Verifying Quantum Computations with the ZX-calculus

Ross Duncan

University of Strathclyde Glasgow

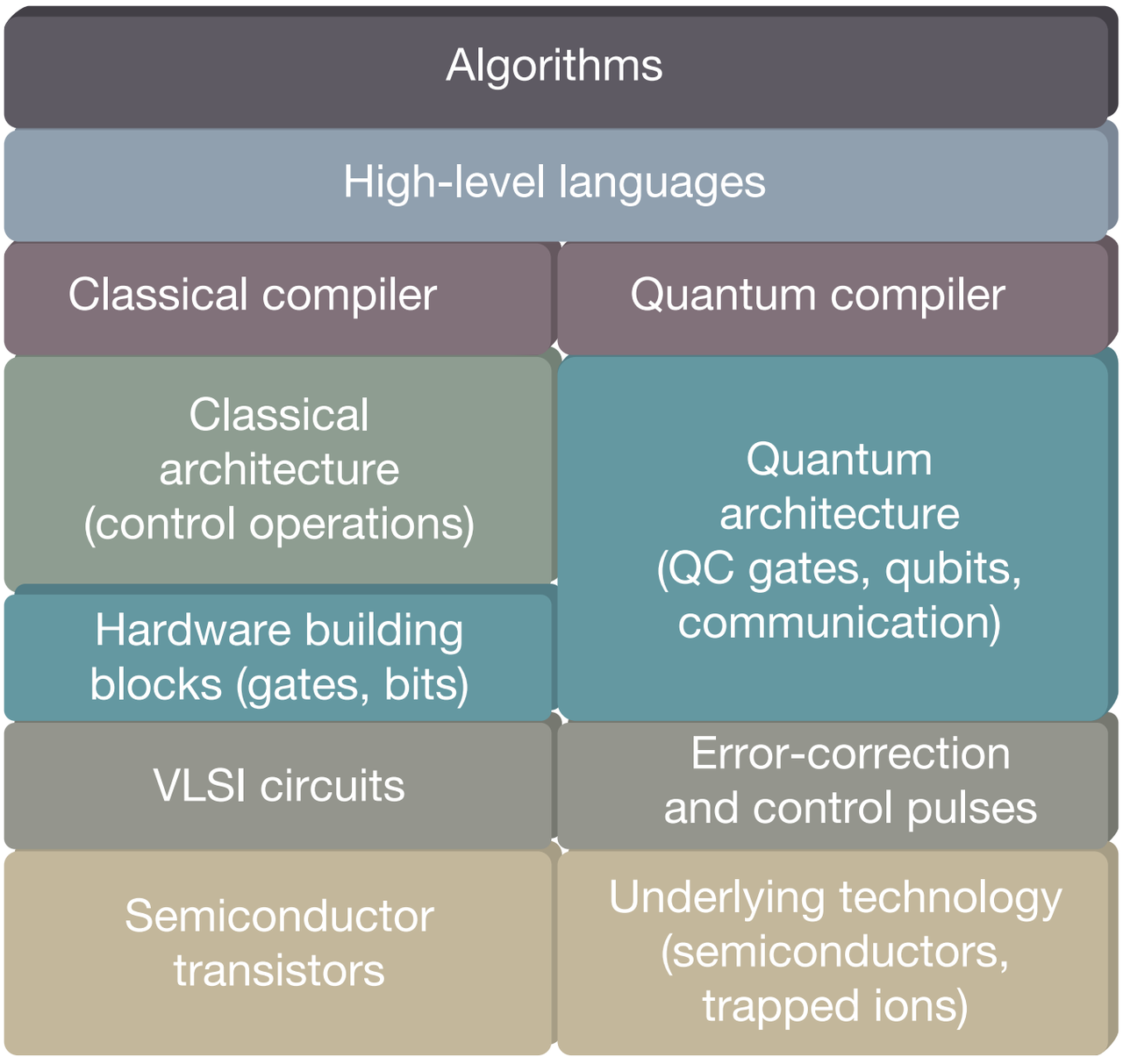
0.

Motivations

“Verifying”

- **Not** verifying that a given computation is *quantum*
- Verifying that your program is *correct:*
  - is the program I *wrote* equivalent to its specification?
  - is the program I *ran* equivalent to the one I wrote?

The Stack



F. T. Chong, D. Franklin, and M. Martonosi. Programming languages and compiler design for realistic quantum hardware. Nature, 549(7671):180–187, 09 2017.

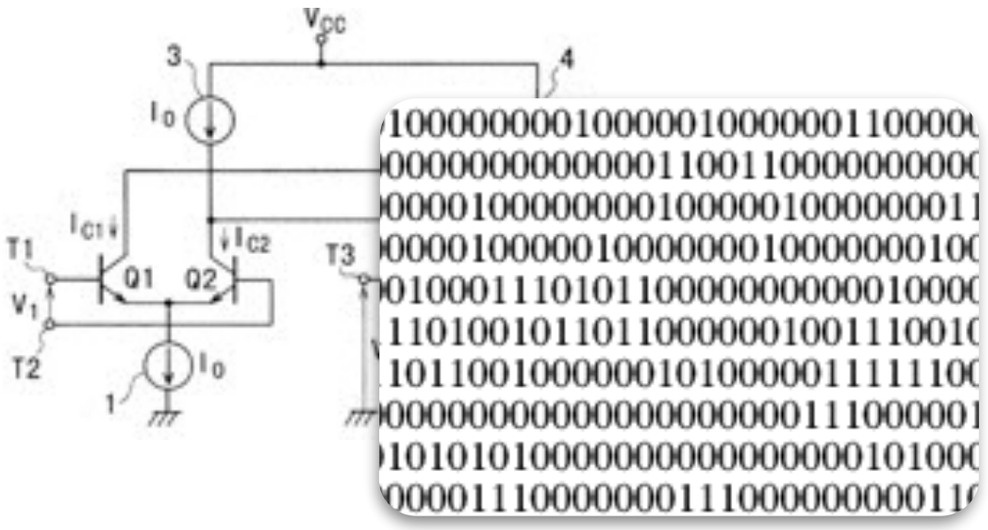
Verifying Quantum Computations

1. No one has any real idea what the architecture of a working QC is going to be — not quantum circuits!

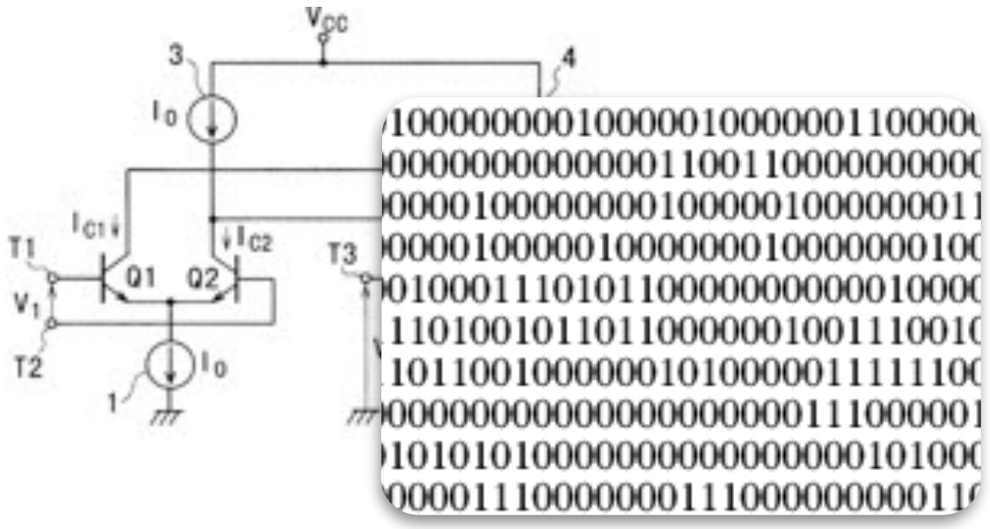
2. Large error-correction overhead will be required — need to deal with this extra layer of complexity

So: the programs we write for QC will not look anything like their implementation — powerful and flexible verification formalisms will be needed!

Motivations



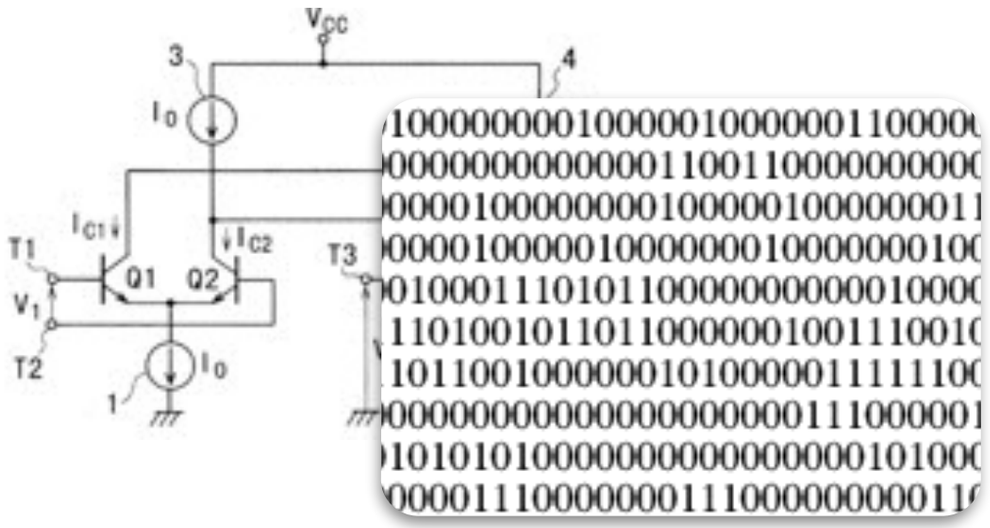
Motivations



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

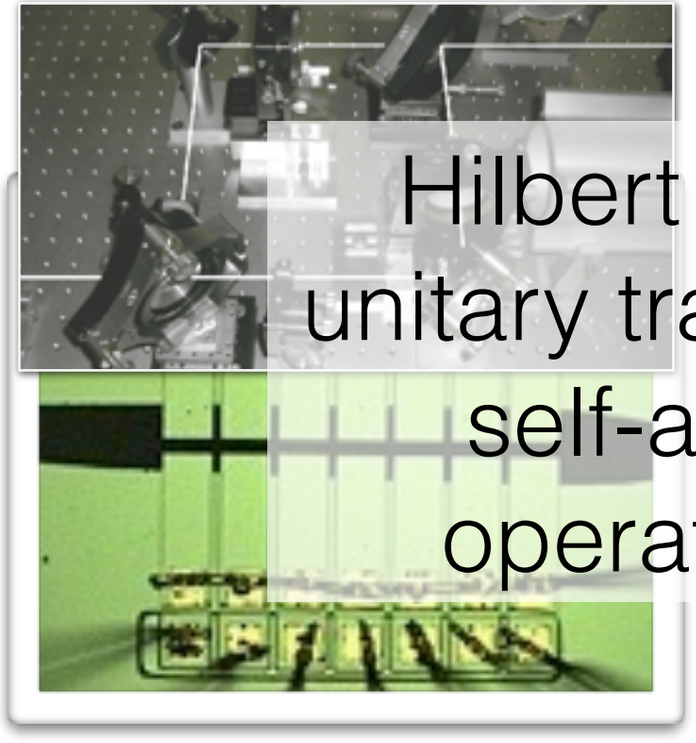
```
fun fact 0 = 1
  | fact x = x * fact (x-1)
```

Motivations



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

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



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

?

Quantum Circuits

Good Points:

+ Universal

+ Clear operational interpretation

Bad points:

- Inflexible

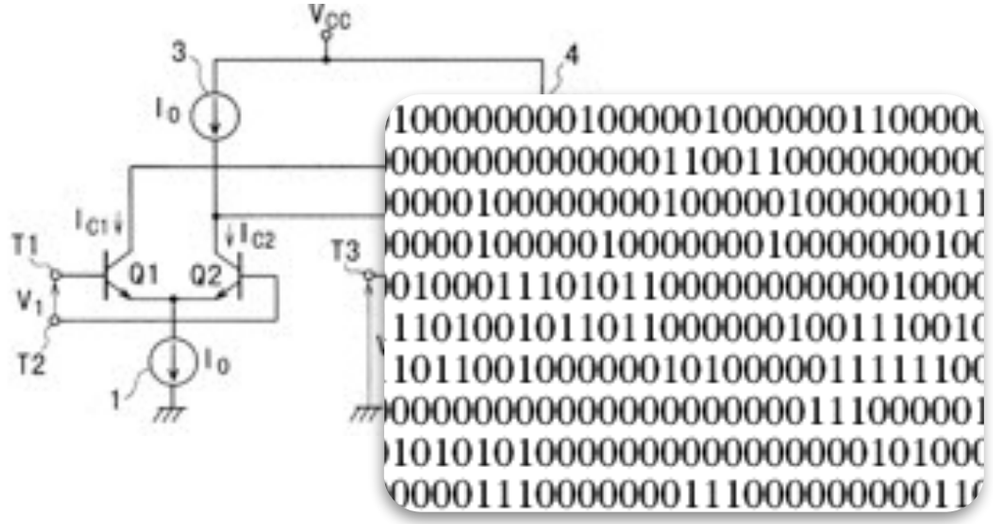
- Mathematically ad hoc

- Few nice algebraic properties

Meh Point:

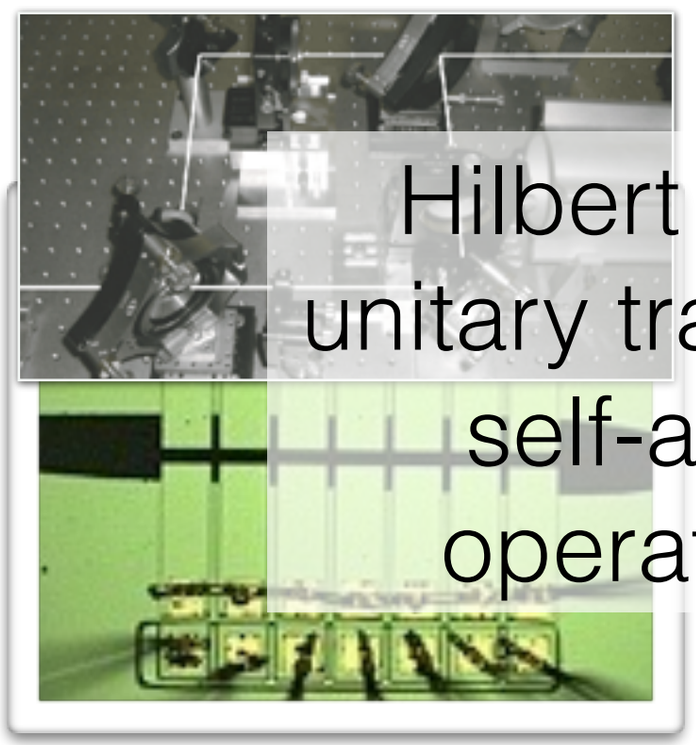
- Not complete

Motivations

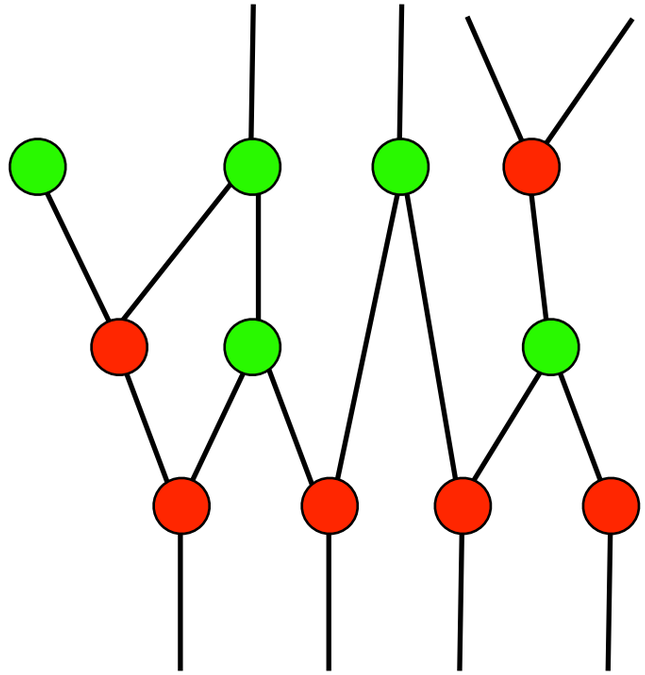


$$\lambda x.\lambda y.\lambda z.xz(yz)$$

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



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



ZX-calculus

Good Points:

+ Universal

+ Derived from the basic algebra of complementarity

+ Powerful algebraic theory

+ Can represent almost anything

Bad point:

- Need to impose operational meaning post-hoc

Meh Point:

- Not complete

ZX-calculus

Good Points:

+ Universal
+ Derived from the basic algebra of complementarity
+ Powerful algebraic theory
+ Can represent almost anything
+ **Now complete for the Clifford + T fragment!**

Bad point:

- Need to impose operational meaning post-hoc

Meh Point:

~~- Not complete~~

Jeandel, Perdrix, Vilmart
A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics

ZX-calculus

Good Points:

+ Universal
+ Derived from the basic algebra of complementarity
+ Powerful algebraic theory
+ Can represent almost anything
+ Now complete for the Clifford + T fragment!
+ **Now universally complete!**

Bad point:

- Need to impos

Ng and Wang
A universal completion of the ZX-calculus
1706.09877

for Clifford+T Quantum Mechanics

ZX-calculus

Good Points:

+ Universal
+ Derived from the basic algebra of complementarity
+ Powerful algebraic theory
+ Can represent almost anything
+ Now complete for the Clifford + T fragment!
+ **Now universally complete!**

Bad point:

- Need to impos

Jeandel, Perdrix, Vilmart
Manuscript

A universal completion of the ZX-calculus
1706.09877

for Clifford+T Quantum Mechanics

1.

Generalities

“Observables”

Non-degenerate, projective observables
on finite dimensional spaces
i.e.
Orthonormal bases

$$A = |a_1\rangle, |a_2\rangle, \ldots, |a_d\rangle$$

Unbiasedness and Phases

A state $|\psi\rangle$ is **unbiased** for a basis A if

$$|\langle a_i \mid \psi \rangle| = \frac{1}{\sqrt{d}}$$

Every unbiased state determines a unitary map via

$$U_\psi : |a_i\rangle \mapsto \sqrt{d}\langle a_i \,|\, \psi\rangle \, |a_i\rangle$$

This is called a **phase map** for A.

Unbiasedness and Phases

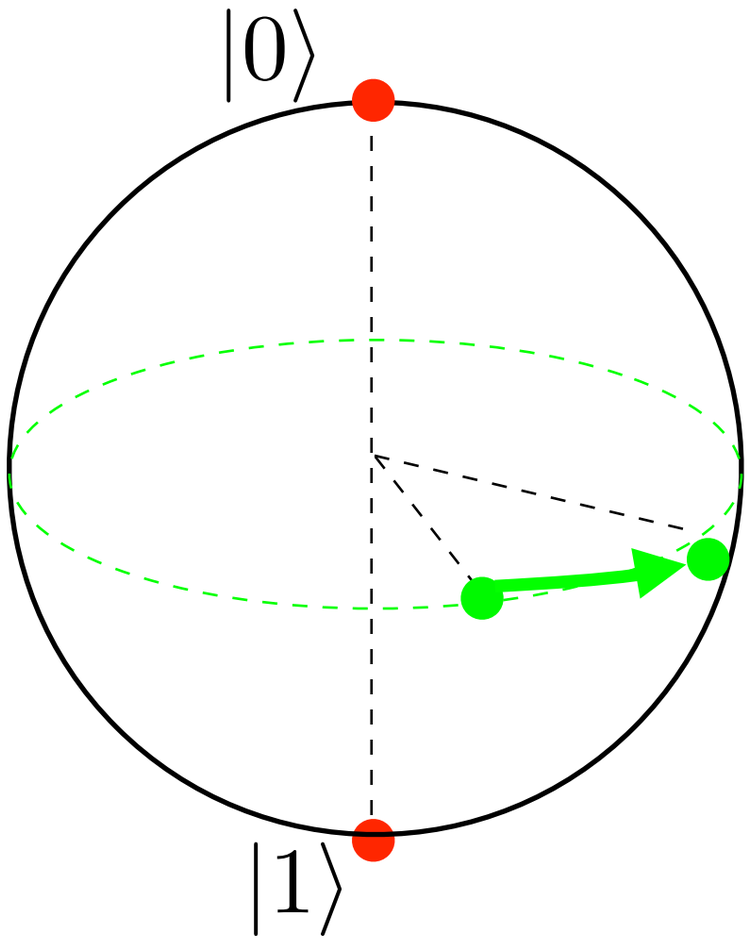
A state $|\psi\rangle$ is **unbiased** for a basis A if

Proposition 1:
The phases of any observable form an abelian group

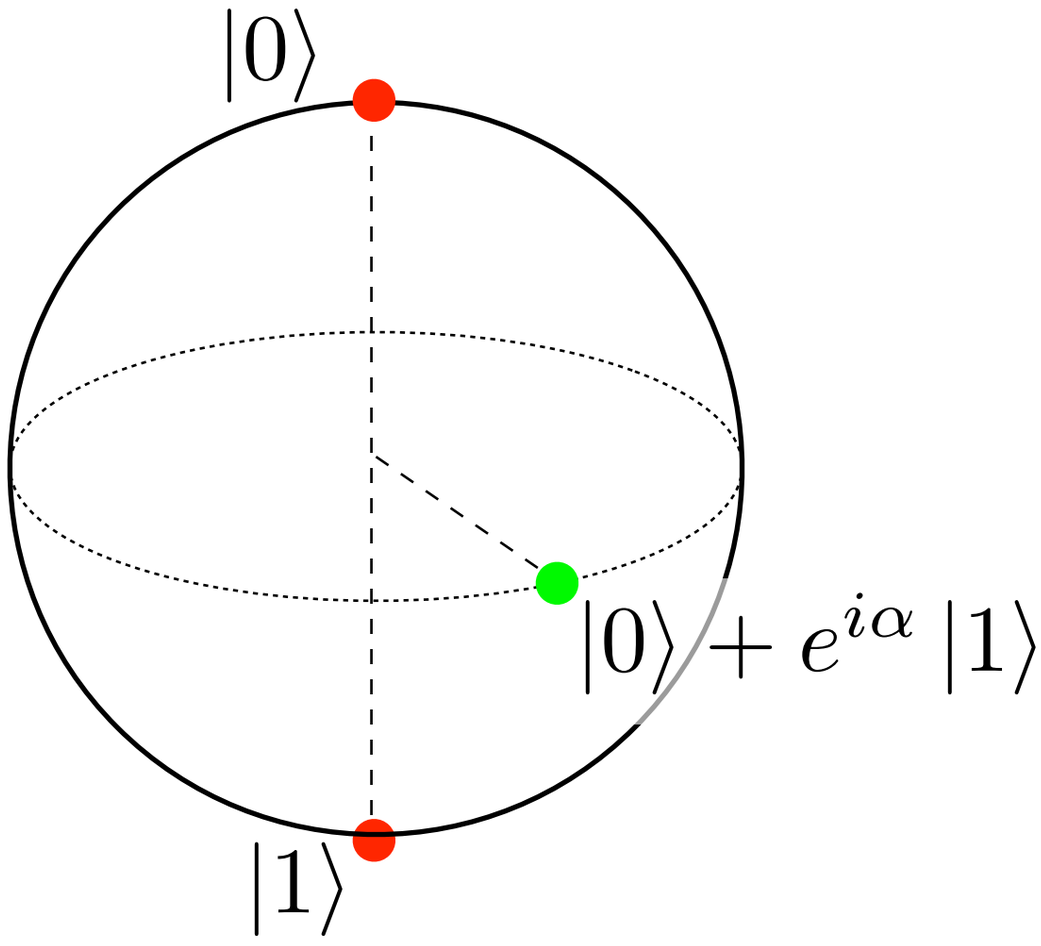
$$U_\psi : |a_i\rangle \mapsto \sqrt{d}\langle a_i \,|\, \psi\rangle \, |a_i\rangle$$

This is called a **phase map** for A.

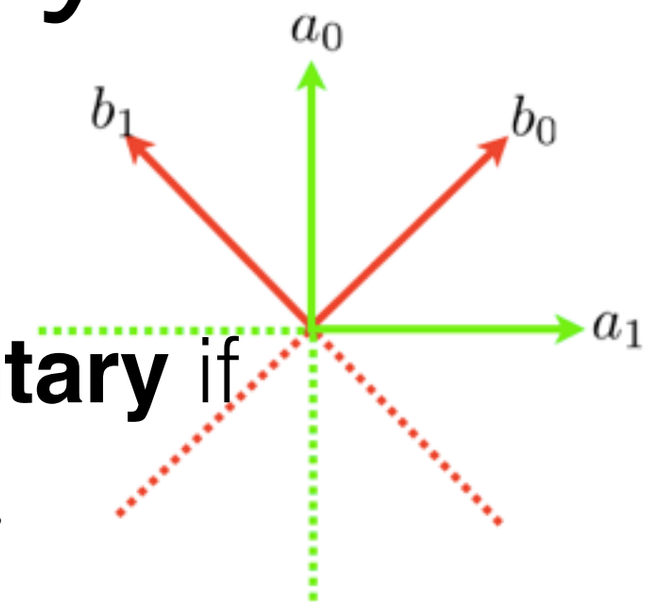
Phases & Unbiased Points



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



Complementarity



Two observables A and B are **complementary** if

$$|\langle a_i \mid b_j \rangle| = \frac{1}{\sqrt{d}} \qquad \forall i, j$$

(aka mutually unbiased)

They are **strongly complementary** if $\{U_{b_i}\}_i$ is a subgroup of the phase group Φ_A.

Observables are Frobenius Algebras

Theorem 2: Observables are in bijection with †-special commutative Frobenius algebras.

$$\delta : A \to A \otimes A \qquad \mu : A \otimes A \to A$$

$$\epsilon : A \to I \qquad \eta : I \to A$$

Via:

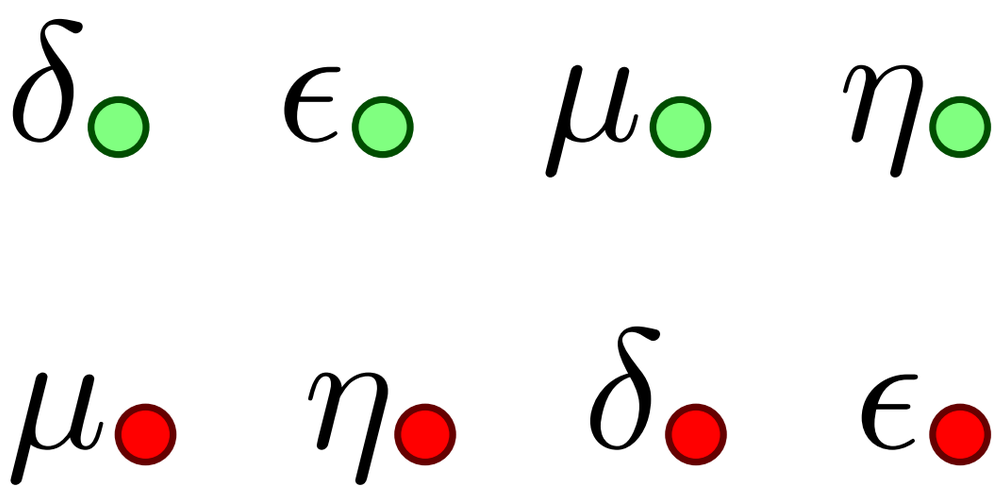
$$\delta :: |a_i\rangle \to |a_i\rangle \otimes |a_i\rangle \qquad \mu = \delta^\dagger$$

$$\epsilon :: |a_i\rangle \to 1 \qquad \eta = \epsilon^\dagger$$

Coecke, Pavlovic, and Vicary, “A new description of orthogonal bases”, MSCS 23(3), 2013. arxiv:0810.0812

Strongly Complementary Observables are Hopf algebras

Theorem 3: Two observables are strongly complementary iff they form a Hopf algebra

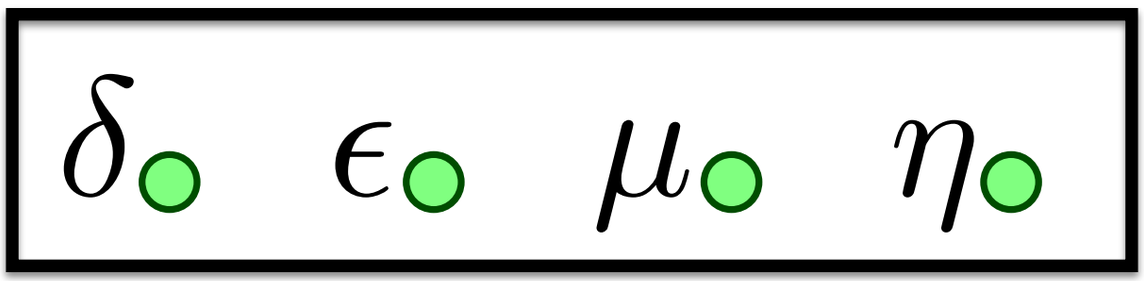


Coecke and Duncan, “Interacting Quantum Observables: categorical algebra and diagrammatics”, NJP 13(043016), 2011, arXiv:0906.4725.

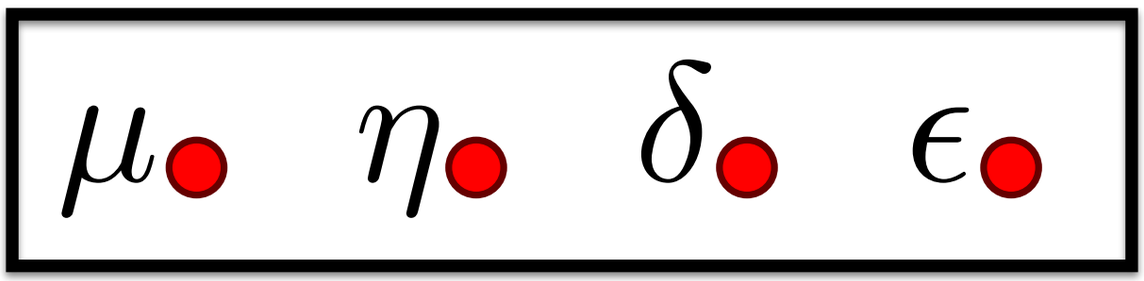
Strongly Complementary Observables are Hopf algebras

Theorem 3: Two observables are strongly complementary iff they form a Hopf algebra

Frobenius



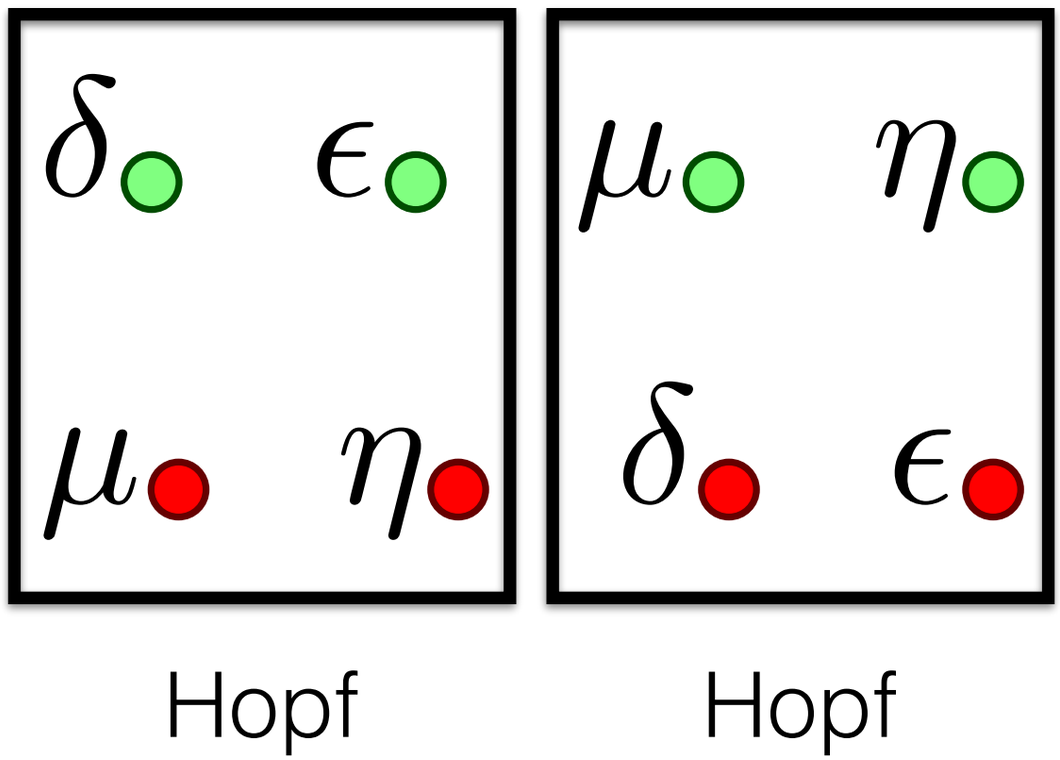
Frobenius



Coecke and Duncan, “Interacting Quantum Observables: categorical algebra and diagrammatics”, NJP 13(043016), 2011, arXiv:0906.4725.

Strongly Complementary Observables are Hopf algebras

Theorem 3: Two observables are strongly complementary iff they form a Hopf algebra



Coecke and Duncan, “Interacting Quantum Observables: categorical algebra and diagrammatics”, NJP 13(043016), 2011, arXiv:0906.4725.

Strong Complementarity

$\Leftrightarrow$

GHZ/Mermin Non-locality

Theorem 4: Two observables are strongly complementary iff they admit a Mermin-style probability-free proof of non-locality.

B. Coecke, RD, A. Kissinger, Q. Wang, Strong Complementarity and Non-locality in Categorical Quantum Mechanics, LiCS 2012, doi: 10.1109/LICS.2012.35
B. Coecke, RD, A. Kissinger, Q. Wang, *Generalised Compositional Theories and Diagrammatic Reasoning*; arXiv:1506.03632

More?

For more on the theoretical perspective, come see my talk on thursday at LIG.

