2 \in [0, 2\pi)$

And so we write the parameterised family of equations as:

$$\left\{ \begin{array}{c} \delta_1 \\ \alpha_1 \\ \alpha_2 \\ \delta_2 \end{array} \right\} = \left\{ \begin{array}{c} \delta_1 \\ \alpha_1 + \alpha_2 \\ \delta_2 \end{array} \right\} \quad (6)$$

$\alpha_1, \alpha_2, \delta_1, \delta_2$

We now instantiate some of the parameters of the spider law, resulting in what is still an infinite, parameterised family:

$$\left\{ \begin{array}{c} \delta_1 \\ \alpha_1 \\ \alpha_2 \\ \delta_2 \end{array} \right\} = \left\{ \begin{array}{c} \delta_1 \\ \alpha_1 + \alpha_2 \\ \delta_2 \end{array} \right\} \quad (7)$$

$\alpha_1, \alpha_2, \delta_1, \delta_2 | \alpha_1 = \pi, \delta_1 = 2$ $\alpha_2, \delta_1, \delta_2 | \delta_1 = 2$

$$= \left\{ \begin{array}{c} \pi \\ \alpha_2 \\ \delta_2 \end{array} \right\} = \left\{ \begin{array}{c} \pi + \alpha_2 \\ \delta_2 \end{array} \right\} \quad (8)$$

α_2, δ_2

3 Verifying phase parameters

Our first result will concern diagrams that contain a finite number of phase variables and no !-boxes. It relies on a certain property of polynomials: That if you know the value of the polynomial $P(Y)$ for sufficiently many values of Y then you can determine all the coefficients of P . For example the polynomial $P(Y_1, Y_2) = a + bY_1 + cY_2 + dY_1Y_2$ can have all of its coefficients determined by knowing the values $P(0, 0)$, $P(0, 1)$, $P(1, 0)$, and $P(1, 1)$. We use this fact by extending the matrix interpretation of simple diagrams to one for decorated diagrams.

3.1 Matrix interpretations

All of the graphical languages considered in this paper come equipped with a complex matrix interpretation, see Definition 2. Moreover for each of these languages a diagram with n inputs and m outputs will be mapped to a matrix with $\dim \mathbb{H}^{\otimes n}$ columns and $\dim \mathbb{H}^{\otimes m}$ rows, where \mathbb{H} represents \mathbb{C}^2 . It is this interpretation that allows us to use these languages to represent transformations in quantum computing. Appendix B contains matrix interpretations for the ZX, ZH and ZW calculi, or see [1] and [6] for the ZH and ZW interpretations, and either [4] or [14] for the ZX interpretation.

A set of diagrams parameterised over α is a set of simple diagrams, and we could extend our interpretation so that a set of simple diagrams is sent to a set of matrices. This would, however, lose any structure from the phase algebra. Instead we try to find a polynomial matrix interpretation; for example one that sends a family of ZH equations $\{\mathbb{E}\}_\alpha$ to a matrix in $\text{Mat}_{\mathbb{C}[\alpha]}$.

While this works well for ZH and $\text{ZW}_{\mathbb{C}}$, there is a complication with ZX: A phase variable α in a ZX diagram corresponds to an $e^{i\alpha}$ in the matrix interpretation. We can try performing the substitution $Y := e^{i\alpha}$, but run into trouble if there is a node containing, for example, $-\alpha$ (and accordingly Y^{-1} in the matrix,) since polynomials do not normally allow negative powers. Rather than stick with standard polynomials we instead move to Laurent polynomials; polynomials that do allow positive and negative powers, and define all the properties we will need of them below.

ZX also introduces one more subtlety: There is an extra relation from the phase group ($2\pi = 0$) that we should take care to reflect in our matrix interpretation. This does not impact universal ZX, but does affect the fragments of ZX with a finite phase group (Example 23 demonstrates this for the Clifford+T fragment.)

Definition 12. A *complex Laurent polynomial interpretation* is a matrix interpretation:

$$\llbracket \cdot \rrbracket : \mathbb{L}[\alpha_1, \dots, \alpha_n] \rightarrow \text{Mat}_{\mathbb{C}[Y_1, Y_1^{-1}, \dots, Y_n, Y_n^{-1}]} \quad (9)$$

The source category here is the PROP of diagrams where generators are now taken not from the phase algebra of \mathbb{L} but from this phase algebra adjoin the phase variables $\alpha_1 \dots \alpha_n$.

See appendix B for explicit interpretations of the ZX, ZW and ZH generators into $\text{Mat}_{\mathbb{C}[Y_1, Y_1^{-1}, \dots, Y_n, Y_n^{-1}]}$.

Example 13. The Z spider from universal ZX is parameterised by an $\alpha \in [0, 2\pi)$, and the (simple) matrix interpretation of some Z spider (with α instantiated at a) is:

$$\llbracket \left\{ \begin{array}{c} \text{---} \\ \text{---} \end{array} \left(\begin{array}{c} \text{---} \\ \alpha \\ \text{---} \end{array} \right) \left. \vphantom{\begin{array}{c} \text{---} \\ \text{---} \end{array}} \right\} \Big|_{\alpha=a} \rrbracket = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & e^{ia} \end{bmatrix} \in \text{Mat}_{\mathbb{C}} \quad (10)$$

Rather than instantiate the value of α before we apply the map, we instead make the substitution $Y = e^{i\alpha}$ to find a Laurent polynomial matrix interpretation:

$$\llbracket \left(\begin{array}{c} \text{---} \\ \alpha \\ \text{---} \end{array} \right) \rrbracket = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & Y \end{bmatrix} \in \text{Mat}_{\mathbb{C}[Y, Y^{-1}]} \quad (11)$$

3.2 Degree of a matrix

Definition 14. *Laurent polynomial degrees (defined in the same manner as e.g. [15]:)*

- The 0 polynomial has degree $-\infty$ by convention
- the non-zero Laurent polynomial $a_n Y^n + a_{n-1} Y^{n-1} + \dots + a_0 + a_{-1} Y^{-1} + \dots + a_{-m} Y^{-m}$ with $a_n \neq 0$ and $a_{-m} \neq 0$ has **positive degree** $n \geq 0$ and **negative degree** $m \geq 0$.

Note that we can factorise this Laurent polynomial as Y^{-m} multiplied by a (non-Laurent) polynomial.

Definition 15. We define here a notion of matrix and diagram degree:

- The Y_j^+ -**degree** of a matrix in $\text{Mat}_{\mathbb{C}[Y_1, Y_1^{-1}, \dots, Y_n, Y_n^{-1}]}$ is the maximum of the positive Y_j -degrees of the entries in that matrix
- The Y_j^- -**degree** is the maximum of the negative Y_j -degrees of the entries in that matrix
- The positive degree of a diagram is the positive degree of the matrix interpretation of that diagram (likewise for negative degrees.) When clear from context we will refer to the degree of a phase variable α_j in the diagram, meaning the degree of Y_j in the interpretation.

Example 16. Here are example positive and negative degrees for first a polynomial, and then a 2×2 matrix of polynomials.

$$\deg_Y^+ (Y^8 + 1 + Y^{-2}) = 8 \qquad \deg_Y^- (Y^8 + 1 + Y^{-2}) = 2 \qquad (12)$$

$$\deg_Y^+ \begin{pmatrix} 2 & Y^{-3} \\ Y & Y^2 - 2 \end{pmatrix} = \max\{0, 0, 1, 2\} = 2 \qquad \deg_Y^- \begin{pmatrix} 2 & Y^{-3} \\ Y & Y^2 - 2 \end{pmatrix} = \max\{0, 3, 0, 0\} = 3 \qquad (13)$$

Proposition 17. For two diagrams \mathbb{D} and \mathbb{D}' we can find an upper bound for the degrees of the horizontal or vertical compositions of \mathbb{D} and \mathbb{D}' , i.e.:

$$\deg_Y^+ (\mathbb{D} \circ \mathbb{D}') \leq \deg_Y^+ \mathbb{D} + \deg_Y^+ \mathbb{D}' \qquad \deg_Y^+ (\mathbb{D} \otimes \mathbb{D}') \leq \deg_Y^+ \mathbb{D} + \deg_Y^+ \mathbb{D}' \qquad (14)$$

$$\deg_Y^- (\mathbb{D} \circ \mathbb{D}') \leq \deg_Y^- \mathbb{D} + \deg_Y^- \mathbb{D}' \qquad \deg_Y^- (\mathbb{D} \otimes \mathbb{D}') \leq \deg_Y^- \mathbb{D} + \deg_Y^- \mathbb{D}' \qquad (15)$$

