A gentle introduction to ZX calculus

Fabrizio Genovese

QSig Workshop
2024/01/26

What are graphical calculi?

As the name suggests, **graphical calculi** allow you to do math pictorially.

What are graphical calculi?

As the name suggests, **graphical calculi** allow you to do math pictorially.

They derive their formal strength from **Category Theory**.

What are graphical calculi?

As the name suggests, **graphical calculi** allow you to do math pictorially.

They derive their formal strength from **Category Theory**.

They have been applied to various fields, such as functional programming, linguistics, linear algebra and most importantly quantum computing.

String Diagrams

This is a wire. It represents a 'system' of sorts.

String Diagrams

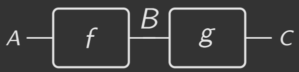
This is a process, turning a system A into a system B.

String Diagrams

The process that 'does nothing' is simply not drawn.

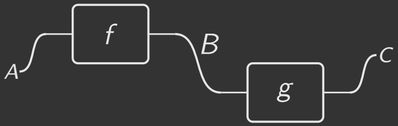
String Diagrams

Processes can be composed if their inputs and outputs match.



String Diagrams

Only topology matters. We can deform these pictures as long as connectivity stays as is.

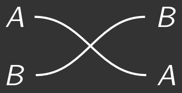


String Diagrams

We can also consider multiple systems at the same time.

String Diagrams

And swap systems' places.

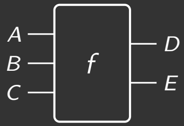


String Diagrams

We also have a **trivial system**, which we don't draw.

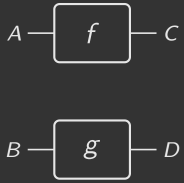
String Diagrams

Processes can act on multiple systems at the same time.



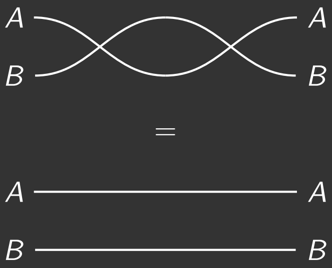
String Diagrams

We can also compose processes in parallel.



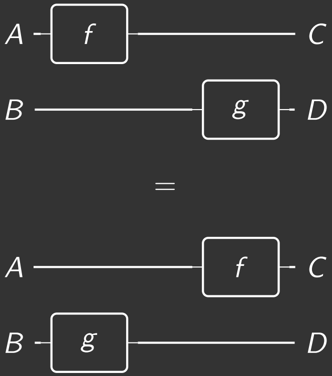
String Diagrams

Finally, some equations hold.



String Diagrams

Finally, some equations hold.



Example: Sets and Functions

A system is just a set.

$$\begin{tikzcd} A \arrow[r, dash] & A \end{tikzcd}$$

Example: Sets and Functions

A process is a function between sets.

Example: Sets and Functions

This is the identity function sending every element to itself.

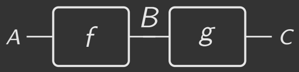
$$A \to A$$
$$a \mapsto a$$

Example: Sets and Functions

Just function composition:

$$A \xrightarrow{g \circ f} C$$

$$(g \circ f)(a) = g(f(a))$$



Example: Sets and Functions

This is the cartesian product

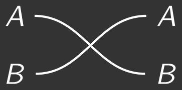
$$A \times B$$

$$\begin{tikzcd} A \arrow[r, dash] & A \\ B \arrow[r, dash] & B \end{tikzcd}$$

Example: Sets and Functions

The swap is the function

$$A \times B \to B \times A$$
$$(a, b) \mapsto (b, a)$$



Example: Sets and Functions

The trivial system is the singleton set.

$$I := \{*\}$$

And indeed:

$$\forall X . X \times \{*\} \simeq X \simeq \{*\} \times X$$

I - - - - - I

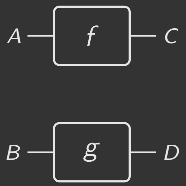
Example: Sets and Functions

Parallel composition of

$$A \xrightarrow{f} C \qquad B \xrightarrow{g} D$$

is just:

$$\begin{aligned} A \times B &\to C \times D \\ (a, b) &\mapsto (f(a), g(b)) \end{aligned}$$



Why does this work?