See also:
R. Duncan and K. Dunne, *Interacting Frobenius algebras are Hopf* in Proc. LiCS, 2016.
DOI: 10.1145/2933575.2934550

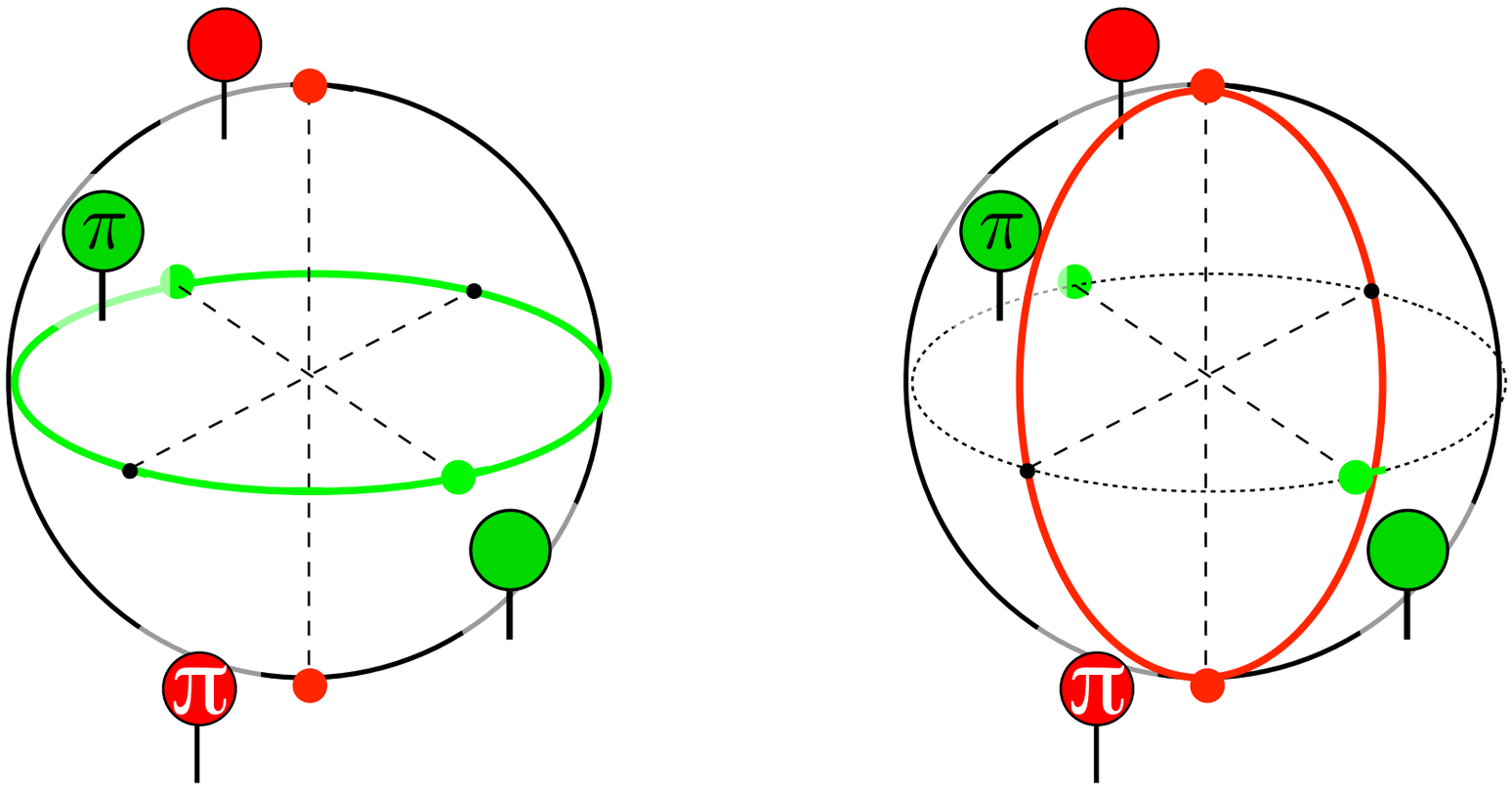
2.

The ZX-Calculus

Z and X Observables

The Pauli **Z** and **X** observables are strongly complementary, with some additional features:

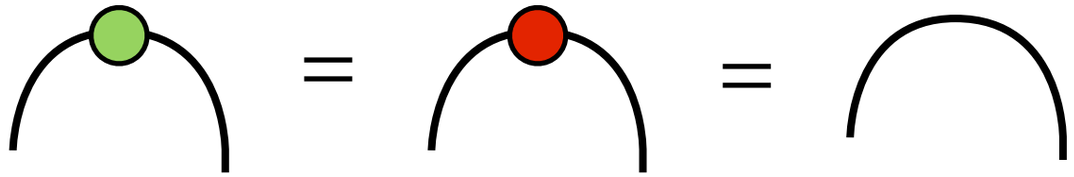
- The phase group is $[0,2\pi)$



- Dimension 2 implies two classical points
- The action of the classical group is $\alpha \mapsto -\alpha$

Z and X Observables

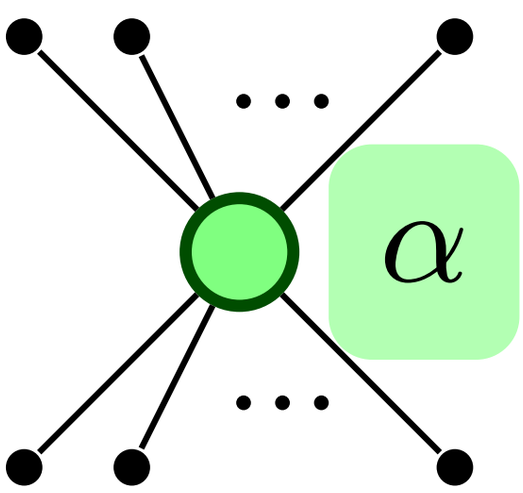
- Both observables generate the same compact structure

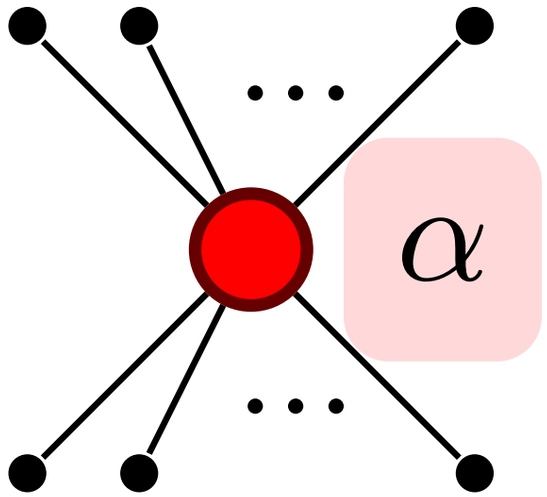


  - *can just treat the diagram as an undirected graph*

- the Z and X are related by a definable unitary
  - *gives rise to colour change rule*

ZX-calculus syntax



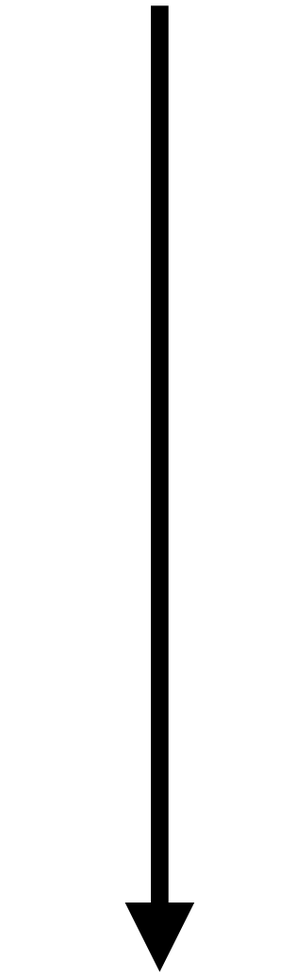


$$\alpha \in [0, 2\pi)$$

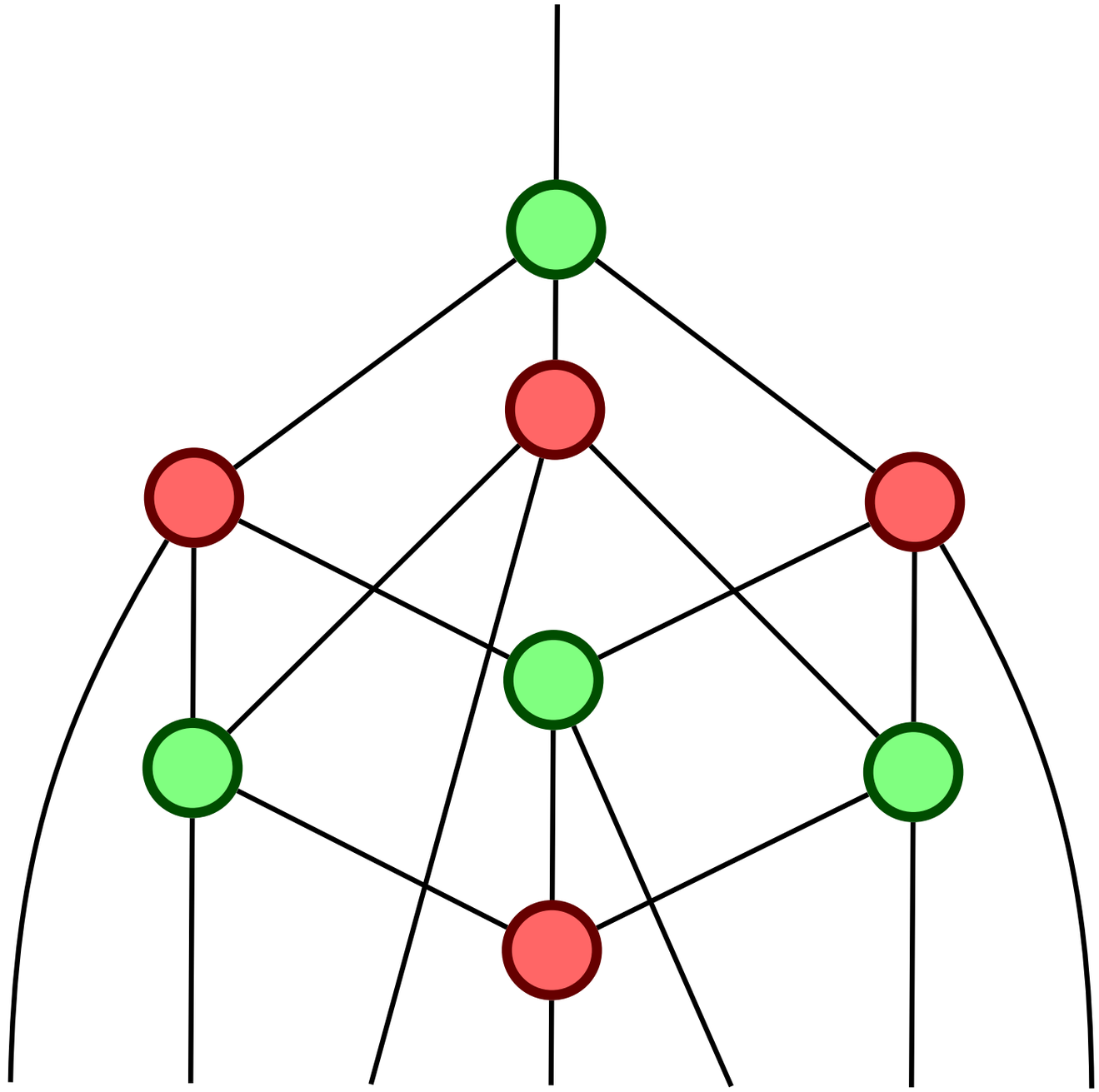
Defn: A *diagram* is an undirected open graph generated by the above vertices.

Example

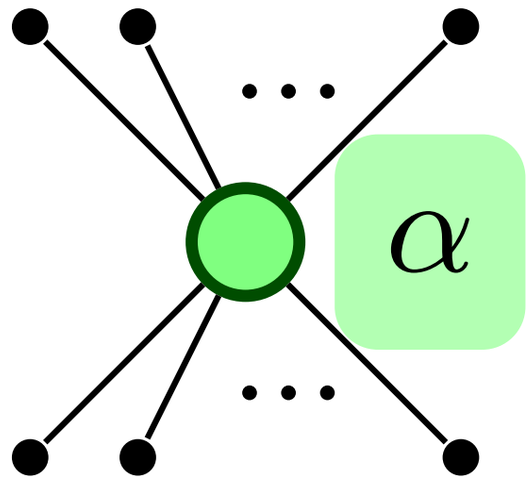
1 qubit



7 qubit

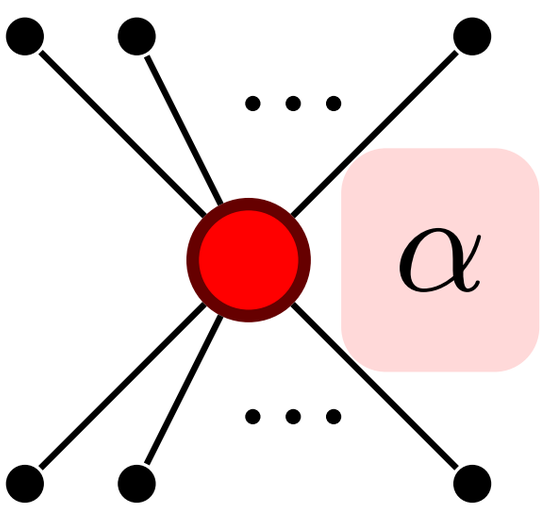


ZX-calculus semantics



$$|0\rangle^{\otimes n} \mapsto |0\rangle^{\otimes m}$$

$$|1\rangle^{\otimes n} \mapsto e^{i\alpha} |1\rangle^{\otimes m}$$



$$|+\rangle^{\otimes n} \mapsto |+\rangle^{\otimes m}$$

$$|-\rangle^{\otimes n} \mapsto e^{i\alpha} |-\rangle^{\otimes m}$$

Representing Qubits

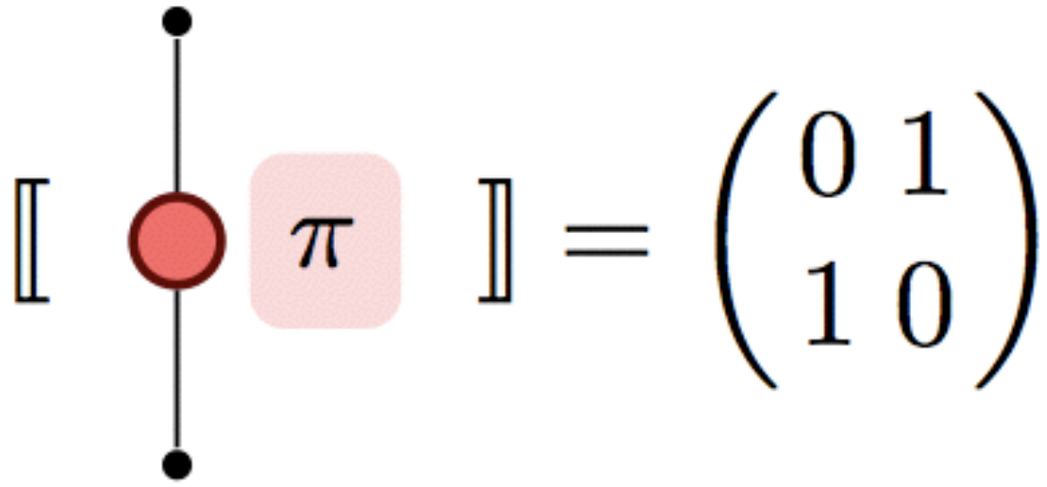
$$[\![\ \ ]\!] = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

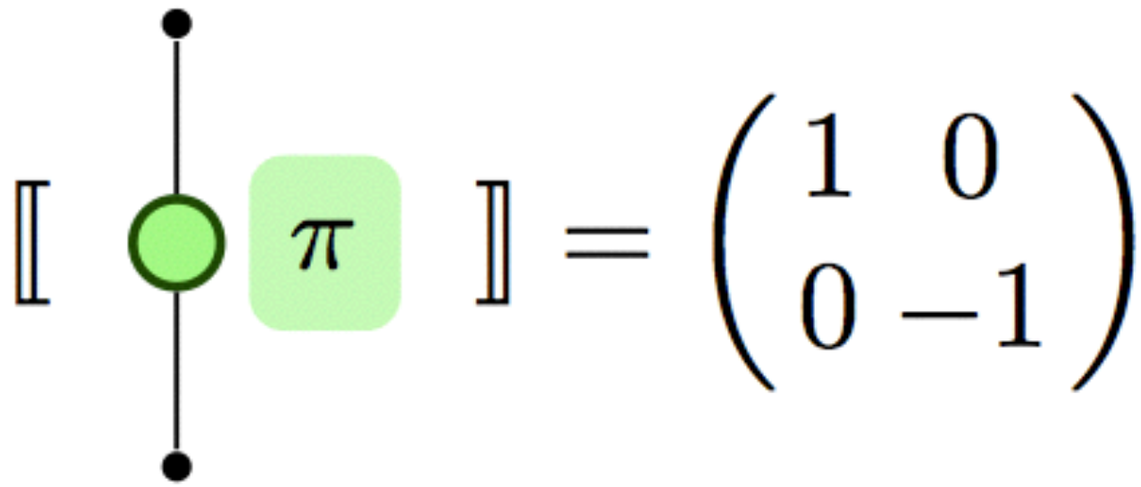
$$[\![\ \ ]\!] = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$[\![\ \ ]\!] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$$

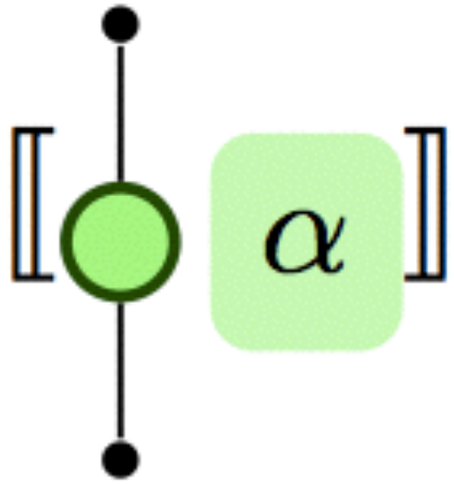
$$[\![\ \ ]\!] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$$

Representing Paulis

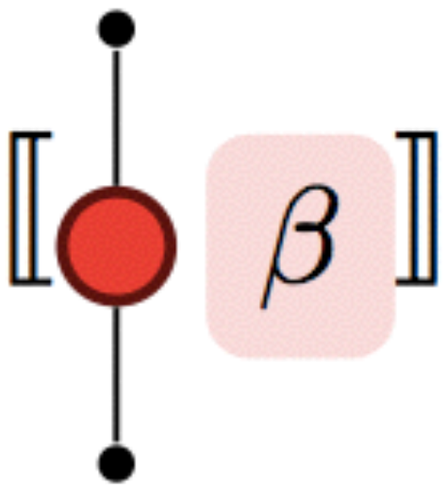




Representing Phase shifts

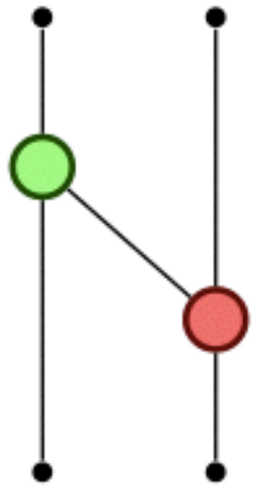
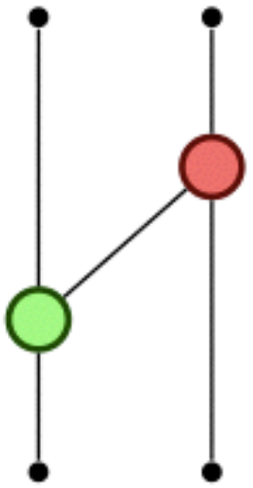


$$= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$$



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

Representing CNot

$$\wedge X = [\![$$  $$]\!] = [\![$$  $$]\!] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The ZX-calculus is universal

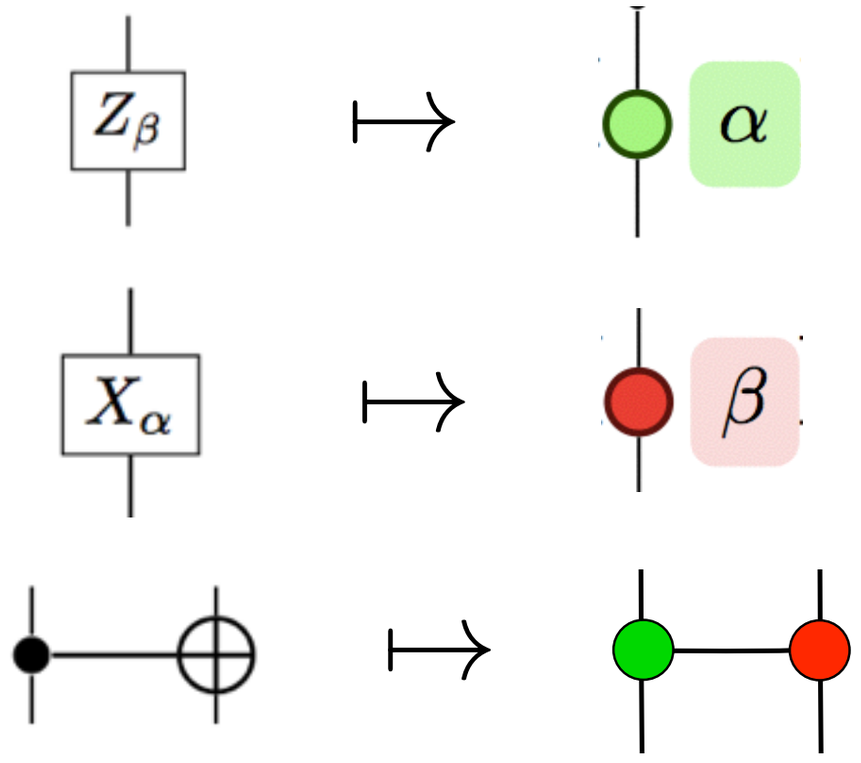
Theorem: Let U be a unitary map on n qubits; then there exists a ZX-calculus term D such that:

$$[\![D]\!] = U$$

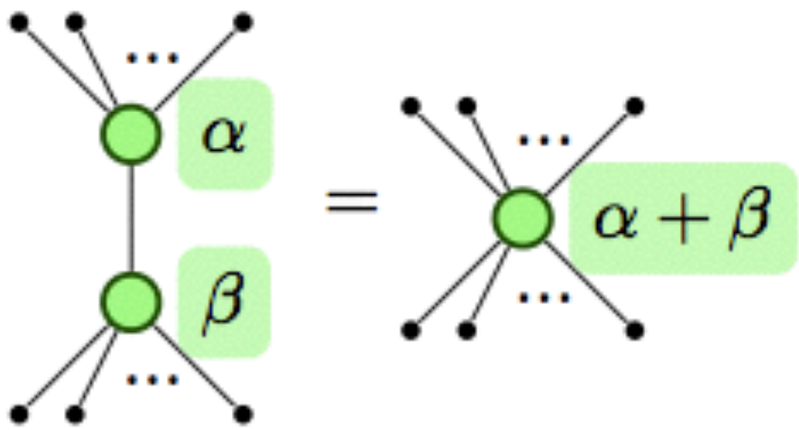
The ZX-calculus is universal

Theorem: Let U be a unitary map on n qubits; then there exists a ZX-calculus term D such that:

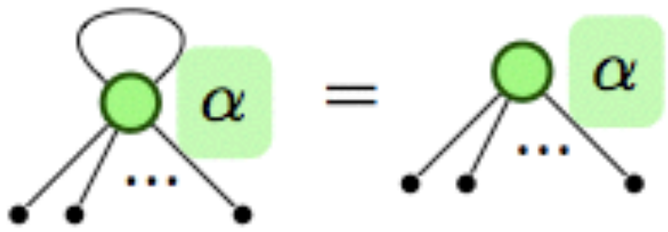
$$[\![D]\!] = U$$



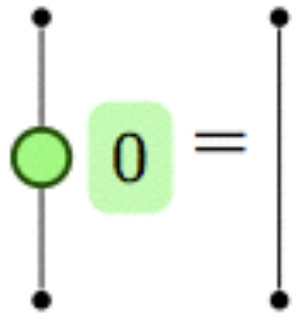
Equations



(spider)



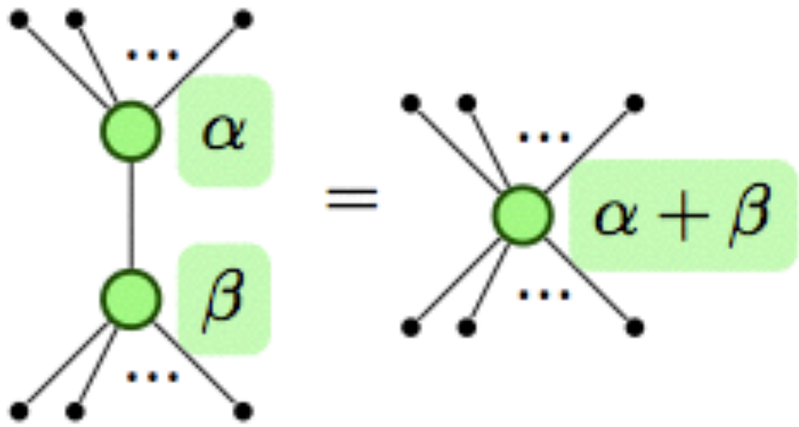
(anti-loop)



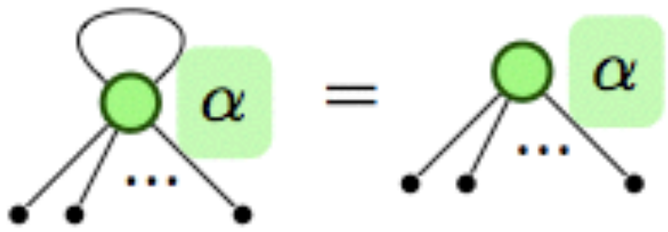
(identity)

Equations

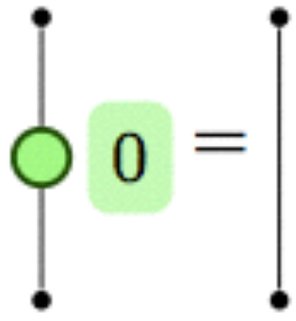
Generalised Spider



(spider)

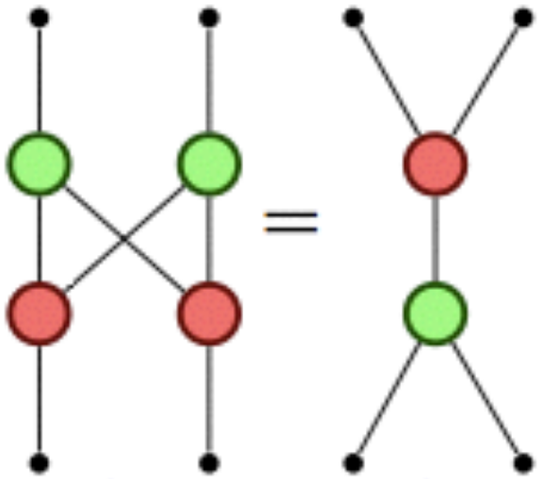


(anti-loop)

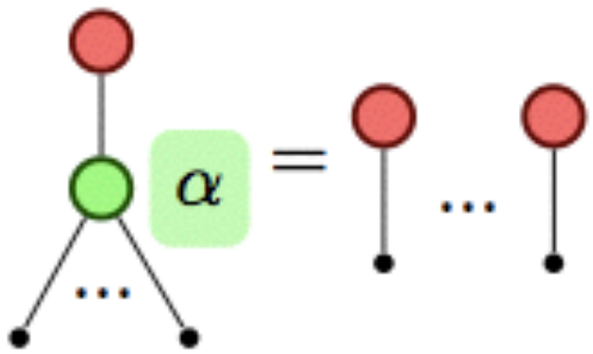


(identity)

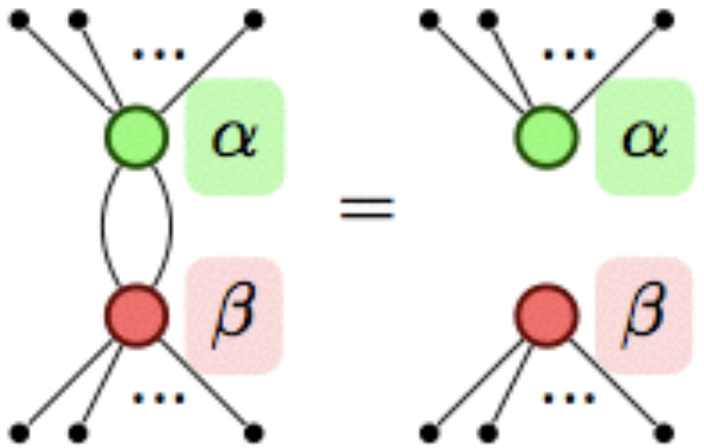
Equations



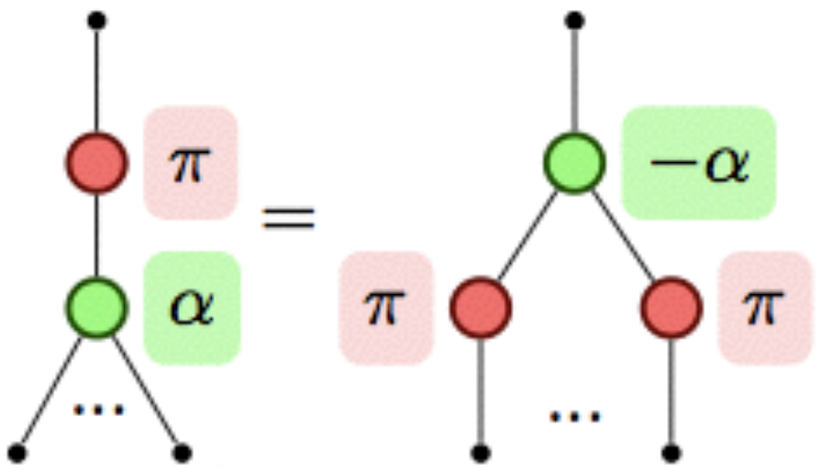
(bialgebra)



(copying)



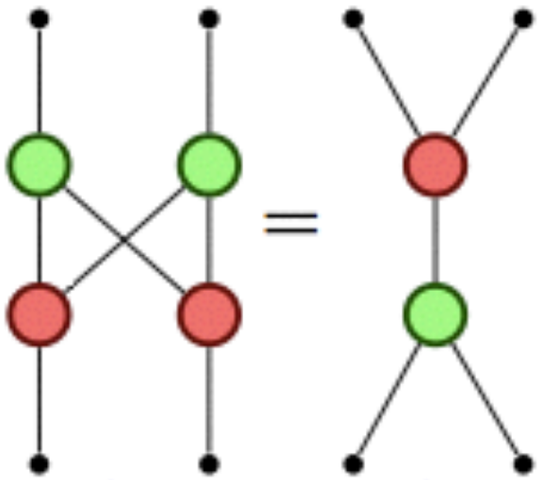
(hopf)



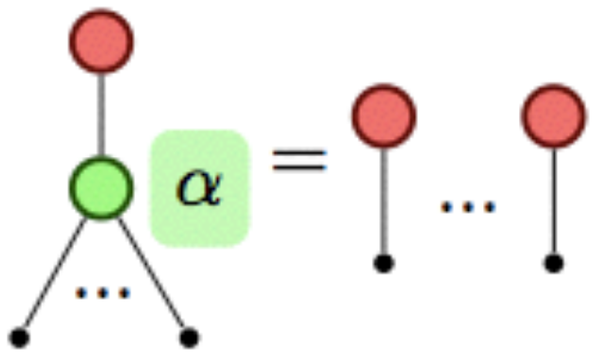
(π-commute)

Equations

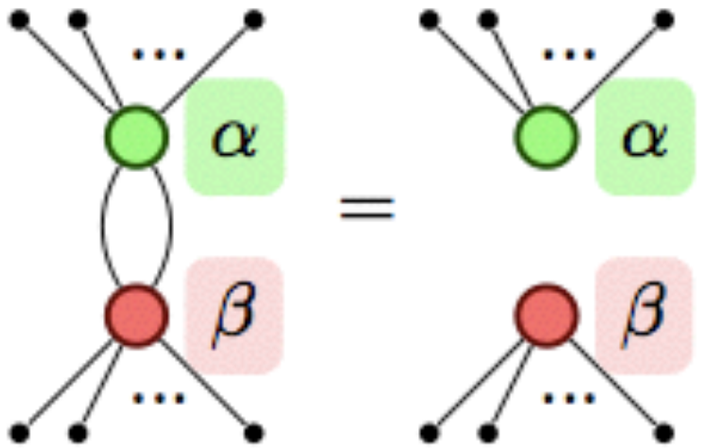
“Strong Complementarity”



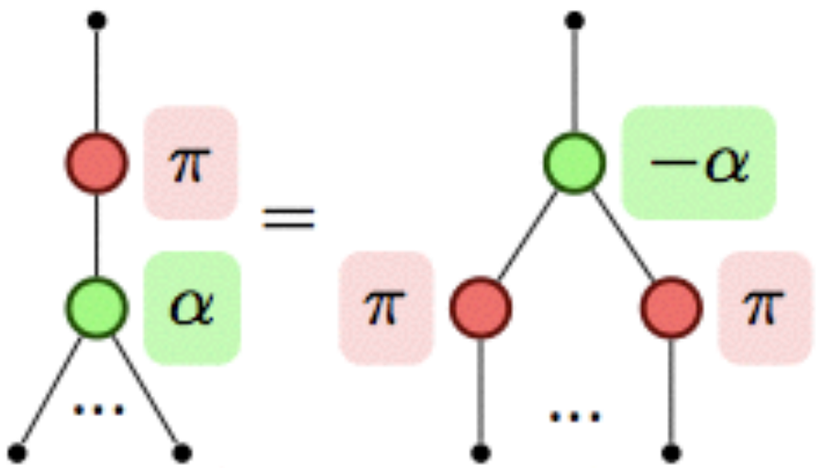
(bialgebra)



(copying)

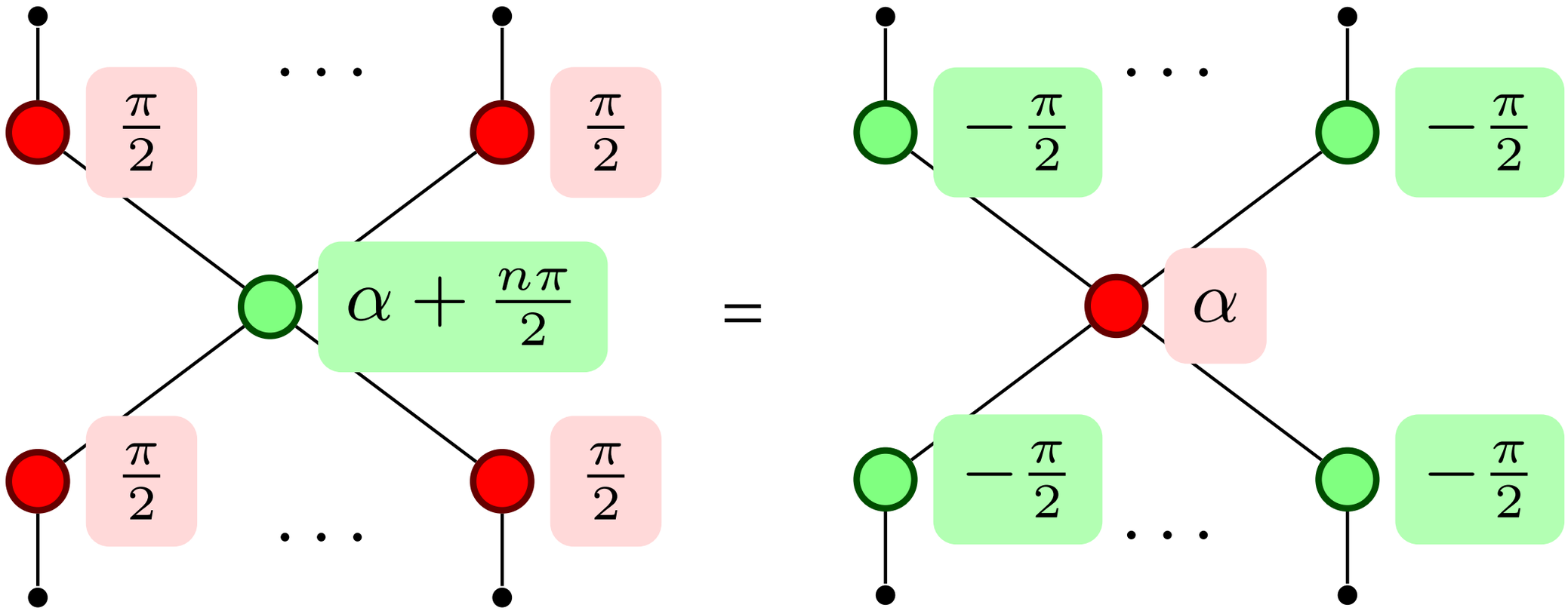


(hopf)