Proof. We first note that for Laurent polynomials P and P' in $\mathbb{C}[Y, Y^{-1}]$, and for $\lambda \in \mathbb{C}$:

$$\deg_Y^+ (\lambda P) \leq \deg_Y^+ P \qquad \deg_Y^- (\lambda P) \leq \deg_Y^- P \qquad (16)$$

$$\deg_Y^+ (P \times P') \leq \deg_Y^+ P + \deg_Y^+ P' \qquad \deg_Y^- (P \times P') \leq \deg_Y^- P + \deg_Y^- P' \qquad (17)$$

$$\deg_Y^+ \left(\sum_j P_j \right) \leq \max_j \deg_Y^+ P_j \qquad \deg_Y^- \left(\sum_j P_j \right) \leq \max_j \deg_Y^- P_j \qquad (18)$$

The composition $A \circ B$ or tensor product $A \otimes B$ of matrices produces a new matrix with entries that are linear combinations of products of the entries of A and B . Therefore:

$$\deg_Y^+ (M \circ M') \leq \deg_Y^+ M + \deg_Y^+ M' \qquad \deg_Y^+ (M \otimes M') \leq \deg_Y^+ M + \deg_Y^+ M' \qquad (19)$$

$$\deg_Y^- (M \circ M') \leq \deg_Y^- M + \deg_Y^- M' \qquad \deg_Y^- (M \otimes M') \leq \deg_Y^- M + \deg_Y^- M' \qquad (20)$$

Recalling that the degree of a diagram is the degree of its polynomial matrix interpretation this gives us the result for \mathbb{D} and \mathbb{D}' . \square

3.3 Finite verification

Theorem 18. *For a diagrammatic equation with phase variables*

$$\{ \mathbb{D}_1 = \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n}$$

that has a Laurent polynomial matrix interpretation, and the equation is sound at all values of $(\alpha_1, \dots, \alpha_n) = (a_1, \dots, a_n) \in A_1 \times \dots \times A_n$, where each $|A_j|$ is sufficiently large, then the equation is sound for all values of $(\alpha_1, \dots, \alpha_n)$. That is:

$$\begin{aligned} & \left[\left[\{ \mathbb{D}_1 \}_{\alpha_1, \dots, \alpha_n} \mid \alpha_1 = a_1, \dots, \alpha_n = a_n \right] \right] = \left[\left[\{ \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n} \mid \alpha_1 = a_1, \dots, \alpha_n = a_n \right] \right] \\ & \quad \forall a_1 \in A_1, \dots, a_n \in A_n \\ \implies & \left[\left[\{ \mathbb{D}_1 \}_{\alpha_1, \dots, \alpha_n} \mid \alpha_1 = a_1, \dots, \alpha_n = a_n \right] \right] = \left[\left[\{ \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n} \mid \alpha_1 = a_1, \dots, \alpha_n = a_n \right] \right] \\ & \quad \forall a_1, \dots, a_n \end{aligned} \quad (21)$$

The necessary size of $|A_j|$ is given by:

$$|A_j| = \max(\deg_{Y_j}^+ \mathbb{D}_1, \deg_{Y_j}^+ \mathbb{D}_2) + \max(\deg_{Y_j}^- \mathbb{D}_1, \deg_{Y_j}^- \mathbb{D}_2) + 1 \quad (22)$$

“The maximum of the positive degrees, plus the maximum of the negative degree, plus one.”

The proof can be found in appendix A.1. A sketch of it is as follows:

- Manipulate the equation $[[\mathbb{D}]] = [[\mathbb{D}']]$ into an equation of the form $M = 0$, where M is a matrix of (non-Laurent) polynomials.
- Perform multivariate polynomial interpolation element-wise on M .
- In doing this interpolation we need to know the degrees of the polynomials in M , which we calculate using Proposition 17

Example 19. *Finding the sizes of the A_j : The following (universal) ZX diagram contains no $!$ -boxes and two phase variables.*

$$\begin{array}{c} \begin{array}{c} \alpha_1 \\ \alpha_2 \end{array} = \begin{array}{c} \alpha_1 + \alpha_2 \end{array} \end{array} \quad \begin{array}{cc} \deg_{\alpha_1}^+ \mathbb{D}_1 = 1 & \deg_{\alpha_2}^+ \mathbb{D}_1 = 1 \\ \deg_{\alpha_1}^- \mathbb{D}_1 = 0 & \deg_{\alpha_2}^- \mathbb{D}_1 = 0 \end{array} \quad \begin{array}{cc} \deg_{\alpha_1}^+ \mathbb{D}_2 = 1 & \deg_{\alpha_2}^+ \mathbb{D}_2 = 1 \\ \deg_{\alpha_1}^- \mathbb{D}_2 = 0 & \deg_{\alpha_2}^- \mathbb{D}_2 = 0 \end{array} \quad (23)$$

We should therefore construct A_1 and A_2 such that $|A_1| = \max\{1, 1\} + \max\{0, 0\} + 1$ and $|A_2| = \max\{1, 1\} + \max\{0, 0\} + 1$. By picking $A_1 = A_2 = \{0, \pi\}$ we therefore know that we can verify this parameterised family of diagram equations for all values of α_1 and α_2 by verifying this equation on the following grid of values:

$$\begin{array}{ccc} & \alpha_1 = 0 & \alpha_1 = \pi \\ \alpha_2 = 0 & (0, 0) & (0, \pi) \\ \alpha_2 = \pi & (\pi, 0) & (\pi, \pi) \end{array} \quad (24)$$

i.e. by verifying the four equations:

$$\left\{ \begin{array}{c} 0 \\ 0 \end{array} \right\} = \begin{array}{c} 0+0 \\ 0+0 \end{array}, \quad \left\{ \begin{array}{c} 0 \\ \pi \end{array} \right\} = \begin{array}{c} 0+\pi \\ 0+\pi \end{array}, \quad \left\{ \begin{array}{c} \pi \\ 0 \end{array} \right\} = \begin{array}{c} \pi+0 \\ \pi+0 \end{array}, \quad \left\{ \begin{array}{c} \pi \\ \pi \end{array} \right\} = \begin{array}{c} \pi+\pi \\ \pi+\pi \end{array} \quad (25)$$

we can assert that the diagram equation in (23) is sound for all values of α_1 and α_2 in $[0, 2\pi)$.

Corollary 20. *In the universal ZX calculus it suffices to check $(\alpha_1, \dots, \alpha_n) \in A_1 \times \dots \times A_n$ to prove an equation parameterised by α_j , where the A_j are sets of distinct angles with*

$$|A_j| = \max\{\deg_{\alpha_j}^+ \mathbb{D}_1, \deg_{\alpha_j}^+ \mathbb{D}_2\} + \max\{\deg_{\alpha_j}^- \mathbb{D}_1, \deg_{\alpha_j}^- \mathbb{D}_2\} + 1 \quad (26)$$

Remark 21. *Corollary 20 was first proved in [7, Theorem 3]. The authors use the symbol μ to count appearances of α_j (with coefficient,) and T_j to denote a large enough set of values. Their method does not use Laurent polynomials, instead examining ranks of certain matrices, but this also means their method does not extend to ZH and ZW.*

The result of [7] is in fact stronger than that of Theorem 18; as they show that under the conditions given here there is a universal proof of the parameterised equation, something that the method given in Theorem 18 does not show. For the purposes of verification, however, it is not important how an equation is derivable, but only whether the equation is sound.

Example 22. *Note that the ZX result required the variables to be linear, but for ZH and ZW this result applies to diagrams whose phases are polynomial (or even Laurent polynomial) in the α_j . For example we can verify the following ZH equation by checking 3 distinct values of α :*


(27)

Example 23. *Consider a Clifford+T ZX diagram that contains at least 8 nodes labeled by a positive α . Our theorem says that for any equation containing this diagram it suffices to try at least 9 distinct values of α , but this is impossible since there are only 8 distinct values of α available in Clifford+T.*

This is because our Laurent polynomial matrix interpretation needs to be viewed not in $\mathbb{C}[Y, Y^{-1}]$ but in $\mathbb{C}[Y]/(Y^8 - 1)$, reflecting the property $8 \times \alpha = 0$ in our phase group. All polynomials in $\mathbb{C}[Y]/(Y^8 - 1)$ have degree at most 7, and so it is never necessary to check more than 8 points.

4 Verifying !-boxes

We now turn our attention to !-boxes. The aim of this section is to show that if an equation holds for $0, \dots, N$!-box instances, then it continues to hold for any number of instances. It then follows that one only needs to check the first $0, \dots, N$ instances in order to verify the entire family. The method relies on the finite dimensionality of what we call the *join* between the inside and outside of a !-box. Sometimes this join is not finite dimensional, and so we examine a property called *separated* which captures when the method will work. Before we can get to that we first make clear how the nesting of !-boxes and phase variables can work.

