Introduction to Categorical Quantum mechanics

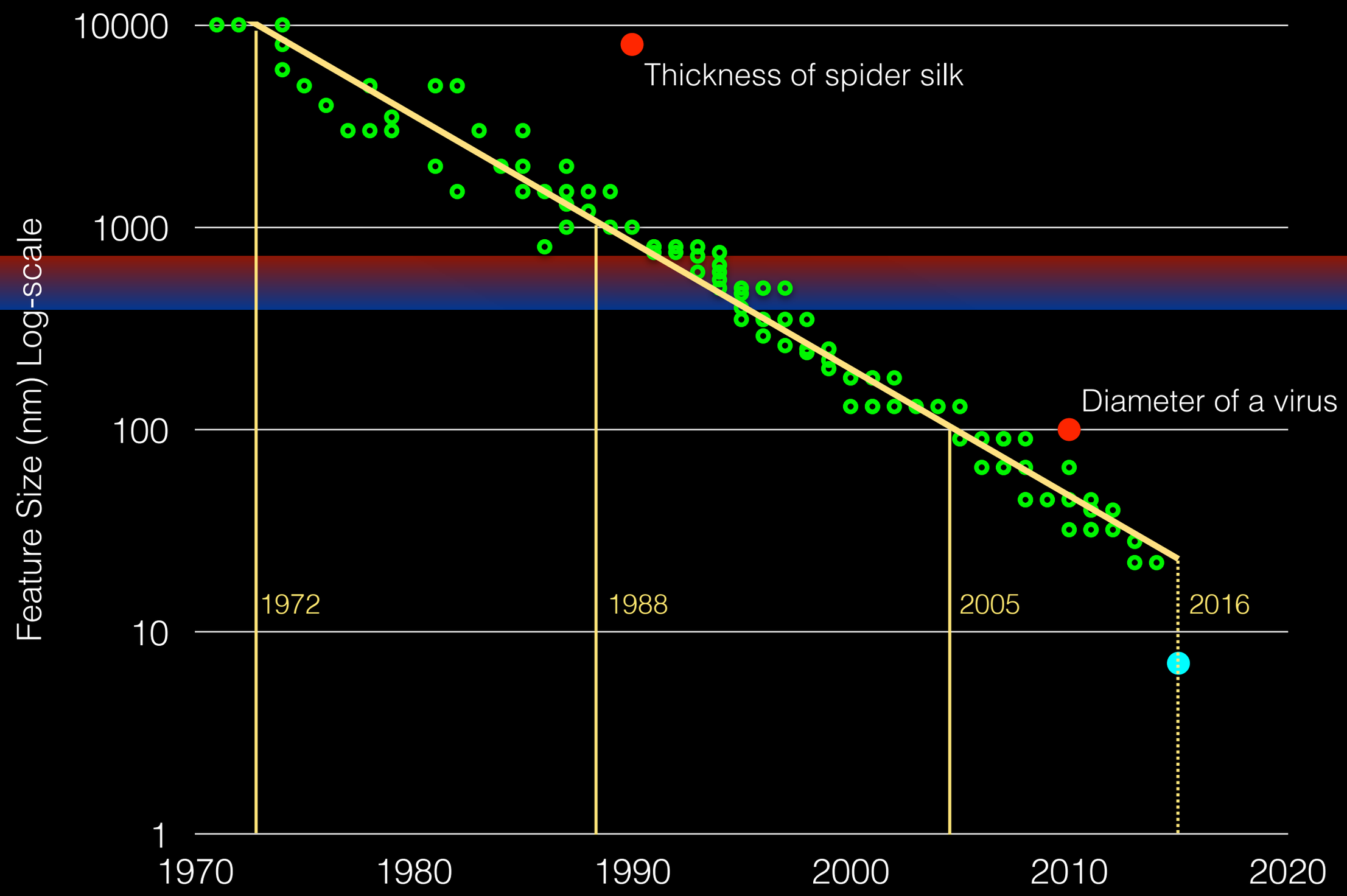
Ross Duncan

University of Strathclyde Glasgow

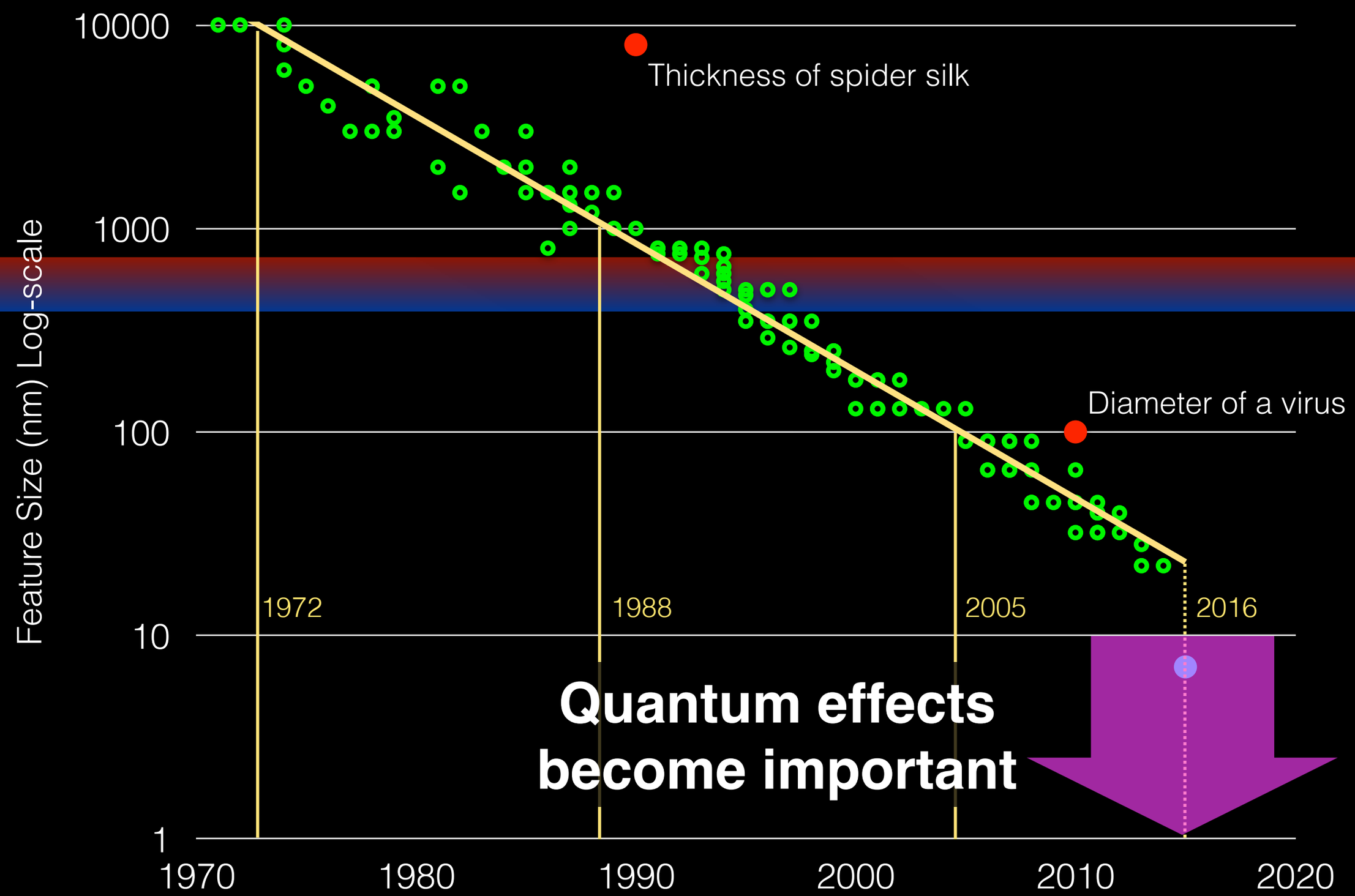
0.

Motivations

Transistors are shrinking



Transistors are shrinking

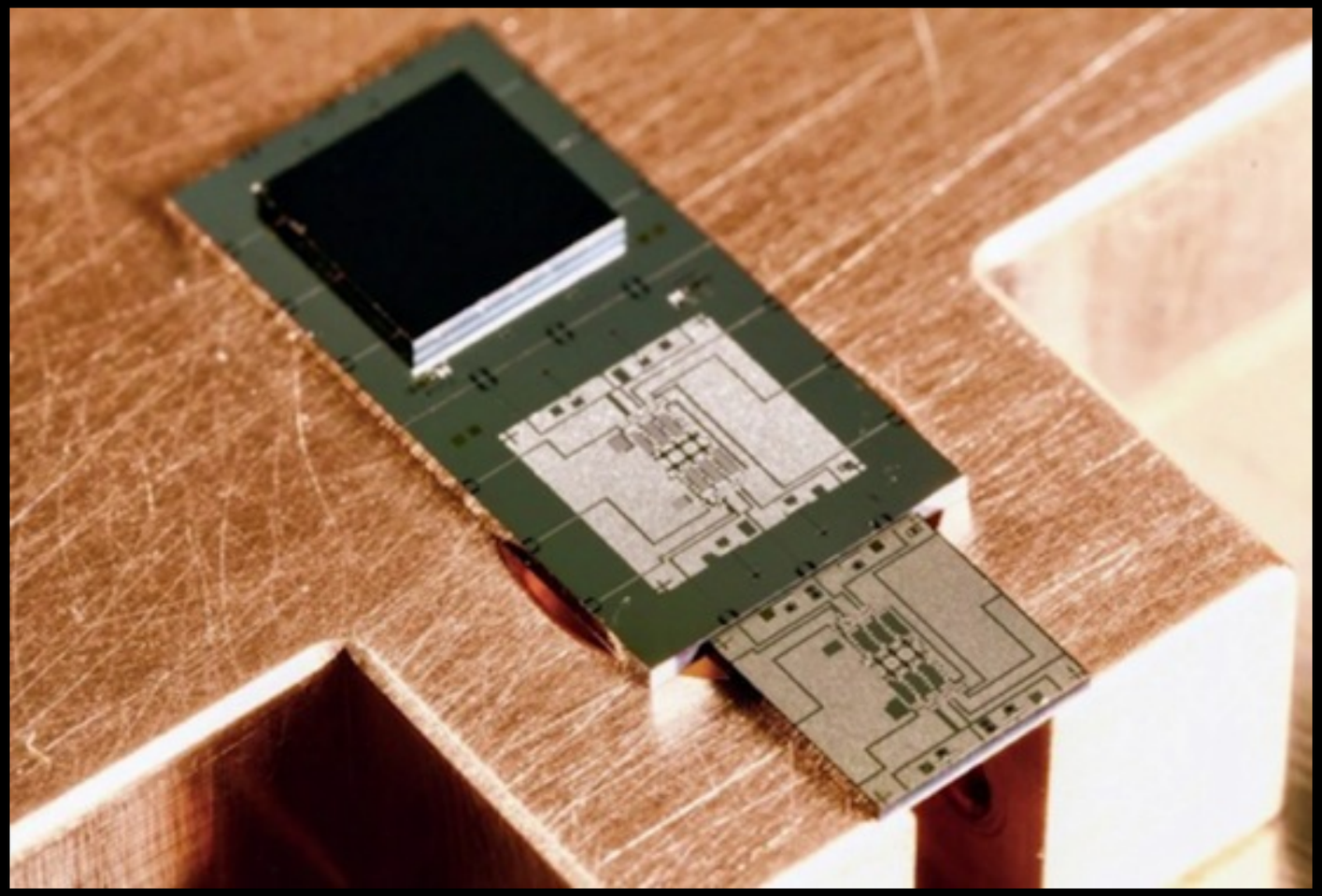


Quantum Computing

- **IDEA**: *exploit* quantum effects for computation
  - Fast algorithms (Shor, Grover)
  - Simulate physical systems (chemistry, materials)
  - Novel cryptographic protocols (QKD, blind computing)
  - …. and more.

Quantum Computing

Research at Google

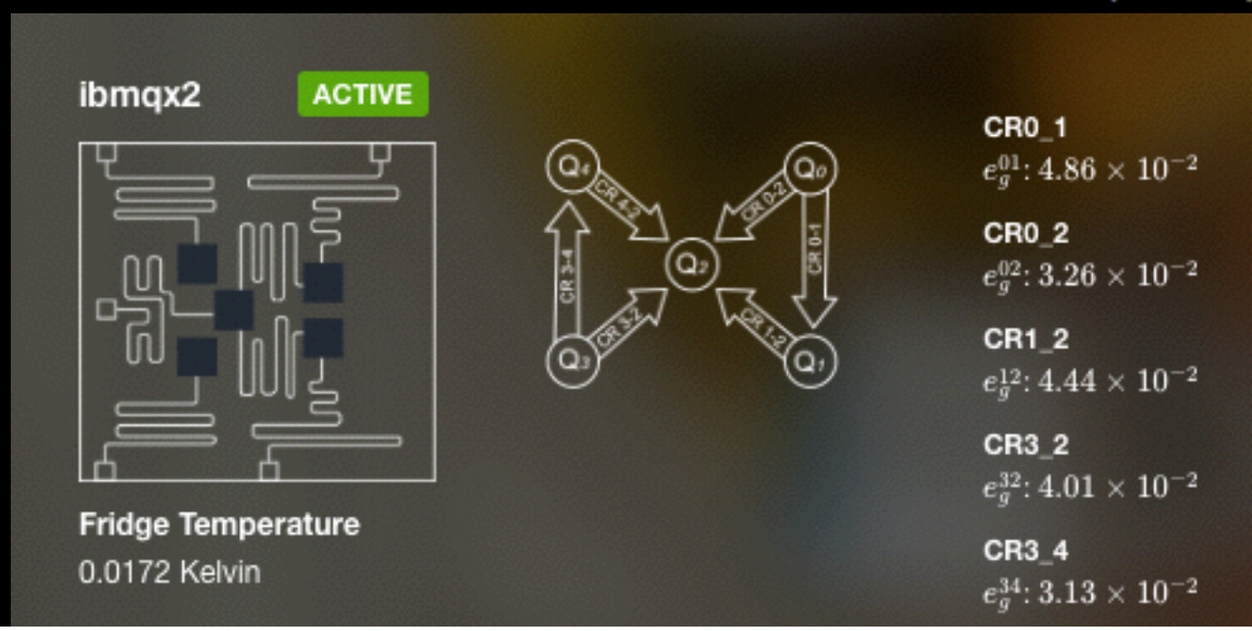


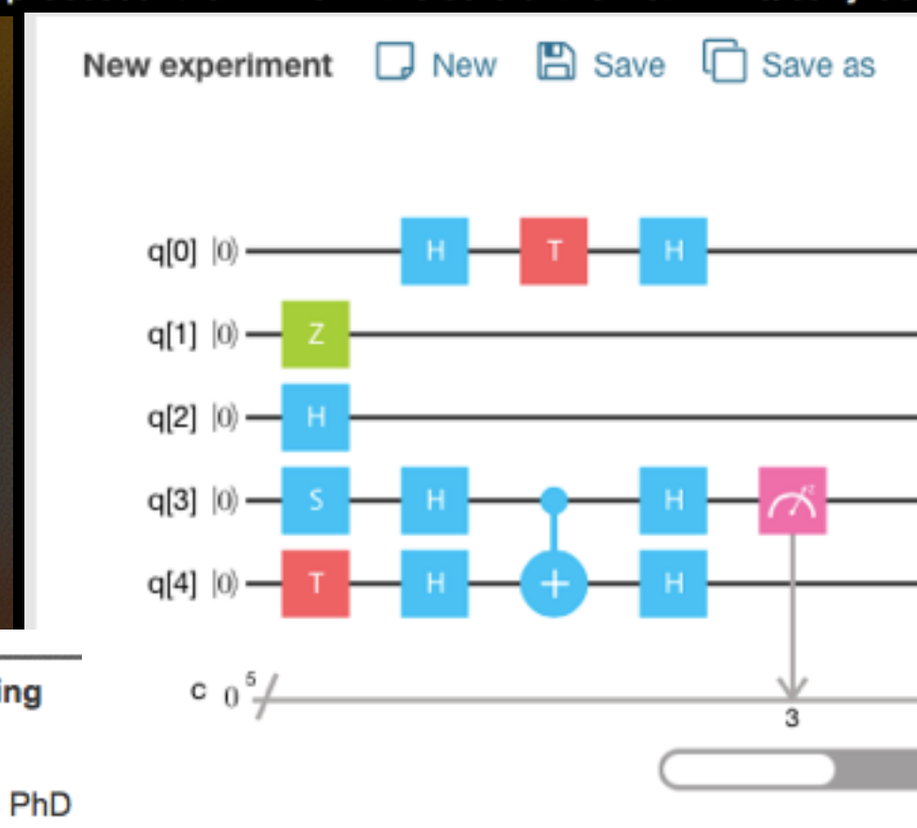
target: 49 qubit machine in the lab by end of 2017

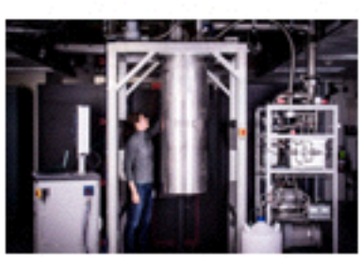
Quantum Computing

What is IBM Q?

IBM Q is an industry-first initiative to build commercially available universal quantum computing systems for business and science. Today, IBM has a sophisticated prototype commercial quantum processor that will form the core of the first IBM Q early-access







IBM Builds Its Most Powerful Universal Quantum Computing Processors

Date added: 17 May 2017

IBM Research Staff Member Katie Pooley, an Applied Physics PhD from Harvard who joined IBM in 2015, at the Thomas J Watson Research Center, is a process integrator on the IBM Q team. In the photo, Pooley is examining a cryostat with the new prototype of a commercial quantum processor inside. (Credit: Andy Aaron, IBM)

5 qubits now;
16 later this year

target: 50 qubit machine *for sale* by 2021

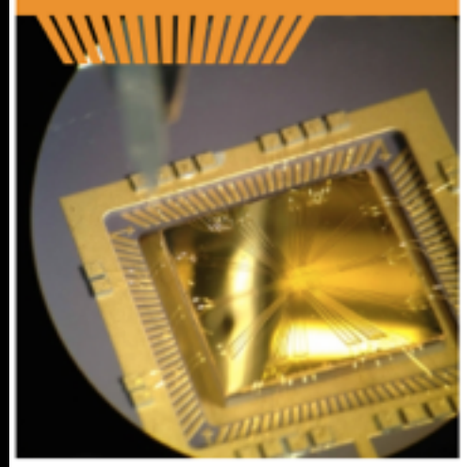
Quantum Computing

NQIT Networked Quantum Information Technologies

target: 400 qubits by 2020

Ion Traps

Ion traps are one of our core technologies, which we are developing for use as quantum information processors.

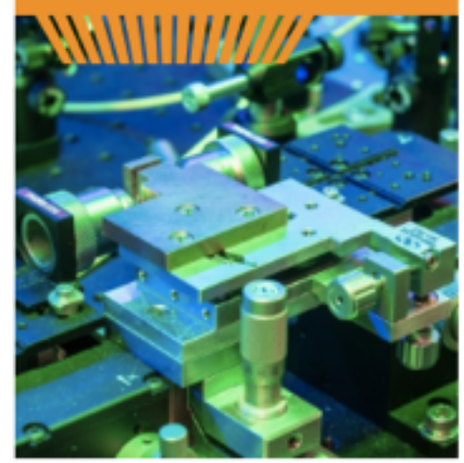


Atom-photon Interfaces

In order to create a powerful quantum computing device by interconnecting many simple quantum processors we need reliable interfaces at the single-quantum level to establish such a connected network.

Photonics

In NQIT we are developing the optics to wire-up individual atoms, by collecting the particles of light which they emit and building a quantum entanglment connection between the atoms.

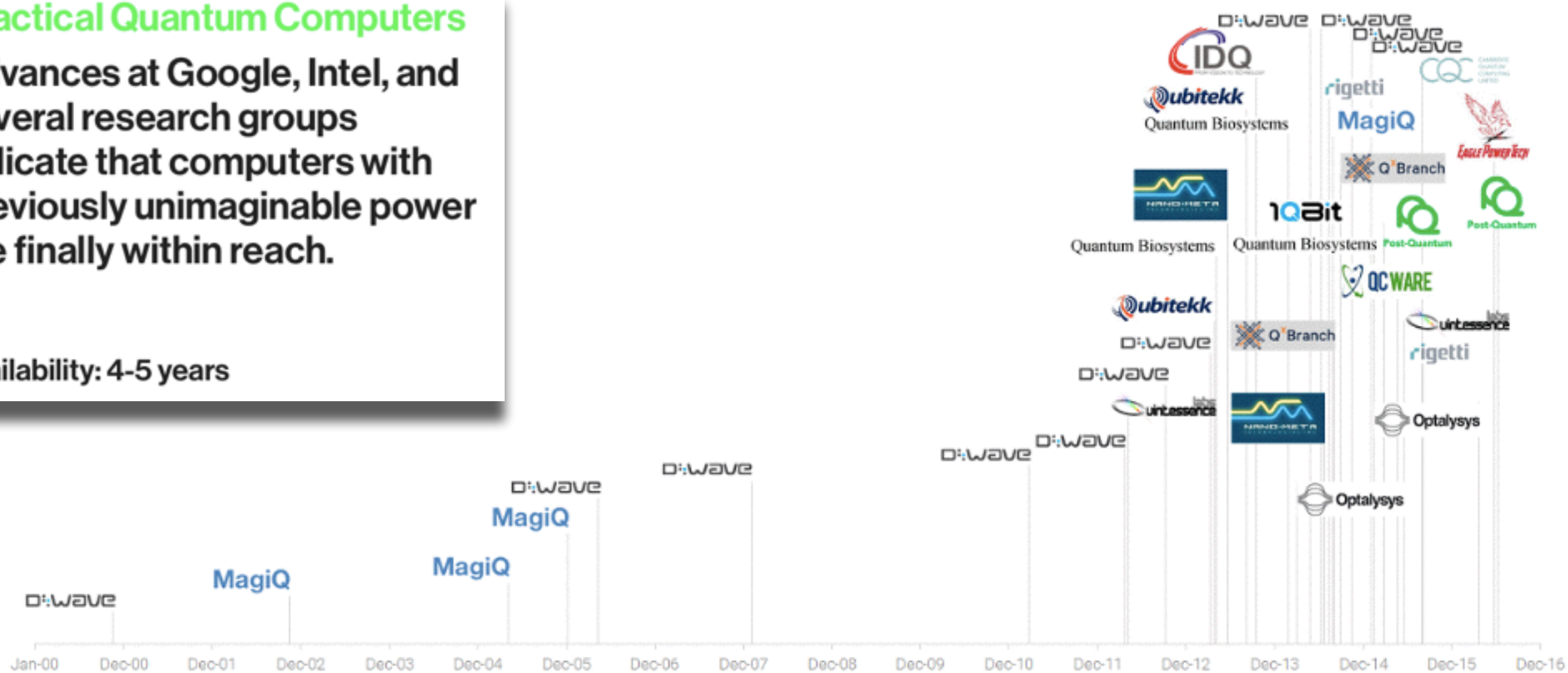


Quantum Computing: 17 Years Of Major Startup Financings In One Timeline

Practical Quantum Computers

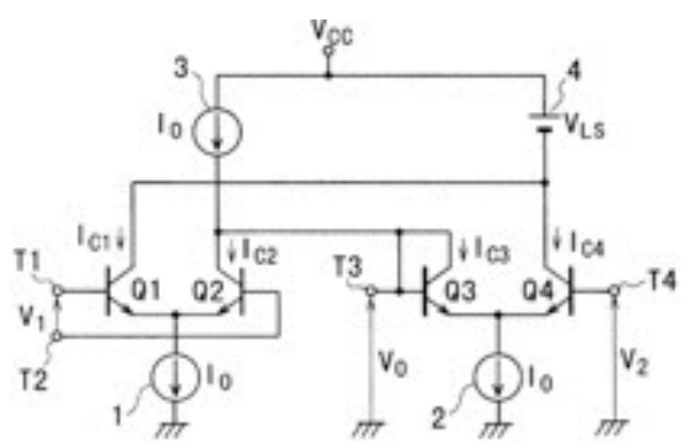
Advances at Google, Intel, and several research groups indicate that computers with previously unimaginable power are finally within reach.

Availability: 4-5 years

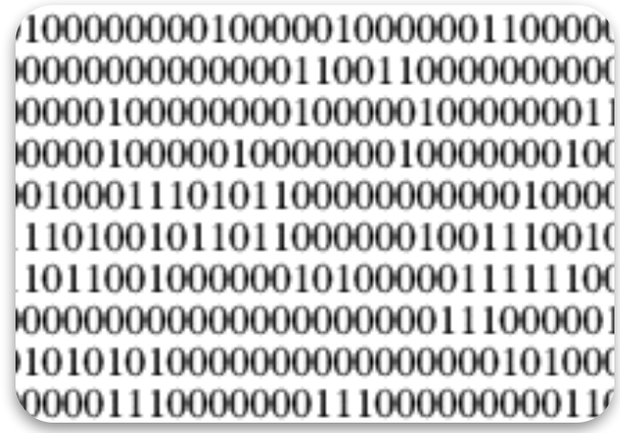


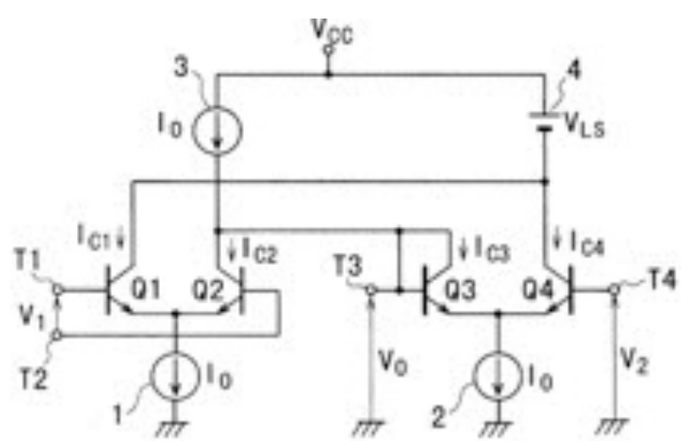
Motivations

Motivations



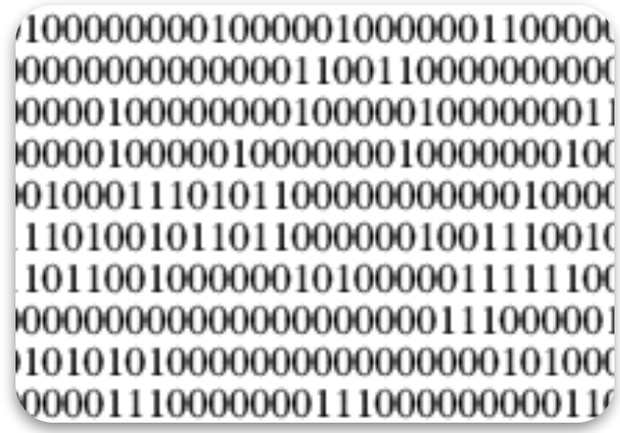
Motivations

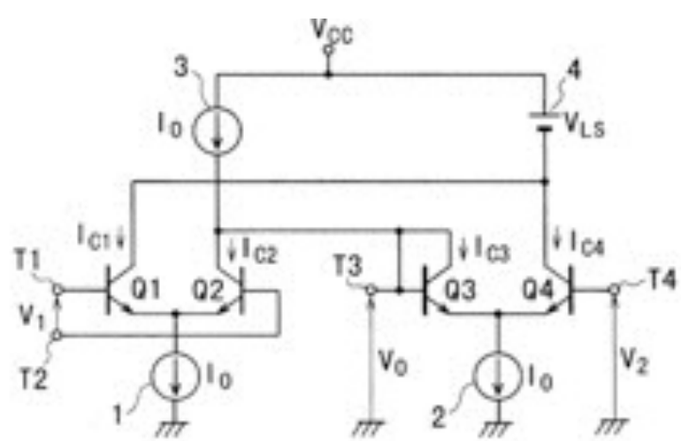




Motivations

```
fun fact 0 = 1
  | fact x = x * fact (x-1)
```

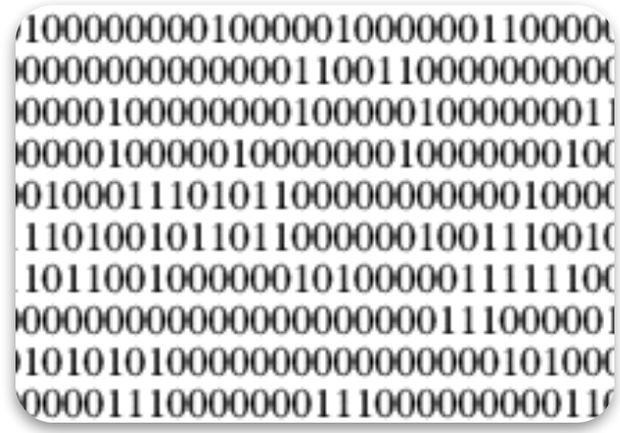


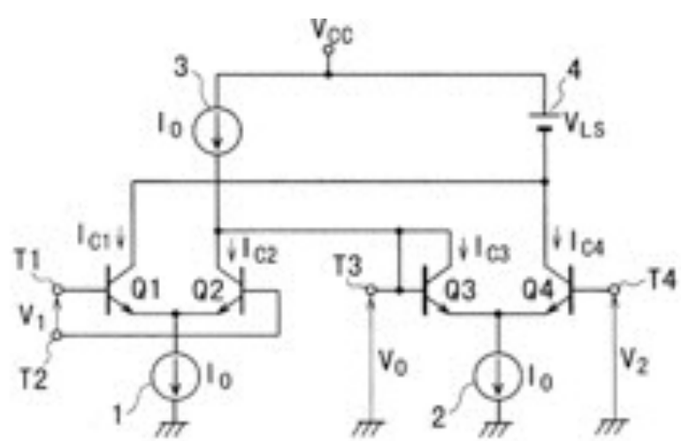


Motivations

$$\lambda x.\lambda y.\lambda z.xz(yz)$$

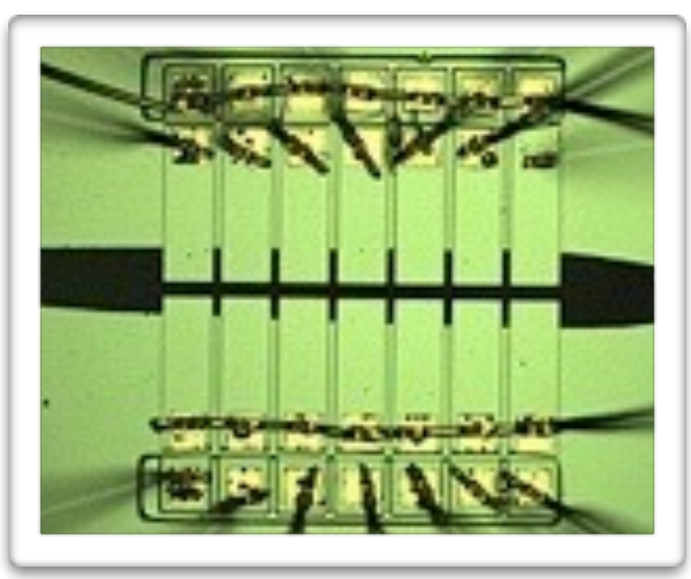
```
fun fact 0 = 1
  | fact x = x * fact (x-1)
```

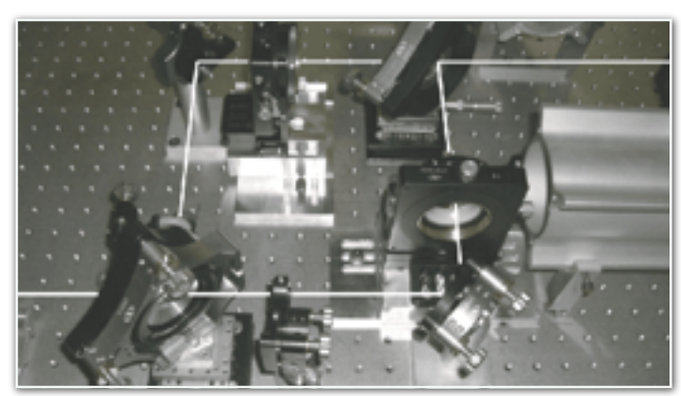




Motivations

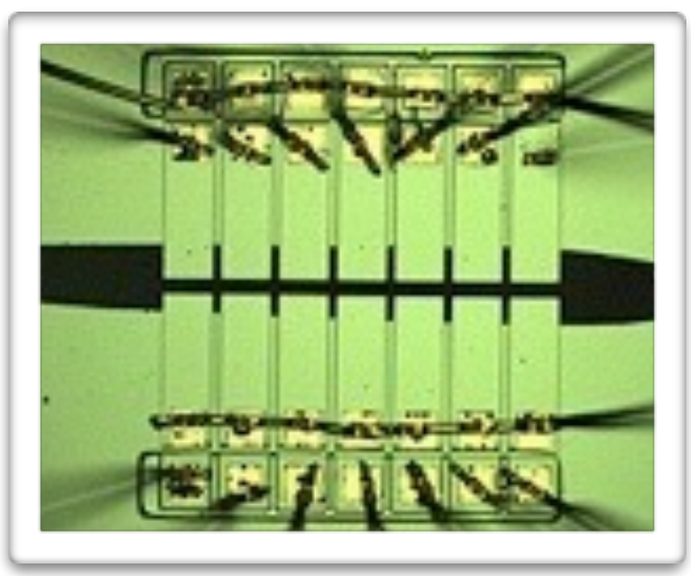
Motivations

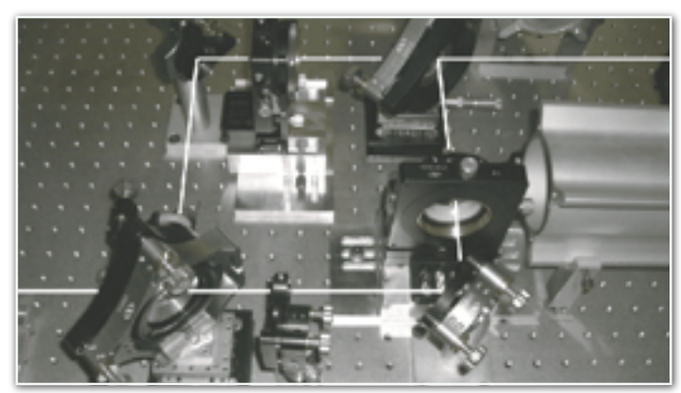




Motivations

Hilbert space,
unitary transforms,
self-adjoint operators....

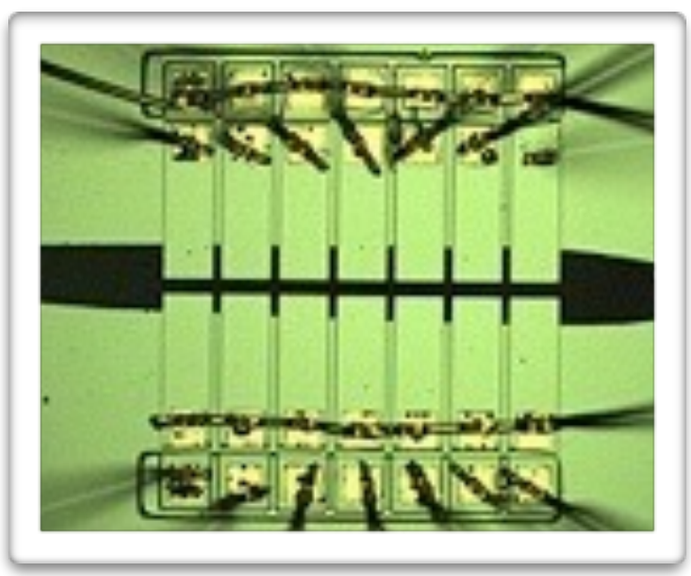


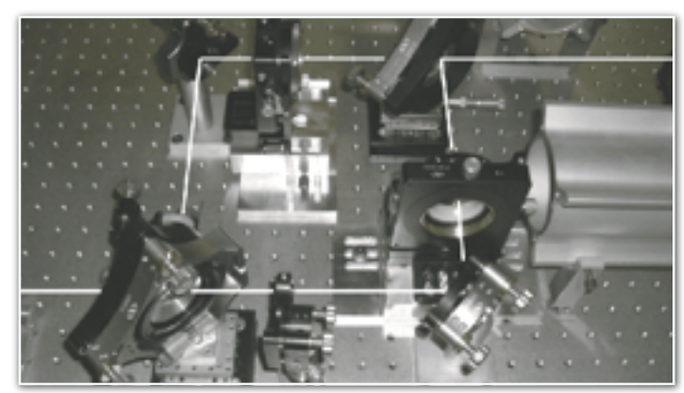


Motivations

????

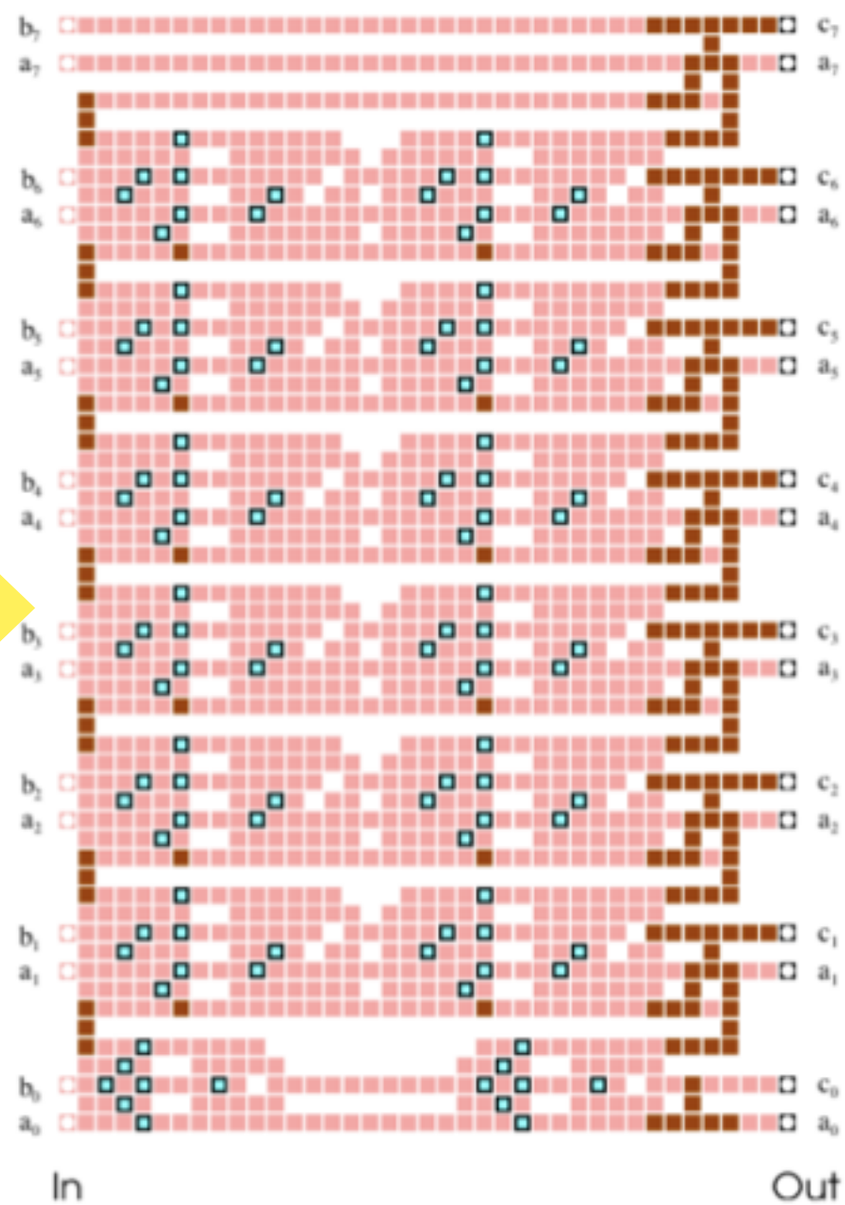
Hilbert space,
unitary transforms,
self-adjoint operators....





The need for abstraction:

This is an
8-bit adder



D ~ 2^1764

What’s so special about quantum?

What’s so special about quantum?

Seek a **mathematical** answer.

Superposition?

Telegraph.co.uk

BEST CONSUMER ONLINE PUBLISHER aop uk

Home | News | Sport | Business | Travel | Jobs | Motoring | Telegraph TV | SEARCH

Earth home
Earth news
Earth watch
Comment
Charles Clover
Greener living
Earth Pulse

Science

Messageboards

Will the QC kill the PC?

Last Updated: 12:01am BST 01/07/2008

- Why we should celebrate Charles Darwin

Quantum computers could become a reality very soon, opening up some fa possibilities - including teleportation, says Richard Gray

It might be the science of the very small, but quantum computing is on the verge some giant problems. For more than 30 years, physicists have dreamed of harne power of atoms to produce computers that would far outstrip the capabilities of t microchips used in today's PCs.

Superposition?

Telegraph.co.uk

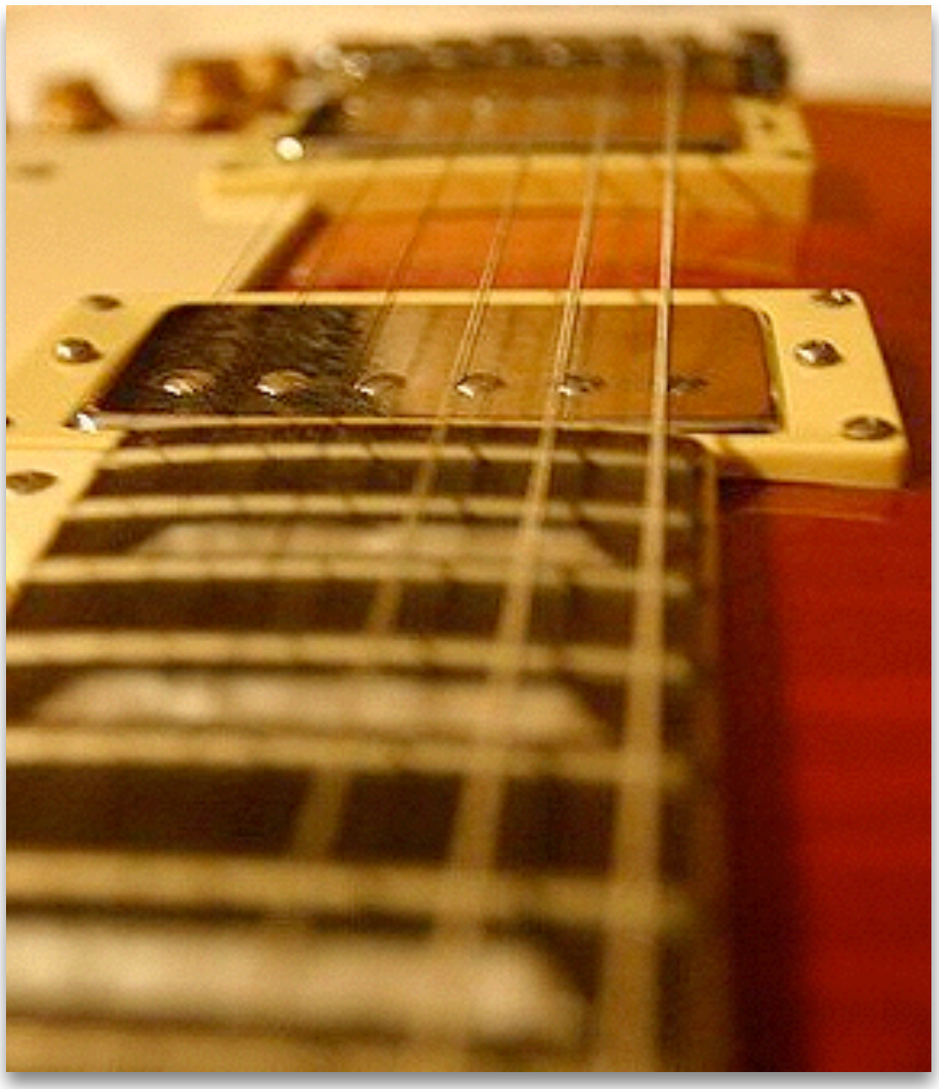
BEST CONSUMER ONLINE PUBLISHER aop uk

News | Sport | Business | Travel | Jobs | Motoring | Telegraph TV | SEARCH

Traditional computers shuffle information in the form of binary numbers, the digits 1 and 0, which are remembered by the "on" and "off" positions of tiny switches, or "bits", on the circuit boards. Quantum computers use atoms and subatomic particles as the switches that perform the memory and processing tasks.

The difference is that in quantum computing, the switches can be "on" and "off" at the same time. This means the basic component, the "qubit", can be involved in multiple calculations, while its strange properties also allow such computers to skip the step-by-step operations that current PCs use.

Superposition?



Classical waves can exhibit superposition too!

No-Cloning and No-Deleting

<u>Theorem</u>: There are no unitary operations D such that

$$D : |\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$$
$$D : |\phi\rangle \mapsto |\phi\rangle \otimes |\phi\rangle$$

unless $|\psi\rangle$and $|\phi\rangle$ are orthogonal [Wooters & Zurek 1982]

<u>Theorem</u>: There are no unitary operations E such that

$$E : |\psi\rangle \mapsto |0\rangle$$
$$E : |\phi\rangle \mapsto |0\rangle$$

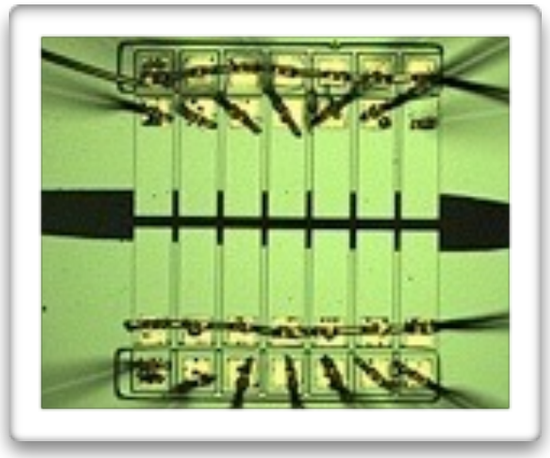
unless $|\psi\rangle$and $|\phi\rangle$ are orthogonal [Pati & Braunstein 2000]

No-Cloning and No-Deleting

Linear types have been proposed* to capture this:

$$!A \qquad\qquad A \otimes B$$

Separate classical and quantum data in a hybrid machine

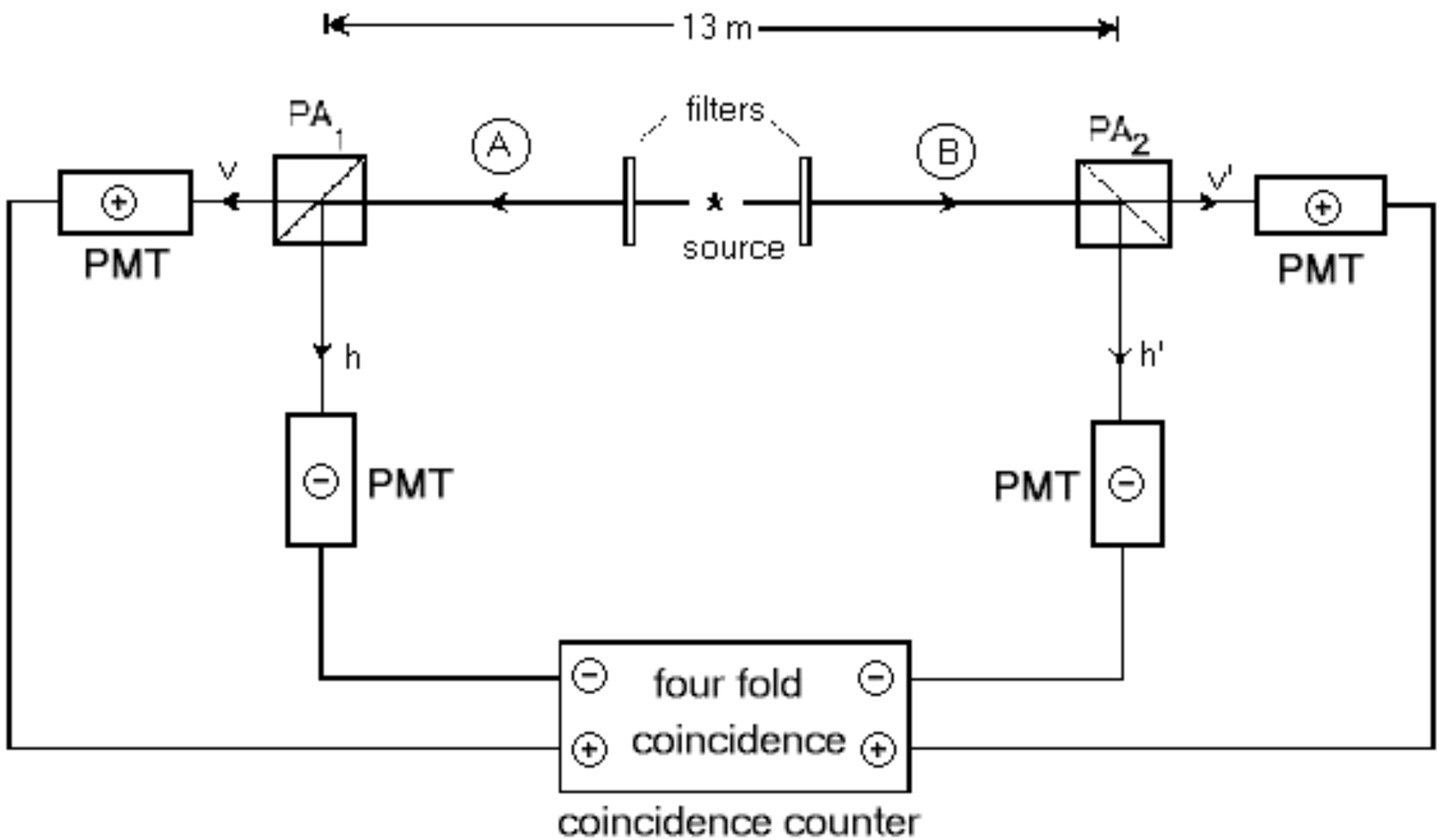


** Hensinger et al *Nature 2005*

But we need additional axioms to get the QM-like behaviour

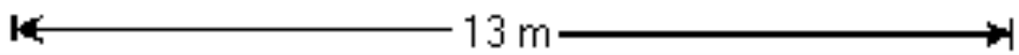
*vanTonder 2003, Selinger and Valiron 2005, Arrighi and Dowek 2003, Altenkirch & Grattage 2005

Non-locality or Contextuality?



* Aspect et al
PRL 1981

Non-locality or Contextuality?



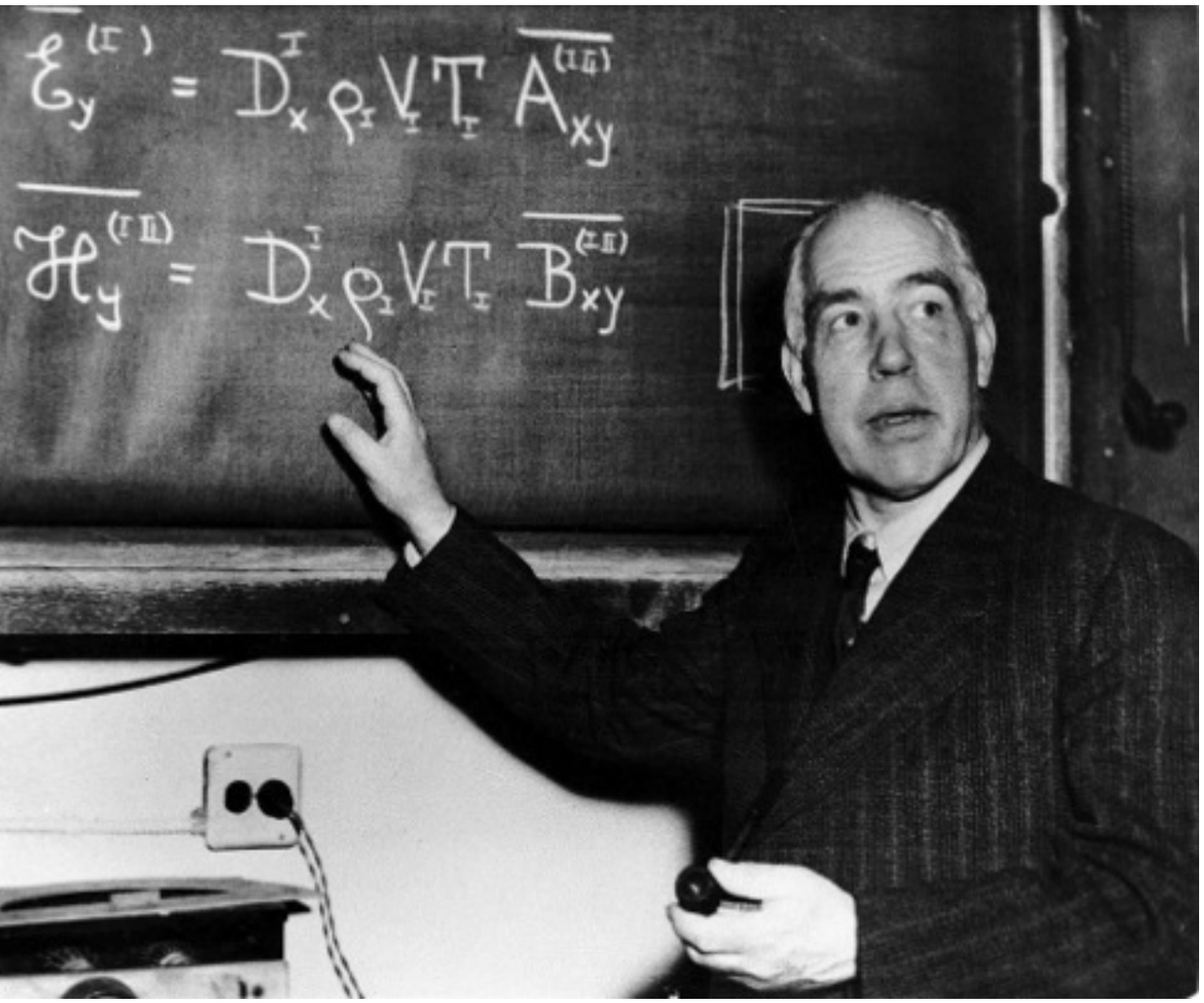
But!