(π-commute)

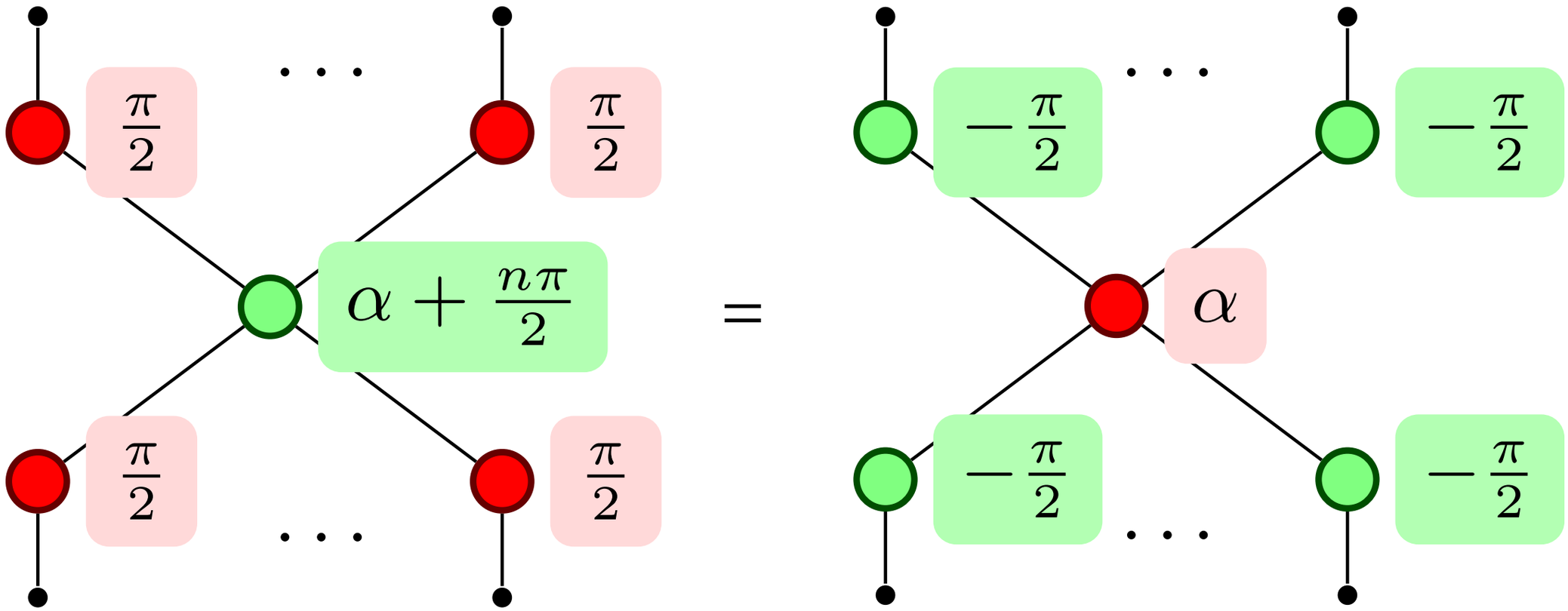
Equations



(colour change)

Equations

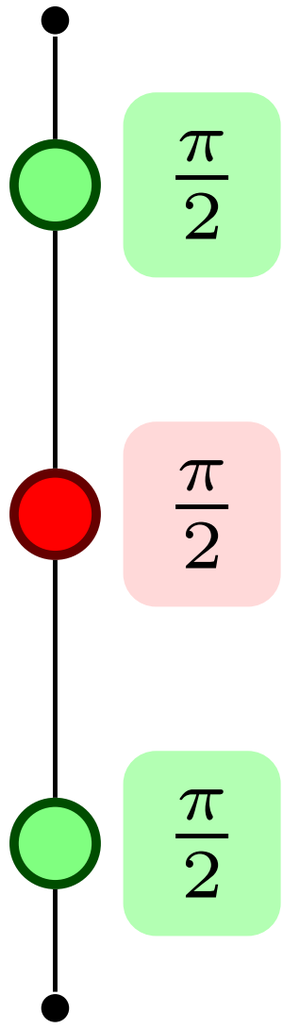
A weird one specific to ZX



(colour change)