4.1 Children, copies, and the nesting order

We begin with some definitions for describing the effect of nesting !-boxes inside a parameterised family of equations. There is a choice to be made when nesting parameters:

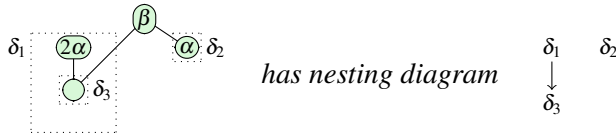
Definition 24. *When a !-box creates new instances of a nested parameter we **copy** that variable name, so that all instances are linked by the same name (the approach taken in [12, §4.4.2],) we could alternatively create new names, each of which is referred to as a **child** of the original parameter name (an approach requested by at least one user of Quantomatic.) When we create child parameters we record the name of its parent, so we can always tell the original ancestor of a parameter.*

Rather than pick one option over the other we will demonstrate our results for both choices. In order to talk about nesting formally we introduce the following definition:

Definition 25. We define a partial order (which we call the **nesting order**) on $!$ -boxes in a diagram:

$$\delta_1 < \delta_2 \quad \text{if } \delta_1 \text{ is inside } \delta_2$$

And use this partial order to draw a nesting diagram. For example this (universal) ZX diagram:



Definition 26. We say an equation is **well nested** if the nesting diagrams corresponding to the left and right hand sides of the equation are identical.

Definition 27. The **join** of a $!$ -box is the collection of wires that leave that $!$ -box, i.e. the edges linking a vertex inside δ to one outside δ . The **size** of a join is the number of wires, and the **dimension** of a join is the dimension of the diagram formed by just the wires of that join, i.e. $\dim \llbracket \mid^{\otimes n} \rrbracket$ where n is the size of the join. This is equivalently $(\dim \llbracket \mid \rrbracket)^n$.

Definition 28. We describe a pair of $!$ -boxes as **separated** if either:

- They are nested, or
- There is no edge joining a vertex in one to a vertex in the other

Note that in many of the languages considered there are elementary operations one can do that will change a diagram that is not separated into one that is. See Section C for more details.

4.2 Verification

Definition 29. Given a parameterised equation \mathbb{E} we say that $\{\mathbb{E}_1, \dots, \mathbb{E}_n\}$ **verifies** \mathbb{E} if:

$$\forall j (\mathbb{E}_j \text{ is sound}) \implies \mathbb{E} \text{ is sound}$$

Theorem 30. Given a family $\mathbb{E} = \{ \mathbb{D}_1 = \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m}$ of diagrammatic equations, parameterised by a $!$ -box δ_1 where δ_1 is separated from all other $!$ -boxes and is nested in no other $!$ -box; then \mathbb{E} is verified by the finite family $\{\mathbb{E}|_{\delta_1=0}, \dots, \mathbb{E}|_{\delta_1=N}\}$ where N is the dimension of the join of δ_1 in \mathbb{D}_1 plus

the dimension of the join of δ_1 in \mathbb{D}_2 . That is:

$$\begin{aligned} n_1 &:= \text{join of } \delta_1 \text{ in } \mathbb{D}_1 \\ n_2 &:= \text{join of } \delta_1 \text{ in } \mathbb{D}_2 \\ N &:= \dim(\mathbb{H}^{\otimes n_1} \oplus \mathbb{H}^{\otimes n_2}) \end{aligned}$$

$$\begin{aligned} & \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \\ &= \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \quad \forall d_1 \leq N \end{aligned} \quad (28)$$

$$\begin{aligned} \implies & \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \\ &= \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \quad \forall d_1 \end{aligned} \quad (29)$$

The proof is presented in appendix A.2. The essence of the proof is to change the presentation of the $!$ -box instances into one that looks like the vertical composition of repeated elements. From there some elementary (albeit fiddly) properties of finite dimensional vector spaces are applied to achieve the result. Note that the the resulting finite family of equations need not be simple, and that if δ_1 were not separated from the other $!$ -boxes then we could not put a bound on N .

Example 31. Consider the following (universal) ZX family of equations, parameterised by a single $!$ -box:

$$\mathbb{E} := \left\{ \begin{array}{c} \text{Diagram 1} \\ \text{Diagram 2} \end{array} \right\}_{\delta} \quad (30)$$


The join between the $!$ -box and the rest of the diagram on the left is two wires (dimension 2^2), and on the right is one wire (dimension 2^1 .) These sum to have dimension 6, and we therefore need only to check the $!$ -box instances $(0, \dots, 6)$ to be sure that the equation \mathbb{E} is sound.

5 Interacting Parameters

Theorem 18 and theorem 30 deal with equations containing multiple phase variables and nested $!$ -boxes respectively. This section will put together the necessary results such that we can combine these approaches to deal with equations containing multiple $!$ -boxes and phase variables, any of which could potentially be nested inside other $!$ -boxes.

Theorem 32. Given an equation \mathbb{E} and ways of finding

- finite verifying sets A_j for the α_j (Theorem 18)
- finite verifying sets D_k for the δ_k (Theorem 30)

then we may verify the entire family \mathbb{E} by checking the (finite) set given by the cartesian product of all the A_j and D_k .

Proof. We define:

$$\bar{D} := D_1 \times D_2 \times \cdots \times D_m \quad (31)$$

$$\bar{\delta} := (\delta_1, \dots, \delta_m) \quad (32)$$

$$A_j(\bar{\delta}) := \text{The verifying set for } \alpha_j \text{ once } E \text{ has had !-boxes instantiated at } \bar{\delta} \quad (33)$$

Construct A_j by choosing as many points as there are in $\max_{\bar{\delta}} \{|A_j(\bar{\delta})|\}$. This is finite because the D_i and the $A_j(\bar{\delta})$ are finite. A_j therefore contains enough points to be a verifying set for $A_j(\bar{\delta}) \quad \forall \bar{\delta} \in \bar{D}$. We now show that $A_1 \times \cdots \times A_n \times D_1 \times \cdots \times D_m$ describes a verifying set for the parameterised equation \mathbb{E} :

$$\begin{aligned} & \mathbb{E}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m} \mid \forall i, j \alpha_j \in A_j, \delta_k \in D_k && \text{is sound} && (34) \\ = & \mathbb{E}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m} \mid \forall i \alpha_j \in A_j, \bar{\delta} \in \bar{D} && \text{is sound (rewrite using } \bar{\delta} \text{ notation)} && (35) \\ \implies & \mathbb{E}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m} \mid \forall i \alpha_j \in A_j(\bar{\delta}), \bar{\delta} \in \bar{D} && \text{is sound (construction of } A_j) && (36) \\ \implies & \mathbb{E}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m} \mid \bar{\delta} \in \bar{D} && \text{is sound (theorem 18)} && (37) \\ \implies & \mathbb{E}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m} && \text{is sound (theorem 30)} && (38) \end{aligned}$$

□

Theorem 33. *Given a parameterised family of equations \mathbb{E} , where the !-boxes are separated and well nested, we can construct a finite set of simple equations $\{\mathbb{E}_\kappa\}_{\kappa \in K}$, such that:*

$$\{\mathbb{E}_\kappa\}_{\kappa \in K} \text{ is sound} \implies \mathbb{E} \text{ is sound} \quad (39)$$

The proof can be found in appendix A.3. The idea of the proof is to iteratively remove dependencies on !-boxes via theorem 30, each time generating a larger set of verifying equations. Once we have removed all !-box dependence we then use theorem 32 to remove phase variable dependence; using the “largest” equation in $\{\mathbb{E}_\kappa\}$ to determine the sizes of the A_j . We argue by the finite nature of all the parts involved that this process terminates.

We did not specify in the statement of our theorem which method of !-box expansion we were following (see Definition 24) and indeed both methods work and are covered in the proof.

6 Conclusions

We have shown how to construct finite sets of equations that verify certain classes of infinite families of equations. To our knowledge this is the first algorithm that can verify equations containing !-boxes, and the first analysis of such algorithms for ZW and ZH. This paves the way for proof assistants to verify parameterised theorems. Further work would include combining this work with conjecture synthesis, so that a computer could generate and verify parameterised hypotheses. One could also implement such methods into proof assistants, such as Quantomatic [9], so that the verifying set could be generated (and ideally checked) automatically.

One final avenue is to develop methods to deal with the side conditions of the (EU) rule of the ZX calculus ([14],) either by extending these results or finding a presentation of the ZX calculus that does not require side conditions. It should be noted that [7] gives some evidence that such a presentation may not exist.

6.1 Acknowledgements

The author would like to thank their supervisors Aleks Kissinger and Bob Coecke as well as Miriam Backens for their help in writing this paper, and the EPSRC for providing the funding grant.