“generalised probabilistic theories” display even stronger non-locality than quantum theory!

Many aspects of contextuality appear in classical settings like databases and NLP!

* Aspect et al
PRL 1981

Complementarity



Quantum systems have properties which are not accessible at the same time.
They are not even simultaneously well-defined!

abstraction

Quantum Theory

Hilbert spaces

Operators

Categorical Quantum Theory

Monoidal categories

(co)Algebras

Commutation rules

Categorical Quantum Theory

formalisation

Monoidal categories
(co)Algebras
Commutation rules

CQT as an “algebraic theory”

PROPs
Distributive laws

Categorical Quantum Theory

Quantum theory as an *internal* theory in a monoidal category

- No assumption of linear structure
- Algebra : $A \otimes A \longrightarrow A$
- Coalgebra : $A \longrightarrow A \otimes A$
- And laws for their interaction.

1.

Monoidal Categories

1. Symmetric Monoidal Categories

A monoidal category M is a category with a bifunctor, $\otimes$ or $\square$,

$$\square : M \times M \to M$$

written for objects a, b of M variously as a "product"

$$(a, b) \to a \square b, a \otimes b, \text{or } a\,b$$

which is associative up to a natural isomorphism

$$\alpha : a(b\,c) \cong (a\,b)c \tag{1}$$

and is equipped with an element e, which is unit up to natural isomorphisms

$$\lambda : e\,a \cong a\,, \qquad \rho : a\,e \cong e\,. \tag{2}$$

These maps must satisfy certain commutativity requirements; for α, a pentagonal diagram

$$\begin{tikzcd} a(b(c\,d)) \arrow[r, "\alpha"] \arrow[d, "1\alpha"'] & (a\,b)(c\,d) \arrow[r, "\alpha"] & ((a\,b)c)d \arrow[d, "\alpha 1"] \\ a((b\,c)d) \arrow[rr, "\alpha"] & & (a(b\,c))d\,, \end{tikzcd} \tag{3}$$

as in § VII.1.(5), and for λ and ρ the two commutativities

$$\begin{tikzcd} a(e\,c) \arrow[r, "\alpha"] \arrow[d, "1\lambda"'] & (a\,e)c \arrow[d, "\rho 1"] \\ a\,c \arrow[r, equal] & a\,c\,, \end{tikzcd} \qquad \lambda = \rho : e\,e \to e\,. \tag{4}$$

A *braiding* for a monoidal category M consists of a family of isomorphisms

$$\gamma_{a,b} : a \square b \cong b \square a \tag{5}$$

natural in a and $b \in M$, which satisfy for e the commutativity

$$\begin{tikzcd} a \square e \arrow[r, "\gamma"] \arrow[d, "\rho"'] & e \square a \arrow[d, "\lambda"] \\ a \arrow[r, equal] & a \end{tikzcd} \tag{6}$$

and which, with the associativity α, make both the following hexagonal diagrams commute (with the symbol $\square$ omitted):

$$\begin{tikzcd} (a\,b)c \arrow[r, "\gamma"] \arrow[d, "\alpha^{-1}"] & c(a\,b) \arrow[d, "\alpha"] & a(b\,c) \arrow[r, "\gamma"] \arrow[d, "\alpha"] & (b\,c)a \arrow[d, "\alpha^{-1}"] \\ a(b\,c) \arrow[d, "1\cdot\gamma"'] & (c\,a)b \arrow[d, "\gamma\cdot 1"] & (a\,b)c \arrow[d, "\gamma\cdot 1"] & b(c\,a) \arrow[d, "1\cdot\gamma"] \\ a(c\,b) \arrow[r, "\alpha"] & (a\,c)b\,, & (b\,a)c \arrow[r, "\alpha^{-1}"] & b(a\,c)\,. \end{tikzcd} \tag{7}$$

Note that the first diagram replaces each $\gamma_{ab,c}$ which has a product $a\,b$ as first index by two γ's with single indices, while the second hexagonal diagram does the same for $\gamma_{a,bc}$ with a product as second index. Note also that the first hexagon of (7) for γ implies the second diagram for γ^{-1}, and conversely. Thus, when γ is a braiding for M, then γ^{-1} is also a braiding for M.

A *symmetric monoidal category*, as already defined in § VII. 7, is a category with a braiding γ such that every diagram

$$\begin{tikzcd} a\,b \arrow[r, "\gamma_{a,b}"] \arrow[dr] & b\,a \arrow[d, "\gamma_{b,a}"] \\ & a\,b \end{tikzcd} \tag{8}$$

commutes. For this case, either one of the hexagons (7) implies the other.

1bis.

Monoidal Categories (Graphically)


PAST / HEAVEN
FUTURE / HELL

Why Diagrams?

Why Diagrams?

$$
\begin{aligned}
&\frac{1}{2}\left(\begin{pmatrix}1\\1\end{pmatrix}\otimes\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{i\gamma}\end{pmatrix}\otimes\begin{pmatrix}0&1\\1&0\end{pmatrix}\right)\\
&\circ\left(\left(\left(\begin{pmatrix}1&0&0&0\\0&0&0&1\end{pmatrix}\otimes\begin{pmatrix}1&1\\1&-1\end{pmatrix}\right)\circ\left(\begin{pmatrix}0&1\\1&0\end{pmatrix}\otimes\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}\right)\right)\circ\right.\\
&\qquad\left.\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)\right)\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)\\
&\circ\left(\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\circ\left(\begin{pmatrix}\cos\frac{\pi}{6}\\ i\sin\frac{\pi}{6}\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&e^{i\beta}\end{pmatrix}\right)\right)\otimes\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{i\alpha}\end{pmatrix}\right)
\end{aligned}
$$

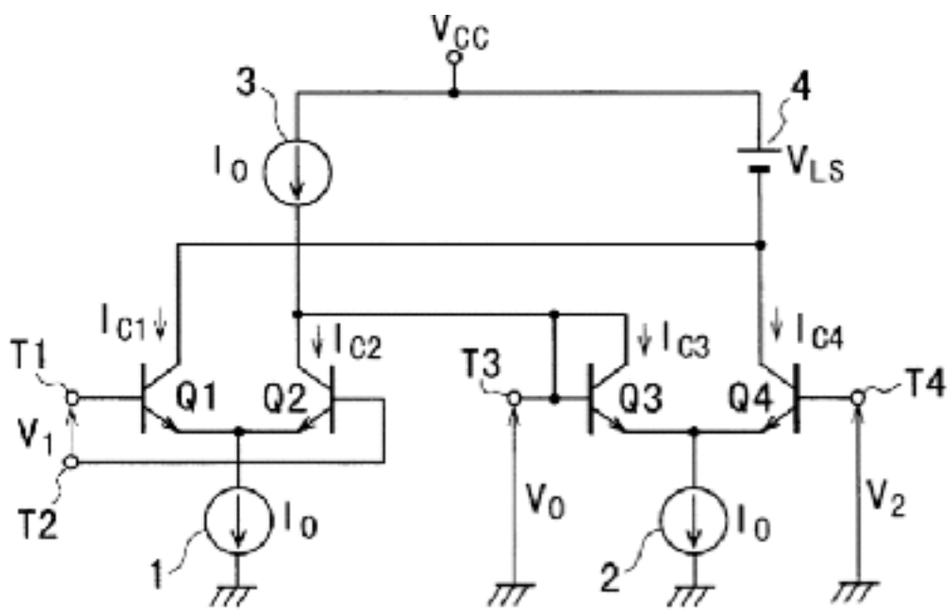
$$\stackrel{?}{=}$$

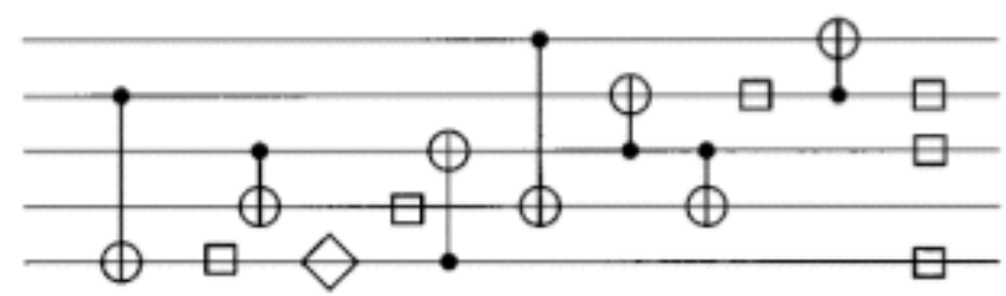
Why Diagrams?

- Great when we have parallel and sequential composition
- Essential for talking about interacting algebraic and coalgebraic things
- Different kinds of diagram give different kinds of monoidal category

Historical Examples

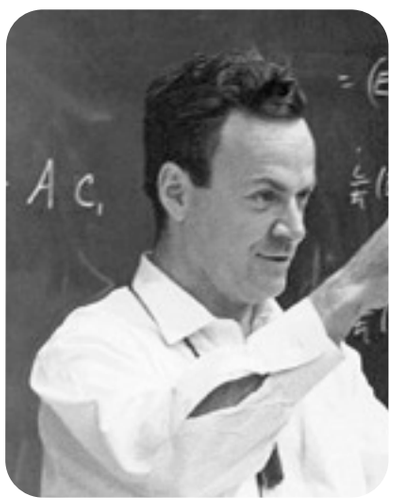
Circuits (classical and quantum) :

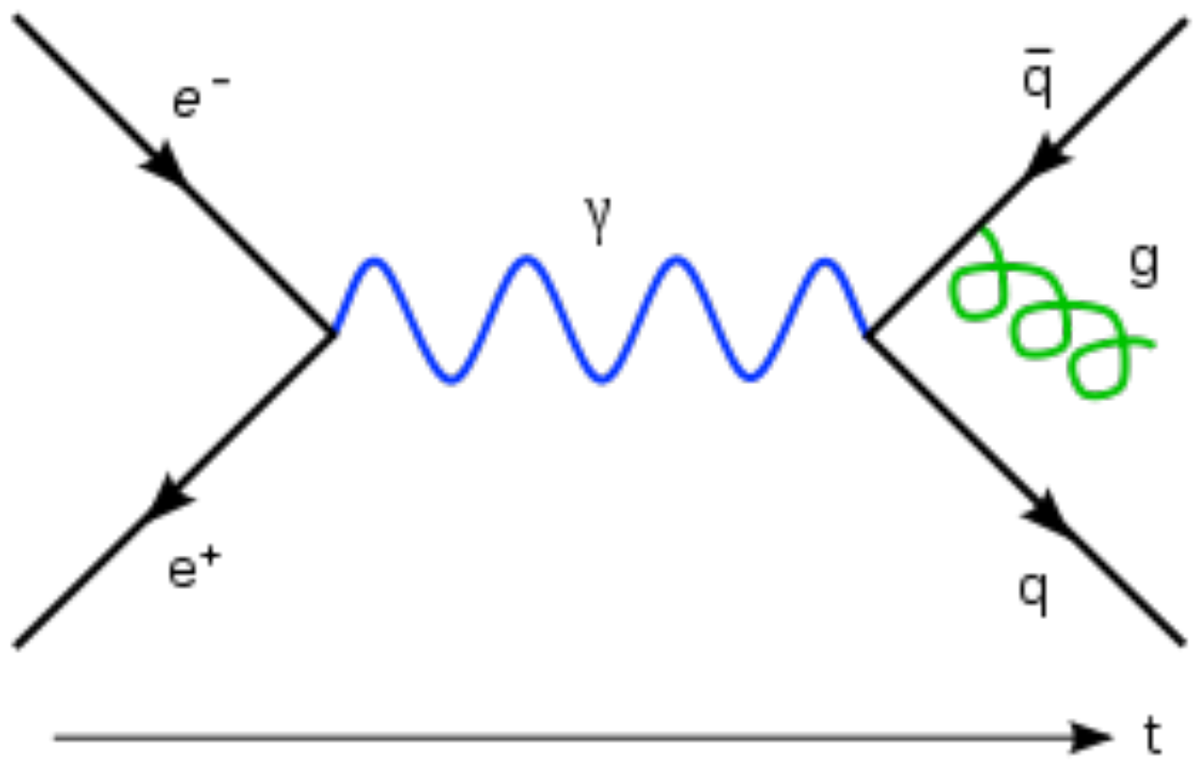




Historical Examples

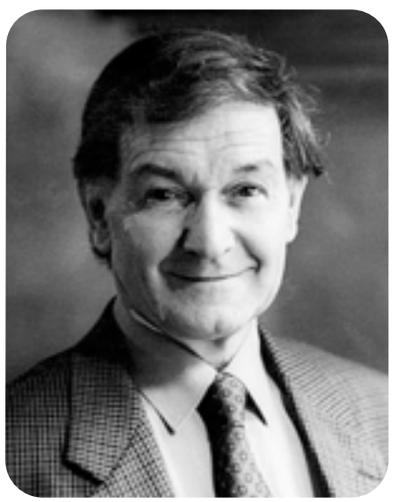
Feynmann Diagrams:

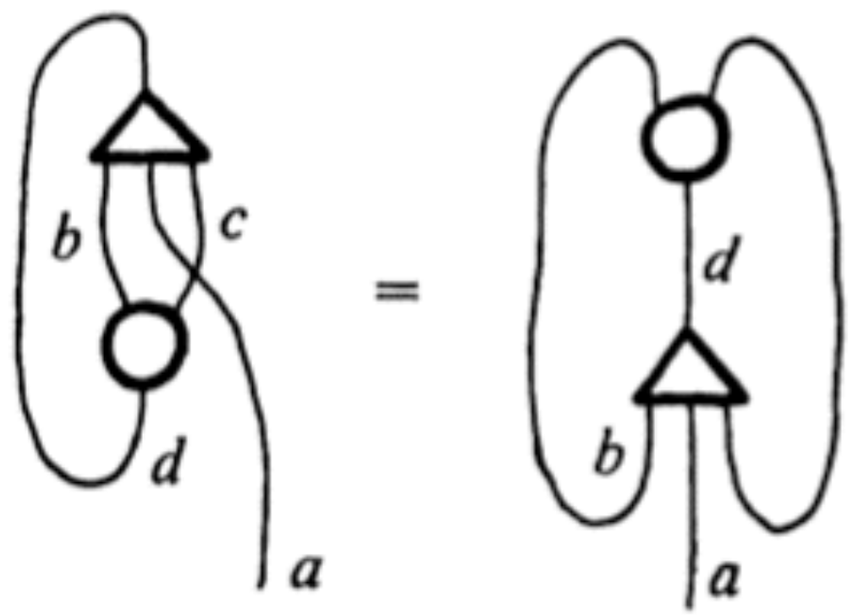




Historical Examples

"Applications of Negative Dimensional Tensors"
(Penrose)





$$= \theta^{bc}_{d}\, \chi^{d}_{bac} \in \mathscr{T}_{a}\,.$$

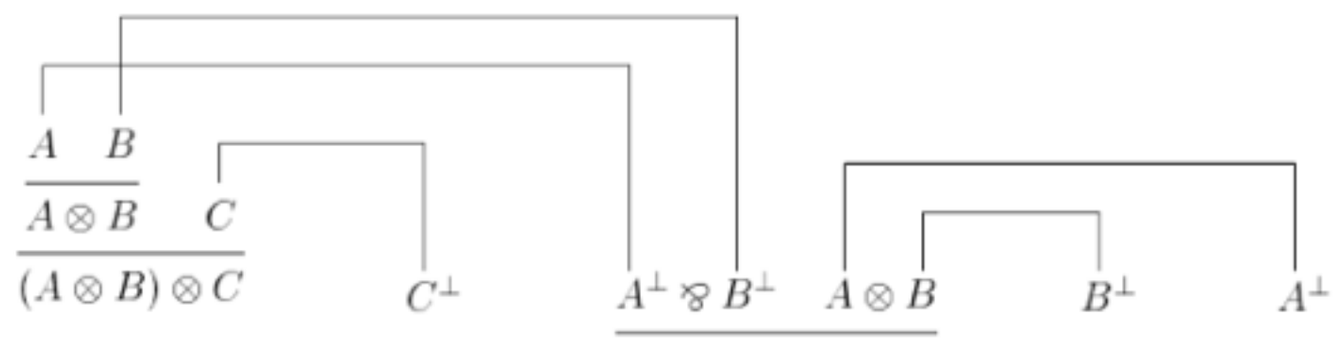
$$= \delta^{a}_{a} = \nu\,.$$

Historical Examples

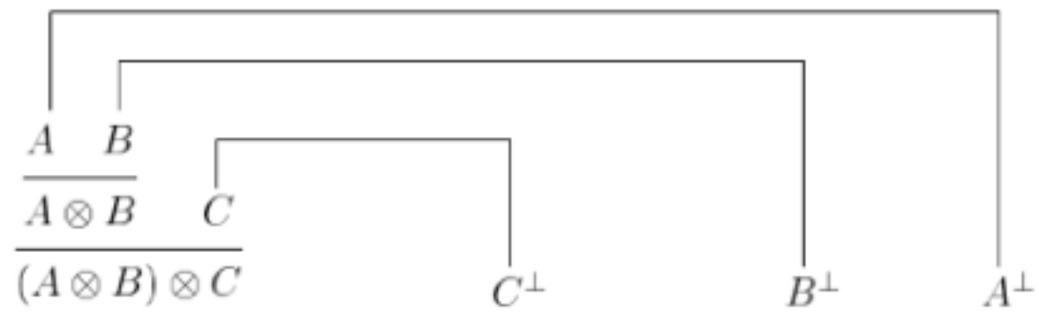
Proofs-Nets in Linear Logic

(Girard, Danos-Regnier, Tortoro de Falco, many others)

For example, the proof net



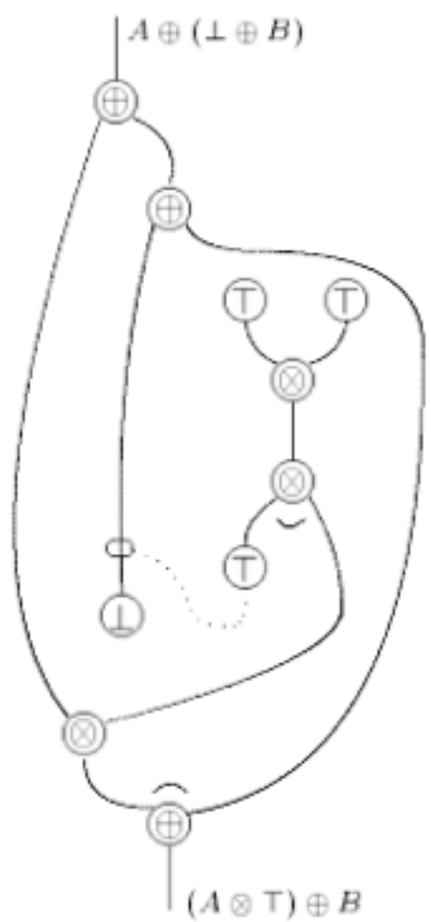
reduces (in three steps) to

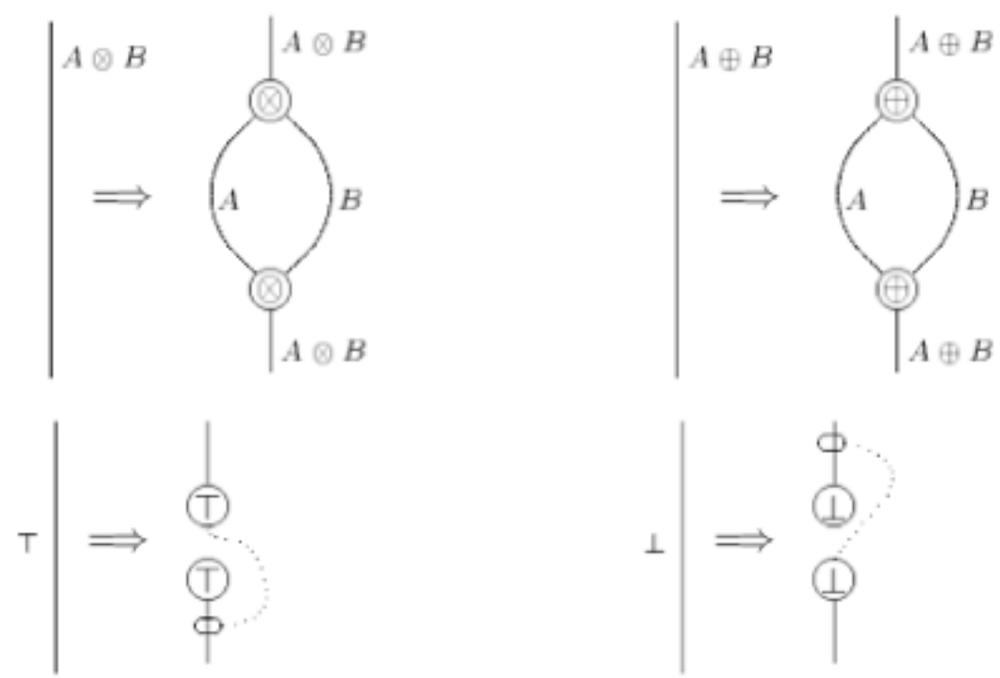


Historical Examples

Proofs-Nets in Linear Logic

(Blute-Cocket-Seely-Trimble, 1996)

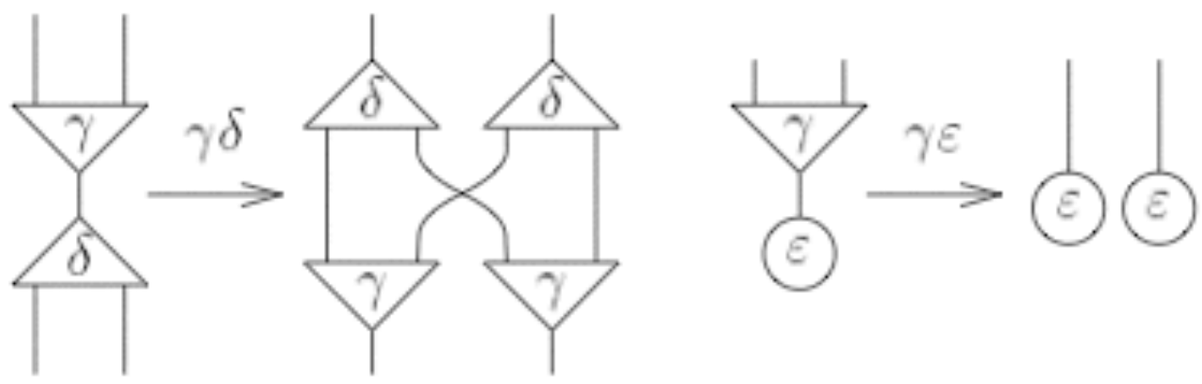


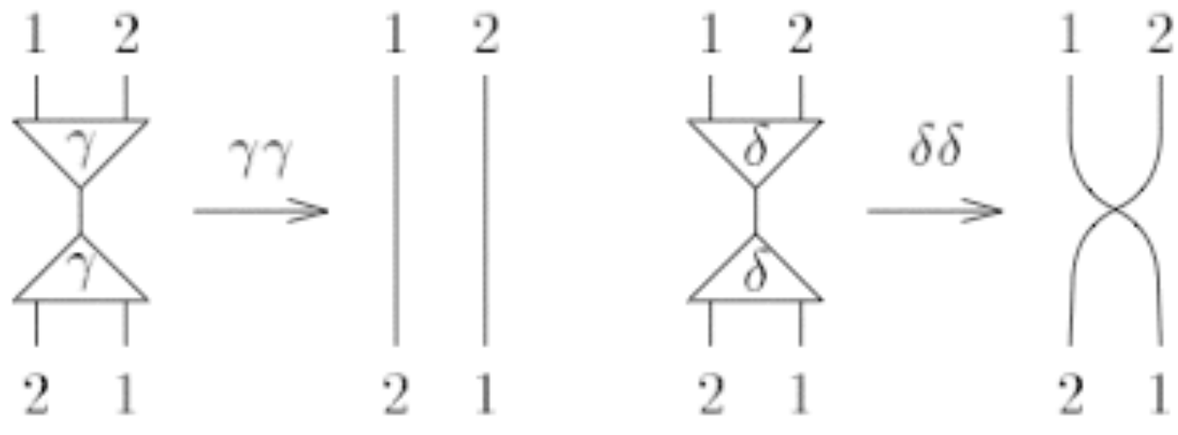


Historical Examples

Interaction Combinators

(Lafont, 1997)





Historical Examples

"Coherence for Compact Closed Categories"

(Kelly-Laplaza, 1980)

with I for the empty signed set; we write P^* for P with the signs reversed; and we write 1 for the one-element signed set with sign $+$.

By an *involution* θ we mean a category which is a coproduct of copies of the arrow-category **2**; these are really the *fixed-point-free* involutions, but we need no others. Such an involution is a special kind of *order* on its object-set $|P|$; and, as with orders in general, we do not distinguish two involutions on $|P|$ which differ only in the "names" of their maps. This object-set $|P|$ becomes *signed* when we attribute $-$ to the source and $+$ to the target of each arrow **2**; we call θ *an involution on the signed set* P when this signing agrees with that of P.

By a *loop* L we mean the free category on a graph of the form

$$A_1 \to A_2 \to \cdots \to A_n \to A_1,$$

for some $n \geq 1$. The composite represented by this string determines a canonical element $\langle L \rangle$ of the set $[L]$ of cycles of L, independently of where the loop is started.

We use $+$ for the coproduct of categories, and henceforth suppose all signed sets and involutions to be *finite*. If θ is an involution on the signed set $P^* \otimes Q$ and ϕ is one on $Q^* \otimes R$, consider the pushout $\theta +_{|Q|} \phi$ in **Cat**, obtained from the coproduct $\theta + \phi$ by identifying the two copies of the discrete category $|Q|$, one in θ and one in ϕ. Write $\phi\theta$ for the full subcategory of $\theta +_{Q} \phi$ determined by the object-set $|P| + |R|$; it is clearly an involution on $P^* \otimes R$; moreover we clearly have $\theta +_{Q} \phi = \phi\theta + \phi \star \theta$, where $\phi \star \theta$ is a coproduct $\sum L_i$ of loops with objects in $|Q|$. If now ψ is a third involution on $R^* \otimes S$, it is further immediate that

Historical Examples

"Coherence for Compact Closed Categories"

(Kelly-Laplaza, 1980)

Coherence for compact closed categories 197

with I for the empty signed set; we write P^* for P with the signs reversed; and we write 1 for the one-element signed set with sign $+$.

By an *involution* θ we mean a category which is a coproduct of copies of the arrow-category **2**; these are really the *fixed-point-free* involutions, but we need no others. Such an involution is a special kind of *order* on its object-set $|P|$; and, as with orders in general, we do not distinguish two involutions on $|P|$ which differ only in the "names" of their maps. This object-set $|P|$ becomes *signed* when we attribute $-$ to the source and $+$ to the target of each arrow **2**; we call θ *an involution on the signed set* P when this signing agrees with that of P.

By a *loop* L we mean the free category on a graph of the form

$$A_1 \to A_2 \to \cdots \to A_n \to A_1,$$

for some $n \geq 1$. The composite represented by this string determines a canonical element $\langle L \rangle$ of the set $[L]$ of cycles of L, independently of where the loop is started.

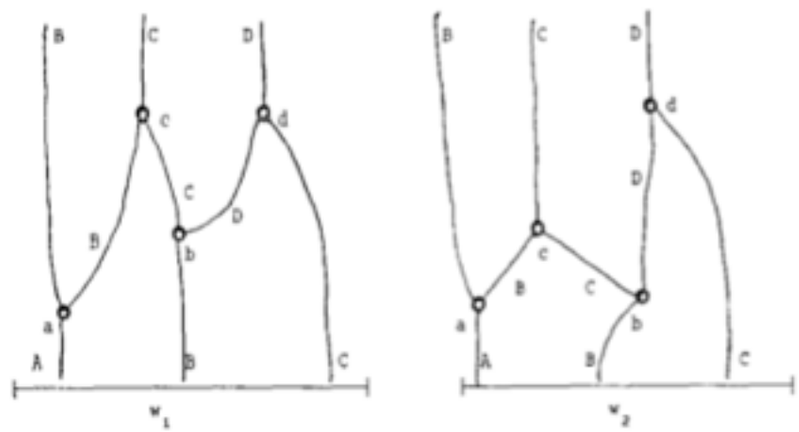
We use $+$ for the coproduct of categories, and henceforth suppose all signed sets and involutions to be *finite*. If θ is an involution on the signed set $P^* \otimes Q$ and ϕ is one on $Q^* \otimes R$, consider the pushout $\theta +_{|Q|} \phi$ in **Cat**, obtained from the coproduct $\theta + \phi$ by identifying the two copies of the discrete category $|Q|$, one in θ and one in ϕ. Write $\phi\theta$ for the full subcategory of $\theta +_Q \phi$ determined by the object-set $|P| + |R|$; it is clearly an involution on $P^* \otimes R$; moreover we clearly have $\theta +_{|Q|} \phi = \phi\theta + \phi \star \theta$, where $\phi \star \theta$ is a coproduct $\sum L_i$ of loops with objects in $|Q|$. If now ψ is a third involution on $R^* \otimes S$, it is further immediate that

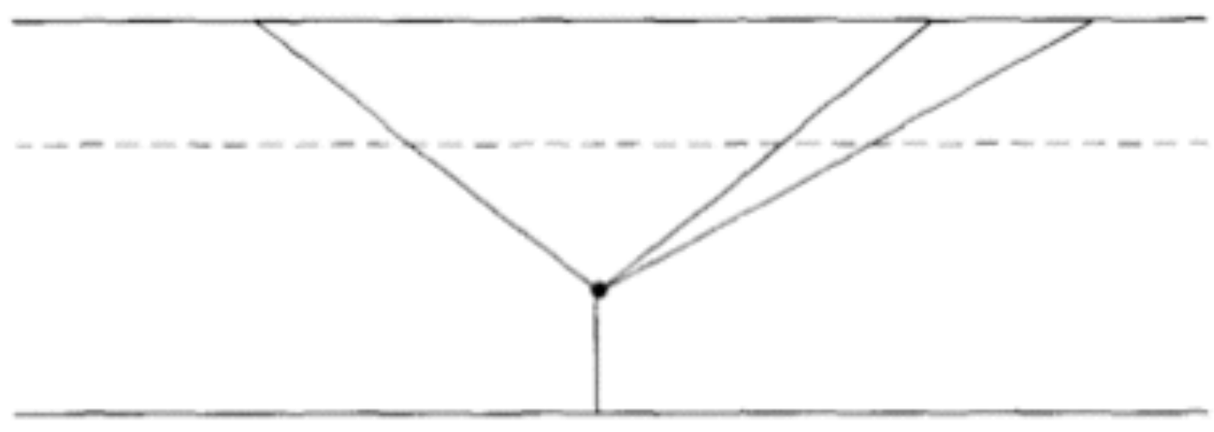
?

Historical Examples

"Geometry of Tensor Calculus I"

(Joyal-Street, 1991)

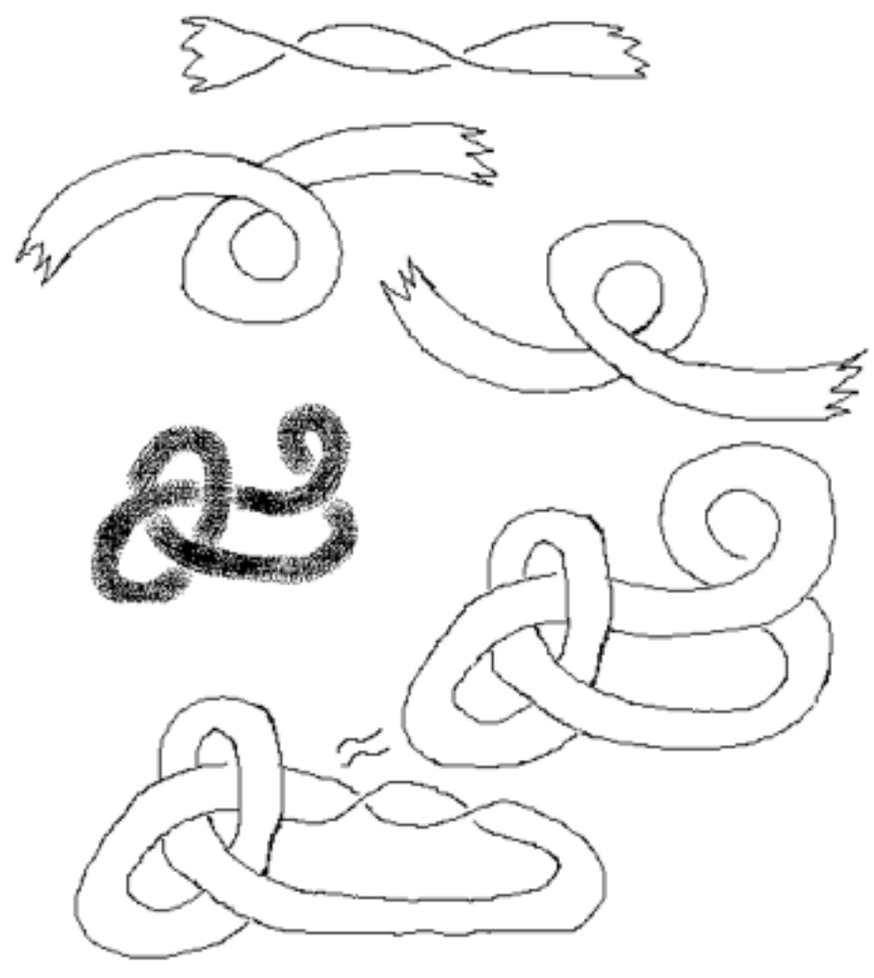




Historical Examples

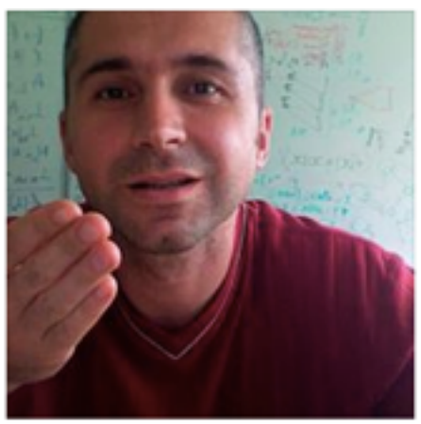
"Traced Monoidal Categories"

(Joyal-Street-Verity, 1996)

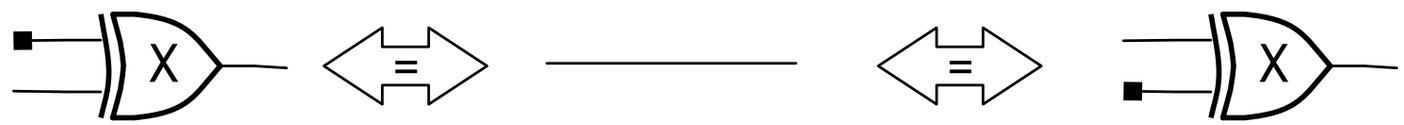


More Recently:

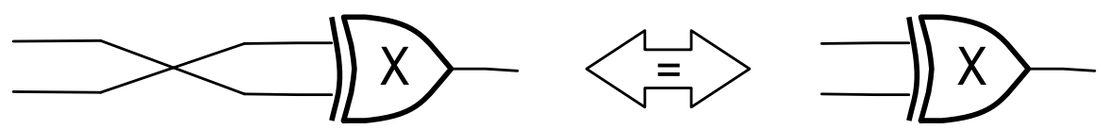
Ghica (2013) - Asynchronous Circuits



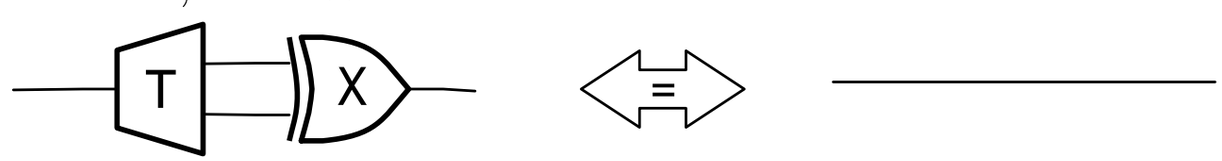
Unit $(U \otimes W); X = (W \otimes U); X = W.$



Commutativity $\gamma_A; X = X.$

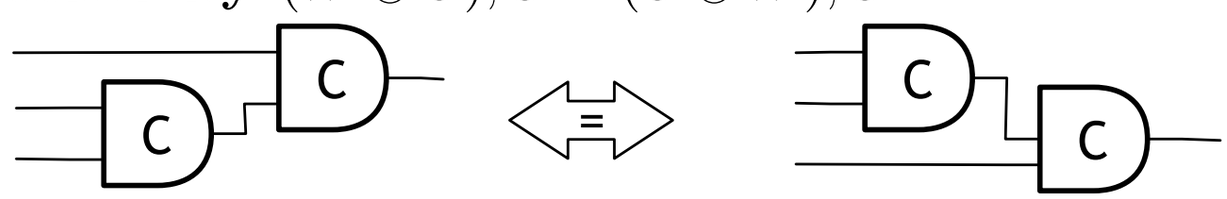


Retract $T; X = W.$



(A, C, P) *is a commutative monoid with* U *an absorbing element.*

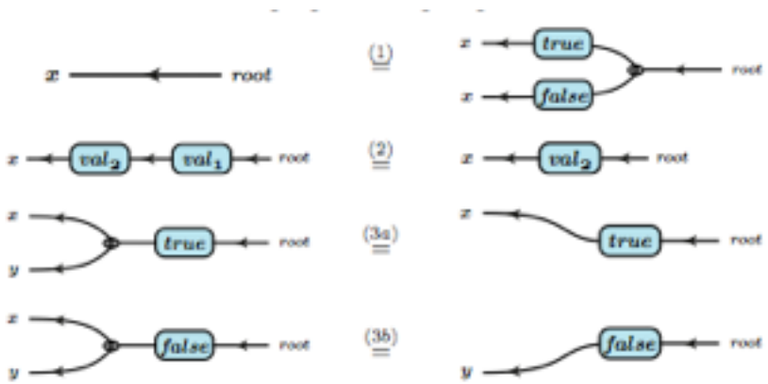
Associativity $(W \otimes C); C = (C \otimes W); C.$

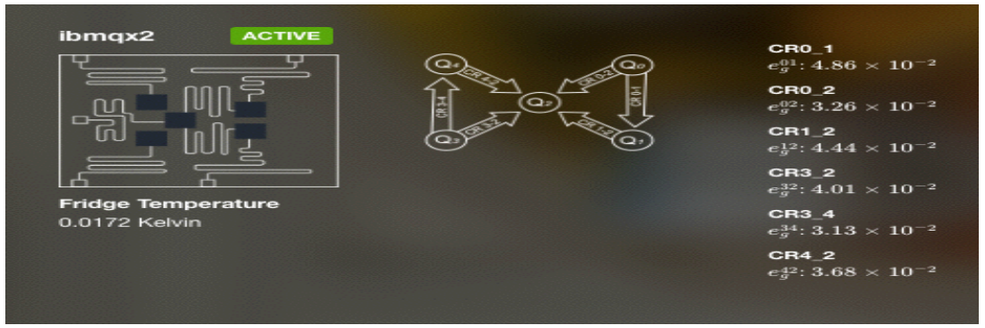


Unit $(P \otimes W); C = (W \otimes P); C = W$

More Recently:

Melliès (2014) - Local State





Grov Kissinger Lin (2013) - Proof Planning

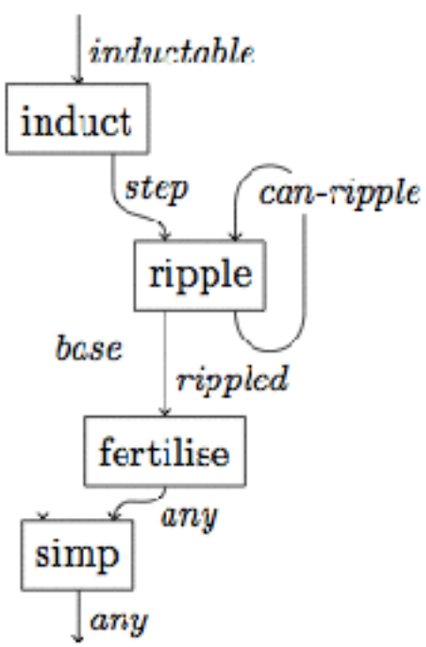
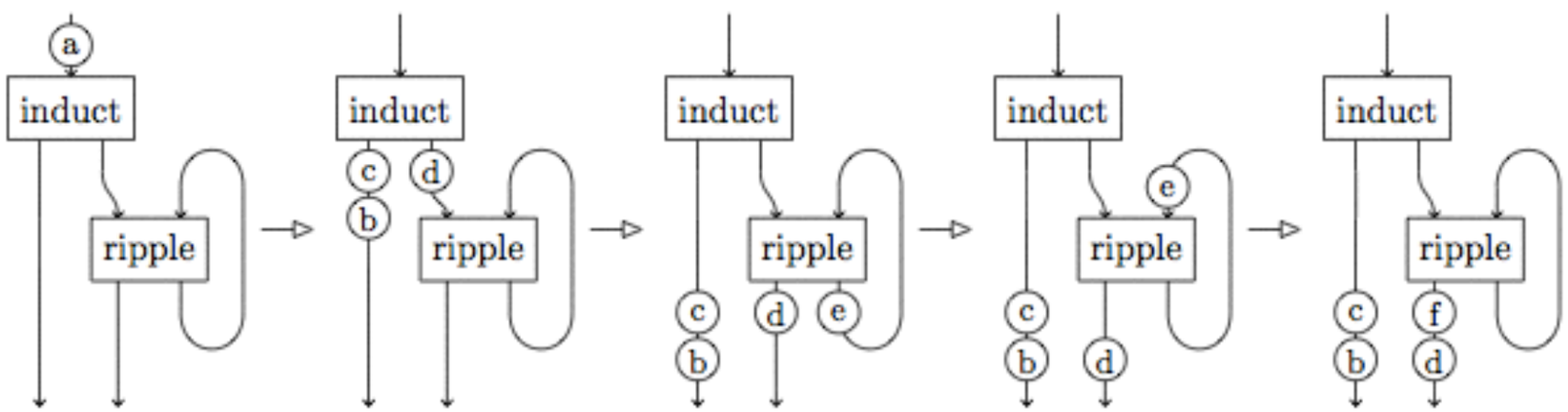
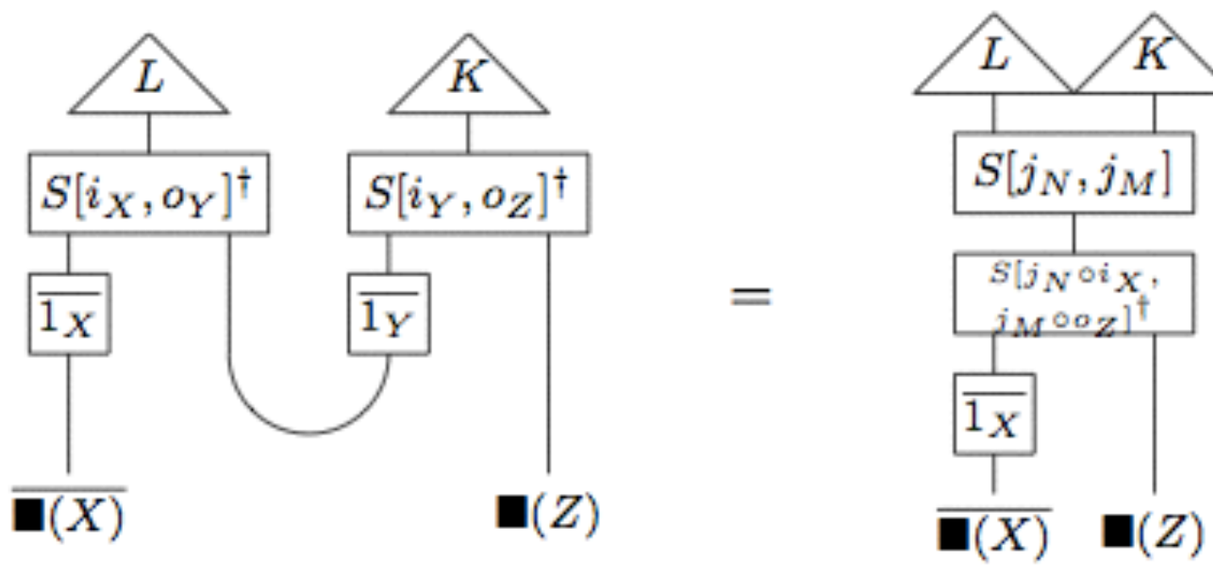


Fig. 2. Rippling



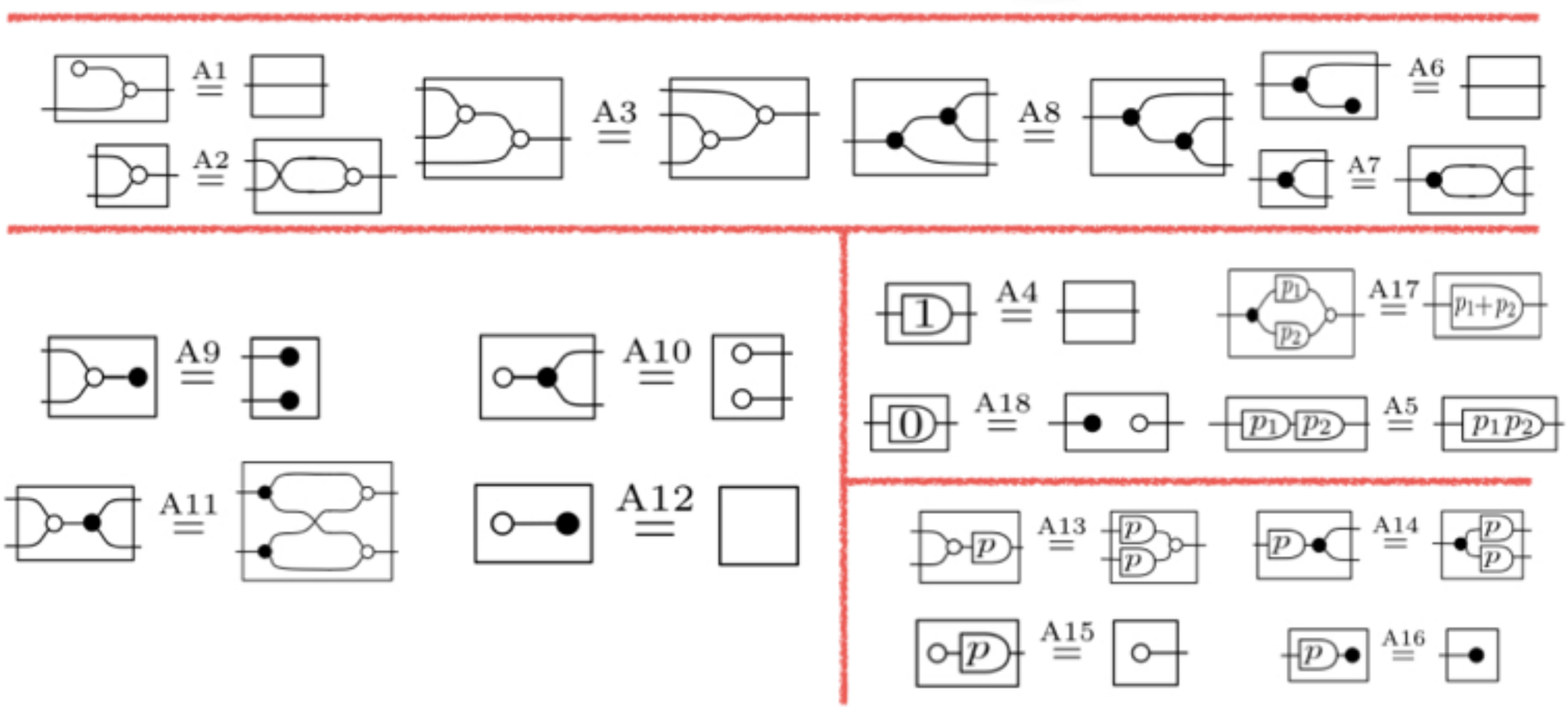
More Recently:

Baez and Fong (2014) — Passive Linear Circuits



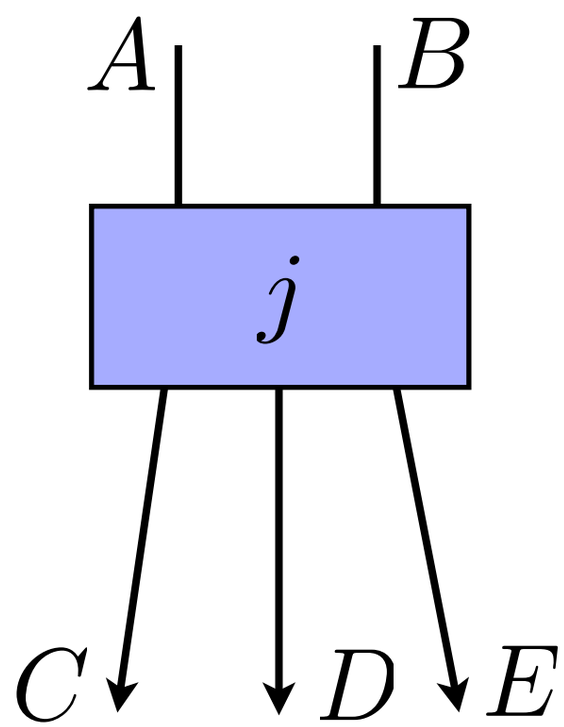
More Recently:

Bonchi Sobocinski Zanasi (2014) — Signal Flow Graphs



Diagrams

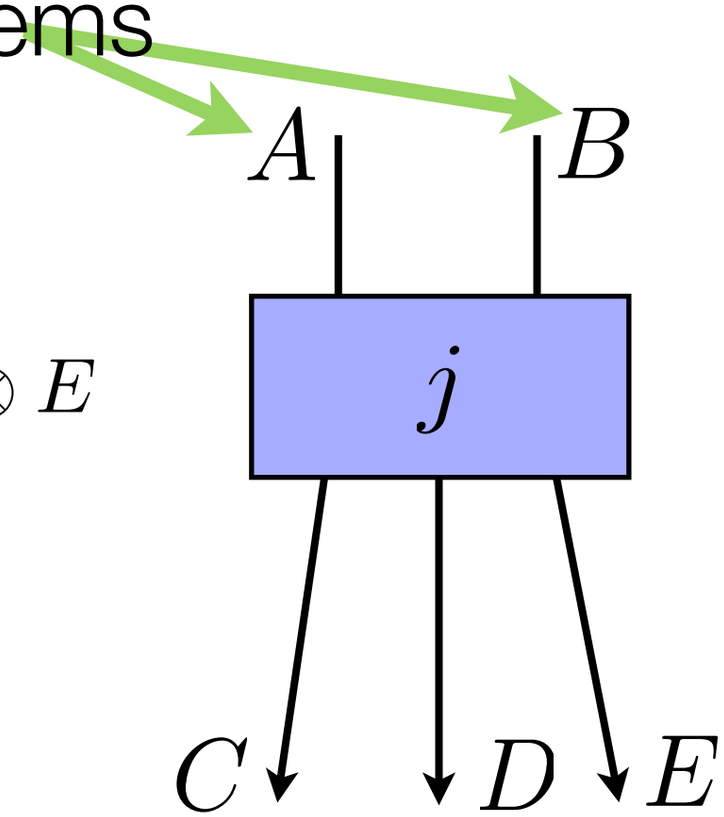
$j : A \otimes B \to C \otimes D \otimes E$



