Quantum Graphical Calculi and their Algebraic Underpinnings

Hector Miller-Bakewell

University of Oxford

2020-09-03

Quantum Circuits

Quantum Graphical Calculi

Interpolation

Phase Homomorphisms

Galois Theory

Quantum Circuits

(Qubit) Quantum Circuits

A qubit is a vector in $\mathbb{C}^2$

$$\begin{pmatrix} a \\ b \end{pmatrix} \tag{1}$$

A register of qubits is a tensor product of qubits

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} \tag{2}$$

Quantum Circuits

A quantum circuit takes a register of n qubits, i.e. a vector in $(\mathbb{C}^2)^{\otimes n}$, and produces a register of n qubits, via a linear map.

So it's just a complex matrix...

- That is too large to efficiently handle
- Knowing the matrix doesn't tell you how to enact the algorithm on hardware
- Two registers are experimentally indistinguishable if $v = e^{i\alpha}v'$ (and we will ignore this)

Quantum Circuits

The purpose of a quantum circuit is to $\circ$-, $\otimes$- factorise the desired algorithm (big square complex matrix) into the component *gates* that your quantum computer can actually perform.

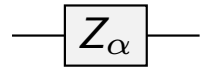
It is important to remember that during this talk we are, ultimately, manipulating matrix factorisations.

Each quantum computer has a different collection of available gates and constraints. For example some gates can only be applied on certain pairs of qubits.

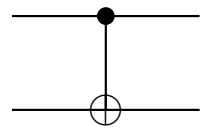
Quantum Circuits

An example, *universal*, collection of quantum hardware gates

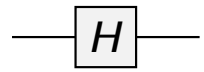
$$Z_\alpha := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \qquad \text{(3)}$$



$$\mathrm{CNOT}_{1,2} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{(4)}$$



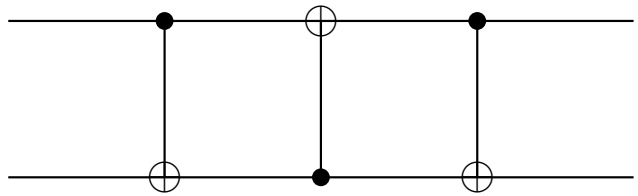
$$\mathrm{H} := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{(5)}$$



Quantum circuits are read left-to-right

Quantum Circuits

This circuit sends the state $v \otimes w$ to $w \otimes v$:



(6)

$$\mathrm{CNOT}_{1,2} \circ \mathrm{CNOT}_{2,1} \circ \mathrm{CNOT}_{1,2} \tag{7}$$

Quantum Circuits

These gates take n qubits to n qubits.

Changing the order of the qubits isn't a native operation (wires cannot be bent or crossed). Quantum Circuits form a PRO not a PROP.

But the existence of the swap operation shows we should be in a PROP.

Quantum Graphical Calculi

Quantum Graphical Calculi

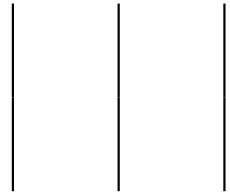
Quantum Graphical Calculi introduce three important things:

- Wire bending
- Morphisms of any arity (don't need the same number of inputs as outputs)
- Complete sets of local rules

Wires

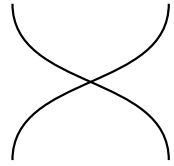
Wire Bending

- Product categories (PROs)



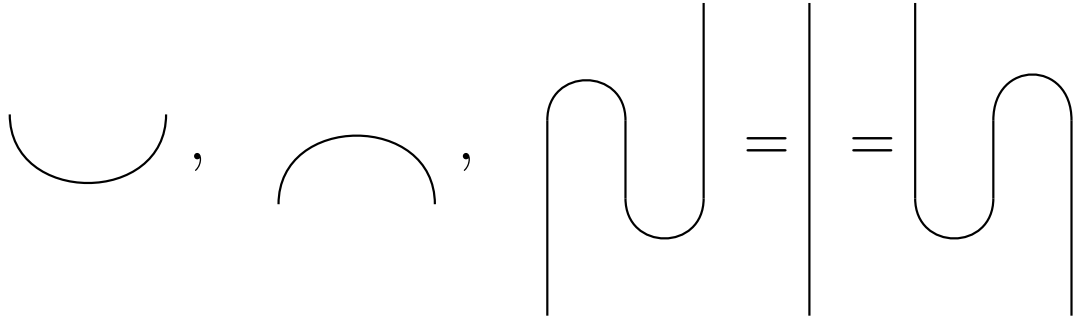
(8)

