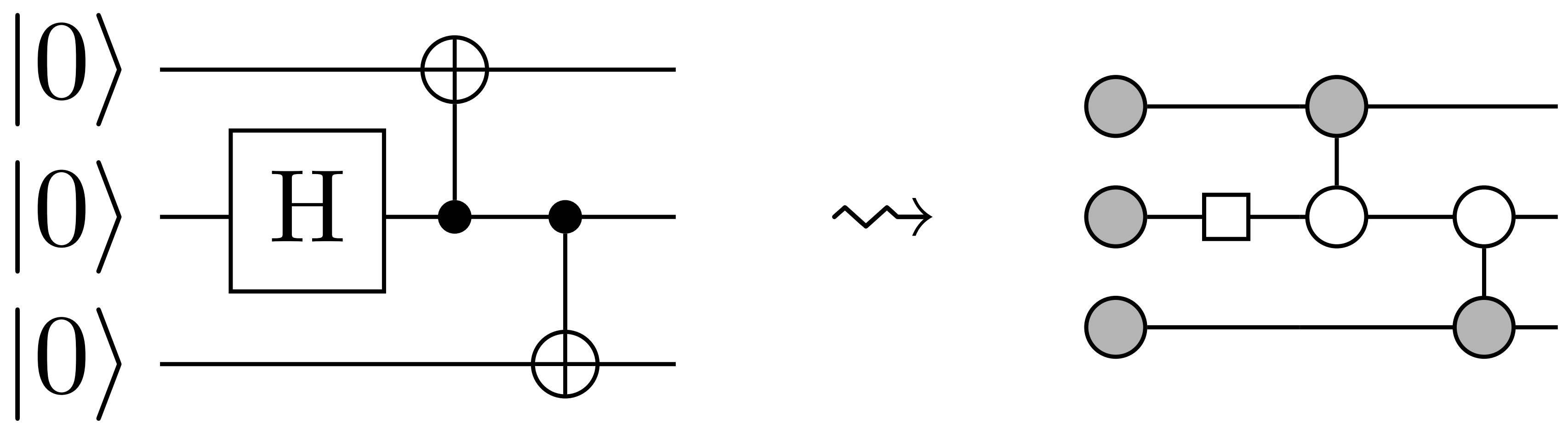
Quantum Compilers

A Taste of ZX Calculus

Robin Kaarsgaard
Department of Mathematics and Computer Science
SDU

ZX-calculus at a glance

- The ZX-calculus is a formal graphical language for representing and reasoning about quantum circuits (and other linear maps).
- It allows the representation of linear maps as *ZX-diagrams,* e.g.,

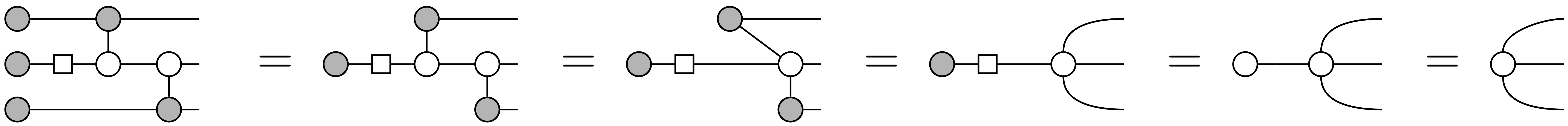


- Close relations to *Penrose notation* and *tensor networks*.
- **Slogan:** *“only connectivity matters”*

ZX-calculus at a glance

- ZX-calculus allows reasoning about the behaviour of ZX-diagrams through a set of graphical rewrite rules.

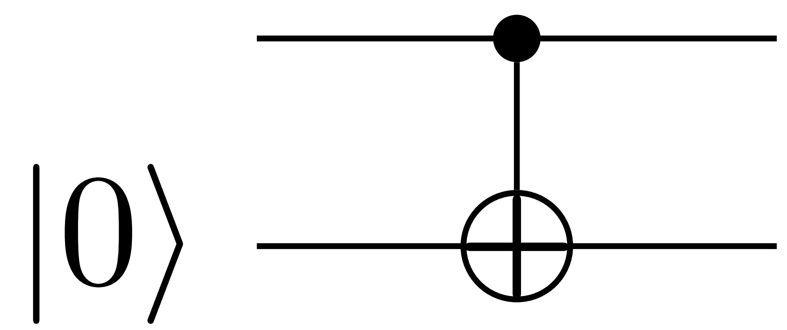
- For example, these rules can be used show that the circuit from before prepares the GHZ-state:



- Rewrite rules are topological in that they concern connectivity rather than precise form.

ZX-calculus from the beginning

- Consider the following quantum circuit:



corresponding to the isometry with matrix (in the computational basis)

$$|00\rangle\langle 0| + |11\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

- What happens if I plug in $|0\rangle$ or $|1\rangle$?

Copying

- If we feed this $\alpha|0\rangle + \beta|1\rangle$, we get

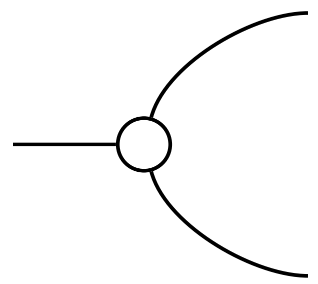
$$\alpha|00\rangle + \beta|11\rangle \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

- **Central observation:** This circuit only successfully copies states in the computational basis. In fact, a copying gadget like this *uniquely* identifies a basis in f.d. Hilbert space.

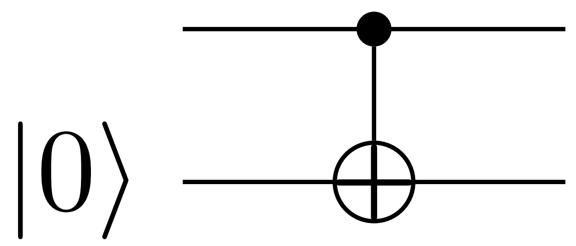
- **Excursion:** A more physics-y way of saying "states in the computational basis on $\mathbb{C}^2$" is "eigenstates for the observable $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$."