Diagrams

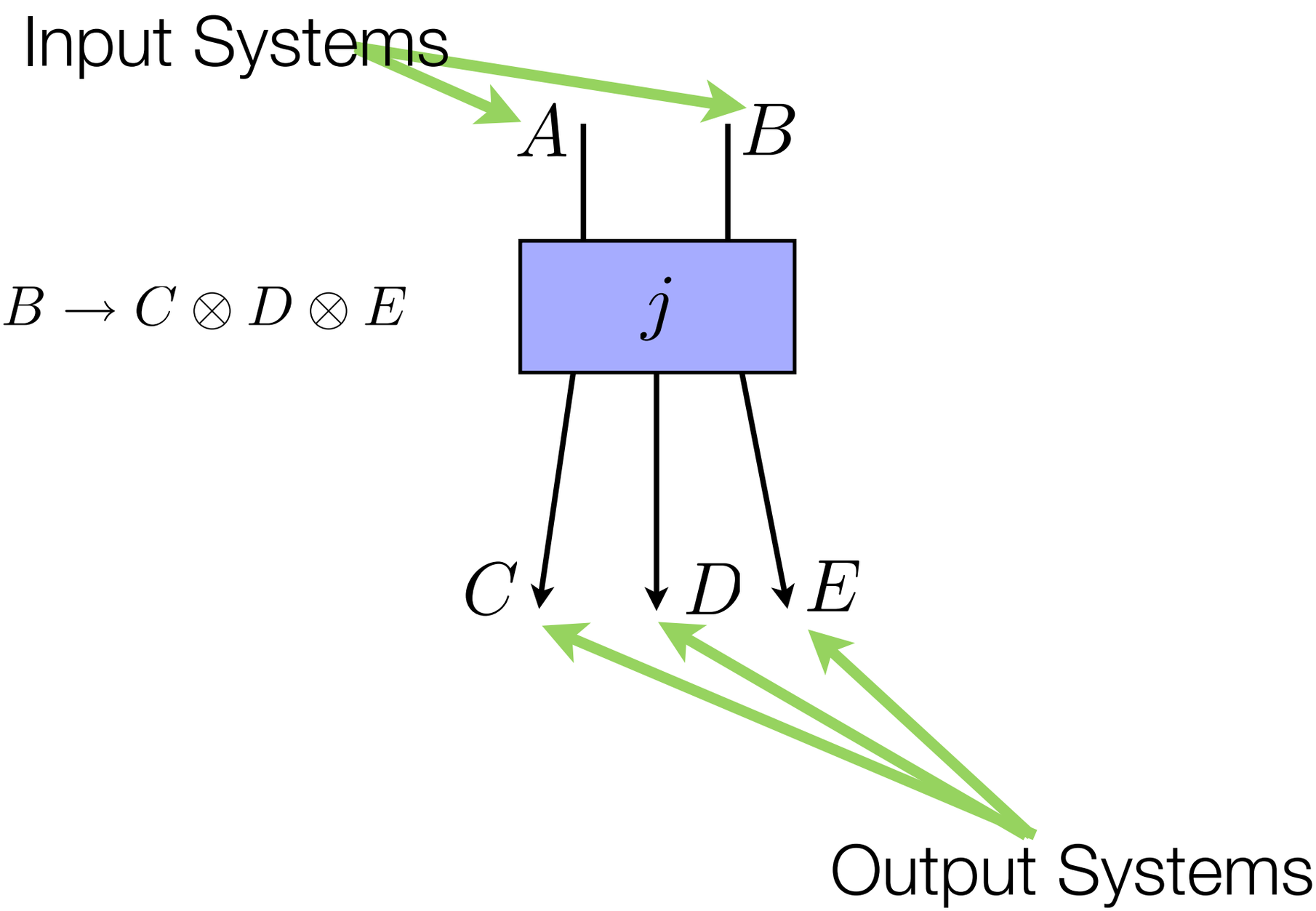
Input Systems

$j : A \otimes B \to C \otimes D \otimes E$

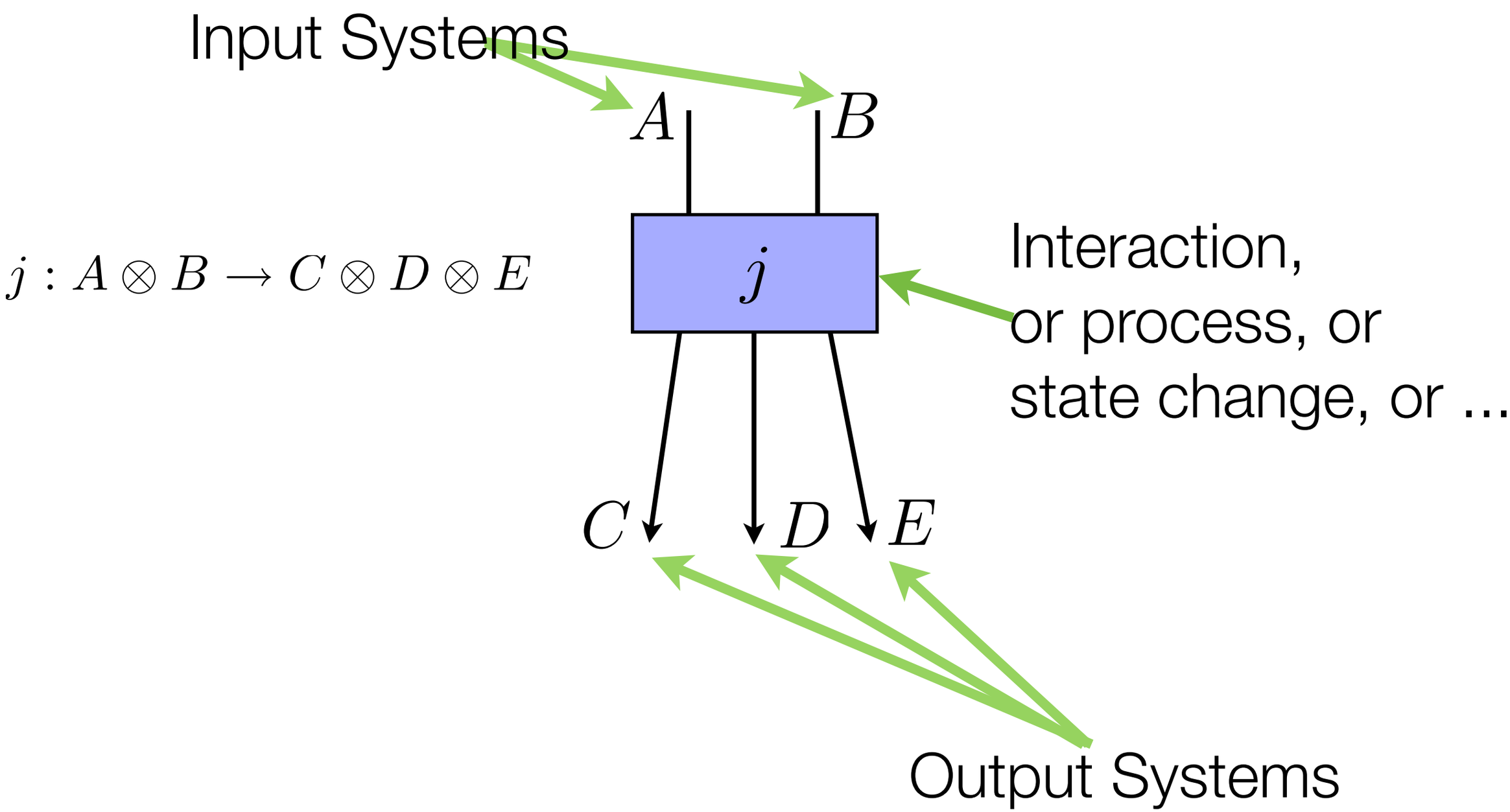


Diagrams

$j : A \otimes B \to C \otimes D \otimes E$

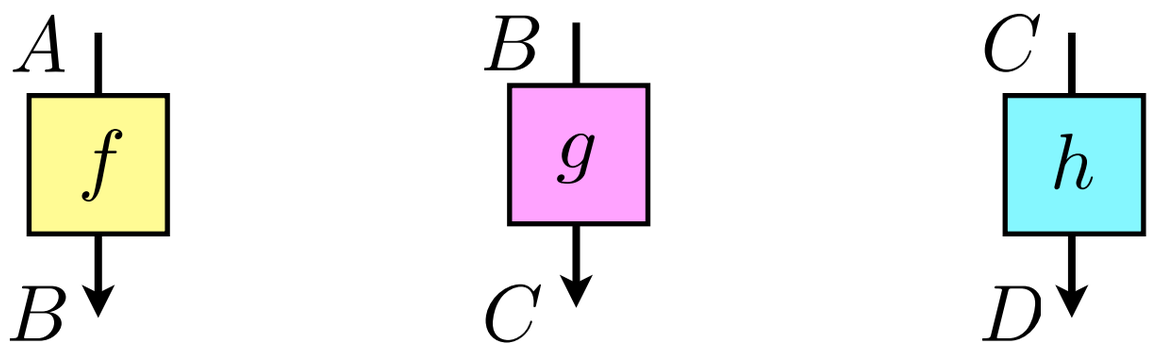


Diagrams


Input Systems
A
B
$j : A \otimes B \to C \otimes D \otimes E$
j
Interaction,
or process, or
state change, or ...
C
D
E
Output Systems

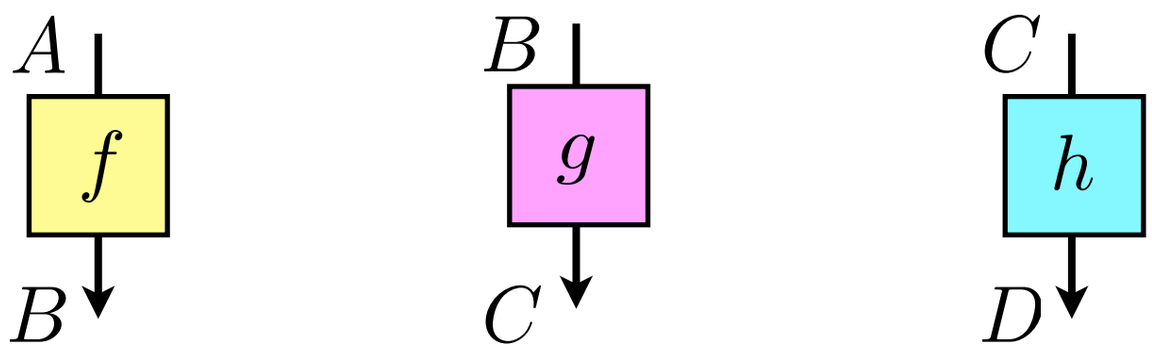
Monoidal Categories

$f : A \to B$ $\quad$ $g : B \to C$ $\quad$ $h : C \to D$

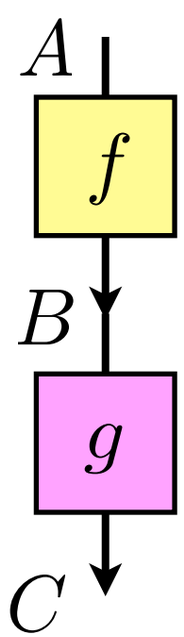


Monoidal Categories

$f : A \to B$ $\quad$ $g : B \to C$ $\quad$ $h : C \to D$

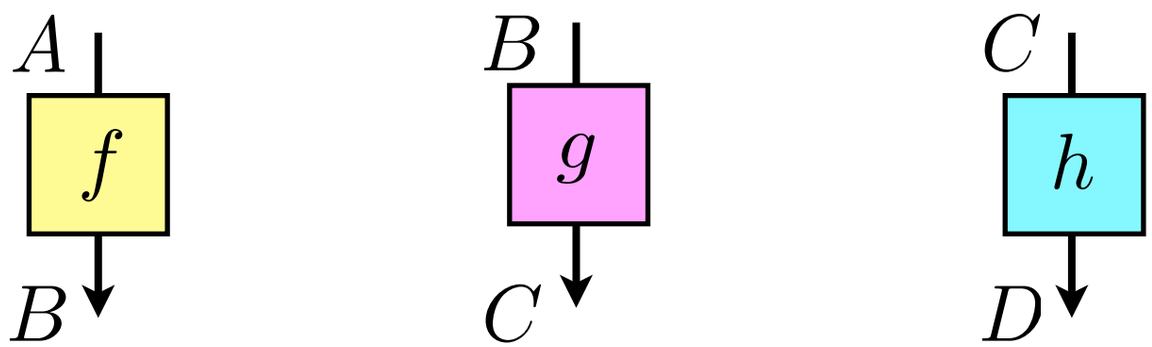


$g \circ f : A \to C$

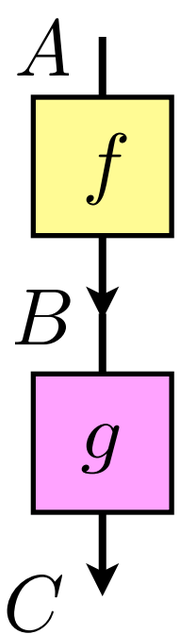


Monoidal Categories

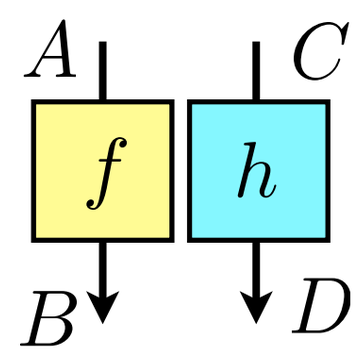
$f : A \to B$ $\quad$ $g : B \to C$ $\quad$ $h : C \to D$



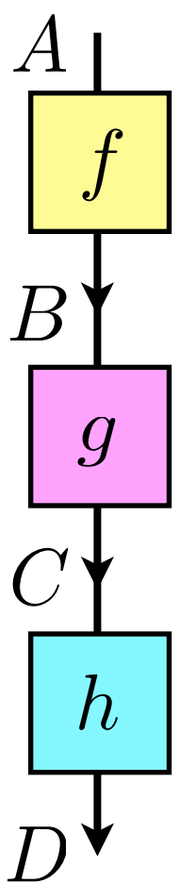
$g \circ f : A \to C$

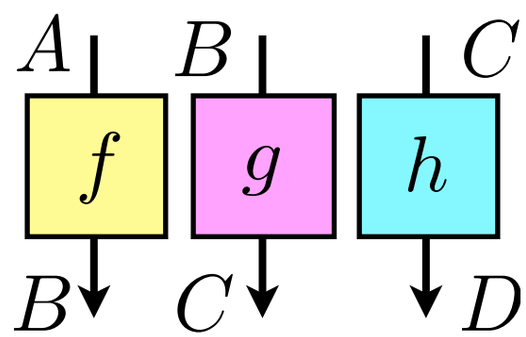


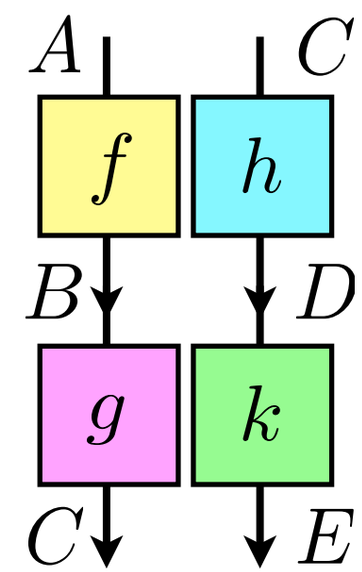
$f \otimes h : A \otimes C \to B \otimes D$



Monoidal Categories







Monoidal Categories

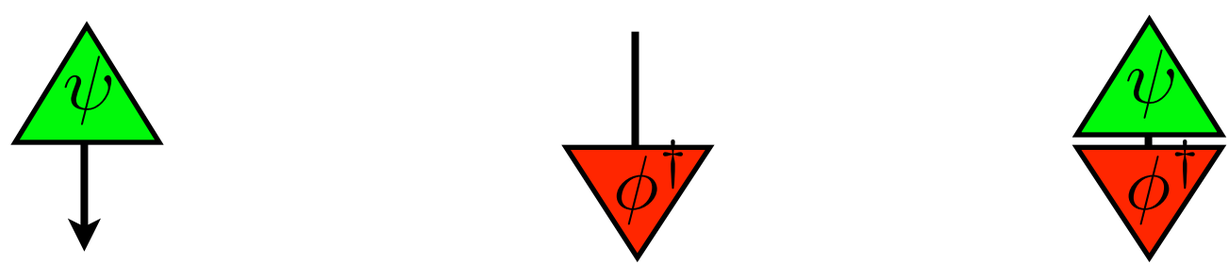
Monoidal categories have a special *unit* object called I which is a left and right identity for the tensor:

$$I \otimes A = A = A \otimes I$$

$$\mathrm{id}_I \otimes f = f = f \otimes \mathrm{id}_I$$

No lines are drawn for I in the graphical notation:

$\psi : I \to A$ $\qquad$ $\phi^\dagger : A \to I$ $\qquad$ $\phi^\dagger \circ \psi : I \to I$



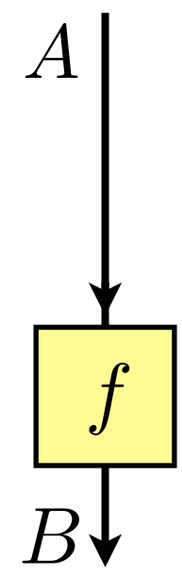
Categories

$$\mathrm{id}_A : A \to A$$

$$\begin{tikzcd} A \arrow[d] \\ \end{tikzcd}$$

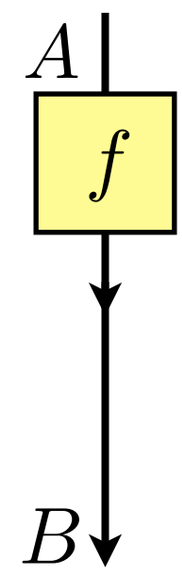
Categories

$$f \circ \mathrm{id}_A : A \to B$$



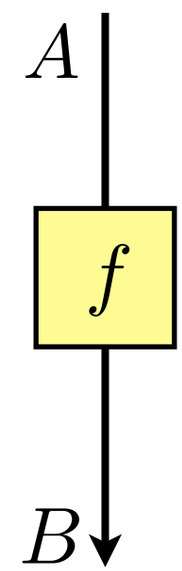
Categories

$$\mathrm{id}_B \circ f : A \to B$$



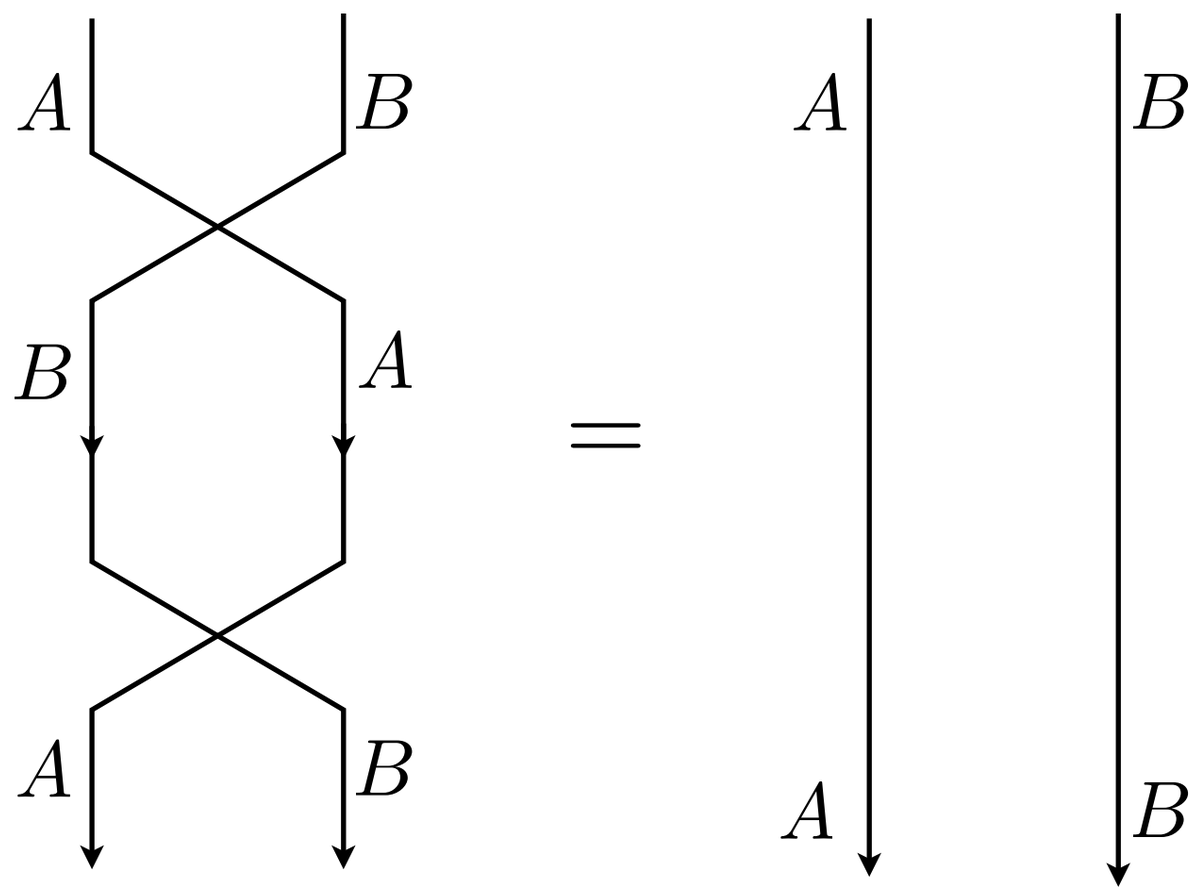
Categories

$$f : A \to B$$



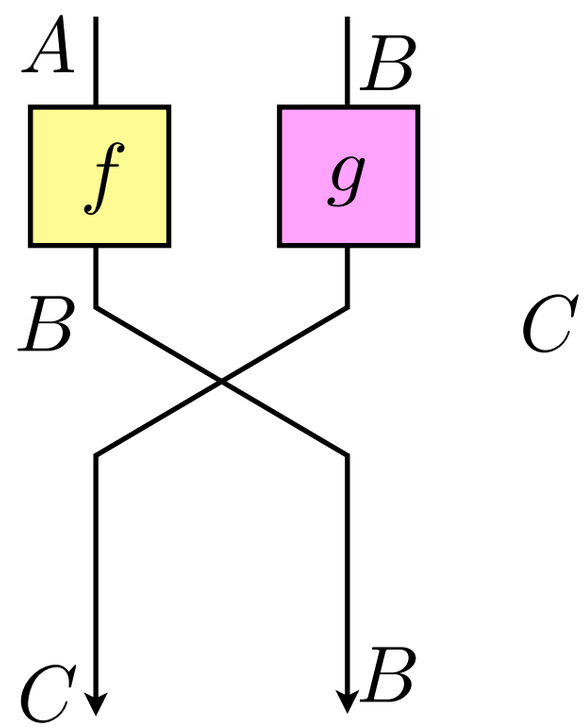
Symmetric Monoidal Categories

$$\sigma_{A,B} : A \otimes B \to B \otimes A$$



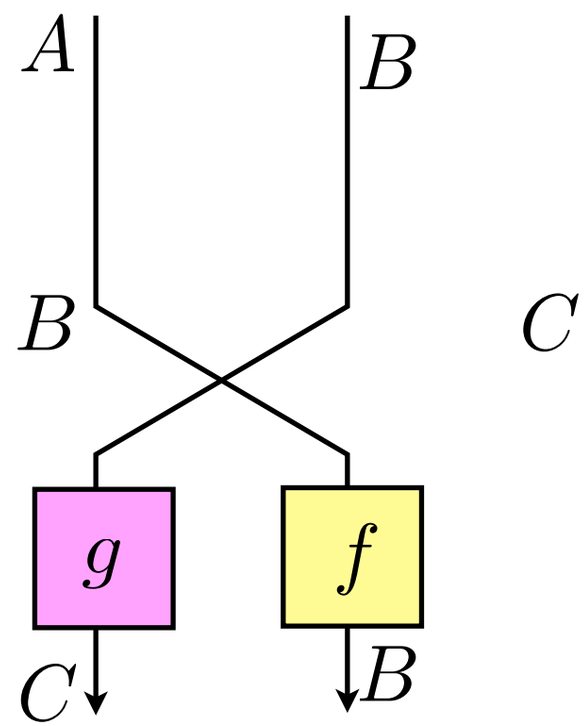
Symmetric Monoidal Categories

$$\sigma_{A,B} : A \otimes B \to B \otimes A$$



Symmetric Monoidal Categories

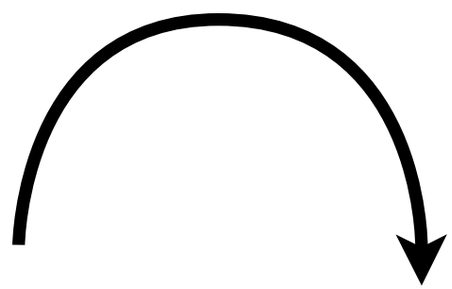
$$\sigma_{A,B} : A \otimes B \to B \otimes A$$

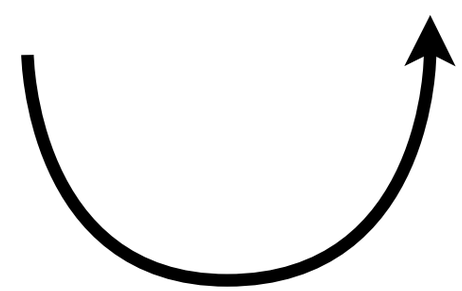


Compact Closure

A symmetric monoidal category is called *compact* if, for every object A, there exists a *dual* object $A*$ and arrows:

$$d : I \to A^* \otimes A \qquad\qquad e : A \otimes A^* \to I$$

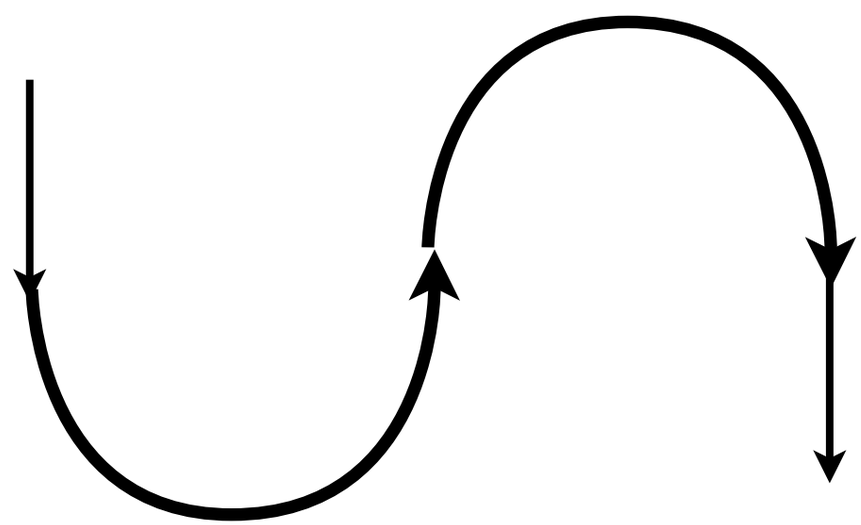




Compact Closure

A symmetric monoidal category is called *compact* if, for every object A, there exists a *dual* object $A*$ and arrows:

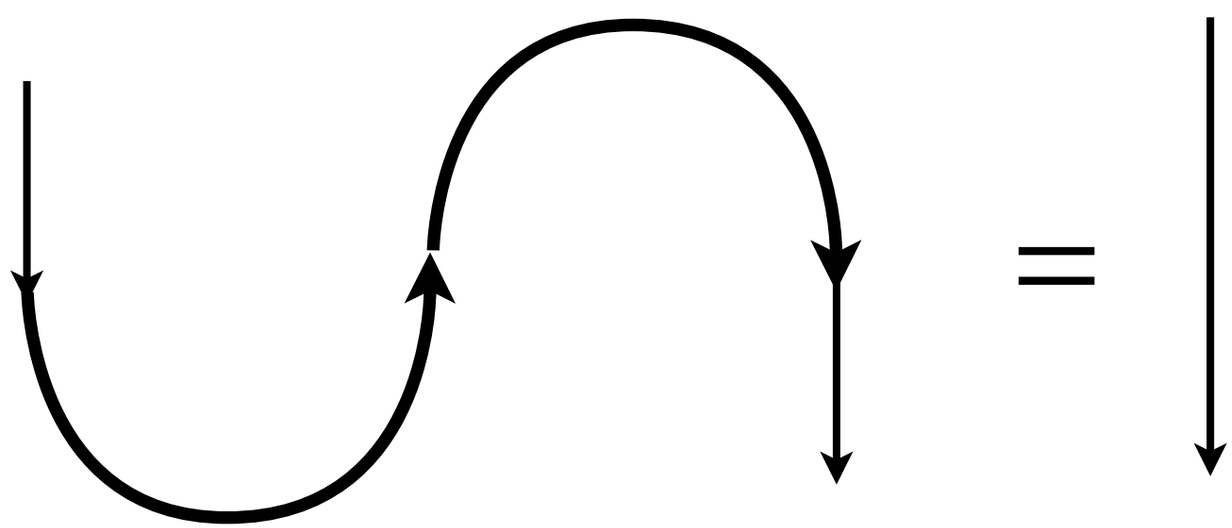
$$d : I \to A^* \otimes A \qquad\qquad e : A \otimes A^* \to I$$



Compact Closure

A symmetric monoidal category is called *compact* if, for every object A, there exists a *dual* object $A*$ and arrows:

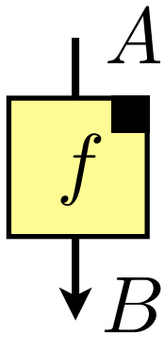
$$d : I \to A^* \otimes A \qquad\qquad e : A \otimes A^* \to I$$

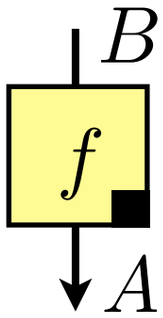


†-Categories

A category is a *†-category* if it is equipped with an involutive functor, $(\cdot)^\dagger$ which reverses the arrows while leaving the objects unchanged.

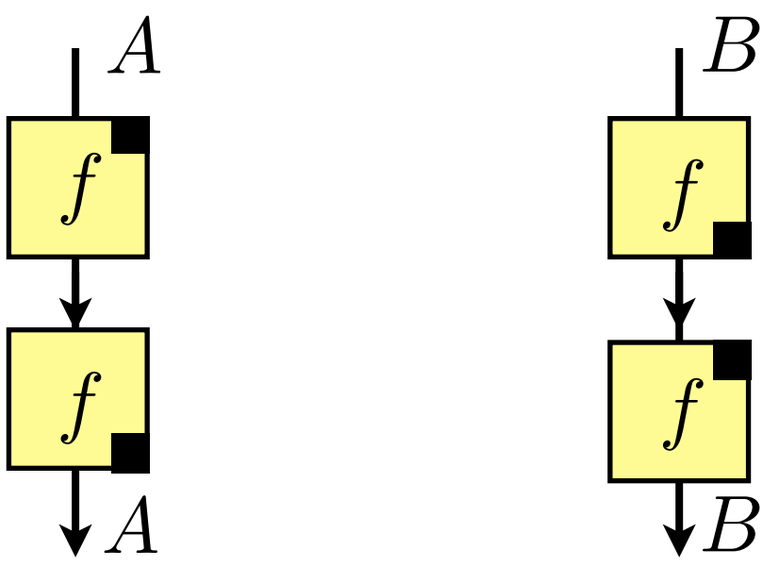
$$f : A \to B \qquad\qquad f^\dagger : B \to A$$





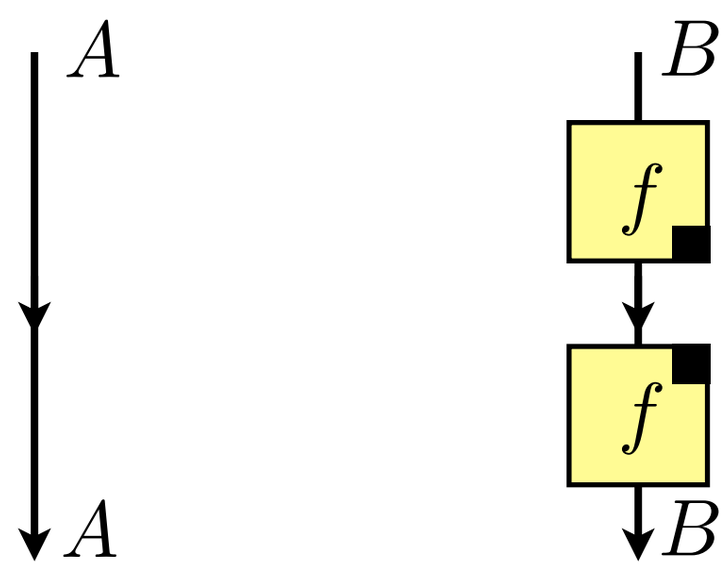
†-Categories

An arrow $f : A \to B$ is called *unitary* when:



†-Categories

An arrow $f : A \to B$ is called *unitary* when:



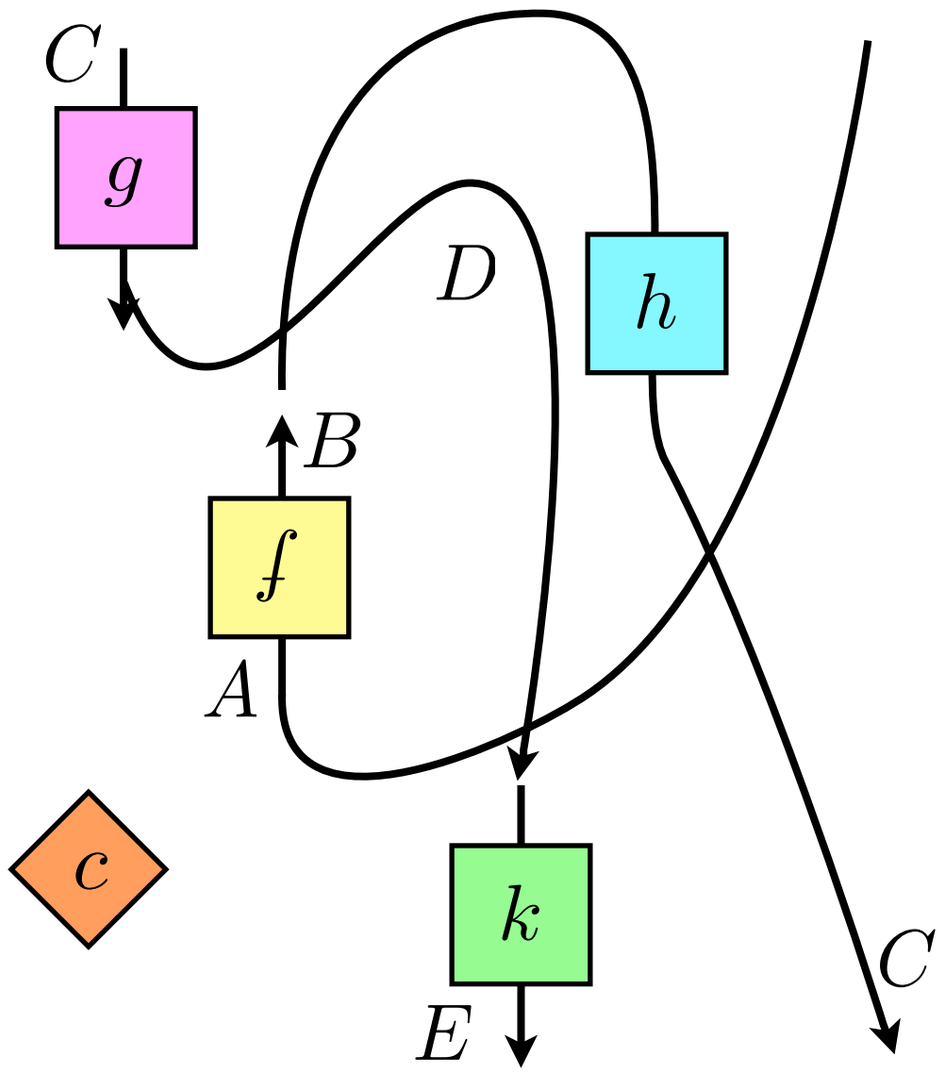
†-Categories

An arrow $f : A \to B$ is called *unitary* when:

$$\begin{tikzcd} A \arrow[d] & B \arrow[d] \\ A & B \end{tikzcd}$$

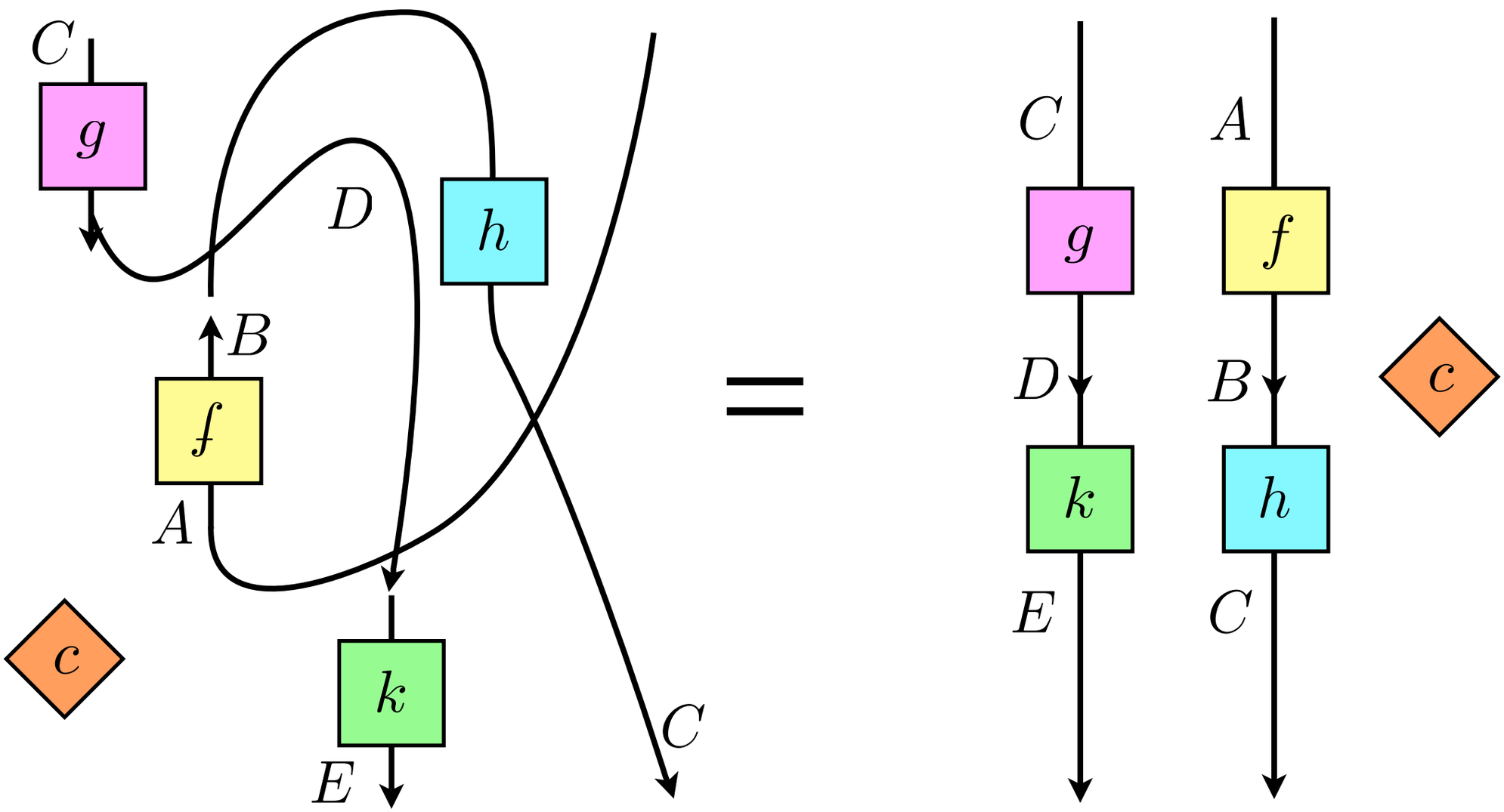
Graphical Calculus Theorem

<u>Thm</u>: one diagram can be deformed to another iff their denotations are equal by the structural equations of the category.



Graphical Calculus Theorem

<u>Thm</u>: one diagram can be deformed to another iff their denotations are equal by the structural equations of the category.



The Category $\mathbf{FDHilb}$

$\mathbf{FDHilb}$ is the category of finite dimensional complex Hilbert spaces. It is †-monoidal with the following structure.

- Objects: finite dimensional Hilbert spaces, A, B, C etc
- Arrows: all linear maps
- Tensor: usual (Kronecker) tensor product; $I = \mathbb{C}$
- $f^\dagger$ is the usual adjoint (conjugate transpose)

A linear map $\psi : I \to A$ picks out exactly one vector. It is a ket and $\psi^\dagger : A \to I$ is the corresponding bra.

Hence $\psi^\dagger \circ \phi : I \to I$ is the inner product $\langle \psi \mid \phi \rangle$.

2.

Quantum Theory in 5 minutes

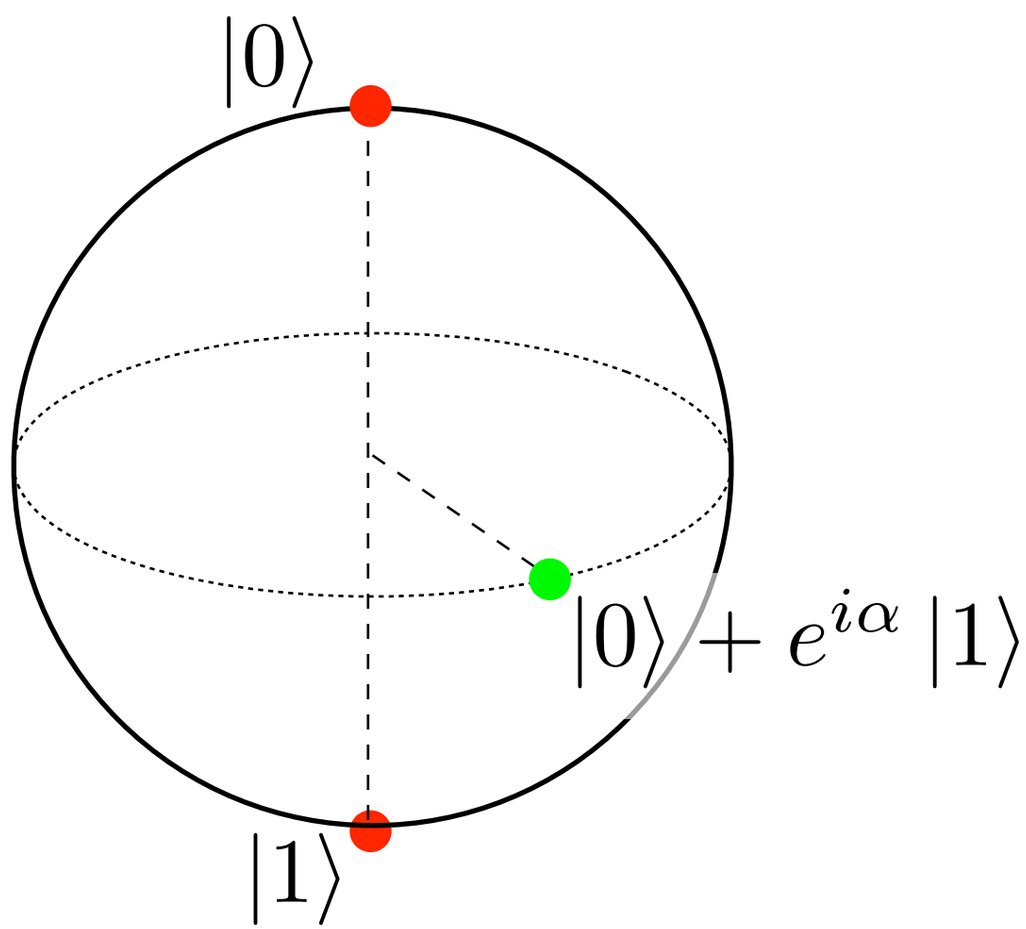
2.

Quantum Theory in 5* minutes

*Might be more than 5

1. Quantum states are represented by **unit vectors** in a complex Hilbert space.

$$|0\rangle\,, |1\rangle\,, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \in \mathbb{C}^2 \;=:\; \mathcal{Q}$$



2. The state space formed by combining two or more systems is the **tensor** product of their individual state spaces

$$|010\rangle := |0\rangle \otimes |1\rangle \otimes |0\rangle \ \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \ = \ \mathcal{Q}^3$$

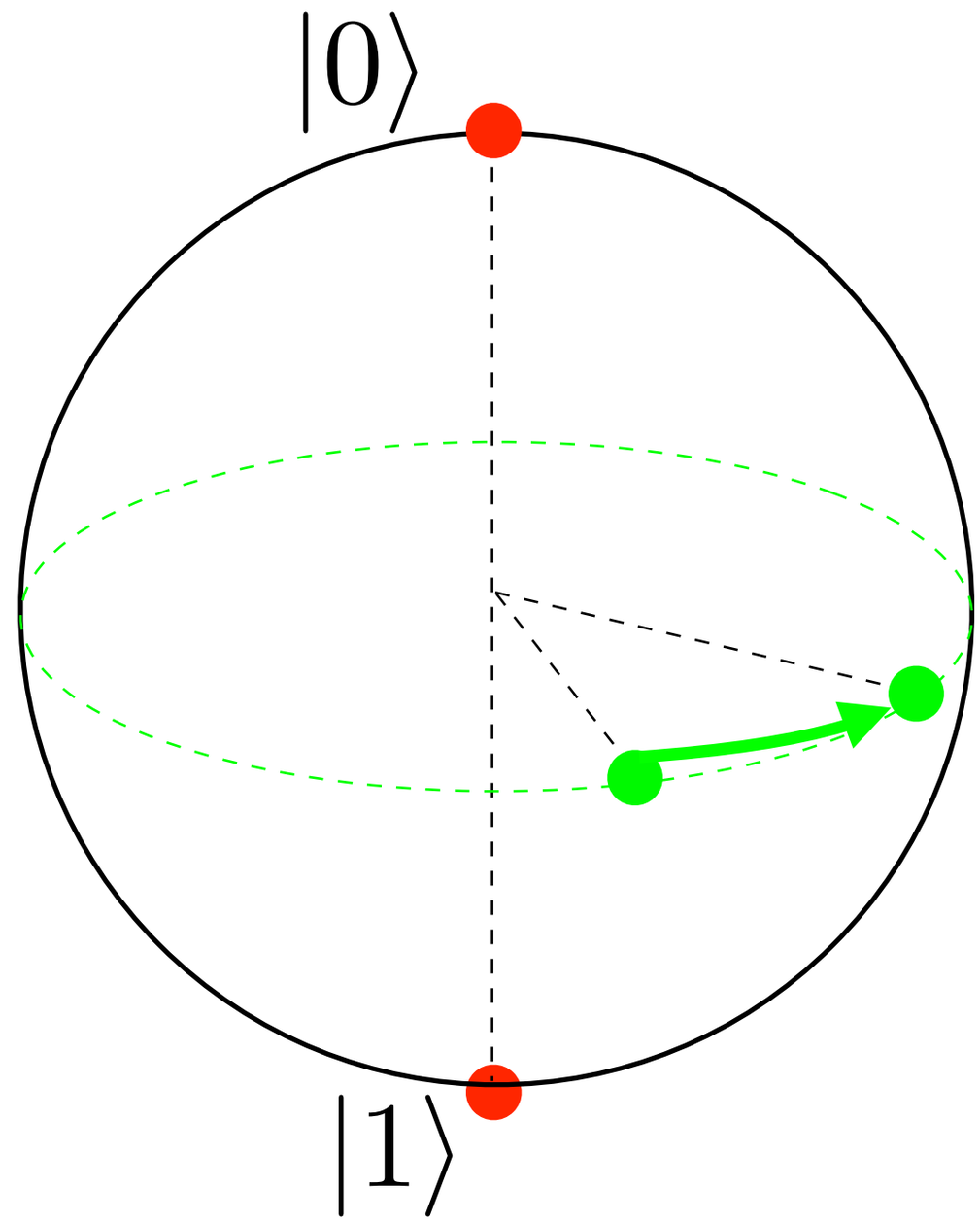
3. For each discrete time step, an undisturbed quantum system evolves according to a **unitary** operator acting on its state space

$$X, Z, H : \mathcal{Q} \to \mathcal{Q} \qquad \wedge X, \wedge Z : Q^2 \to Q^2$$

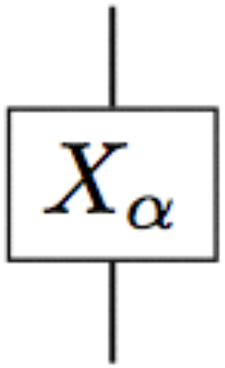
...**but** the quantum state is not directly accessible... more on this later!

Example: Z-Rotation

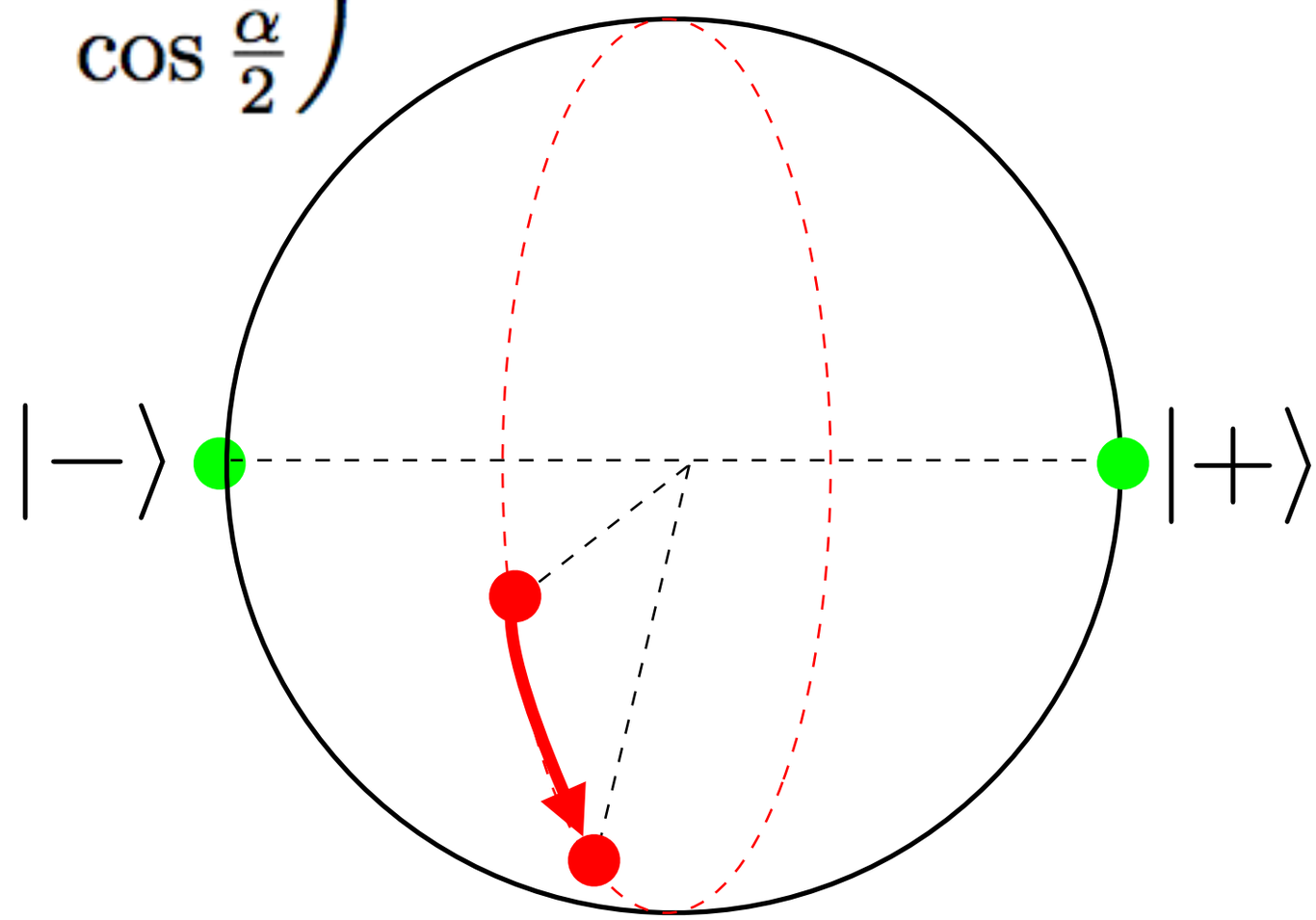
$$= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}$$



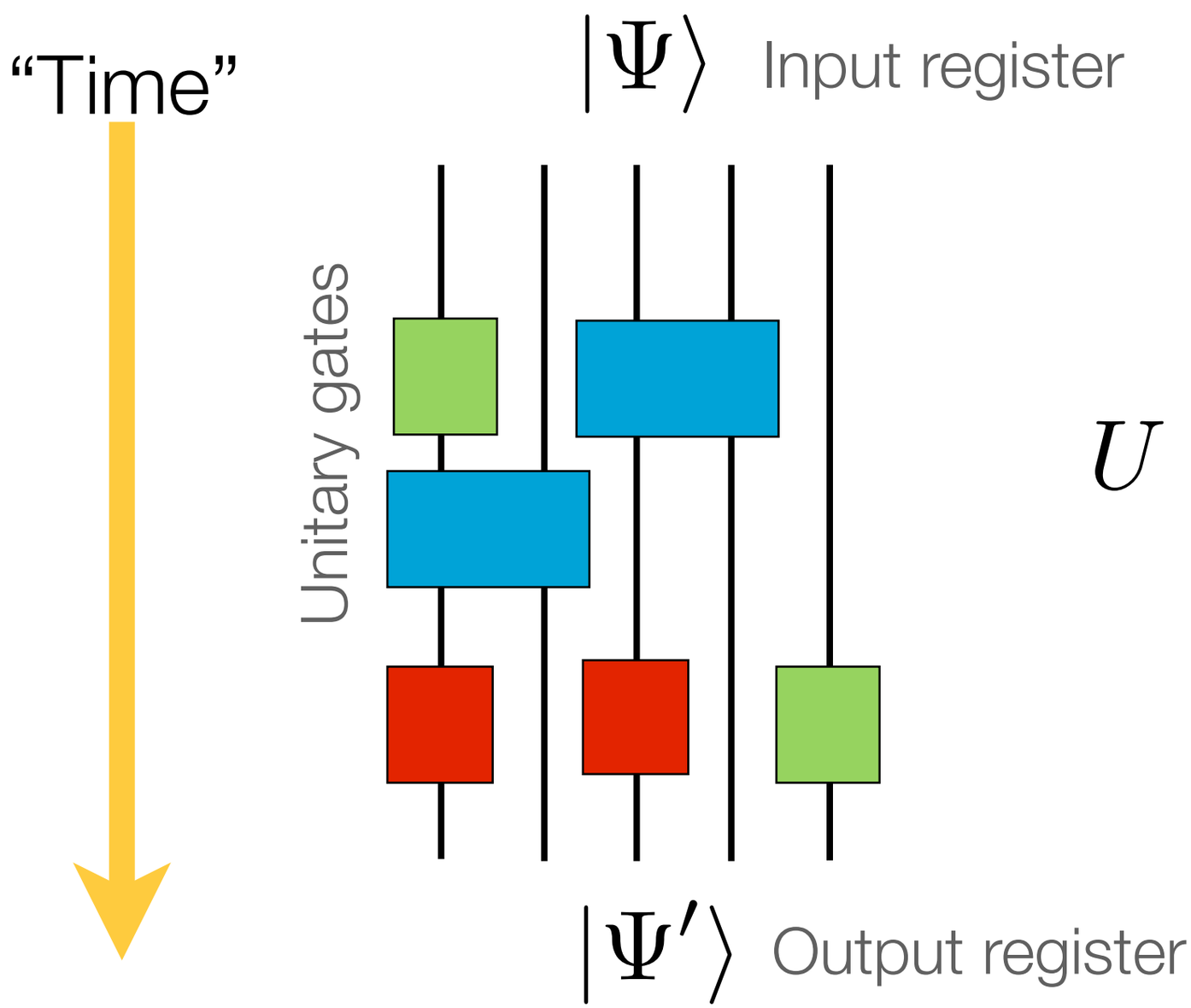
Example: X-Rotation



$$= \begin{pmatrix} \cos\frac{\alpha}{2} & -i\sin\frac{\alpha}{2} \\ -i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$$



Quantum Circuits

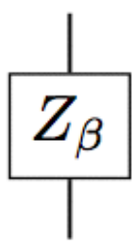


$$U : \mathbb{C}^{2^n} \longrightarrow \mathbb{C}^{2^n}$$

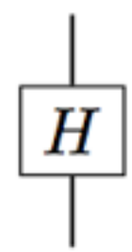
Universality

We say that a model of quantum computation is **universal** if it can represent all unitary maps.