- Product categories with Permutations (PROPs)



(9)

- Add compact closure



(10)

Interpretation

$$[\![\cdot]\!] : \mathbf{Wire} \to \mathrm{Mat}_{\mathbb{C}} \tag{11}$$

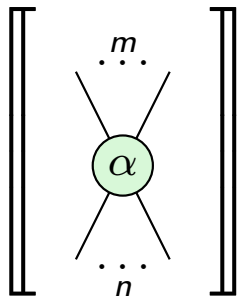
$$[\![\; | \;]\!] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad [\![\; \times \;]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{12}$$

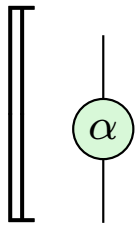
$$[\![\; \cup \;]\!] = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \qquad [\![\; \cap \;]\!] = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \tag{13}$$

ZX

ZX - Green Spider

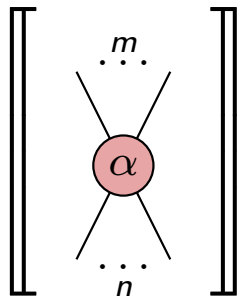
$$[\![\cdot]\!] : \mathbf{ZX} \to \mathrm{Mat}_{\mathbb{C}} \tag{14}$$

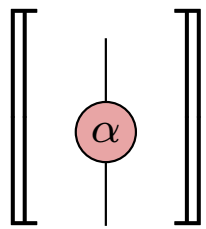
$$[\![\;  \;]\!] = |0\rangle^{\otimes m}\langle 0|^{\otimes n} + e^{i\alpha}|1\rangle^{\otimes m}\langle 1|^{\otimes n} \tag{15}$$

$$[\![\;  \;]\!] = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \tag{16}$$

ZX - Red Spider

$$[\![\cdot]\!] : \mathbf{ZX} \to \mathrm{Mat}_{\mathbb{C}} \tag{17}$$

$$[\![\text{ 
}]\!] = |+\rangle^{\otimes m}\langle +|^{\otimes n} + e^{i\alpha}|-\rangle^{\otimes m}\langle -|^{\otimes n} \tag{18}$$

$$[\![\text{ 
}]\!] = \frac{1}{2}\begin{pmatrix} 1+e^{i\alpha} & 1-e^{i\alpha} \\ 1-e^{i\alpha} & 1+e^{i\alpha} \end{pmatrix} \tag{19}$$

ZX - Hadamard

$$[\![\cdot]\!] : \mathbf{ZX} \to \mathrm{Mat}_{\mathbb{C}} \tag{20}$$

$$[\![\quad \boxed{} \quad]\!] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{21}$$

It's redundant as a generator, but so useful that we keep it.

Fragments

A **fragment** of a calculus is the graphical calculus generated by a subset of the generators.