ZX-diagrams: Gadgets, composition, wiring

- Let's use the following notation for this gadget:

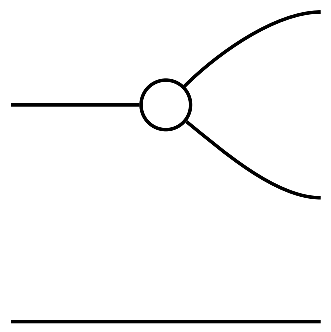


$=$



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

- We will use an empty wire to denote the identity.
- The meaning of parallel composition (above/below) is tensor product, e.g.,

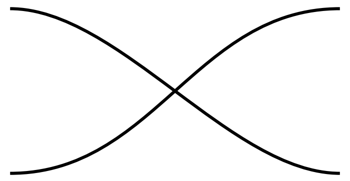


$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- The meaning of sequential composition (left/right) is ordinary composition of linear maps.

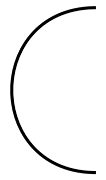
Symmetries

- We write the SWAP-gate in ZX-calculus by just swapping wires

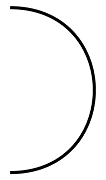


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- We can also bend wires by composing with *caps* and *cups*, corresponding to the (unnormalised) Bell state and effect:



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

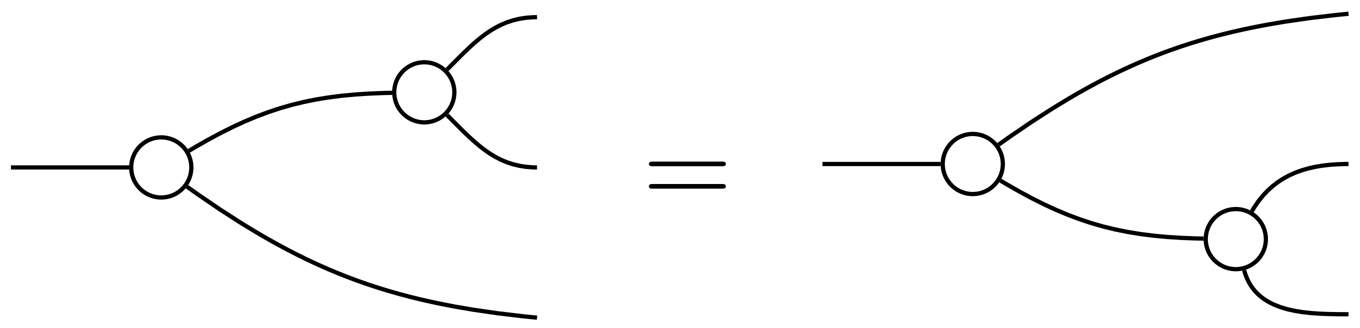


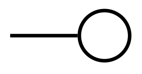
$$= \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$$

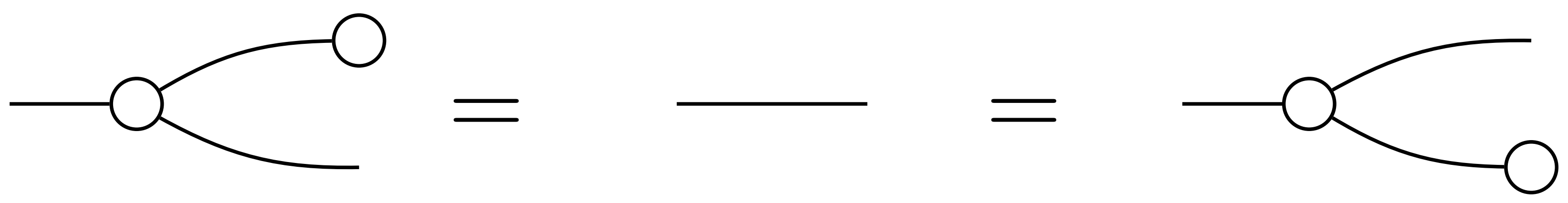
- Swapping and wire bending works very satisfyingly as one would expect: You can slide gadgets along the wire of a SWAP, and turn inputs into outputs (and vice versa) using cups and caps.

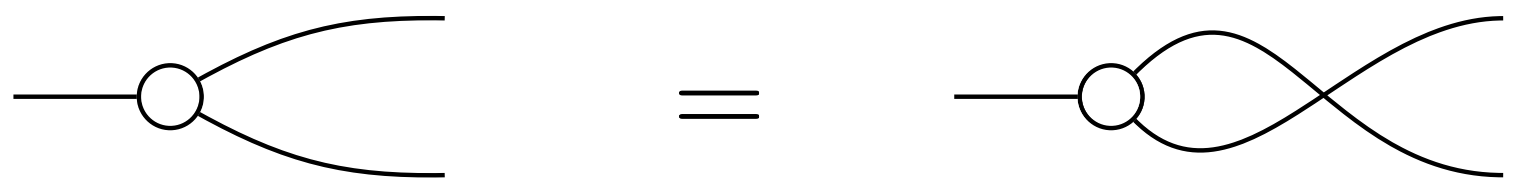
Copying in Z

- We notice that the copying gadget is *coassociative* in that



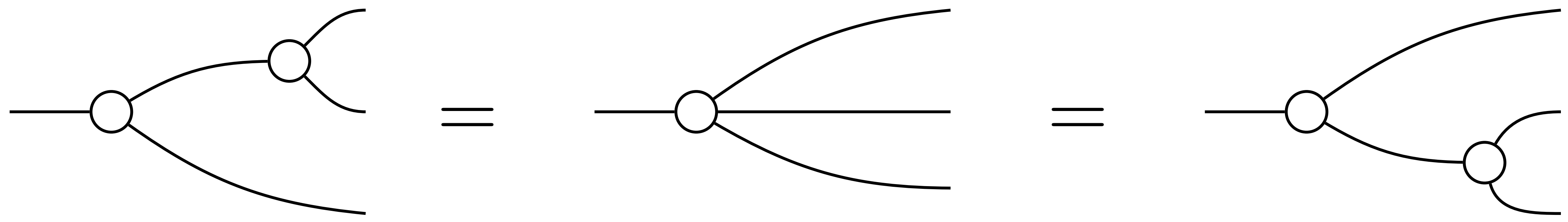
- Writing  for the (unnormalised!) effect $\langle 0| + \langle 1|$, we see that it is also *counital* and *cocommutative* in that