A very deep theorem in category theory says that the calculus we just described is **sound and complete** with respect to free symmetric strict monoidal categories (FSSMCs).

Why does this work?

A very deep theorem in category theory says that the calculus we just described is **sound and complete** with respect to free symmetric strict monoidal categories (FSSMCs).

Sound means that whatever can be proved graphically can be proved in a FSSMC.

Why does this work?

A very deep theorem in category theory says that the calculus we just described is **sound and complete** with respect to free symmetric strict monoidal categories (FSSMCs).

Sound means that whatever can be proved graphically can be proved in a FSSMC.

Complete means the opposite: Whatever can be proved in a FSSMC can be proved by means of graphical manipulations.

But what is a FSSMC?

In line with traditional algebra, a FSSMC is just a **symmetric monoidal category** which does not satisfy any supplemental equation.

But what is a FSSMC?

In line with traditional algebra, a FSSMC is just a **symmetric monoidal category** which does not satisfy any supplemental equation.

A lot of interesting structures can be seen as symmetric monoidal categories. Among those the **sets and functions**, which is why our example works.

But what is a FSSMC?

In line with traditional algebra, a FSSMC is just a **symmetric monoidal category** which does not satisfy any supplemental equation.

A lot of interesting structures can be seen as symmetric monoidal categories. Among those the **sets and functions**, which is why our example works.

Since sets and functions do not form a free symmetric monoidal category, completeness does not hold: there are equations expressed purely in terms of sets and functions that cannot be proved graphically without adding more ‘stuff’.

Example: $\mathbf{FdHilb}_{\mathbb{C}}$

A system is a finite-dimensional complex Hilbert space.

$$V \quad \text{———} \quad V$$

Example: **FdHilb**$_{\mathbb{C}}$

A process is a linear map.

Example: **FdHilb**$_{\mathbb{C}}$

This is the **tensor** product

$$V \otimes W$$

Example: **FdHilb**$_{\mathbb{C}}$

The trivial system is $\mathbb{C}$, seen as a 1-dimensional Hilbert space on itself.

$$I := \mathbb{C}$$

And indeed:

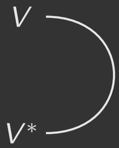
$$\forall V. V \otimes \mathbb{C} \simeq V \simeq \mathbb{C} \otimes V$$

Example: $\mathbf{FdHilb}_{\mathbb{C}}$

But the graphical calculus for vector spaces has more stuff!
This bent wire is the linear map:

$$V \otimes V^* \to \mathbb{C}$$

$$\sum_i a_i \left|e_i\right\rangle \otimes \sum_j b_j \left\langle e_j\right| \mapsto \sum_{i,j} a_i b_j \left\langle e_i | e_j \right\rangle$$

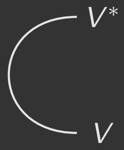


Example: **FdHilb**$_{\mathbb{C}}$

But the graphical calculus for vector spaces has more stuff! This other bent wire is the linear map:

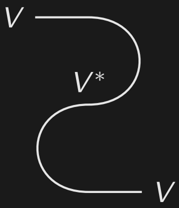
$$\mathbb{C} \to V^* \otimes V$$

$$c \mapsto c \sum_i \langle e_i| \otimes |e_i\rangle$$



Example: **FdHilb**$_{\mathbb{C}}$

Let's do some calculations.



$$V \simeq V \otimes \mathbb{C} \to V \otimes V^* \otimes V \mapsto \mathbb{C} \otimes V \simeq V$$

$$\sum_i a_i |e_i\rangle \simeq \sum_i a_i |e_i\rangle \otimes 1 \mapsto \sum_i a_i |e_i\rangle \otimes \sum_j \langle e_j| \otimes |e_j\rangle \mapsto \sum_{i,j} a_i \langle e_j|e_i\rangle |e_j\rangle$$