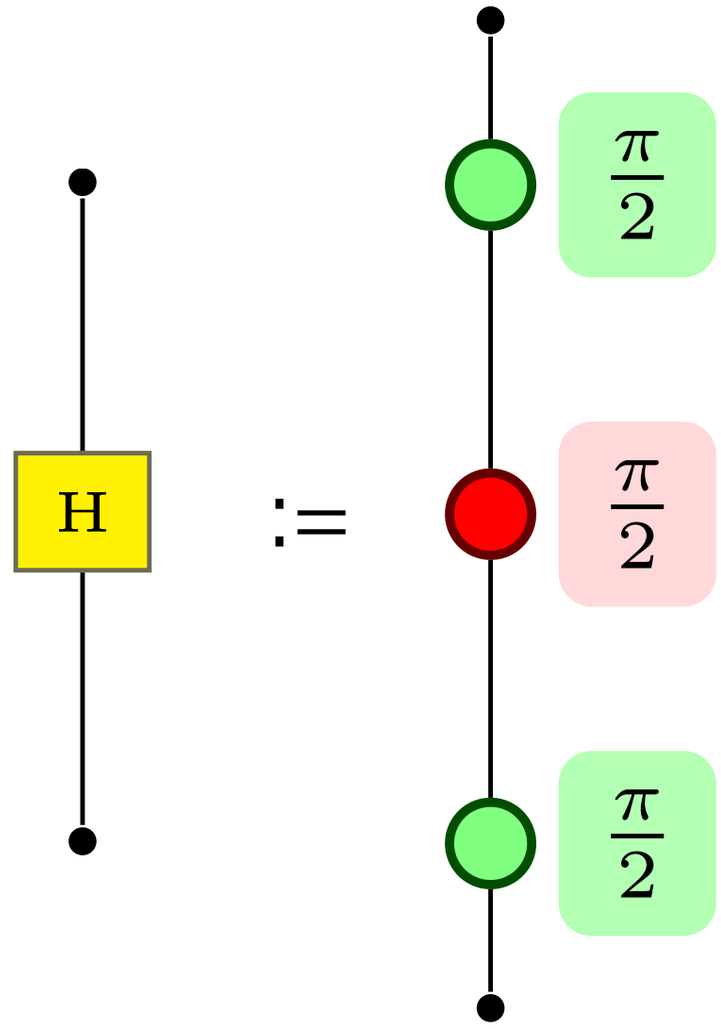
Representing Hadamard

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

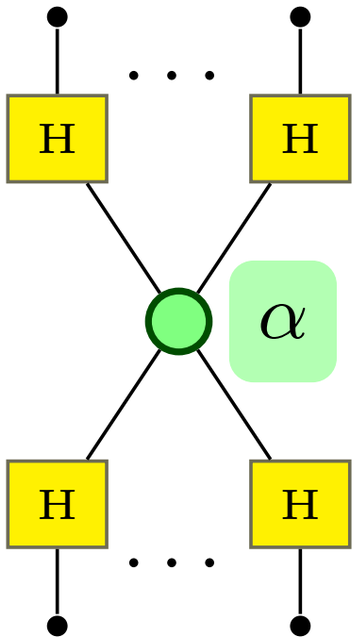


$]\!]$

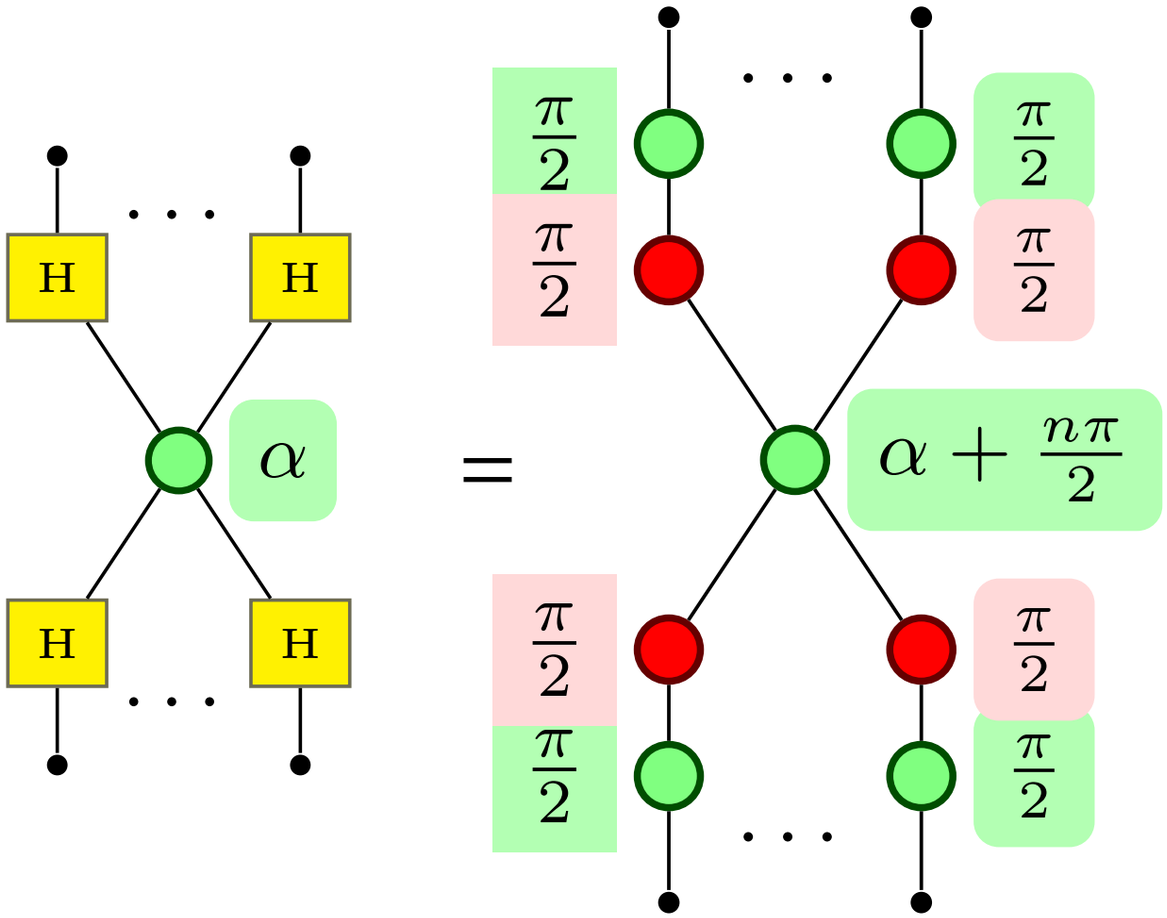
More on the Hadamard



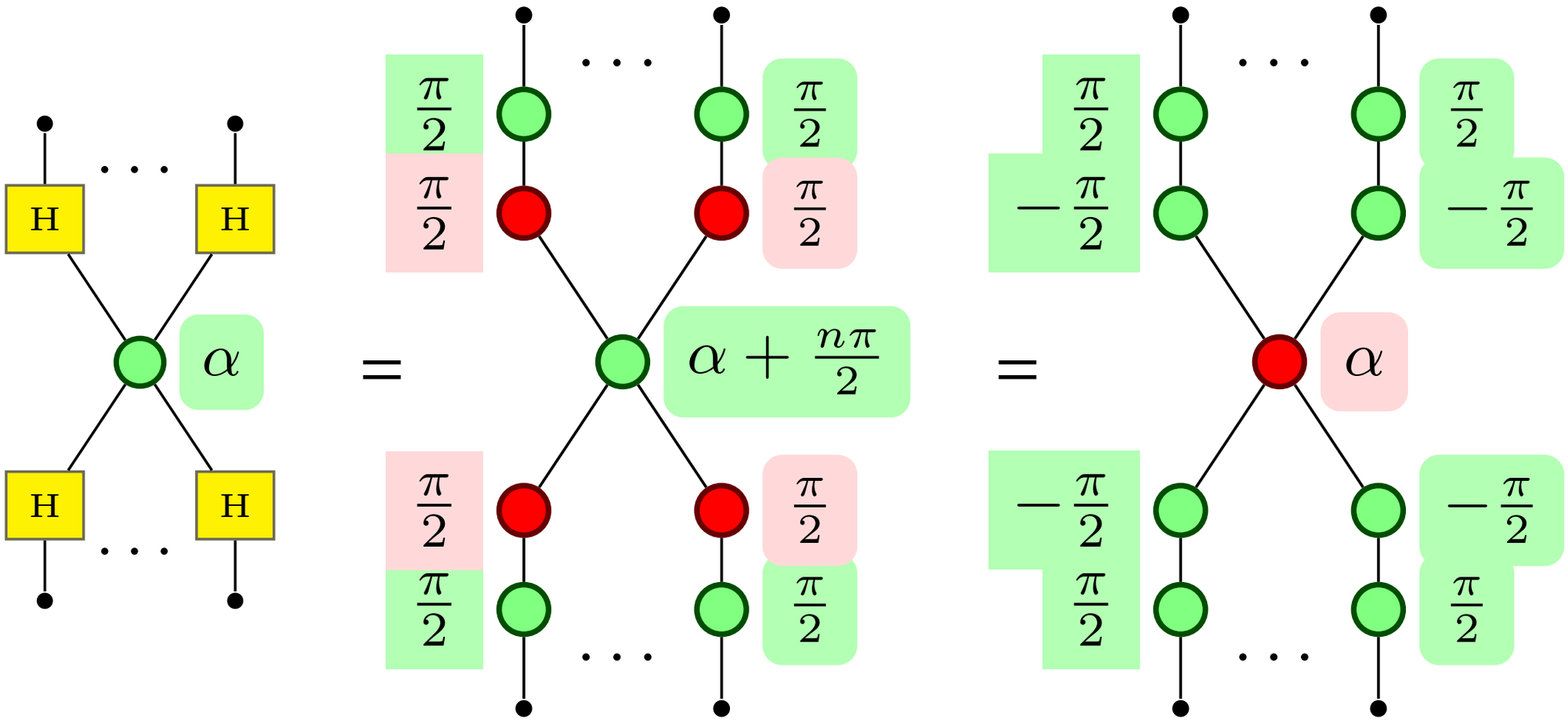
More on the Hadamard



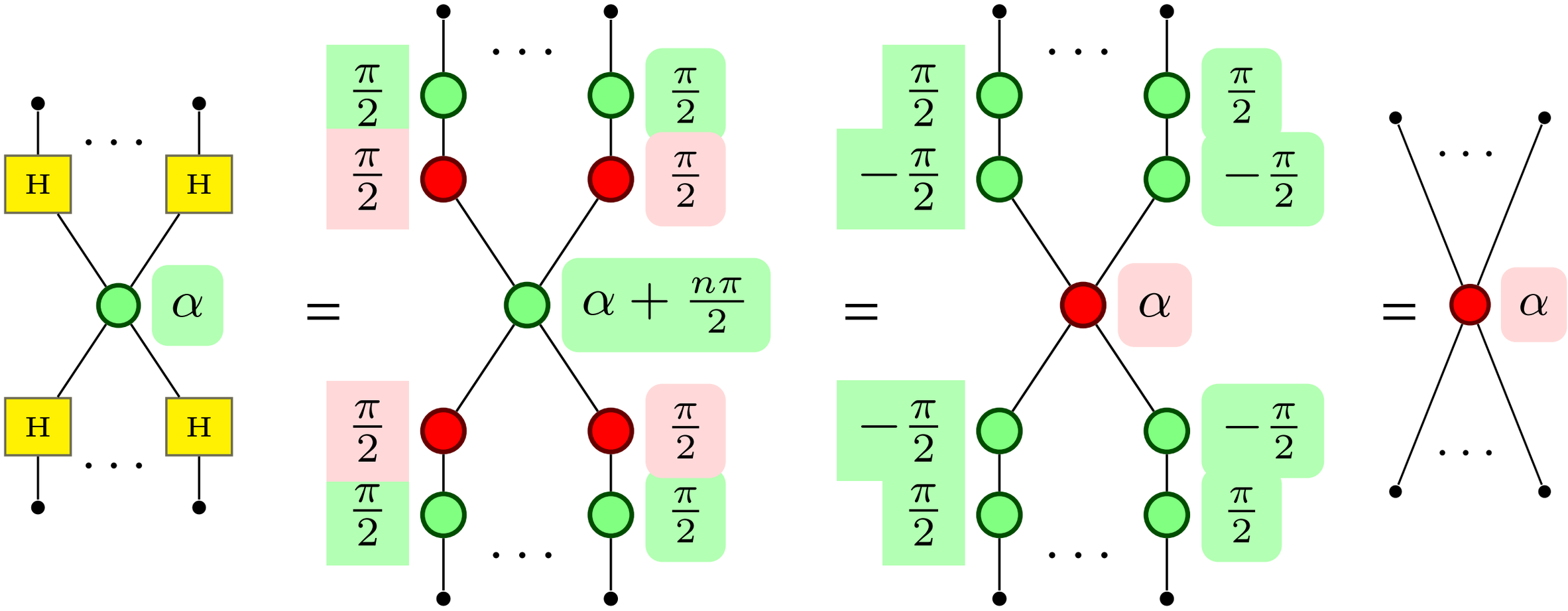
More on the Hadamard



More on the Hadamard

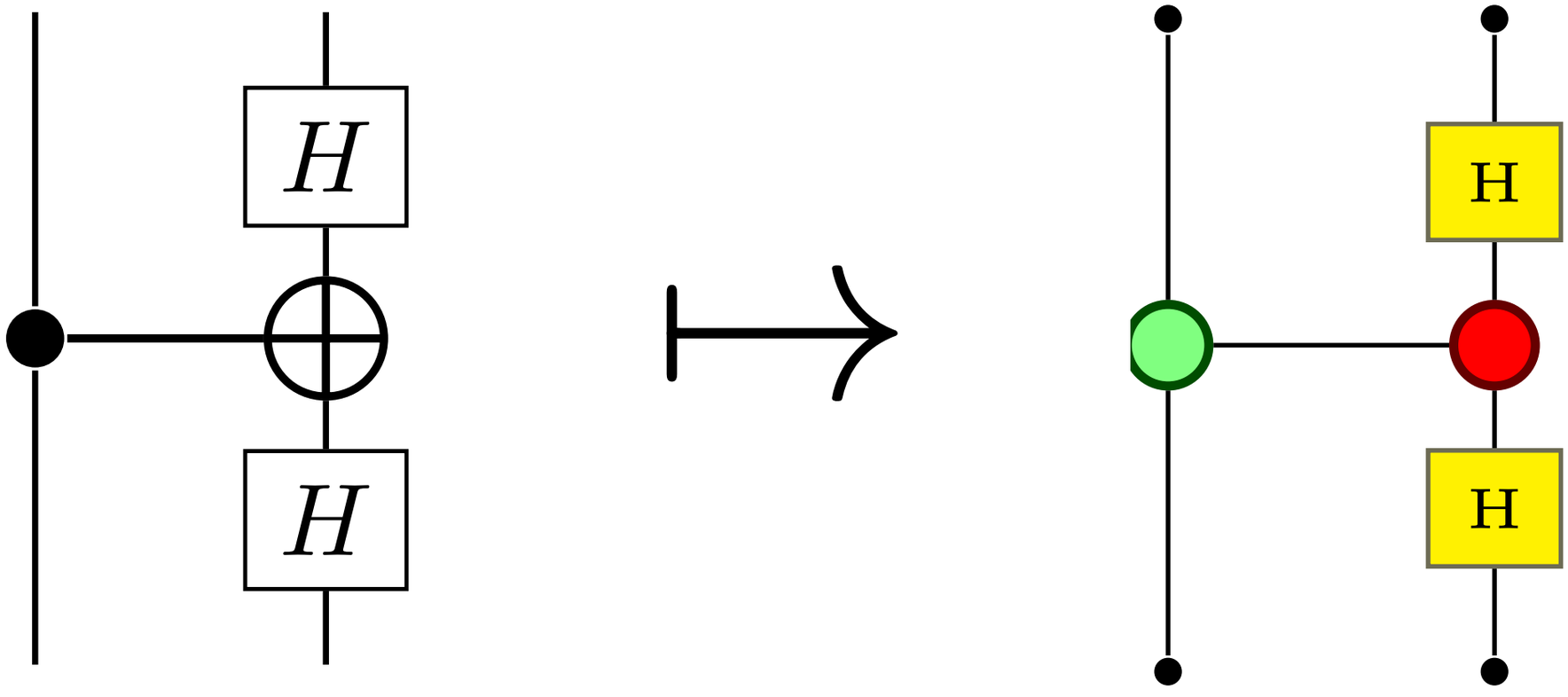


More on the Hadamard

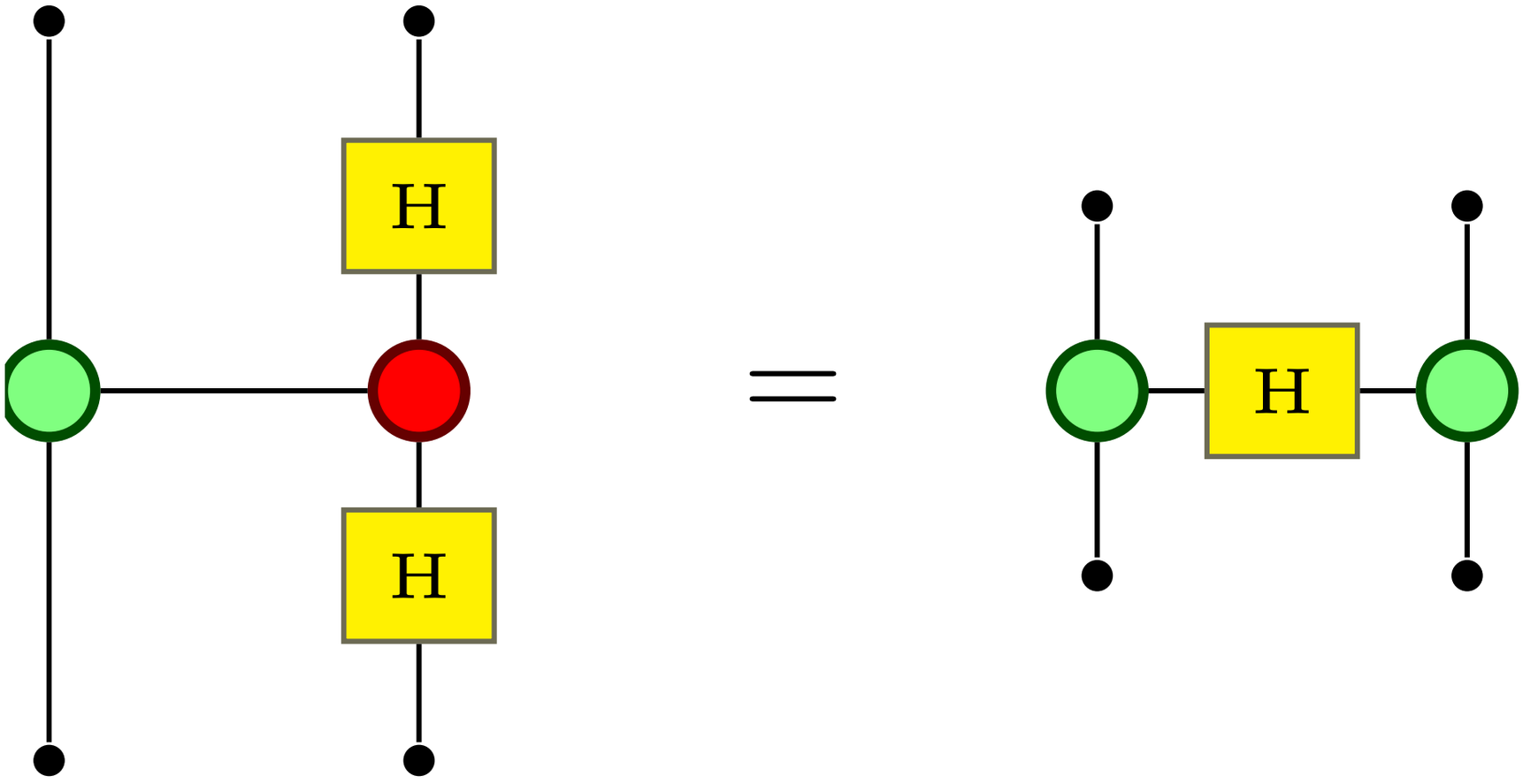


Corollary: total symmetry between red and green

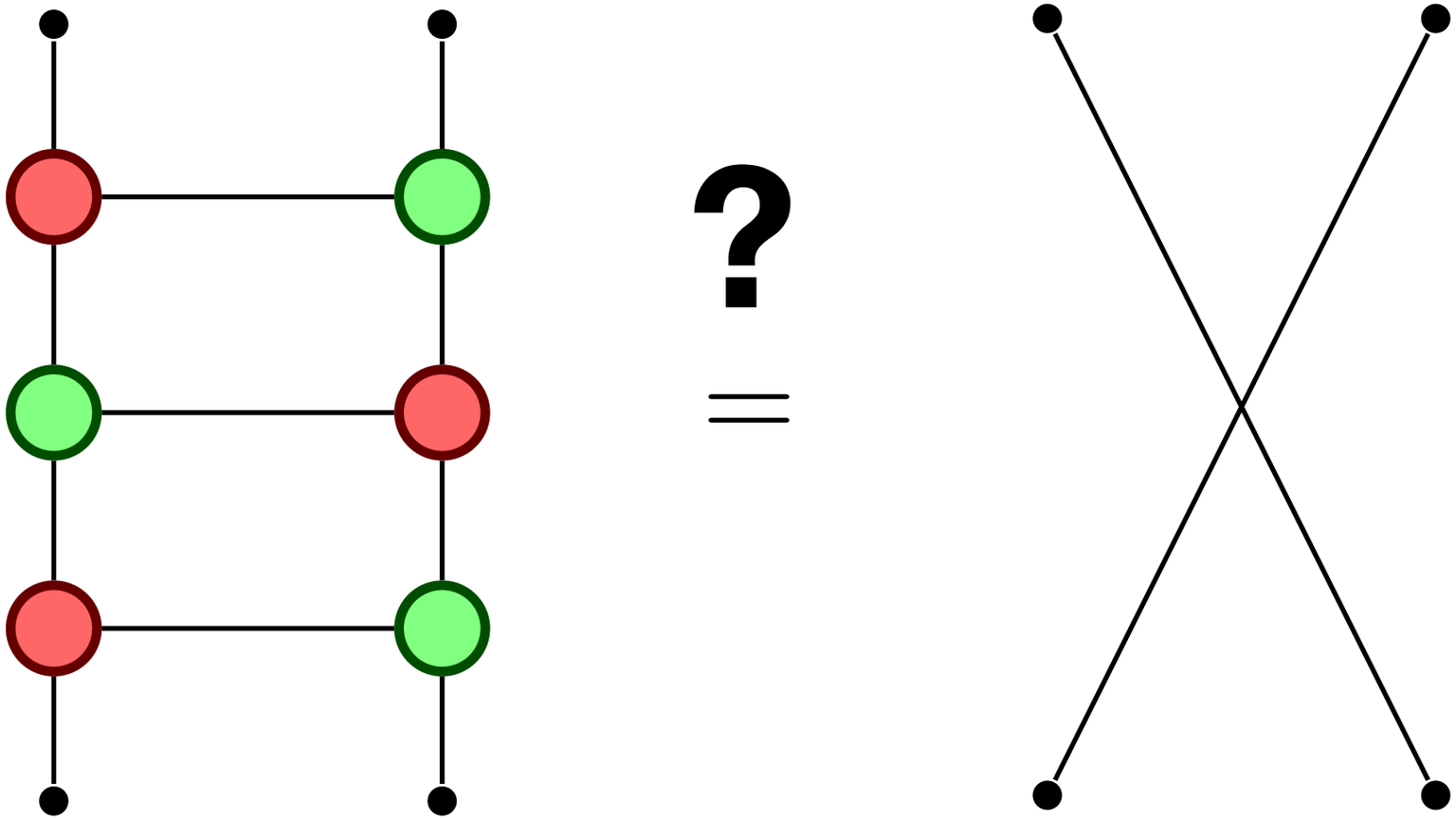
Example: Controlled-Z



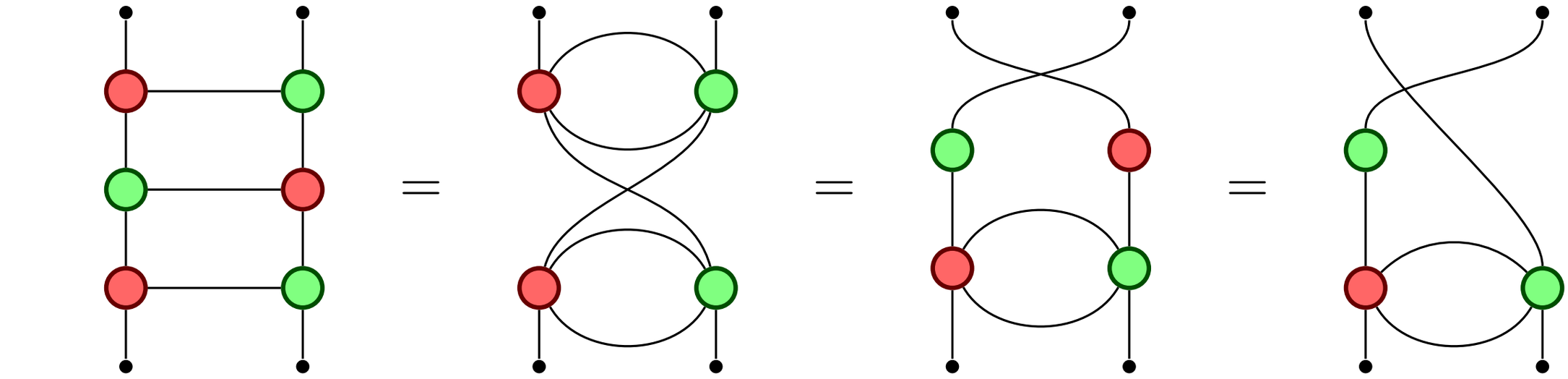
Example: Controlled-Z

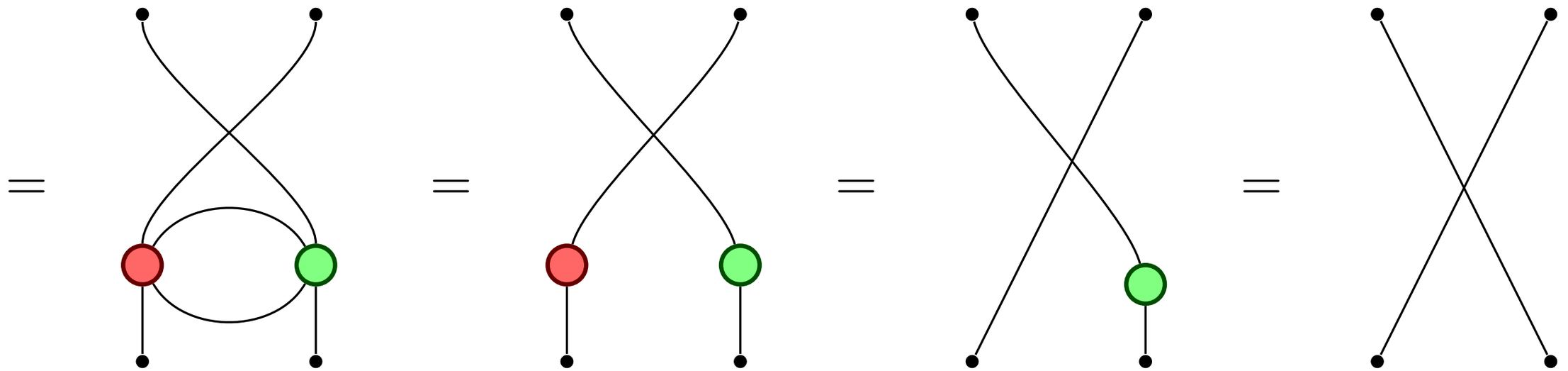


Example: CNOTS

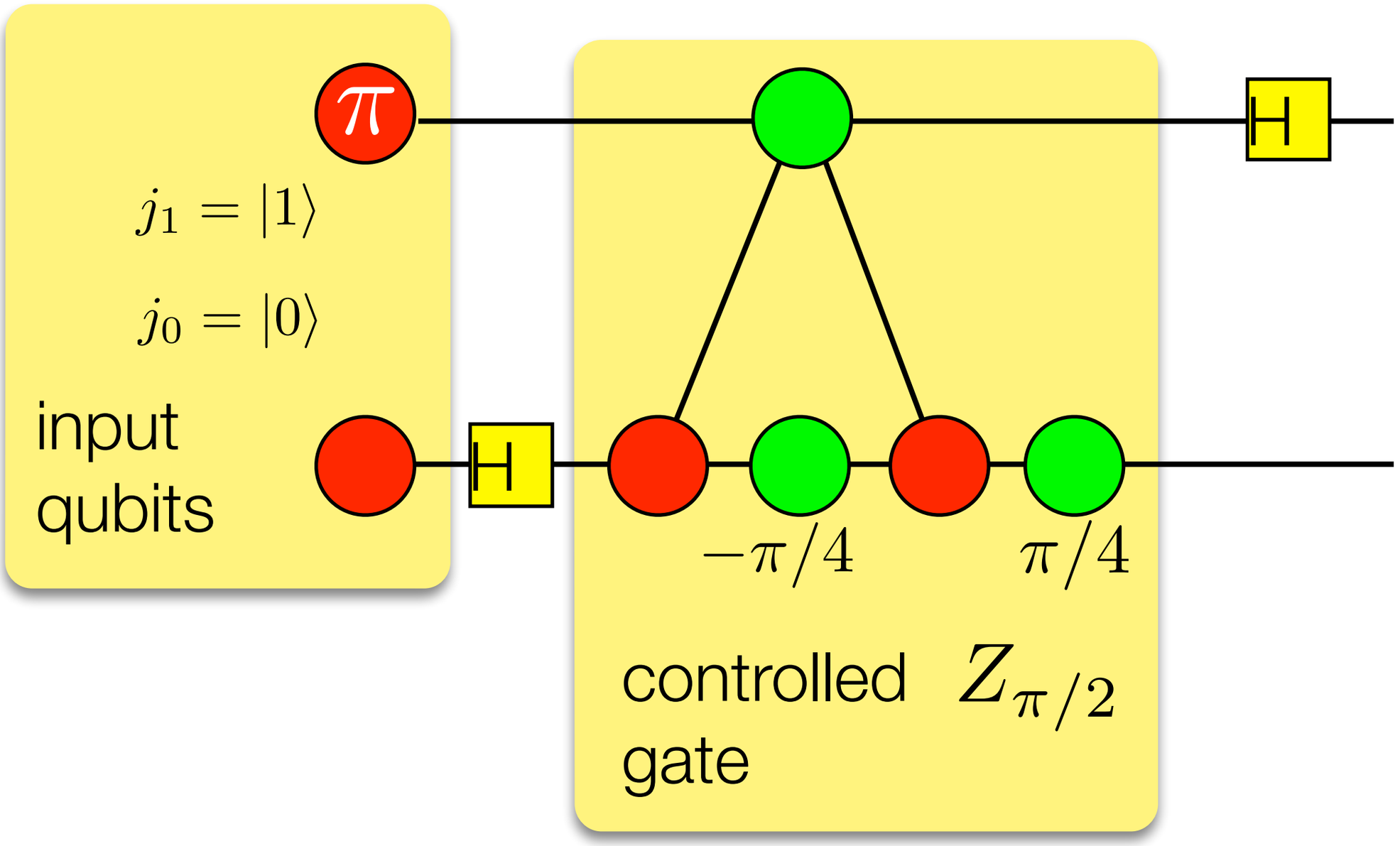


Example: CNOTS

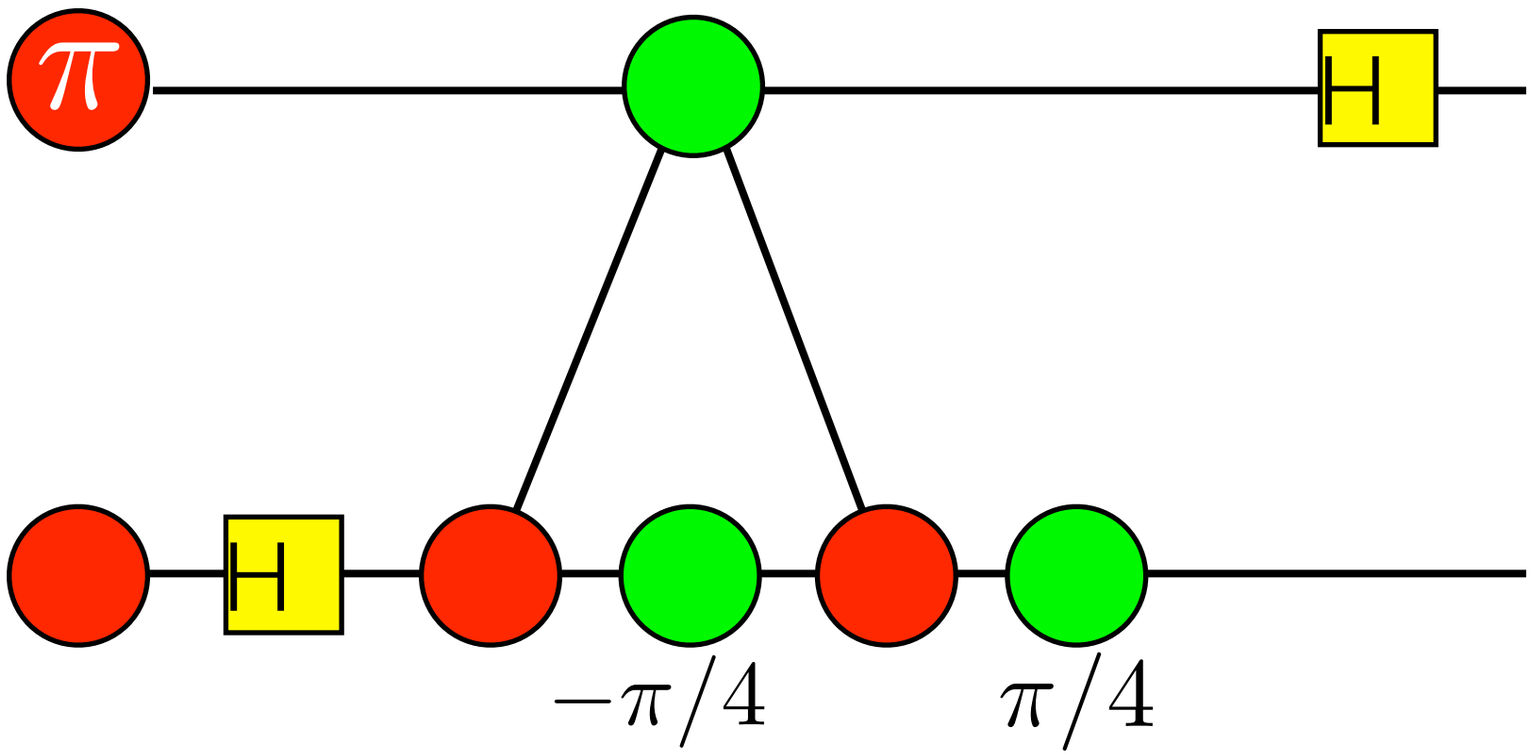




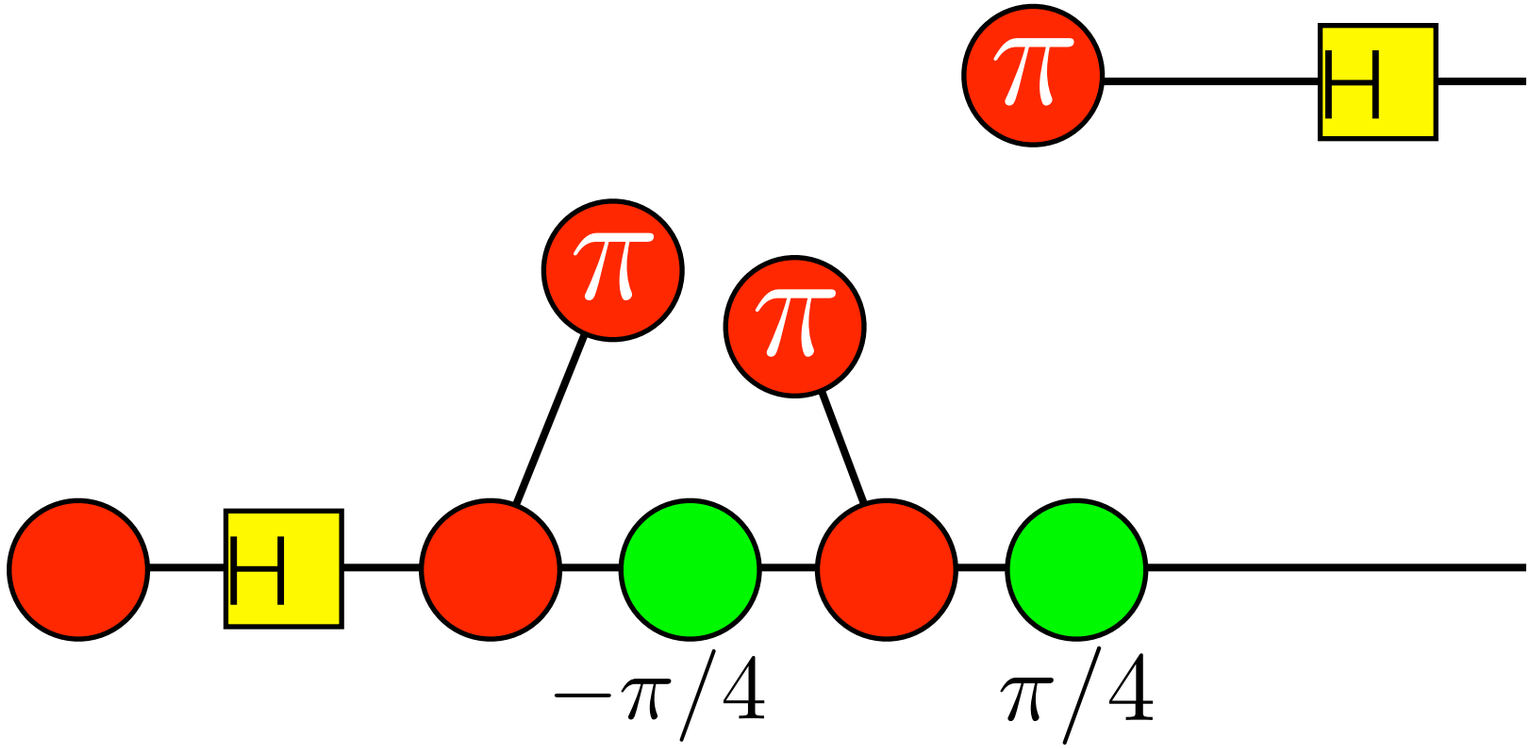
Example: 2-Qubit Quantum Fourier Transform



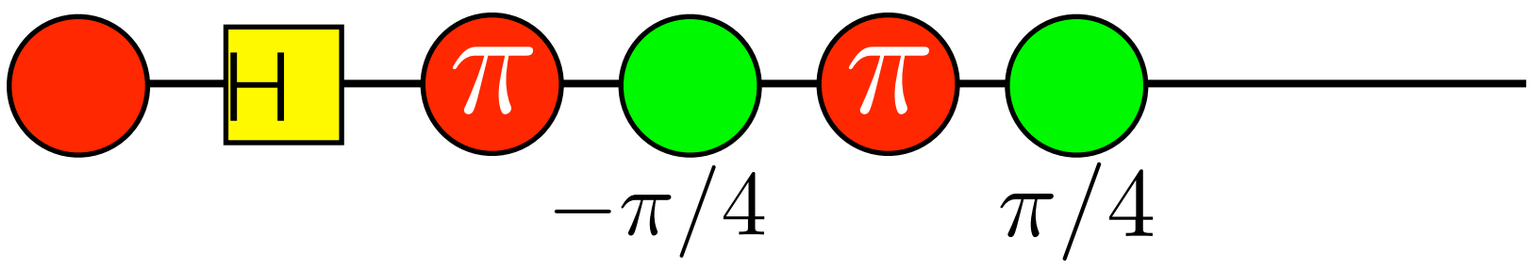
Example: 2-Qubit Quantum Fourier Transform



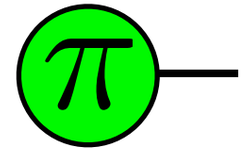
Example: 2-Qubit Quantum Fourier Transform

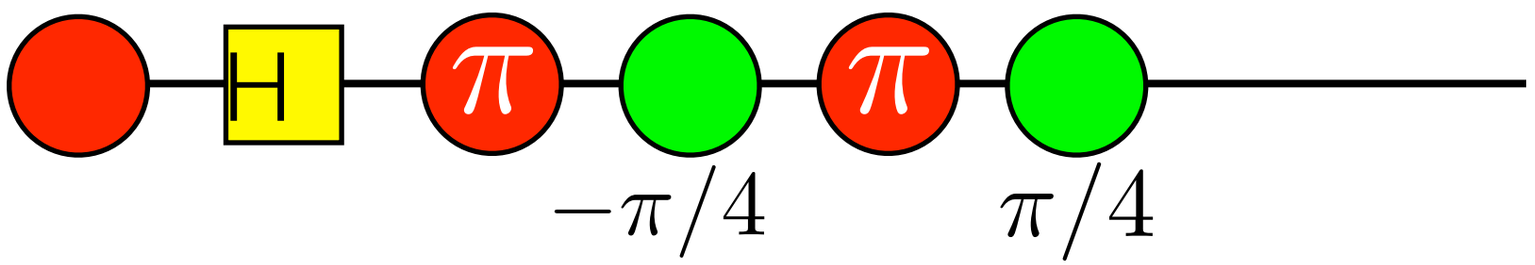


Example: 2-Qubit Quantum Fourier Transform

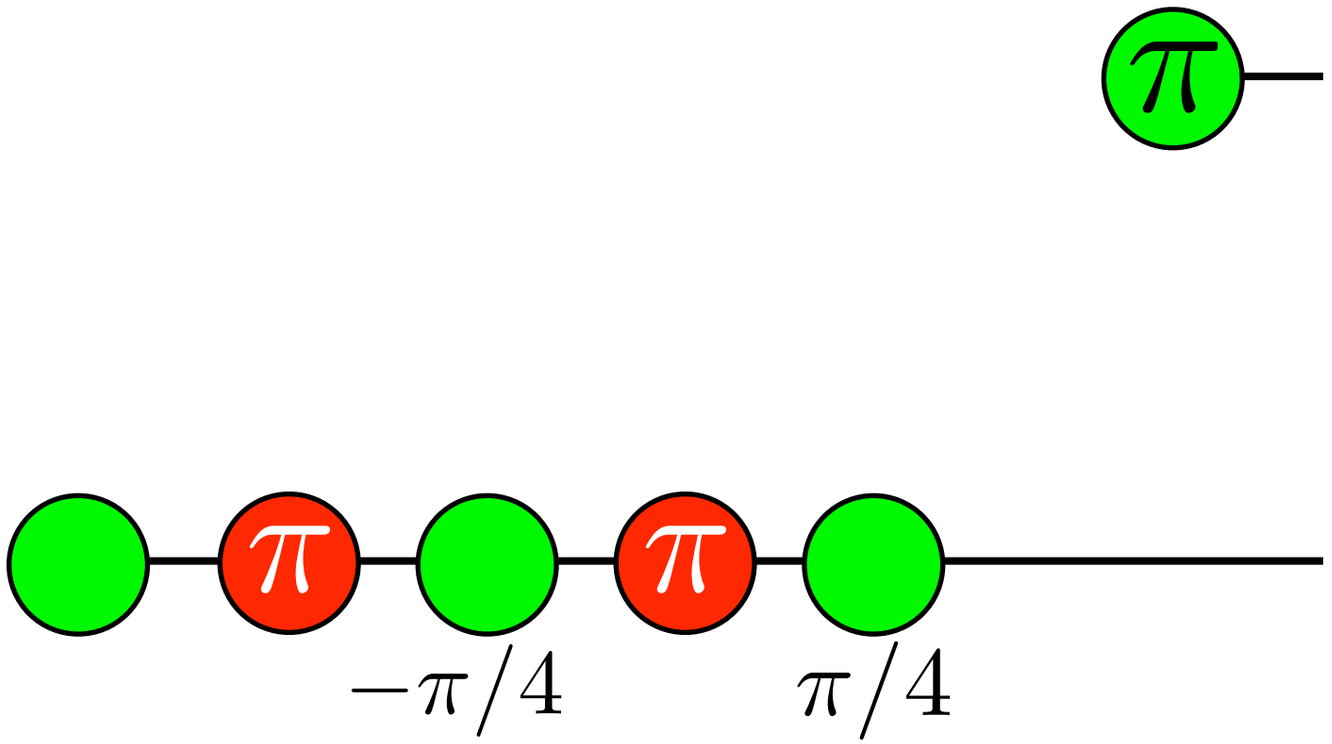


Example: 2-Qubit Quantum Fourier Transform

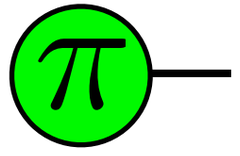


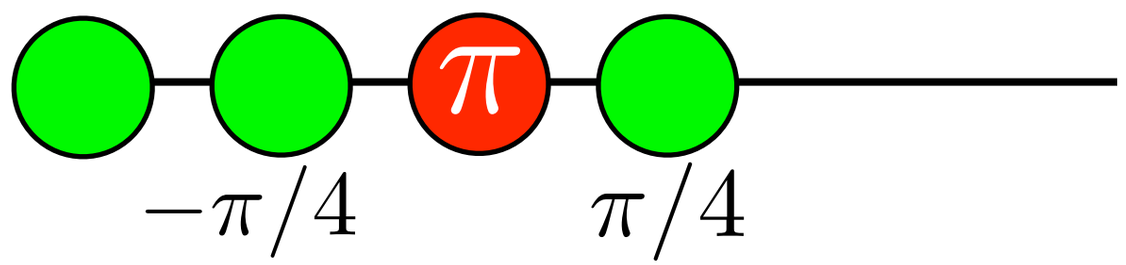


Example: 2-Qubit Quantum Fourier Transform

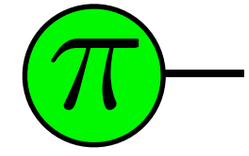


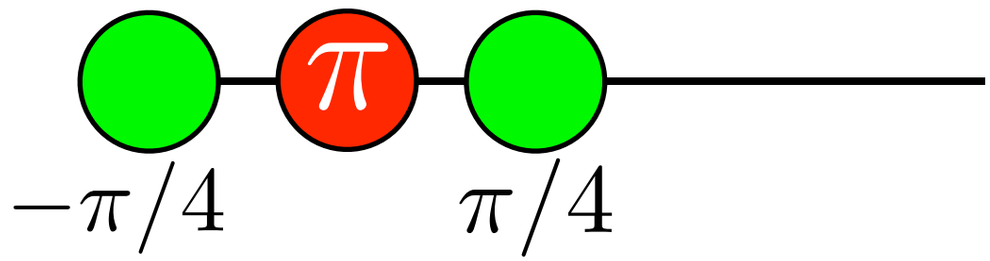
Example: 2-Qubit Quantum Fourier Transform



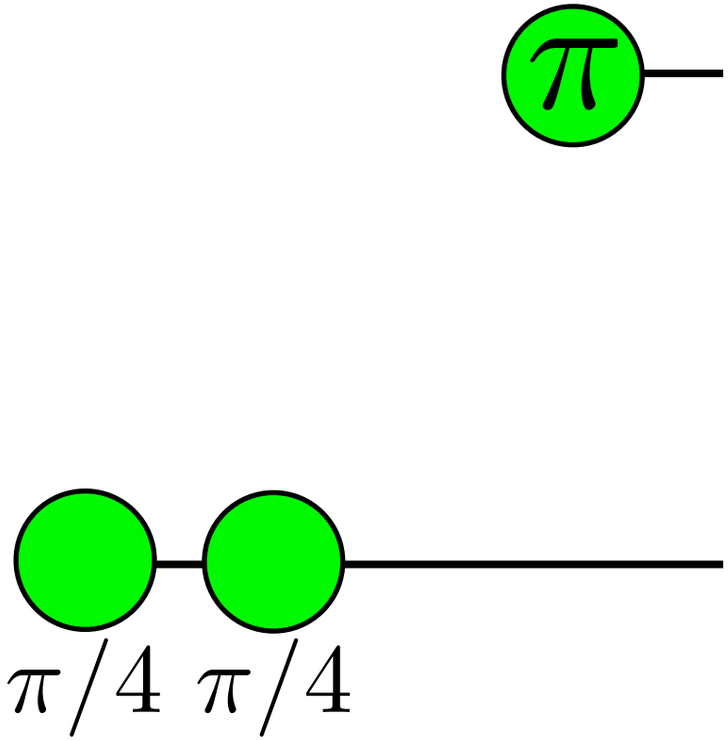


Example: 2-Qubit Quantum Fourier Transform

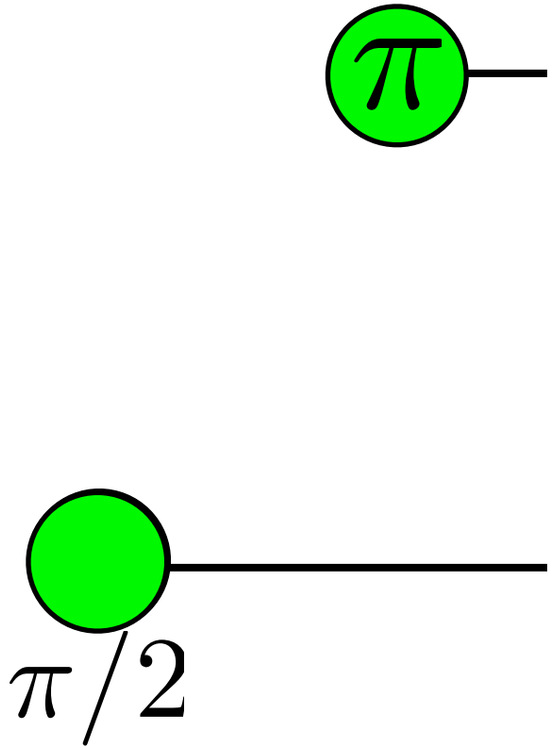




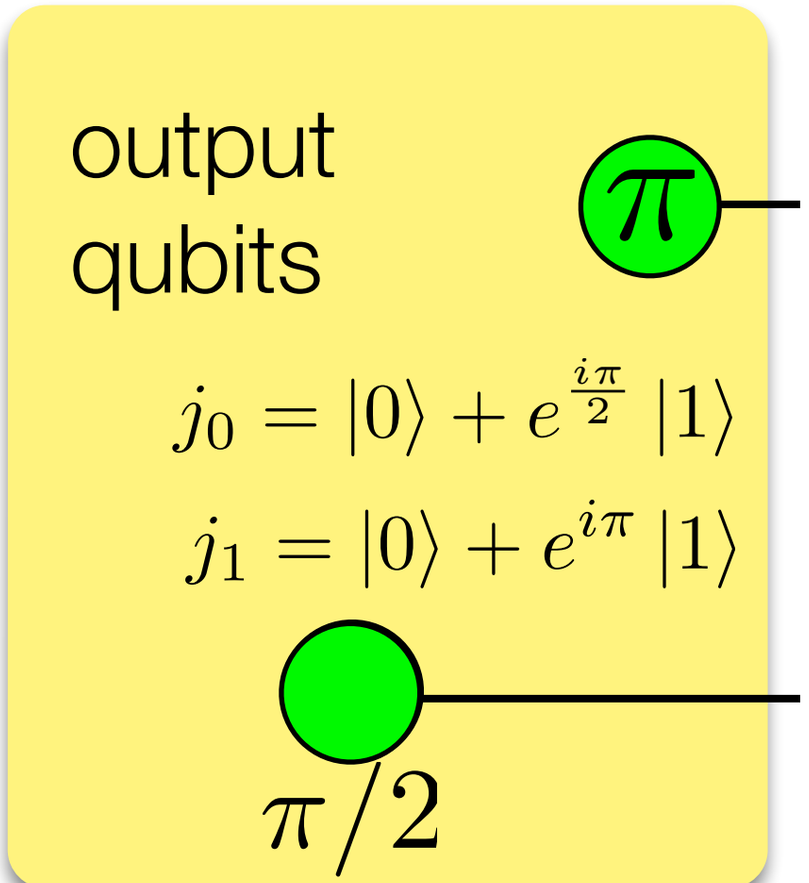
Example: 2-Qubit Quantum Fourier Transform



Example: 2-Qubit Quantum Fourier Transform



Example: 2-Qubit Quantum Fourier Transform



The ZX-calculus is complete

Question:

If $[\![D_1]\!] = [\![D_2]\!]$ then is it provable that $D_1 \overset{ZX}{=} D_2$?

The ZX-calculus is complete

Question:

If $[\![D_1]\!] = [\![D_2]\!]$ then is it provable that $D_1 \overset{ZX}{=} D_2$?

Theorem (Backens, 2012) **:**

If D_1 and D_2 are from the **stabilizer** fragment then YES.

M. Backens. The zx-calculus is complete for stabilizer quantum mechanics. New Journal of Physics, 16(9):093021, 2014. arXiv:1307.7025

The ZX-calculus is complete

Question:

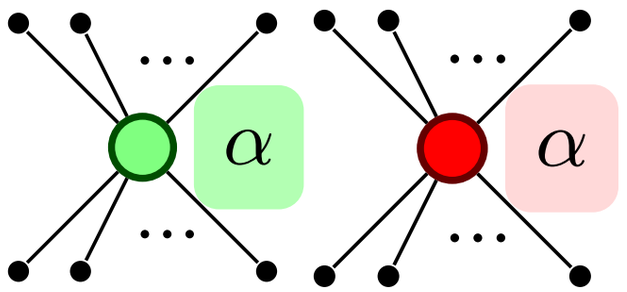
If $[\![D_1]\!] = [\![D_2]\!]$ then is it provable that $D_1 \overset{ZX}{=} D_2$?

Theorem (Backens, 2012) **:**

If D_1 and D_2 are from the **stabilizer** fragment then YES.

Stabilizer fragment:

Clifford group +
Stabilizer states



$$\alpha \in \{0, \frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}\}$$

M. Backens. The zx-calculus is complete for stabilizer quantum mechanics. New Journal of Physics, 16(9):093021, 2014. arXiv:1307.7025

The ZX-calculus is complete

Question:

If $[\![D_1]\!] = [\![D_2]\!]$ then is it provable that $D_1 \overset{ZX}{=} D_2$?

The ZX-calculus is complete

Question:

If $[\![D_1]\!] = [\![D_2]\!]$ then is it provable that $D_1 \overset{ZX}{=} D_2$?

Theorem (Jeandel, Perdrix & Vilmart **vs** Ng & Wang, 2017) **:**

If we add some new axioms (and maybe generators)
then YES.

The ZX-calculus is complete

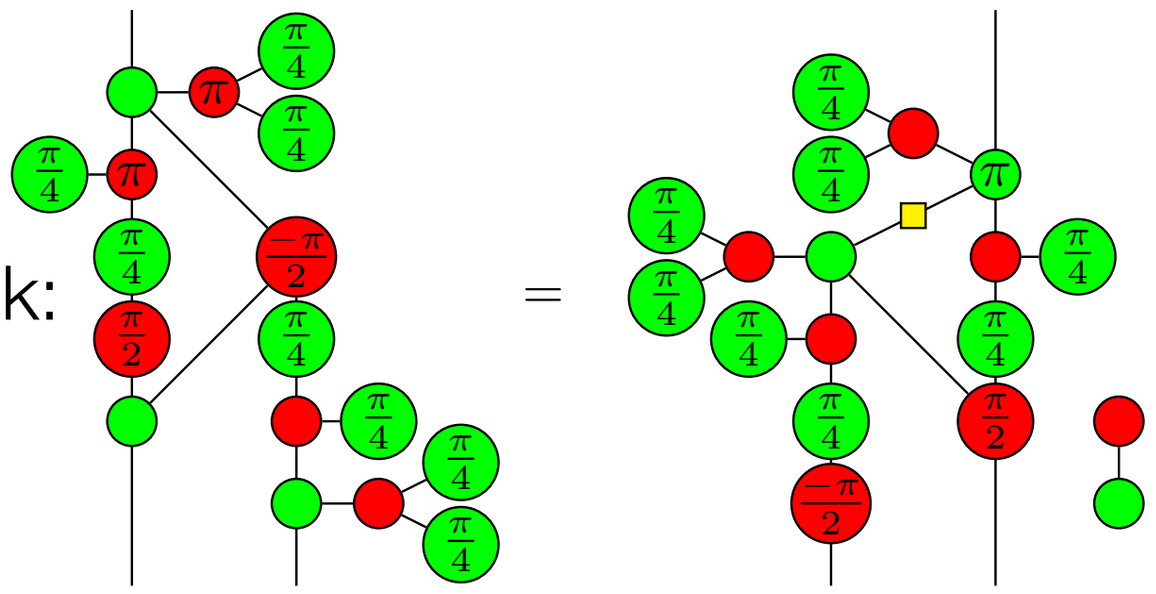
Question:

If $[\![D_1]\!] = [\![D_2]\!]$ then is it provable that $D_1 \overset{ZX}{=} D_2$?

Theorem (Jeandel, Perdrix & Vilmart **vs** Ng & Wang, 2017) **:**

If we add some new axioms (and maybe generators) then YES.

But the new axioms kinda suck:



3.

Application: the colour code

Liam's project :

* Formalise the "smallest interesting colour code" in the ZX-calculus

* Formally verify its basic properties in `quantomatic`

Liam's project :

* Formalise the "smallest interesting colour code" in the ZX-calculus

* Formally verify its basic properties in `quantomatic`

Liam's project :

* Formalise the "smallest interesting colour code" in the ZX-calculus

* Formally verify its basic properties in `quantomatic`

Liam doesn't know anything about quantum theory!

THE SMALLEST INTERESTING COLOUR CODE

September 26, 2016

What is the smallest interesting colour code? The first possible answer is the 7 qubit Steane code. Except, it isn't especially interesting. In particular, the transversal gates of the Steane code are the Clifford group. Really interesting codes have transversal gates outside the Clifford group, and may be used in concert with gauge-fixing or magic state distillation.

Those familiar with the field will immediately retort that the 15 qubit Reed-Muller code is a colour code as was observed in 2006 by Bombin and Martin-Delgado. And it is interesting. The non-Clifford gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

is transversal for the 15 qubit code, in the sense that

$$T_L^\dagger = T^{\otimes 15}.$$

https://earltcampbell.com/2016/09/26/the-smallest-interesting-colour-code/

THE SMALLEST INTERESTING COLOUR CODE

September 26, 2016

What is the smallest interesting colour code? The first possible answer is the 7 qubit Steane code. Except, it isn't especially interesting. In particular, the transversal gates of the Steane code are the Clifford group. Really interesting codes have transversal gates outside the Clifford group, and may be used in concert with gauge-fixing or magic state distillation.

Those familiar with the field will immediately retort that the 15 qubit Reed-Muller code is a colour code as was observed in 2006 by Bombin and Martin-Delgado. And it is interesting. The non-Clifford gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

is transversal for the 15 qubit code, in the sense that $T_L^\dagger = T^{\otimes 15}$.

https://earltcampbell.com/2016/09/26/the-smallest-interesting-colour-code/

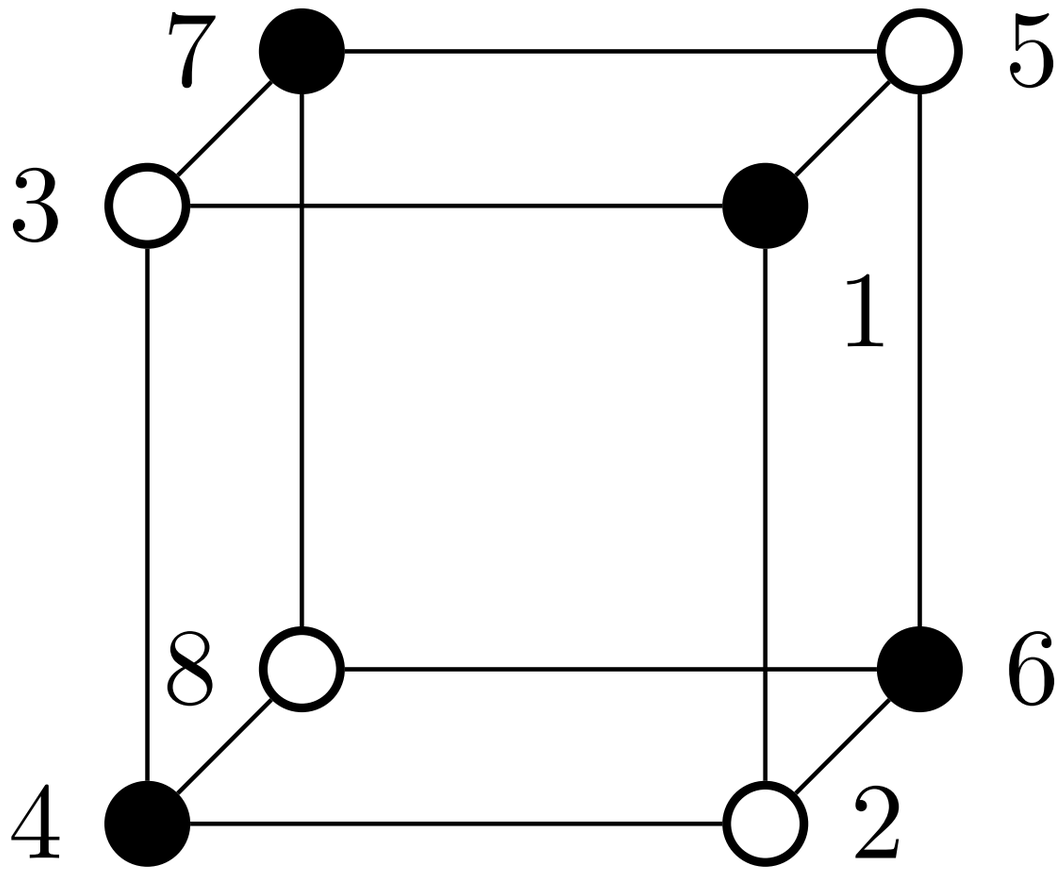
The smallest interesting colour code

- **[[8,3,2]] code:**
  - 8 physical qubits
  - 3 logical qubits
  - distance 2

The smallest interesting colour code

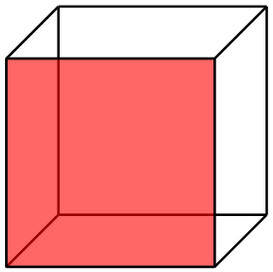
logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$

The smallest interesting colour code



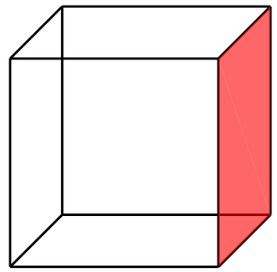
The smallest interesting colour code

X_{L1}



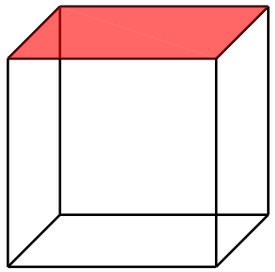
$X \otimes X \otimes X \otimes X \otimes I \otimes I \otimes I \otimes I$

X_{L2}



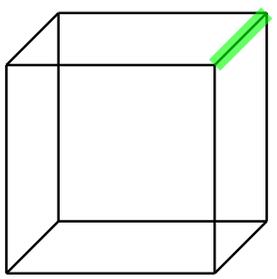
$X \otimes X \otimes I \otimes I \otimes X \otimes X \otimes I \otimes I$

X_{L3}



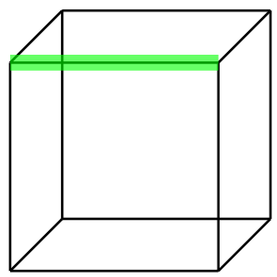
$X \otimes I \otimes X \otimes I \otimes X \otimes I \otimes X \otimes I$

Z_{L1}



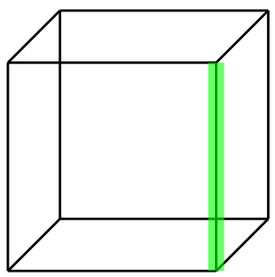
$Z \otimes I \otimes I \otimes I \otimes Z \otimes I \otimes I \otimes I$

Z_{L2}



$Z \otimes I \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I$

Z_{L3}



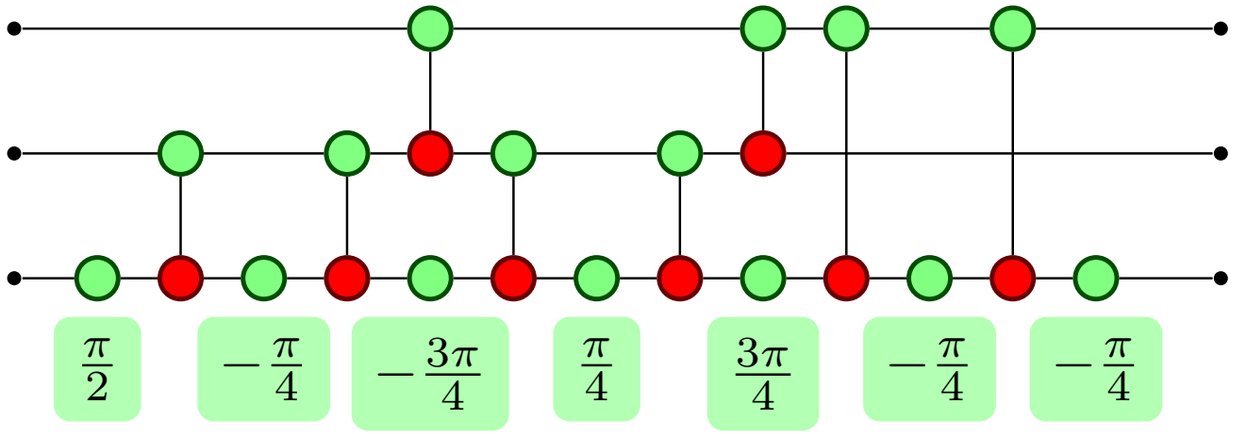
$Z \otimes Z \otimes I \otimes I \otimes I \otimes I \otimes I \otimes I$