Copying in Z

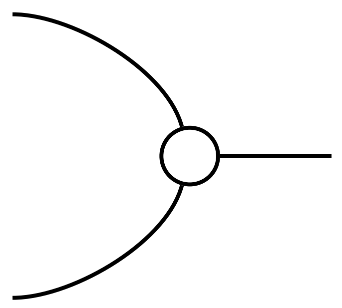
- Since it doesn’t matter how we copy precisely, we might as well write copying twice as a node with one input line and three output lines, i.e.,



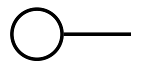
and so on for arbitrary Z-basis copying.

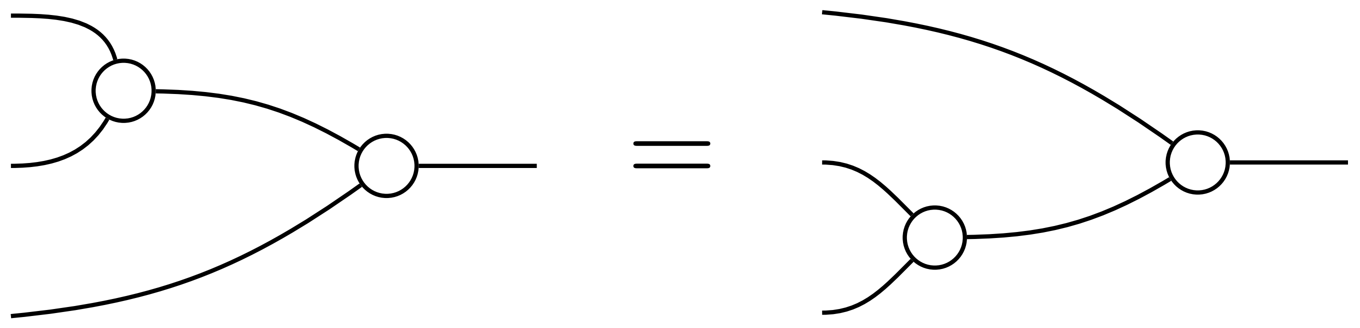
Cocopying in Z

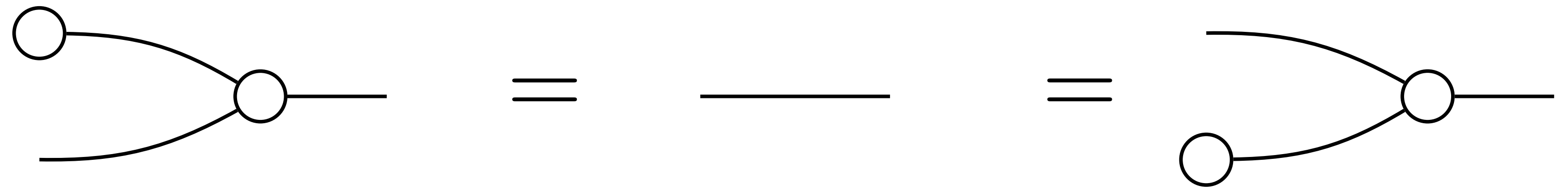
- Since Z-copying is a linear map on a Hilbert space, it has a Hermitian adjoint given by

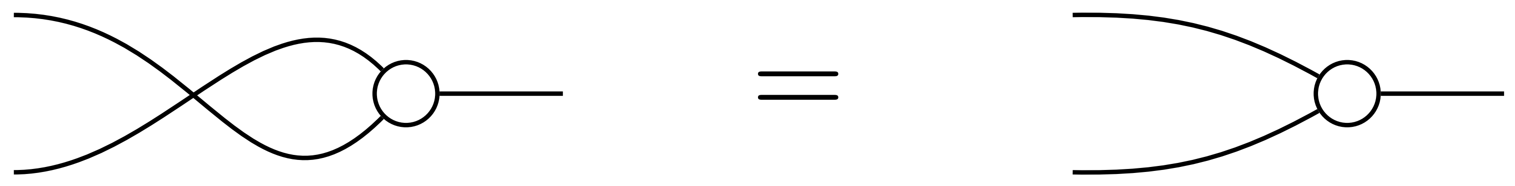


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

- Dually, writing  for the unnormalised state $|0\rangle + |1\rangle$, we get that this satisfies the dual properties (associativity, unitality, commutativity)