But

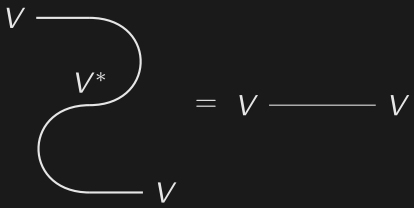
$$\sum_{i,j} a_i \langle e_j|e_i\rangle |e_j\rangle = \sum_{i,j} \delta_i^j a_i |e_j\rangle = \sum_i a_i |e_i\rangle$$

Example: **FdHilb**$_{\mathbb{C}}$

But

$$\sum_{i,j} a_i \langle e_j | e_i \rangle |e_j\rangle = \sum_{i,j} \delta_i^j a_i |e_j\rangle = \sum_i a_i |e_i\rangle$$

And so:



We found a new graphical equation!

The ZX calculus

The ZX calculus is a graphical calculus that is sound and complete with respect to the category of complex finite dimensional Hilbert spaces of dimension 2^n, so stuff that looks like $\bigotimes_n \mathbb{C}^2$ for all n. This is qbit land.

The ZX calculus

The ZX calculus is a graphical calculus that is sound and complete with respect to the category of complex finite dimensional Hilbert spaces of dimension 2^n, so stuff that looks like $\bigotimes_n \mathbb{C}^2$ for all n. This is qbit land.

This means that everything you can algebraically do with qubits and quantum circuits, you can do graphically in ZX.

The ZX calculus

The ZX calculus is a graphical calculus that is sound and complete with respect to the category of complex finite dimensional Hilbert spaces of dimension 2^n, so stuff that looks like $\bigotimes_n \mathbb{C}^2$ for all n. This is qbit land.

This means that everything you can algebraically do with qubits and quantum circuits, you can do graphically in ZX.

ZX was originally proposed by Coecke and Dunkan in 2008, and took several ordes of researchers and almost 10 years to prove complete.

The ZX calculus

Before continuing, remember that computations in quantum computing are made in a complex vector space of finite dimension 2^n. n is the number of qbits we're operating on[1].

[1] Yes, things can and are more complicated as you can use density matrices and the like. We have something for that too but it's out of scope for this talk

The ZX calculus

Before continuing, remember that computations in quantum computing are made in a complex vector space of finite dimension 2^n. n is the number of qbits we're operating on[1].

For any given qubit, we use two bases: The *computational basis*, denoted $|0\rangle, |1\rangle$ and the Hadamard basis, denoted $|+\rangle, |-\rangle$.

[1]Yes, things can and are more complicated as you can use density matrices and the like. We have something for that too but it's out of scope for this talk

The ZX calculus

Before continuing, remember that computations in quantum computing are made in a complex vector space of finite dimension 2^n. n is the number of qbits we're operating on[1].

For any given qubit, we use two bases: The *computational basis*, denoted $|0\rangle, |1\rangle$ and the Hadamard basis, denoted $|+\rangle, |-\rangle$.

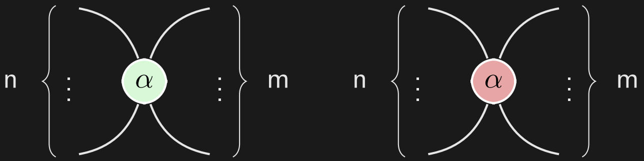
They are related as follows:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

[1] Yes, things can and are more complicated as you can use density matrices and the like. We have something for that too but it's out of scope for this talk

The main ingredients of the ZX calculus

The main ingredients of the ZX calculus are called **spiders**. For each $n, m \in \mathbb{N}$, there are only two spiders, **green** and **red**:



The green spider corresponds to the linear map $\bigotimes_n \mathbb{C}^2 \to \bigotimes_m \mathbb{C}^2$:

$$\underbrace{|0\ldots0\rangle}_{m}\underbrace{\langle0\ldots0|}_{n} + e^{i\alpha}\underbrace{|1\ldots1\rangle}_{m}\underbrace{\langle1\ldots1|}_{n}$$