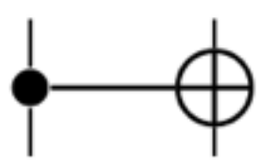
The circuit model requires a small set of gates to be universal:



$$= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}$$



$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

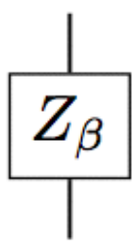


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

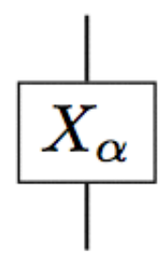
Universality

We say that a model of quantum computation is **universal** if it can represent all unitary maps.

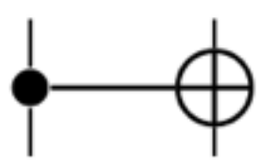
The circuit model requires a small set of gates to be universal:



$$= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}$$

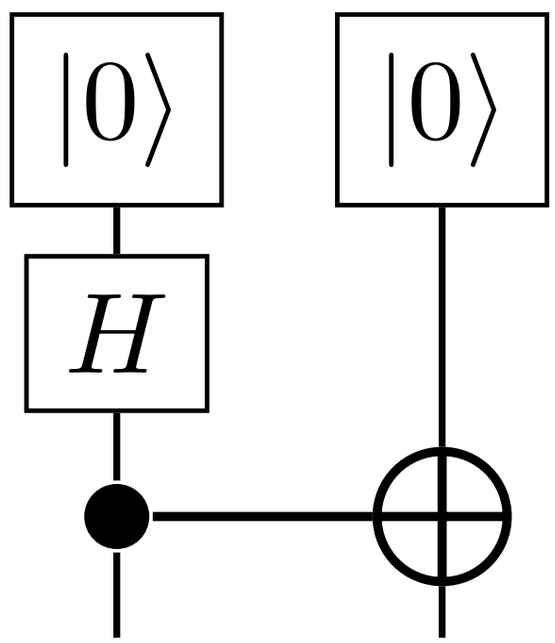


$$= \begin{pmatrix} \cos\frac{\alpha}{2} & -i\sin\frac{\alpha}{2} \\ -i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$$

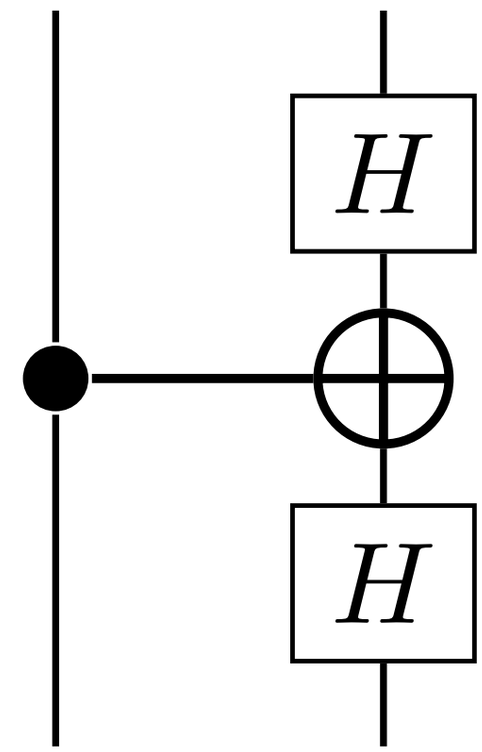


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Quantum Circuits



Preparing a Bell state



Controlled-Z gate

Quantum Observables

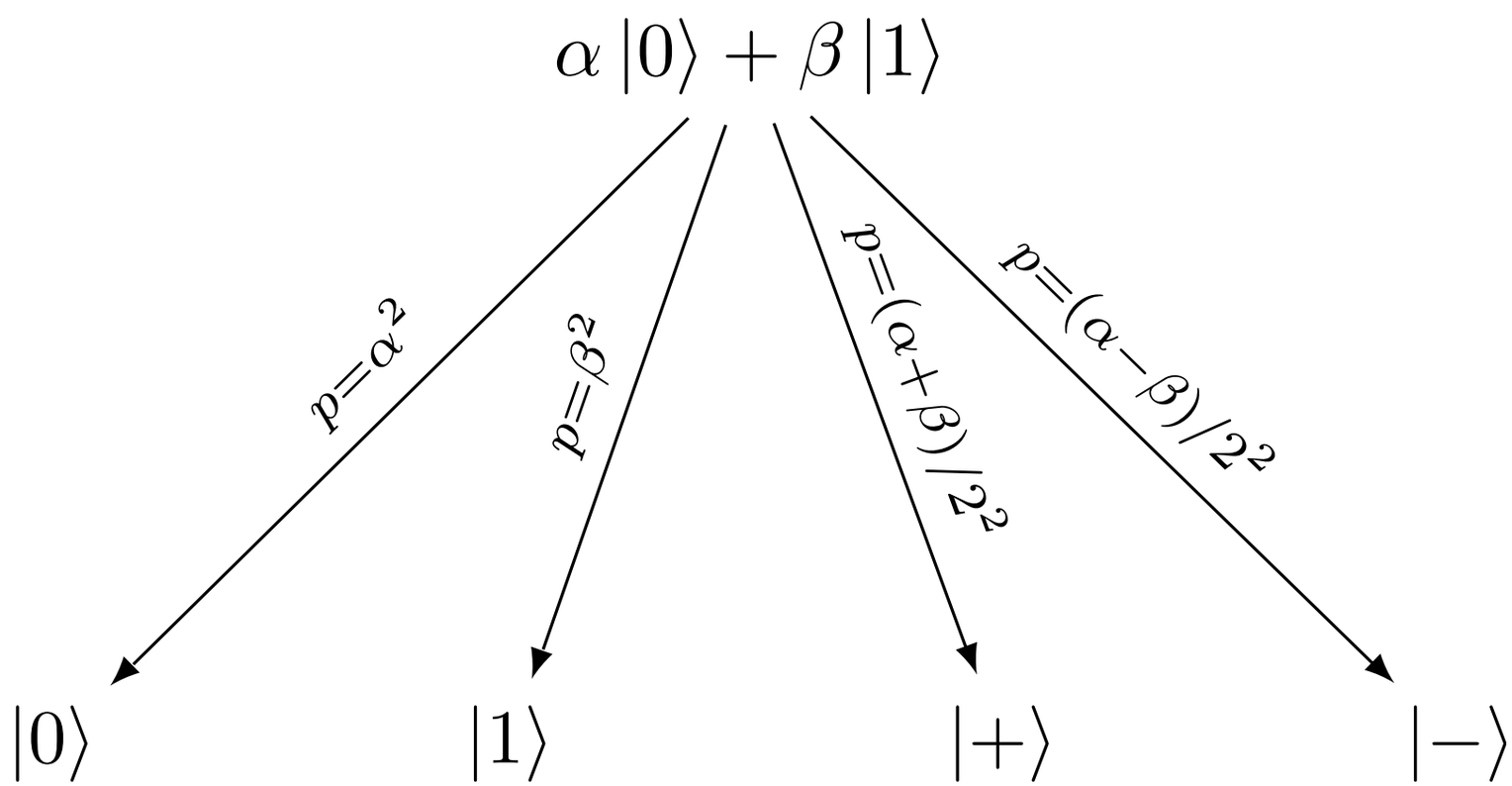
4. Each observable quantity O is represented as self-adjoint operator $\hat{O} = \sum_i \lambda_i \left| e_i \right\rangle \left\langle e_i \right|$:

- The possible values of O are the eigenvalues λ_i of $\hat{O}$
- When we observe O for a system in state $|\psi\rangle$, there is probability $\langle e_i \mid \psi \rangle^2$ of observing λ_i.
- If λ_i is the outcome of the measurement, the system is then in state $|e_i\rangle$.

X and Z Spins

We can measure the spin of qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

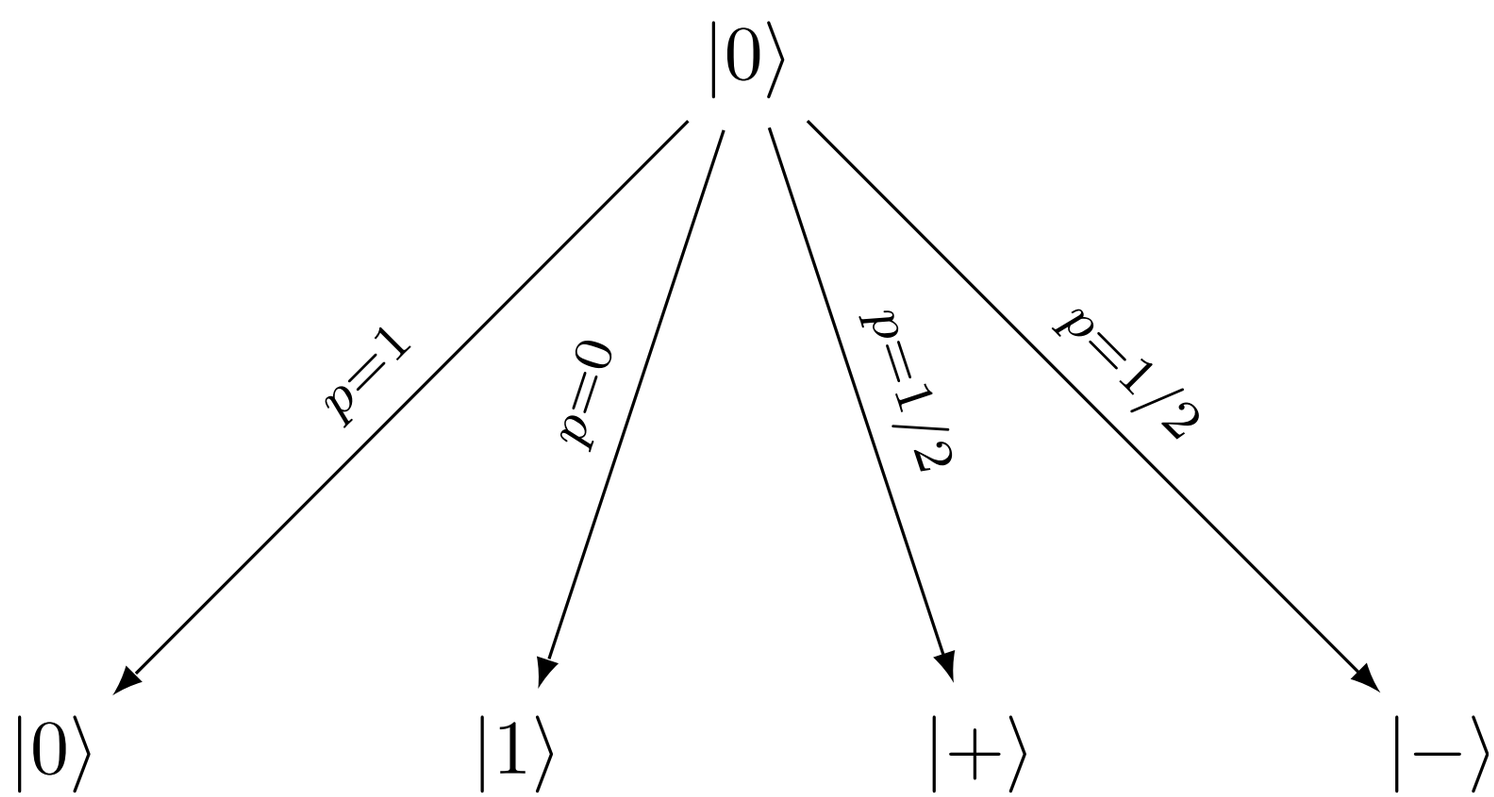
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



X and Z Spins

We can measure the spin of qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



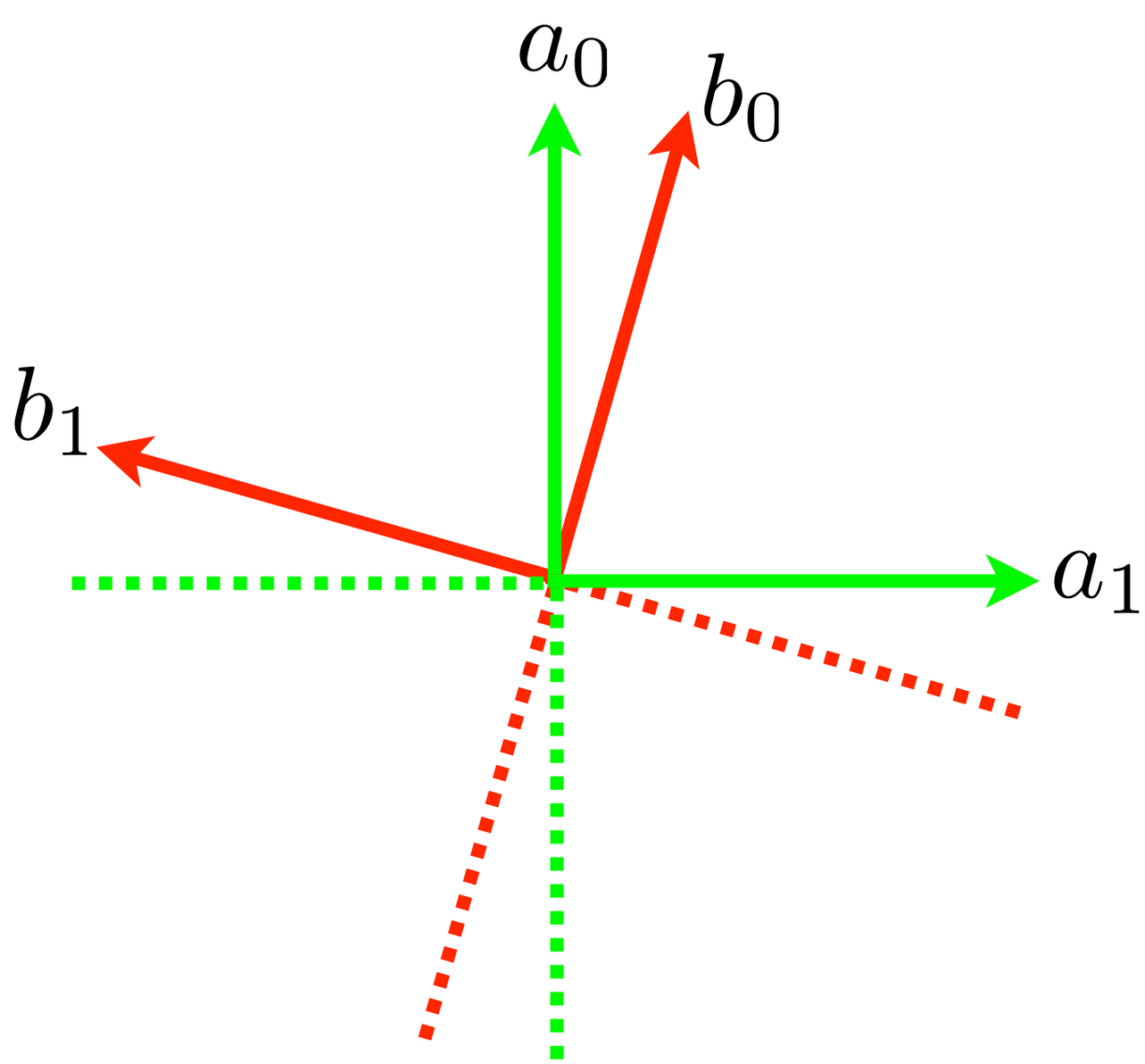
Quantum Observables

Measuring A then B may give a different answer than measuring B first then A!

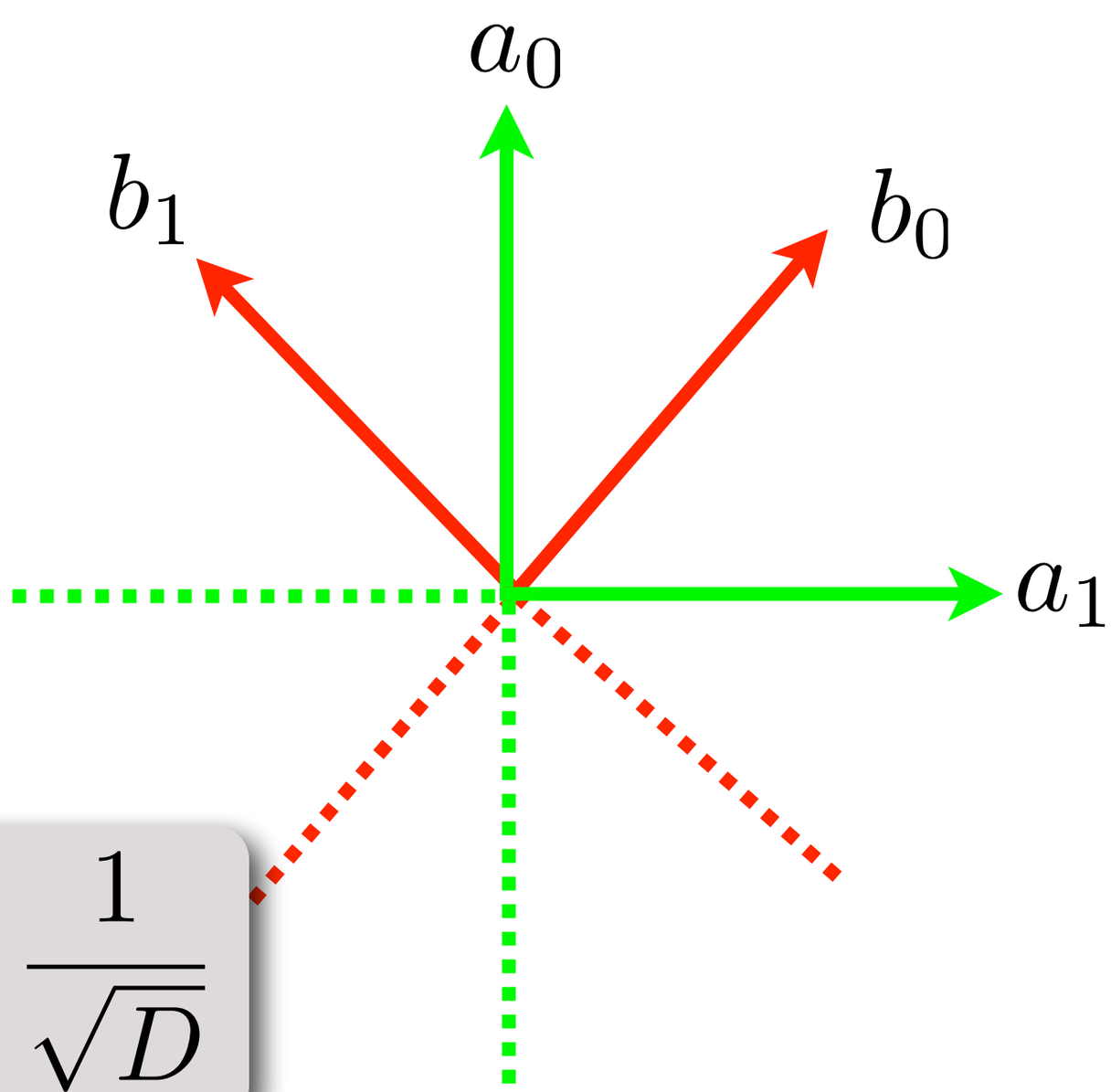
Not all observables are well defined at the same time:

- Two observables are compatible if their operators commute
- Two operators commute if they have the same eigenvectors
- Identify a non-degenerate observable with its **eigenbasis**

Incompatible Observables

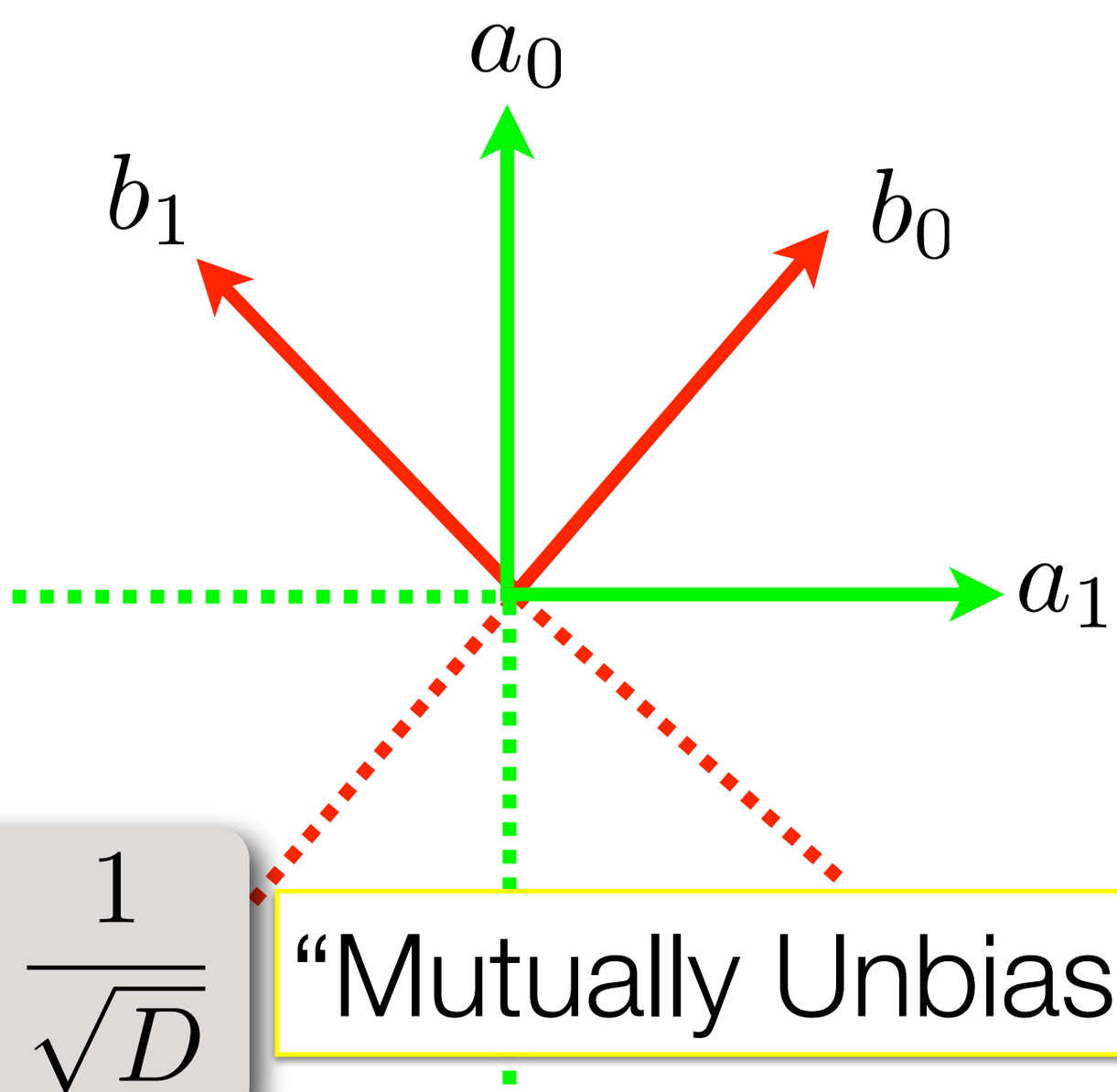


Complementary Observables



$$|\langle a_i \mid b_j \rangle| = \frac{1}{\sqrt{D}}$$

Complementary Observables



$$|\langle a_i \mid b_j \rangle| = \frac{1}{\sqrt{D}}$$

"Mutually Unbiased Bases"

3.

Categorical Quantum Mechanics

No-Cloning and No-Deleting

<u>Theorem</u>: There are no unitary operations D such that

$$D : |\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$$
$$D : |\phi\rangle \mapsto |\phi\rangle \otimes |\phi\rangle$$

unless $|\psi\rangle$and $|\phi\rangle$ are orthogonal [Wooters & Zurek 1982]

<u>Theorem</u>: There are no unitary operations E such that

$$E : |\psi\rangle \mapsto |0\rangle$$
$$E : |\phi\rangle \mapsto |0\rangle$$

unless $|\psi\rangle$and $|\phi\rangle$ are orthogonal [Pati & Braunstein 2000]

“Classical” Quantum States

When can a quantum state be treated as if classical?

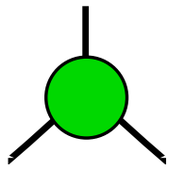
- no-go theorems allow copying and deleting of *orthogonal* states;

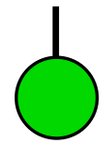
In other words:

- A quantum state may be copied and deleted if it is an eigenstate of some *known observable.*

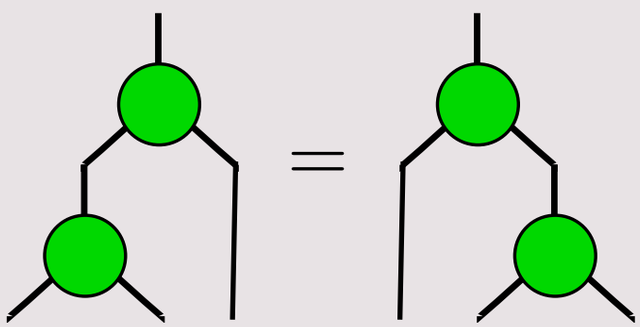
We’ll use this property to formalise *observables* in terms of *copying* and *deleting* operations.

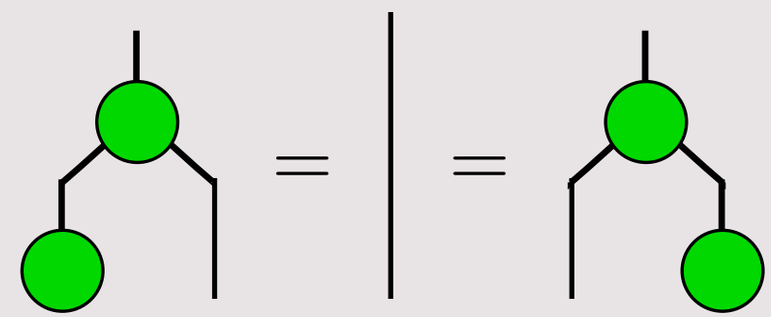
Observables

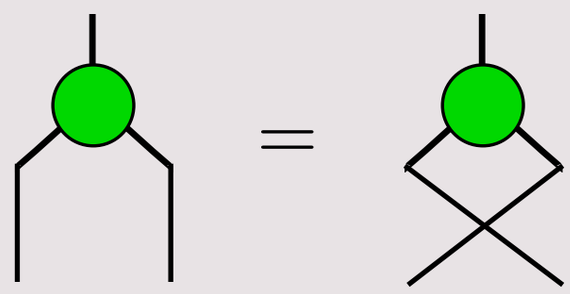
$\delta =$ 

$\epsilon =$ 

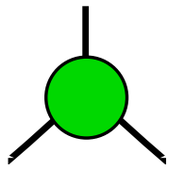
Comonoid Laws

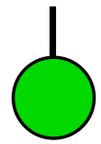


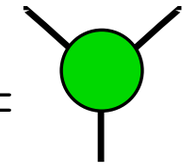


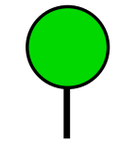


Observables

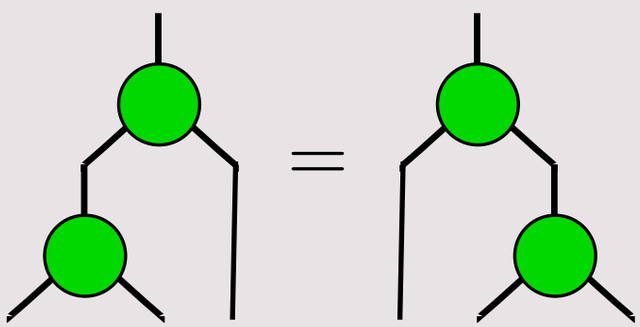
$\delta =$ 

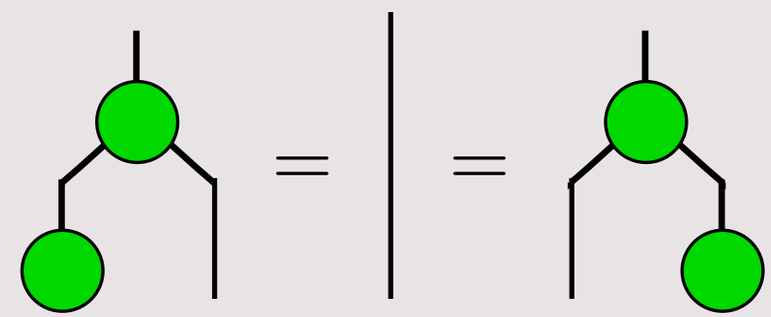
$\epsilon =$ 

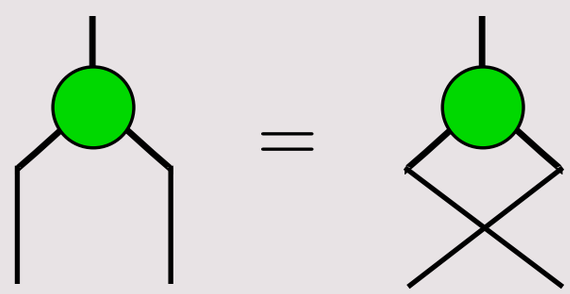
$\delta^\dagger =$ 

$\epsilon^\dagger =$ 

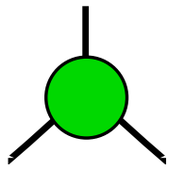
Comonoid Laws

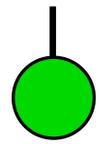


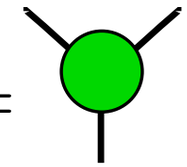


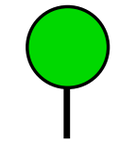


Observables

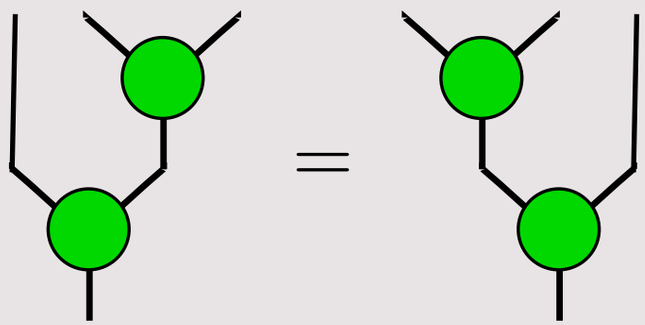
$\delta =$ 

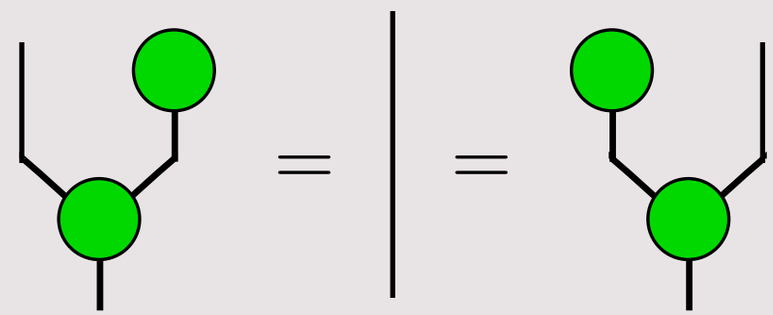
$\epsilon =$ 

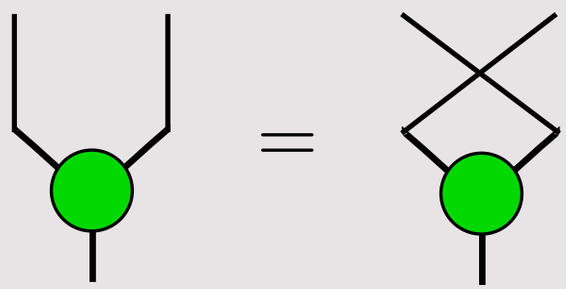
$\delta^\dagger =$ 

$\epsilon^\dagger =$ 

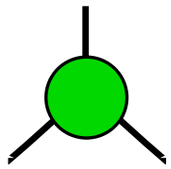
Monoid Laws

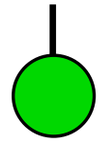


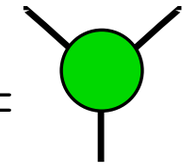


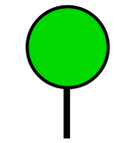


Observables

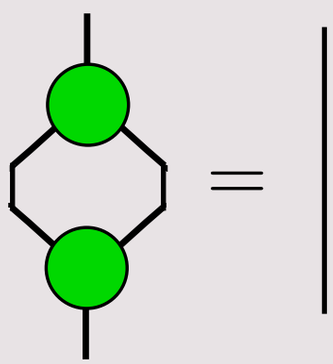
$\delta =$ 

$\epsilon =$ 

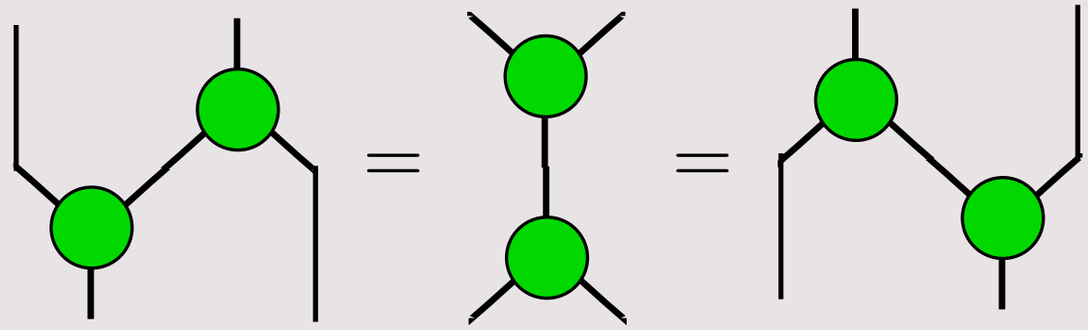
$\delta^\dagger =$ 

$\epsilon^\dagger =$ 

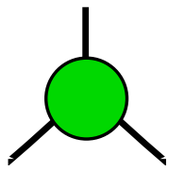
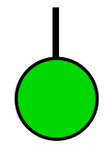
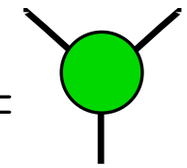
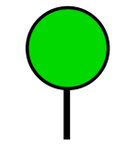
Isometry Law



Frobenius Law



Observables

$\delta =$  $\epsilon =$  $\delta^\dagger =$  $\epsilon^\dagger =$ 

In other words: an observable is a *special commutative †-Frobenius algebra*

Observables

Given any finite dimensional Hilbert space we can define a Frobenius algebra by

$$\delta : A \to A \otimes A :: a_i \mapsto a_i \otimes a_i$$

$$\epsilon : A \to I :: \sum_i a_i \mapsto 1$$

Observables

Given any finite dimensional Hilbert space we can define a Frobenius algebra by

$$\delta : A \to A \otimes A :: a_i \mapsto a_i \otimes a_i$$
$$\epsilon : A \to I :: \sum_i a_i \mapsto 1$$

<u>Example</u>: $\delta : \begin{array}{l} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{array}$ $\epsilon : |0\rangle + |1\rangle \mapsto 1$

define a Frobenius algebra over qubits; the standard basis is copied and erased.

Observables

Given any finite dimensional Hilbert space we can define a Frobenius algebra by

$$\delta : A \to A \otimes A :: a_i \mapsto a_i \otimes a_i$$
$$\epsilon : A \to I :: \sum_i a_i \mapsto 1$$

<u>Example</u>: $\delta : \begin{array}{l} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle \end{array}$ $\qquad \epsilon : |0\rangle + |1\rangle \mapsto 1$

define a Frobenius algebra over qubits; the standard basis is copied and erased.

<u>Theorem</u>: in $\mathbf{FDHilb}$, †-SCFAs are in bijective correspondence to bases. [Coecke, Pavlovic, Vicary]

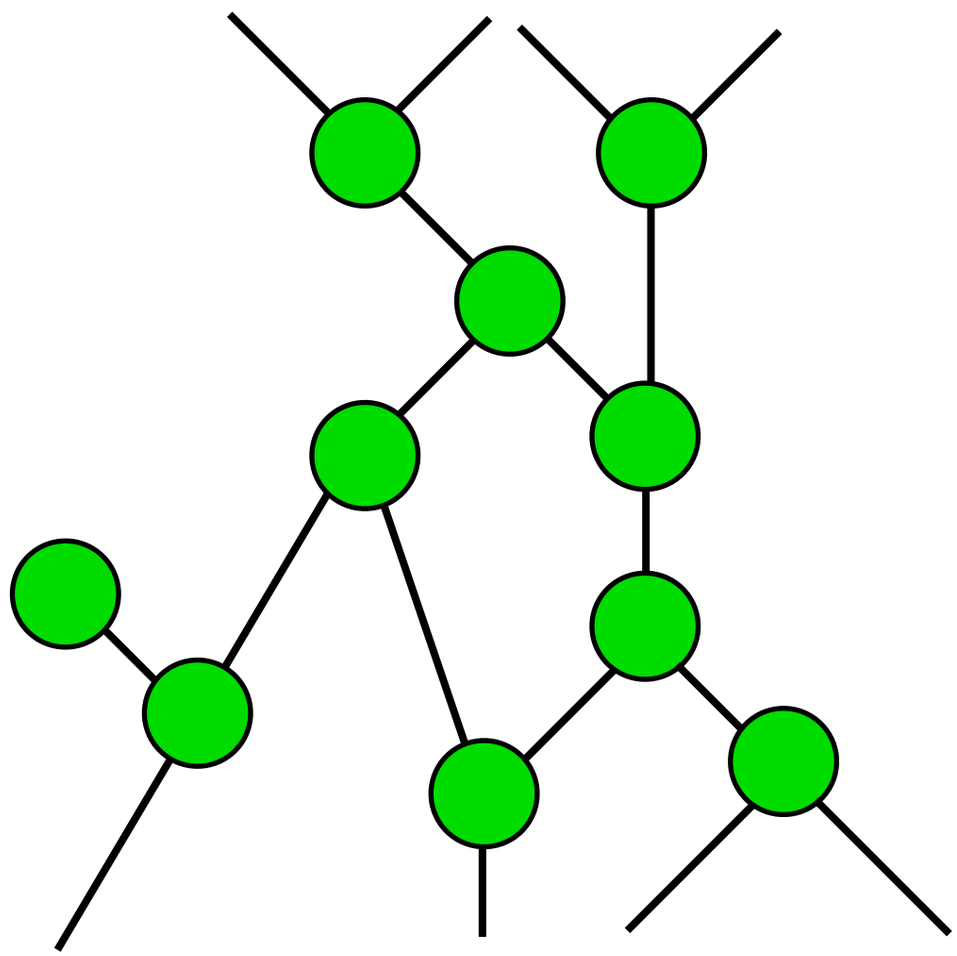
Spider Theorem

<u>Theorem</u>: any maps constructed from δ and ε , and their adjoints, whose graph is connected, is determined uniquely by the number of inputs and outputs.

Coecke & Paquette 2006

Spider Theorem

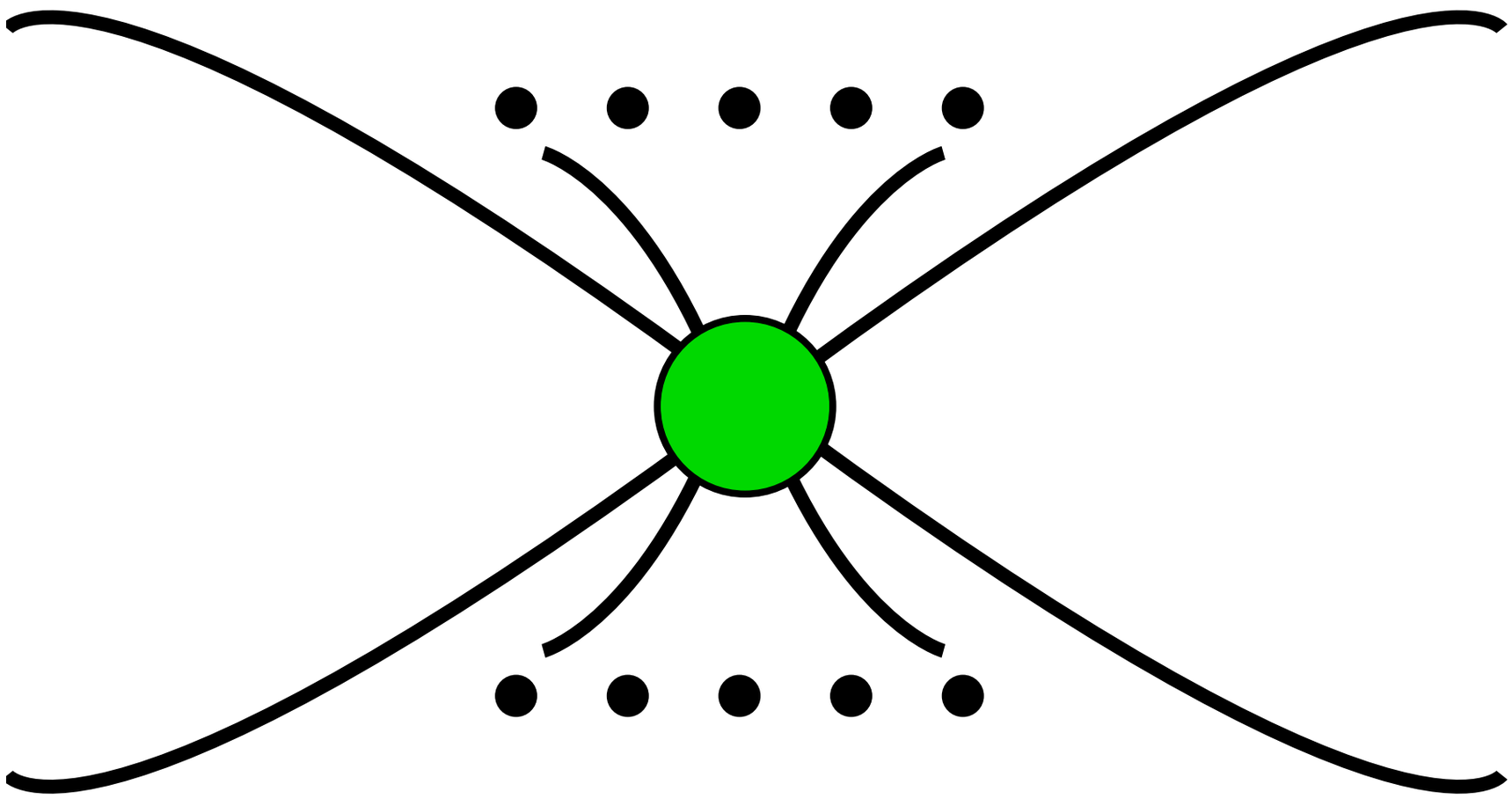
<u>Theorem</u>: any maps constructed from δ and ε , and their adjoints, whose graph is connected, is determined uniquely by the number of inputs and outputs.



Coecke & Paquette 2006

Spider Theorem

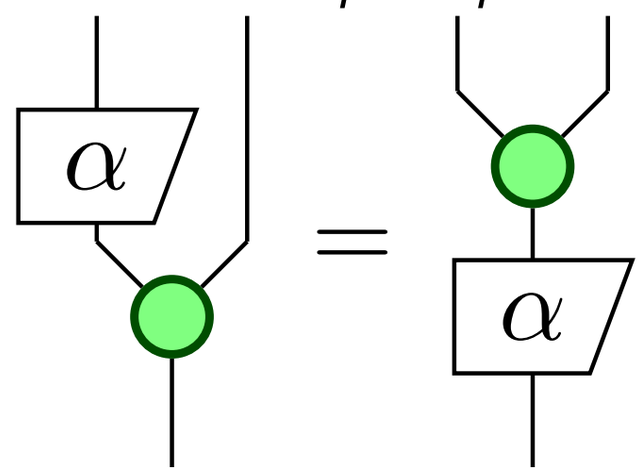
<u>Theorem</u>: any maps constructed from δ and ε , and their adjoints, whose graph is connected, is determined uniquely by the number of inputs and outputs.



Coecke & Paquette 2006

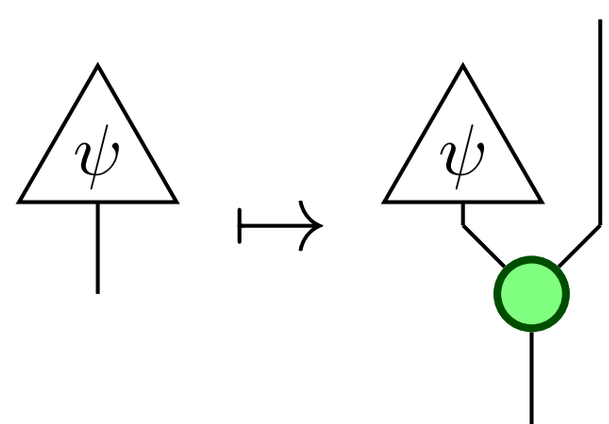
Phases

Defn. a map $\alpha : A \longrightarrow A$ is called a *pre-phase* if:



A pre-phase is a *phase* if it is unitary.

Defn: a point $\psi : I \longrightarrow A$ is called *unbiased* if the map



is a phase.

$$\Lambda(\psi) : \psi \mapsto \mu \circ (\psi \otimes \mathrm{id})$$

Phases

Lemma. let $\alpha : A \longrightarrow A$ be a phase; then there exists an unbiased point $\psi : I \longrightarrow A$ such that:

$$
\begin{aligned}
&1.\ \alpha = \Lambda(\psi);\\
&2.\ \alpha^{\circ} = \alpha;\\
&3.\ \alpha^{\dagger} = \Lambda(\psi_{\circ});\\
&4.\ \mu(\psi \otimes \psi_{\circ}) = \eta.
\end{aligned}
$$

Corollary: α is a phase iff $\alpha^{\dagger}$ is a phase.

Phases

Lemma. let $\alpha : A \longrightarrow A$ be a phase; then there exists an unbi

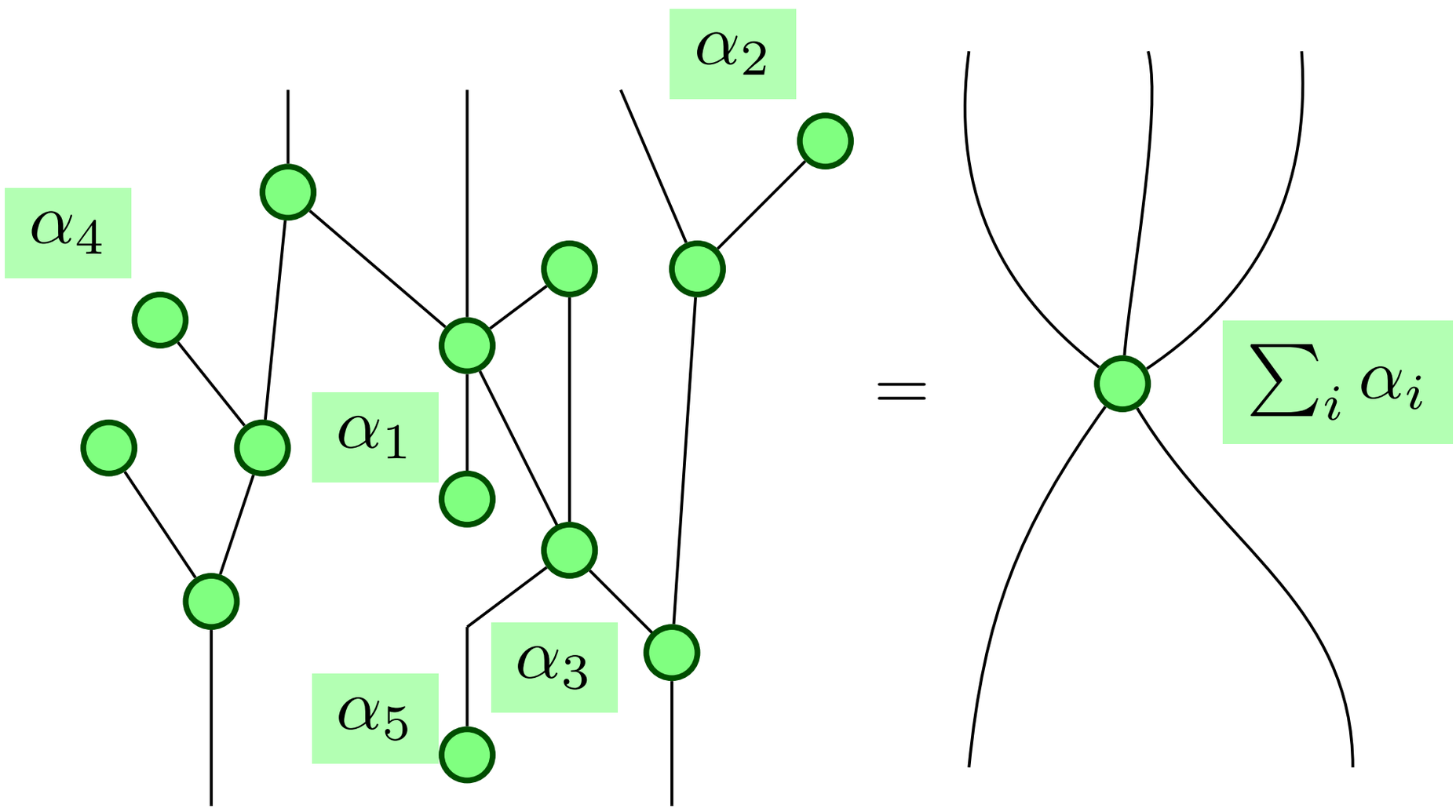
Proposition 6:
1. The phases are an abelian group
2. The unbiased points are an abelian group
3. They're isomorphic

$$3.\ \alpha^\dagger = \Lambda(\psi_{\bullet});$$
$$4.\ \mu(\psi \otimes \psi_{\bullet}) = \eta.$$

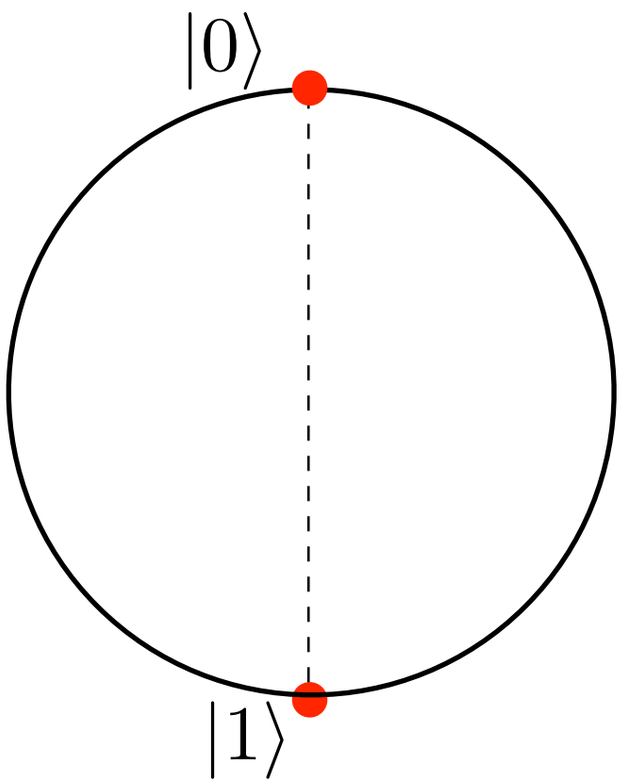
Corollary: α is a phase iff $\alpha^\dagger$ is a phase.