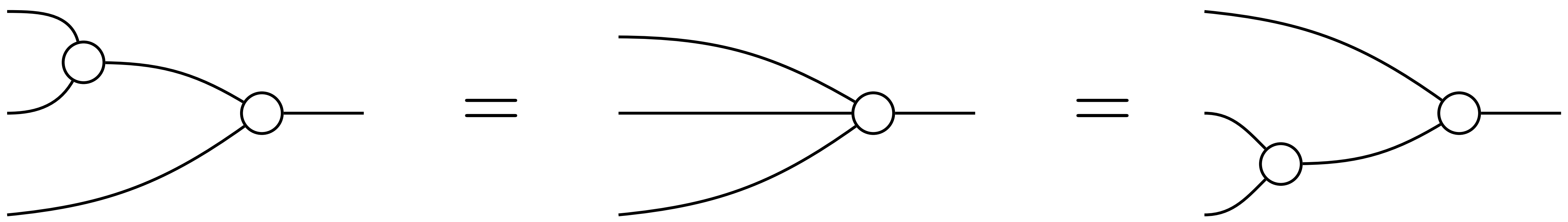




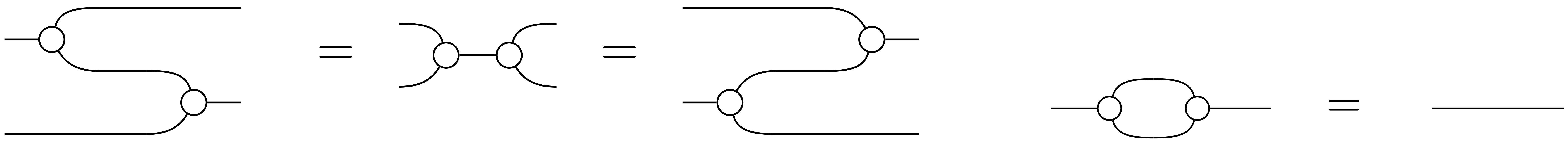


Cocopying in Z

- Likewise, since it doesn't matter how we cocopy precisely, we might as well write cocopying twice as a node with three inputs and one output, i.e.,



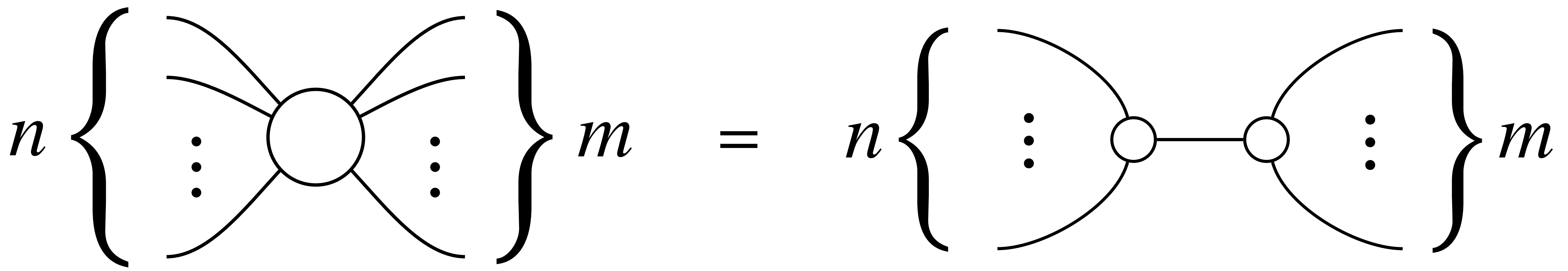
and so on for arbitrary Z-basis cocopying. In fact, we have that the combination of copying and cocopying satisfies the laws



- **Consequence:** It doesn't matter how we combine copiers and cocopiers, or whether we have to cross wires to do so, the only thing that matters is the number of inputs and outputs.

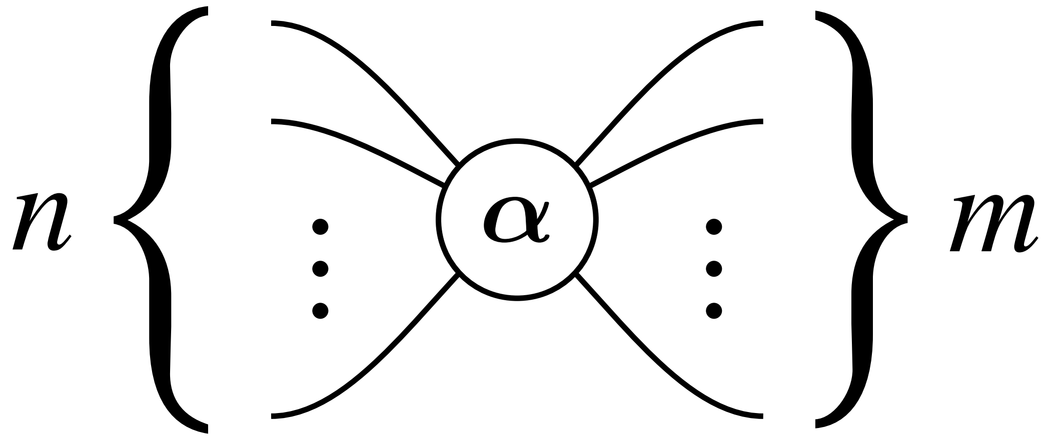
Spiders

- By combining an n-way Z-cocopying gadget with an m-way Z-copying gadget, we get the fundamental building block of ZX-calculus, the (Z-)*spider*:



$$= \quad |0\rangle^{\otimes m}\langle 0|^{\otimes n} + |1\rangle^{\otimes m}\langle 1|^{\otimes n}$$

- It turns out to be convenient to allow a phase $e^{i\alpha}$ to be conditionally applied, yielding the *phased (Z-)spider*



$$= \quad |0\rangle^{\otimes m}\langle 0|^{\otimes n} + e^{i\alpha}|1\rangle^{\otimes m}\langle 1|^{\otimes n}$$

- When a phase is 0 we leave the node empty and recover ordinary spiders.

- In the special case where n and m are both 1, we recover the usual *phase gates*: $|0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|$.

Other bases

- So far we have only looked at spiders in the Z-basis. To build interesting gates, we need other bases as well.
- Clearly not feasible to have all of them – we'll run out of discernible colors very quickly!
- **Hypothesis:** We can maximise expressivity if we choose an observable such that its eigenbasis is *maximally unlike* the Z-basis.
- But what does that mean?

Complementarity

- Say that two orthonormal bases $\{\,|\alpha_i\rangle\}_{i\in I}$, $\{\,|\beta_i\rangle\}_{i\in I}$ on some f.d. Hilbert space H are *mutually unbiased* when

$$|\langle\alpha_i|\beta_j\rangle|^2 = \langle\alpha_i|\beta_j\rangle\langle\beta_j|\alpha_i\rangle = \frac{1}{\dim(H)}$$

  for all $i, j \in I$.