The smallest interesting colour code

$$CCZ_{L_1,L_2,L_3} = T \otimes T^\dagger \otimes T^\dagger \otimes T \otimes T^\dagger \otimes T \otimes T \otimes T^\dagger$$

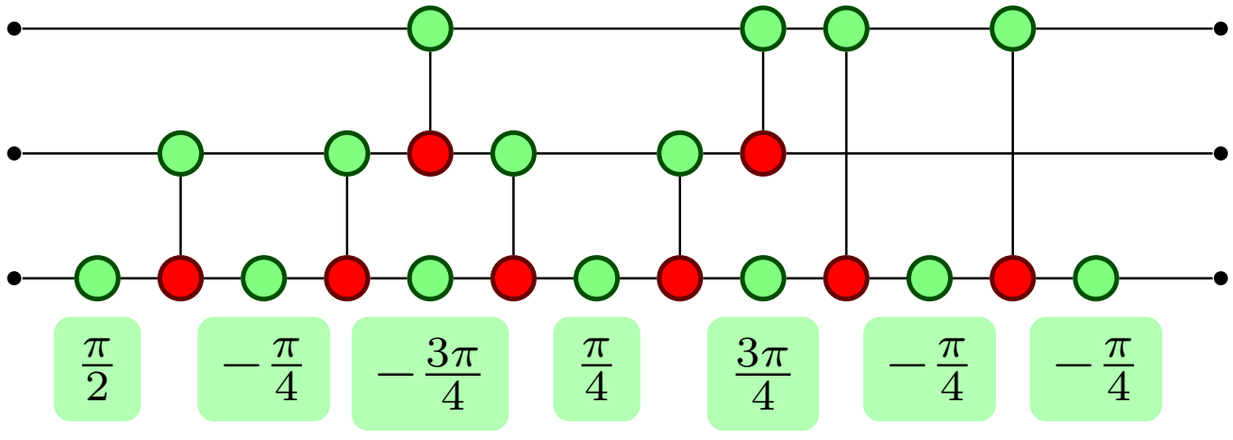
The smallest interesting colour code

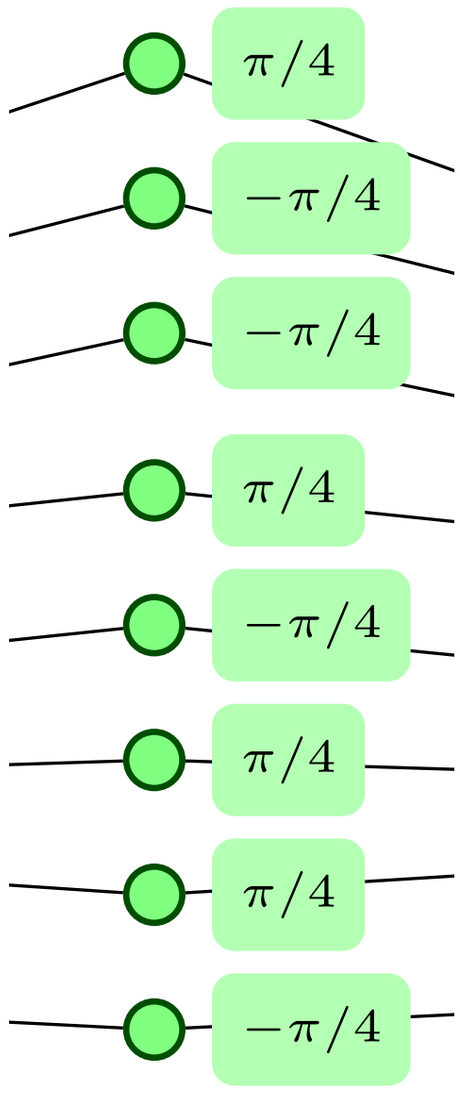
$$CCZ_{L_1,L_2,L_3} = T \otimes T^\dagger \otimes T^\dagger \otimes T \otimes T^\dagger \otimes T \otimes T \otimes T^\dagger$$



The smallest interesting colour code

$$CCZ_{L_1,L_2,L_3} = T \otimes T^\dagger \otimes T^\dagger \otimes T \otimes T^\dagger \otimes T \otimes T \otimes T^\dagger$$



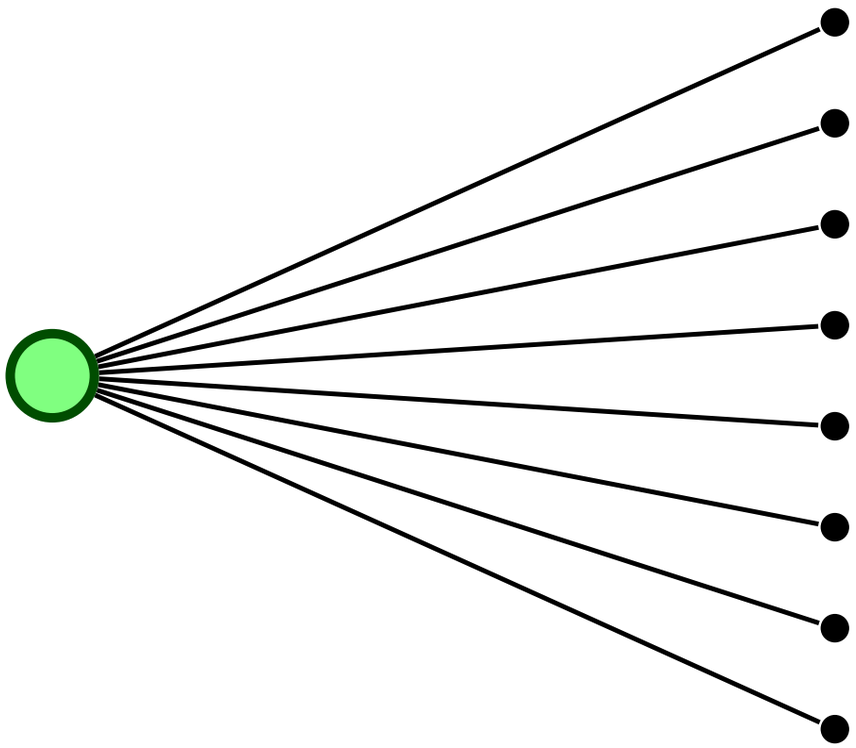


Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$

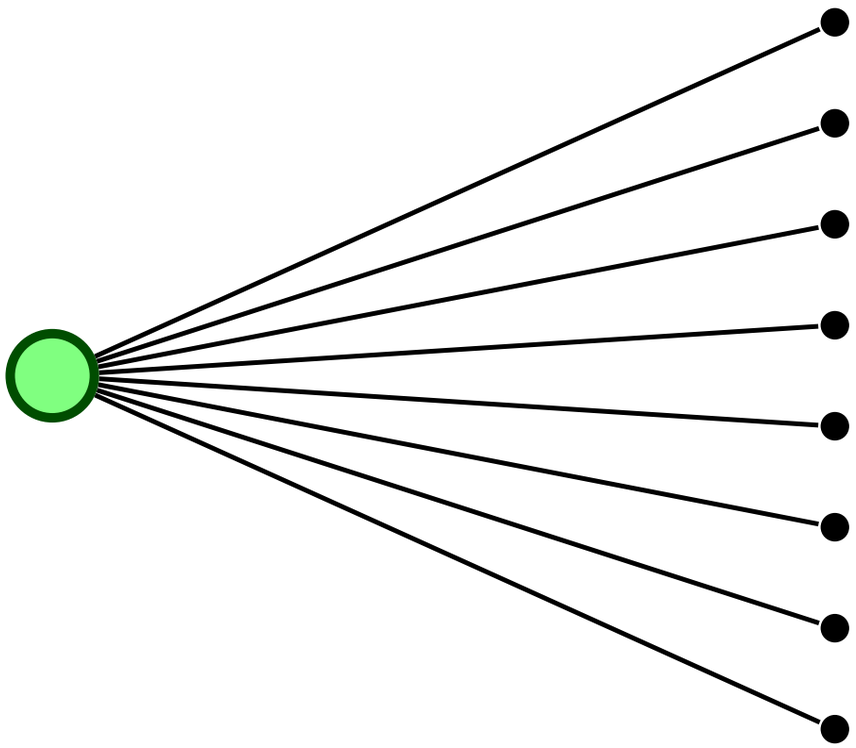
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



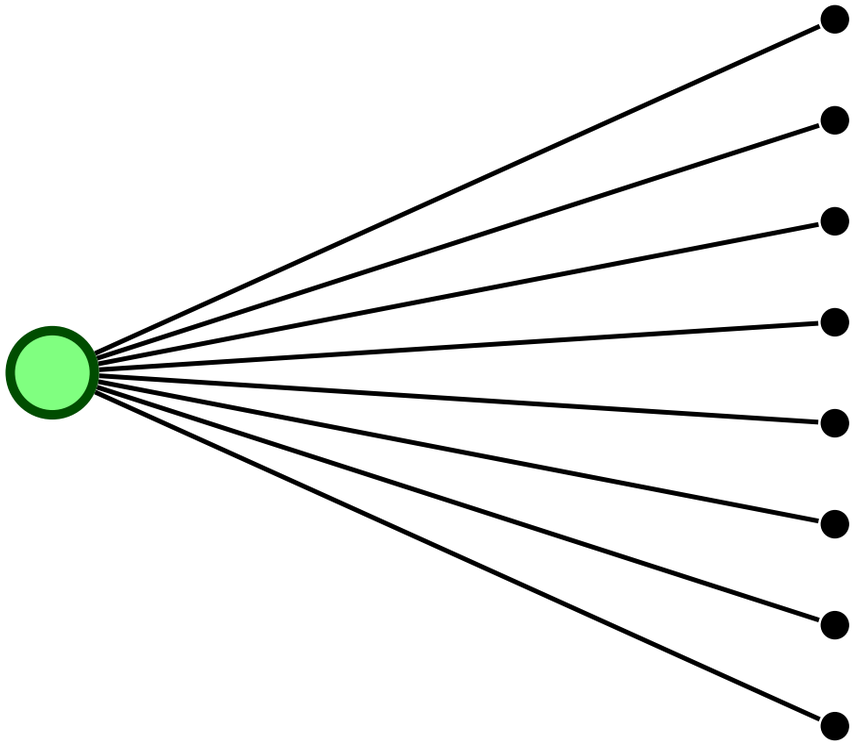
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



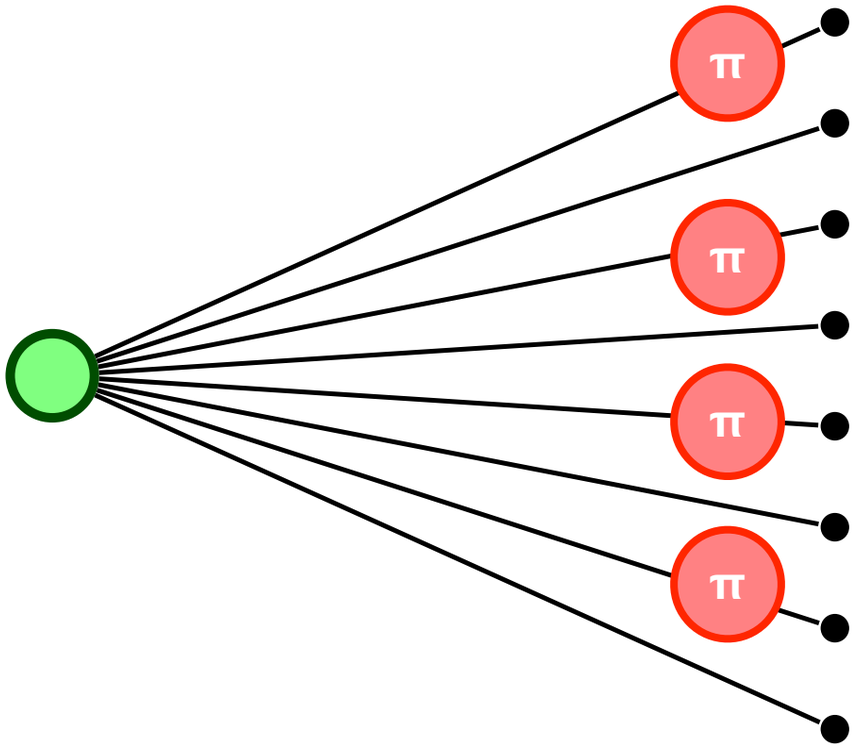
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



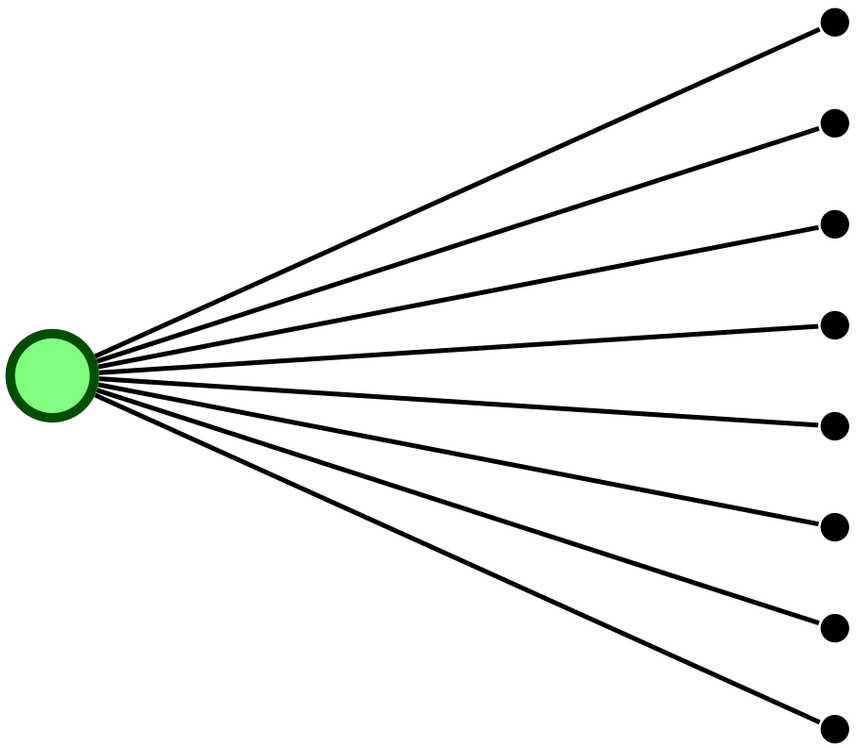
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



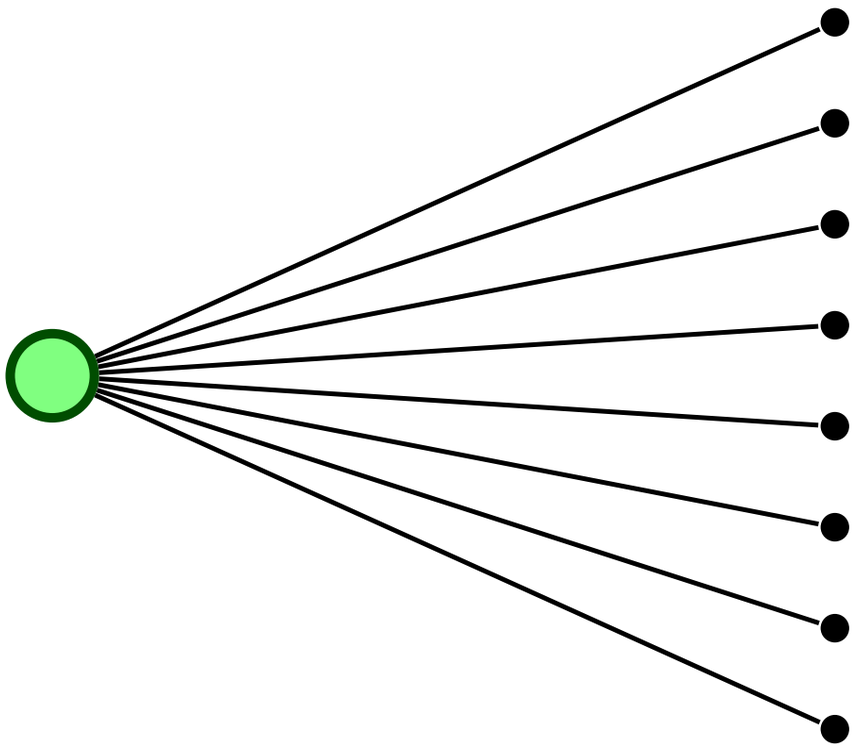
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



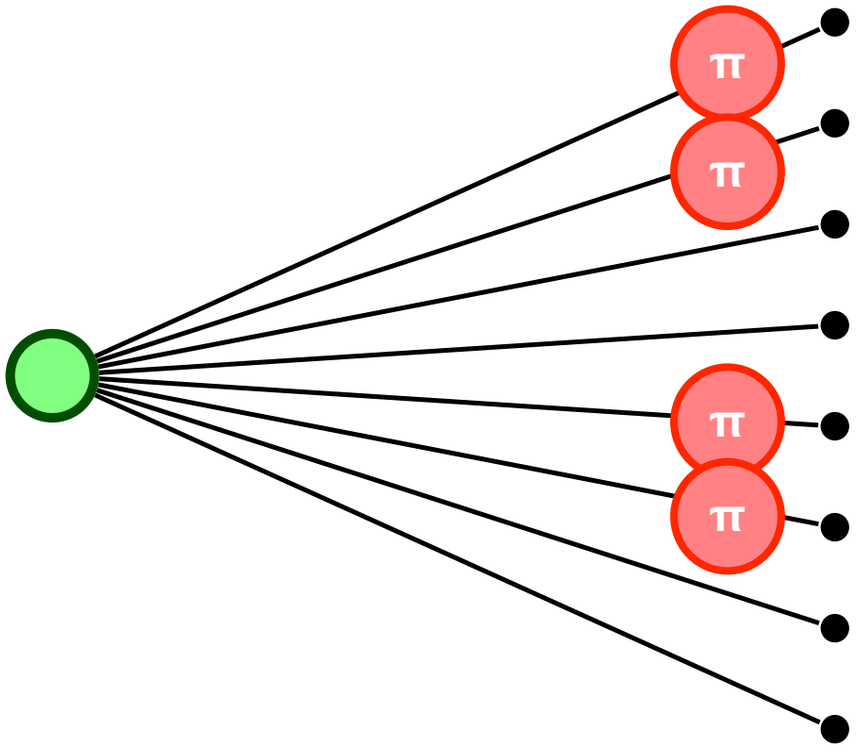
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



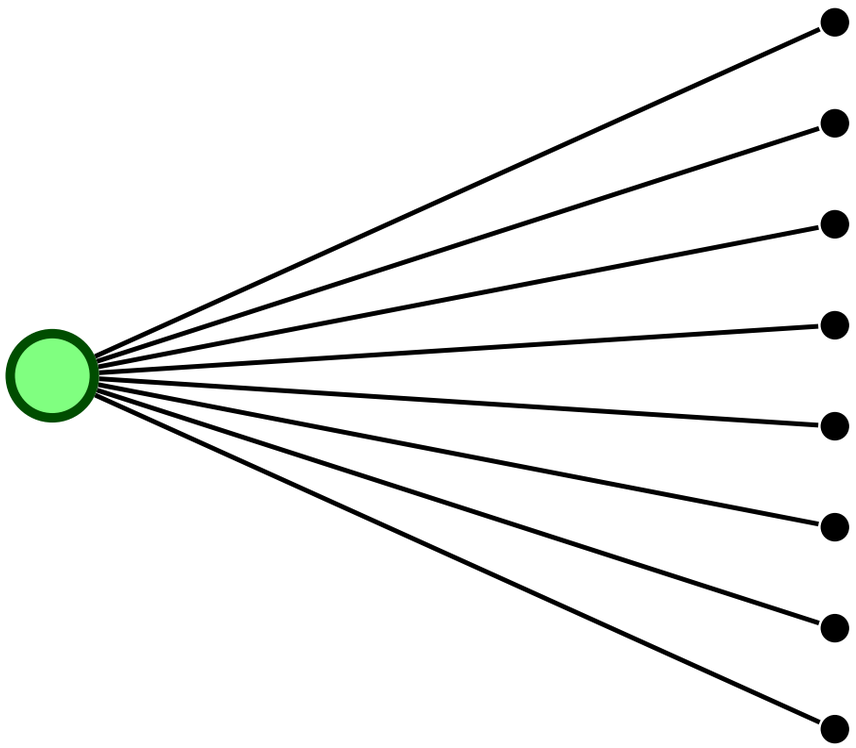
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



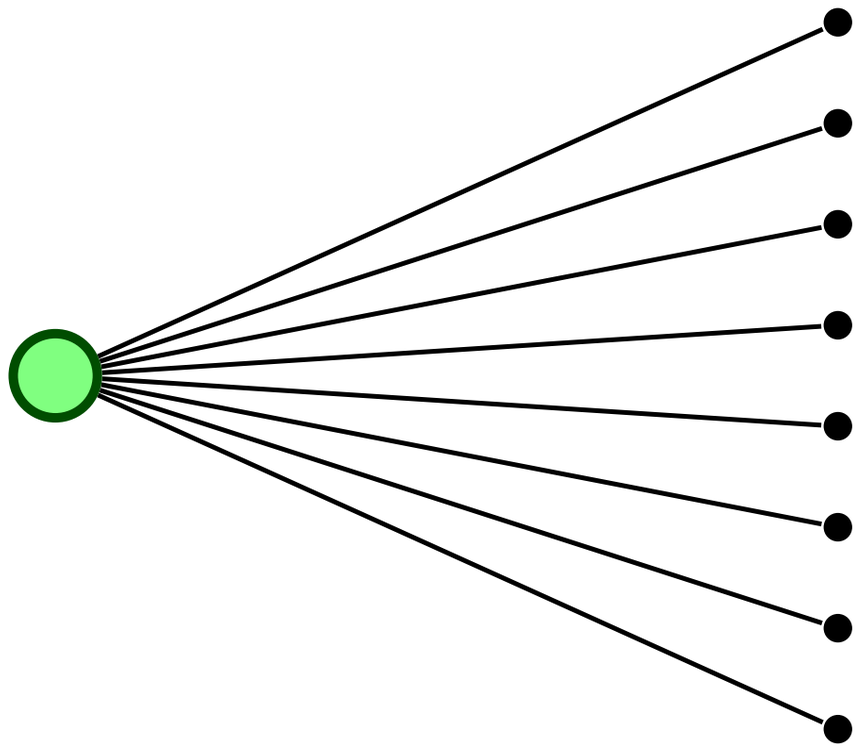
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$



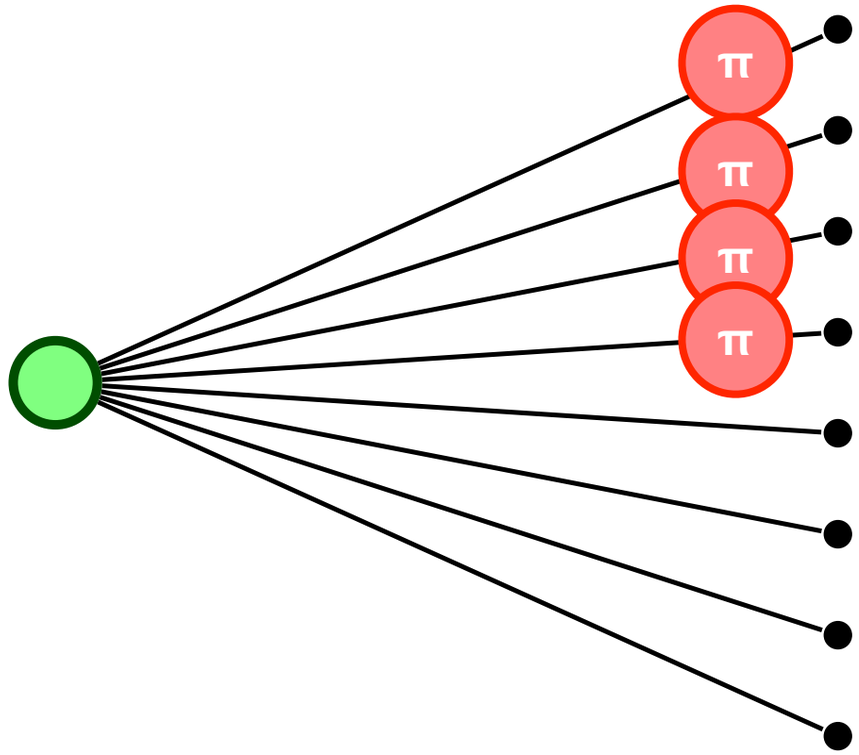
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$

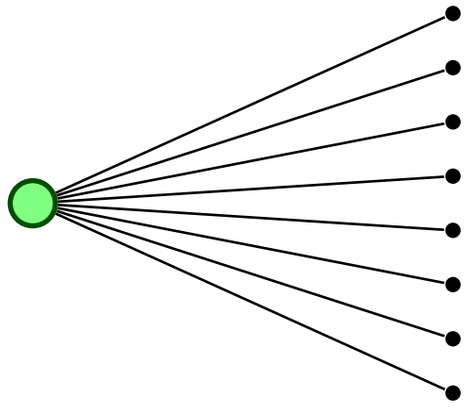


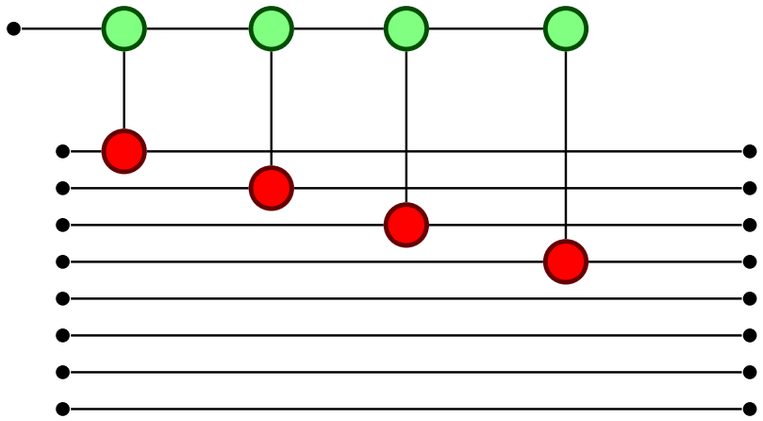
Encoding

logical state	codeword state
$\|000\rangle$	$\frac{1}{\sqrt{2}}(\|00000000\rangle + \|11111111\rangle)$
$\|001\rangle$	$\frac{1}{\sqrt{2}}(\|10101010\rangle + \|01010101\rangle)$
$\|010\rangle$	$\frac{1}{\sqrt{2}}(\|11001100\rangle + \|00110011\rangle)$
$\|011\rangle$	$\frac{1}{\sqrt{2}}(\|01100110\rangle + \|10011001\rangle)$
$\|100\rangle$	$\frac{1}{\sqrt{2}}(\|11110000\rangle + \|00001111\rangle)$
$\|101\rangle$	$\frac{1}{\sqrt{2}}(\|01011010\rangle + \|10100101\rangle)$
$\|110\rangle$	$\frac{1}{\sqrt{2}}(\|00111100\rangle + \|11000011\rangle)$
$\|111\rangle$	$\frac{1}{\sqrt{2}}(\|10010110\rangle + \|01101001\rangle)$

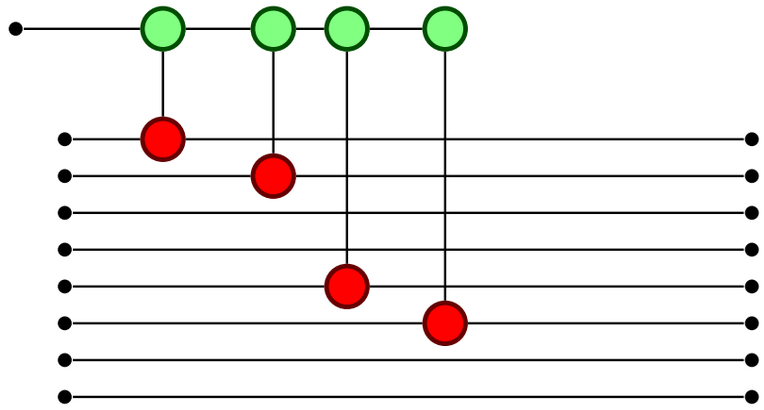


Encoding

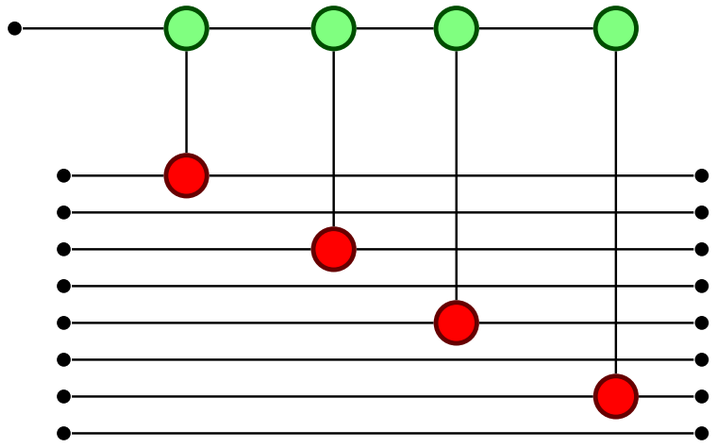




(qubit 1)

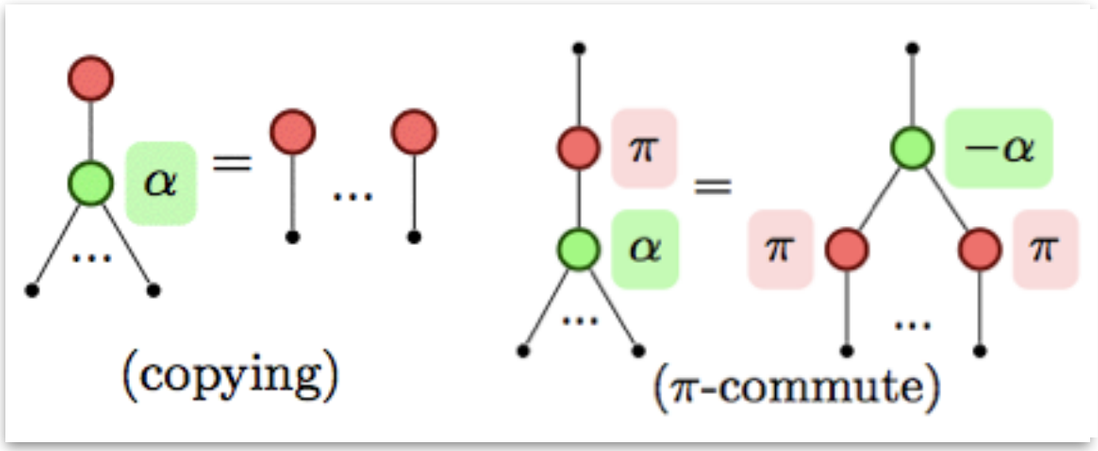


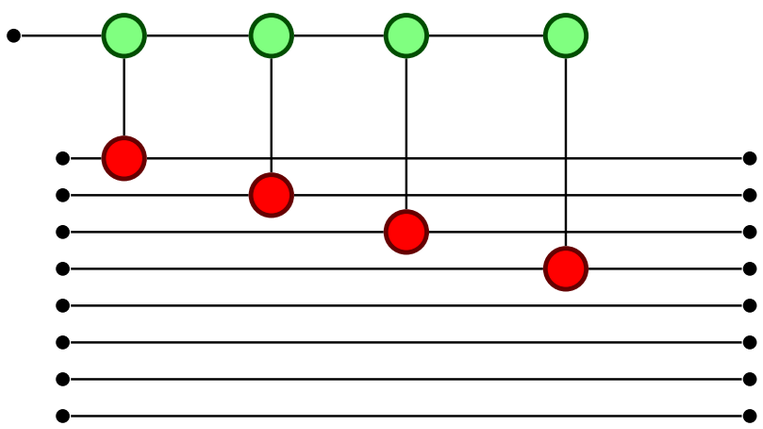
(qubit 2)



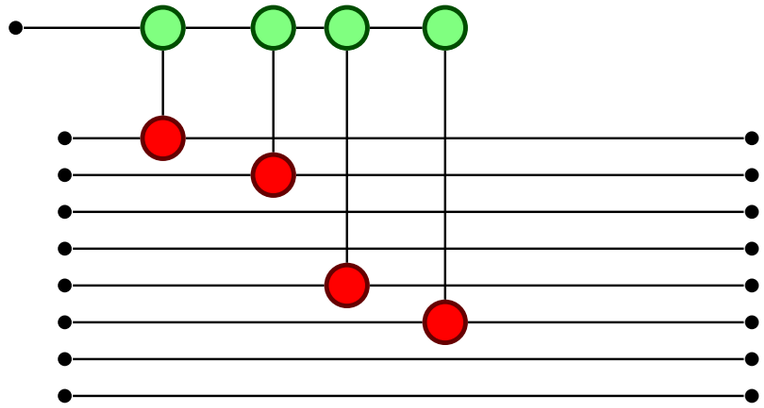
(qubit 3)

Encoding

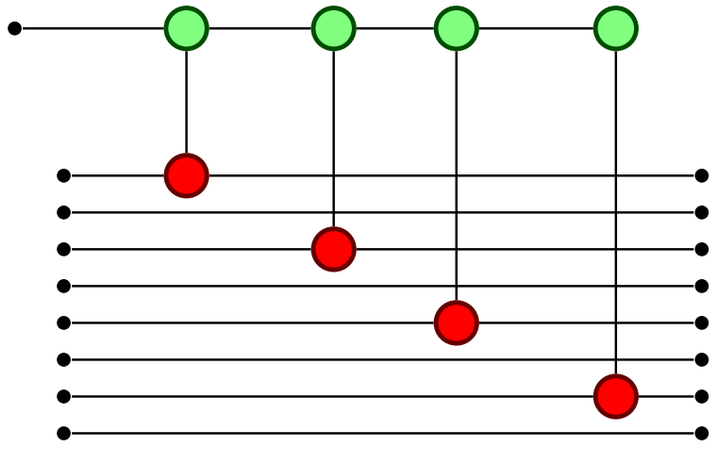




(qubit 1)

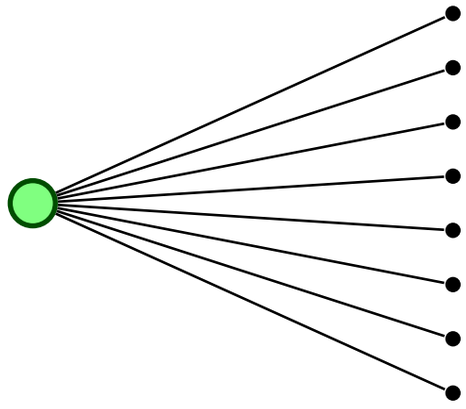


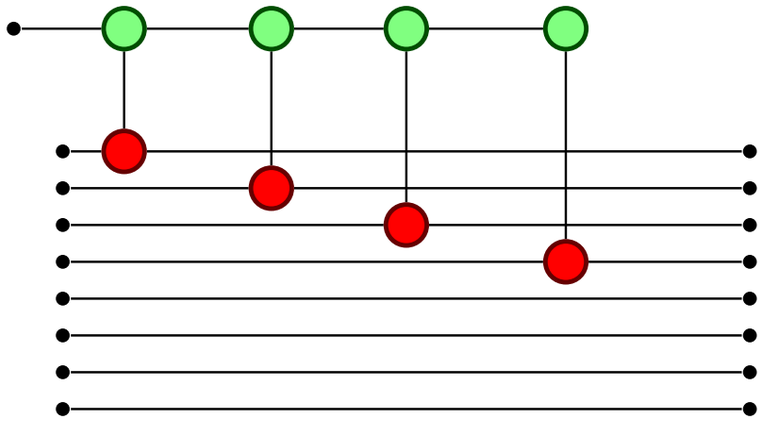
(qubit 2)