Generalised Spider

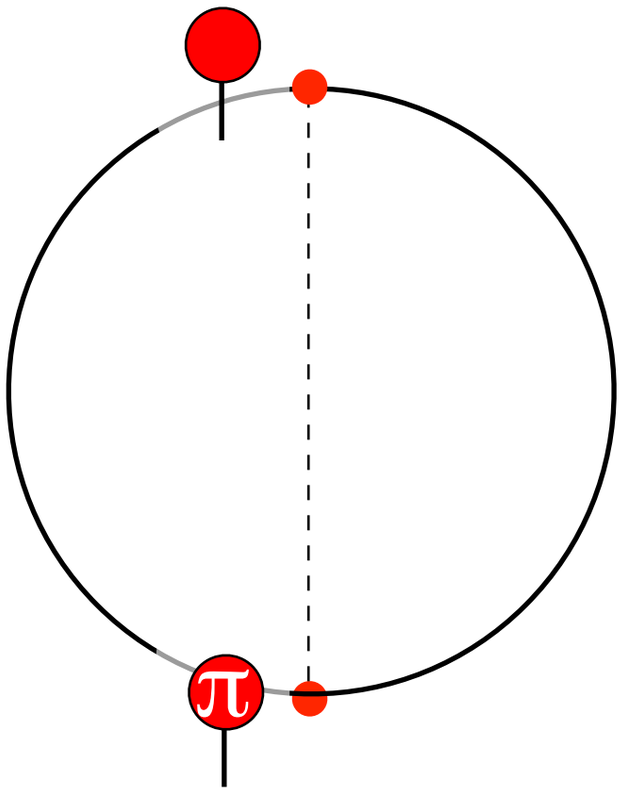
Thm: Any connected monochrome diagram with phases is determined completely by its arity and the sum of its phases.



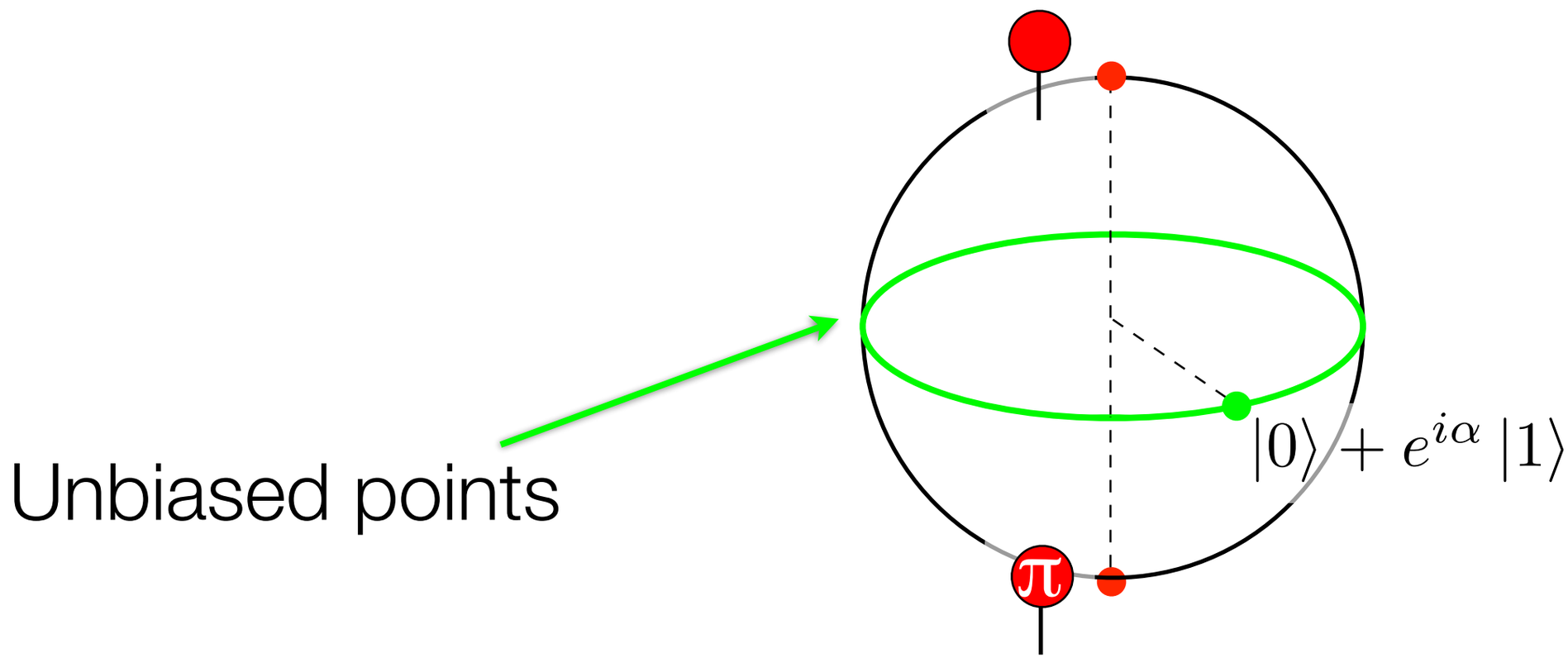
Example: qubits



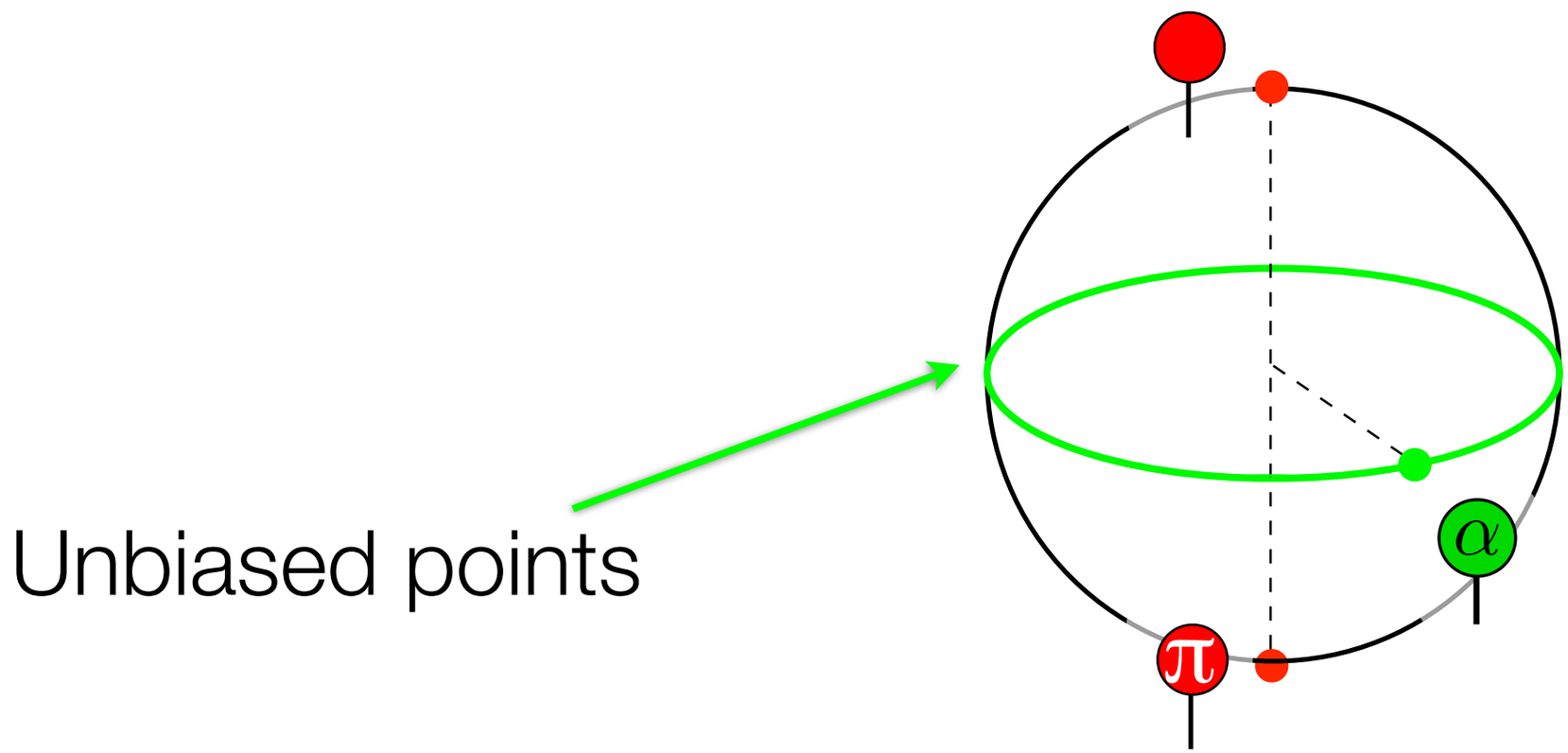
Example: qubits



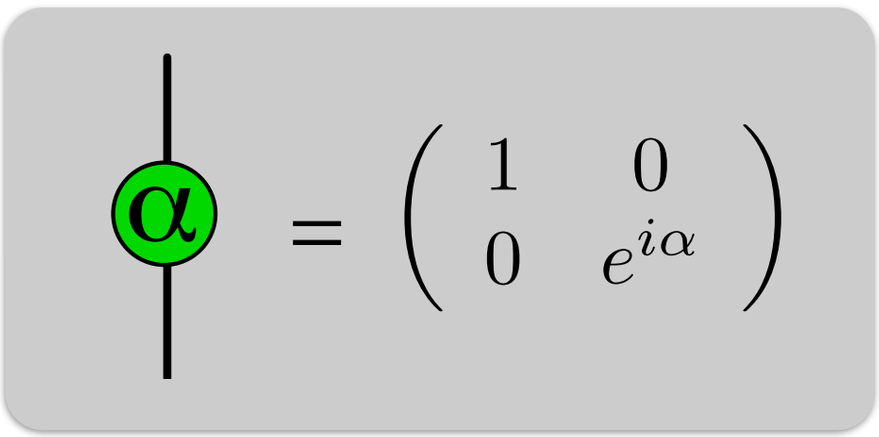
Example: qubits



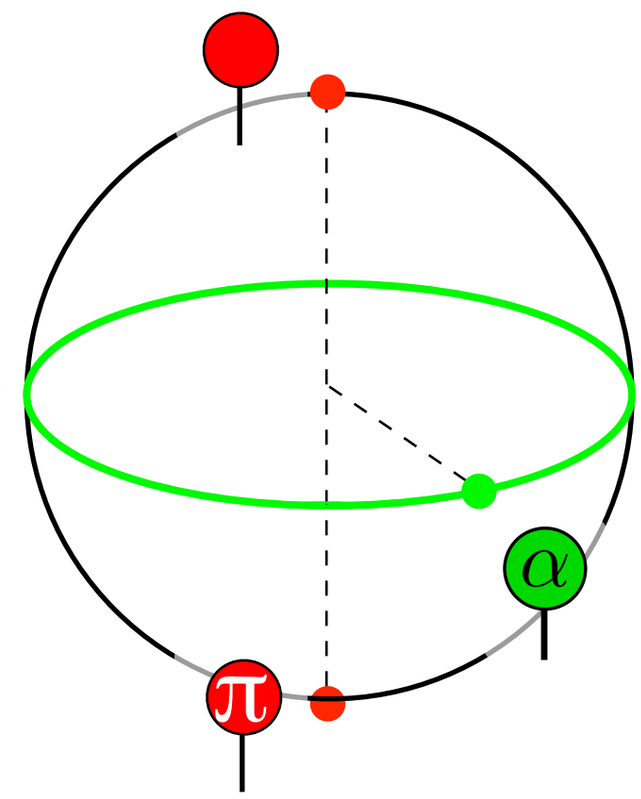
Example: qubits



Example: qubits

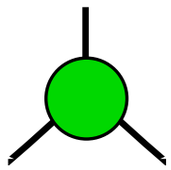


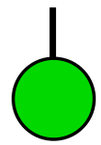
$$= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$

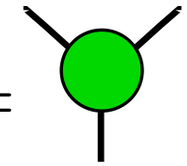


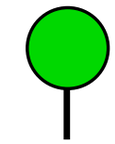
Unbiased points

Two kinds of points

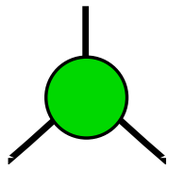
$\delta =$ 

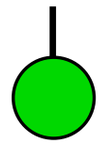
$\epsilon =$ 

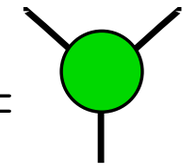
$\delta^\dagger =$ 

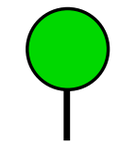
$\epsilon^\dagger =$ 

Two kinds of points

$\delta =$ 

$\epsilon =$ 

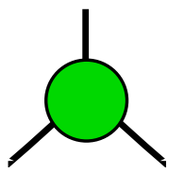
$\delta^\dagger =$ 

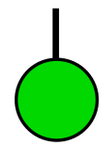
$\epsilon^\dagger =$ 

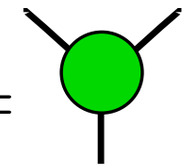
Classical Points

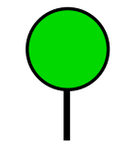
Those points which can be copied by δ

Two kinds of points

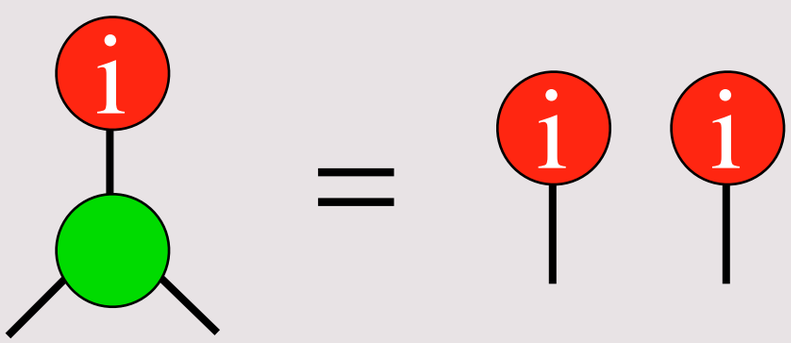
$\delta =$ 

$\epsilon =$ 

$\delta^\dagger =$ 

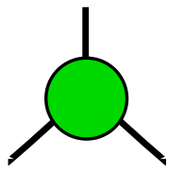
$\epsilon^\dagger =$ 

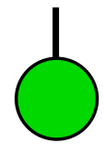
Classical Points

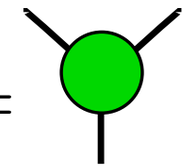


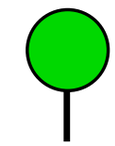
Those points which can be copied by δ

Two kinds of points

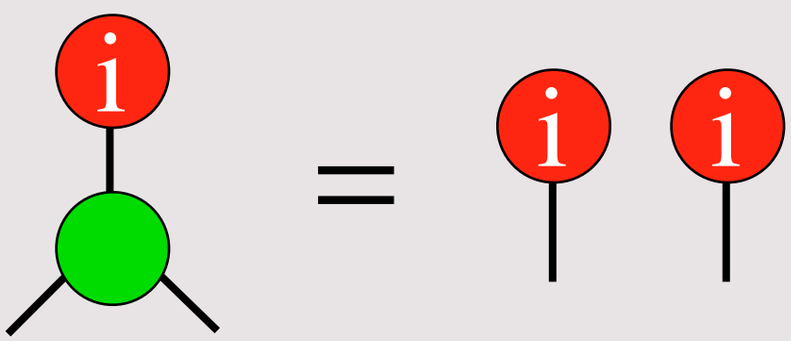
$\delta =$ 

$\epsilon =$ 

$\delta^\dagger =$ 

$\epsilon^\dagger =$ 

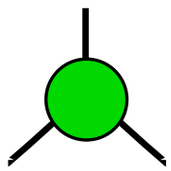
Classical Points

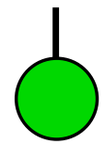


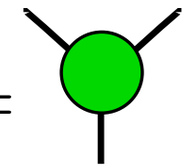
Those points which can be copied by δ

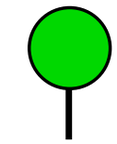
* to keep the pictures tidy, a scalar factor has been omitted (and everywhere from here on)

Two kinds of points

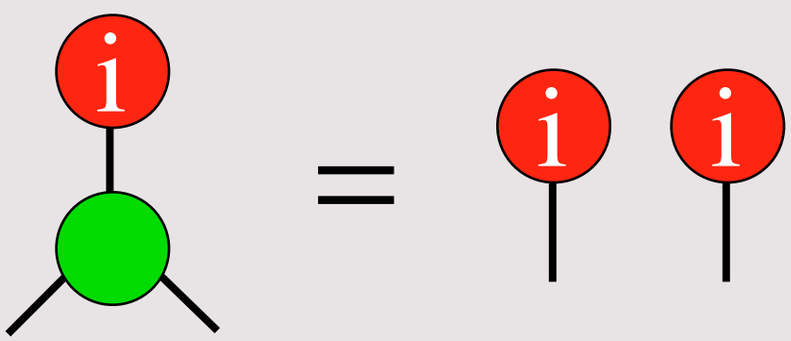
$\delta =$ 

$\epsilon =$ 

$\delta^\dagger =$ 

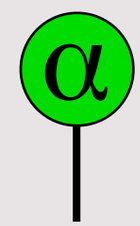
$\epsilon^\dagger =$ 

Classical Points

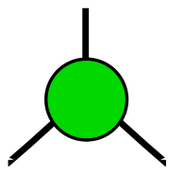


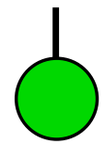
Those points which can be copied by δ

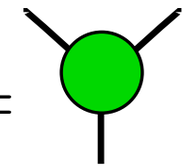
Unbiased Points

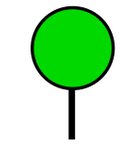


Two kinds of points

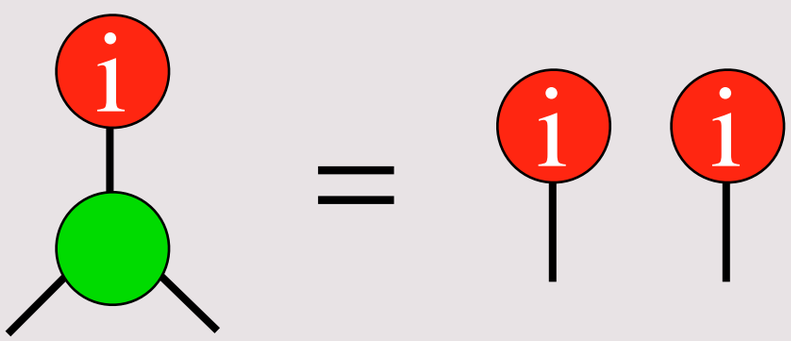
$\delta =$ 

$\epsilon =$ 

$\delta^\dagger =$ 

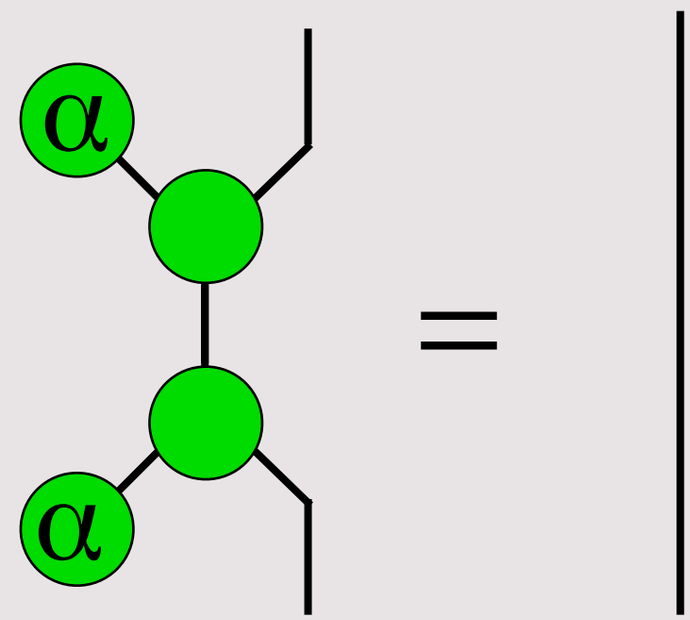
$\epsilon^\dagger =$ 

Classical Points

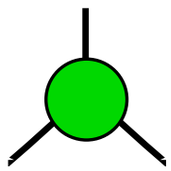


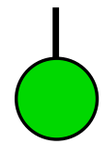
Those points which can be copied by δ

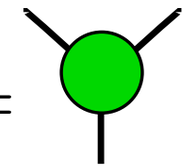
Unbiased Points

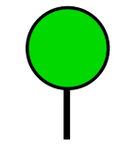


Two kinds of points

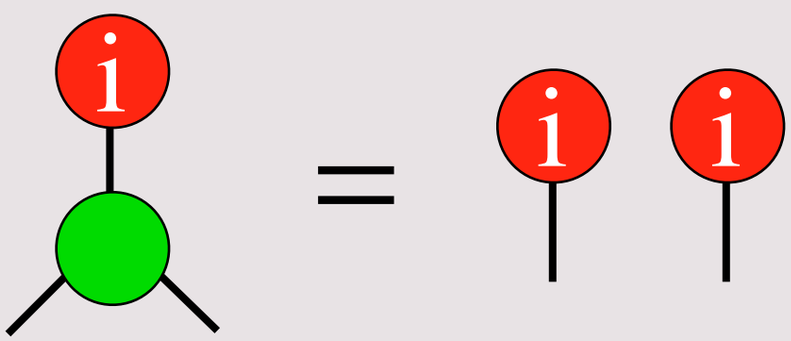
$\delta =$ 

$\epsilon =$ 

$\delta^\dagger =$ 

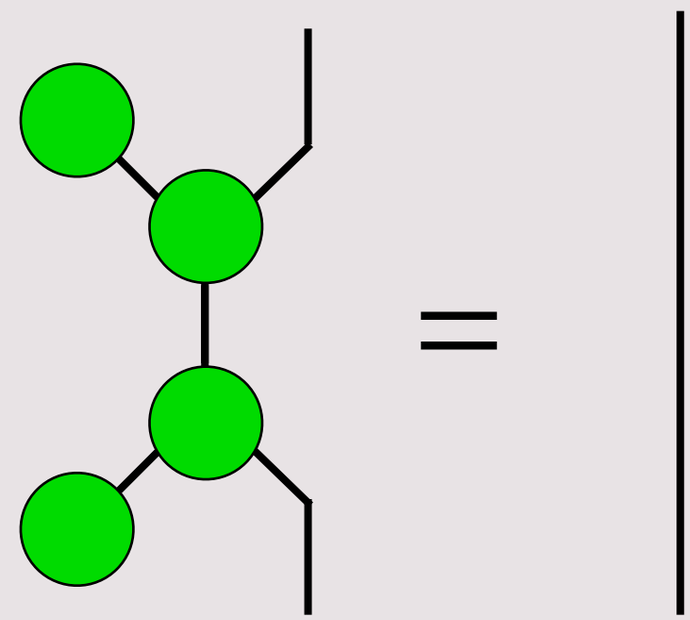
$\epsilon^\dagger =$ 

Classical Points

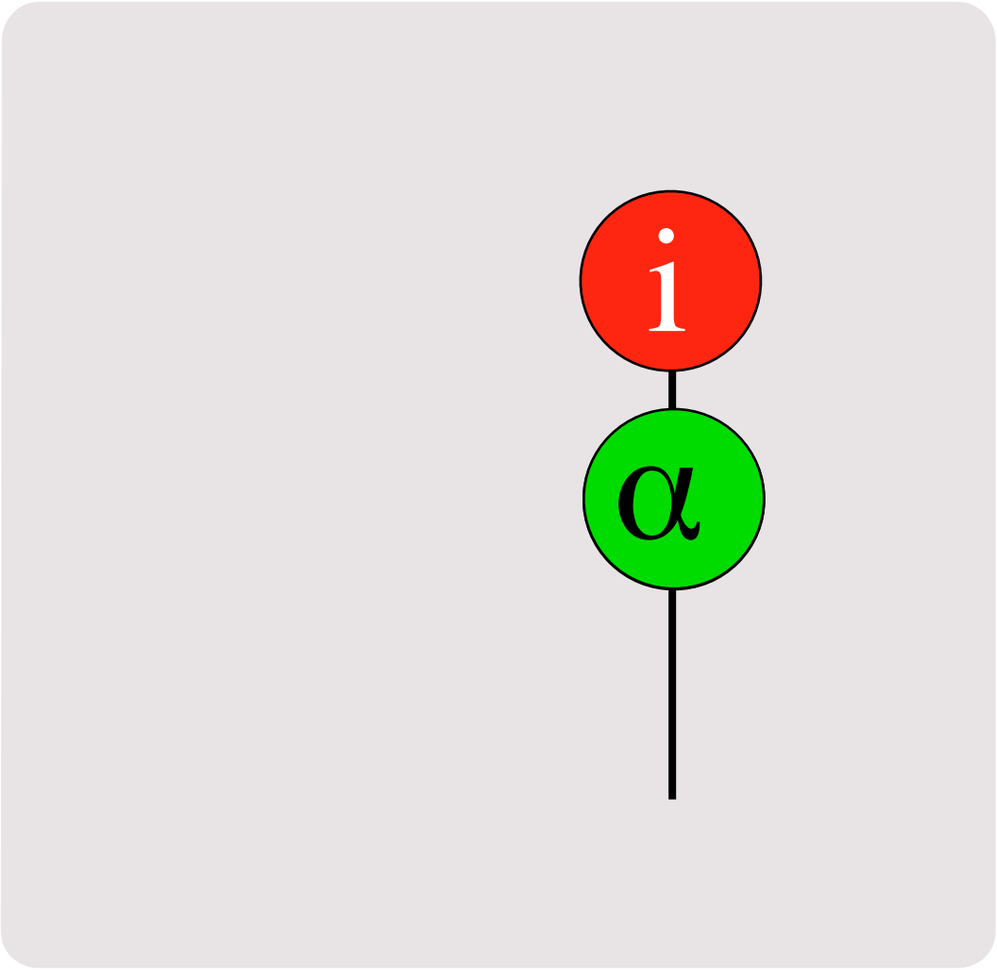


Those points which can be copied by δ

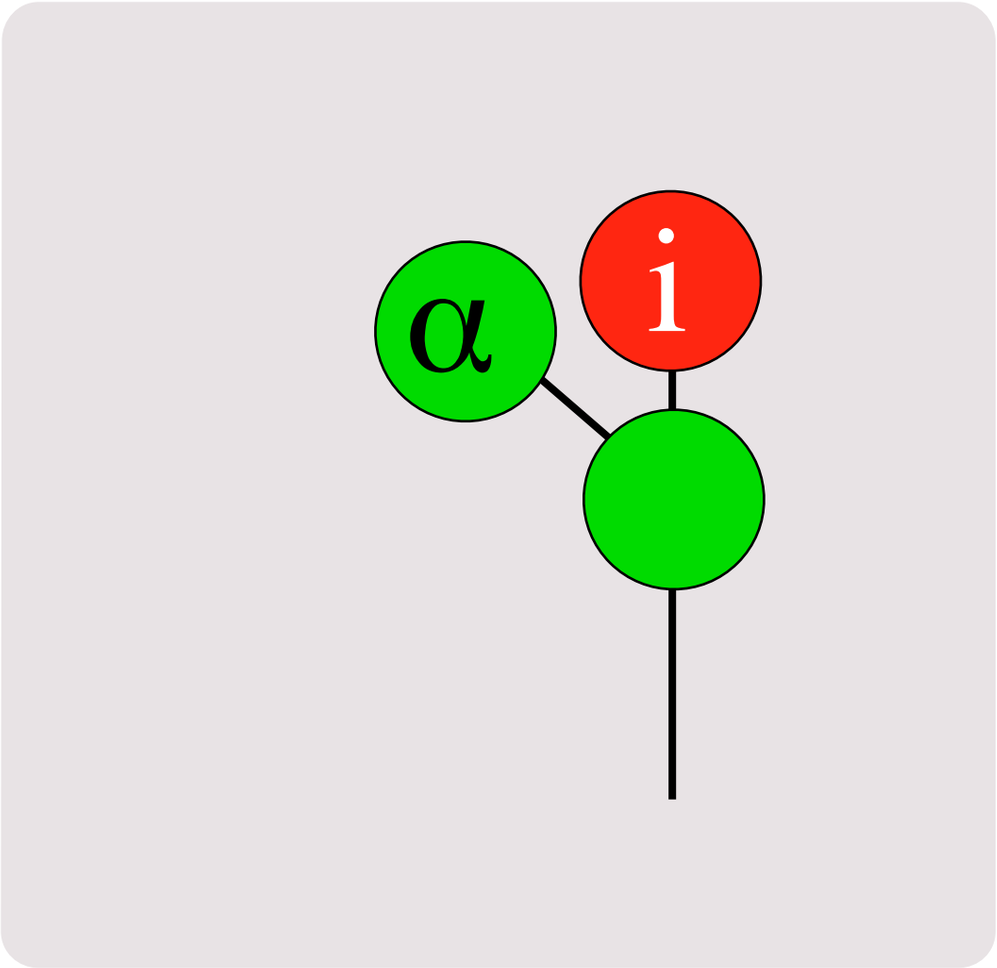
Unbiased Points



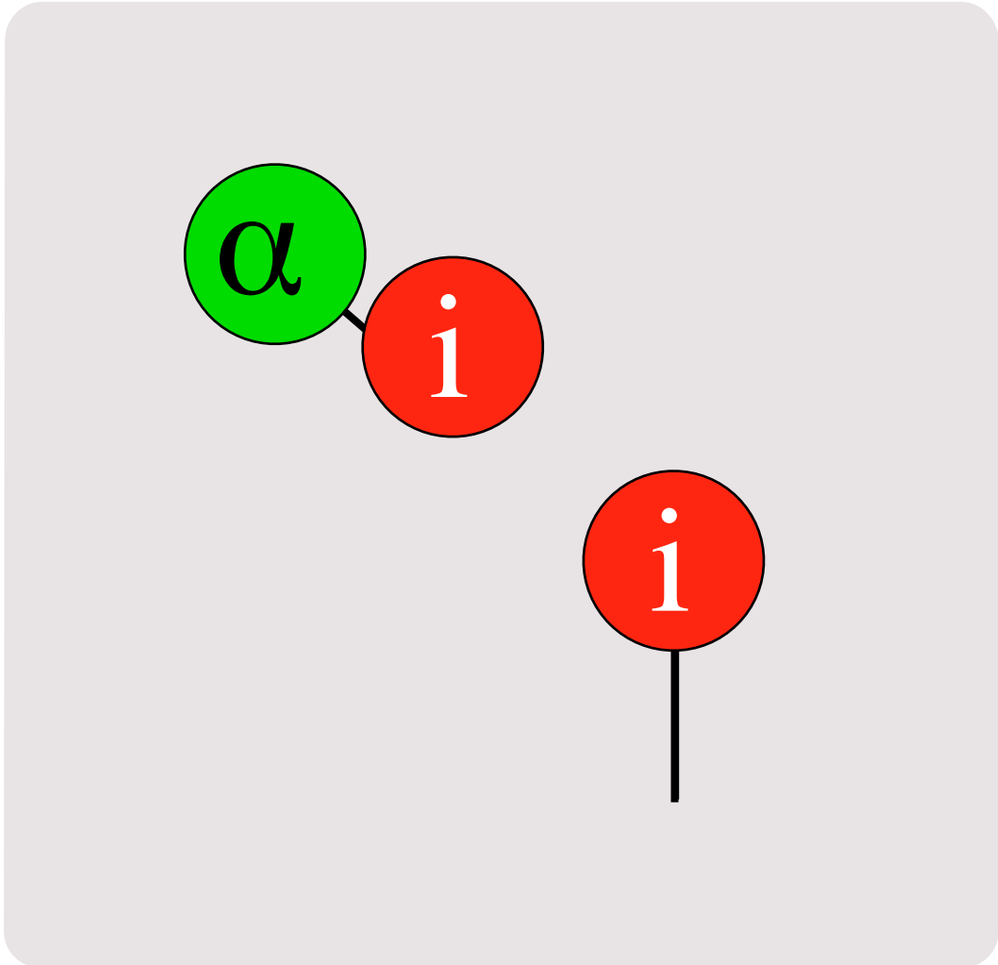
Classical points are eigenvectors



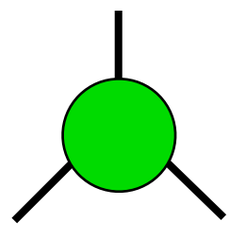
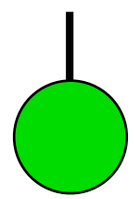
Classical points are eigenvectors



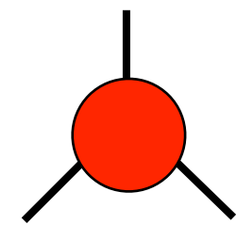
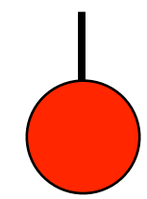
Classical points are eigenvectors



Complementary Observables

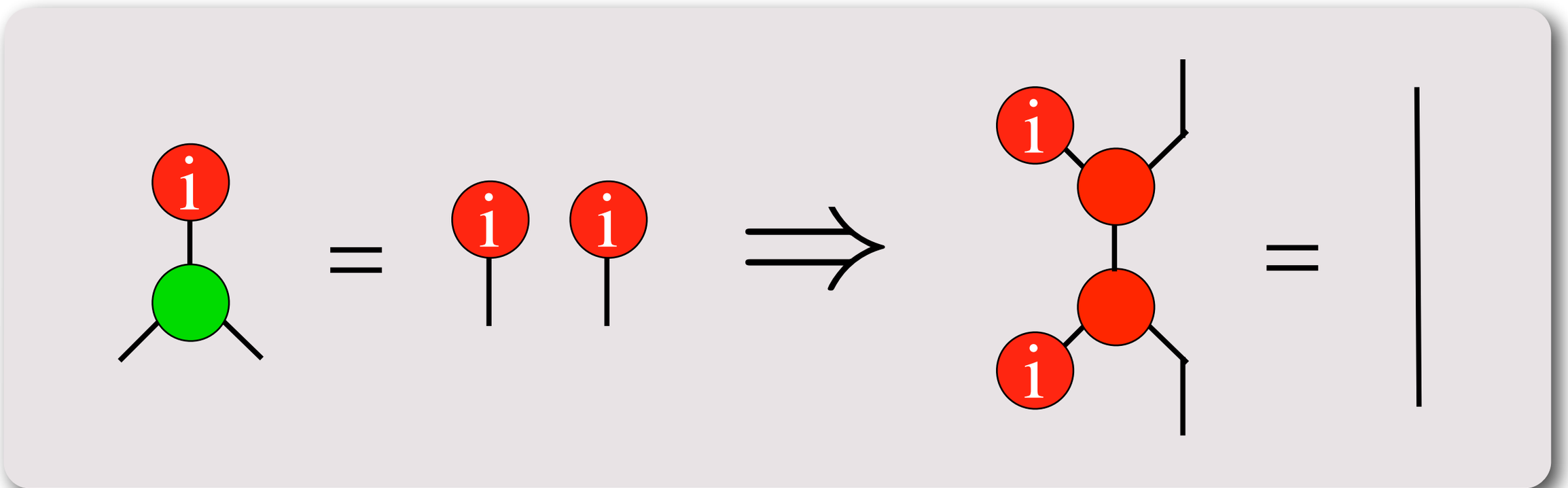
$\delta_Z =$  $\epsilon_Z =$ 

$|i\rangle \mapsto |ii\rangle$ $\quad$ $|+\rangle \mapsto 1$

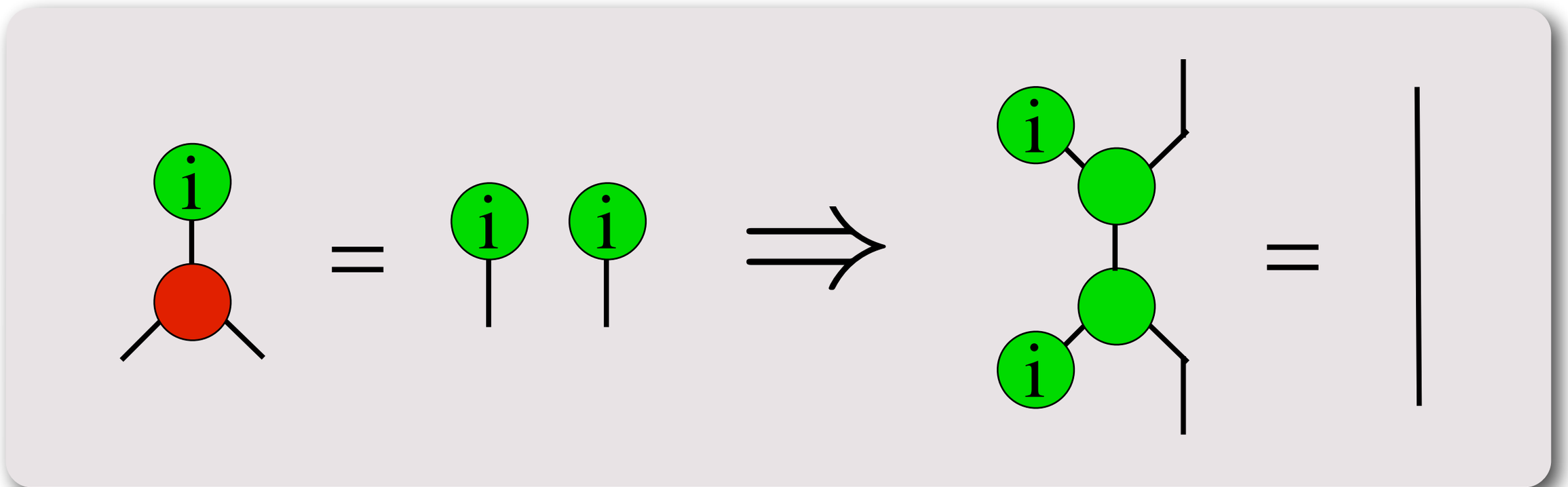
$\delta_X =$  $\epsilon_X =$ 

$|\pm\rangle \mapsto |\pm\pm\rangle$ $\quad$ $|0\rangle \mapsto 1$

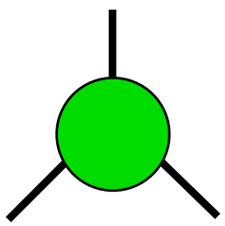
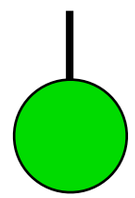
Complementary Observables

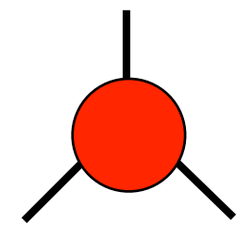
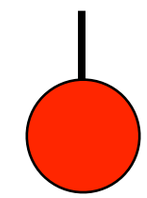


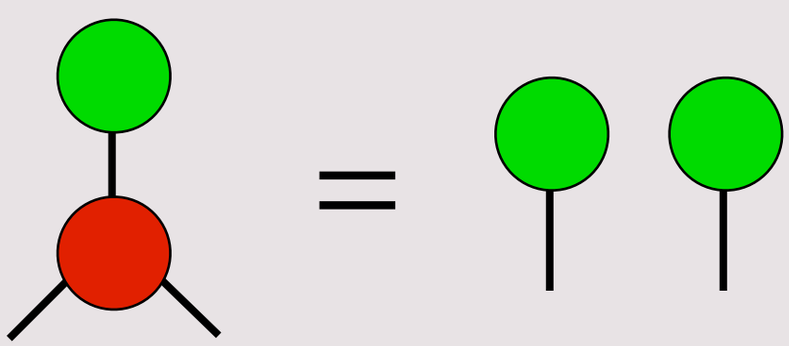
Complementary Observables

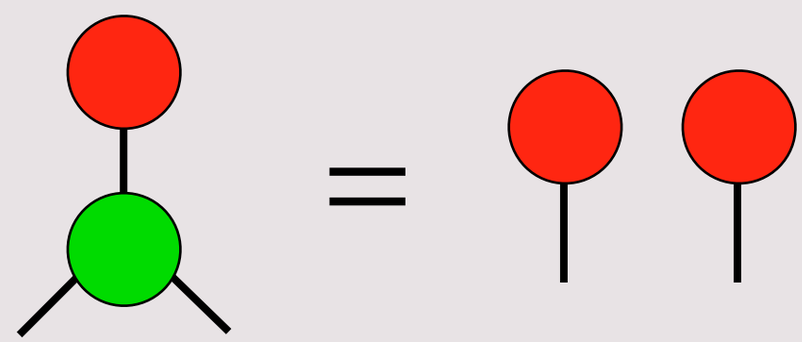


Complementary Observables

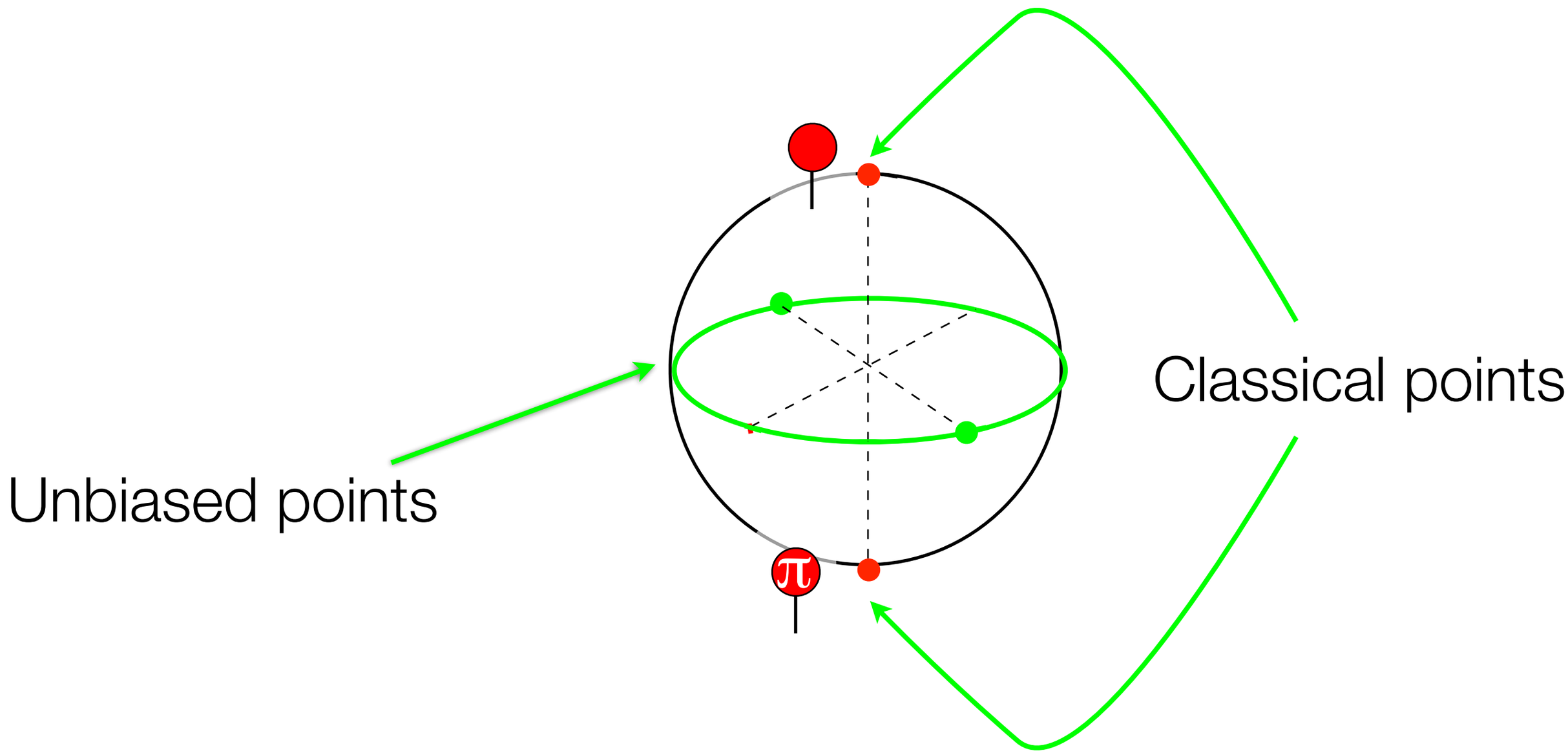
$\delta_Z =$  $\epsilon_Z =$ 

$\delta_X =$  $\epsilon_X =$ 

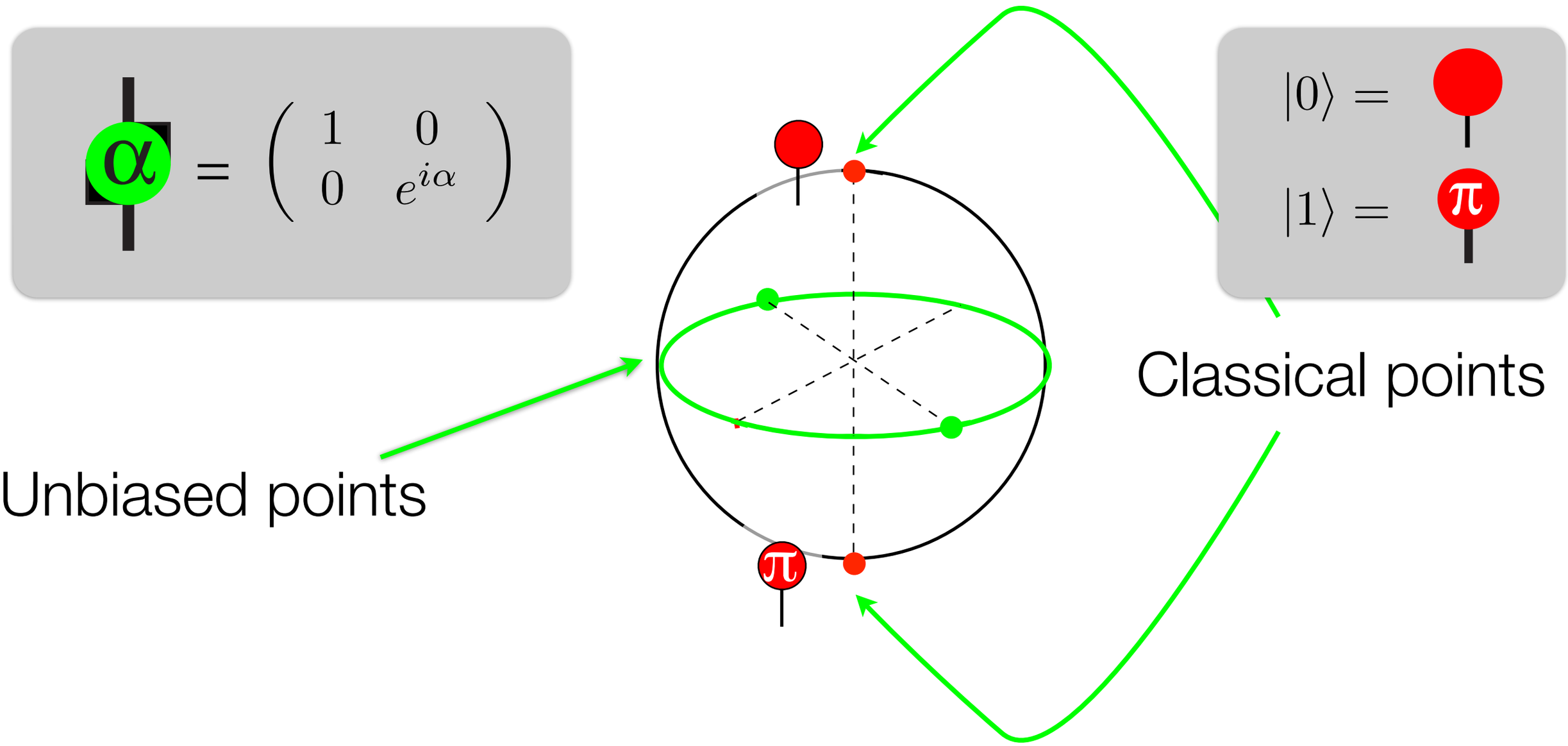




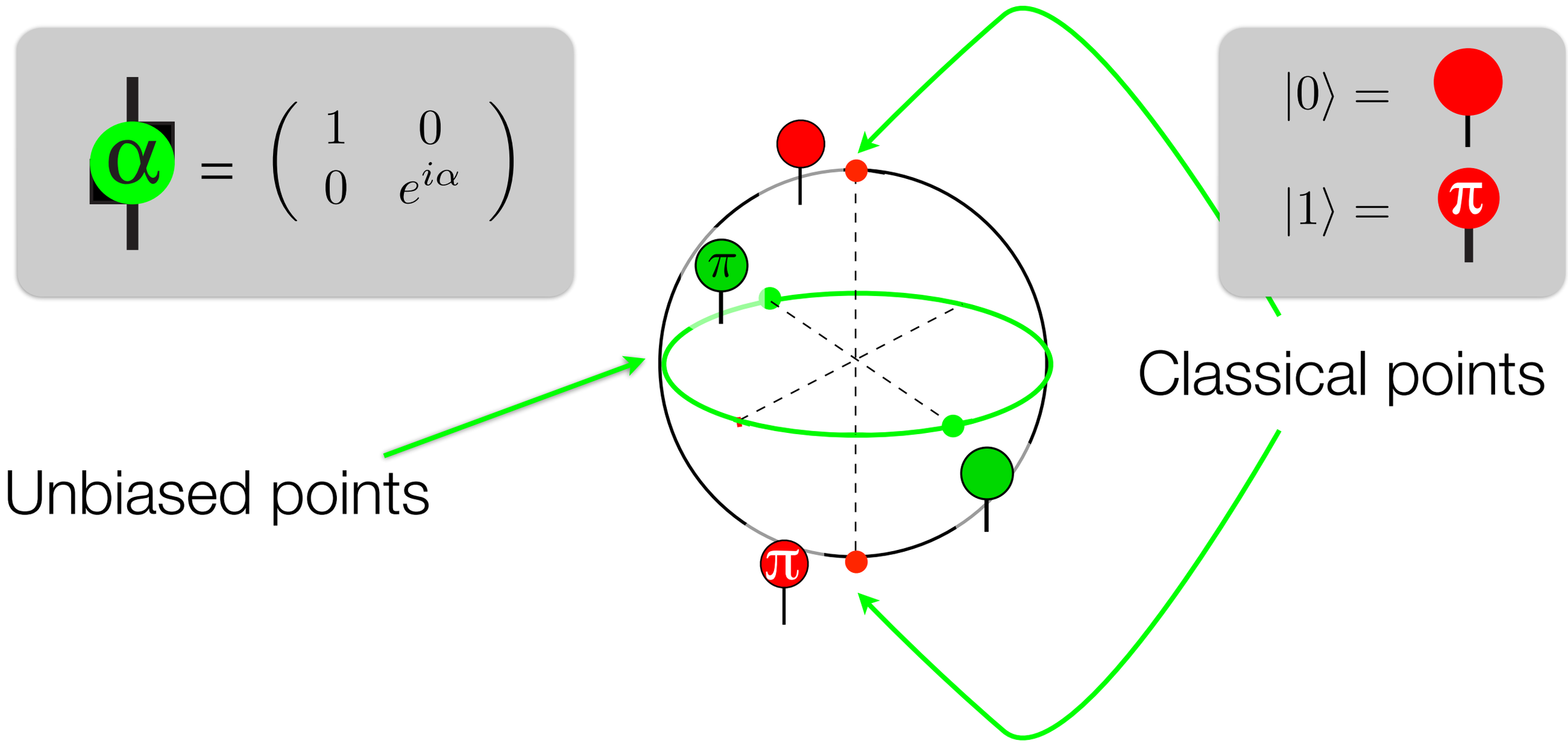
Example: qubits



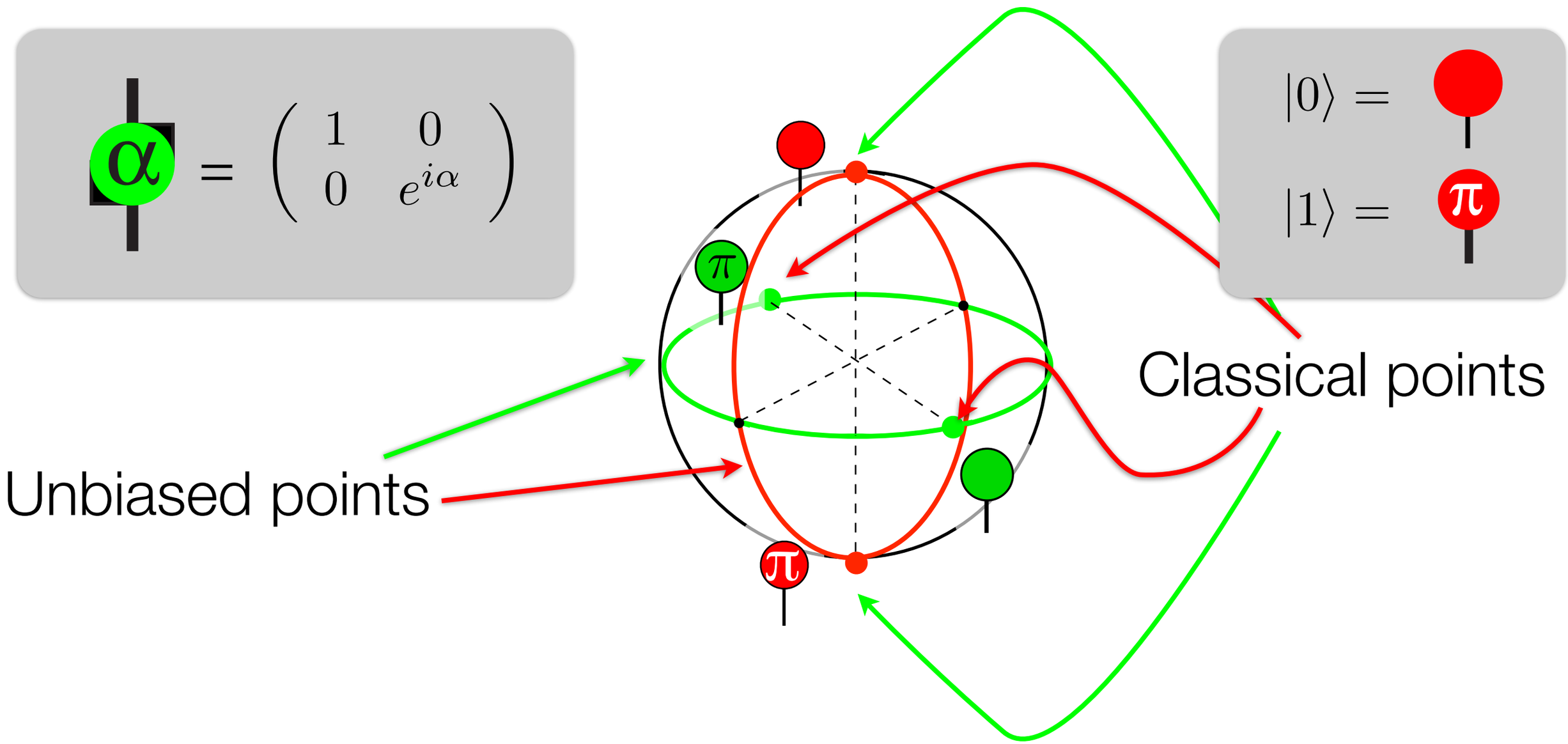
Example: qubits



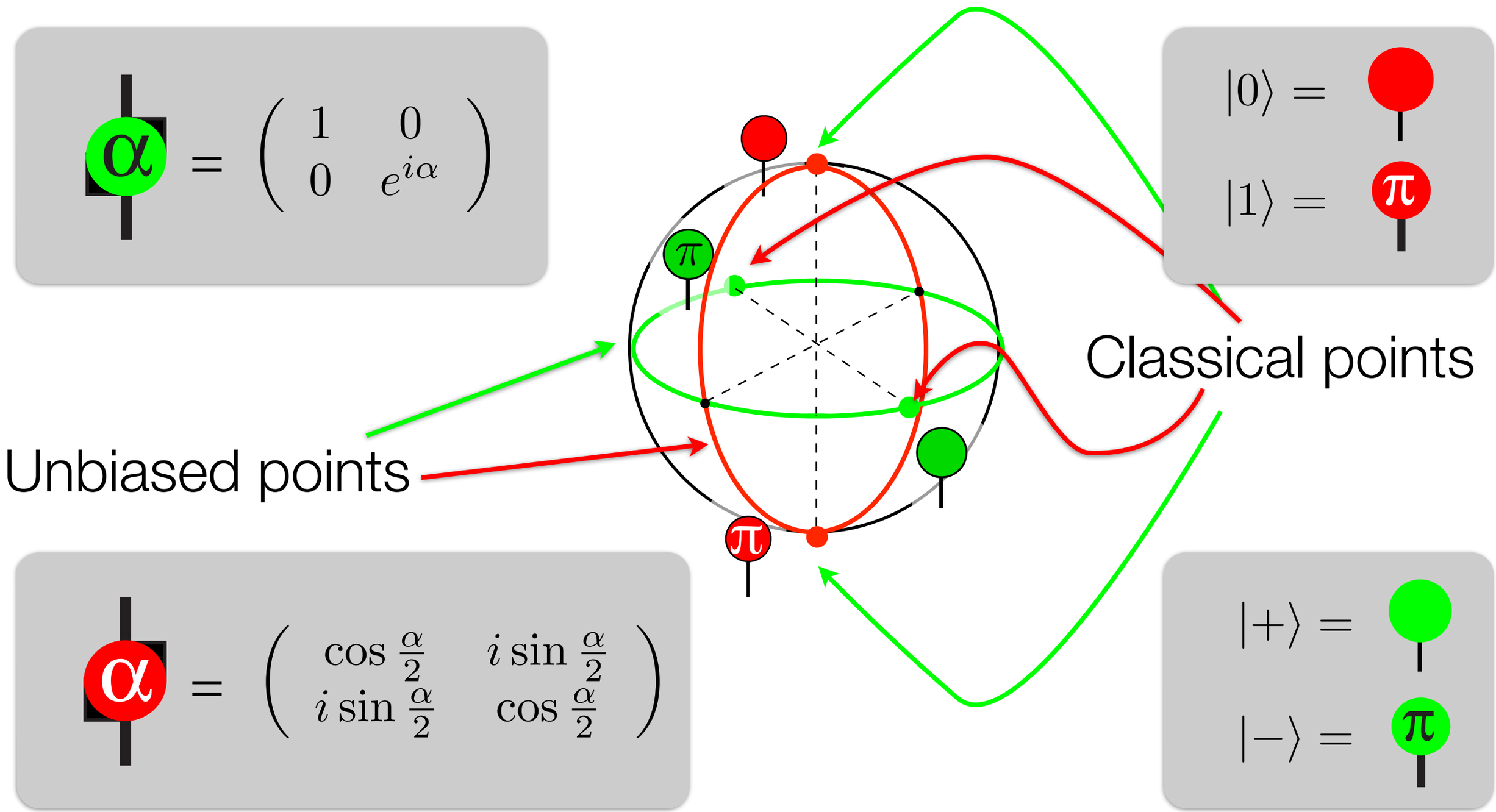
Example: qubits



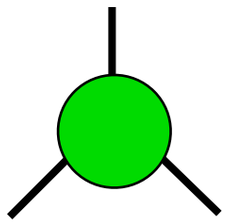
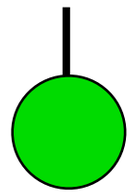
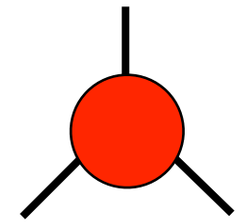
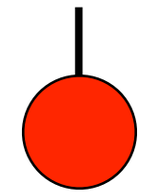
Example: qubits