- Say that two observables are *complementary* when their eigenbases are mutually unbiased.

- **Operationally:** When observables M and N are complementary, measuring *any* M-eigenstate $|\alpha\rangle$ in the N-eigenbasis (or vice versa) reveals *no information* about $|\alpha\rangle$ (cf. uncertainty)

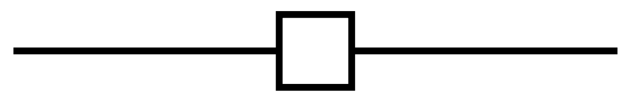
Complementarity

- A canonical choice of observable complementary to Z is $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with eigenbasis $\{\,|+\rangle, |-\rangle\}$.

- In fact, X is the *unique* observable that is *strongly complementary* to Z, meaning that it satisfies some additional algebraic properties.

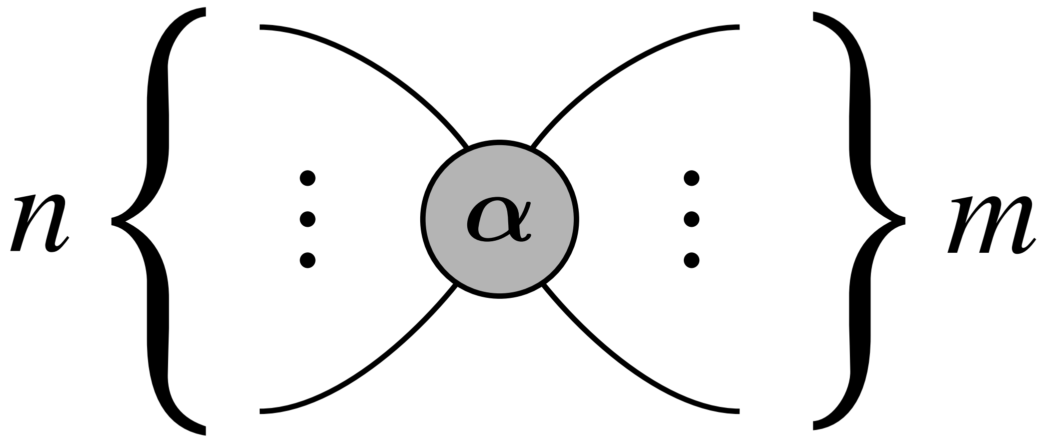
- Notice that $HZH = X$ and $HXH = Z$ (with H the Hadamard gate).

- In ZX-calculus, we write H as a little box:



X-Spiders

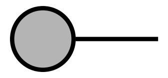
- We define *phased X-spiders* as



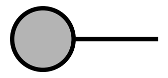
$$= \quad |+\rangle^{\otimes m}\langle +|^{\otimes n} + e^{i\alpha}\,|-\rangle^{\otimes m}\langle -|^{\otimes n}$$

- The X-(co)copiers appear as special cases, as do phase gates conjugated by Hadamard: $|+\rangle\langle +| + e^{i\alpha}\,|-\rangle\langle -|$.

- Notice in particular that the unit is the state



$$= H\left(|0\rangle + |1\rangle\right) = |+\rangle + |-\rangle = \sqrt{2}\,|0\rangle$$

- **Dubious convention:** In ZX-calculus, like in much of physics, we tend to disregard (non-zero) global scalars, and, e.g., just use  $= |0\rangle$. This is inaccurate, but it is safe in the sense that we can always recover non-zero global scalars again (up to global phase).

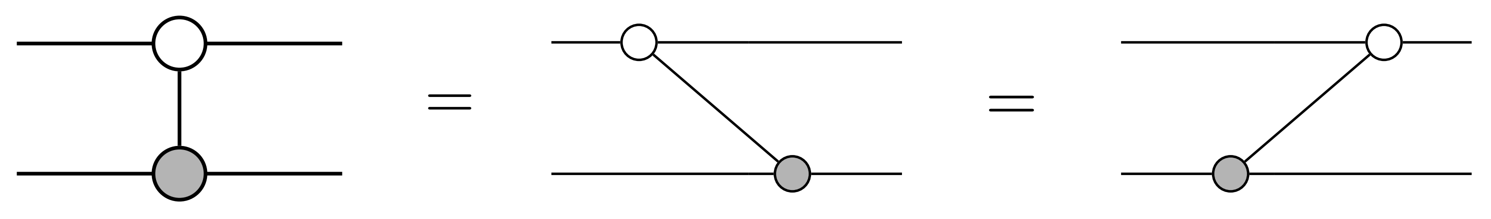
Universality

- Phase gates are Z-rotations up to global phase, while phase gates conjugated by Hadamard are X-rotations up to global phase.

- **Euler decomposition:** Any unitary U on $\mathbb{C}^2$ can be written as a product of Z-rotations and X-rotations, $U = e^{i\phi} R_Z(\alpha)\, R_X(\beta)\, R_Z(\gamma)$ for some $\alpha, \beta, \gamma, \varphi \in [0,2\pi)$.

- **Two-level unitaries suffice:** Any unitary on $\mathbb{C}^{2^n}$ can be written as a network of 1-qubit unitaries and CNOTs.

- CNOT is expressible in ZX-calculus as



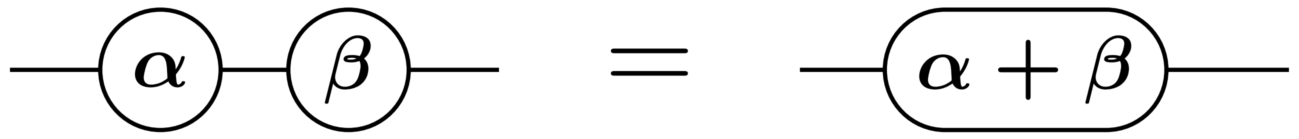
so it follows that ZX-calculus can express any unitary (it enjoys *exact universality*).