The red spider corresponds to the linear map $\bigotimes_n \mathbb{C}^2 \to \bigotimes_m \mathbb{C}^2$:

$$\underbrace{|+\cdots+\rangle}_{m}\underbrace{|+\cdots+\rangle}_{n} + e^{i\alpha}\underbrace{|-\cdots-\rangle}_{m}\underbrace{\langle-\cdots-|}_{n}$$

The main ingredients of the ZX calculus

Notice that choosing $n, m = 1$ and $\alpha = 0$ the green and red spider become:

$$|0\rangle\langle 0| + |1\rangle\langle 1| \qquad\qquad |+\rangle\langle +| + |-\rangle\langle -|$$

And so[2]:

[2]When the phase is 0, it is customary not to write it.

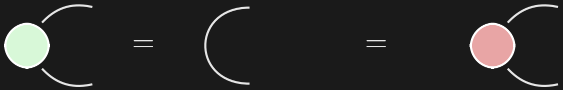
The main ingredients of the ZX calculus

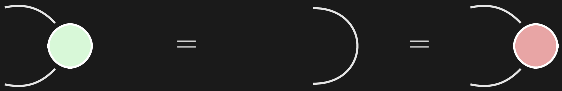
Notice that choosing $n, m = 1$ and $\alpha = 0$ the green and red spider become:

$$|0\rangle\langle 0| + |1\rangle\langle 1| \qquad\qquad |+\rangle\langle +| + |-\rangle\langle -|$$

And so[2]:

Similarly, choosing (n, m) to be $(0, 2)$ and $(2, 0)$:





[2] When the phase is 0, it is customary not to write it.

The main ingredients of the ZX calculus

Choosing $(n, m) = (1, 1)$ and $\alpha = \pi$ instead,

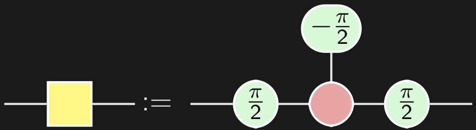
Correspond to a π rotation around the Z and X axis of the Bloch sphere, respectively, and so to the Z and X Pauli matrices.

The main ingredients of the ZX calculus

Choosing $(n, m) = (1, 1)$ and $\alpha = \pi$ instead,

Correspond to a π rotation around the Z and X axis of the Bloch sphere, respectively, and so to the Z and X Pauli matrices.

We define the Hadamard gate as:



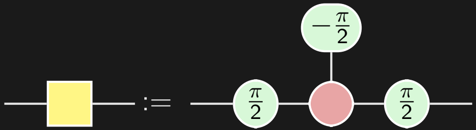
Which corresponds to the usual $|+\rangle \langle 0| + |-\rangle \langle 1|$.

The main ingredients of the ZX calculus

Choosing $(n, m) = (1, 1)$ and $\alpha = \pi$ instead,

Correspond to a π rotation around the Z and X axis of the Bloch sphere, respectively, and so to the Z and X Pauli matrices.

We define the Hadamard gate as:

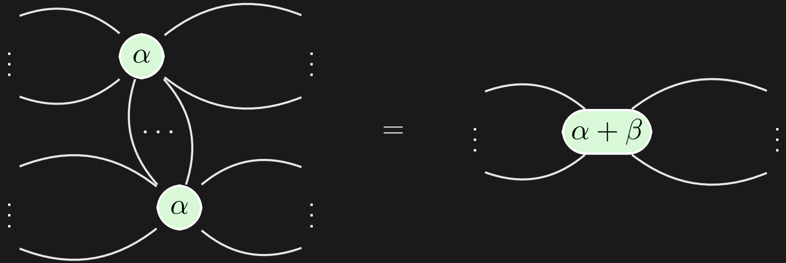


Which corresponds to the usual $|+\rangle \langle 0| + |-\rangle \langle 1|$.

Every ZX diagram is made **only** of green/red spiders.