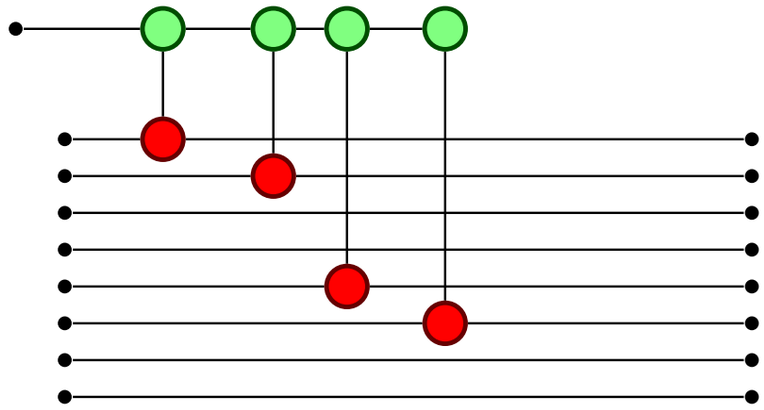
(qubit 3)

Encoding

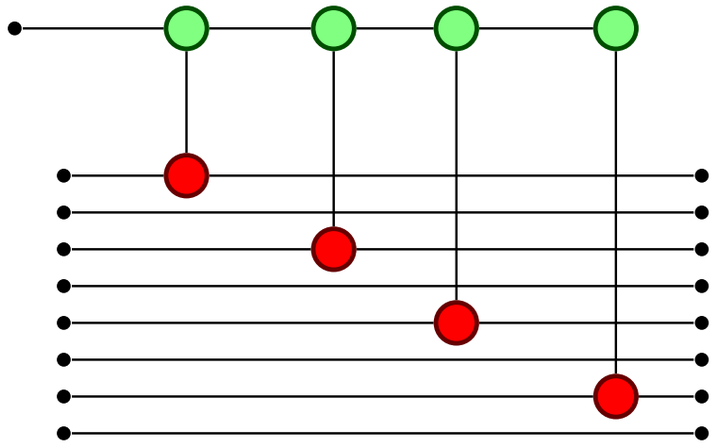




(qubit 1)



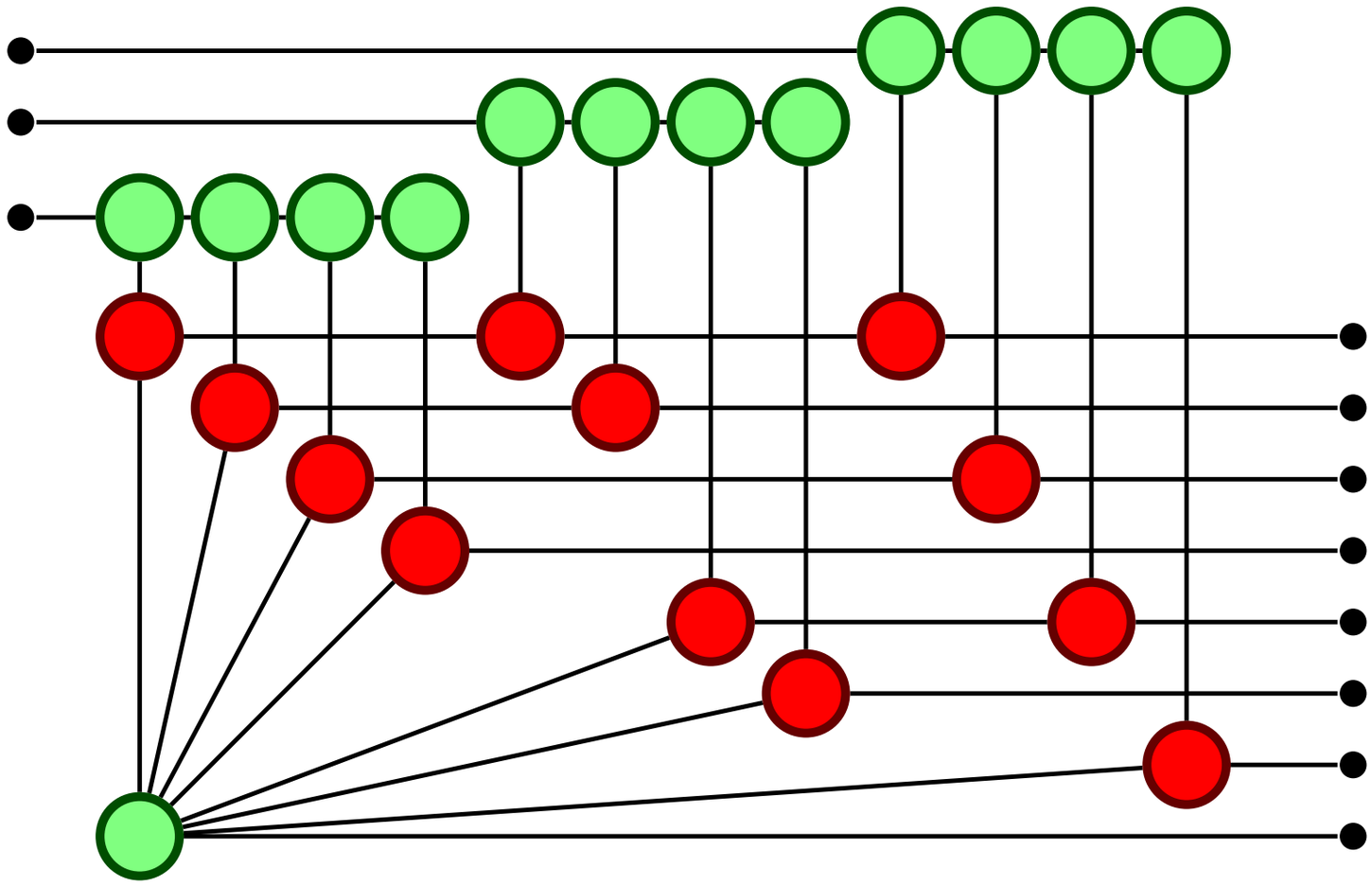
(qubit 2)



(qubit 3)

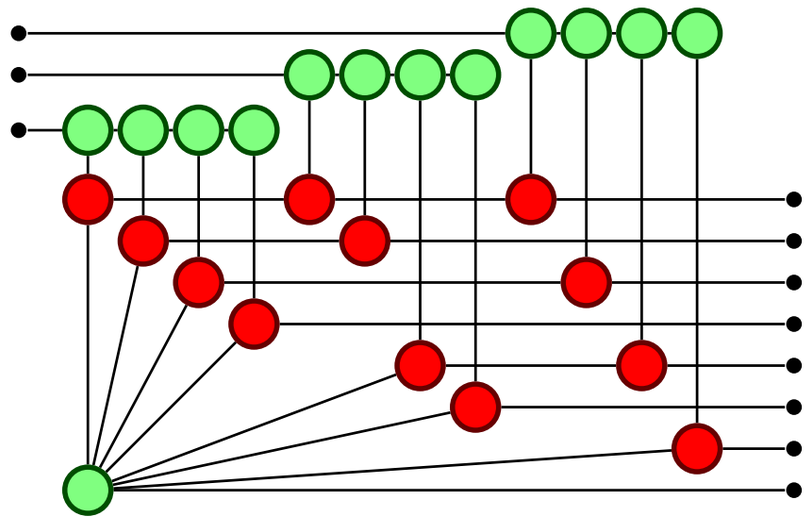
Encoding

Enc :=



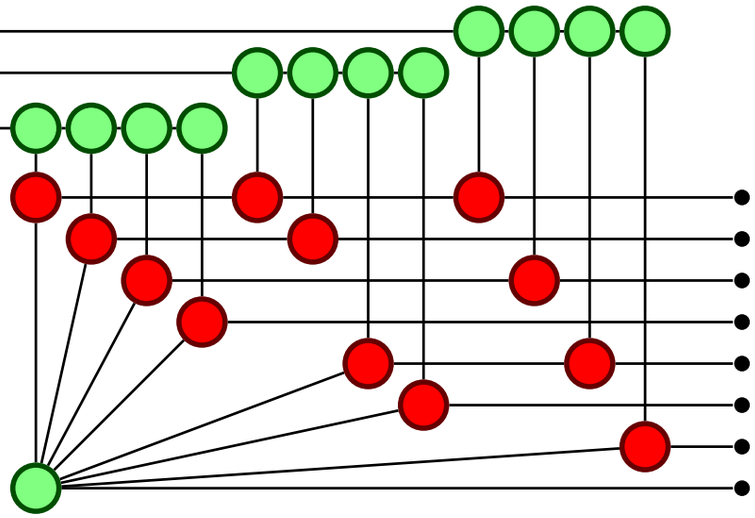
Encoding

Enc :=

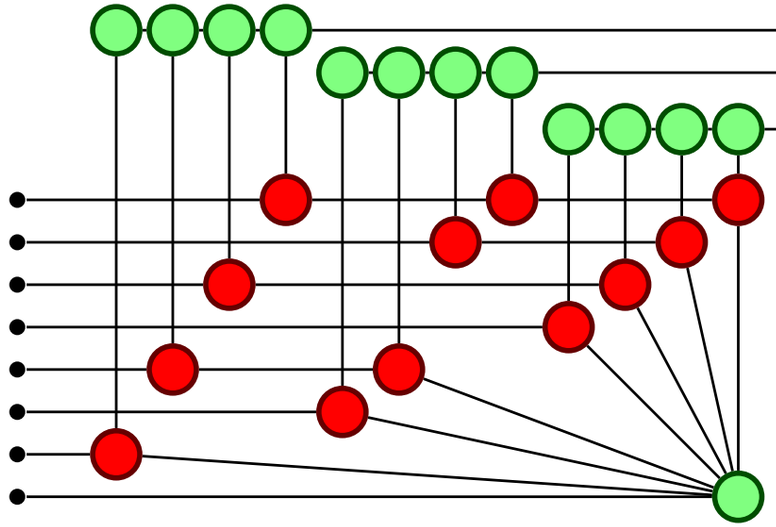


Encoding

$\mathrm{Enc} :=$



$\mathrm{Enc}^\dagger =$



Summary of results

Summary of results

1. $\mathrm{Enc}^\dagger \circ \mathrm{Enc} = \mathrm{id}_3$

Summary of results

1. $\mathrm{Enc}^\dagger \circ \mathrm{Enc} = \mathrm{id}_3$
2. Enc *is a unitary embedding.*

Summary of results

1. $\mathrm{Enc}^\dagger \circ \mathrm{Enc} = \mathrm{id}_3$

2. Enc *is a unitary embedding.*

3. Find P satisfying :

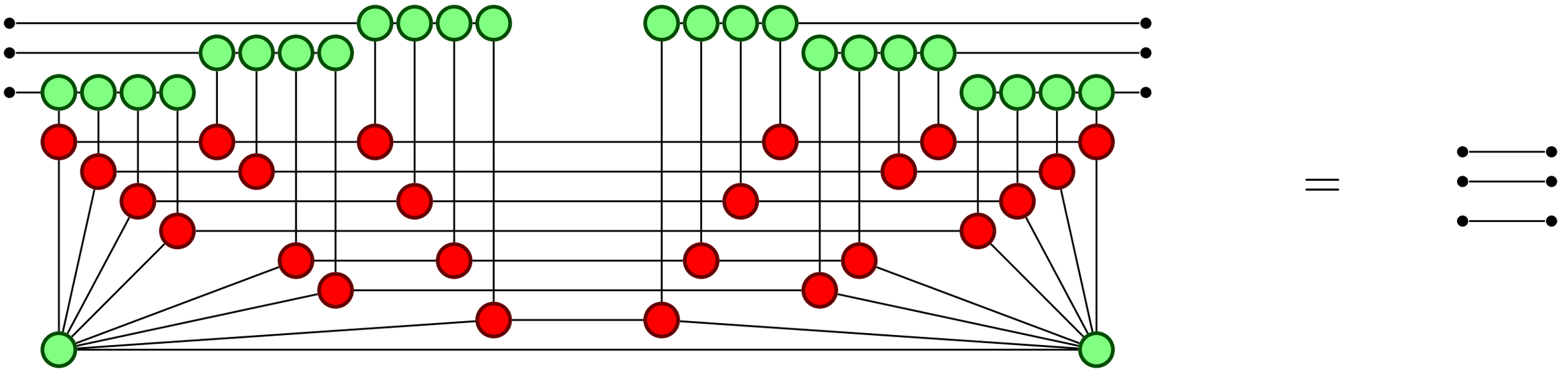
$$L = \mathrm{Enc}^\dagger \circ P \circ \mathrm{Enc}$$

where

$$L \in \{X, Z, \mathrm{CNOT}, \mathrm{CCZ}\}$$

Encode-Decode

- Lemma :

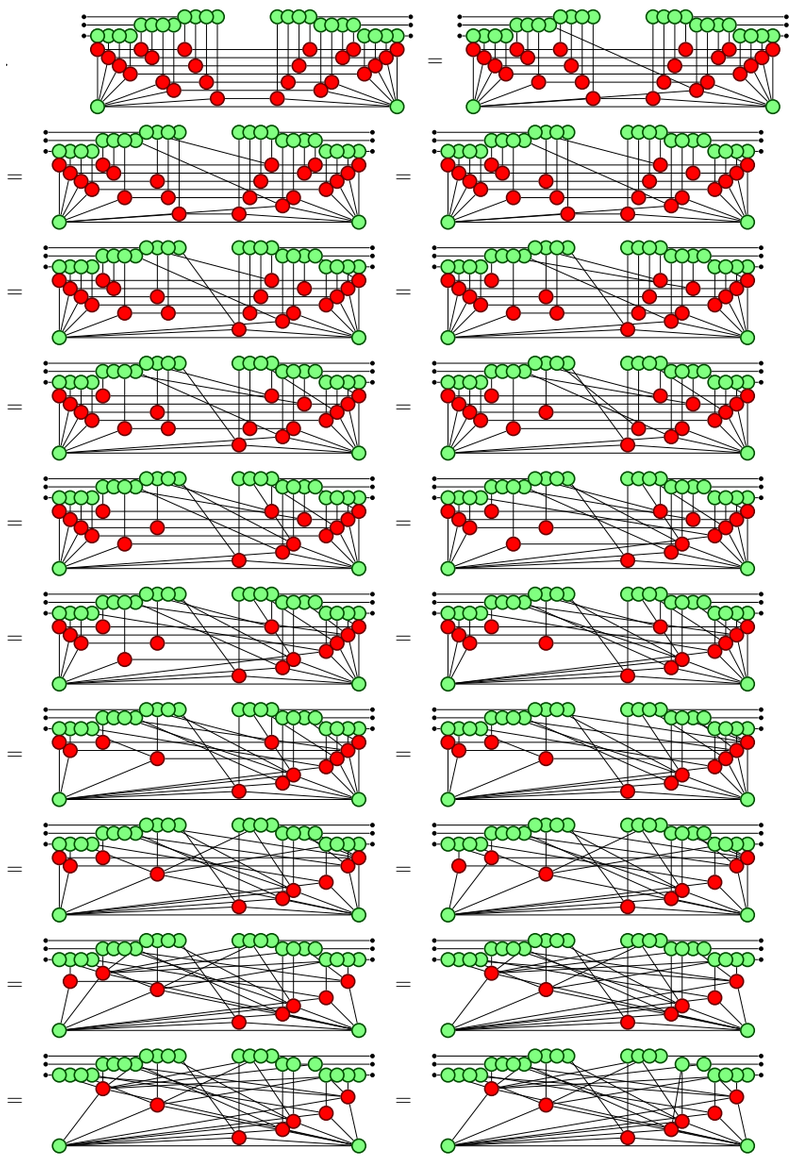


Encode-Decode

- Proof :

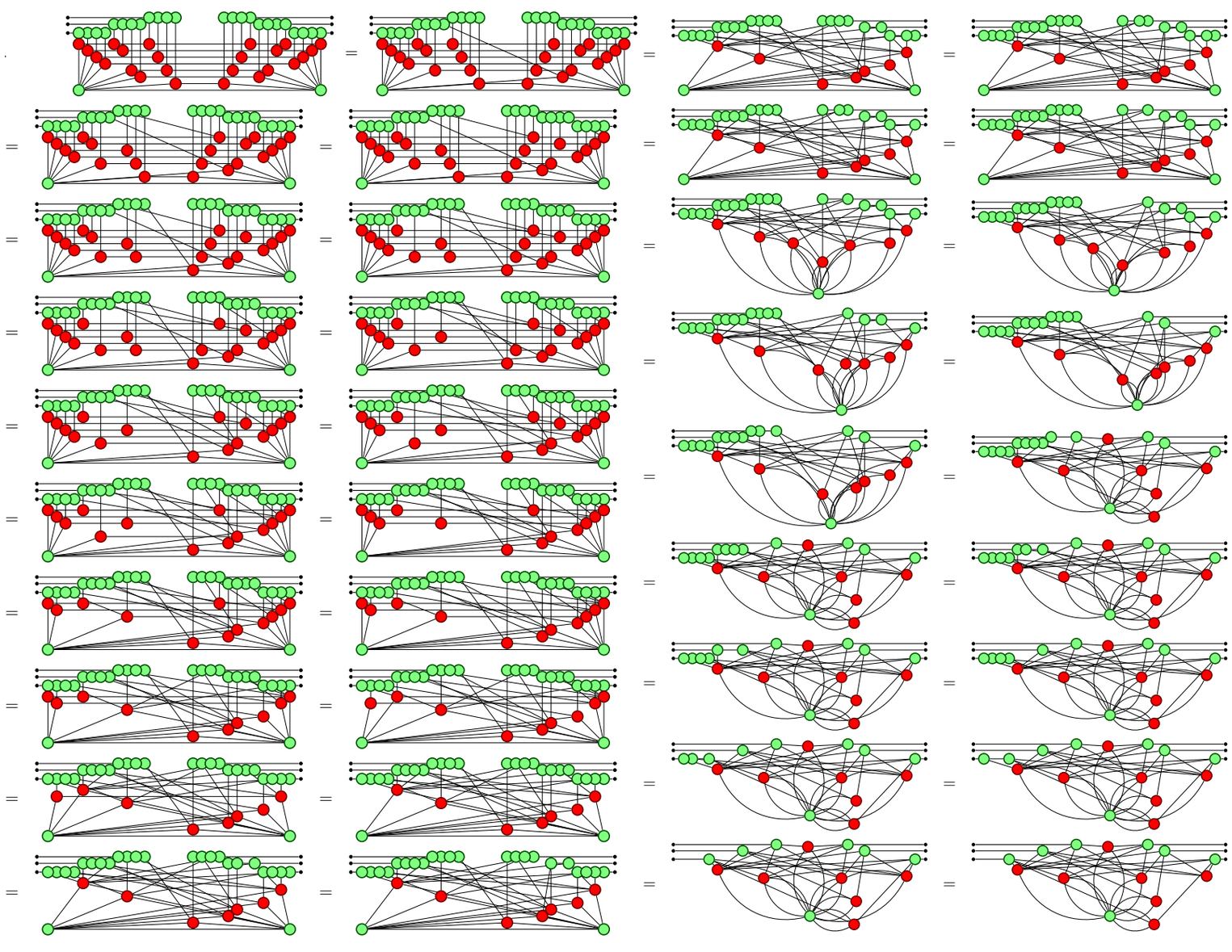
Encode-Decode

- Proof :



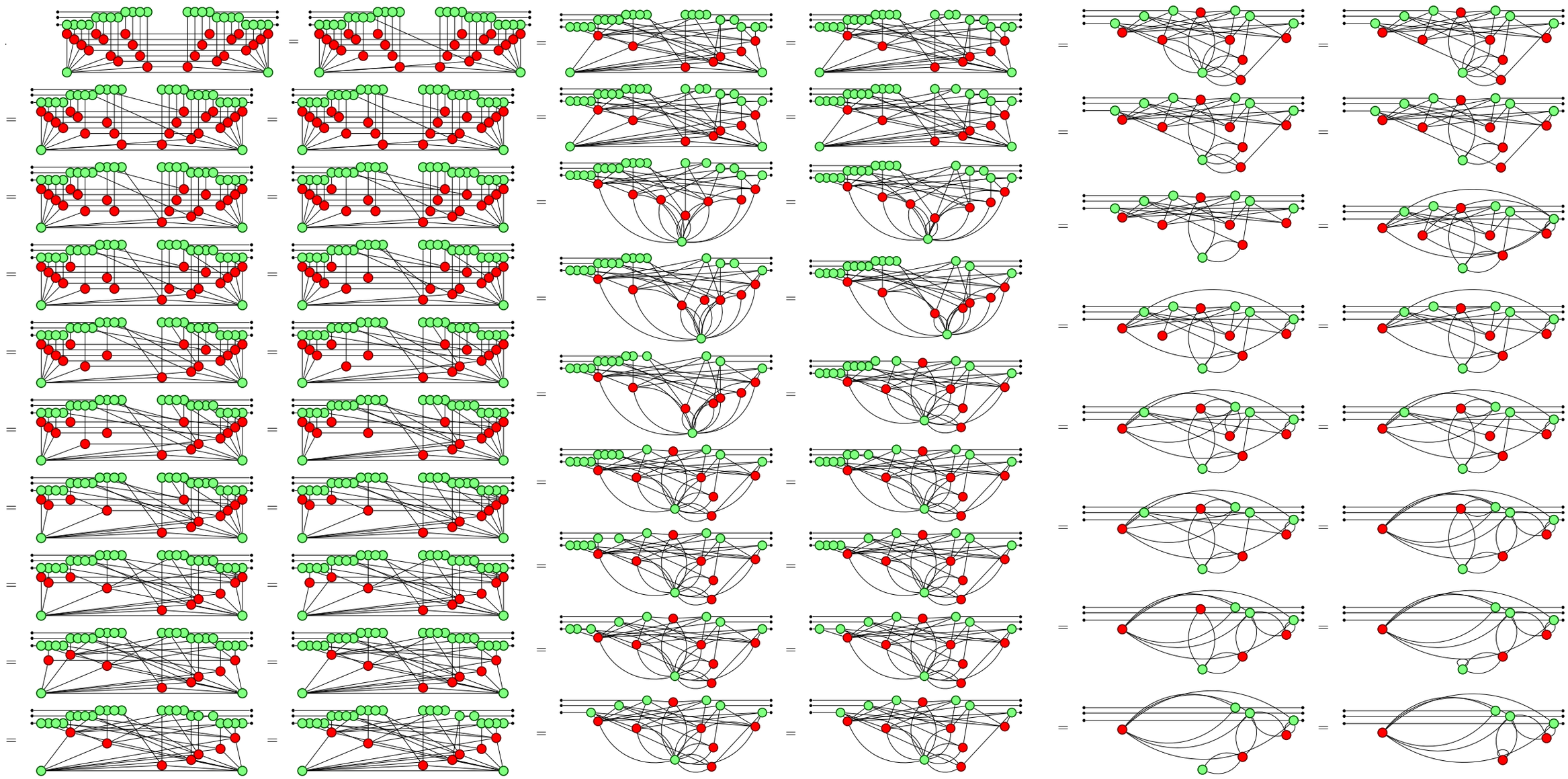
Encode-Decode

- Proof :



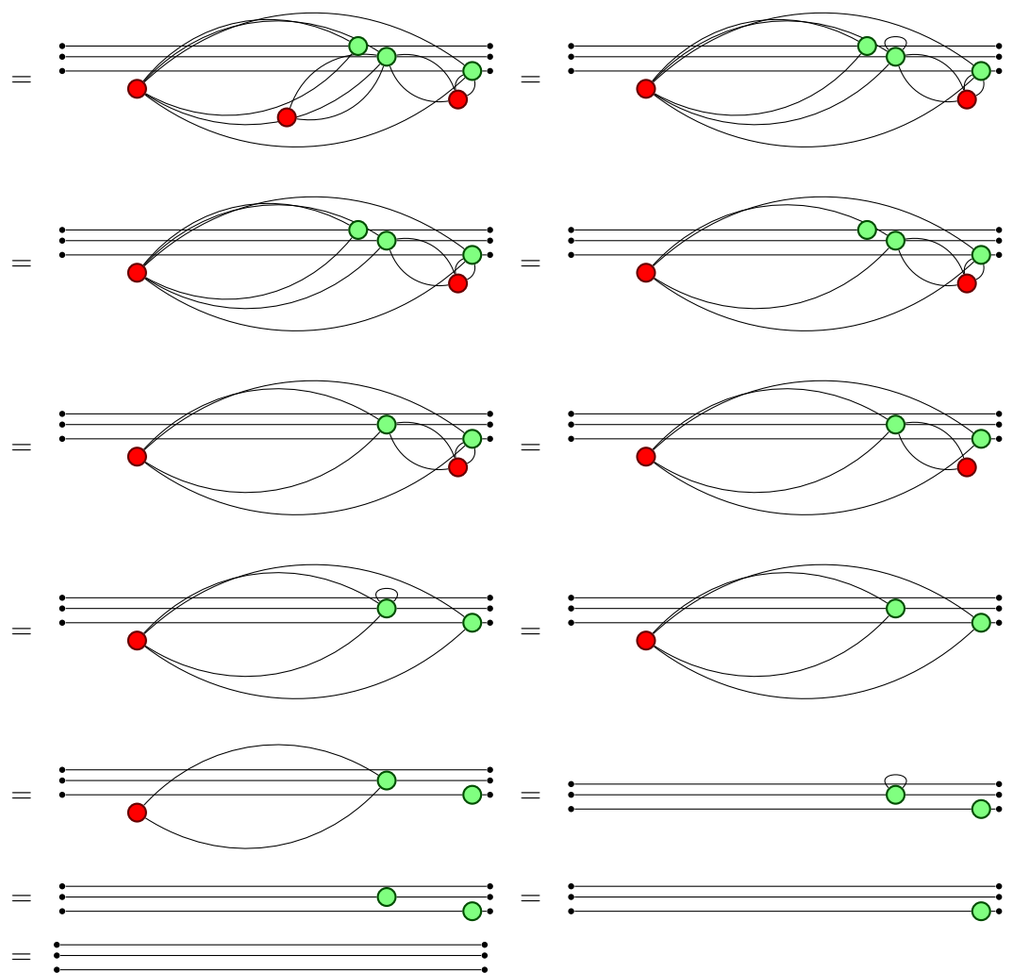
Encode-Decode

- Proof :



Encode-Decode

- Proof (cont.):



□

STOP!

Quanto time!

arXiv Help

To: Ross Duncan <ross.duncan@strath.ac.uk>

Reply-To: help@arxiv.org

[arXiv #197065] Request oversize exception for submit/191538

Dear Ross,

We can usually get around the timeout issue, but not this time.
proceed with uploading the PDF.

It will likely go on hold after it is submitted. Send us an email the

--

Jim

arXiv admin

Try it at home:

1. Download quantomatic

http://quantomatic.github.io

2. Download the proof development

https://gitlab.cis.strath.ac.uk/kwb13215/Colour-Code-QPL

4.

Application: the one-way model

Application 1: MBQC

1WQC is a quantum computer design based on single qubit projective measurements on a graph state.

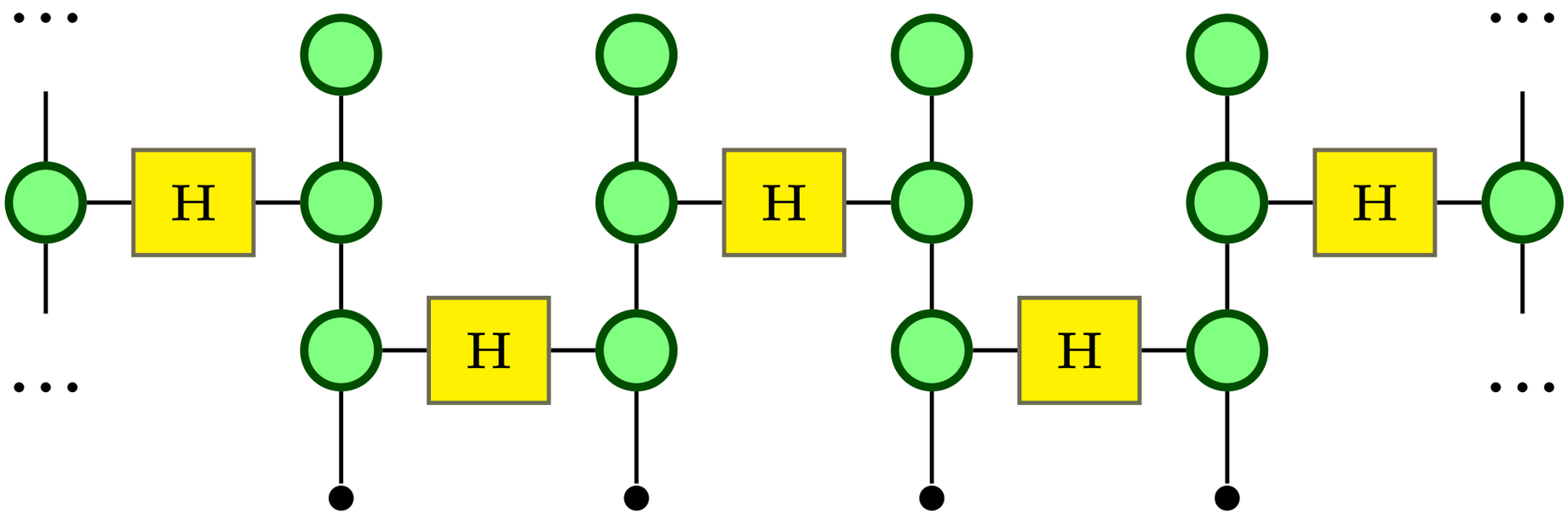
- We can use the ZX-calculus to translate from the 1WQC to circuit model
- Relies on the Hopf algebra normal form
- Produces circuits with minimal space complexity

Graph States

Let G = (V,E) be a simple, undirected graph. Then define:

$$|G\rangle = \bigotimes_{(v,u)\in E} CZ_{vu} \bigotimes_{v\in V} |+\rangle$$

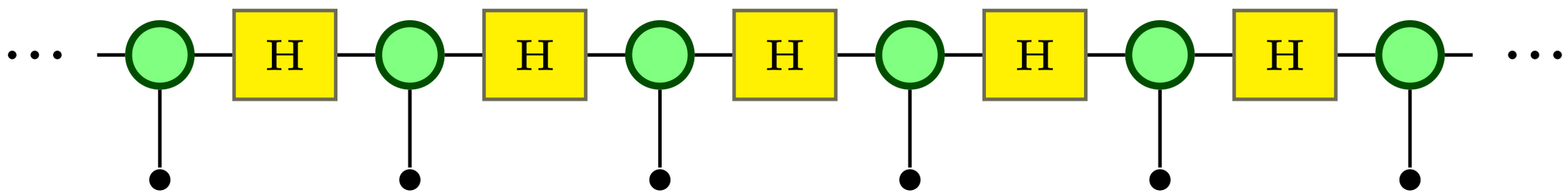
Viewed as circuit we get this:



Graph States

Let G = (V,E) be a simple, undirected graph. Then define:

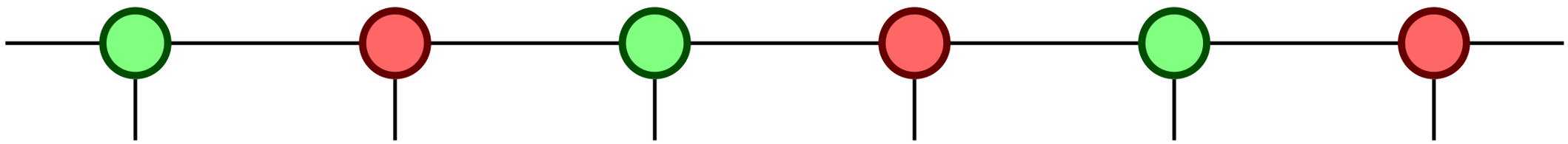
$$|G\rangle = \bigotimes_{(v,u)\in E} CZ_{vu} \bigotimes_{v\in V} |+\rangle$$



Graph States

Let G = (V,E) be a simple, undirected graph. Then define:

$$|G\rangle = \bigotimes_{(v,u)\in E} CZ_{vu} \bigotimes_{v\in V} |+\rangle$$

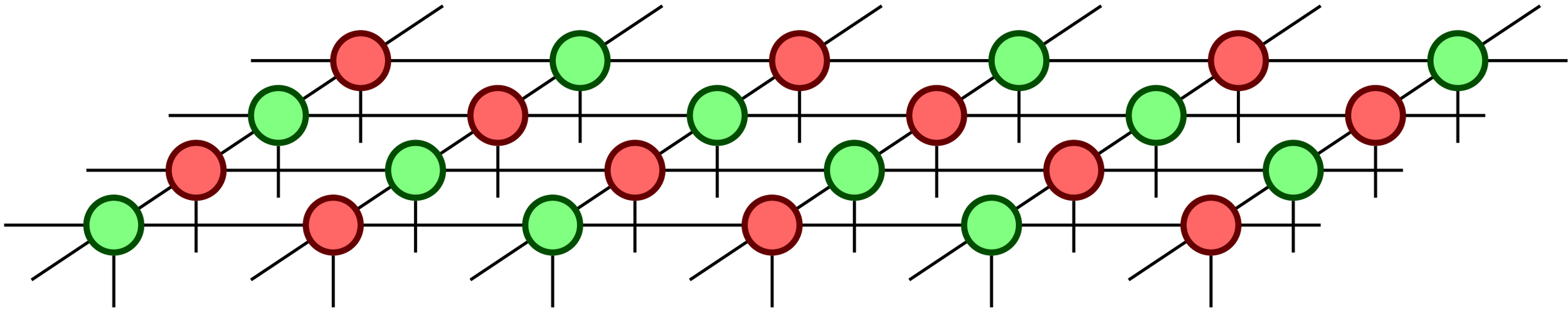


Graph States

Let G = (V,E) be a simple, undirected graph. Then define:

$$|G\rangle = \bigotimes_{(v,u)\in E} CZ_{vu} \bigotimes_{v\in V} |+\rangle$$

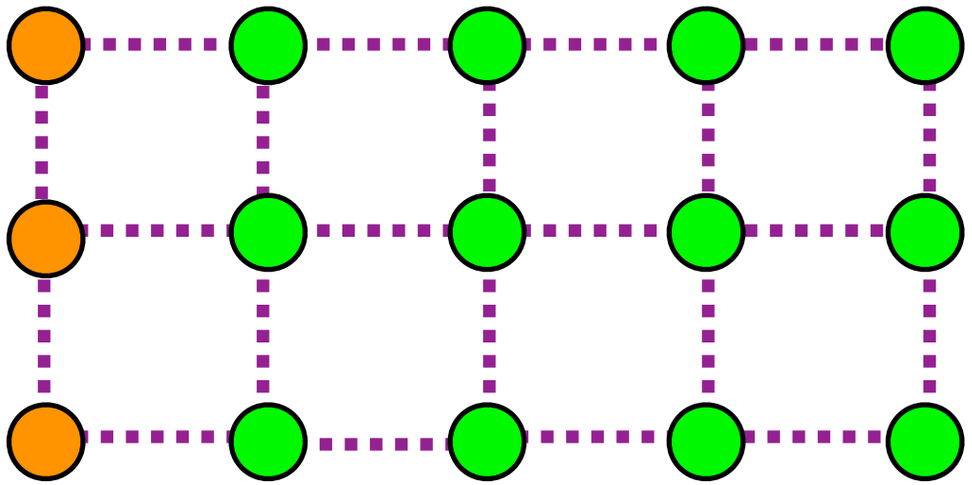
Or in 2D:



Raussendorf and Briegel. PRL (86) 2001
Raussendorf, Browne, Briegel J. Mod. Opt. (46) 2003

The One-Way Model

A graph state, coupled to some input qubits:



The only operation is to measure single qubits in the basis:

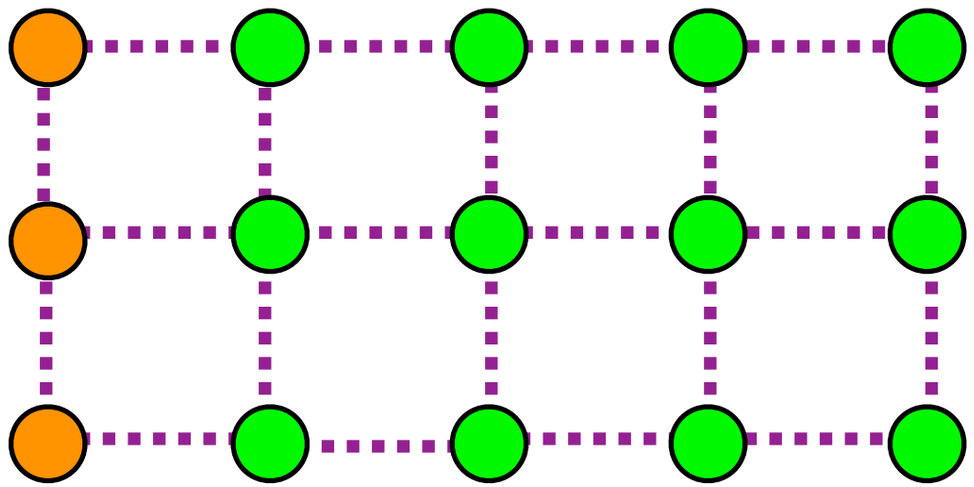
$$|+_\alpha\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle)$$

$$|-_\alpha\rangle := \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle)$$

Raussendorf and Briegel. PRL (86) 2001
Raussendorf, Browne, Briegel J. Mod. Opt. (46) 2003

The One-Way Model

A graph state, coupled to some input qubits:

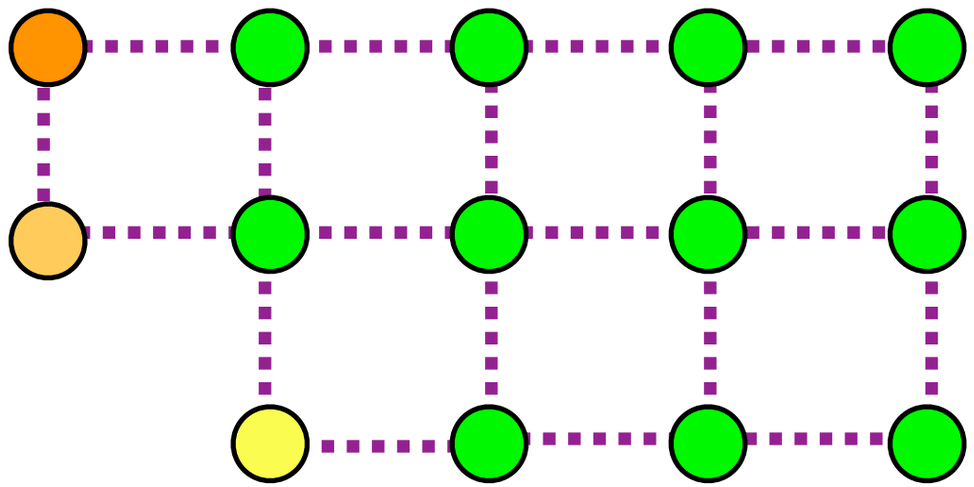


* Measured qubits are removed from the cluster;
* The outcome of measurement alters the remaining state.