References

- [1] Miriam Backens & Aleks Kissinger (2019): *ZH: A Complete Graphical Calculus for Quantum Computations Involving Classical Non-linearity*. *Electronic Proceedings in Theoretical Computer Science* 287, p. 23–42, doi:10.4204/eptcs.287.2.
- [2] Niel de Beaudrap & Dominic Horsman (2020): *The ZX calculus is a language for surface code lattice surgery*. *Quantum* 4, p. 218, doi:10.22331/q-2020-01-09-218.
- [3] B. Coecke & A. Kissinger (2017): *Picturing Quantum Processes*. Cambridge University Press, doi:10.1017/9781316219317.
- [4] Bob Coecke & Ross Duncan (2008): *Automata, Languages and Programming: 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part II*, chapter Interacting Quantum Observables, pp. 298–310. Springer Berlin Heidelberg, Berlin, Heidelberg, doi:10.1007/978-3-540-70583-3_25.
- [5] Craig Gidney & Austin G. Fowler (2019): *Efficient magic state factories with a catalyzed $|CCZ\rangle$ to $2|T\rangle$ transformation*. *Quantum* 3, p. 135, doi:10.22331/q-2019-04-30-135.
- [6] Amar Hadzihasanovic (2015): *A Diagrammatic Axiomatisation for Qubit Entanglement*. *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*, doi:10.1109/lics.2015.59.
- [7] Emmanuel Jeandel, Simon Perdrix & Renaud Vilmart (2018): *Diagrammatic Reasoning beyond Clifford+T Quantum Mechanics*. *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science - LICS '18*, doi:10.1145/3209108.3209139.
- [8] Aleks Kissinger, Alex Merry & Matvey Soloviev (2014): *Pattern graph rewrite systems*. 143, Open Publishing Association, p. 54–66, doi:10.4204/eptcs.143.5.
- [9] Aleks Kissinger & Vladimir Zamdzhiev (2015): *Quantomatic: A Proof Assistant for Diagrammatic Reasoning*. *Lecture Notes in Computer Science*, p. 326–336, doi:10.1007/978-3-319-21401-6_22.
- [10] Saunders MacLane (1965): *Categorical algebra*. *Bull. Amer. Math. Soc.* 71(1), pp. 40–106, doi:10.1090/S0002-9904-1965-11234-4. Available at <https://projecteuclid.org:443/euclid.bams/1183526392>.
- [11] Thomas Sauer Mariano Gasca (2000): *On the history of multivariate polynomial interpolation*. *Journal of Computational and Applied Mathematics* 122, pp. 23–35, doi:10.1016/S0377-0427(00)00353-8. Available at <https://www.sciencedirect.com/science/article/pii/S0377042700003538>.
- [12] Alexander Merry (2014): *Reasoning with $!$ -Graphs*. Ph.D. thesis, University of Oxford. Available at <http://arxiv.org/abs/1403.7828>.
- [13] K. F. Ng & Q. Wang (2017): *A universal completion of the ZX-calculus*. ArXiv e-prints:1706.09877.
- [14] Renaud Vilmart (2019): *A Near-Minimal Axiomatisation of ZX-Calculus for Pure Qubit Quantum Mechanics*. *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, doi:10.1109/lics.2019.8785765.
- [15] Eric W. Weisstein: *Laurent Polynomial*. Available at <http://mathworld.wolfram.com/LaurentPolynomial.html>. From MathWorld—A Wolfram Web Resource.

A Proofs

We show here any proofs that were not included in the main text.

A.1 Proof of theorem 18

Theorem 18. *For a diagrammatic equation with phase variables*

$$\{ \mathbb{D}_1 = \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n}$$

that has a Laurent polynomial matrix interpretation, and the equation is sound at all values of $(\alpha_1, \dots, \alpha_n) = (a_1, \dots, a_n) \in A_1 \times \dots \times A_n$, where each $|A_j|$ is sufficiently large, then the equation is sound for all values of $(\alpha_1, \dots, \alpha_n)$. That is:

$$\begin{aligned} \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n} \Big|_{\alpha_1=a_1, \dots, \alpha_n=a_n} \right] &= \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n} \Big|_{\alpha_1=a_1, \dots, \alpha_n=a_n} \right] \\ &\quad \forall a_1 \in A_1, \dots, a_n \in A_n \end{aligned} \tag{21}$$

$$\implies \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n} \Big|_{\alpha_1=a_1, \dots, \alpha_n=a_n} \right] = \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n} \Big|_{\alpha_1=a_1, \dots, \alpha_n=a_n} \right] \quad \forall a_1, \dots, a_n$$

The necessary size of $|A_j|$ is given by:

$$|A_j| = \max(\deg_{Y_j}^+ \mathbb{D}_1, \deg_{Y_j}^+ \mathbb{D}_2) + \max(\deg_{Y_j}^- \mathbb{D}_1, \deg_{Y_j}^- \mathbb{D}_2) + 1 \tag{22}$$

“The maximum of the positive degrees, plus the maximum of the negative degree, plus one.”

Proof. We are seeking the multivariate complex polynomials that populate the matrices $\llbracket \mathbb{D}_1 \rrbracket$ and $\llbracket \mathbb{D}_2 \rrbracket$. We begin by combining the two matrices of Laurent polynomials into one matrix of (not-Laurent) polynomials and a scale factor of the form $Y_1^{m_1} \dots Y_n^{m_n}$.

- We define:

$$M_1 := \llbracket \mathbb{D}_1 \rrbracket \quad M_2 := \llbracket \mathbb{D}_2 \rrbracket \tag{40}$$

and wish to show $M_1 = M_2$.

- First we pull enough copies of $Y_1^{-1}, \dots, Y_n^{-1}$ out of each side so that we have an equation of the form:

$$M'_1 \prod_j (Y_j^{-1})^{\deg_{Y_j}^- M_1} = M'_2 \prod_j (Y_j^{-1})^{\deg_{Y_j}^- M_2} \tag{41}$$

Where M'_1 and M'_2 are matrices of (not-Laurent) polynomials.

- Let $m_j := \max(\deg_{Y_j}^- M_1, \deg_{Y_j}^- M_2)$ and multiply both sides by $\prod_j Y_j^{m_j}$ to clear any negative powers of Y_j .

$$M'_1 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_1} = M'_2 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_2} \tag{42}$$

- Then subtract the right hand side from the left:

$$M'_1 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_1} - M'_2 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_2} = 0 \quad (43)$$

$$\mathbb{M} := M'_1 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_1} - M'_2 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_2} \quad (44)$$

Note that \mathbb{M} is a matrix of (not-Laurent) polynomials. The statement $\mathbb{M} = 0$ can be viewed as a stating that each entry of \mathbb{M} is equal to the 0 polynomial.

- We will use the notation $\deg_{Y_j} \cdot$ for the degree of a (not-Laurent) polynomial, or matrix of polynomials. We could continue to use the term positive degree, the definitions coincide, but want to make it clear that we are no longer in a Laurent polynomial setting.
- We wish to find a bound for the maximum degree of any polynomial in \mathbb{M} :

$$\deg_{Y_j} \mathbb{M} = \deg_{Y_j} M'_1 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_1} - M'_2 \prod_j Y_j^{m_j - \deg_{Y_j}^- M_2} \quad (45)$$

$$\leq \max(\deg_{Y_j} M'_1 + m_j - \deg_{Y_j}^- M_1, \deg_{Y_j} M'_2 + m_j - \deg_{Y_j}^- M_2) \quad (46)$$

$$= \max(\deg_{Y_j}^+ M_1 + \deg_{Y_j}^- M_1 + m_j - \deg_{Y_j}^- M_1, \deg_{Y_j}^+ M_2 + \deg_{Y_j}^- M_2 + m_j - \deg_{Y_j}^- M_2) \quad (47)$$

$$= \max(\deg_{Y_j}^+ M_1 + m_j, \deg_{Y_j}^+ M_2 + m_j) \quad (48)$$

$$= \max(\deg_{Y_j}^+ M_1, \deg_{Y_j}^+ M_2) + m_j \quad (49)$$

$$= \max(\deg_{Y_j}^+ M_1, \deg_{Y_j}^+ M_2) + \max(\deg_{Y_j}^- M_1, \deg_{Y_j}^- M_2) \quad (50)$$

- Suppose we know that our diagram equation is sound for parameter choices in a large enough *regular grid* of values. (A technique that appears to date to before the 20th century, according to [11].)

$$\left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n | \alpha_1 = a_1, \dots, \alpha_n = a_n} \right] = \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n | \alpha_1 = a_1, \dots, \alpha_n = a_n} \right] \quad (51)$$

for $(a_1, \dots, a_n) \in A_1 \times \dots \times A_n$

where $|A_j| = \deg_{Y_j}(\mathbb{M}) + 1$

$$A_j := \{a_{j,0}, \dots, a_{j, \deg_{Y_j}}\}$$

By picking a polynomial entry P of \mathbb{M} , expressing P using the multi-index β as $P = \sum_{\beta} c_{\beta} Y_j^{\beta}$, and then evaluating P at every point in $A_1 \times \dots \times A_n$ we construct the system of equations:

$$\begin{bmatrix} c_{0, \dots, 0} a_{0, \dots, 0}^{0, \dots, 0} & c_{1, \dots, 0} a_{0, \dots, 0}^{1, \dots, 0} & \dots & c_{\deg_{Y_1}, \dots, \deg_{Y_n}} a_{0, \dots, 0}^{\deg_{Y_1}, \dots, \deg_{Y_n}} \\ \vdots & \vdots & \ddots & \vdots \\ c_{0, \dots, 0} a_{|A_1|, \dots, |A_n|}^{0, \dots, 0} & c_{1, \dots, 0} a_{|A_1|, \dots, |A_n|}^{1, \dots, 0} & \dots & c_{\deg_{Y_1}, \dots, \deg_{Y_n}} a_{|A_1|, \dots, |A_n|}^{\deg_{Y_1}, \dots, \deg_{Y_n}} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \quad (52)$$