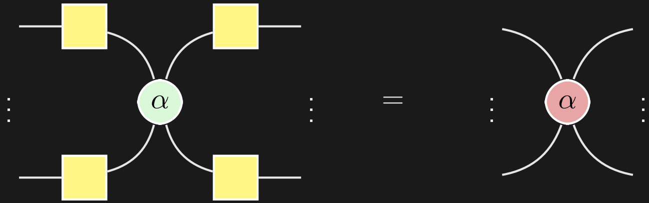
Rules of the ZX calculus

Different spiders can be connected by connecting their legs. Using the definitions, the following graphical equations can be proven. First, spiders of the same color fuse:



Rules of the ZX calculus

Second, we can turn a red spider into a green spider and viceversa using hadamards.



Rules of the ZX calculus

Third, π-phase spiders slide past spiders of opposite color, and change their sign:

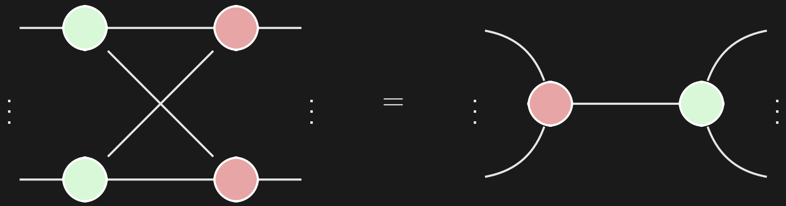
Rules of the ZX calculus

Third, π-phase spiders slide past spiders of opposite color, and change their sign:

As for 0-phase Spiders of opposite colors, they copy each other:

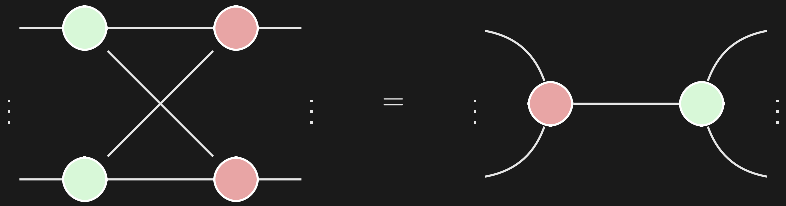
Rules of the ZX calculus

The second to last rule is called **bialgebra rule**:



Rules of the ZX calculus

The second to last rule is called **bialgebra rule**:



The very last rule is called **Hopf's rule**, and says that couple of wires connecting spiders of opposite color get deleted.

Soundess and completeness

Using the definitions of red and green spiders in terms of linear maps, one can prove that all these diagrammatic equations hold.

Soundess and completeness

Using the definitions of red and green spiders in terms of linear maps, one can prove that all these diagrammatic equations hold.

What is **very surprising** is that the opposite is also true: Every algebraic equation in finite dimensional complex Hilbert spaces of dimension 2^n can be proved diagrammatically using **only** the rewriting rules listed here!

Why should I care?

ZX calculus provides a **rewriting system** for quantum computing.

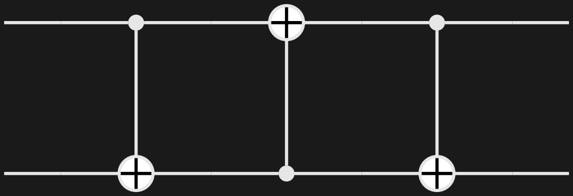
Why should I care?

ZX calculus provides a **rewriting system** for quantum computing.

As ZX diagrams are basically decorated graphs, we can now apply the last 50 years or so of research in graph rewriting to the task or simplifying quantum circuits.

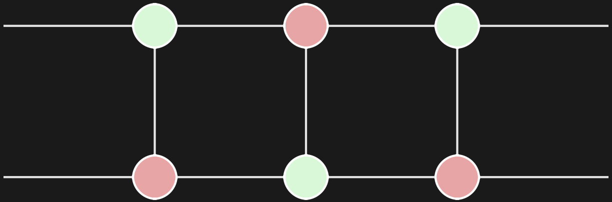
Example: 3 CNOTs

Consider the following quantum circuit, just 3 CNOTs in series.