Raussendorf and Briegel. PRL (86) 2001
Raussendorf, Browne, Briegel J. Mod. Opt. (46) 2003

The One-Way Model

A graph state, coupled to some input qubits:

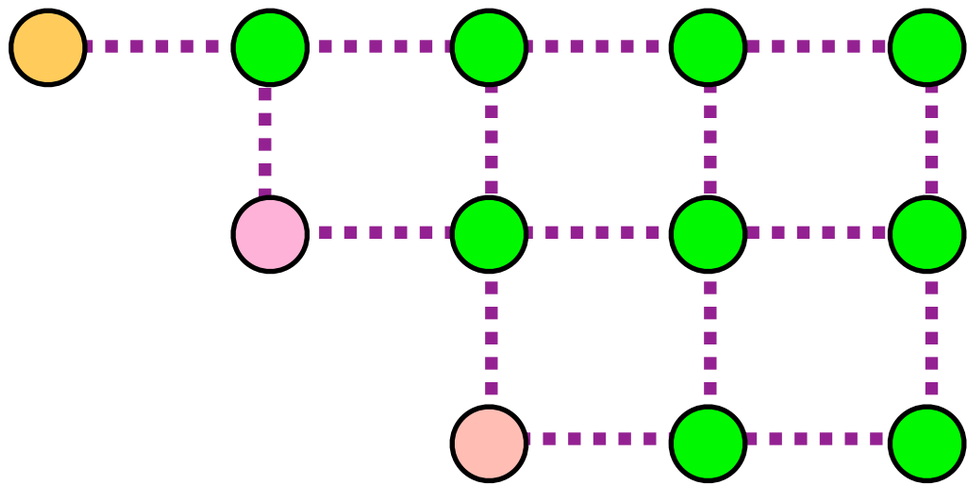


* Measured qubits are removed from the cluster;
* The outcome of measurement alters the remaining state.

Raussendorf and Briegel. PRL (86) 2001
Raussendorf, Browne, Briegel J. Mod. Opt. (46) 2003

The One-Way Model

A graph state, coupled to some input qubits:



* Measured qubits are removed from the cluster;
* The outcome of measurement alters the remaining state.

Raussendorf and Briegel. PRL (86) 2001
Raussendorf, Browne, Briegel J. Mod. Opt. (46) 2003

The One-Way Model

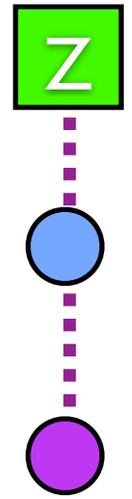
A graph state, coupled to some input qubits:

* Measured qubits are removed from the cluster;
* The outcome of measurement alters the remaining state.

Raussendorf and Briegel. PRL (86) 2001
Raussendorf, Browne, Briegel J. Mod. Opt. (46) 2003

The One-Way Model

A graph state, coupled to some input qubits:



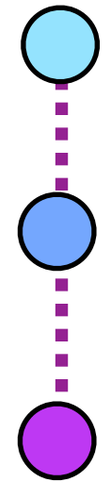
* Measured qubits are removed from the cluster;
* The outcome of measurement alters the remaining state.

Finally, any output qubits can be corrected by a local Pauli

Raussendorf and Briegel. PRL (86) 2001
Raussendorf, Browne, Briegel J. Mod. Opt. (46) 2003

The One-Way Model

A graph state, coupled to some input qubits:

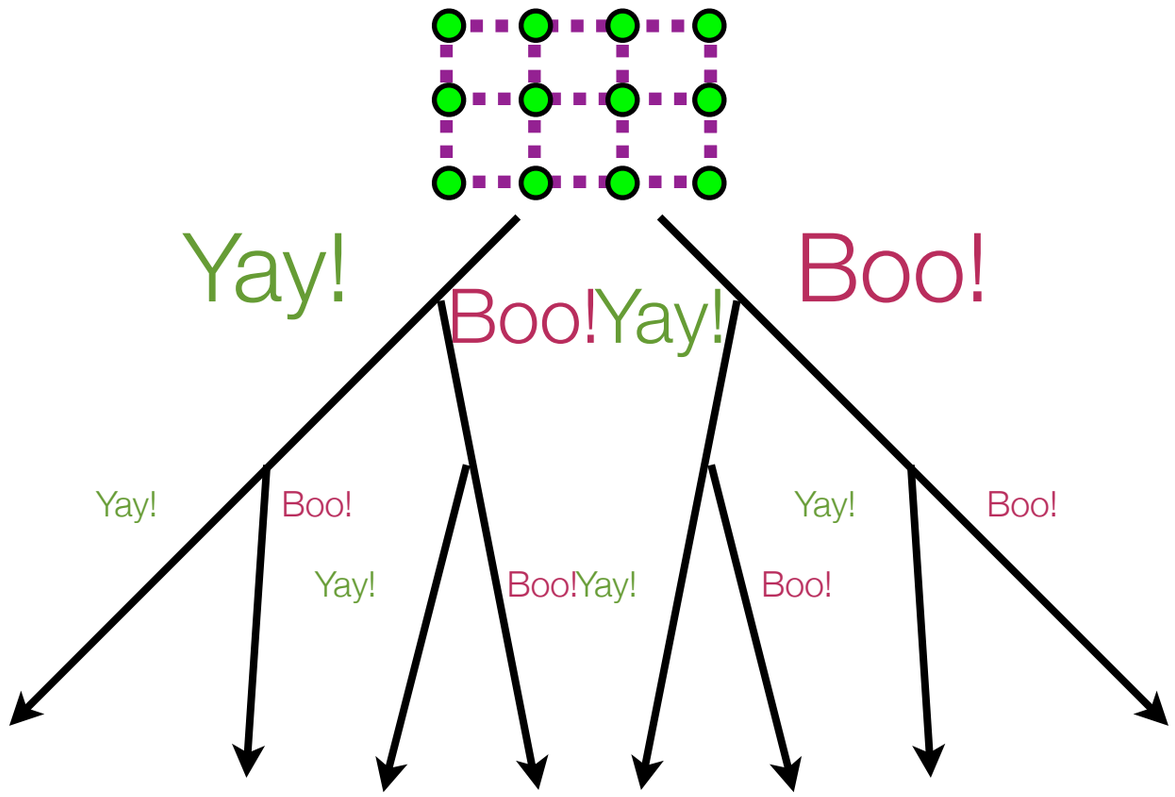


* Measured qubits are removed from the cluster;
* The outcome of measurement alters the remaining state.

Finally, any output qubits can be corrected by a local Pauli

Non-determinism

Non-determinism of measurements leads to probabilistic branching

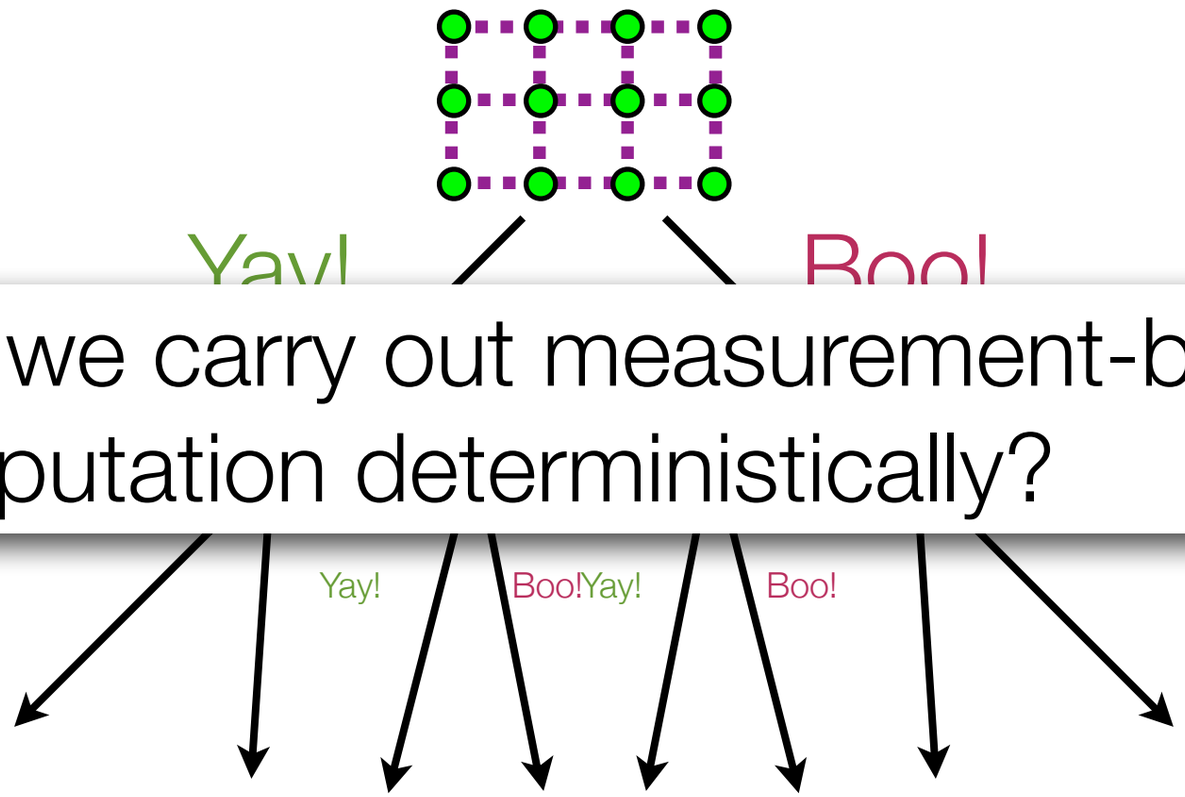


Attempt to control branching by using *adaptive measurements*:

(choice of later measurements depends on the outcome of earlier ones)

Non-determinism

Non-determinism of measurements leads to probabilistic branching

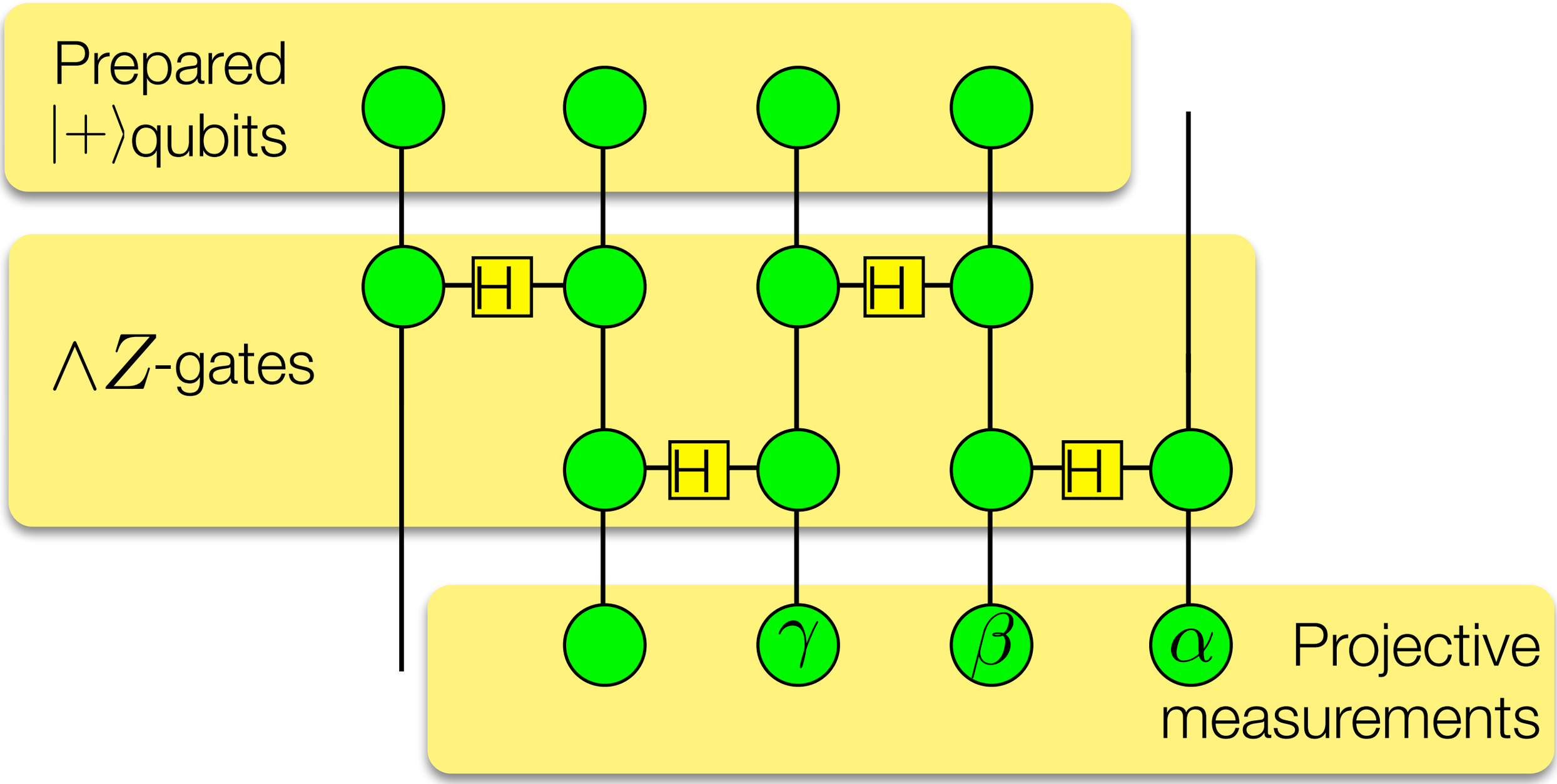


Can we carry out measurement-based computation deterministically?

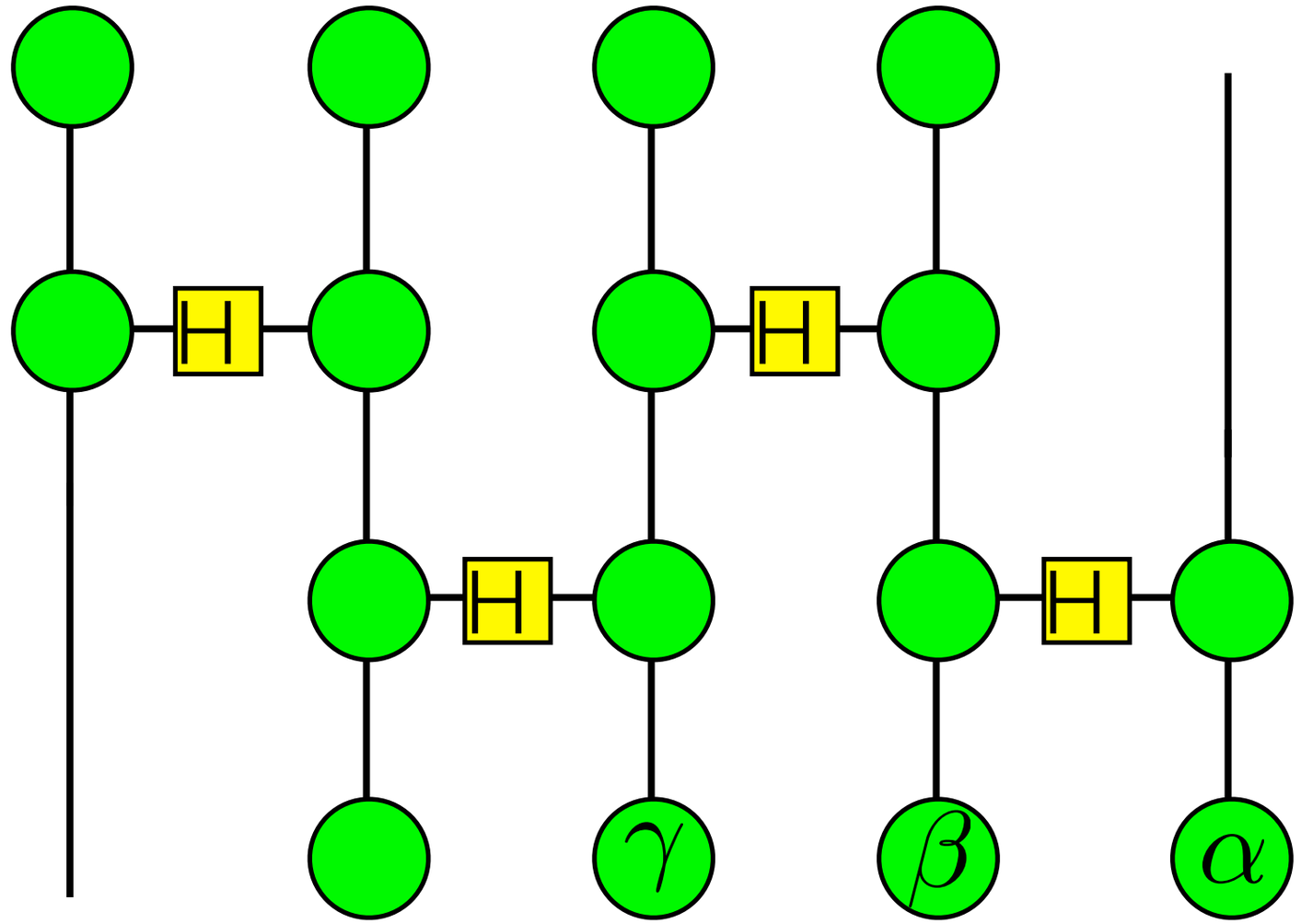
Attempt to control branching by using *adaptive measurements*:

(choice of later measurements depends on the outcome of earlier ones)