Which we view as:

$$[V] \begin{bmatrix} c_{0, \dots, 0} \\ \vdots \\ c_{\deg_{Y_1}, \dots, \deg_{Y_n}} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \quad (53)$$

Where V contains all the products $a_1^{\beta_1} \times \dots \times a_n^{\beta_n}$, β ranging from $(0, \dots, 0)$ to $(\deg Y_1, \dots, \deg Y_n)$. Thankfully V decomposes as:

$$V = V_1 \otimes \dots \otimes V_n \quad (54)$$

$$V_j = \begin{bmatrix} a_{j,0}^0 & a_{j,0}^1 & \dots & a_{j,0}^{\deg Y_j} \\ a_{j,1}^0 & a_{j,1}^1 & \dots & a_{j,1}^{\deg Y_j} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j,\deg Y_j}^0 & a_{j,\deg Y_j}^1 & \dots & a_{j,\deg Y_j}^{\deg Y_j} \end{bmatrix} \quad (55)$$

- Since $\det(A \otimes B) \neq 0$ if and only if $\det(A) \neq 0$ and $\det(B) \neq 0$, and since $\det(V_j) \neq 0$ because each V_j is a Vandermonde matrix, we know that $\det(V) \neq 0$. Since V is therefore invertible we know that all the coefficients c_β must be 0, and therefore P is the 0 polynomial.
- In the presence of a regular grid on which \mathbb{D}_1 and \mathbb{D}_2 agree we know:

$$\Rightarrow \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n | \alpha_1 \in A_1, \dots, \alpha_n \in A_n} \right] = \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n | \alpha_1 \in A_1, \dots, \alpha_n \in A_n} \right] \quad (56)$$

$$\Rightarrow P = 0 \quad \text{for any entry } P \text{ of } M \quad (57)$$

$$\Rightarrow \mathbb{M} = 0 \quad (58)$$

$$\Rightarrow M'_1 \prod_j Y^{m_j - \deg_{Y_j}^- M_1} - M'_2 \prod_j Y^{m_j - \deg_{Y_j}^- M_2} = 0 \quad (59)$$

$$\Rightarrow M'_1 \prod_j Y^{m_j - \deg_{Y_j}^- M_1} = M'_2 \prod_j Y^{m_j - \deg_{Y_j}^- M_2} \quad (60)$$

$$\Rightarrow M_1 = M_2 \quad (61)$$

$$\Rightarrow \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n} \right] = \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n} \right] \quad (62)$$

- By setting d_j to $\deg_{Y_j} \mathbb{M} + 1$ (which we can calculate using equation (50)), and $|A_j| = d_j$ we attain our result; that if we know that the interpretations of the families of diagrams agree on the regular grid described by the sizes d_j then the interpretations agree on all points in the phase group.

□

A.2 Proof of theorem 30

Theorem 30. *Given a family $\mathbb{E} = \left\{ \mathbb{D}_1 = \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m}$ of diagrammatic equations, parameterised by a $!$ -box δ_1 where δ_1 is separated from all other $!$ -boxes and is nested in no other $!$ -box; then \mathbb{E} is verified by the finite family $\{\mathbb{E}|_{\delta_1=0}, \dots, \mathbb{E}|_{\delta_1=N}\}$ where N is the dimension of the join of δ_1 in \mathbb{D}_1 plus*

the dimension of the join of δ_1 in \mathbb{D}_2 . That is:

$$\begin{aligned} n_1 &:= \text{join of } \delta_1 \text{ in } \mathbb{D}_1 \\ n_2 &:= \text{join of } \delta_1 \text{ in } \mathbb{D}_2 \\ N &:= \dim(\mathbb{H}^{\otimes n_1} \oplus \mathbb{H}^{\otimes n_2}) \end{aligned}$$

$$\begin{aligned} & \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \\ &= \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \quad \forall d_1 \leq N \end{aligned} \tag{28}$$

$$\begin{aligned} \implies & \left[\left\{ \mathbb{D}_1 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \\ &= \left[\left\{ \mathbb{D}_2 \right\}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m} \right] \quad \forall d_1 \end{aligned} \tag{29}$$

The idea of the proof is:

1. Manipulate the diagrams into what we call **series !-box form**
2. Move to the matrix interpretation
3. Manipulate the equation between two matrices into an expression on a single vector space of dimension N
4. Demonstrate the required property as a condition on subspaces

We will require the “only topology matters” meta-rule for our diagrams, suitable spider laws, a matrix interpretation, and finite dimensionality of \mathbb{H} .

Proof. We begin by showing series !-box form on a diagram containing a single !-box:

$$\left\{ \mathbb{D} \right\}_\delta \tag{63}$$

First we will manipulate the diagram (via “only topology matters”) until it is in the following form:

$$\mathbb{D} = \begin{array}{c} \boxed{B} \\ \vdots \\ \boxed{G} \\ \vdots \end{array} \tag{64}$$

!-box δ around subdiagram B
 n connecting wires from B to G
 remaining diagram G
 m inputs for G

We note that the nodes inside G that join with B must be spiders; since there can be arbitrary many instances of B the connecting node in G must be able to have arbitrary arity. There may also be p boundaries that are internal to B (and therefore δ .) which we will deal with momentarily. We will now rely on the existence of a spider law such that we may do the following:

$$\text{Spider} = \text{Series of Spiders} \tag{65}$$

Which is the ability to “spread” a spider with n outputs into n repeated copies of a spider with 1 output, with suitable initial, terminal, and joining subdiagrams. We do this so that each instance of the $!$ -box is connected to its own copy of the spider, and these copies are joined in sequence.

This is possible in ZX, ZH and ZW. To give a ZX example (where the spider law is simple:)

$$\left\{ \begin{array}{c} \delta \\ \left[\begin{array}{c} B \\ \vdots \\ G \end{array} \right] \\ \delta | \delta = d \end{array} \right\} = \begin{array}{c} \text{end node} \quad d \text{ instances of } B \quad \text{initial node inside } G \\ \text{---} \bullet \text{---} \left[B \right] \text{---} \dots \text{---} \left[B \right] \left[B \right] \text{---} \left[G \right] \end{array} \quad (66)$$

Note that although we have only used one example node and joining wire we can perform this action on all nodes and joining wires. Where two wires travel from the $!$ -box to the same spider inside G we first spread out that spider so each wire from the $!$ -box connects to a different spider in G . Here is an example for n wires between B and G , and p boundaries inside δ (which we stretch down to be below each copy of B in this representation, just for visibility.)

$$\begin{array}{c} n \text{ end nodes} \quad d \text{ instances of } B \quad n \text{ nodes inside } G \\ \left[\begin{array}{c} B \\ \vdots \\ B \end{array} \right] \text{---} \dots \text{---} \left[\begin{array}{c} B \\ \vdots \\ B \end{array} \right] \left[\begin{array}{c} G \\ \vdots \\ G \end{array} \right] \\ p \quad p \quad m \end{array} \quad (67)$$

From here it is easy to see that we have the diagram $G : m \rightarrow n$, beside d copies of a diagram we call $B : p + n \rightarrow n$ (containing the p boundary nodes and the new connecting spiders), and finally an ending diagram $C : n \rightarrow 0$. We call this the **series !-box form**.

Definition 34. *Series !-box form* for a given (non-nested, separated) $!$ -box $\delta_1 = d$ in a diagram is a presentation (as in equation 67) of each the δ_1 -instantiated diagrams as

$C :=$ the end cap of spiders

$B :=$ repeated element, which may contain $\alpha_1, \dots, \alpha_n, \delta_2, \dots, \delta_m$, and some boundary nodes

$G :=$ the rest of the diagram outside of B , which may contain $\alpha_1, \dots, \alpha_n, \delta_2, \dots, \delta_m$, and some boundary nodes

Such that the d instances of δ_1 are spread out as d instances of B . In the case where you consider a $!$ -box to create child instances of parameters then B will contain children of the α_j and $\delta_{k>1}$, rather than copies.

Claim: In the languages ZX, ZW and ZH, for any diagram \mathbb{D} and any value of d we can put $\mathbb{D} \Big|_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m} \delta_1 = d$ into series !-box form as in the example above.

Proof of claim: Inspection of the spider rules in each language.