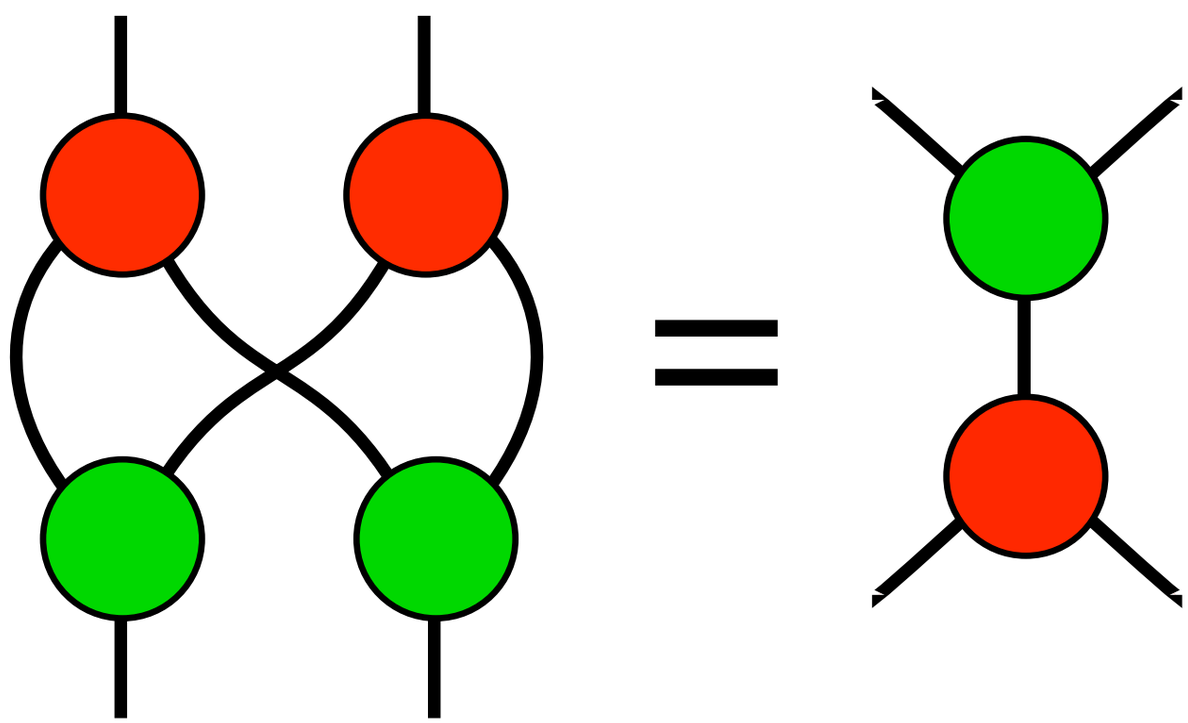
Example: qubits



Strong Complementarity

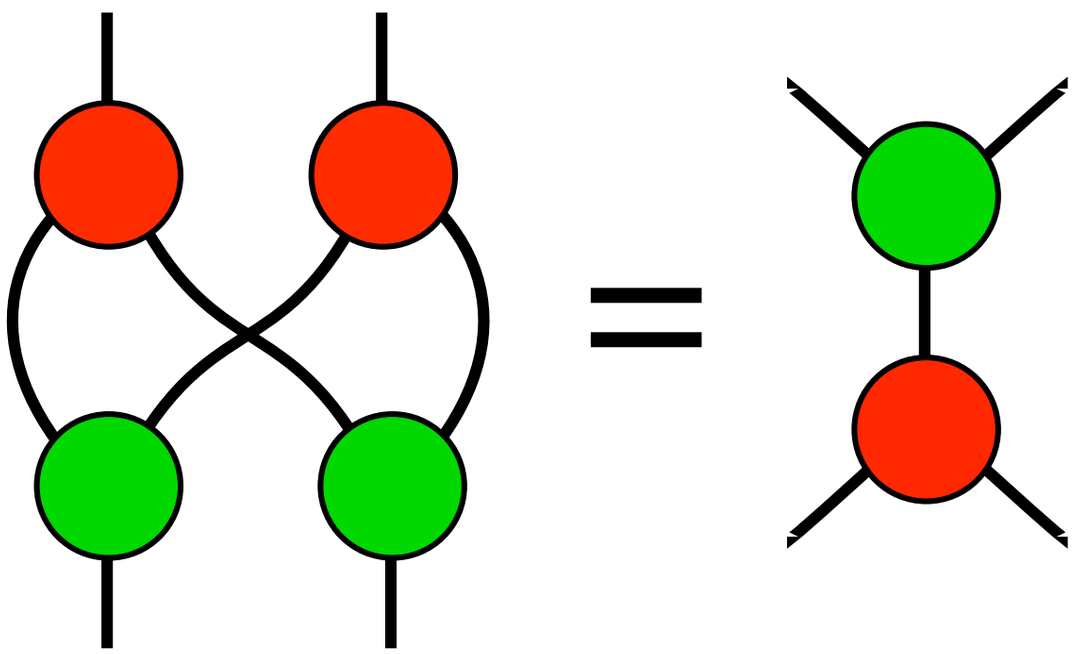
$\delta_Z =$  $\epsilon_Z =$  $\delta_X =$  $\epsilon_X =$ 

A pair of complementary observables are called *strongly complementary* when they satisfy this equation:



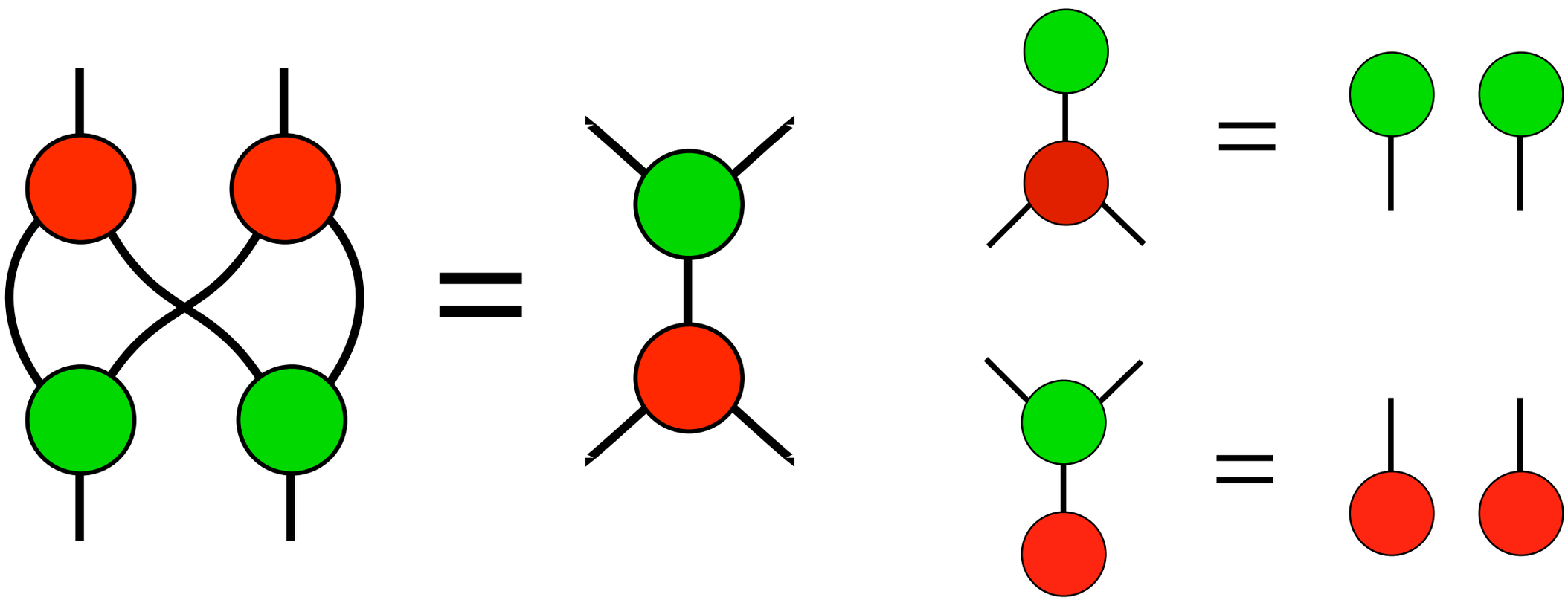
Strong Complementarity

<u>Corollary</u>: strongly complementary observables form a *bialgebra*

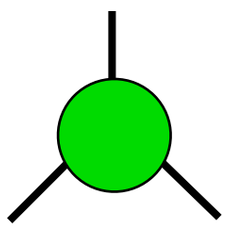
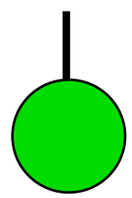


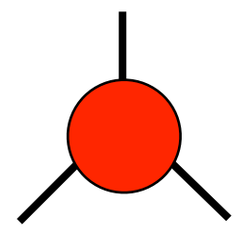
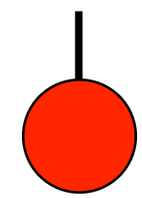
Strong Complementarity

<u>Corollary</u>: strongly complementary observables form a *bialgebra*

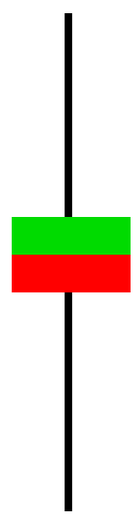
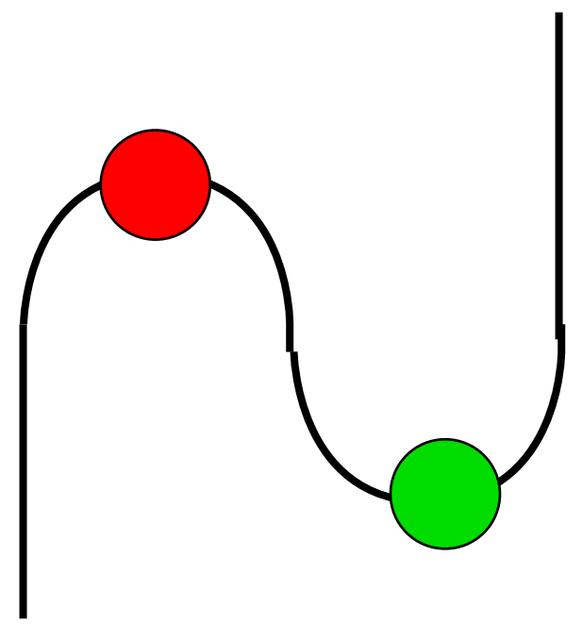


The antipode

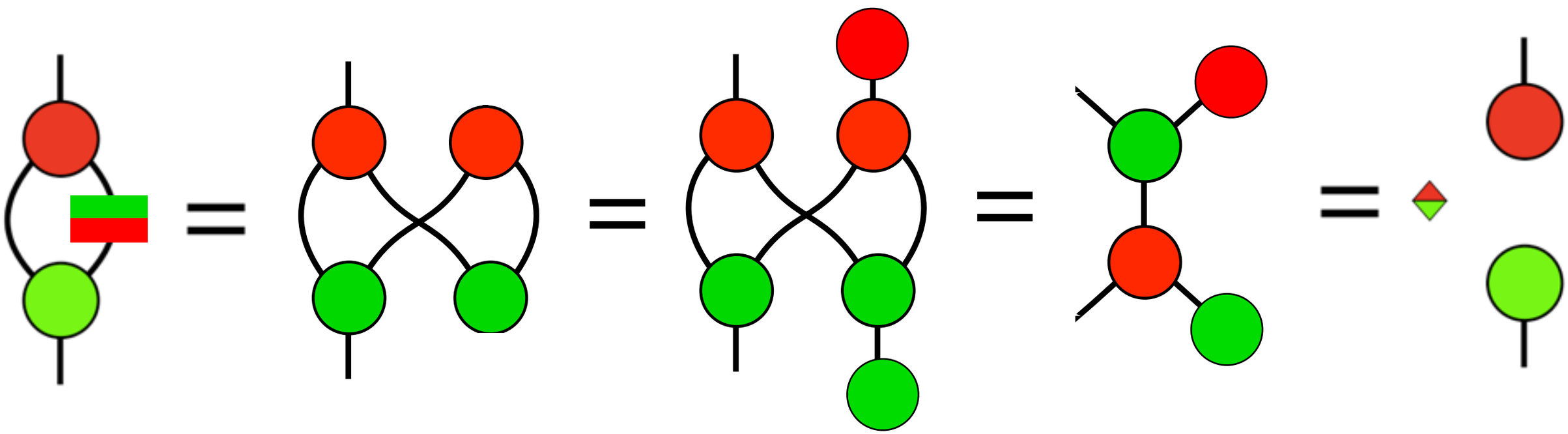
$\delta_Z =$  $\epsilon_Z =$ 

$\delta_X =$  $\epsilon_X =$ 

Define the map S by:

$S =$  $:=$ 

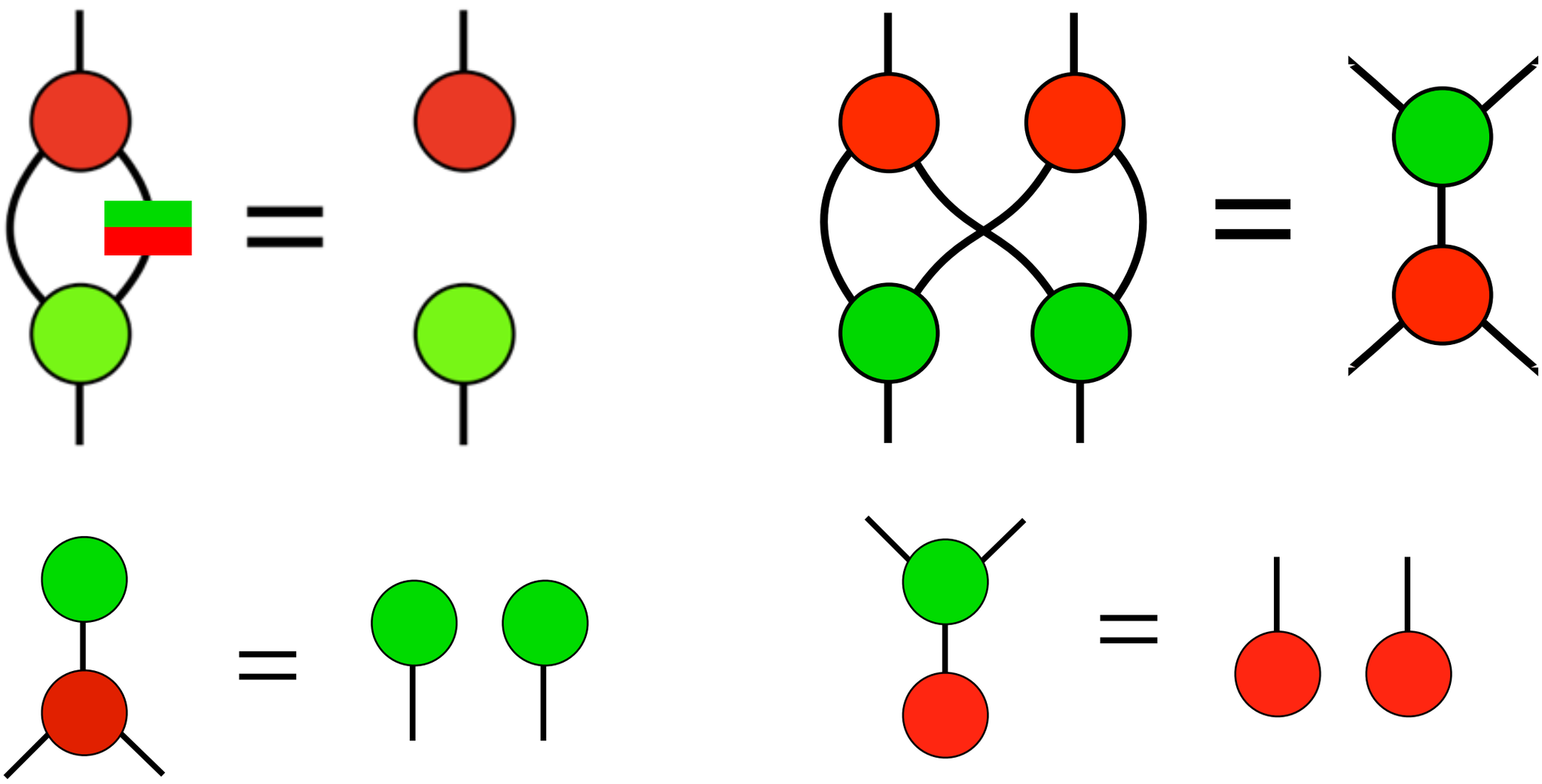
The antipode



* If we have “enough classical points” this can be proved without strong complementarity

Strongly complementary observables form Hopf algebras

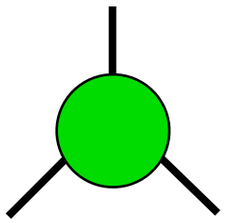
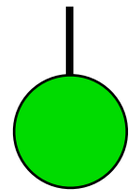
Theorem:

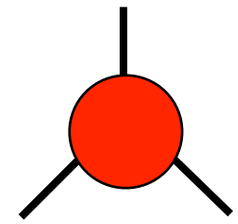
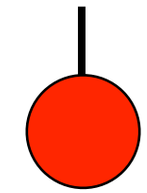


Strong Complementarity

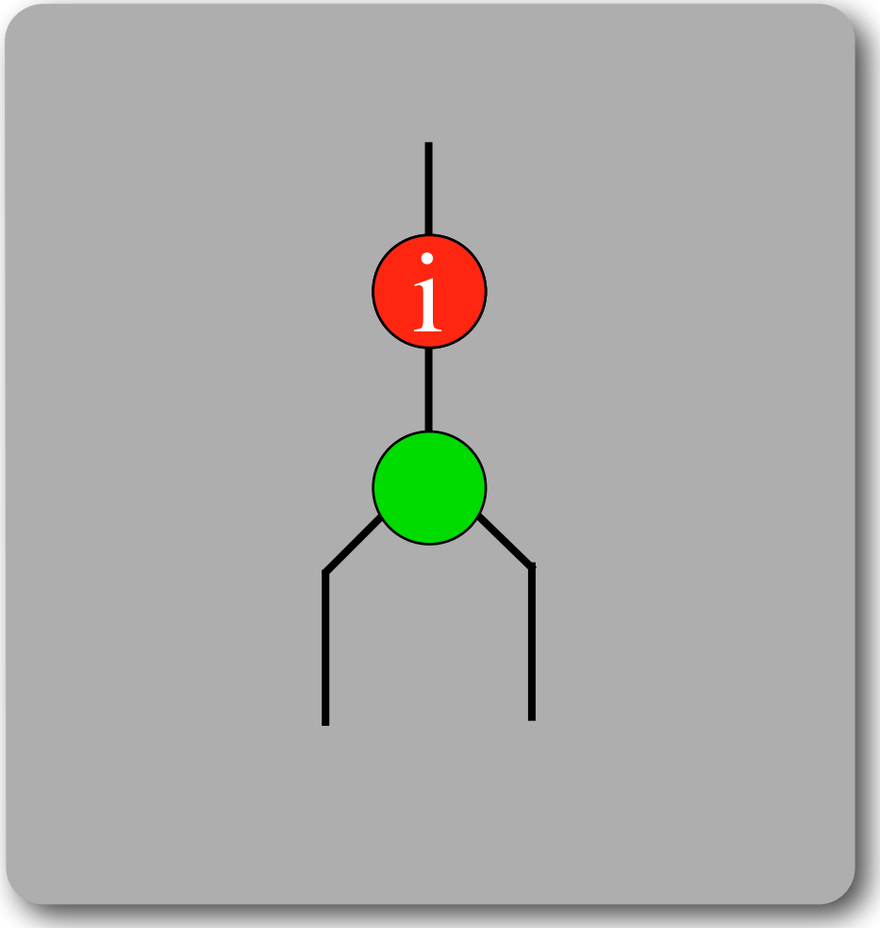
The following are equivalent characterisations of strong complementarity:

Comonoid Homomorphism

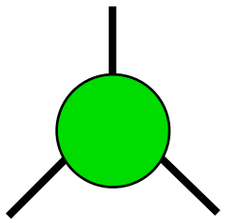
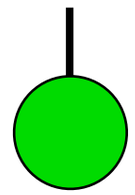
$\delta_Z =$  $\epsilon_Z =$ 

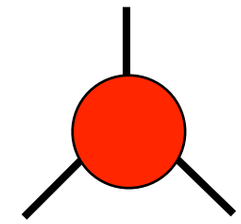
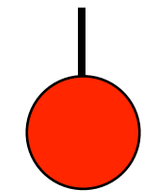
$\delta_X =$  $\epsilon_X =$ 

The classical maps are comonoid homomorphisms

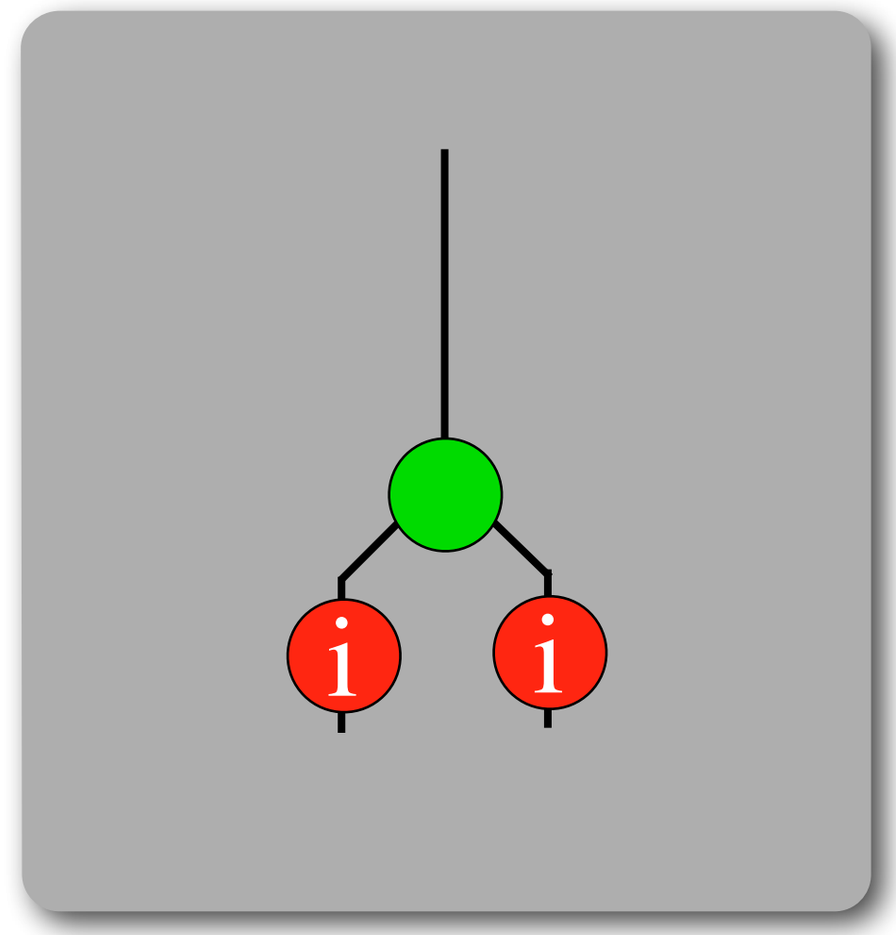


Comonoid Homomorphism

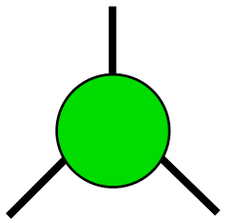
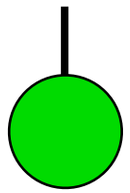
$\delta_Z =$  $\epsilon_Z =$ 

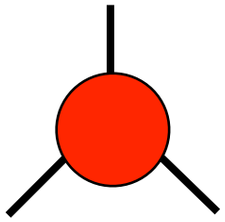
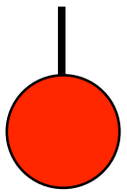
$\delta_X =$  $\epsilon_X =$ 

The classical maps are comonoid homomorphisms

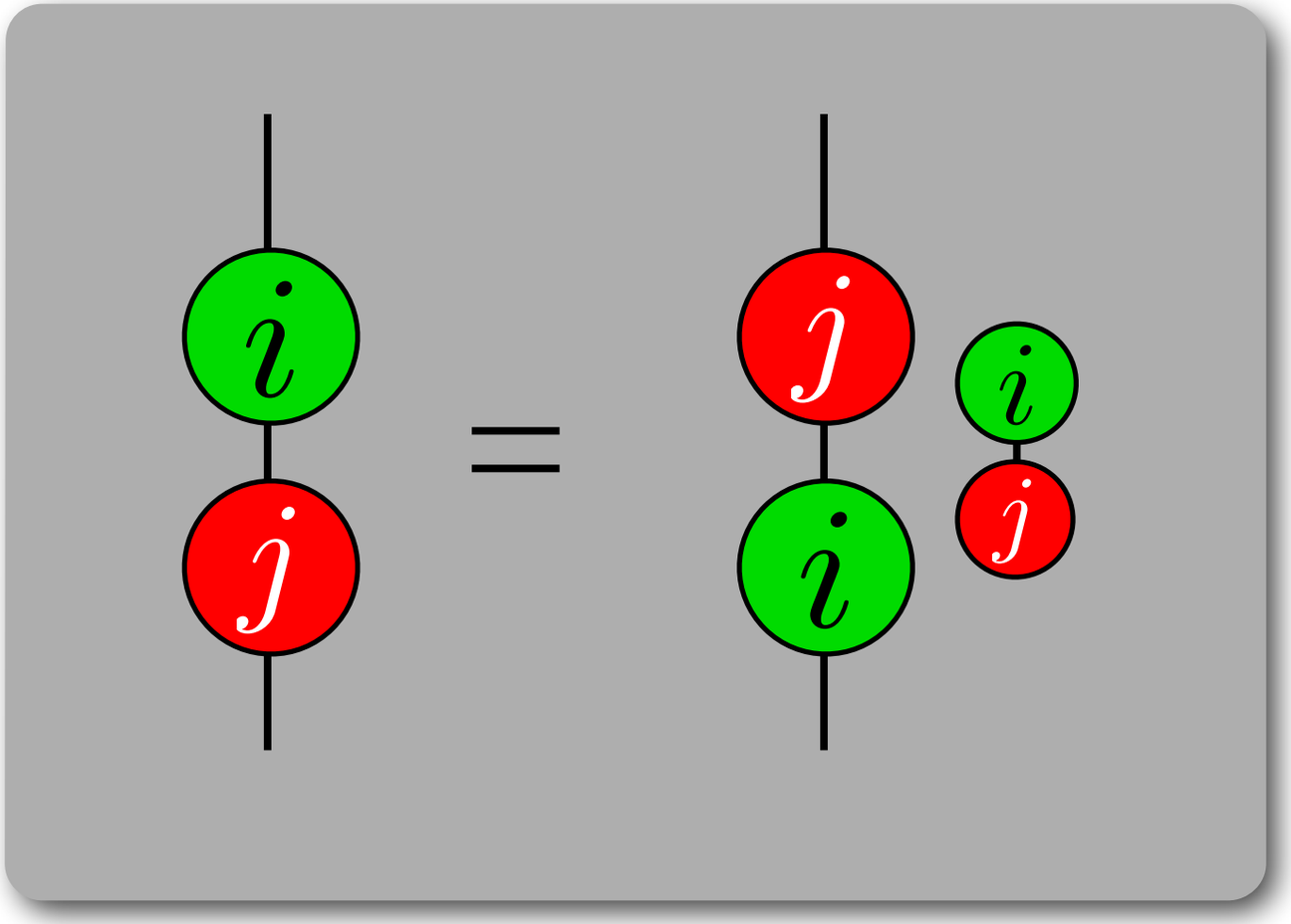


Classical Phases Commute

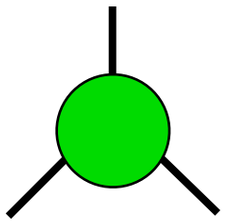
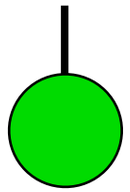
$\delta_Z =$  $\epsilon_Z =$ 

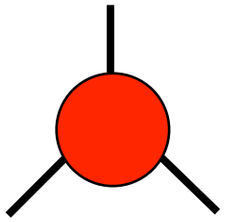
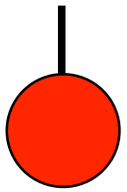
$\delta_X =$  $\epsilon_X =$ 

The classical maps satisfy canonical commutation relations

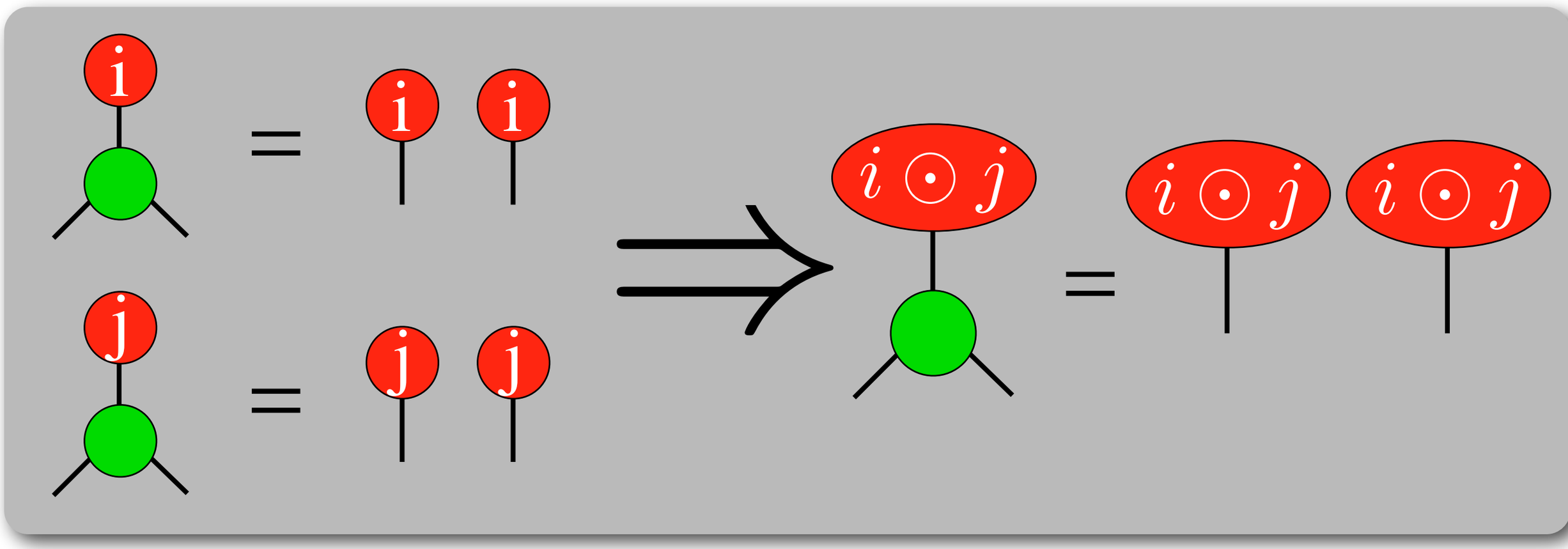


Closedness Property

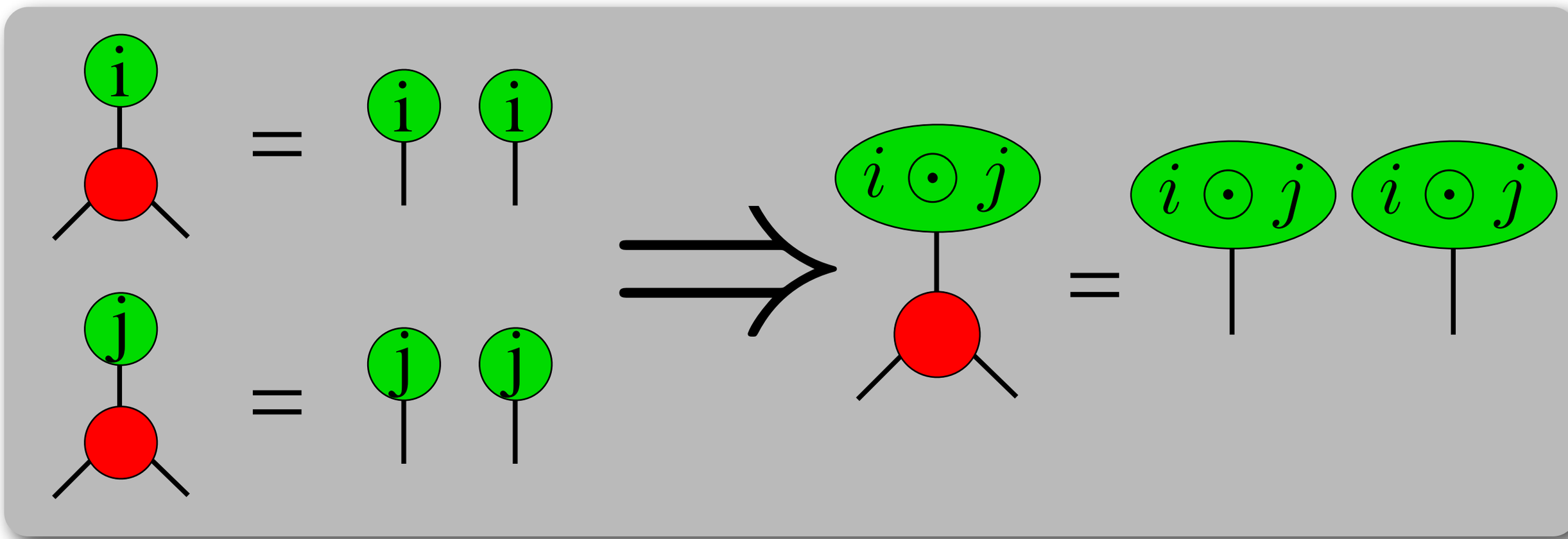
$\delta_Z =$  $\epsilon_Z =$ 

$\delta_X =$  $\epsilon_X =$ 

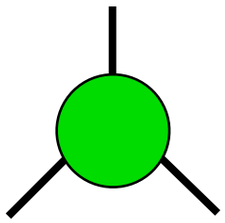
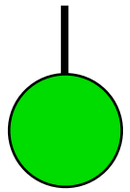
Closedness Property

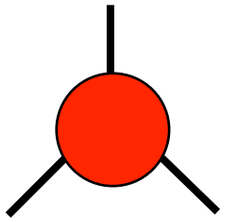
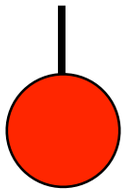


Closedness Property



Closedness Property

$\delta_Z =$  $\epsilon_Z =$ 

$\delta_X =$  $\epsilon_X =$ 

Theorem:
In $\mathbf{fdHilb}$, strongly complementary observables exist for every dimension.

... but in big enough dimension, it is possible to construct MUBs which are not closed.

arXiv:1601.04964
LiCS 2016.

“Interacting Frobenius Algebras are Hopf”

RD + Kevin Dunne

4.

The ZX-calculus

ZX-calculus

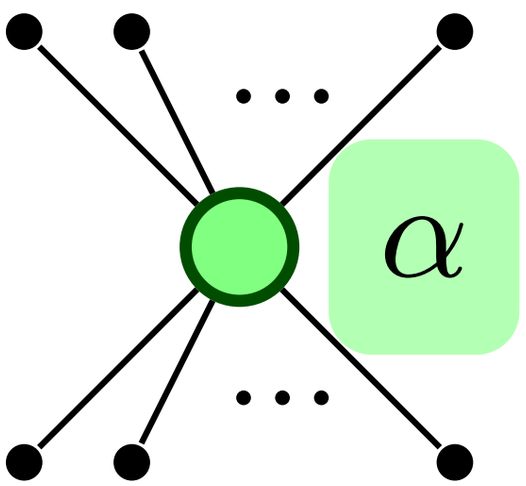
Good Points:

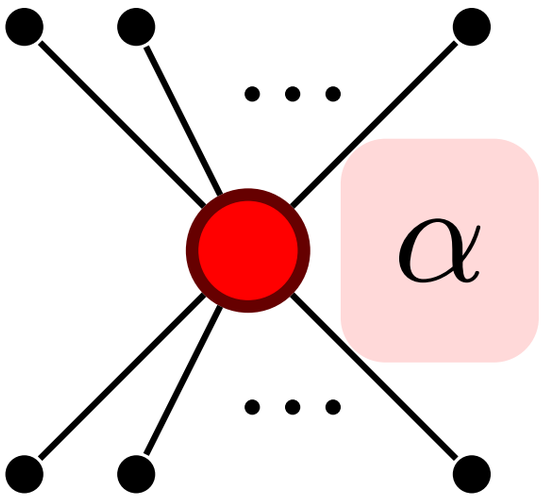
+ Graphical language for reasoning about QC
+ Universal
+ Derived from the basic algebra of complementarity
+ Powerful algebraic theory
+ Complete!

Bad point:

- Need to impose operational meaning post-hoc

ZX-calculus syntax

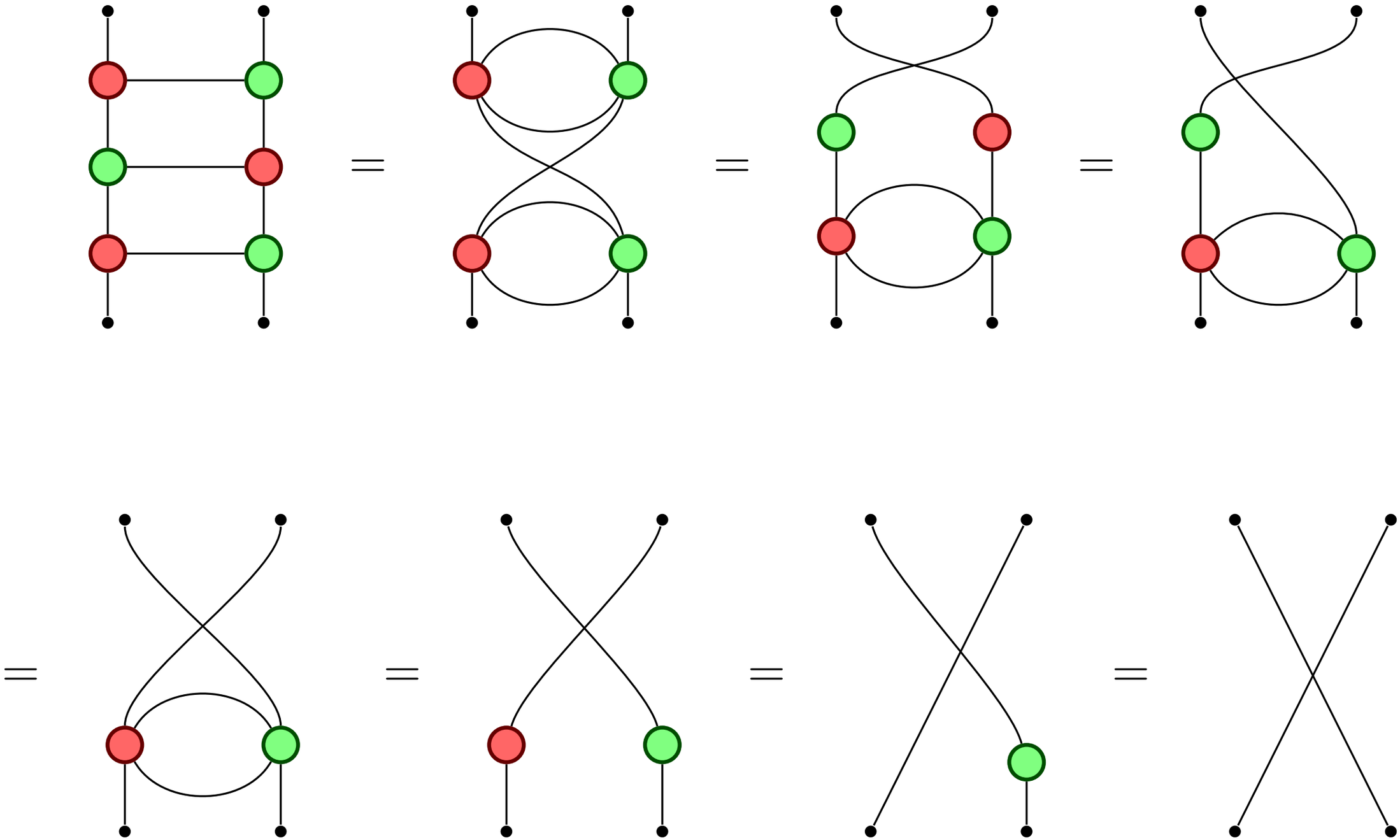




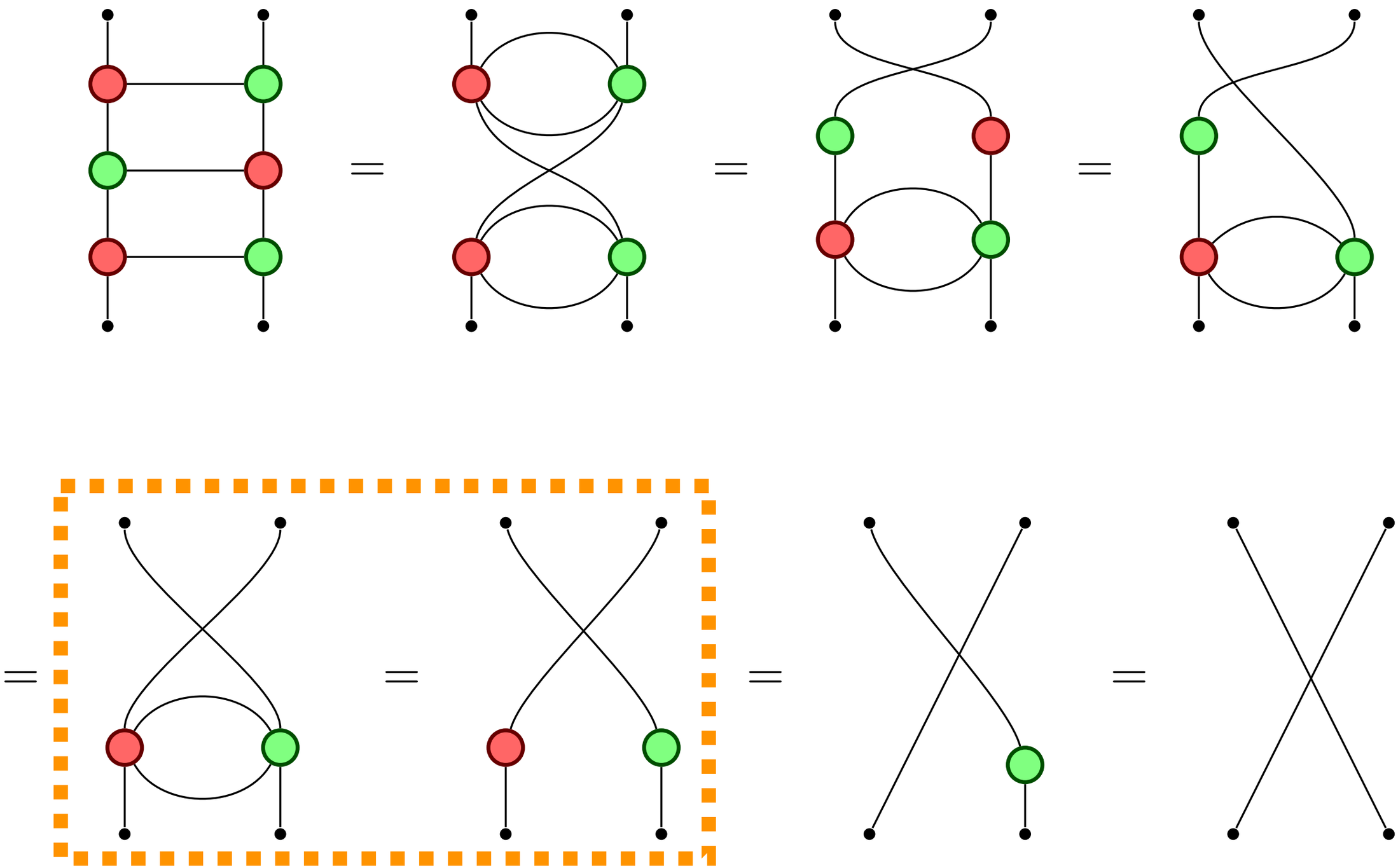
$$\alpha \in [0, 2\pi)$$

Defn: A *diagram* is an undirected open graph generated by the above vertices.