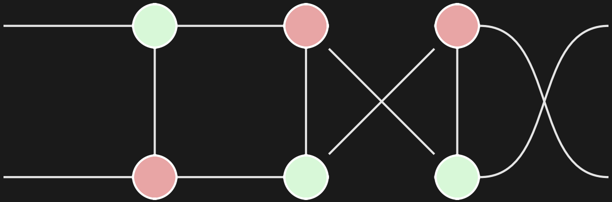
Example: 3 CNOTs

Let's translate this to a ZX diagram.



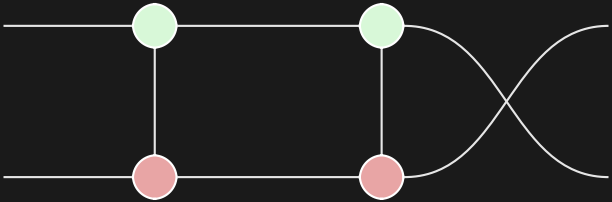
Example: 3 CNOTs

Only topology matters: flip the third gate vertically.



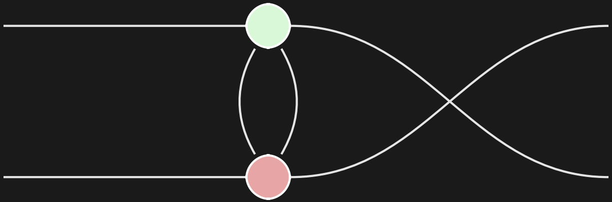
Example: 3 CNOTs

Apply the bialgebra rule.



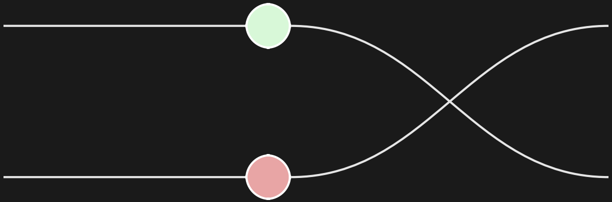
Example: 3 CNOTs

Then, spider fusion.



Example: 3 CNOTs

Finally, apply Hopf's rule.

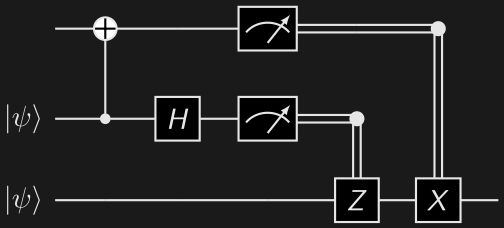


Example: 3 CNOTs

0-phase spiders are identities, so:

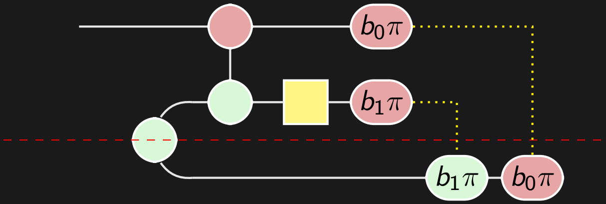
Example: Quantum teleportation

Consider the following quantum teleportation protocol



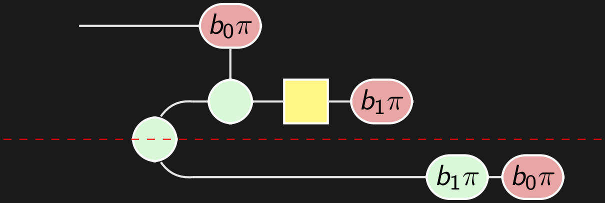
Example: Quantum teleportation

Translate it to ZX-diagrams. b_0, b_1 are either 0 or 1 (booleans).



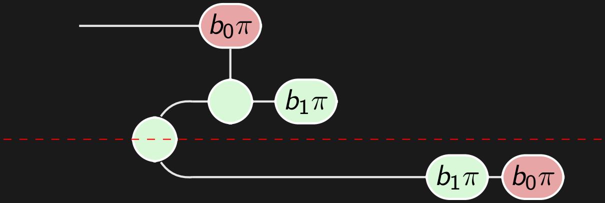
Example: Quantum teleportation

Apply spider fusion.