The **Clifford** fragment of ZX has $\alpha \in < \frac{\pi}{2} >$

The **Clifford+T** fragment of ZX has $\alpha \in < \frac{\pi}{4} >$

The **Universal** fragment of ZX has $\alpha \in [0, 2\pi)$

$< \frac{\pi}{4} > \subset G \subset [0, 2\pi)$

ZX - Rules

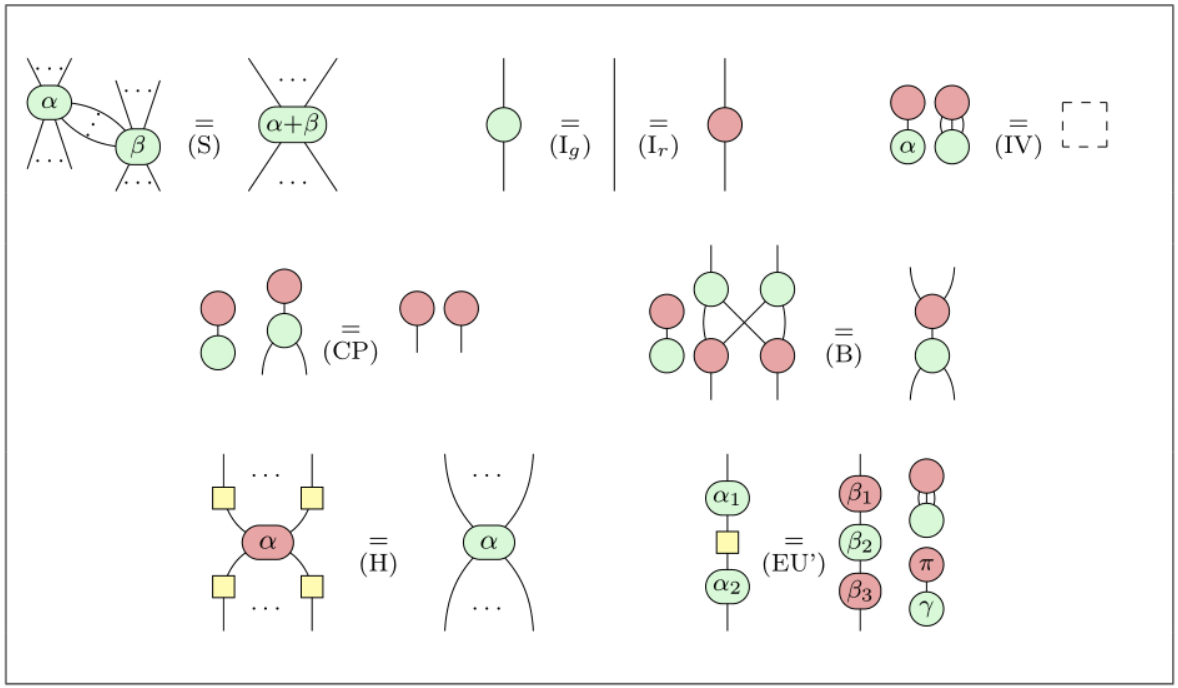
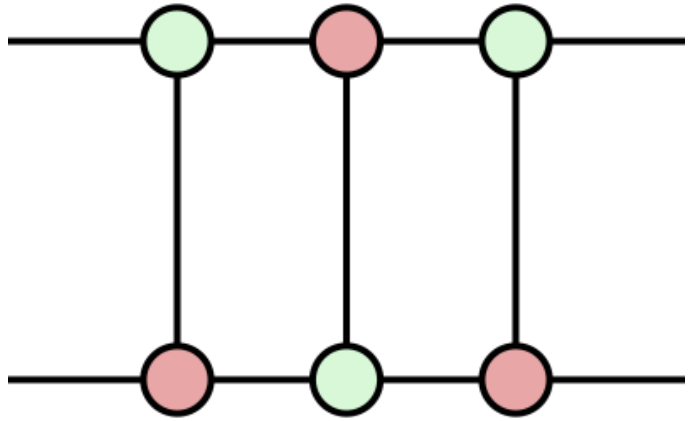
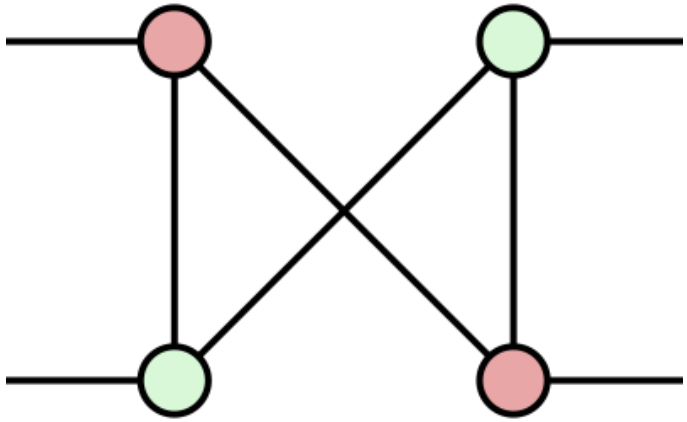


Figure 6.6: Set of rules ZX for the ZX-Calculus with scalars from Ref. [Vil19]. The right-hand side of (IV) is an empty diagram. (...) denote zero or more wires, while (.$^{\cdot}$) denote one or more wires. In rule (EU'), $\beta_1, \beta_2, \beta_3$ and γ can be determined as follows: $x^+ := \frac{\alpha_1+\alpha_2}{2}$, $x^- := x^+ - \alpha_2$, $z := -\sin x^+ + i\cos x^-$ and $z' := \cos x^+ - i\sin x^-$, then $\beta_1 = \arg z + \arg z', \beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right), \beta_3 = \arg z - \arg z', \gamma = x^+ - \arg(z) + \frac{\pi-\beta_2}{2}$ where by convention $\arg(0) := 0$ and $z' = 0 \implies \beta_2 = 0$.