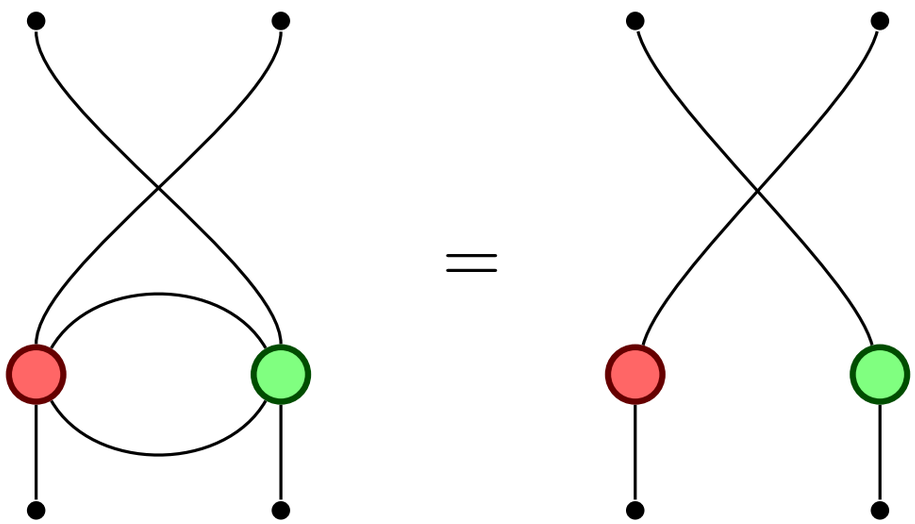
Example: CNOTS



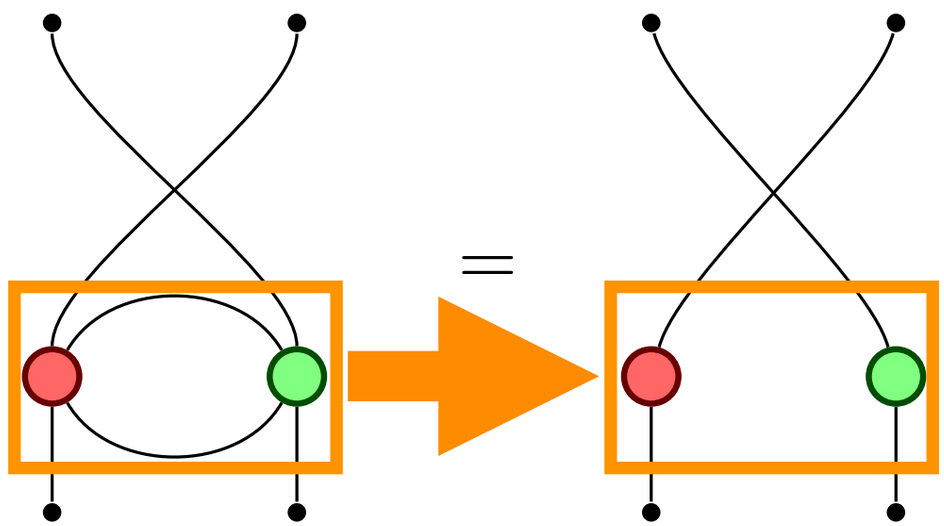
Example: CNOTS



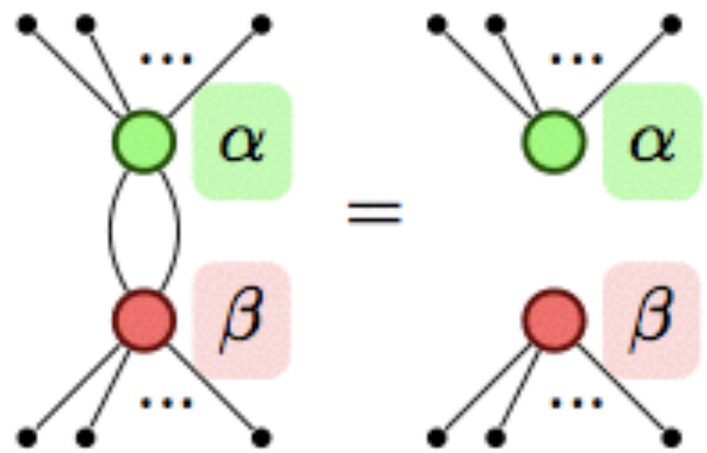
Equational Reasoning



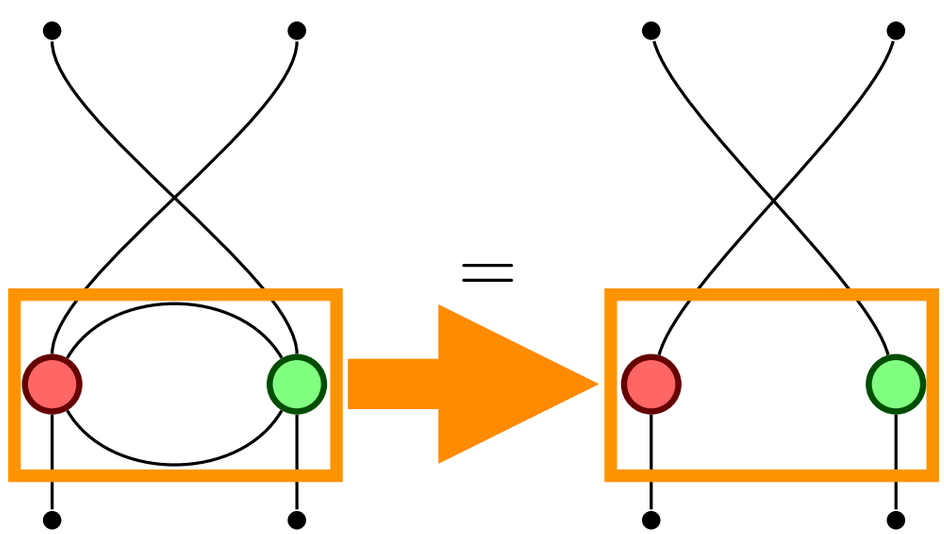
Equational Reasoning



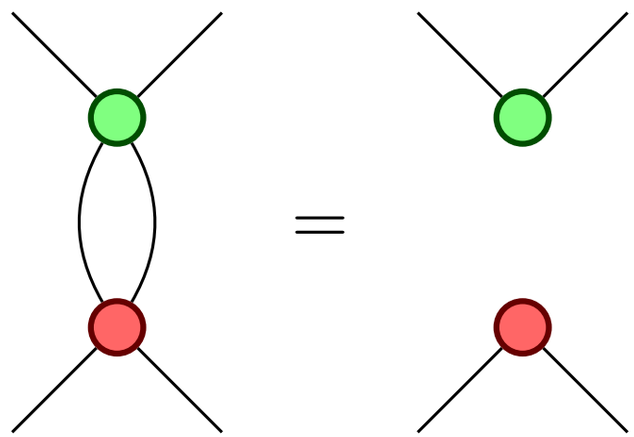
Equational Reasoning

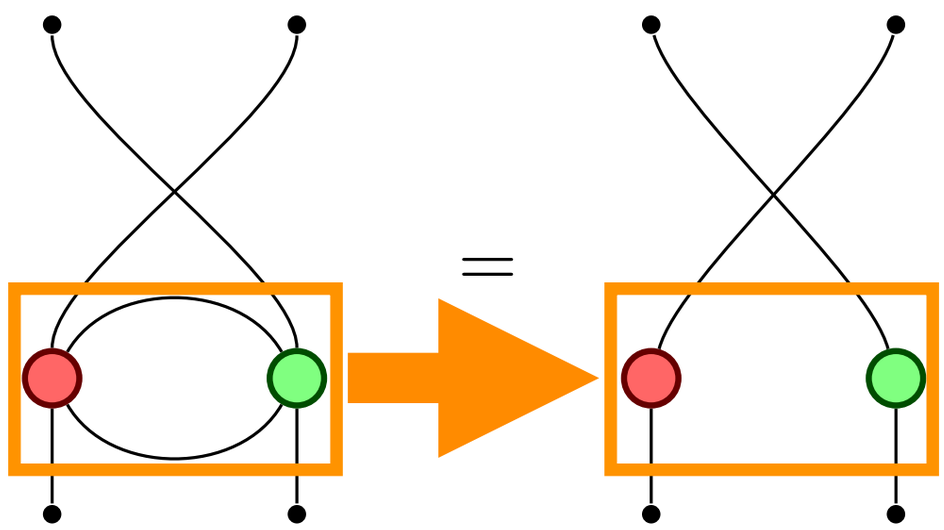


(hopf)

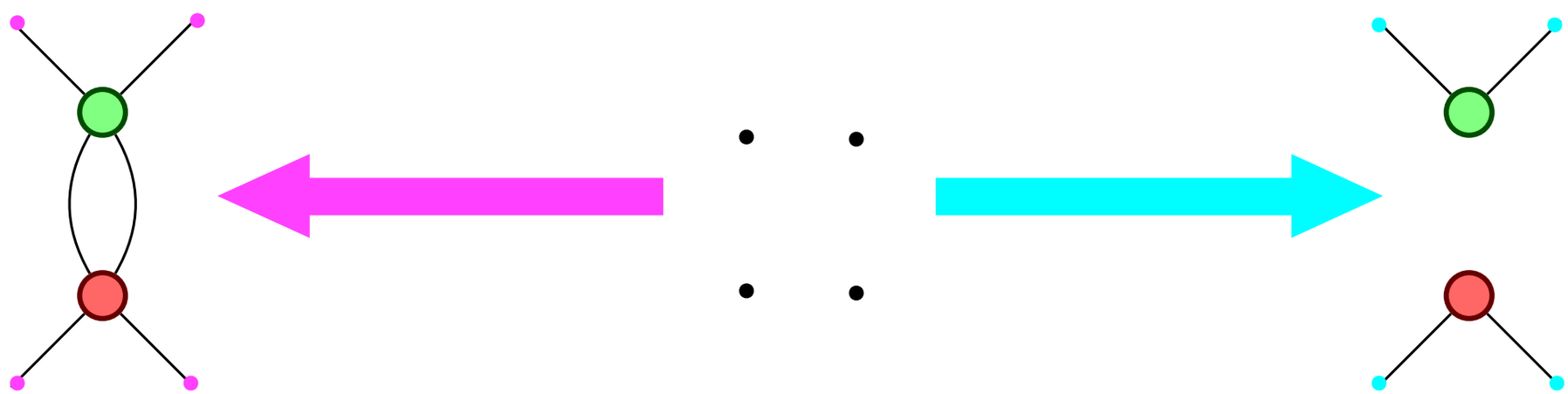


Equational Reasoning

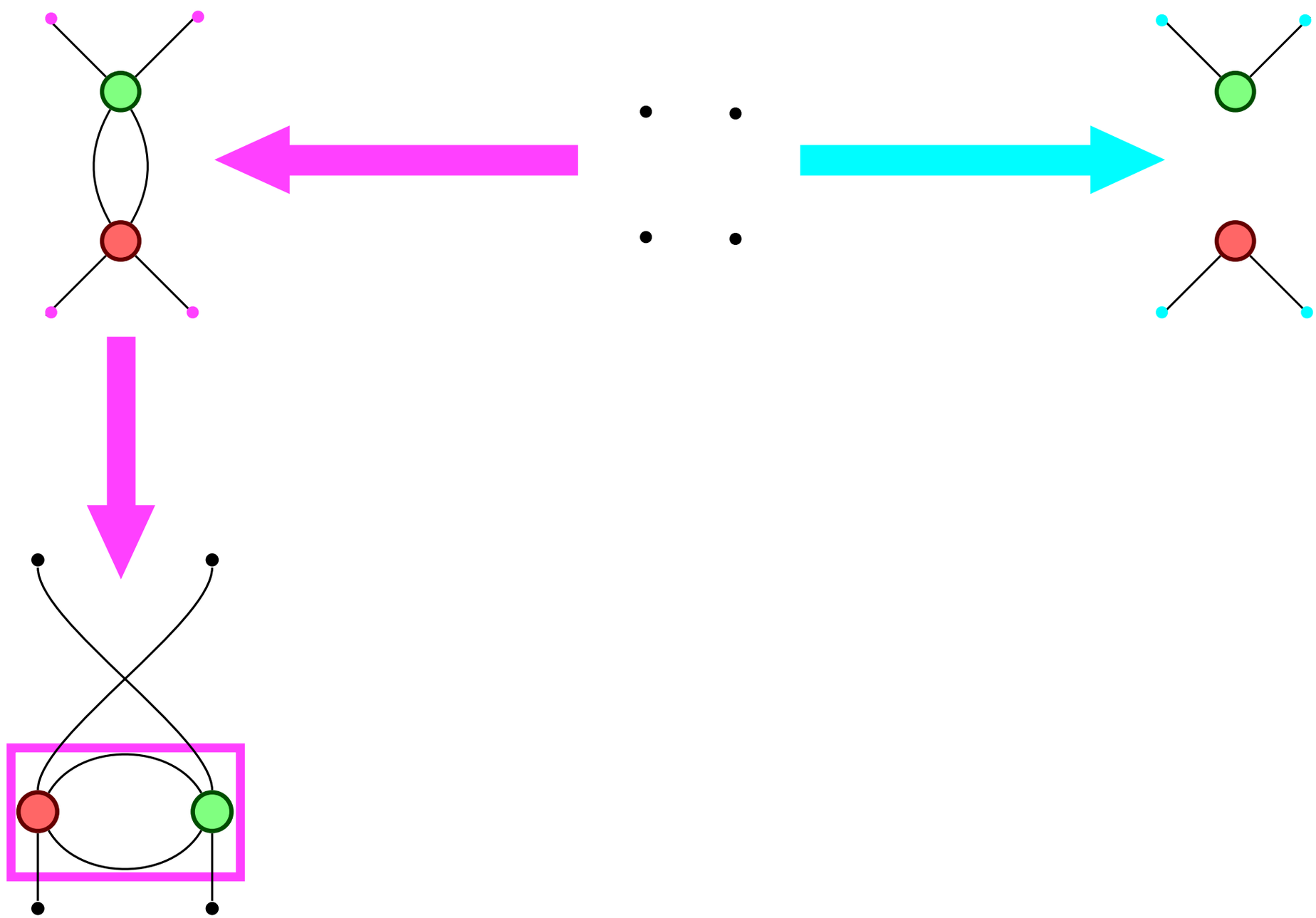




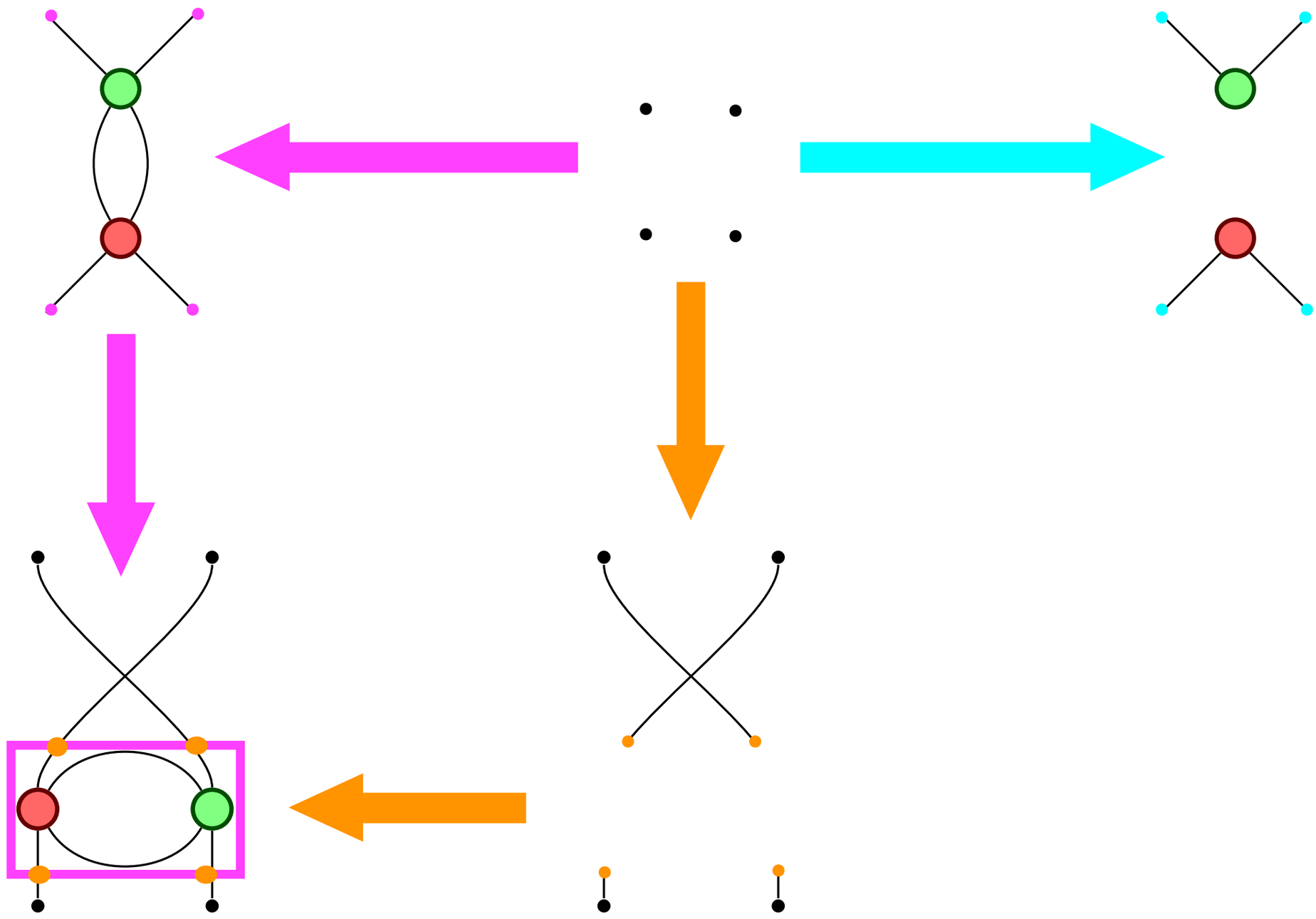
Equational Reasoning



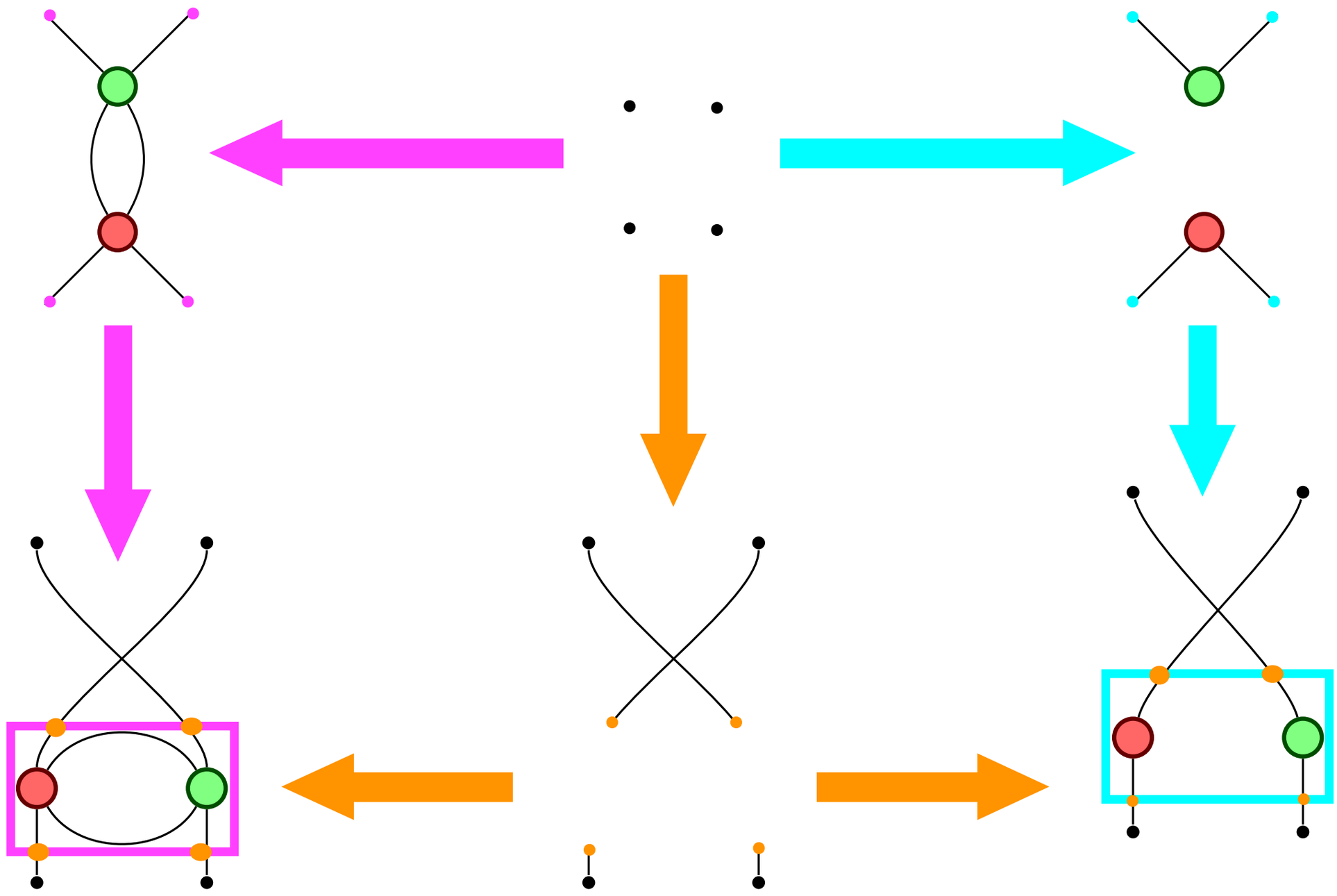
Equational Reasoning



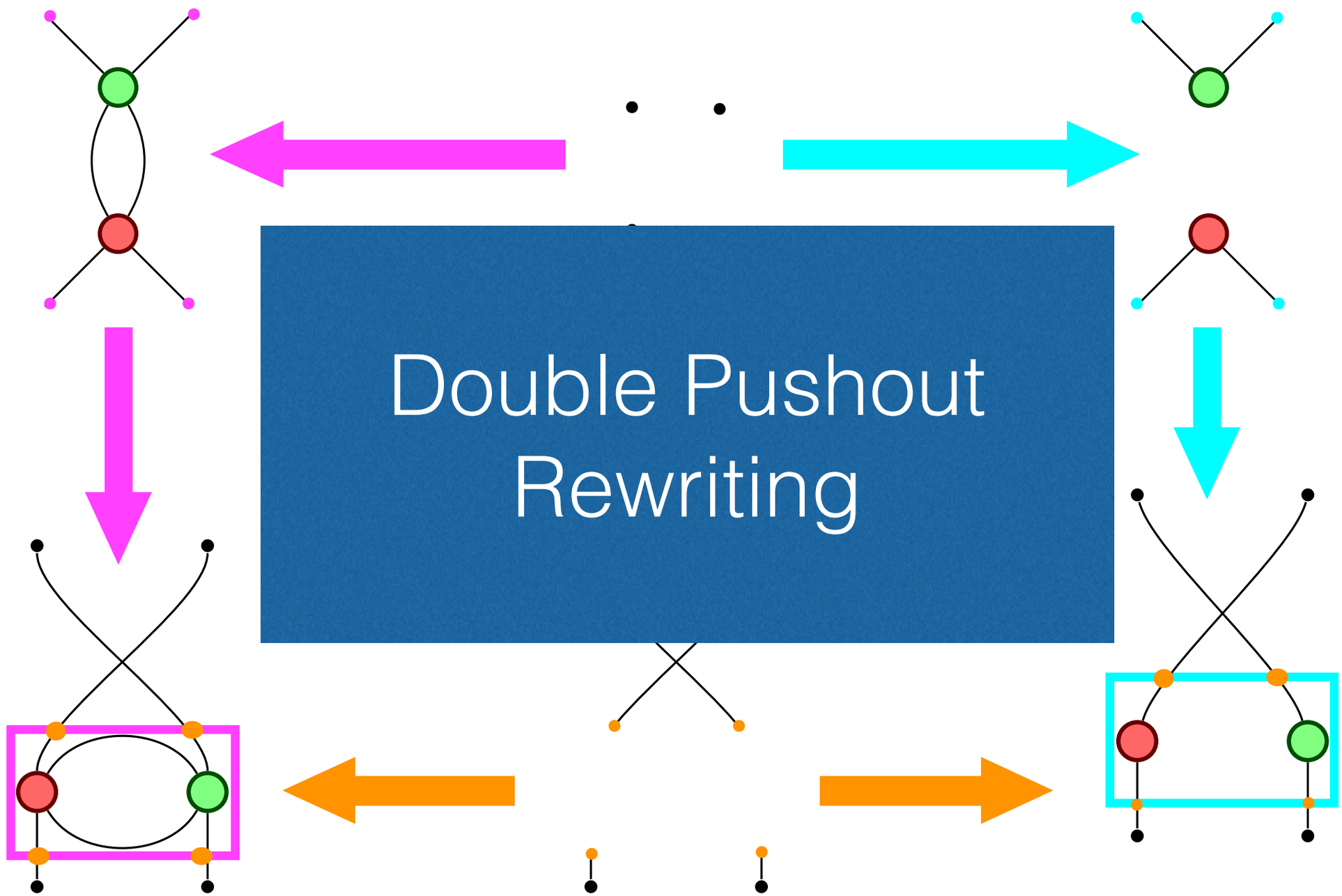
Equational Reasoning



Equational Reasoning

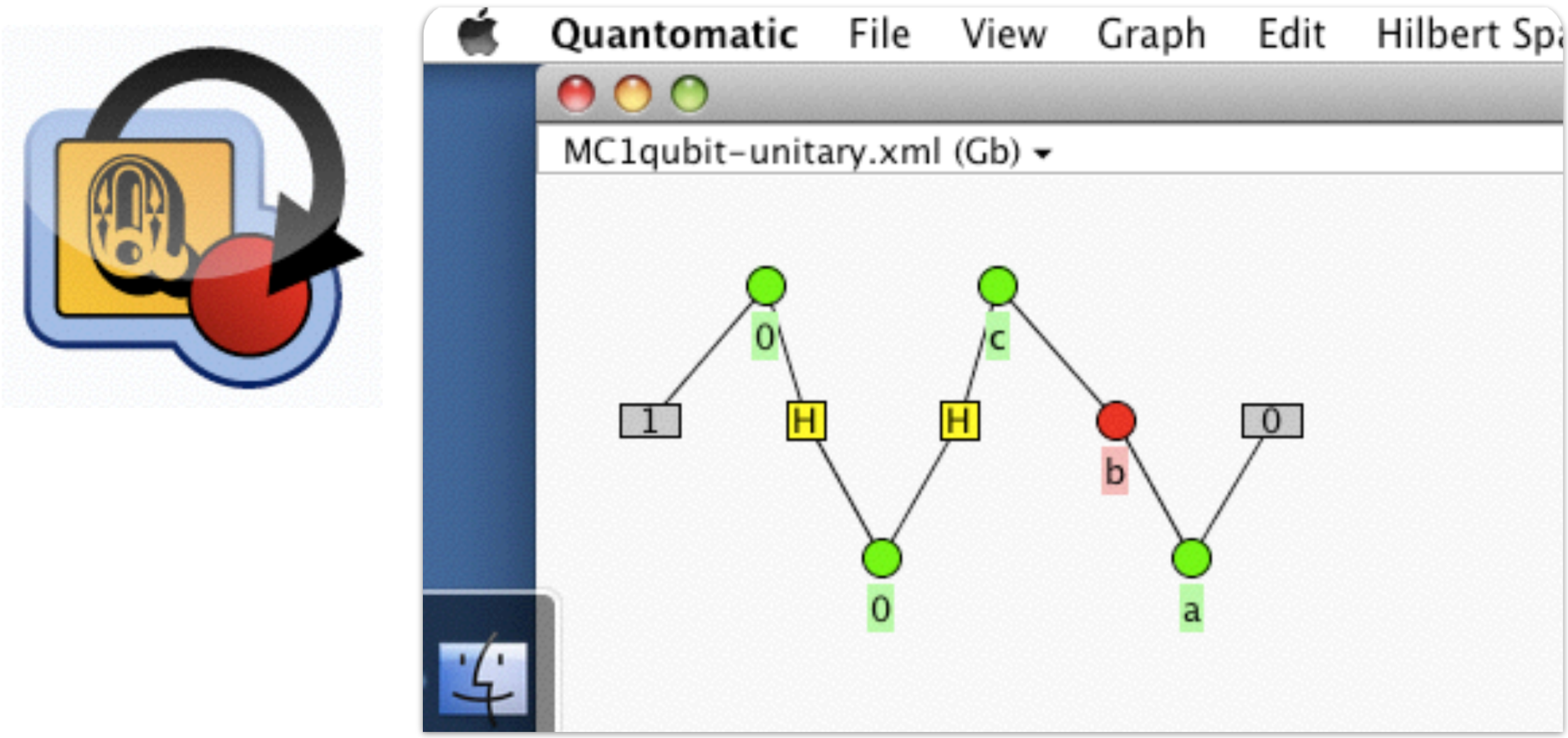


Equational Reasoning



Advertising

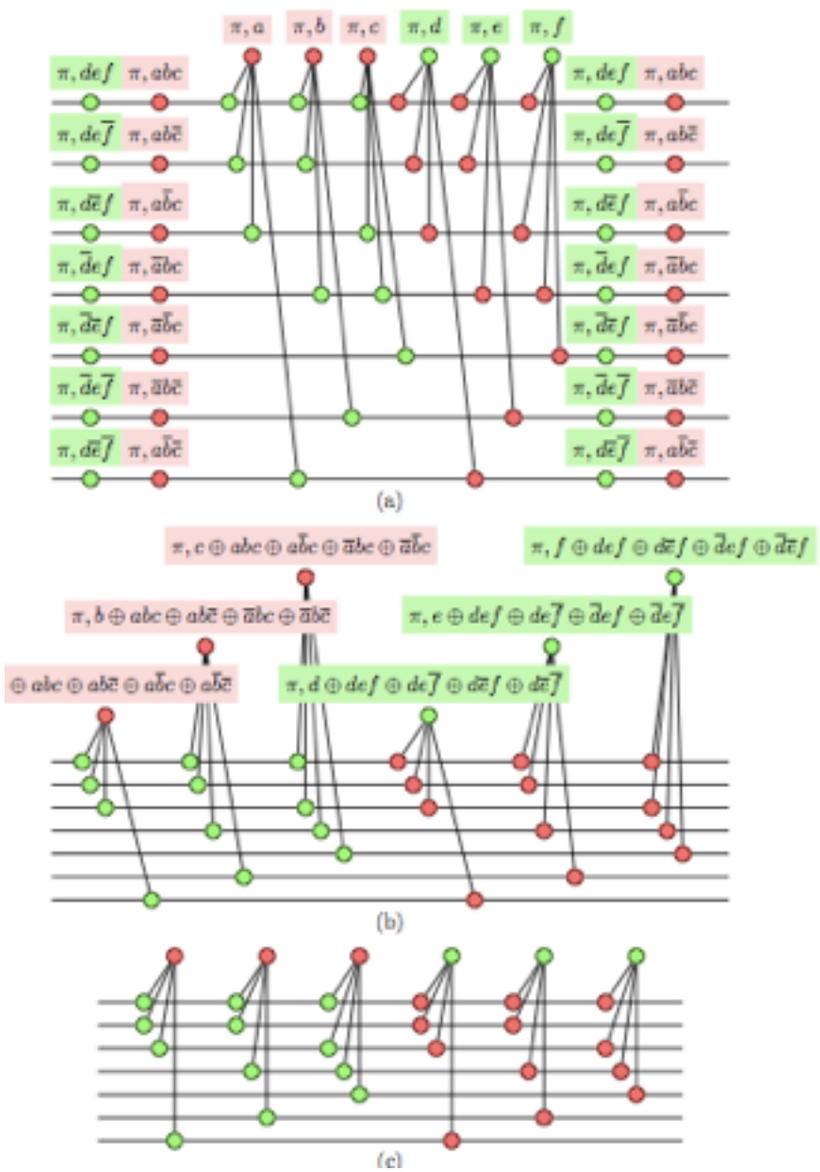
Graphical tool for doing graphical calculations:

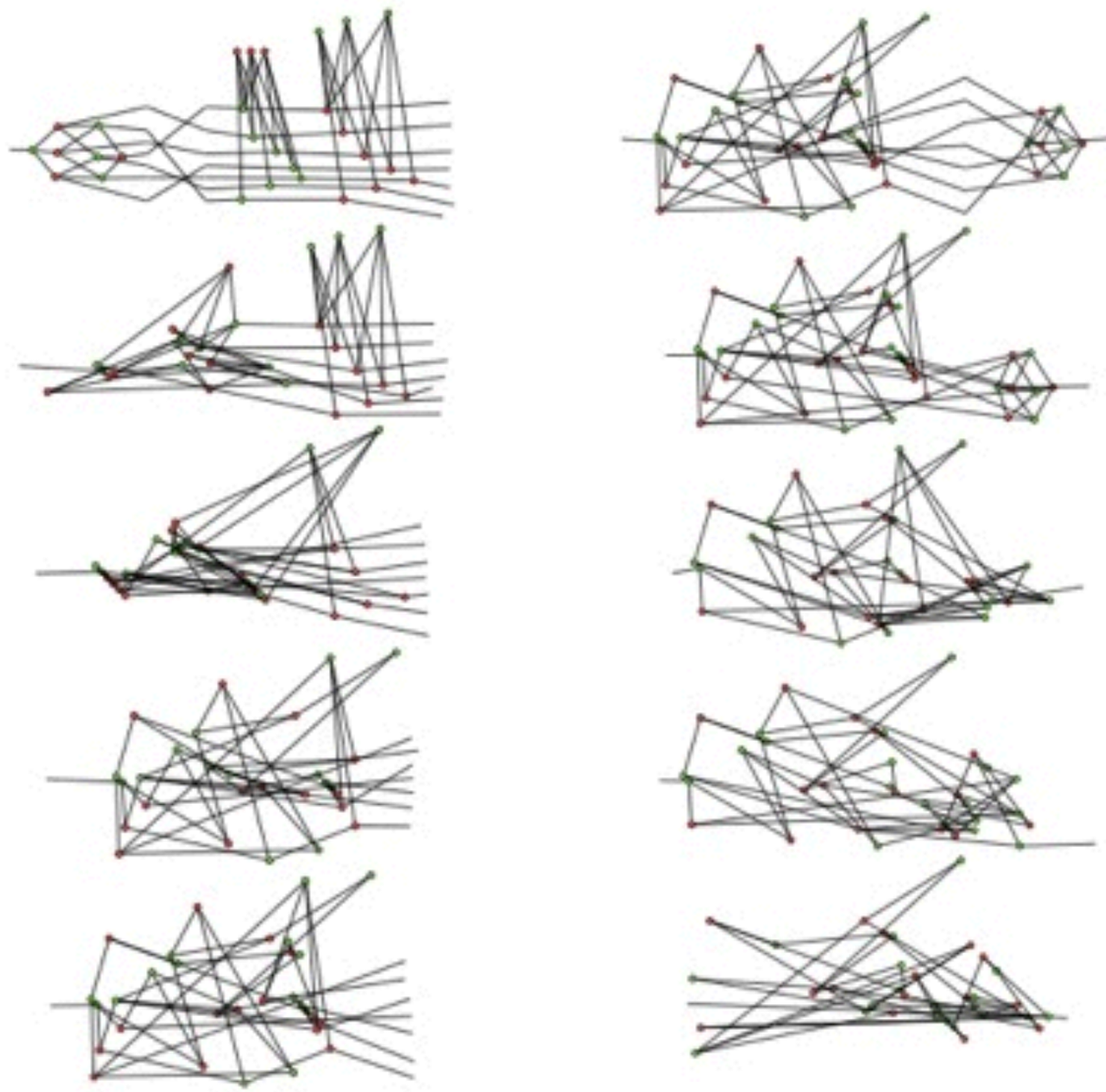


http://quantomatic.github.io

Application: QECC

ZX-calculus can demonstrate the correctness Quantum Error Correcting Codes:



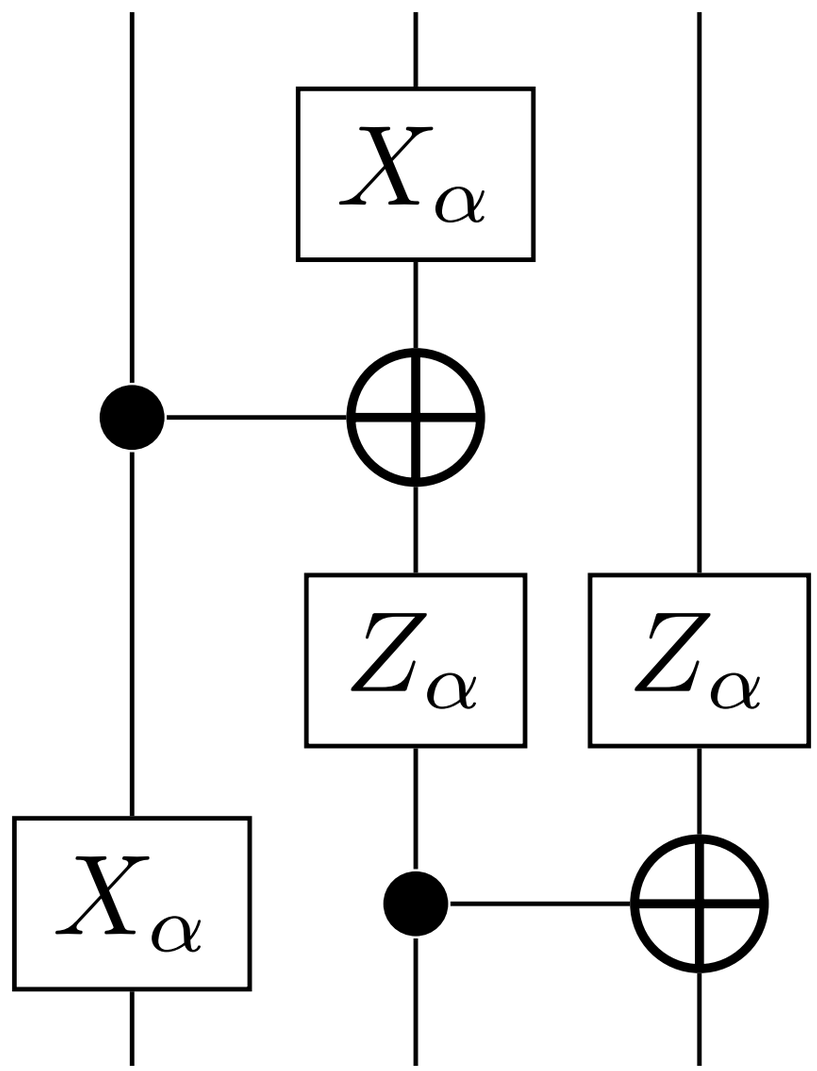


5.

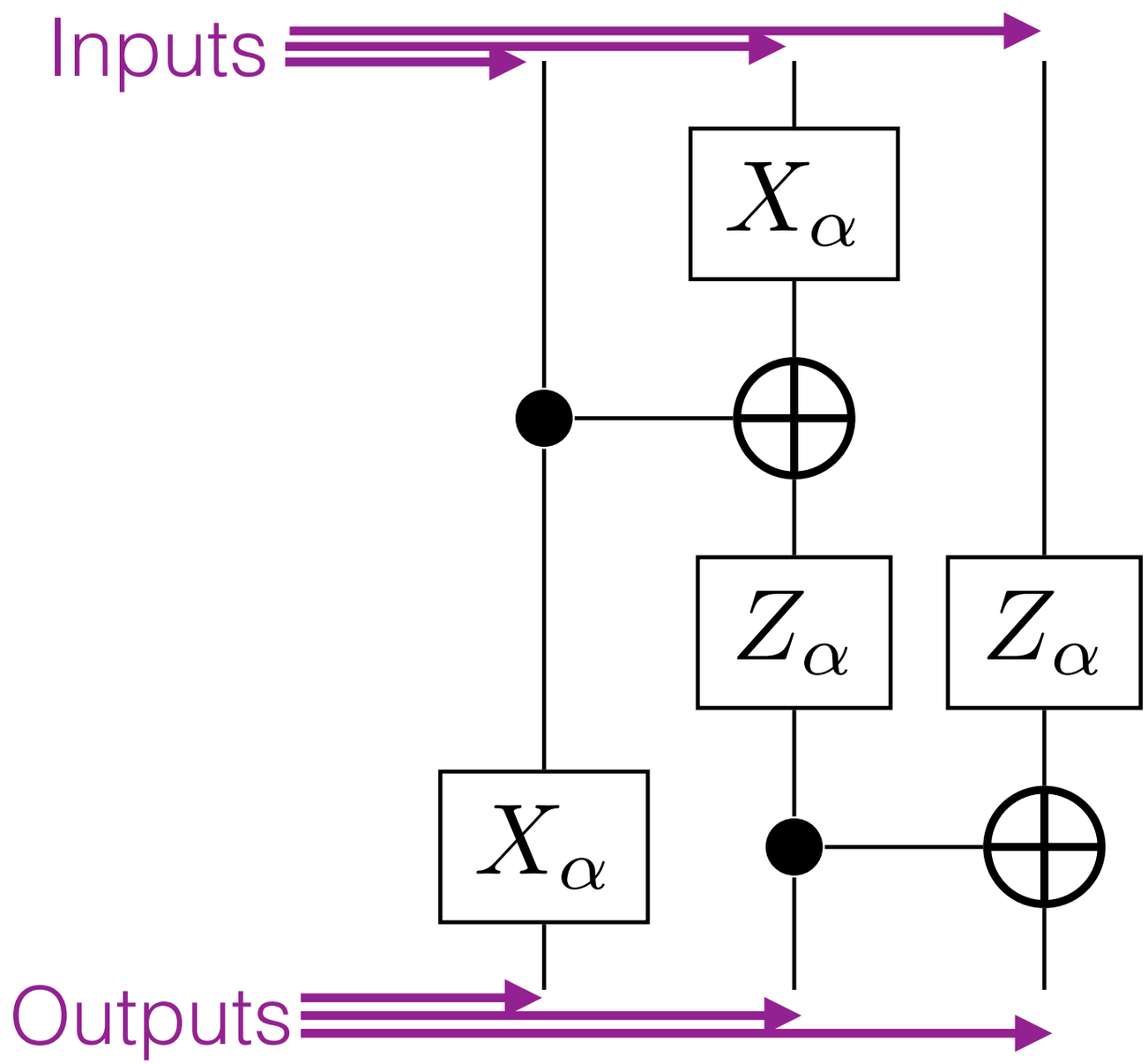
Compiling.