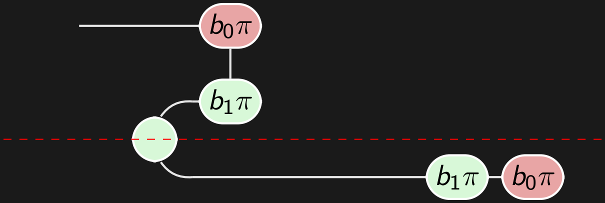
Example: Quantum teleportation

Hadamard gates flip spider's colors.



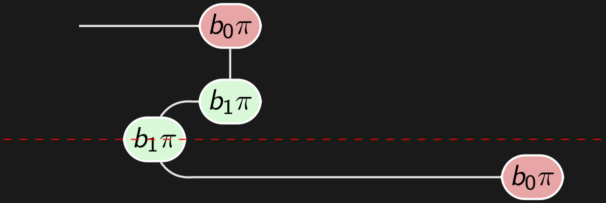
Example: Quantum teleportation

Apply spider fusion again.



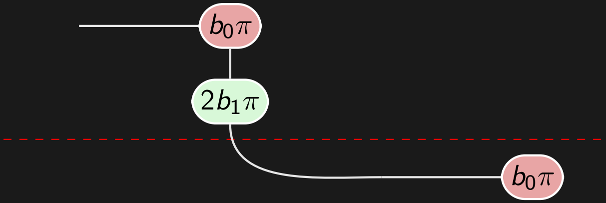
Example: Quantum teleportation

Fuse! Fuse! Fuse!



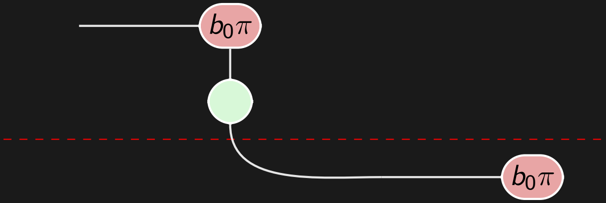
Example: Quantum teleportation

Fuse more! Fuse more!



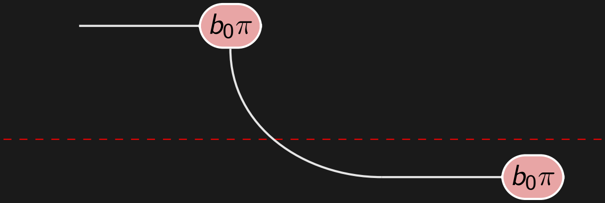
Example: Quantum teleportation

Now, $2\pi b_1 = 0$ is either 0 or 2π. Since phases have period 2π,



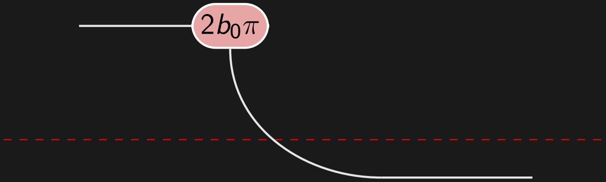
Example: Quantum teleportation

Zero phase spiders with only two legs are identity wires!



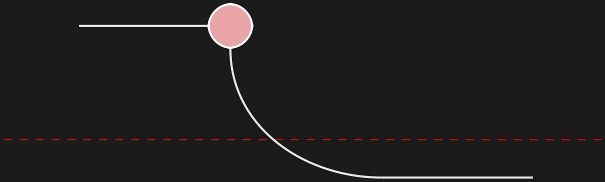
Example: Quantum teleportation

Fuse again!



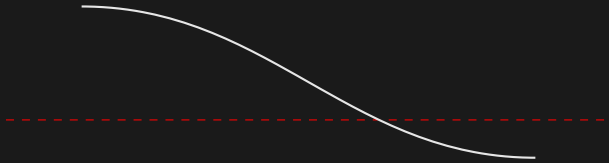
Example: Quantum teleportation

Same argument as before, and phase is 0



Example: Quantum teleportation

Which once again means identity wires!



Thank you

That's it from me. Thank you very much!