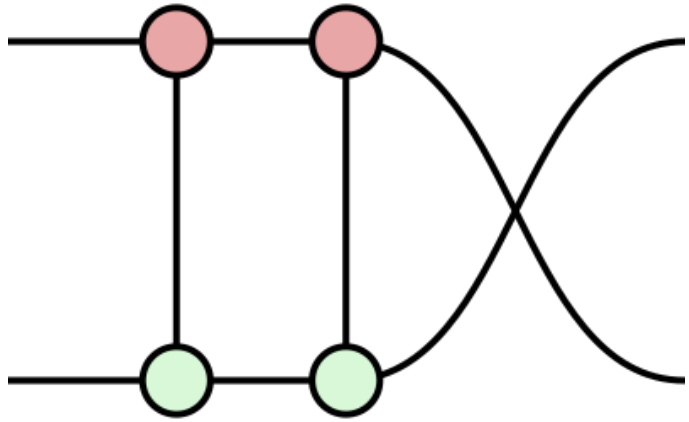
ZX - Derivation



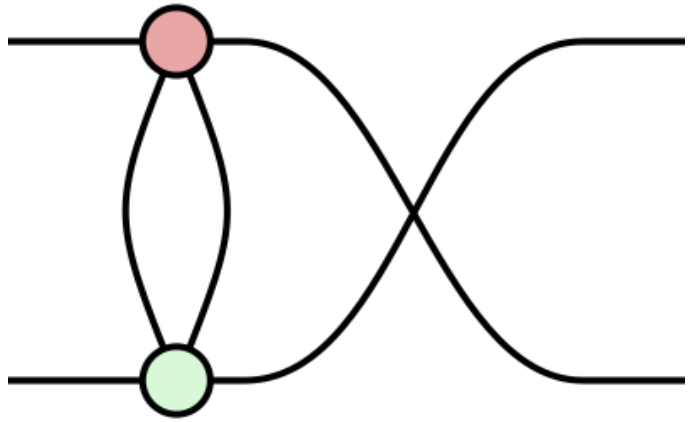
ZX - Derivation



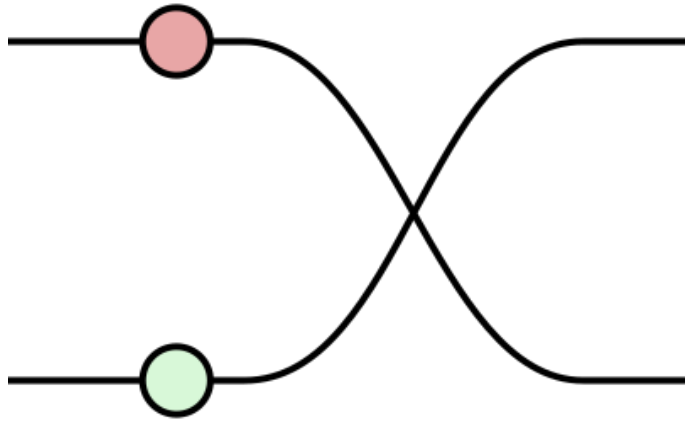
ZX - Derivation



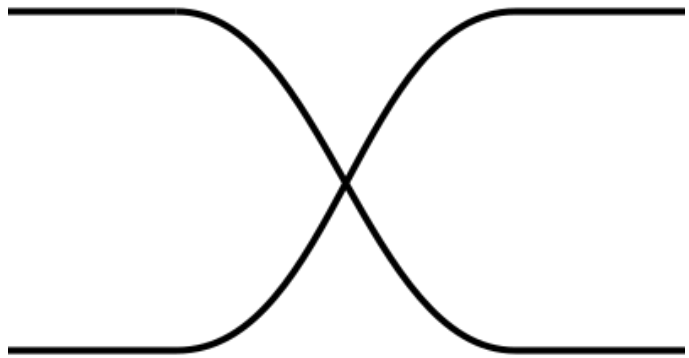
ZX - Derivation



ZX - Derivation



ZX - Derivation



ZX - Summary

Quantum Circuits (with the standard gate set) are ZX diagrams

ZX is universal for matrices : $(\mathbb{C}^2)^{\otimes m} \to (\mathbb{C}^2)^{\otimes n}$

ZX is sound and complete

That (EU') rule is horrible.