We will just use the variable names $\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m$ here and assume we are copying parameters, but the technique is identical for when one is creating child parameters and we will point out the different intricacies along the way. We aim to show

$$\begin{aligned}
& \left[\left\{ \mathbb{D}_1 \right\} \alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m \right] \\
&= \left[\left\{ \mathbb{D}_2 \right\} \alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m \right] \quad \forall d_1 \leq N \\
&\implies \left[\left\{ \mathbb{D}_1 \right\} \alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m \right] \quad (68) \\
&= \left[\left\{ \mathbb{D}_2 \right\} \alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m \mid \alpha_1 = a_1, \dots, \delta_1 = d_1, \dots, \delta_m = d_m \right] \quad \forall d_1
\end{aligned}$$

$$N := \dim(\mathbb{H}^{\otimes n_1} \oplus \mathbb{H}^{\otimes n_2})$$

$$n_1 := \text{join of } \delta_1 \text{ in } \mathbb{D}_1$$

$$n_2 := \text{join of } \delta_1 \text{ in } \mathbb{D}_2$$

We would like to move directly to the matrix interpretation of diagram (67), but we have the following problems:

- the p dangling wires from every copy of B
- the parameters inside every copy of B (either linked copies or discrete children)

We solve these problems (and justify these solutions below) by considering B as parameterised by:

- Instances of $\alpha_j \forall j$
- Instances of $\delta_k \forall k > 1$
- Input vectors $v \in \mathbb{H}^{\otimes p}$ that “plug” the inputs inside B .

Since we can show equivalence of complex matrices by showing that they perform the same operation on any input, we need to show that for any choice of $\alpha_j, \delta_{k>1}$ and for any input that equation (68) holds. (And that if we are creating child instances of parameters then these equations hold for any choice of each of those independently.) Once we have specified values of $\alpha_j, \delta_{k>1}$ we may use our matrix interpretation to get a complex matrix, but we need to do this for every possible choice of $\alpha_j, \delta_{k>1}$.

Assuming we have made choices for the α_j and $\delta_{k>1}$, we wish to justify that we can choose the input vector for the p inputs of B independently. To do this we note that we can determine equality of complex matrices by showing they perform the same operation on all basis elements.

Claim: The set of all vectors of the form $\{v_d \otimes \dots \otimes v_1 \otimes x\}$ where $v_j \in \mathbb{H}^{\otimes p}$ and $x \in \mathbb{H}^{\otimes m}$ contains a basis for $\mathbb{H}^{\otimes(m+dp)}$.

Proof of claim: Note that we may form a basis for $V \otimes V'$ by taking the tensor products of the bases of V and V' , and therefore the above set contains all the basis elements of $\mathbb{H}^{\otimes p} \otimes \dots \otimes \mathbb{H}^{\otimes p} \otimes \mathbb{H}^{\otimes m} \cong \mathbb{H}^{\otimes(m+dp)}$.

Given a choice of values for the α_j , $\delta_{k>1}$ and v we denote this choice by q and use B_q to mean “the sub-diagram B from the series !-box form with this choice of variables”. If one is copying variable names then these values must be the same in each copy of B_q , but we will show the more general case of when you cannot assume that each instance of B_q contains the same choices of values for variables. (Even when creating children of the α_j and $\delta_{k>1}$ these children are contained entirely inside each instance of B so specifying a choice for q for each B determines all the values for parameters inside B .)

The last thing to define here is G_q . G_q is the subdiagram G instantiated with the values described by q , same as for B_q . Once we have chosen values for q we may consider the matrix interpretation of the diagram:

$$\llbracket C \rrbracket \llbracket B_{q_d} \rrbracket \dots \llbracket B_{q_1} \rrbracket \llbracket G_{q_0} \rrbracket \quad (69)$$

$$G_q : \mathbb{H}^{\otimes m} \rightarrow \mathbb{H}^{\otimes n} \quad (70)$$

$$B_q : \mathbb{H}^{\otimes n} \rightarrow \mathbb{H}^{\otimes n} \quad (71)$$

$$C : \mathbb{H}^{\otimes n} \rightarrow \mathbb{C} \quad (72)$$

Given an equation $\mathbb{D}_1 = \mathbb{D}_2$ of two families of diagrams, both parameterised by a (non-nested, separated) !-box δ_1 (among other parameters) we wish to remove our dependence on δ_1 by instead verifying a finite set of equations, each of which has a different value for δ_1 . Note that for this to be the case we require the number of inputs to be equal; i.e. $m_1 = m_2 = m$ and $p_1 = p_2 = p$, but we do not require $n_1 = n_2$ in equation 67. With the aim of reducing notational clutter we instantiate $\delta_1 = d$ and express D_1 and D_2 in series !-box form, with matrix interpretations:

$$\llbracket C_1 \rrbracket \llbracket B_{1,q_d} \rrbracket \dots \llbracket B_{1,q_1} \rrbracket \llbracket G_{1,q_0} \rrbracket \quad (73)$$

$$\llbracket C_2 \rrbracket \llbracket B_{2,q_d} \rrbracket \dots \llbracket B_{2,q_1} \rrbracket \llbracket G_{2,q_0} \rrbracket \quad (74)$$

And we wish to know when these two interpretations are equal. Rather than consider the matrices acting on two independent spaces we view them as acting on the direct sum of those two spaces and represent these maps as block matrices. (We drop the $\llbracket \cdot \rrbracket$ notation when it would appear inside a matrix.)

$$\begin{aligned} & \llbracket C_1 \rrbracket \llbracket B_{1,q_d} \rrbracket \dots \llbracket B_{1,q_1} \rrbracket \llbracket G_{1,q_0} \rrbracket \\ &= \llbracket C_2 \rrbracket \llbracket B_{2,q_d} \rrbracket \dots \llbracket B_{2,q_1} \rrbracket \llbracket G_{2,q_0} \rrbracket \end{aligned} \quad \forall d, q \quad (75)$$

$$\iff [1 \quad -1] \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} B_{1,q_d} & 0 \\ 0 & B_{2,q_d} \end{bmatrix} \dots \begin{bmatrix} B_{1,q_1} & 0 \\ 0 & B_{2,q_1} \end{bmatrix} \begin{bmatrix} G_{1,q_0} & 0 \\ 0 & G_{2,q_0} \end{bmatrix} \begin{bmatrix} \text{id}_m \\ \text{id}_m \end{bmatrix} = 0 \quad \forall d, q \quad (76)$$

Think of this as copying an input vector $x \in \mathbb{H}^m$ as $x :: x$ in $\mathbb{H}^m \oplus \mathbb{H}^m$, then applying

$$\llbracket C_1 \rrbracket \llbracket B_{1,q_d} \rrbracket \dots \llbracket B_{1,q_1} \rrbracket \llbracket G_{1,q_0} \rrbracket$$

and

$$\llbracket C_2 \rrbracket \llbracket B_{2,q_d} \rrbracket \dots \llbracket B_{2,q_1} \rrbracket \llbracket G_{2,q_0} \rrbracket$$

to the left and right copies respectively. After that we apply a minus sign to the right hand result and add that to the left hand result, effectively comparing them and demanding the difference to be 0. We seek to prove:

$$\begin{aligned}
& [1 \quad -1] \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} B_{1,q_d} & 0 \\ 0 & B_{2,q_d} \end{bmatrix} \cdots \begin{bmatrix} B_{1,q_1} & 0 \\ 0 & B_{2,q_1} \end{bmatrix} \begin{bmatrix} G_{1,q_0} & 0 \\ 0 & G_{2,q_0} \end{bmatrix} \begin{bmatrix} \text{id}_m \\ \text{id}_m \end{bmatrix} = 0 \quad \forall d \leq N, q \\
\implies & [1 \quad -1] \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} B_{1,q_d} & 0 \\ 0 & B_{2,q_d} \end{bmatrix} \cdots \begin{bmatrix} B_{1,q_1} & 0 \\ 0 & B_{2,q_1} \end{bmatrix} \begin{bmatrix} G_{1,q_0} & 0 \\ 0 & G_{2,q_0} \end{bmatrix} \begin{bmatrix} \text{id}_m \\ \text{id}_m \end{bmatrix} = 0 \quad \forall d, q
\end{aligned} \tag{77}$$

Recalling that q is the choice of values for α_j , $\delta_{k>1}$ and $v \in \mathbb{H}^{\otimes p}$, we use Q to denote the set of all possible choices. We use B'_q for the matrix that acts as the direct sum of $B_{1,q}$ and $B_{2,q}$:

$$B'_q := \begin{bmatrix} B_{1,q} & 0 \\ 0 & B_{2,q} \end{bmatrix} \tag{78}$$

and inductively define the spaces:

$$V_0 := \text{span} \left\{ \bigcup_{q \in Q} \text{Im} \left(\begin{bmatrix} G_{1,q} & 0 \\ 0 & G_{2,q} \end{bmatrix} \begin{bmatrix} \text{id}_m \\ \text{id}_m \end{bmatrix} \right) \right\} \tag{79}$$

$$V_j := \text{span} \left\{ V_{j-1} \cup \bigcup_{q \in Q} B'_q V_{j-1} \right\} \tag{80}$$