Oh look category theory can do something useful

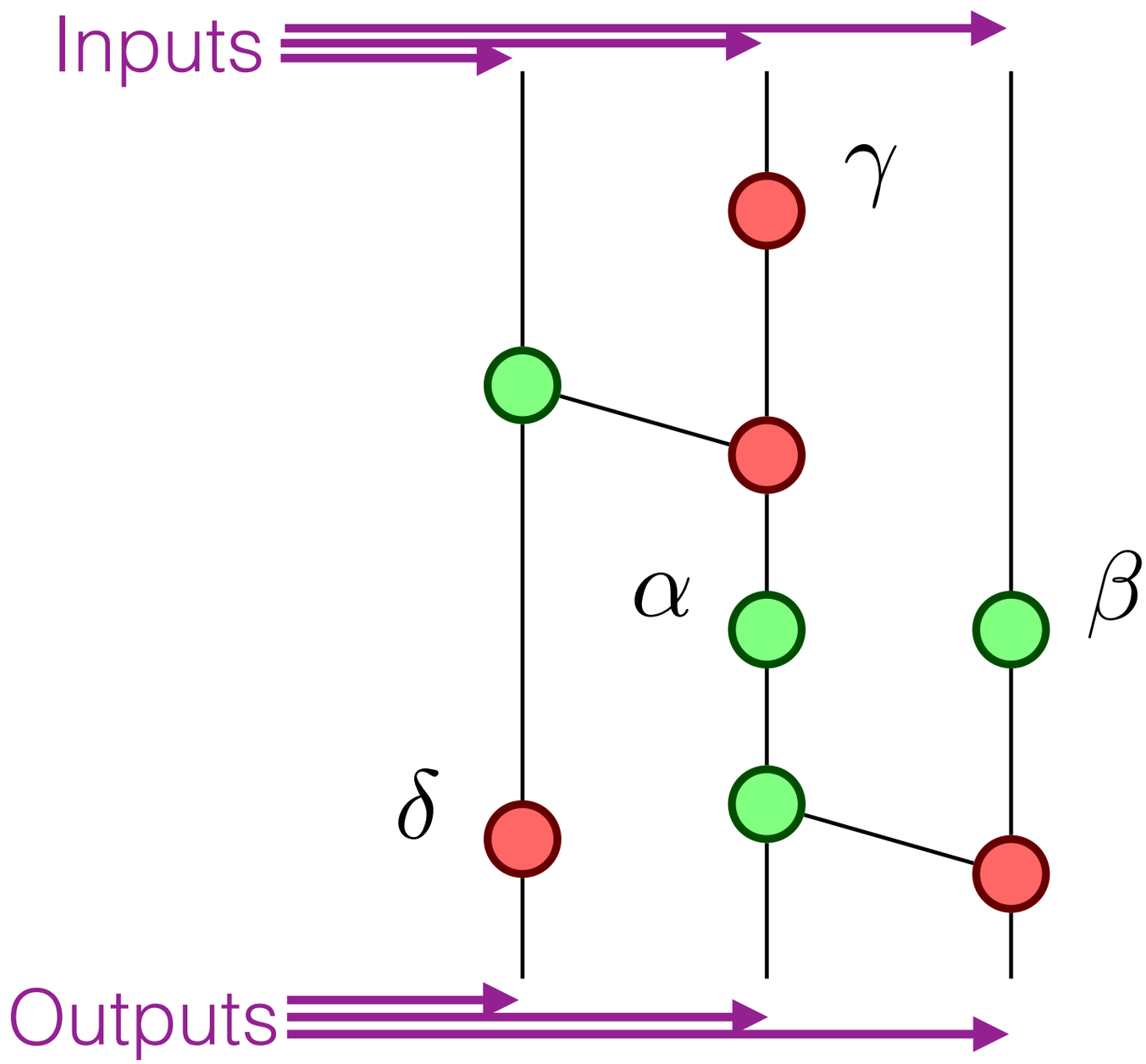
Circuit Perspective



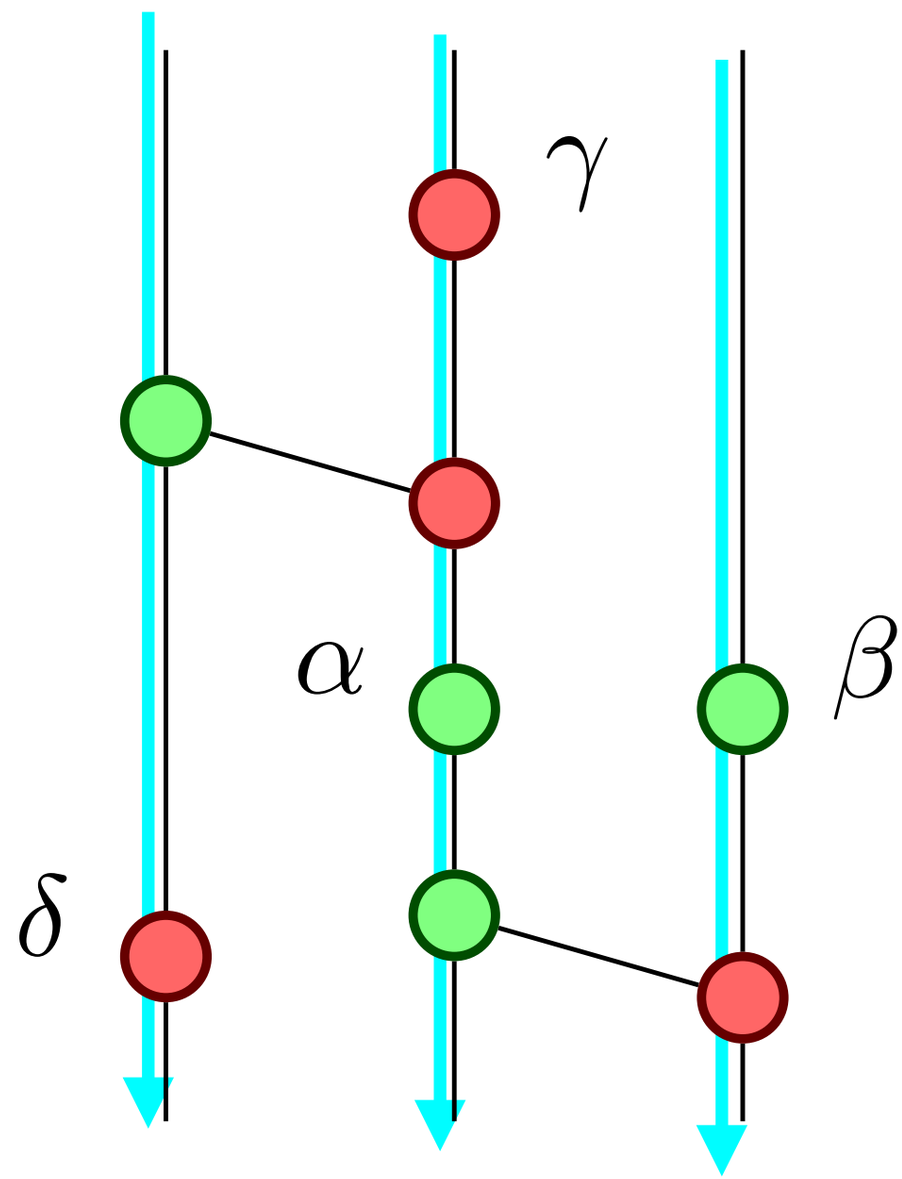
Circuit Perspective



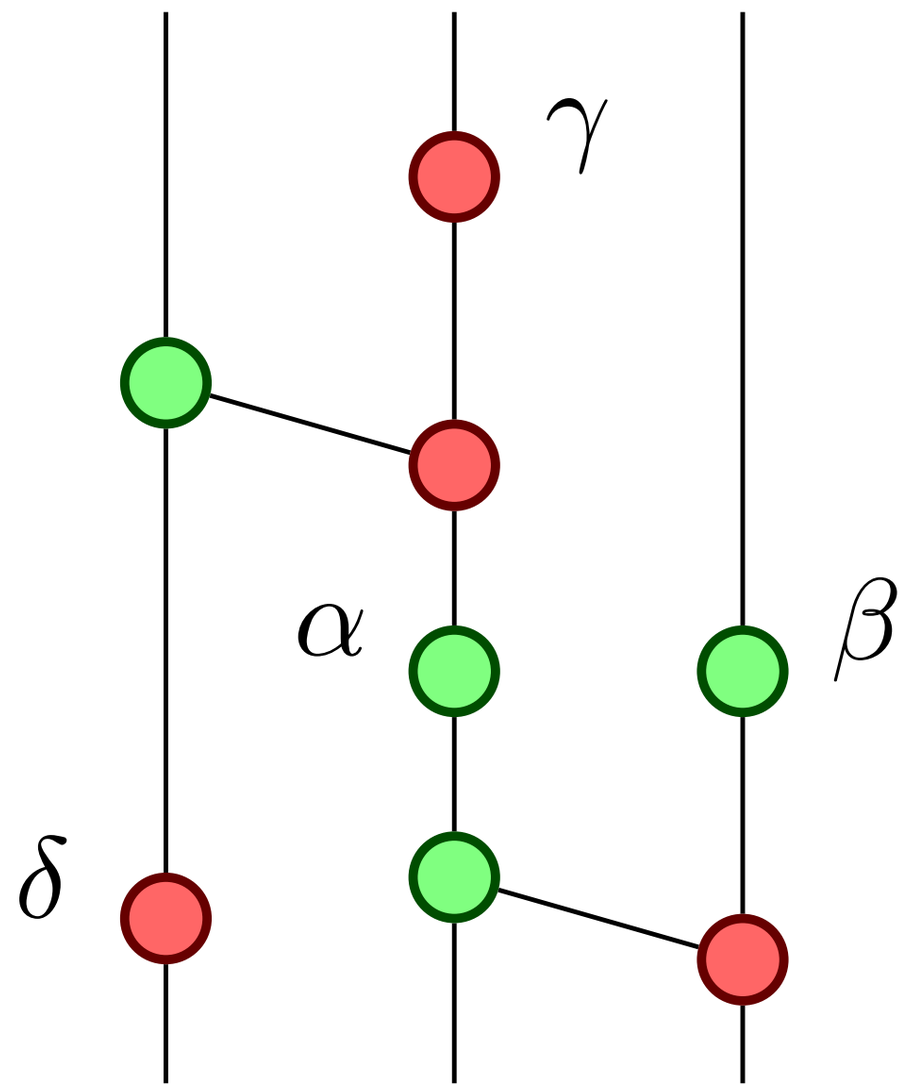
Circuit Perspective



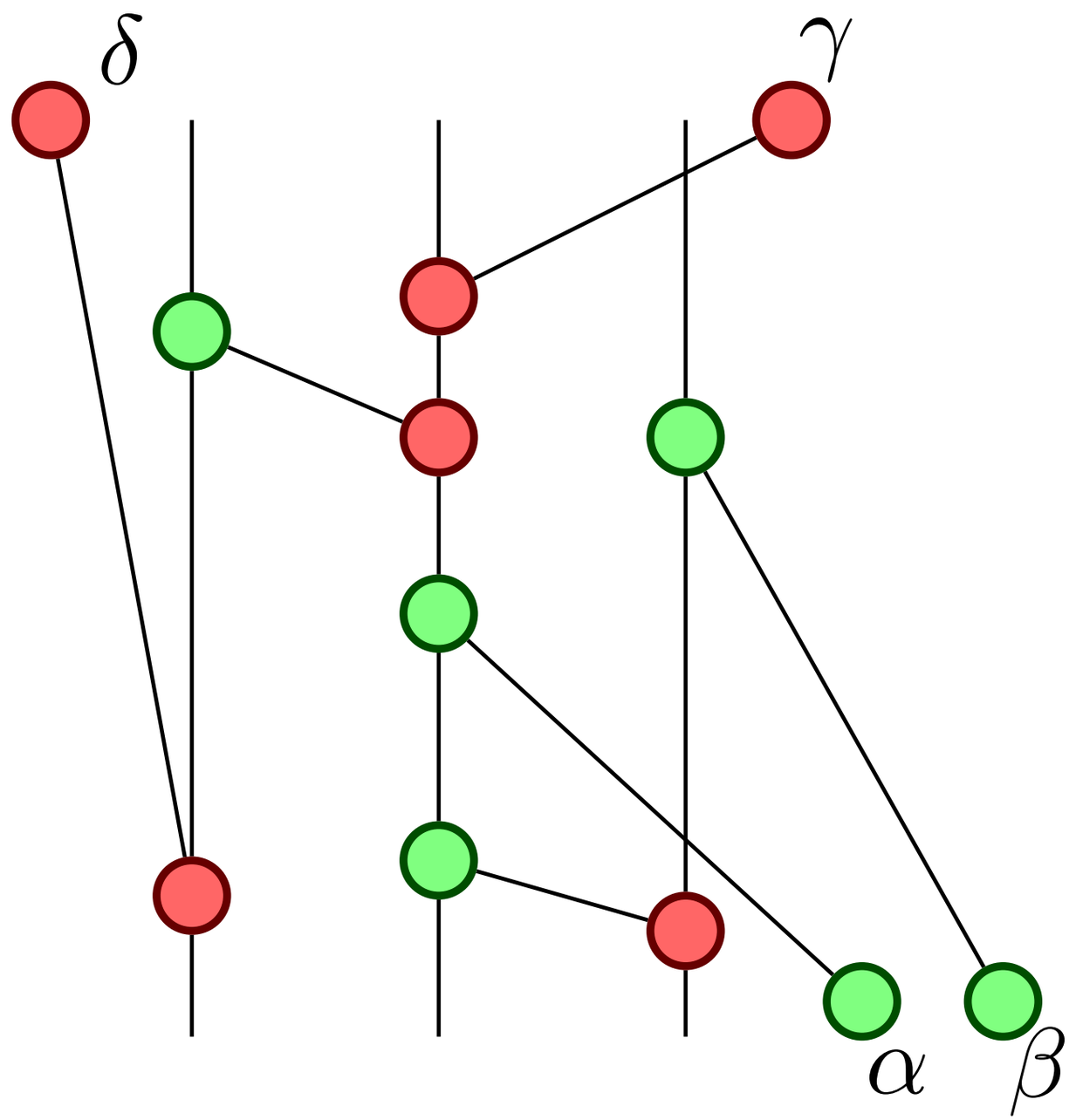
Circuit Perspective



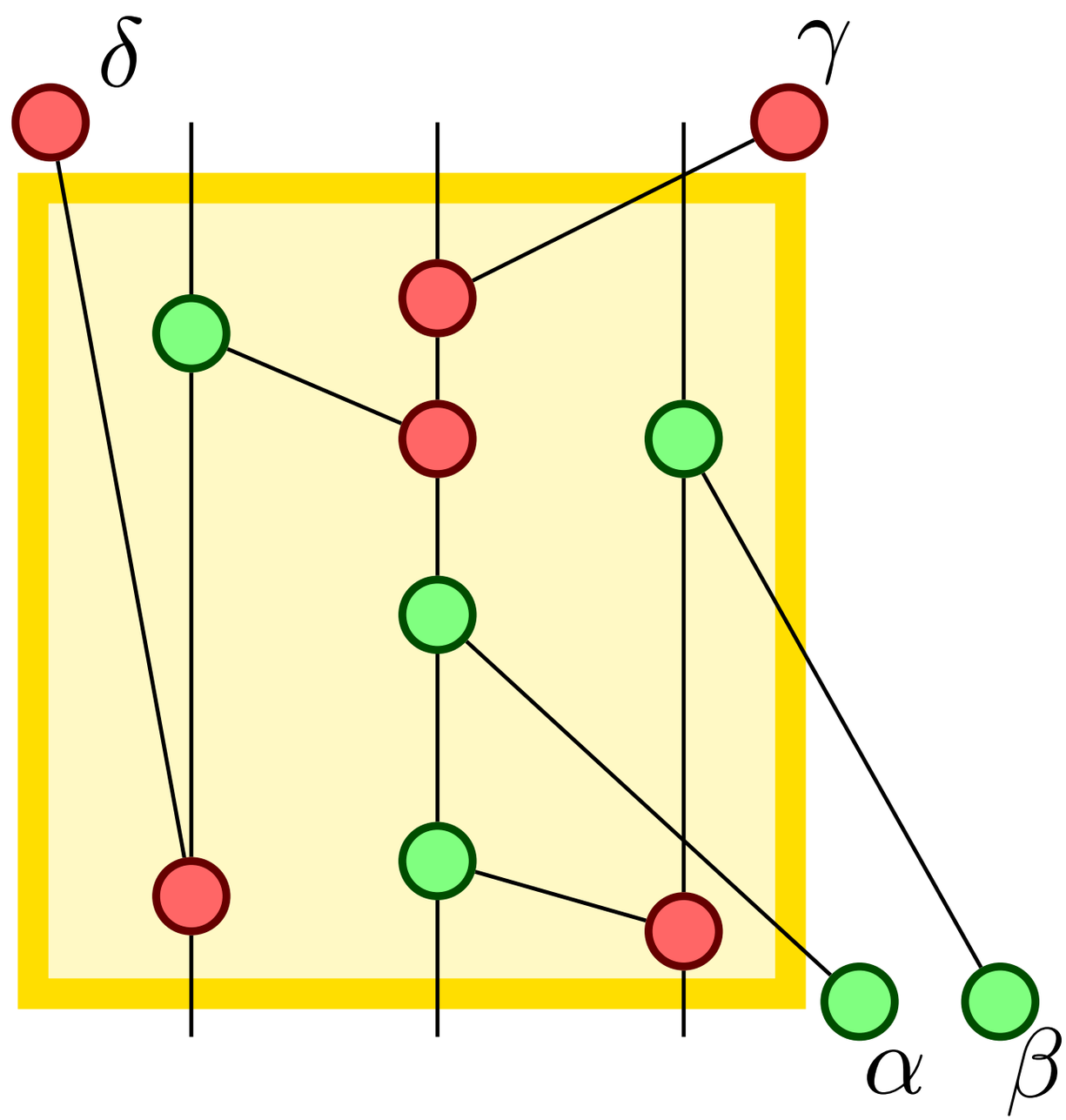
Circuit Perspective



??? Perspective

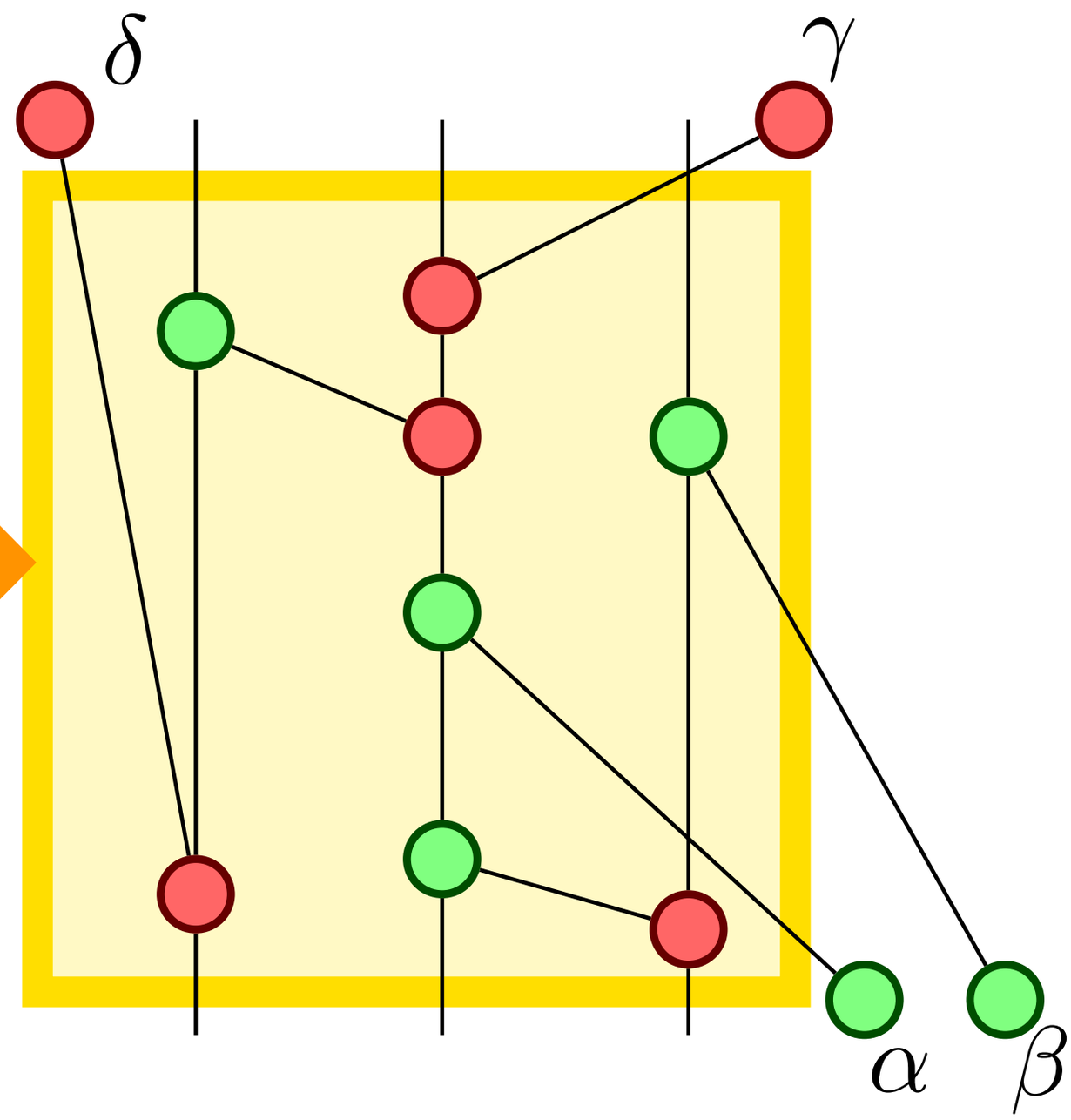


??? Perspective



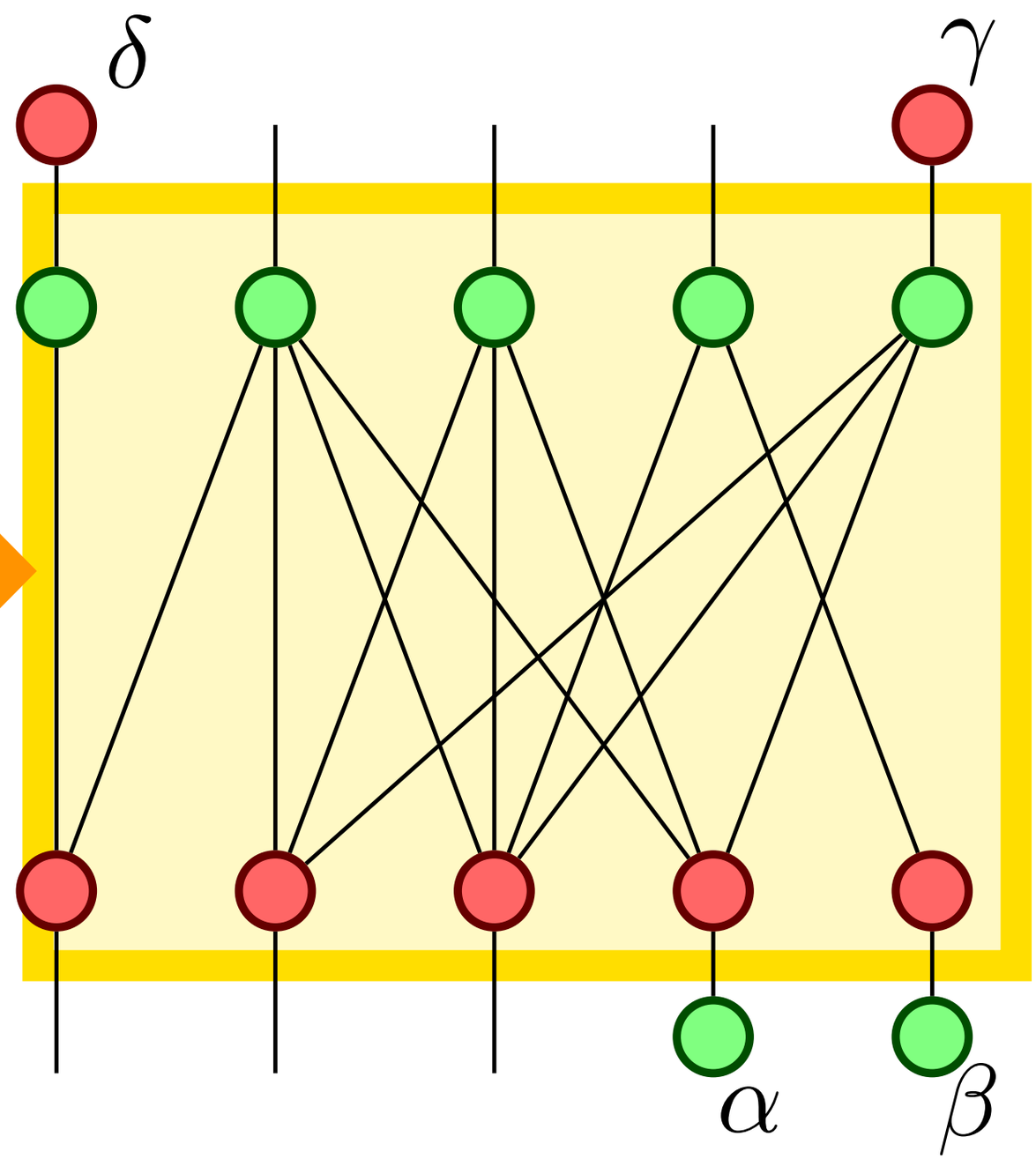
??? Perspective

Hopf algebra expression

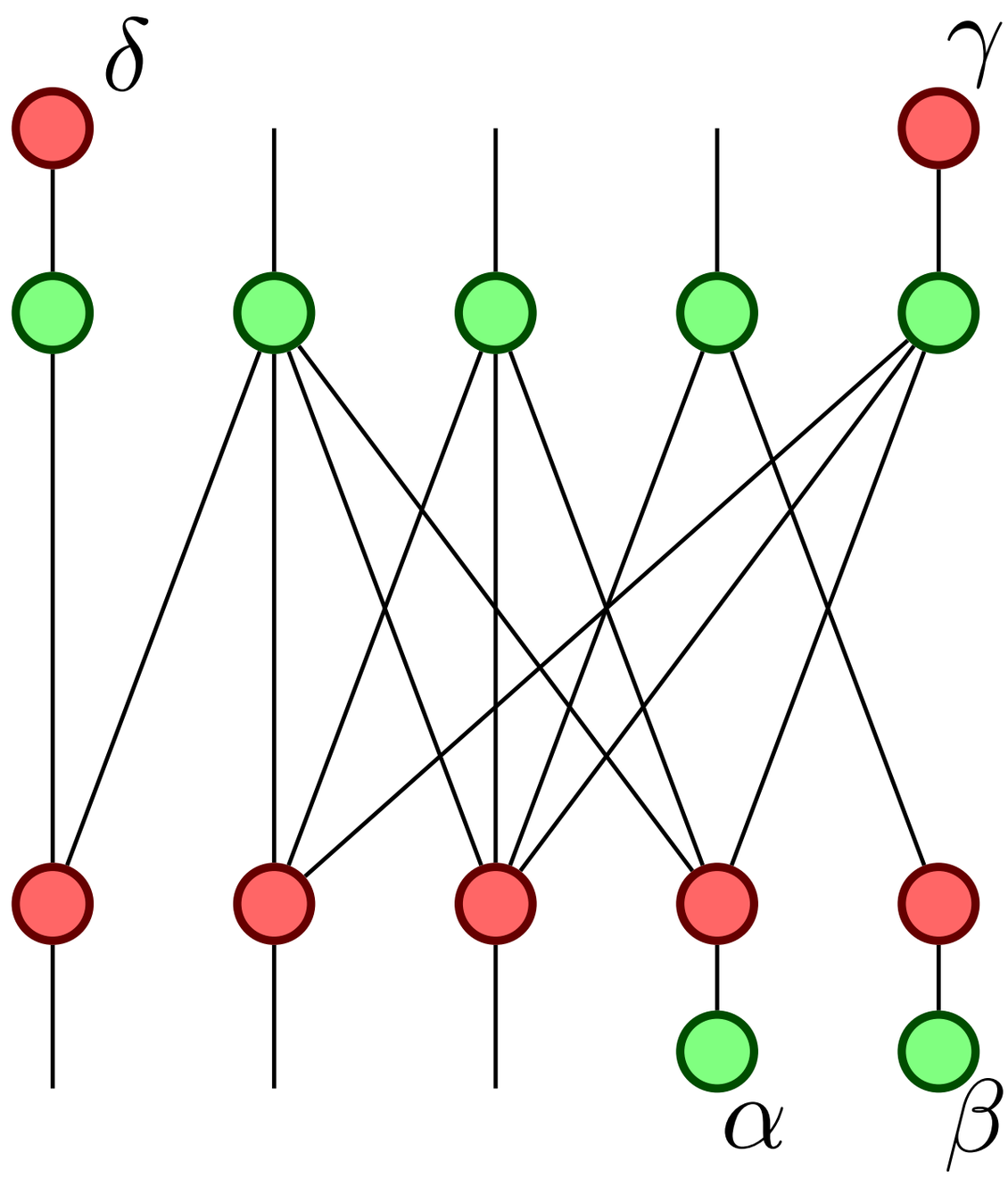


??? Perspective

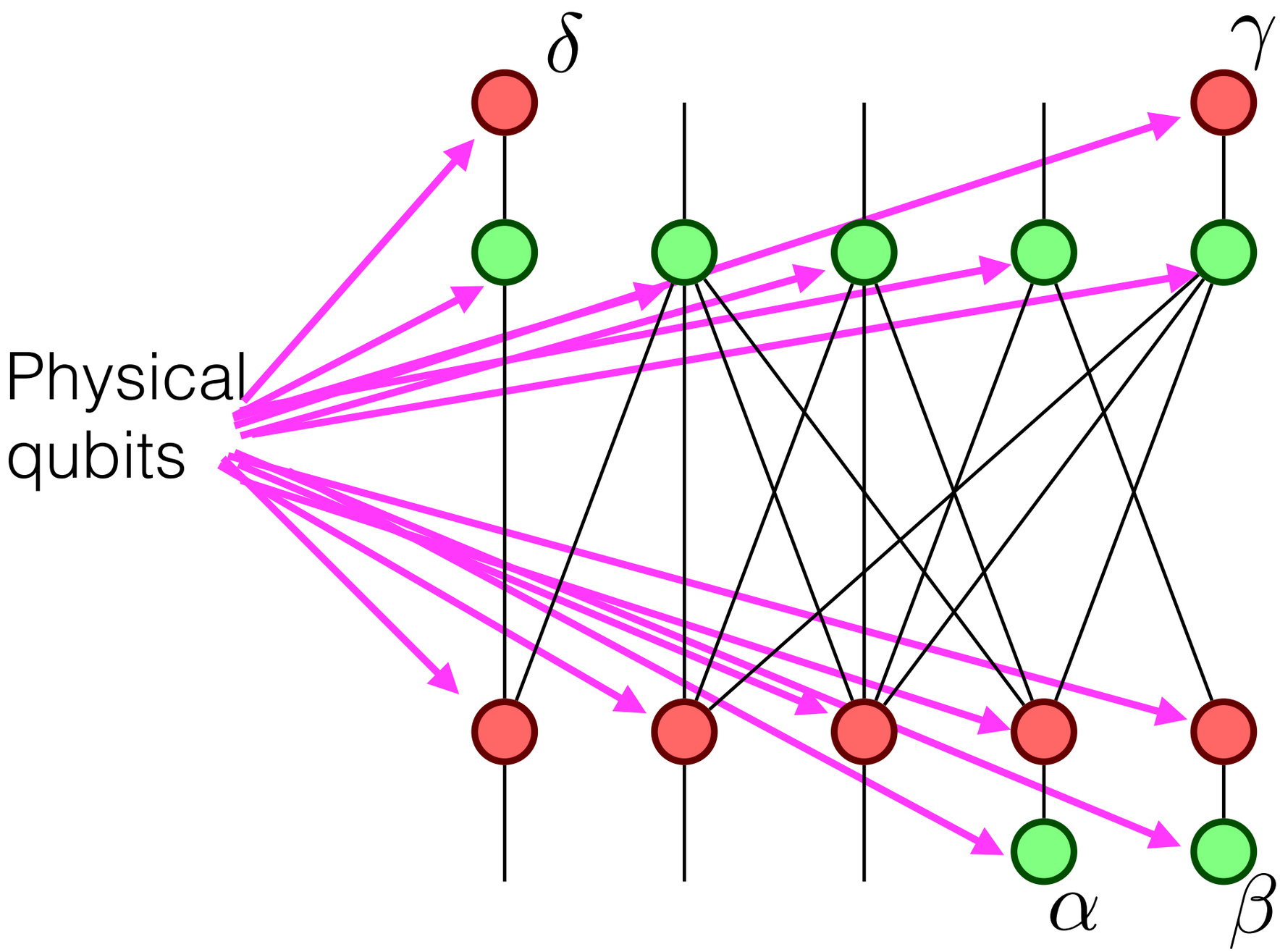
Hopf algebra
normal form



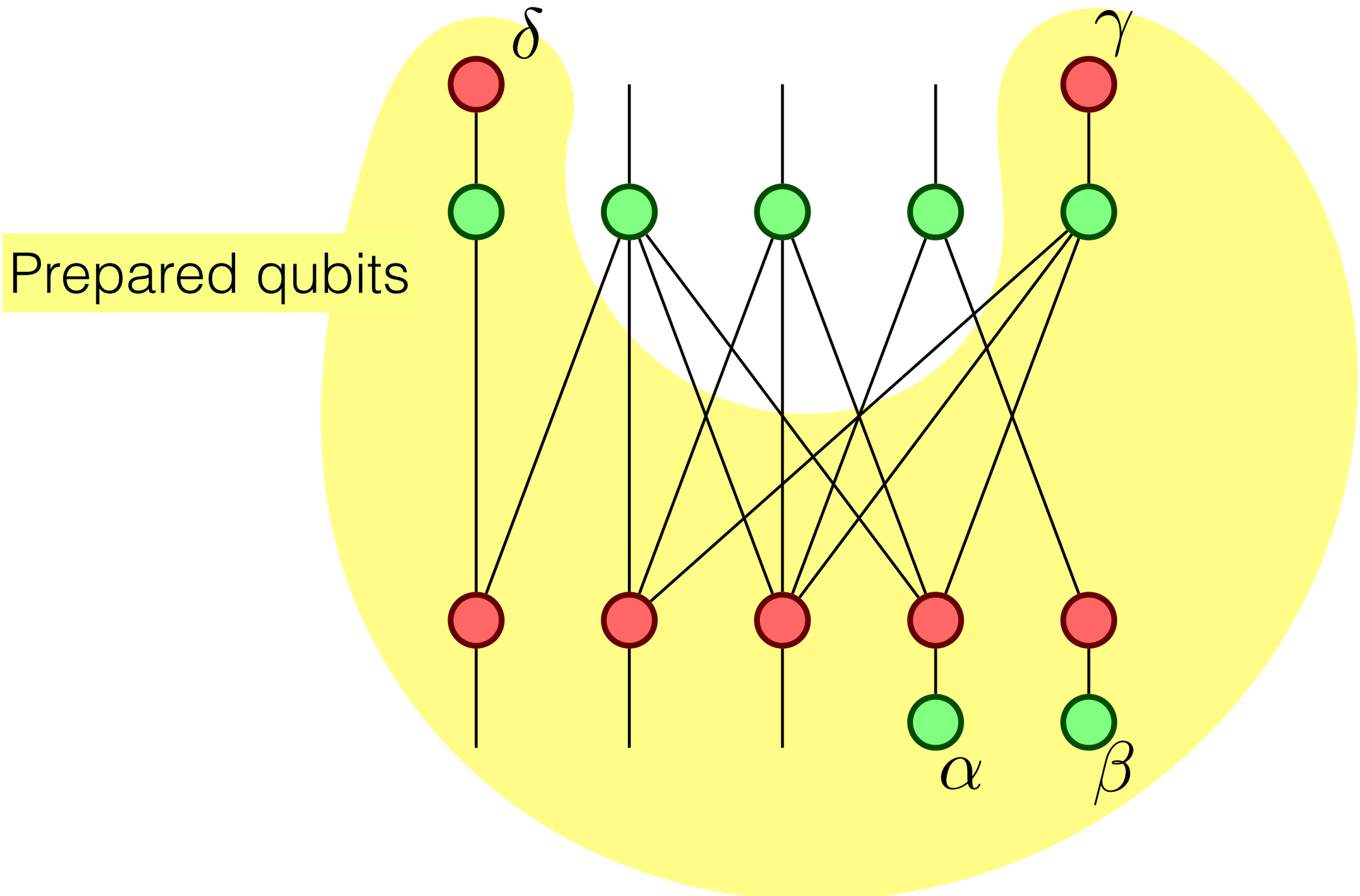
MBQC Perspective



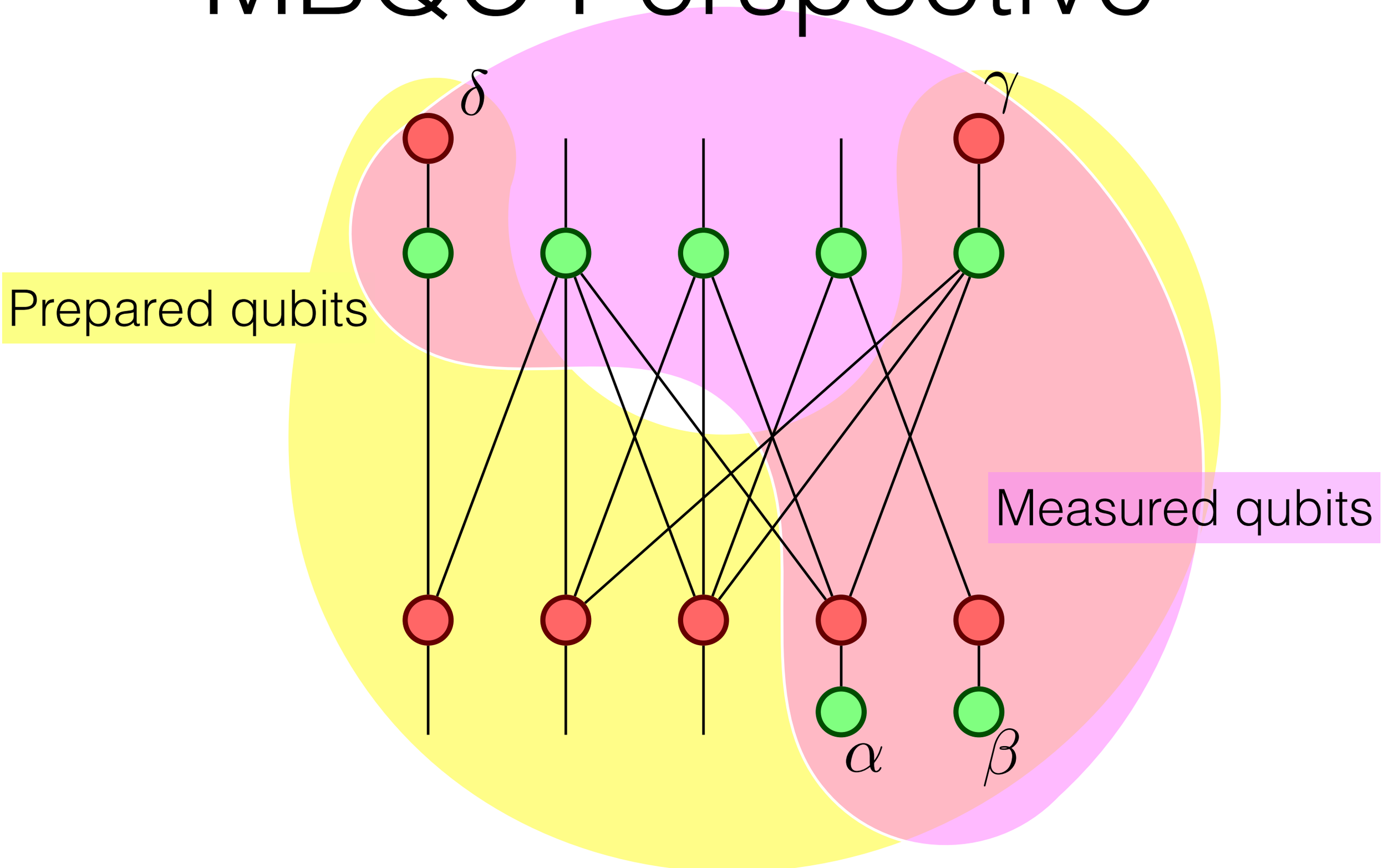
MBQC Perspective



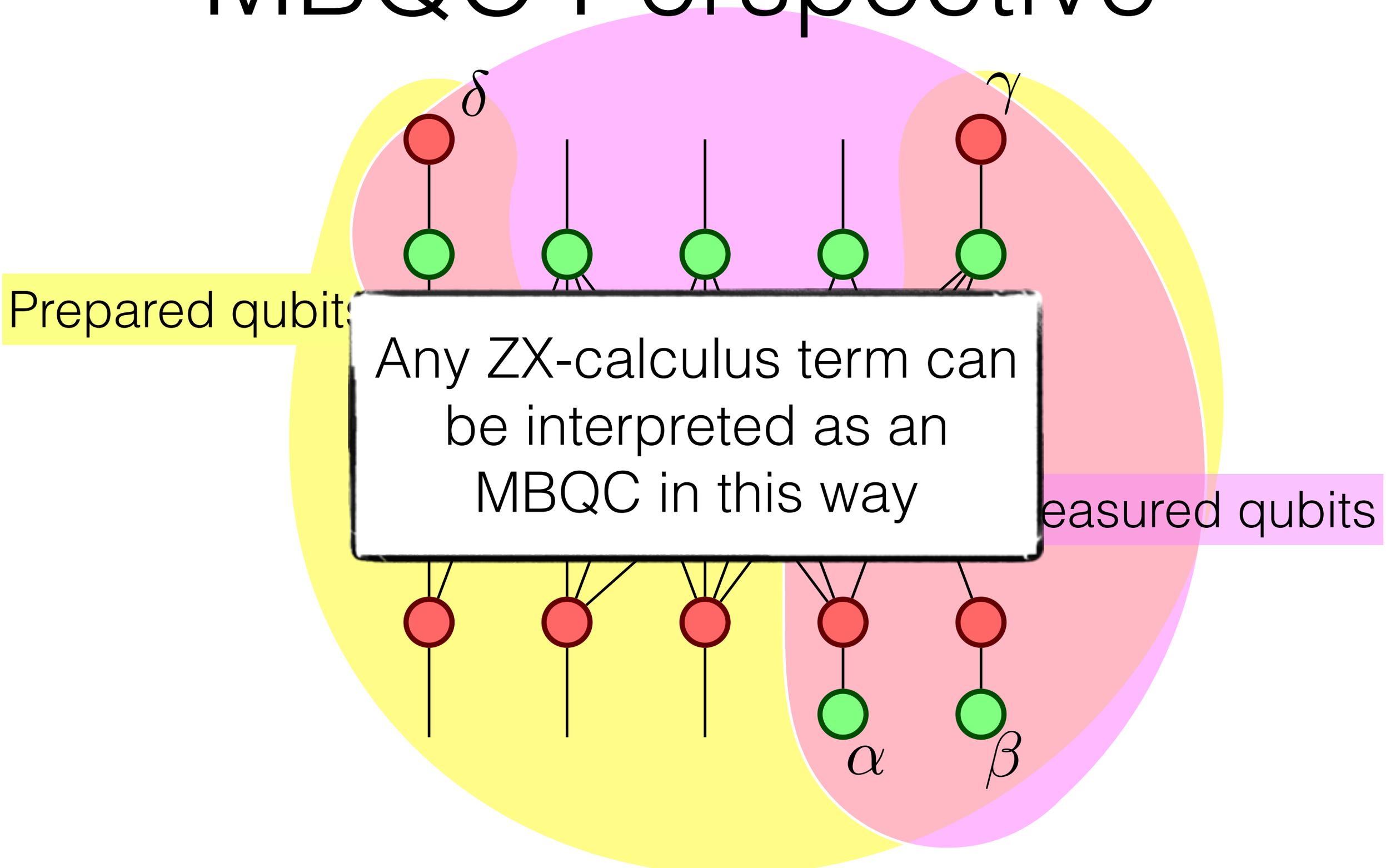
MBQC Perspective



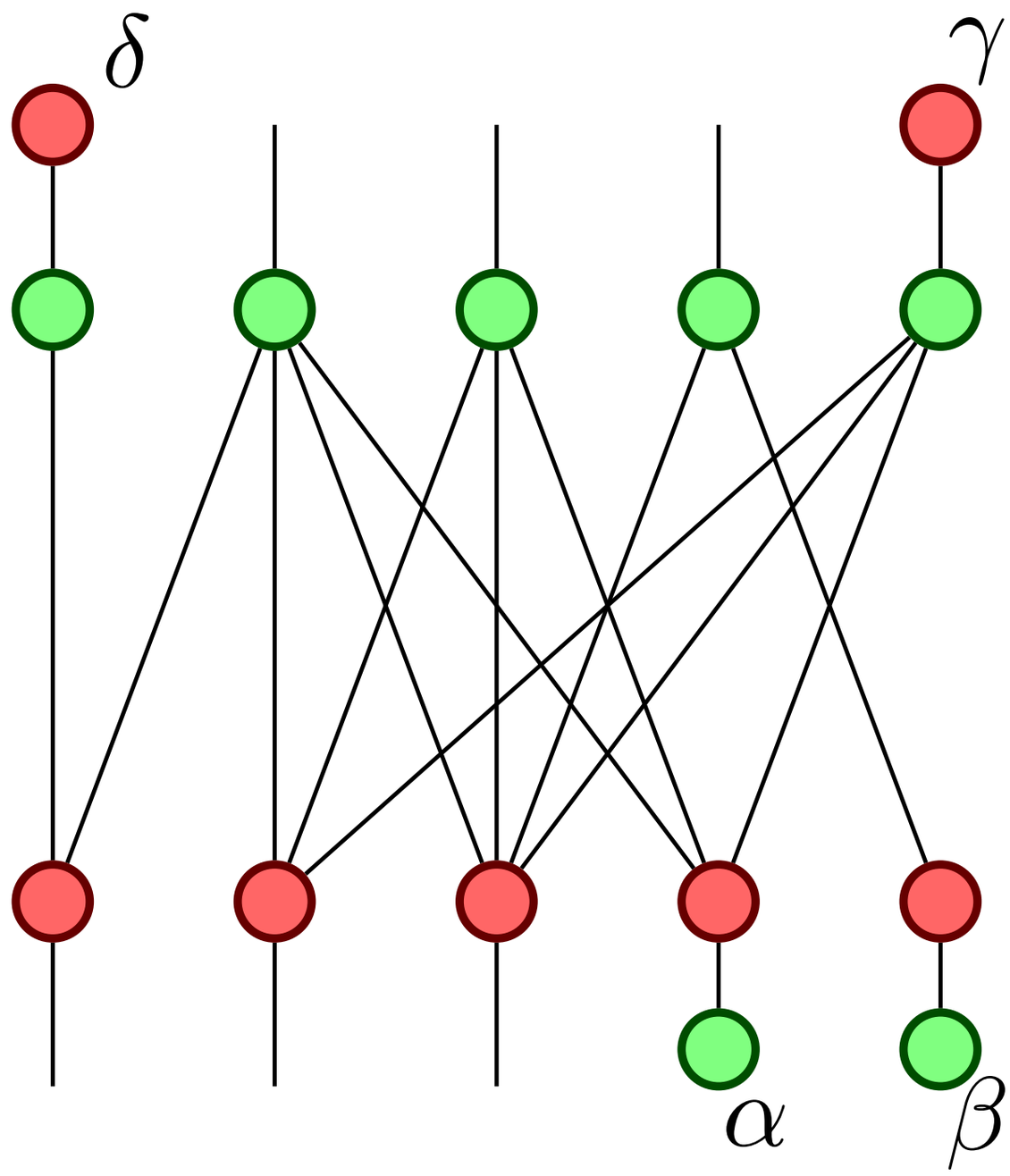
MBQC Perspective



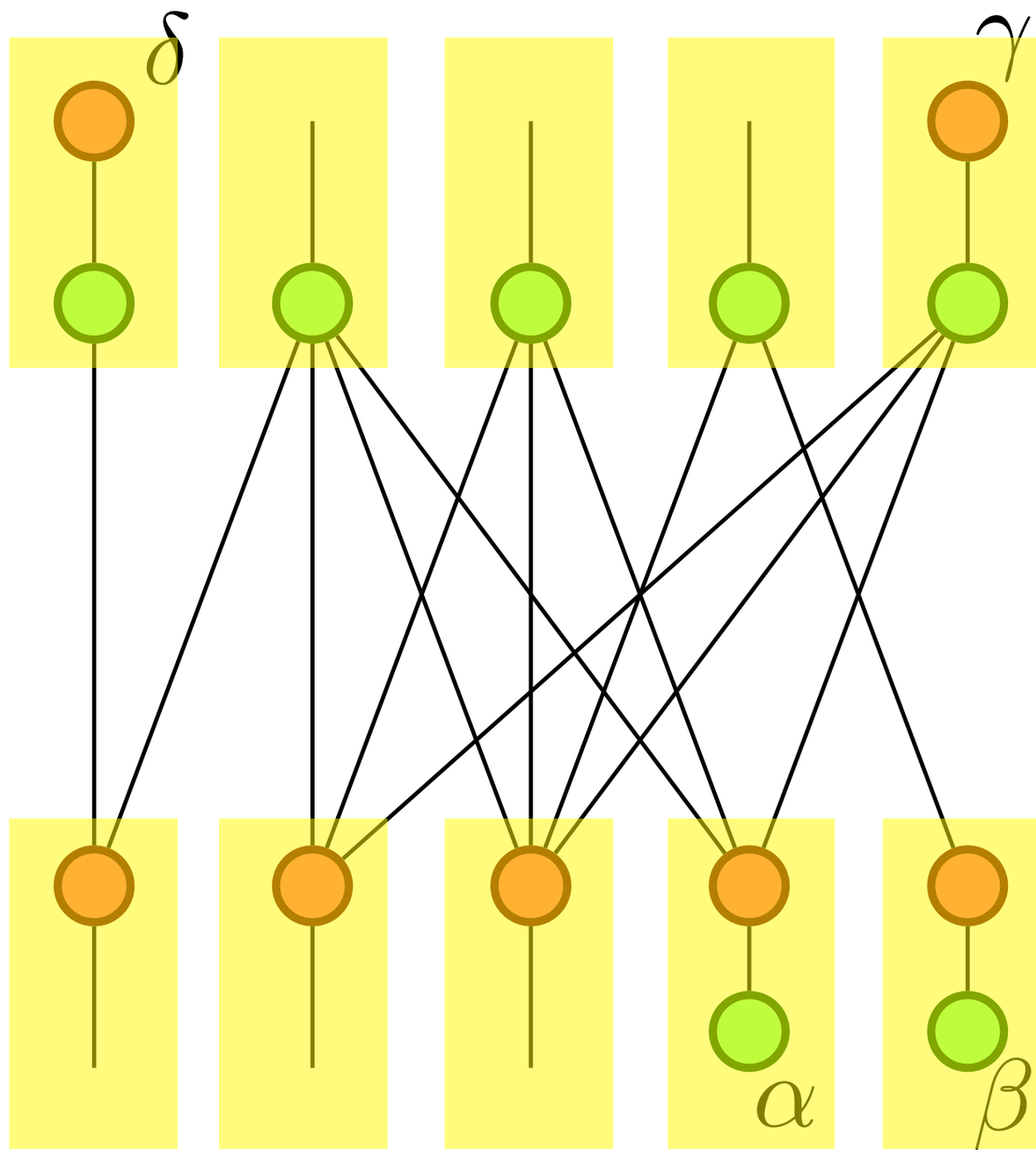
MBQC Perspective



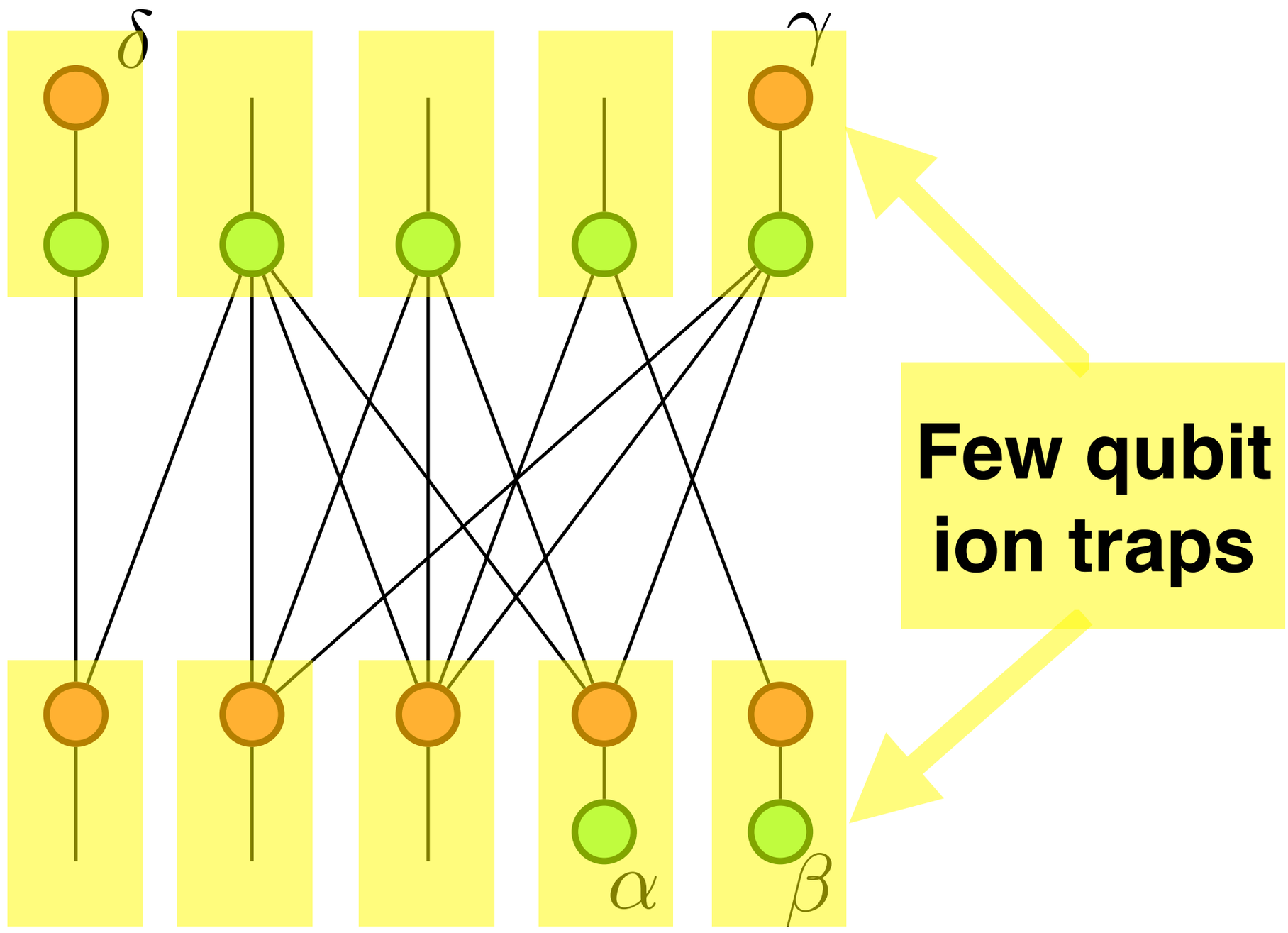
NQIT Perspective



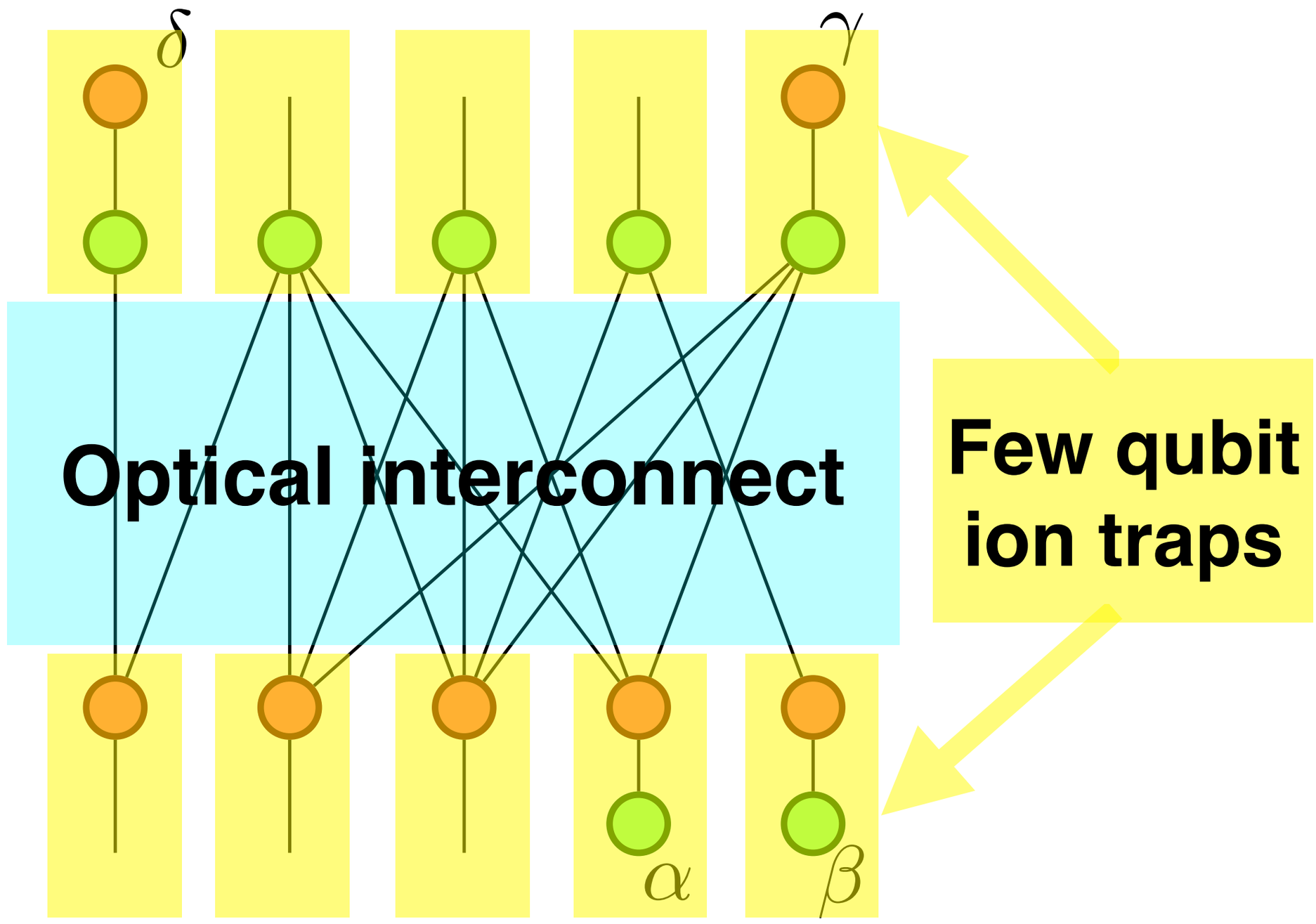
NQIT Perspective



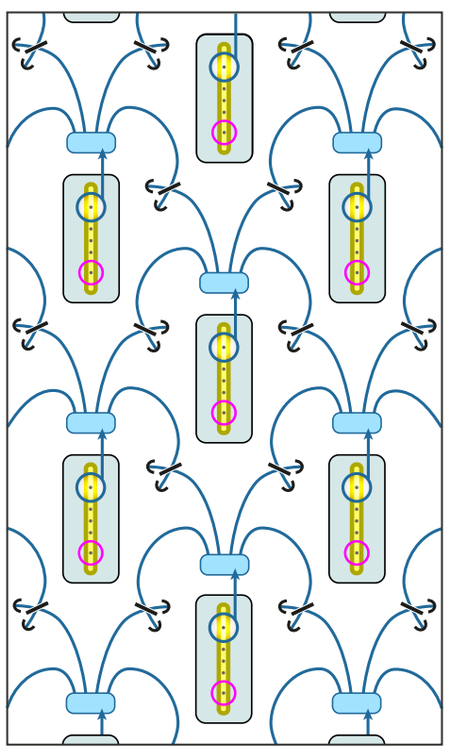
NQIT Perspective

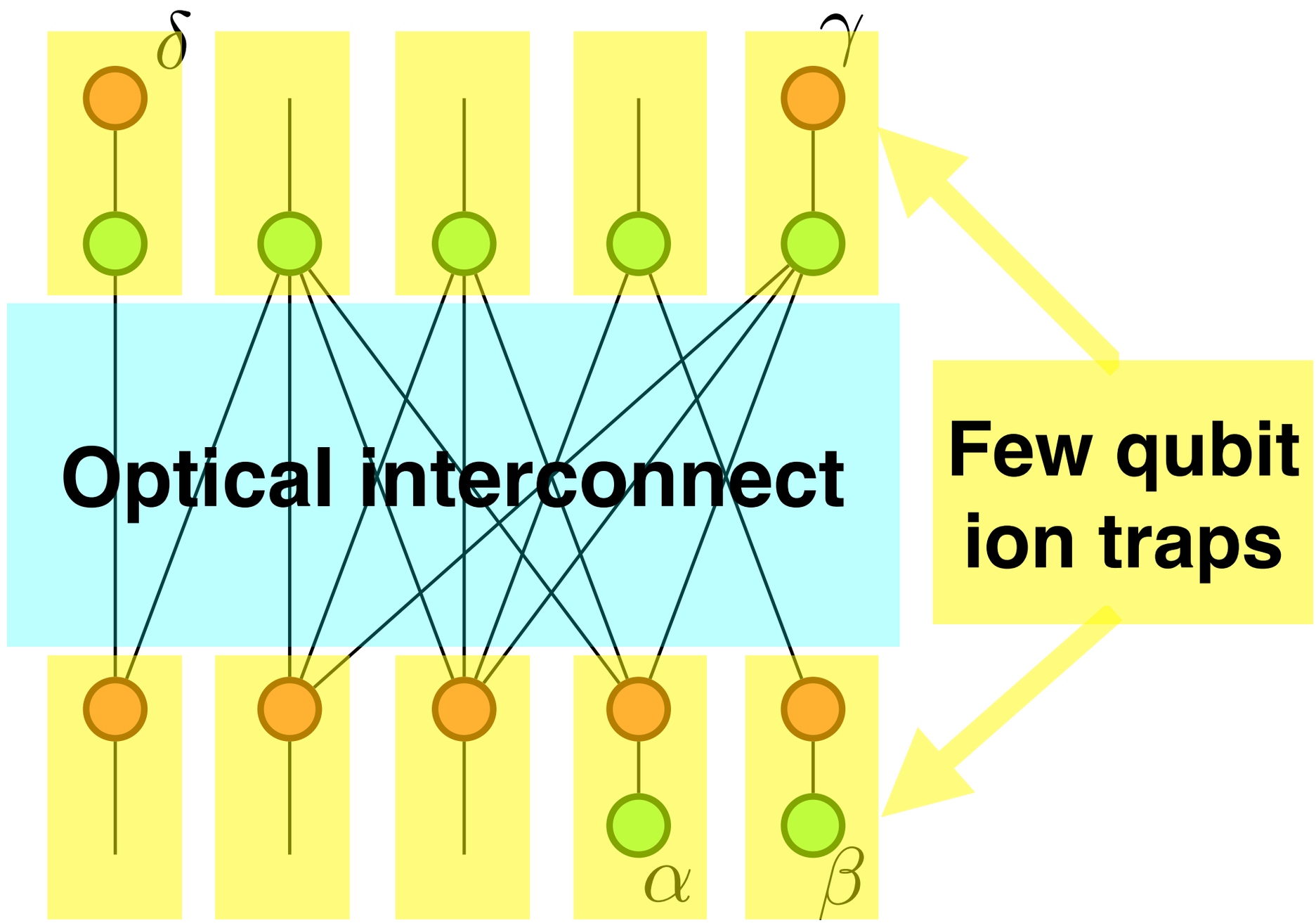


NQIT Perspective



NQIT Perspective





SUMMARY

- Quantum computing needs a different logico-algebraic basis to classical computing.
- Categorical analysis of concepts of QM reveals the key structures behind algorithms etc
- Diagrammatic syntax and DPO rewriting give tools to work efficiently with this theory
- New structural insights give new approaches and techniques to working with quantum computers