$\beta_1, \beta_2, \beta_3$ and γ can be determined as follows: $x^+ := \frac{\alpha_1+\alpha_2}{2}$, $x^- := x^+ - \alpha_2$, $z := -\sin x^+ + i\cos x^-$ and $z' := \cos x^+ - i\sin x^-$, then $\beta_1 = \arg z + \arg z', \beta_2 = 2\arg\left(i + \left|\frac{z}{z'}\right|\right), \beta_3 = \arg z - \arg z', \gamma = x^+ - \arg(z) + \frac{\pi-\beta_2}{2}$ where by convention $\arg(0) := 0$ and $z' = 0 \implies \beta_2 = 0$.

ZQ

ZQ - Z spider

$$[\![\cdot]\!] : \mathbf{ZQ} \to \mathrm{Mat}_{\mathbb{C}} \tag{22}$$

$$[\![\; \overset{m}{\cdots} \; \underset{n}{\cdots} \;]\!] = |0\rangle^{\otimes m}\langle 0|^{\otimes n} + |1\rangle^{\otimes m}\langle 1|^{\otimes n} \tag{23}$$

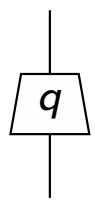
$$[\![\; \circ \;]\!] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{24}$$

ZQ - Decorated edges

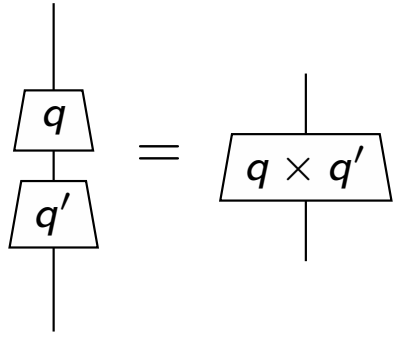
$$[\![\cdot]\!] : \mathbf{ZQ} \to \mathrm{Mat}_{\mathbb{C}} \tag{25}$$

$$q = q_w + iq_x + jq_y + kq_z \in \hat{Q} \tag{26}$$

$$\left[\!\!\left[\quad \right]\!\!\right] = \begin{pmatrix} q_w - iq_z & -q_y - iq_x \\ -iq_y + iq_x & q_w + iq_z \end{pmatrix} \tag{27}$$



ZQ - Q Rule



(28)

This captures everything from (EU') in ZX

ZQ - Summary

ZQ is based on Z spiders and decorated edges

Neatly captures the ‘weirdness’ of Euler Angle Decomposition

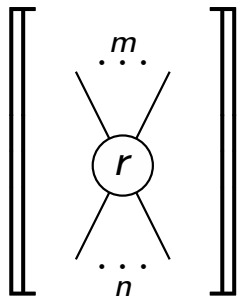
No longer looks like the standard gate set for quantum computers

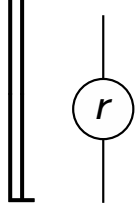
But does start to resemble the optimisation process inside TriQ

ZW

ZW - White Spider

$$[\![\cdot]\!] : \mathbf{ZW}_R \to \mathrm{Mat}_R \tag{29}$$

$$[\![\text{  }]\!] = |0\rangle^{\otimes m}\langle 0|^{\otimes n} + r|1\rangle^{\otimes m}\langle 1|^{\otimes n} \tag{30}$$

$$[\![\text{  }]\!] = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \tag{31}$$

ZW - Black Spider

$$[\![\cdot]\!] : \mathbf{ZW}_R \to \mathrm{Mat}_R \tag{32}$$

$$\left[\!\!\left[\; \overset{m}{\cdot\vdots\cdot} \; \right]\!\!\right] = \Sigma_k |\underbrace{0 \ldots 0}_{k-1} \, 1 \, \underbrace{0 \ldots 0}_{m-k}\rangle \tag{33}$$

$$\left[\!\!\left[\; \right]\!\!\right] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{34}$$