The V_j form an ascending sequence of subspaces, each containing the potential images of up to j applications of B'_q :

$$V_j \geq \text{Im} (B'_{q_k} \dots B'_{q_1} V_0) \quad \forall k \leq j \quad \forall q_k, \dots, q_1 \in Q \tag{81}$$

Claim: There is a number b such that

- if $j < b$ then $V_j > V_{j-1}$
- if $j \geq b$ then $V_j = V_{j-1}$
- $b \leq \dim(\mathbb{H}^{n_1} \oplus \mathbb{H}^{n_2})$

Proof of claim: Define $N := \dim(\mathbb{H}^{n_1} \oplus \mathbb{H}^{n_2})$ and then

- $V_{j-1} \leq V_j \quad \forall j$
- if $V_j = V_{j-1}$ then $V_{j+1} = V_j$
- $V_j \leq \mathbb{H}^{n_1} \oplus \mathbb{H}^{n_2} \quad \forall j$
- $\dim V_{j-1} \leq \dim V_j \leq N \quad \forall j$
- The strictly increasing section of the sequence of the $\dim V_j$ must have length less than N
- We declare b to be the number such that $V_c = V_b \quad \forall c \geq b$, and note $b \leq N$

Let W be the kernel of the map $[1 \quad -1] \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix}$

Claim:

$$\begin{aligned} V_j &\leq W & \forall j \leq N & \quad (82) \\ \implies V_j &\leq W & \forall j & \end{aligned}$$

Proof of claim: Since $V_c = V_N$ when $c \geq N \geq b$ it is enough to show that this is the case for all V_j when $j \leq N$. This is implied by the assumption in our theorem; that for $d \leq N$ our diagrammatic equation holds, and so for any choice of d and q_1, \dots, q_d this matrix equation holds:

$$[1 \quad -1] \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} B_{1,q_d} & 0 \\ 0 & B_{2,q_d} \end{bmatrix} \cdots \begin{bmatrix} B_{1,q_1} & 0 \\ 0 & B_{2,q_1} \end{bmatrix} \begin{bmatrix} G_{1,q_0} & 0 \\ 0 & G_{2,q_0} \end{bmatrix} \begin{bmatrix} \text{id}_m \\ \text{id}_m \end{bmatrix} = 0 \quad (83)$$

We have shown that for any choice of inputs $v \in \mathbb{H}^p \otimes \dots \otimes \mathbb{H}^p \otimes \mathbb{H}^m$, and parameters $\alpha_j, \delta_{k>1}$ our matrix equations hold, and by extension they hold on all elements of the space $\mathbb{H}^{\otimes(m+dp)}$, i.e. that:

$$\begin{aligned} &\forall d \leq N \forall q_d \dots q_1 \\ &[1 \quad -1] \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} B_{1,q_d} & 0 \\ 0 & B_{2,q_d} \end{bmatrix} \cdots \begin{bmatrix} B_{1,q_1} & 0 \\ 0 & B_{2,q_1} \end{bmatrix} \begin{bmatrix} G_{1,q_0} & 0 \\ 0 & G_{2,q_0} \end{bmatrix} \begin{bmatrix} \text{id}_m \\ \text{id}_m \end{bmatrix} = 0 \quad (84) \end{aligned}$$

$$\begin{aligned} \implies &\forall d \forall q_d \dots q_1 \\ &[1 \quad -1] \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix} \begin{bmatrix} B_{1,q_d} & 0 \\ 0 & B_{2,q_d} \end{bmatrix} \cdots \begin{bmatrix} B_{1,q_1} & 0 \\ 0 & B_{2,q_1} \end{bmatrix} \begin{bmatrix} G_{1,q_0} & 0 \\ 0 & G_{2,q_0} \end{bmatrix} \begin{bmatrix} \text{id}_m \\ \text{id}_m \end{bmatrix} = 0 \quad (85) \end{aligned}$$

And therefore:

$$\llbracket C_1 \rrbracket \llbracket B_{1,q_d} \rrbracket \cdots \llbracket B_{1,q_1} \rrbracket \llbracket G_{1,q_0} \rrbracket = \llbracket C_2 \rrbracket \llbracket B_{2,q_d} \rrbracket \cdots \llbracket B_{2,q_1} \rrbracket \llbracket G_{2,q_0} \rrbracket \quad \forall d \leq N \forall q_d \dots q_1 \quad (86)$$

$$\implies \llbracket C_1 \rrbracket \llbracket B_{1,q_d} \rrbracket \cdots \llbracket B_{1,q_1} \rrbracket \llbracket G_{1,q_0} \rrbracket = \llbracket C_2 \rrbracket \llbracket B_{2,q_d} \rrbracket \cdots \llbracket B_{2,q_1} \rrbracket \llbracket G_{2,q_0} \rrbracket \quad \forall d \forall q_d \dots q_1 \quad (87)$$

And therefore for any choice of value for α_j and $\delta_{k>1}$:

$$\llbracket \{ \mathbb{D}_1 \}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \delta_1 = d} \rrbracket = \llbracket \{ \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \delta_1 = d} \rrbracket \quad \forall d \leq N \quad (88)$$

$$\implies \llbracket \{ \mathbb{D}_1 \}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \delta_1 = d} \rrbracket = \llbracket \{ \mathbb{D}_2 \}_{\alpha_1, \dots, \alpha_n, \delta_1, \dots, \delta_m | \delta_1 = d} \rrbracket \quad \forall d \quad (89)$$

□

A.3 Proof of theorem 33

Theorem 33. *Given a parameterised family of equations \mathbb{E} , where the $!$ -boxes are separated and well nested, we can construct a finite set of simple equations $\{\mathbb{E}_\kappa\}_{\kappa \in K}$, such that:*

$$\{\mathbb{E}_\kappa\}_{\kappa \in K} \text{ is sound} \implies \mathbb{E} \text{ is sound} \quad (39)$$

Proof. Throughout this proof we iterate on the set $\{\mathbb{E}_\kappa\}$. While at all times $\{\mathbb{E}_\kappa\}$ is a finite verifying set for \mathbb{E} , it is only at the end that $\{\mathbb{E}_\kappa\}$ is a finite verifying set of simple equations. We first show the existence of an ordered list of the $!$ -boxes present in E , compatible with the nesting order on both of the nesting diagrams of E .

Definition 35. *We construct the ordered list $\delta_{k_1} \succ \delta_{k_2} \succ \dots \succ \delta_{k_n}$ by recursively picking a $!$ -box that is nested in no other $!$ -boxes, then removing that $!$ -box from the nesting diagram. Repeat on the new nesting diagram.*

Definition 36. *The algorithm **!-Removal**:*

- **If we are copying variable names:** *Given a verifying set of equations $\{\mathbb{E}_\kappa\}_{\kappa \in K}$, and a $!$ -box δ_k nested in no other $!$ -boxes present in the \mathbb{E}_κ :*
*We define **!-Remove**(δ_k) as the process described in theorem 30. It acts on the set $\{\mathbb{E}_\kappa\}_{\kappa \in K}$ by acting on each of the \mathbb{E}_κ in turn, finding the value N_κ , and creating the new verification set:*

$$\{\mathbb{E}_\kappa\}_{\kappa \in K'} := \bigcup_{\kappa \in K} \{\mathbb{E}_\kappa \big|_{\delta_k=1}, \dots, \mathbb{E}_\kappa \big|_{\delta_k=N_\kappa}\} \quad (90)$$

- **If we are creating child instances:** *We do as above, but we pick the $!$ -box δ_k such that all its child instances are nested in no other $!$ -boxes present in the \mathbb{E}_κ , and we act not only on each of the \mathbb{E}_κ in turn but also on each of the child instances of δ_k in turn.*

Claims:

- **!-Remove**(δ_k) removes any dependency on δ_k in the verifying set $\{\mathbb{E}_\kappa\}_{\kappa \in K'}$
- $\{\mathbb{E}_\kappa\}_{\kappa \in K'}$ verifies $\{\mathbb{E}_\kappa\}_{\kappa \in K}$
- **!-Remove**(δ_k) does not alter the nesting ordering of any remaining $!$ -boxes and phase variables in the verification pair
- The ordered list $\delta_{k_1} \succ \delta_{k_2} \succ \dots$ provides us with a sequence of $!$ -boxes such that we can apply **!-Remove**($\delta_{k_{n+1}}$) to the output of **!-Remove**(δ_{k_n}).
- This ordered sequence of **!-Removes** results in a finite verifying set that has no dependence on any $!$ -box.

Proof of claims: The first, second and fifth claims follow from Theorem 30. The third and fourth of these claims are easy when we are copying variable names, but when creating child instances of $!$ -boxes below δ_k one should view instantiation as creating (distinctly named) copies of the nesting structure that exists below δ_k .

Removing phase variables is trickier than removing $!$ -boxes, because we know by theorem 32 that to do so in a manner compatible with $!$ -box removal we first need to know the largest number of $!$ -box

instances we are going to need. Since we have already constructed the $\{\mathbb{E}_\kappa\}_{\kappa \in K}$ we can find the equation that resulted from every !-box δ_k being instantiated at its largest amount, N_k , and use that equation.