Reasoning about ZX-diagrams

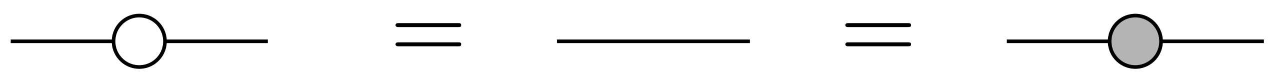
- ZX-calculus allows a number of rewrite rules to reason about linear maps.
- A prime application of ZX-calculus is to prove equalities of linear maps (such as quantum circuits) by turning them into ZX-diagrams and applying rewrite rules until one turns into the other.
    - You can also use this for directed rewriting (e.g., circuit optimisation), but some care must be exercised to ensure circuit-to-circuit translation.

Spider fusion

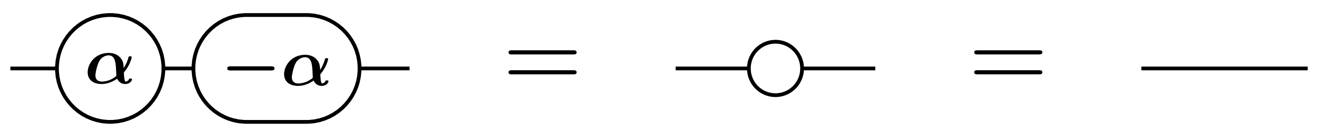
- When two spiders of the same color are connected by at least one edge they can be merged into one node with their phases added together (modulo 2π).
- Elegantly subsumes the rules of (co)associativity and (co)unitality, as well as the interaction between copiers and cocopiers of the same color.
- Also subsumes the rule that two rotations of the Bloch sphere along the same axis can be combined into one:



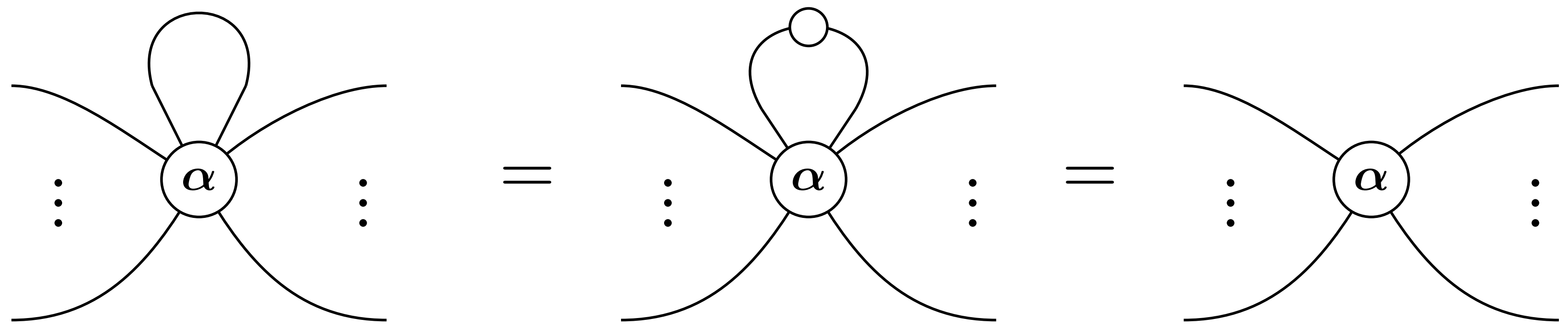
Identity removal



- A phased spider with one input, one output, and a trivial phase is just the identity.
- Together with spider fusion, this says that the inverse to a rotation by α is a rotation by $-\alpha$ since

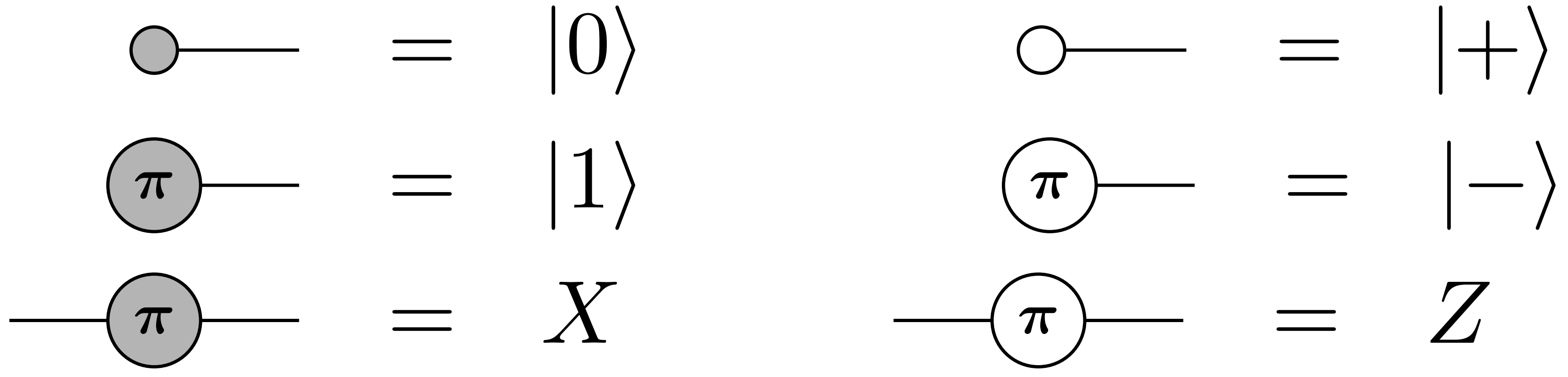


- In combination with spider fusion it also allows us to remove self-loops:

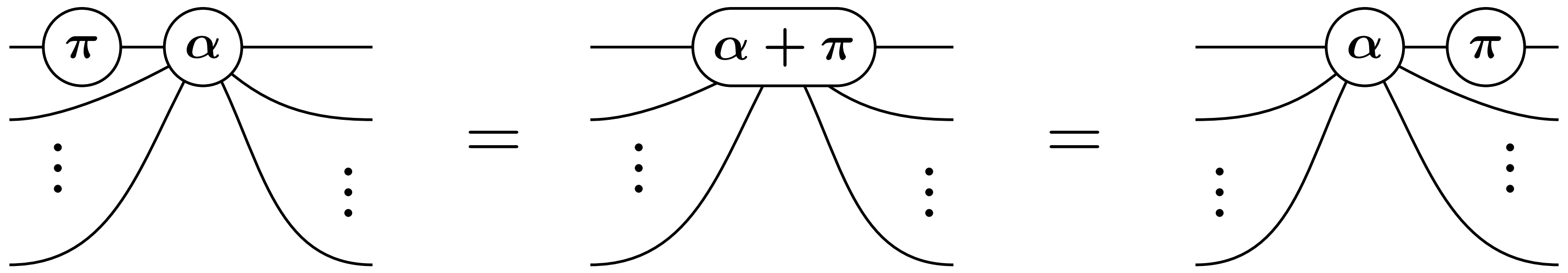


Copy and π-commutation

- We have that Pauli operations and their eigenstates are given by

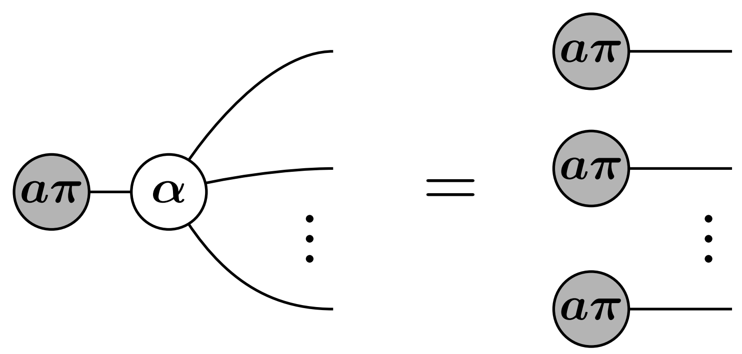


- Same-color interactions are already covered by spider fusion:

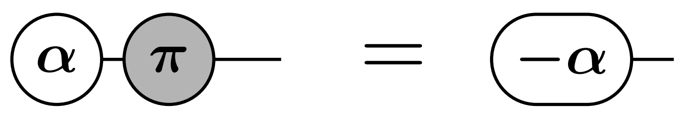


Copy and π-commutation

- For interaction with different color spiders, we need the copy and π-commutation rules (for Boolean variable $a \in \{0,1\}$):

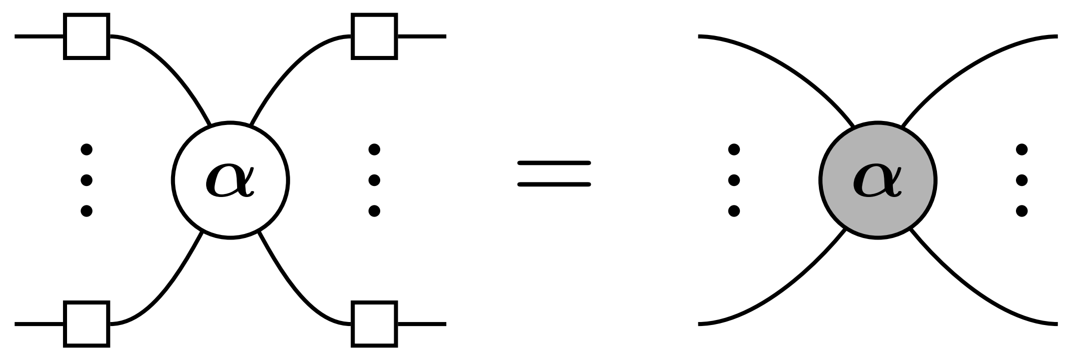


- Notice the important special case

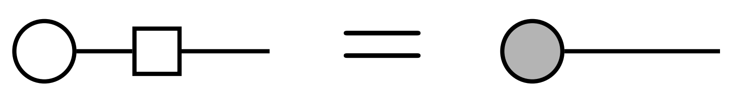


Color changing

- We remarked earlier that $HZH = X$ and $HXH = Z$. We also have $HH = I$.
- This becomes the rules

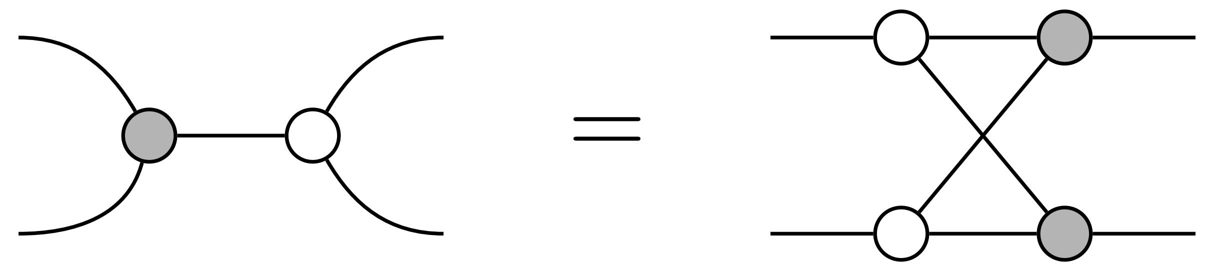


- Notice that the spider color changing rule also applies when the number of inputs or outputs is zero, e.g.,

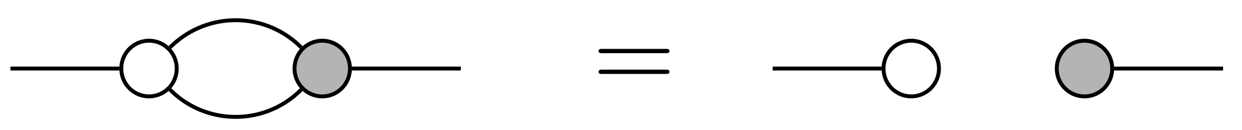


Bialgebra and Hopf rule

- So far, we have said that the white and gray spiders corresponded to (eigenbases of) complementary observables, but we haven't used this.
- This important relationship is formalised by the *bialgebra rule*:

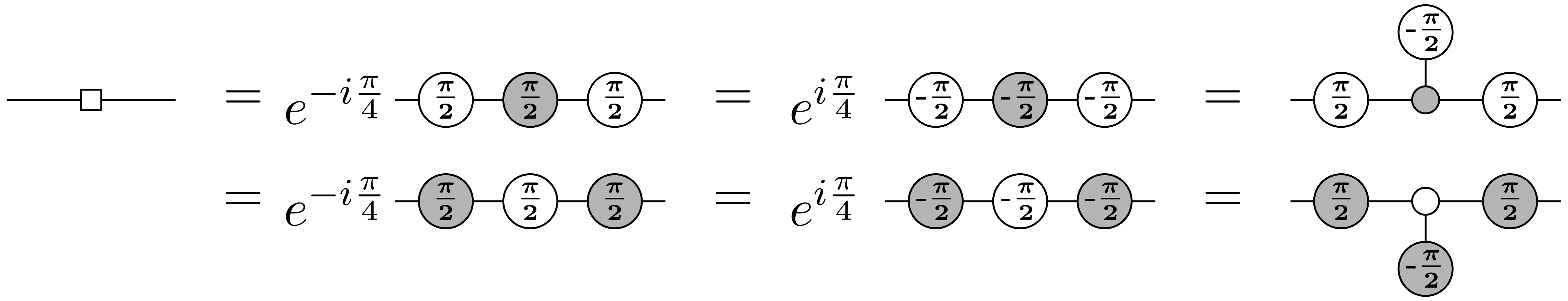


- In fact, the X and Z observables satisfy an additional rule that makes them *strongly complementary,* namely the *Hopf rule*:



Meta rules

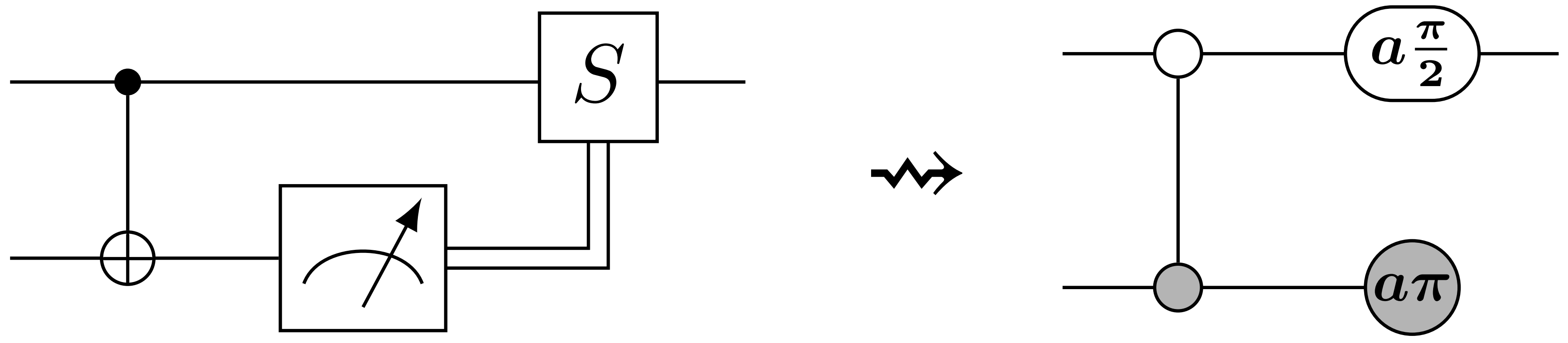
- Hadamard is defined to be any one of the following six diagrams:



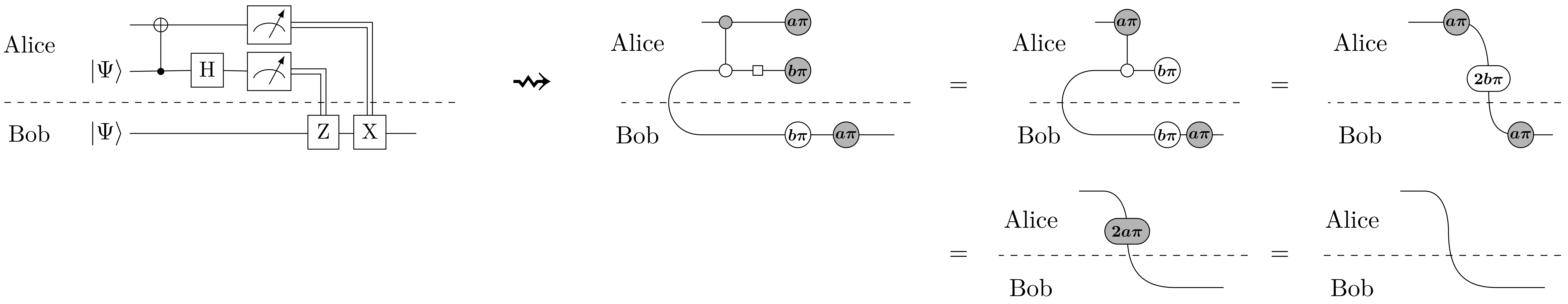
- Only connectivity matters: you can deform diagrams any way you'd like, so long as inputs and outputs are preserved.
- All rules hold with inputs and outputs exchanged.
- All rules hold with colors exchanged.
- All rules hold with phases negated.

Measurement

- Programs and protocols relying on measurements are represented in ZX-calculus by introducing a Boolean variable.
- For example,



Teleportation example



Online examples

- GHZ circuit.
- SWAP circuit.