ZW - Summary

ZW is strongly linked to the physics of fermionic oscillators

ZW has a normal form for diagrams

ZW is based on a ring, and is universal for R-bits

RING

RING - Generators

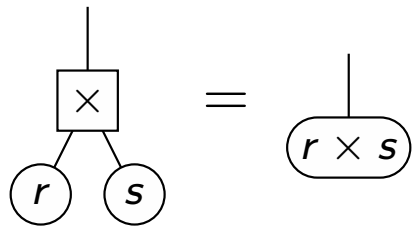
$$[\![\cdot]\!] : \mathrm{RING}_R \to \mathsf{Mat}_R \tag{35}$$

$$[\![\; \times \;]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{36}$$

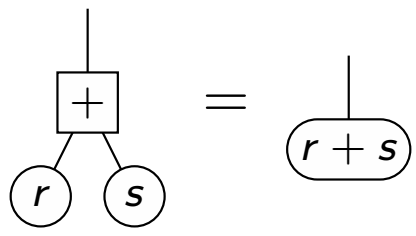
$$[\![\; + \;]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \tag{37}$$

$$[\![\; r \;]\!] = \begin{pmatrix} 1 \\ r \end{pmatrix} \tag{38}$$

RING - Generators



(39)



(40)

RING - Summary

RING is actually very close to ZW

RING is universal, sound and complete

RING will be our example going forwards

Quantum Graphical Calculi - Summary

All of these calculi are sound and complete

Your choice of generators controls how algebraic your language ends up feeling

Interpolation

Interpolation

Let's start with polynomial interpolation:

p is a polynomial of degree at most d in $\mathbb{C}[X]$

If we know the value $p(x)$ at $d+1$ points

Then we can determine the coefficients of p

Interpolation

$$p := ax^2 + bx + c \tag{41}$$

$$\text{if} \tag{42}$$

$$p(0) = 0 \qquad p(1) = 1 \qquad p(2) = 2 \tag{43}$$

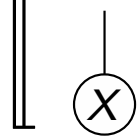
$$\text{then} \tag{44}$$

$$a = 0 \qquad b = 1 \qquad c = 0 \tag{45}$$

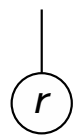
Phase Variables

What does it mean to have a variable in your diagram?

$$\left[\!\!\left[\; \right]\!\!\right] = ? \tag{46}$$

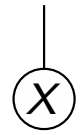


$$\left[\!\!\left[\; \right]\!\!\right] = \begin{pmatrix} 1 \\ r \end{pmatrix} \tag{47}$$



Phase Variables

Let's codify this.



$$\in \mathrm{RING}_{\mathbb{C}[X]} \tag{48}$$

$$\left[\!\!\left[\quad \right]\!\!\right] = \begin{pmatrix} 1 \\ X \end{pmatrix} \in \mathsf{Mat}_{\mathbb{C}[X]} \tag{49}$$

$$\begin{array}{ccc} \mathrm{RING}_{\mathbb{C}[X]} & \xrightarrow{ev_X} & \mathrm{RING}_{\mathbb{C}} \\ \downarrow{\scriptstyle [\![\cdot]\!]} & & \downarrow{\scriptstyle [\![\cdot]\!]} \\ \mathbb{C}[X]\text{-bit} & \xrightarrow{ev_X} & \mathbb{C}\text{-bit} \end{array} \tag{50}$$

Phase Variables

$$[\![D_1]\!] = [\![D_2]\!] \qquad D_1,\ D_2 \in \mathrm{RING}_{\mathbb{C}[X]} \tag{51}$$

$$[\![D_1]\!] = [\![D_2]\!] \qquad \in \mathrm{Mat}_{\mathbb{C}[X]} \tag{52}$$

$$[\![D_1]\!] - [\![D_2]\!] = 0 \qquad \in \mathrm{Mat}_{\mathbb{C}[X]} \tag{53}$$

When is a matrix of polynomials equal to 0? When all the entries are the 0 polynomial.

How do we show a polynomial is 0? Show that p(X) = 0 for $d + 1$ many values of X.

Matrix degree

So how do we work out the maximum degree of the polynomials in a matrix?

We know how much each generator of our calculus can contribute to the degree.