Definition 37. We use \mathbb{E}' to denote the !-box free equation that is the result of instantiating each !-box δ_k at its largest required amount N_k

Claim: The equation \mathbb{E}' contains the largest number of instances of α_j compared to any other equation \mathbb{E}_κ

Proof of claim: The number of instances of α_j is determined by the number of times the !-boxes have been instantiated.

Definition 38. The algorithm α -Removal: Given a verifying set $\{\mathbb{E}_\kappa\}_{\kappa \in K}$ we construct the set A_j for variable α_j by considering the degree of α_j in \mathbb{E}' , and then choosing enough valid values of α_j to reach the amount dictated by theorem 18. We then form:

$$\{\mathbb{E}_\kappa\}_{\kappa \in K'} := \bigcup_{\kappa \in K, a \in A_j} \{\mathbb{E}_\kappa \mid_{\alpha_j=a}\} \quad (91)$$

Claim: By theorem 32 $\{\mathbb{E}_\kappa\}_{\kappa \in K'}$ verifies $\{\mathbb{E}_\kappa\}_{\kappa \in K}$

And finally:

Claim: Starting with the verifying set $\{\mathbb{E}\}$: After applying !-Removes in the order dictated by \prec and then applying all possible α -Removes we construct a finite set $\{\mathbb{E}_\kappa\}_{\kappa \in K}$ of simple equations that verifies \mathbb{E} .

□

B Generators and degrees

We show here the generators of our three example languages (ZX, ZH and $ZW_{\mathbb{C}}$), and then show the matrix degrees of these interpretations.

B.1 Generators

B.1.1 ZX

- The Z spider has the following interpretation in $\text{Mat}_{\mathbb{C}}$

$$\left[\left[\left\{ \begin{array}{c} \vdots \\ \text{Z spider} \\ \vdots \end{array} \right\} \mid_{\alpha=a} \right] \right] = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & e^{ia} \end{bmatrix} \quad (92)$$

Making the substitution $Y := e^{i\alpha}$ (and therefore $Y^n = e^{in\alpha}$) the Z spider has this interpretation in $\text{Mat}_{\mathbb{C}[Y, Y^{-1}]}$:

$$\left[\left[\begin{array}{c} \vdots \\ \text{X} \\ \vdots \end{array} \right] \right] = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & Y \end{bmatrix} \quad (93)$$

- The Hadamard node has the following interpretation

$$\left[\left[\begin{array}{c} \vdots \\ \text{H} \\ \vdots \end{array} \right] \right] = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (94)$$

And admits no parameters.

- The X spider interpretation is found by applying Hadamards nodes on all inputs and outputs of the corresponding Z spider.

B.1.2 ZH

- The H box in ZH has the following interpretation in $\text{Mat}_{\mathbb{C}}$

$$\left[\left\{ \left[\begin{array}{c} \vdots \\ \text{H} \\ \vdots \end{array} \right] \right\}_{\alpha=a} \right] = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & & \vdots \\ \vdots & & \ddots & \\ 1 & \dots & 1 & a \end{bmatrix} \quad (95)$$

We can simply equate $Y := \alpha$ and get the interpretation in $\text{Mat}_{\mathbb{C}[Y, Y^{-1}]}$:

$$\left[\left[\begin{array}{c} \vdots \\ \text{H} \\ \vdots \end{array} \right] \right] = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & & \vdots \\ \vdots & & \ddots & \\ 1 & \dots & 1 & Y \end{bmatrix} \quad (96)$$

- The Z spider in ZH admits no parameters, and has the following interpretation

$$\left[\left[\begin{array}{c} \vdots \\ \text{Z} \\ \vdots \end{array} \right] \right] = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & 1 \end{bmatrix} \quad (97)$$

B.1.3 ZW

We are explicitly using $ZW_{\mathbb{C}}$ here for compatibility with the other languages.

- The Crossing x has interpretation

$$\left[\left[\begin{array}{c} \diagup \diagdown \\ \diagdown \diagup \\ \times \end{array} \right] \right] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (98)$$

- The W spider in bra-ket notation has interpretation

$$\left[\left[\begin{array}{c} \vdots \\ \diagdown \diagup \\ \bullet \\ \diagup \diagdown \\ \vdots \end{array} \right] \right] = \sum_{k=1}^n \underbrace{|0 \dots 0\rangle}_{k-1} \underbrace{|10 \dots 0\rangle}_{n-k} \quad (99)$$

- The Z spider is parameterised by $\alpha \in \mathbb{C}$ and has interpretation

$$\left[\left\{ \left[\begin{array}{c} \vdots \\ \diagdown \diagup \\ \alpha \\ \diagup \diagdown \\ \vdots \end{array} \right] \right\}_{\alpha=a} \right] = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & a \end{bmatrix} \quad (100)$$

We can again simply equate $Y := \alpha$ and get the interpretation in $\text{Mat}_{\mathbb{C}[Y, Y^{-1}]}$:

$$\left[\left[\begin{array}{c} \vdots \\ \diagdown \diagup \\ \alpha \\ \diagup \diagdown \\ \vdots \end{array} \right] \right] = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & 0 & Y \end{bmatrix} \quad (101)$$

B.2 degrees

We will consider nodes parameterised by a single variable α , and express their degree with respect to Y following the convention of appendix B.1.

B.2.1 ZX

Using $Y^n := e^{ni\alpha}$, the degrees in Y of the generators (for $n \geq 0$) are:

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = n \tag{102}$$

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } -n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{103}$$

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = n \tag{104}$$

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } -n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{105}$$

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \vdots \\ \square \\ \vdots \\ \vdots \end{array} = 0 \tag{106}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{102}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } -n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = n \tag{103}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{104}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } -n\alpha \\ \diagup \quad \diagdown \\ \vdots \end{array} = n \tag{105}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \vdots \\ \square \\ \vdots \\ \vdots \end{array} = 0 \tag{106}$$

B.2.2 ZH

We equate $Y := \alpha$, and for P any Laurent polynomial:

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } P(\alpha) \\ \diagup \quad \diagdown \\ \vdots \end{array} = \deg_Y^{+} P \tag{107}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } P(\alpha) \\ \diagup \quad \diagdown \\ \vdots \end{array} = \deg_Y^{-} P \tag{107}$$

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \circ \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{108}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \circ \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{108}$$

B.2.3 ZW

We equate $Y := \alpha$, and for P any Laurent polynomial:

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{109}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \bullet \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{109}$$

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \otimes \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{110}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \otimes \\ \diagup \quad \diagdown \\ \vdots \end{array} = 0 \tag{110}$$

$$\deg_{\alpha}^{+} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } P(\alpha) \\ \diagup \quad \diagdown \\ \vdots \end{array} = \deg_Y^{+} P \tag{111}$$

$$\deg_{\alpha}^{-} \begin{array}{c} \vdots \\ \diagdown \quad \diagup \\ \text{\scriptsize } P(\alpha) \\ \diagup \quad \diagdown \\ \vdots \end{array} = \deg_Y^{-} P \tag{111}$$

$$\tag{112}$$

C Separability

We describe a non-separated pair of !-boxes as **separable** if we can perform the following operation:

$$\begin{array}{c} \delta_2 \\ \vdots \\ \square_{B_2} \\ \vdots \\ \vdots \\ \vdots \\ \square_{B_1} \\ \vdots \\ \delta_1 \end{array} = \begin{array}{c} \delta_2 \\ \vdots \\ \square_{B'_2} \\ \vdots \\ \square_{B_3} \\ \vdots \\ \square_{B'_1} \\ \vdots \\ \delta_1 \end{array} \tag{113}$$

We define pairs of nodes as separable if we can always separate !-boxes that are joined by edges between these pairs of nodes. Note that we only need to consider nodes that have arbitrary arity, since only they can be connected to !-boxes.

- The following pairs of nodes are separable, by language:

$$\text{ZX: } (\text{green spider}, \text{red spider}) \quad (\text{green spider}, \text{green spider}) \quad (\text{red spider}, \text{red spider}) \quad (114)$$

$$\text{ZH: } (\text{white spider}, \text{white spider}) \quad (\text{white spider}, \text{grey spider}) \quad (\text{grey spider}, \text{white spider}) \quad (115)$$

$$\text{ZW: } (\text{white spider}, \text{white spider}) \quad (\text{white spider}, \text{black spider}) \quad (116)$$

The proofs of these follow immediately from the spider and bialgebra laws in the respective languages.

- The following pairs of nodes are assumed to not be separable, by language:

$$\text{ZX: } \text{Always separable} \quad (117)$$

$$\text{ZH: } (\text{white spider}, \text{white spider}) \quad (\text{white spider}, \text{white spider}) \quad (118)$$

$$\text{ZW: } (\text{black spider}, \text{black spider}) \quad (119)$$

Note that it is enough to specify the phase-free versions of these interactions, because phases can always be moved away from the critical nodes.