Matrix degree

$$\deg\left(\ \boxed{+}\ \right) = 0 \qquad \deg\left(\ \boxed{\times}\ \right) = 0 \tag{54}$$

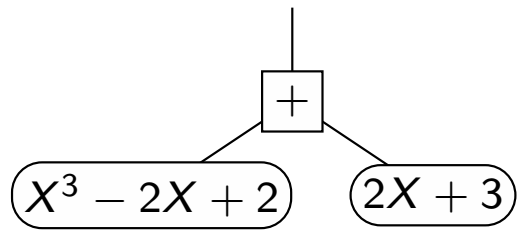
$$\deg\left(\ \boxed{f(X)}\ \right) = \min(\deg(f(X)), 0) \tag{55}$$

$$\deg\left(D_1 \otimes D_2\right) \leq \deg(D_1) + \deg(D_2) \tag{56}$$

$$\deg\left(D_1 \circ D_2\right) \leq \deg(D_1) + \deg(D_2) \tag{57}$$

Matrix degree

$$\deg\left(\quad\right) \leq (0+3+1) \tag{58}$$



This is easy in RING and ZW, fiddly in ZX, and impossible(?) in ZQ.

Recap

How can we tell if two diagrams containing variables are equal without calculating the interpretation? Check a finite number of values of that variable.

This scales up to diagrams containing a finite number of distinct variables.

We talked about the qubit version, but it can be made to work with arbitrary rings.

Phase Homomorphisms

Phase Homomorphisms

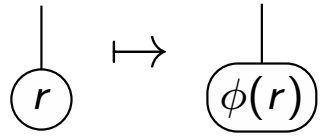
Phase homomorphisms are actually functors between PROPs

Starting with the ring homomorphism

$$\phi : R \to S \tag{59}$$

we construct

$$\hat{\phi} : \mathrm{RING}_R \to \mathrm{RING}_S \tag{60}$$



(61)

Phase Homomorphism Pairs

Phase homomorphisms aren't useful for this talk unless there is a similar action on the interpretation

$$\phi : R \to S \tag{62}$$

$$\hat{\phi} : \mathrm{RING}_R \to \mathrm{RING}_S \tag{63}$$

$$\tilde{\phi} : R\text{-bit} \to S\text{-bit} \tag{64}$$

s.t.
$$\begin{array}{ccc} \mathrm{RING}_R & \xrightarrow{\hat{\phi}} & \mathrm{RING}_S \\ \downarrow{\scriptstyle [\![\,\cdot\,]\!]} & & \downarrow{\scriptstyle [\![\,\cdot\,]\!]} \\ R\text{-bit} & \xrightarrow{\tilde{\phi}} & S\text{-bit} \end{array} \quad \text{commutes} \tag{65}$$

For RING and ZW we construct $\hat{\phi}$ by applying ϕ on phases, and $\tilde{\phi}$ by applying ϕ on each matrix entry

Phase Homomorphism Pairs

What can we do with these pairs?

$$[\![D_1]\!] = [\![D_2]\!] \tag{66}$$

$$\implies \tilde{\phi}[\![D_1]\!] = \tilde{\phi}[\![D_2]\!] \tag{67}$$

$$\implies \left[\!\!\left[\hat{\phi} D_1 \right]\!\!\right] = \left[\!\!\left[\hat{\phi} D_2 \right]\!\!\right] \tag{68}$$

So from a sound equation we get another sound equation

Aside - phase homomorphisms of derivations

$$\textsc{ring} \vdash D_1 = D_2 \tag{69}$$

$$D_1 \overset{r_1}{=} D' \overset{r_2}{=} D'' \ldots \overset{r_n}{=} D_2 \tag{70}$$

$$\implies \hat{\phi} D_1 \overset{\hat{\phi} r_1}{=} \hat{\phi} D' \overset{\hat{\phi} r_2}{=} \hat{\phi} D'' \ldots \overset{\hat{\phi} r_n}{=} \hat{\phi} D_2 \tag{71}$$

$$\implies \hat{\phi} D_1 \overset{r_1}{=} \hat{\phi} D' \overset{r_2}{=} \hat{\phi} D'' \ldots \overset{r_n}{=} \hat{\phi} D_2 \tag{72}$$

$$\textsc{ring} \vdash \hat{\phi} D_1 = \hat{\phi} D_2 \tag{73}$$

So $\hat{\phi}$ also preserves derivations in $\textsc{ring}$ and ZW, but not in ZX

Phase Homomorphism Pairs

Phase homomorphism pairs allow us to generate new, sound equations by applying homomorphisms to phases.

For RING and ZW we construct $\hat{\phi}$ by applying ϕ on phases, and $\tilde{\phi}$ by applying ϕ on each matrix entry

For ZX the phase endomorphisms of the finite additive group G, $< \pi/4 > \subset G \subset [0, 2\pi)$, are the automorphisms $\alpha \mapsto j\alpha$, $j \equiv 1$ or 7 mod 8.

Galois Theory

Galois Theory

Galois Theory (at least those bits we will need for this talk) concerns pairs of fields $K \subset L$, and the field automorphisms of L that preserve K.

During this we examine L and K as fields, but also examine L as a K-vector space, and examine how irreducible polynomials in $K[X]$ factorise in $L[X]$.

Galois Theory - Example

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(\sqrt{2})$ forms a 2-dimensional $\mathbb{Q}$ vector space, as every element of $\mathbb{Q}(\sqrt{2})$ is of the form $a + b\sqrt{2}$ with a and b in $\mathbb{Q}$.

Galois Theory - Example

The field automorphisms of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ are:

$$id : a + b\sqrt{2} \mapsto a + b\sqrt{2} \tag{74}$$

$$\tau : a + b\sqrt{2} \mapsto a - b\sqrt{2} \tag{75}$$

τ permutes the roots of the irreducible polynomial $X^2 + 2 \in \mathbb{Q}[X]$ once it has been factorised as $(X - \sqrt{2})(X + \sqrt{2})$ in $\mathbb{Q}(\sqrt{2})[X]$

Fundamental Theorem of Galois Theory

Part of the fundamental theorem of Galois theory:

If L over K is a finite, normal field extension inside $\mathbb{C}$ then the Galois Group $\mathrm{Gal}(L/K)$ of field automorphisms of L that fix K has order $\dim_K(L)$

Note that we'll be working inside $\mathbb{C}$

The Plan

Starting with the question $[\![D_1(X)]\!] \stackrel{?}{=} [\![D_2(X)]\!]$ we will

- Work out how many values of X we need for interpolation
- Construct a Galois Group that has a large enough orbit
- Constrained such that the automorphisms fix every constant in our diagram
- Turn the Galois automorphisms into phase automorphism pairs
- Then check a single value x for X

The Plan

$$[\![D_1(x)]\!] = [\![D_2(x)]\!] \tag{76}$$

$$\implies \left[\!\!\left[\hat{\phi}_1 D_1(x) \right]\!\!\right] = \left[\!\!\left[\hat{\phi}_1 D_2(x) \right]\!\!\right] \tag{77}$$

$$\implies [\![D_1(\phi_1 x)]\!] = [\![D_2(\phi_1 x)]\!] \tag{78}$$

$$\implies [\![D_1(\phi_2 x)]\!] = [\![D_2(\phi_2 x)]\!] \tag{79}$$

$$\vdots \tag{80}$$

$$\implies [\![D_1(\phi_d x)]\!] = [\![D_2(\phi_d x)]\!] \tag{81}$$

$\therefore$ by interpolation $[\![D_1(X)]\!] = [\![D_2(X)]\!]$.

Justification

To justify the Galois Theory part:

For any list of natural numbers $d_1, \ldots, d_n$ and finitely generated field extension K of $\mathbb{Q}$ we can construct elements $a_1, \ldots, a_n$ of $\mathbb{C}$ (which happen to be roots of unity) such that

$$\mathrm{Gal}(K(a_1, \ldots, a_n)/K) \cong \mathrm{Gal}(K(a_1)/K) \times \cdots \times \mathrm{Gal}(K(a_n)/K) \tag{82}$$

$$|\mathrm{Gal}(K(a_j)/K)| \geq d_j \qquad \forall j \tag{83}$$

Recap

Starting with the question

$$[\![D_1(X)]\!] \stackrel{?}{=} [\![D_2(X)]\!] \tag{84}$$

we can verify it by checking a single, well-chosen, value

$$[\![D_1(x)]\!] \stackrel{?}{=} [\![D_2(x)]\!] \tag{85}$$

We can do this for RING, ZW, and ZX

Going backwards

If a phase appears less often that its algebraic degree then check if it can be replaced with a phase variable.

Summary

We covered:

- Quantum circuits are a type of ZX diagram
- ZX, ZW, ZQ, RING
- Interpolation of polynomials allows us to verify parameterised diagram equations via finite sampling
- Homomorphisms can be done at the level of diagrams, giving us semantics and syntax preserving phase homomorphism pairs
- Galois Theory allows us to combine these ideas, letting us verify equations with a single sample
- These matrix factorisations have intrinsic algebraic properties that we can and should use.

Thank you.