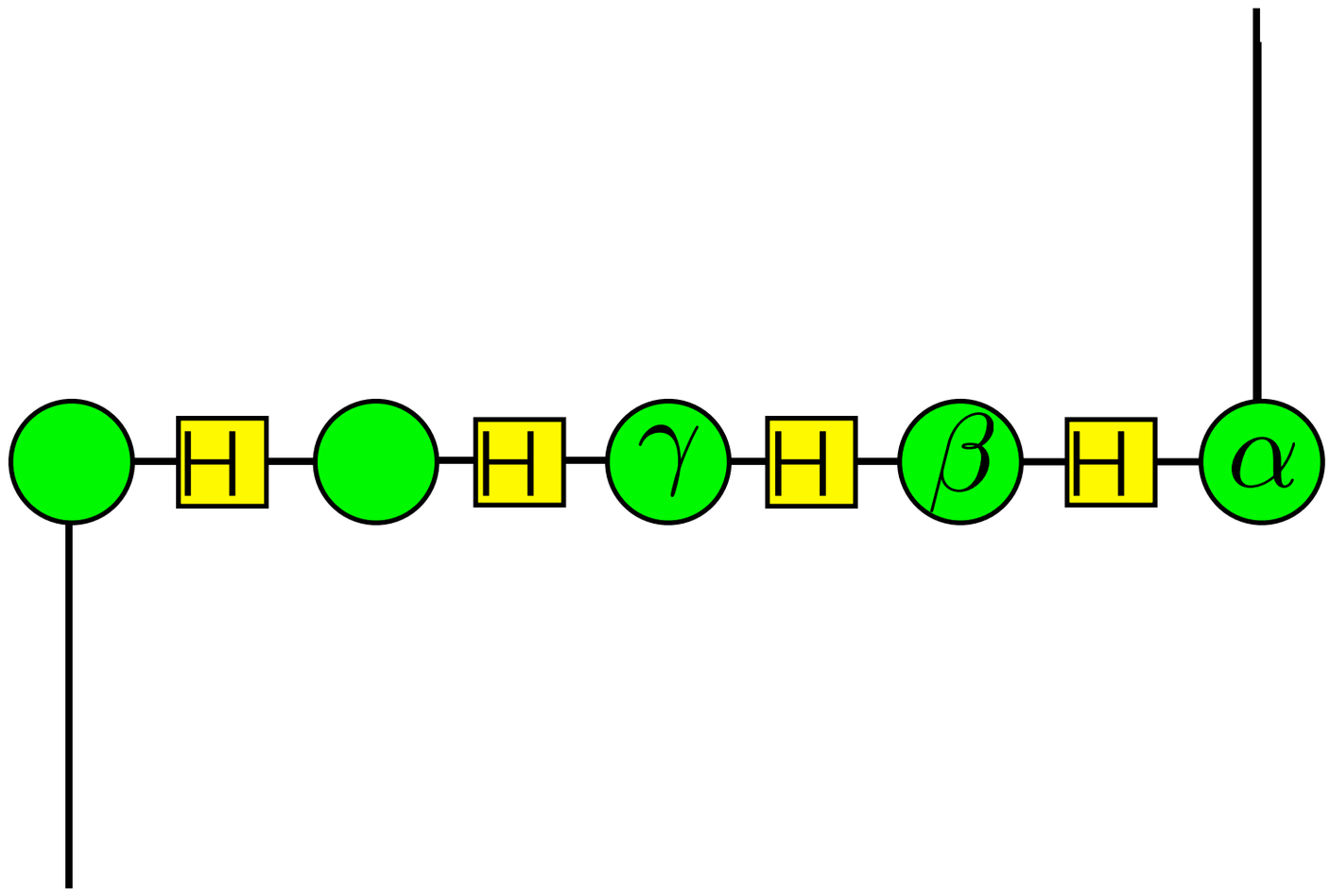
Example: 1-Qubit Unitary



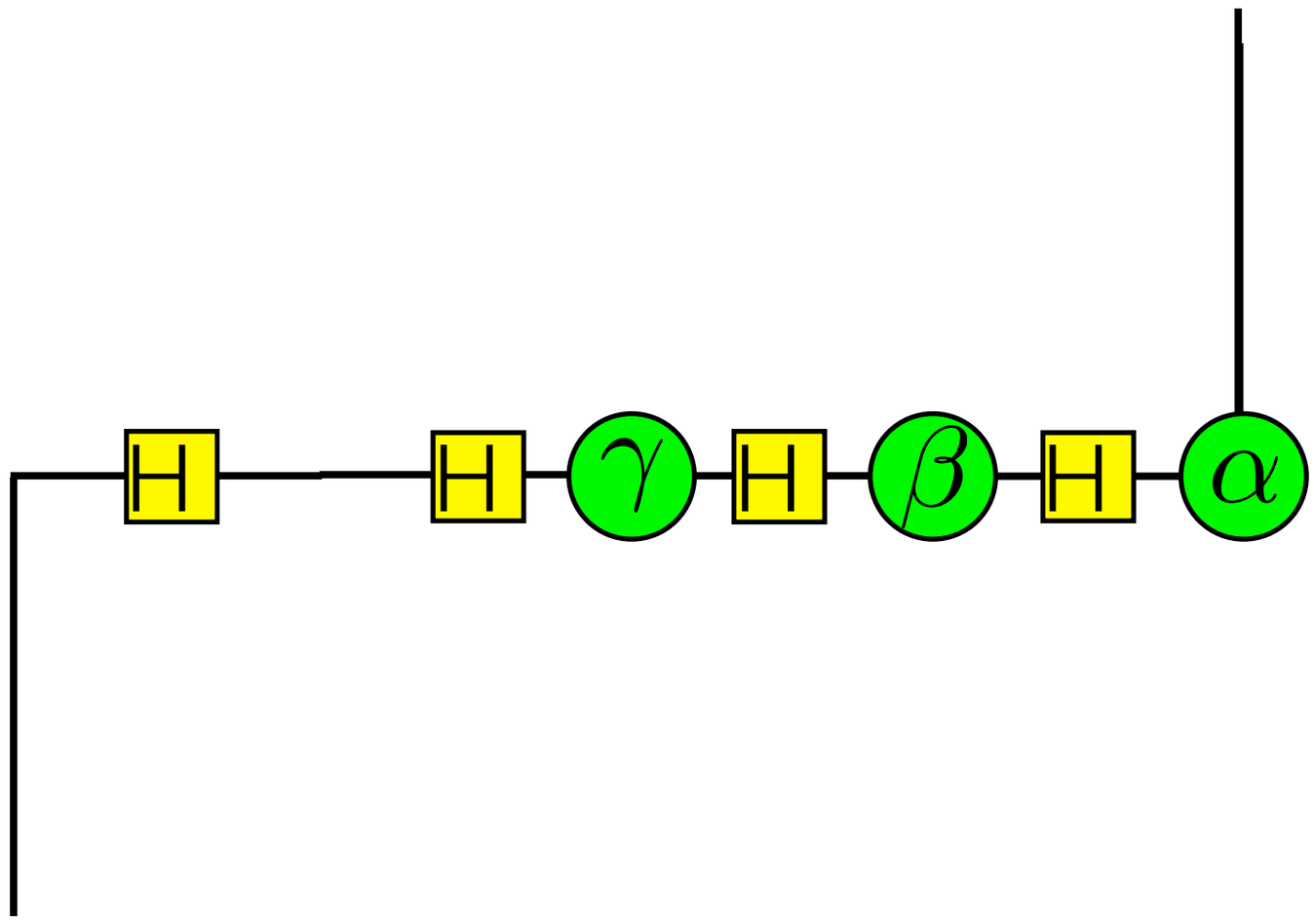
Example: 1-Qubit Unitary



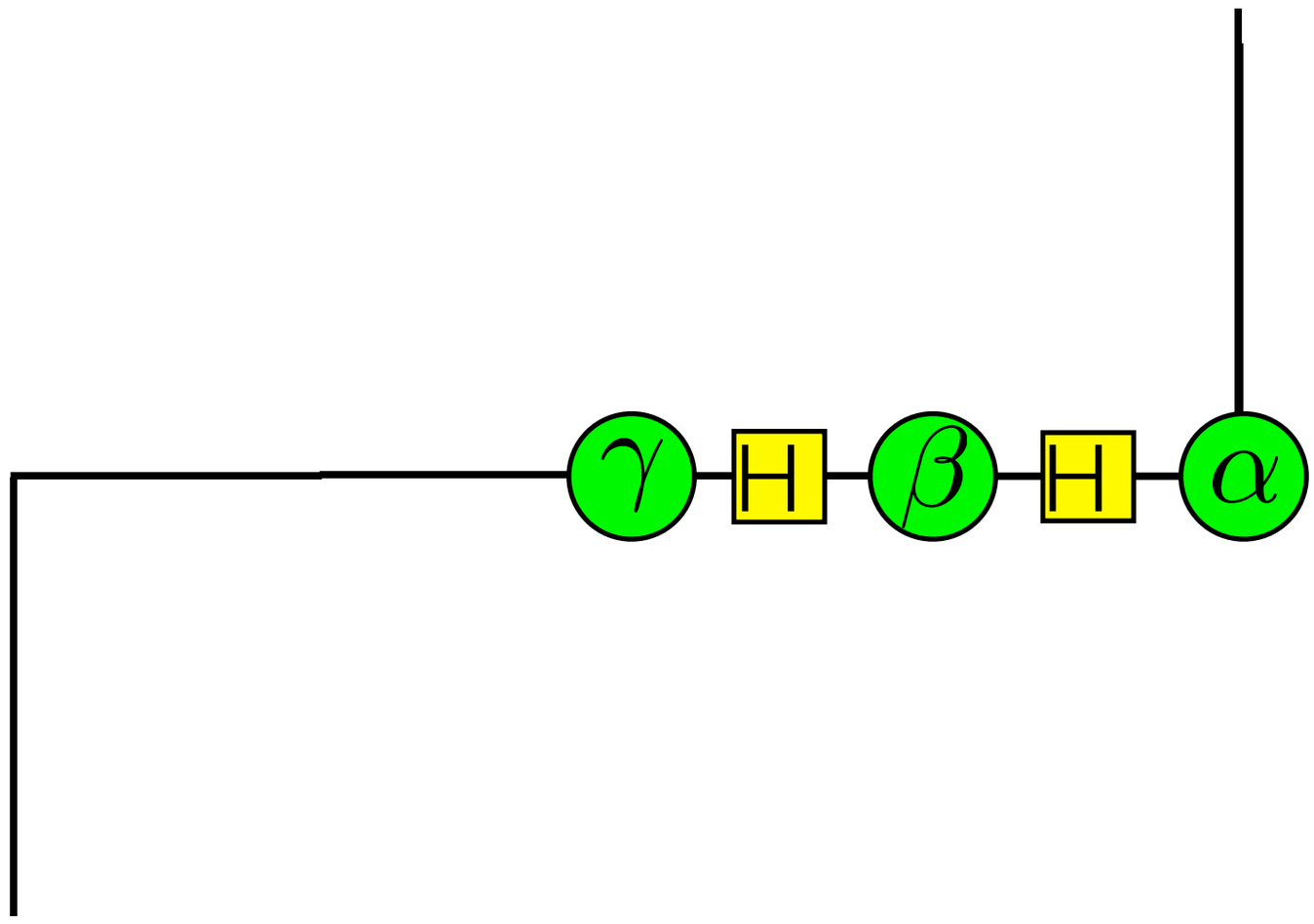
Example: 1-Qubit Unitary



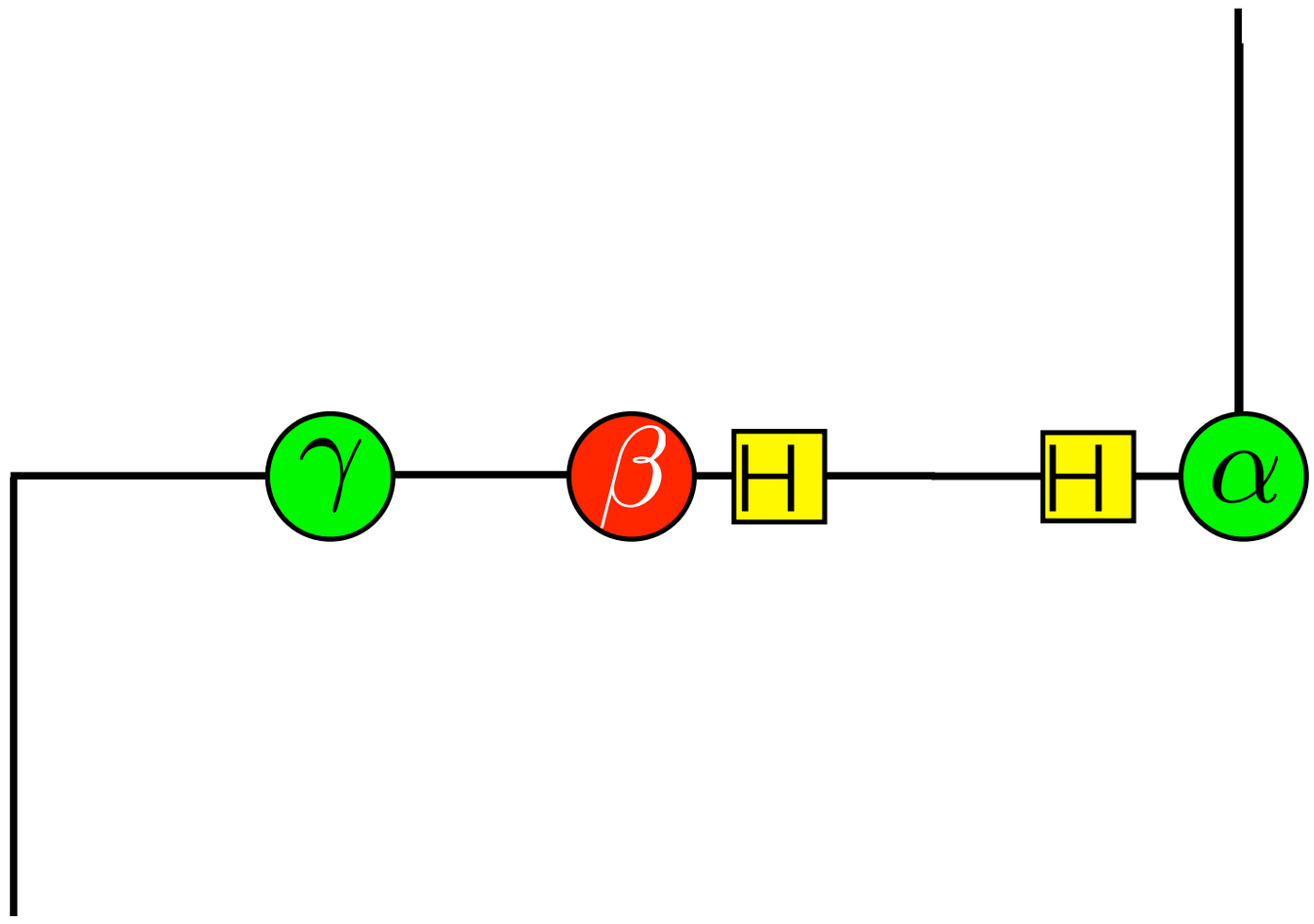
Example: 1-Qubit Unitary



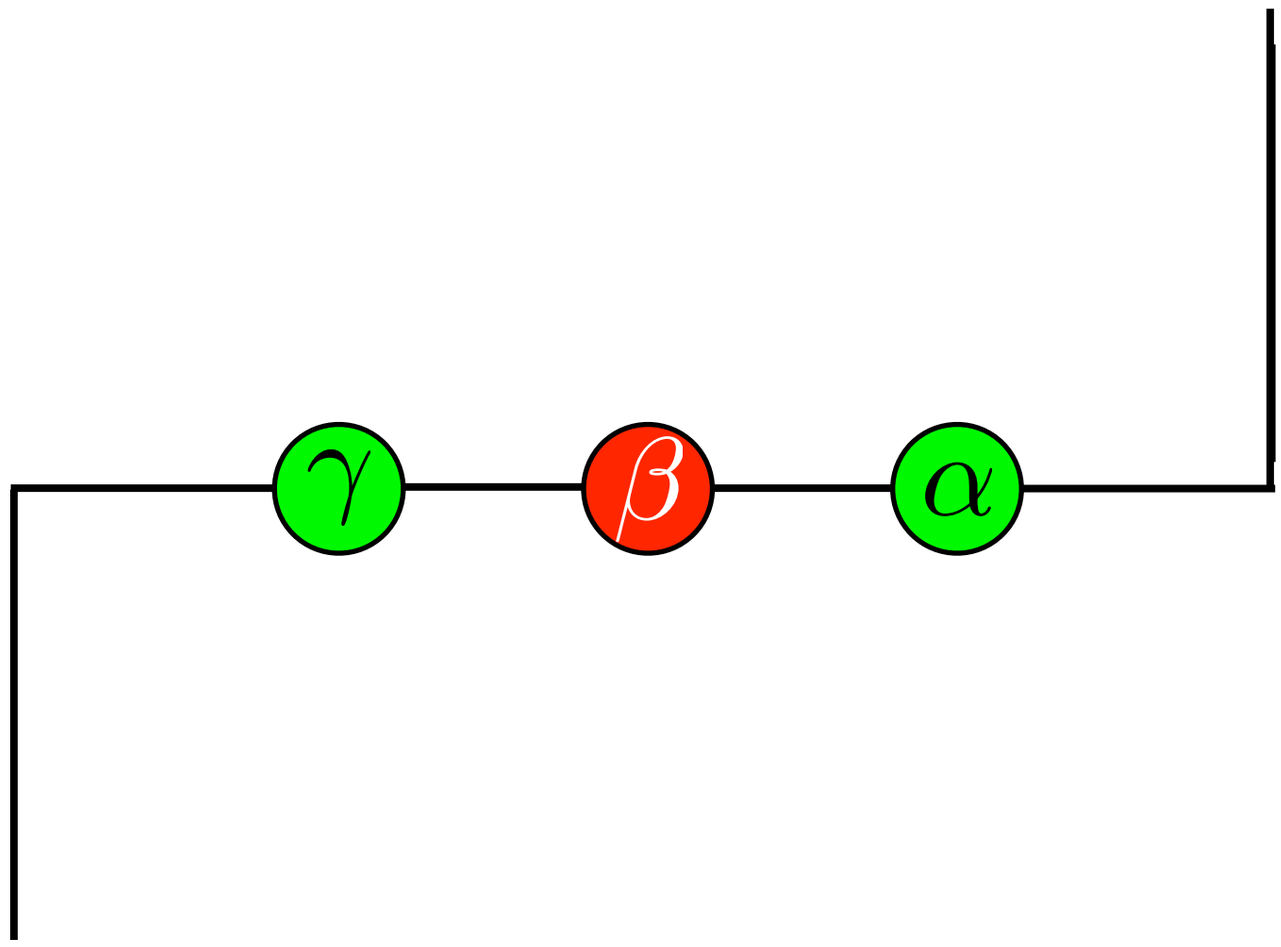
Example: 1-Qubit Unitary



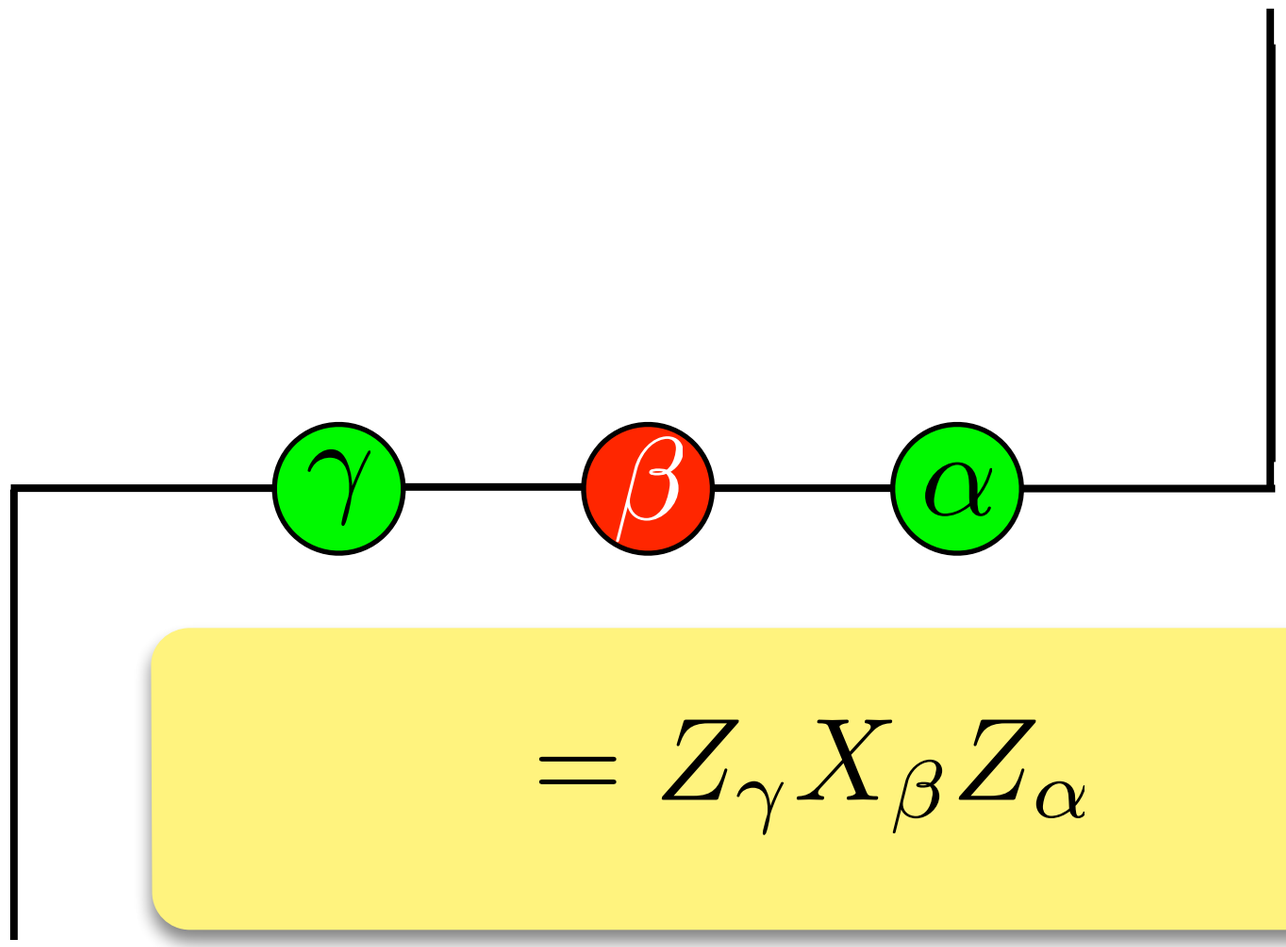
Example: 1-Qubit Unitary



Example: 1-Qubit Unitary



Example: 1-Qubit Unitary



$$= Z_\gamma X_\beta Z_\alpha$$

How to Measure

Suppose we have a measuring device for the standard 1-qubit basis:

$|0\rangle$ $|1\rangle$

Yay! $|-\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix} \frac{1}{\sqrt{2}} = [\ \pi\ 0\ ]$

$[\ 0\ \pi\ ] = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$ Boo!

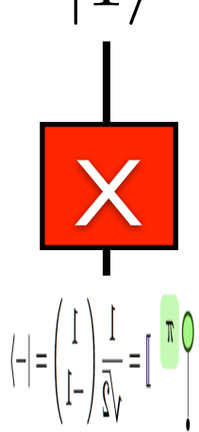
How to Measure

Suppose we have a measuring device for the standard 1-qubit basis:

$|0\rangle$

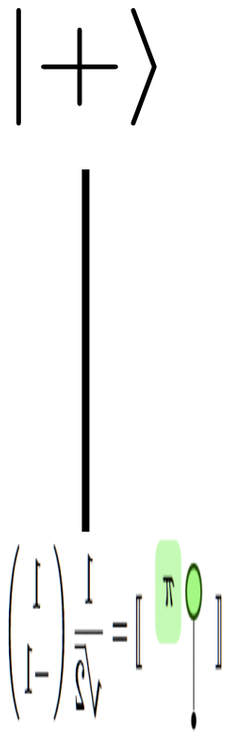
Yay!

$|1\rangle$



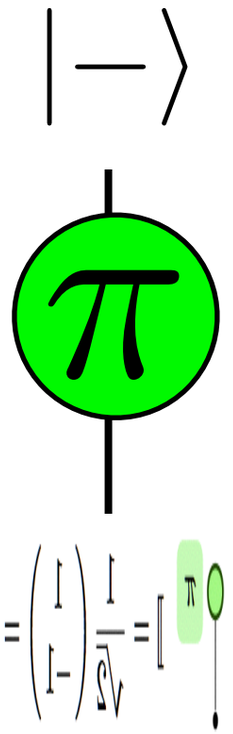
Yay!

Should be this:



Yay!

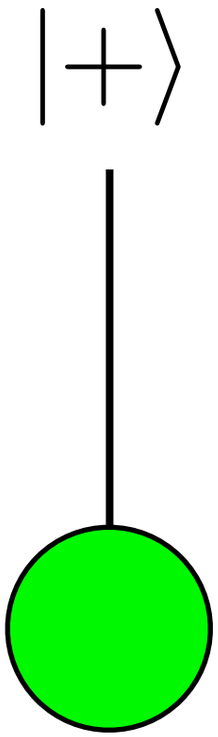
$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \left[\ \pi\ \right]$$



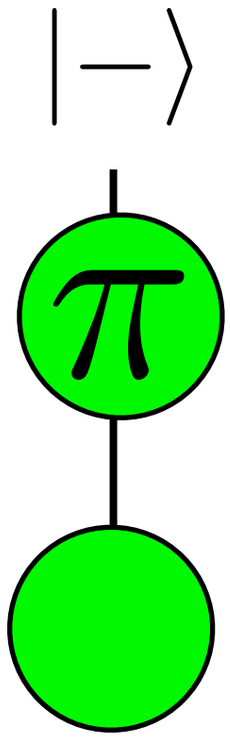
$$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \left[\ \pi\ \right]$$

Yay!

Should be this:

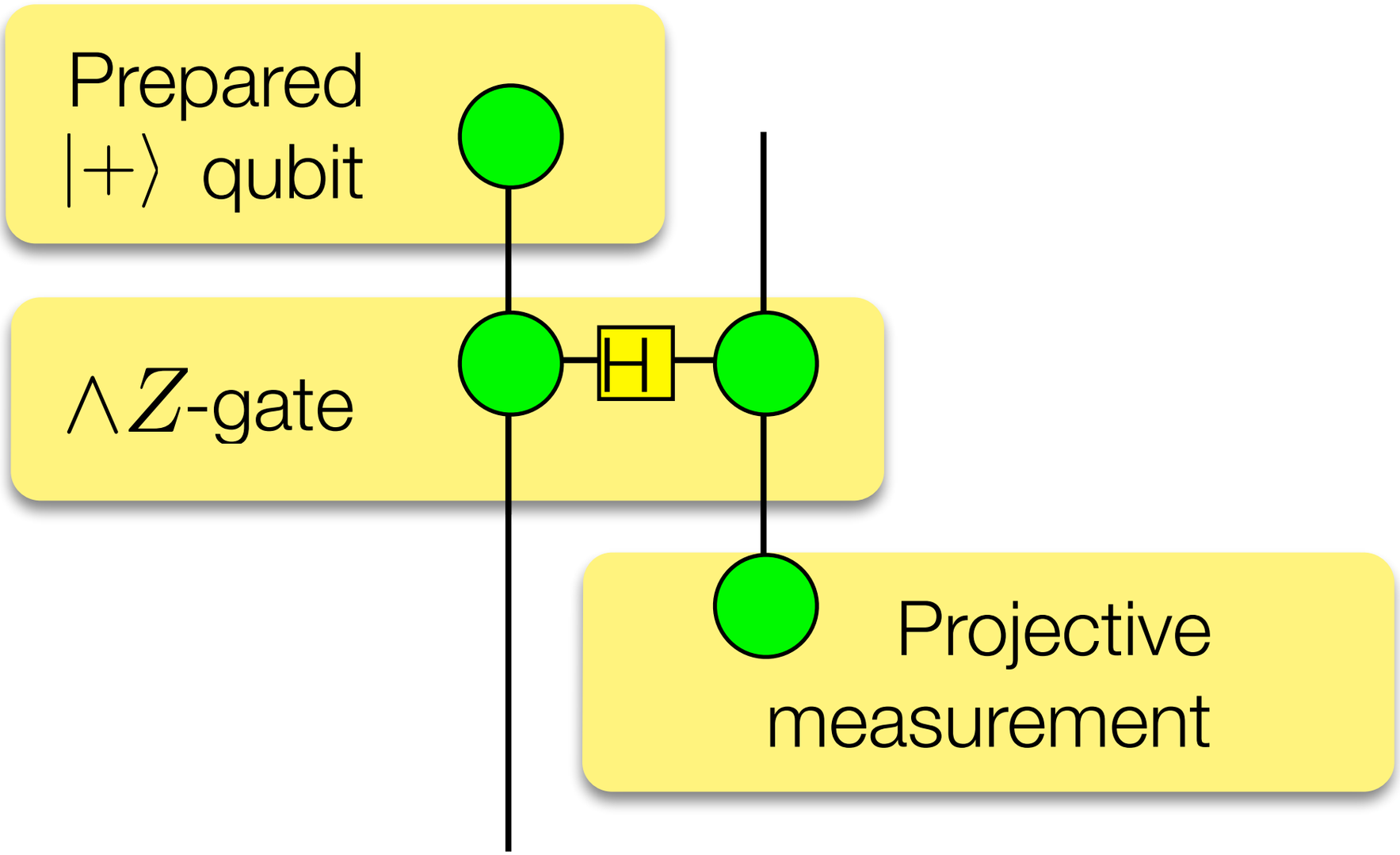


Yay!

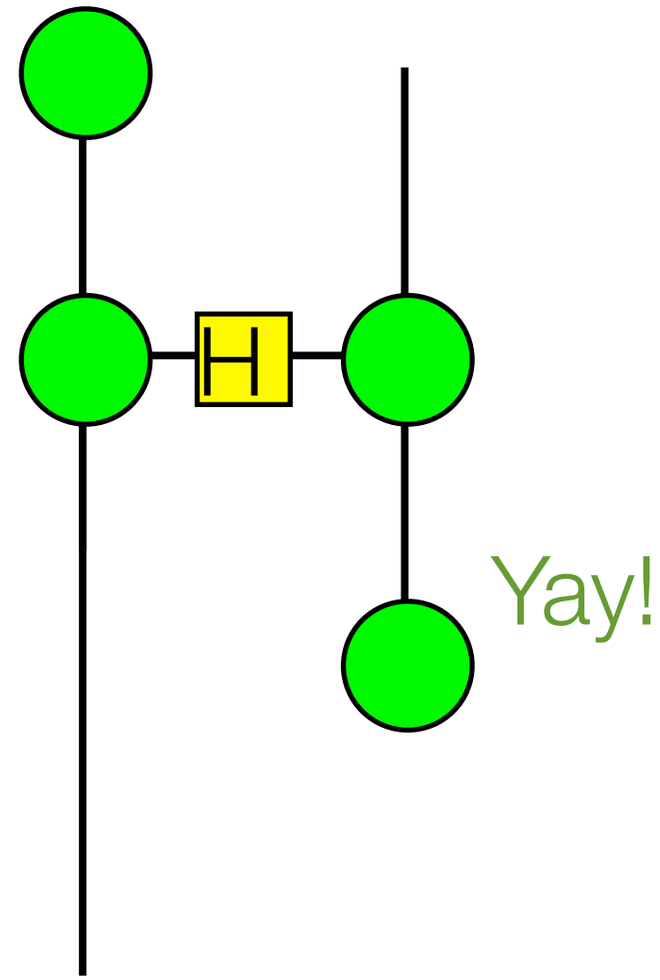


Yay!

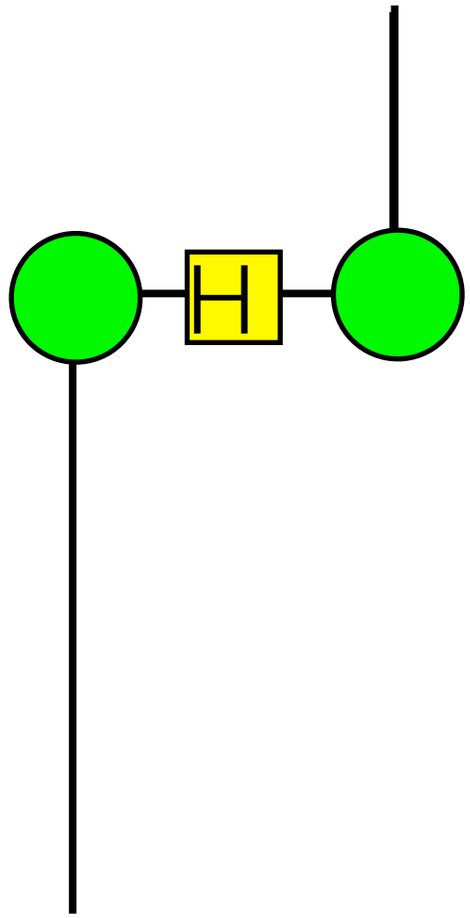
Example: Hadamard



Example: Hadamard

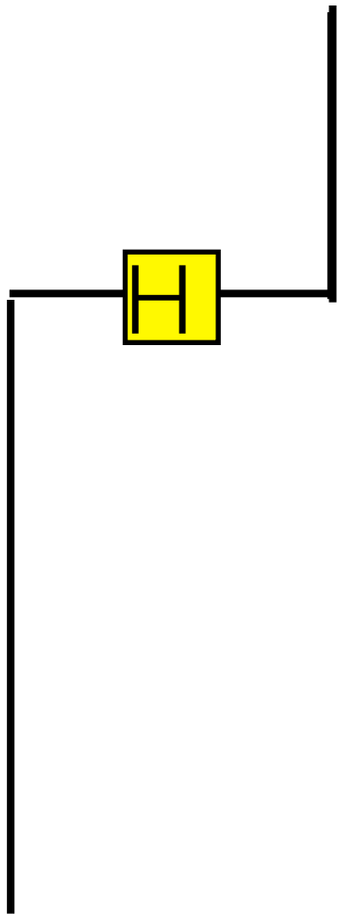


Example: Hadamard



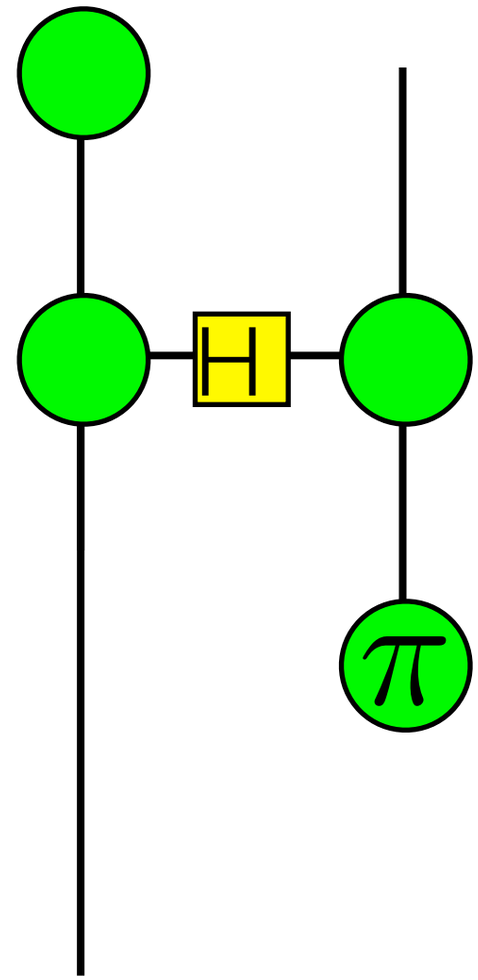
Yay!

Example: Hadamard

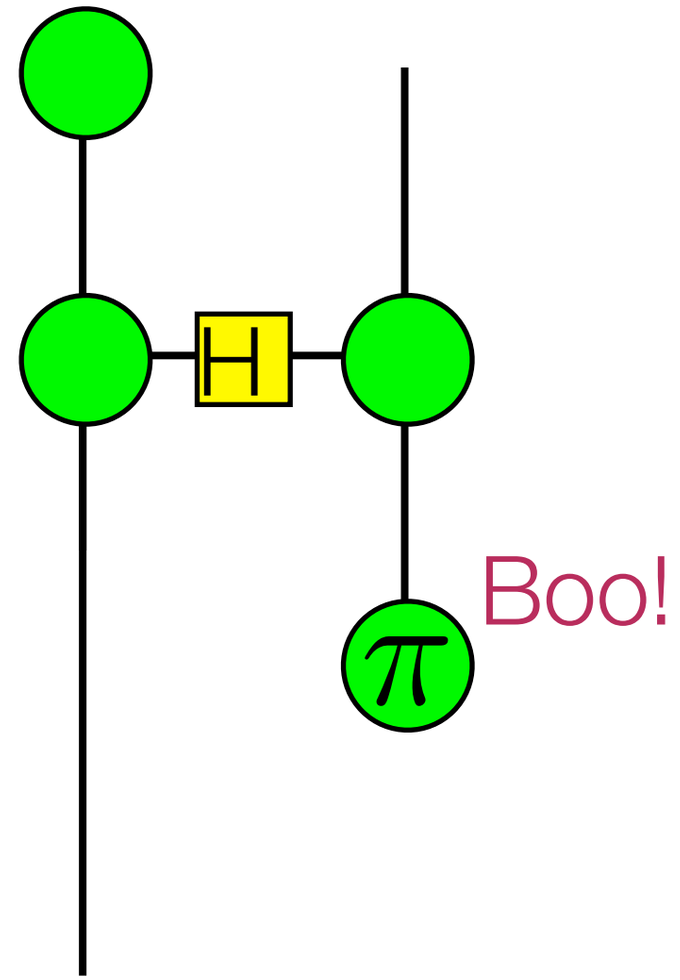


Yay!

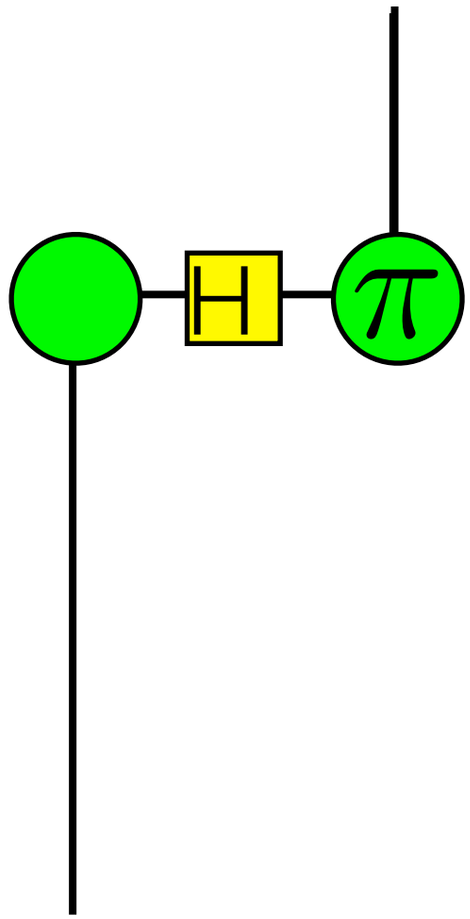
Example: Hadamard



Example: Hadamard

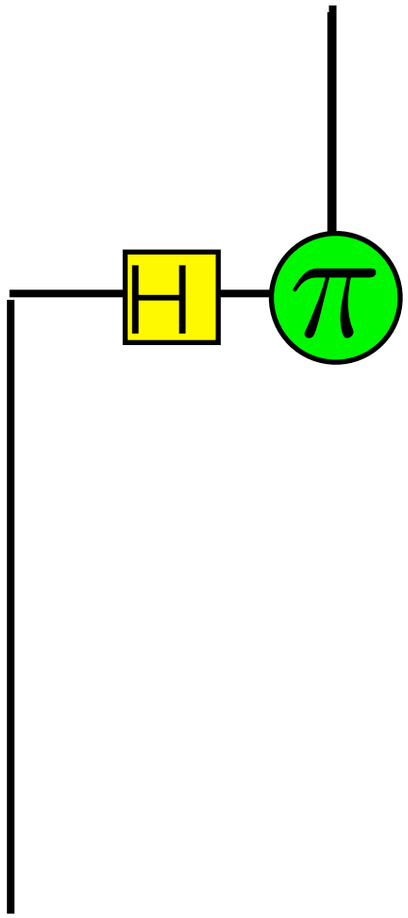


Example: Hadamard



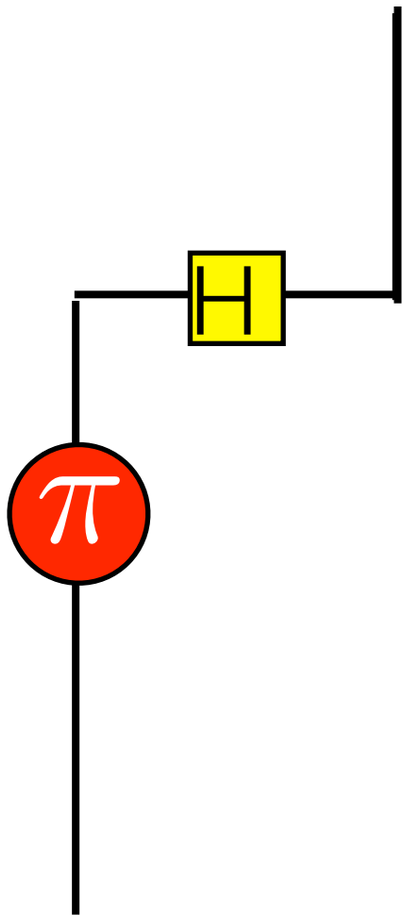
Boo!

Example: Hadamard



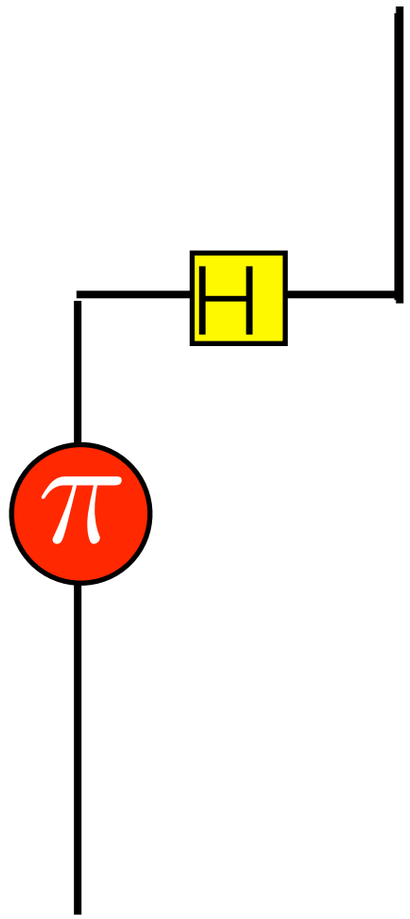
Boo!

Example: Hadamard



Boo!

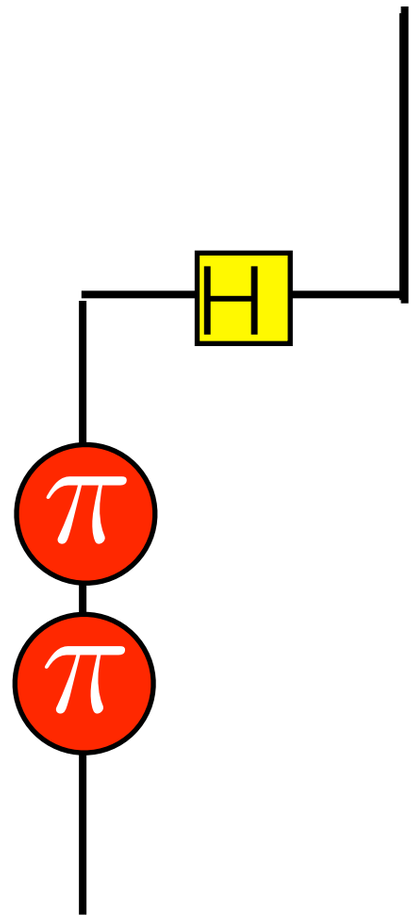
Example: Hadamard



Boo!

Add correction here:

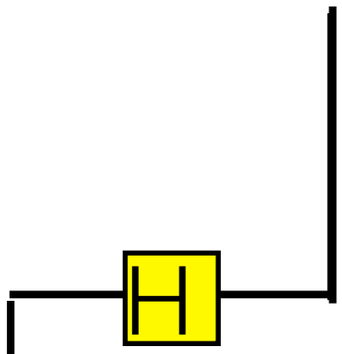
Example: Hadamard



Boo!

Add correction here:

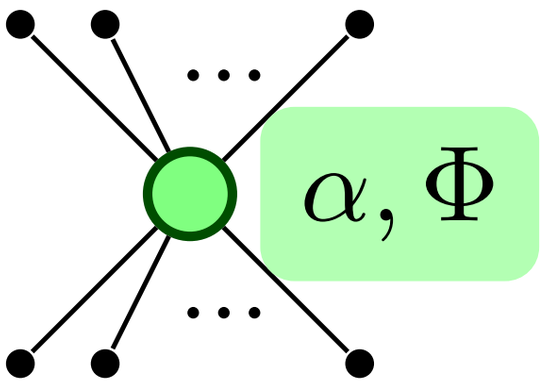
Example: Hadamard

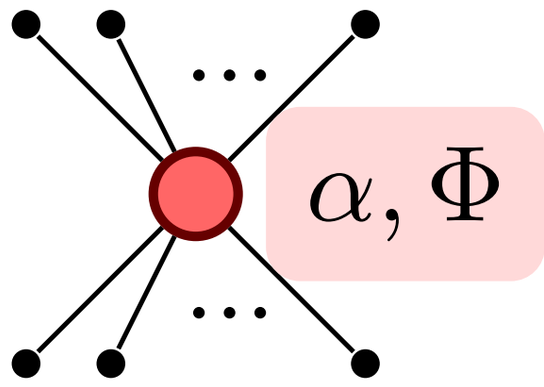


Add correction here:

Boo!

Conditional ZX

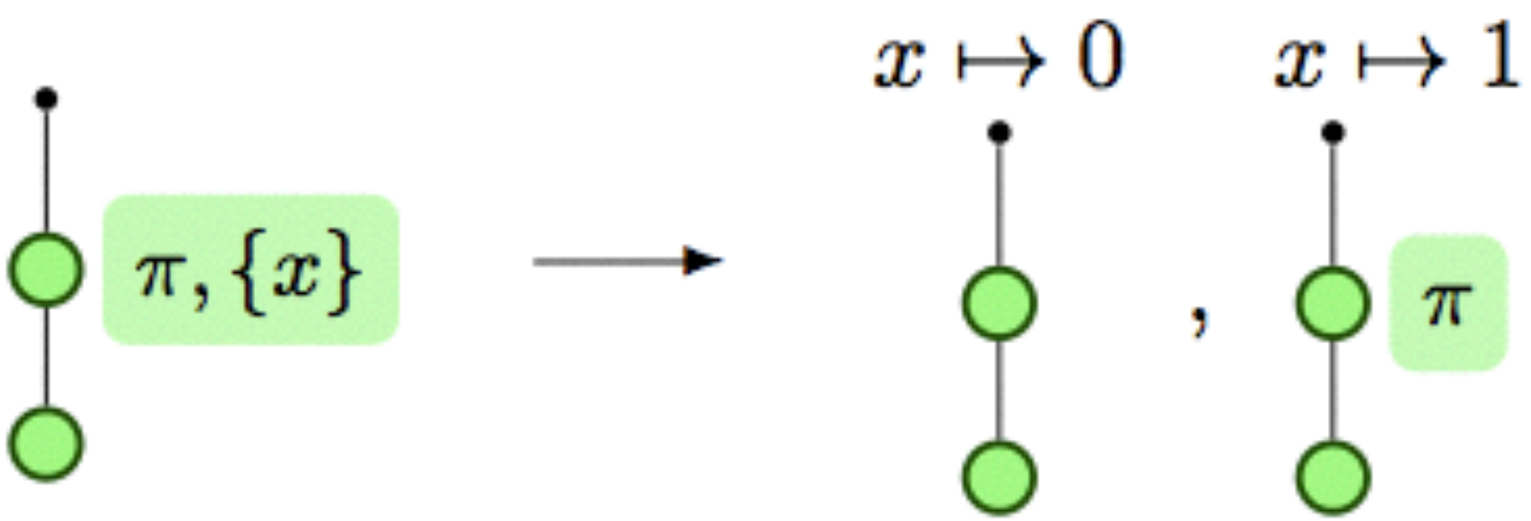




$$\rho \mapsto \sum_{v \in 2^S} [\![\hat{v}(D)]\!] \rho [\![\hat{v}(D)]\!]^\dagger$$

Example

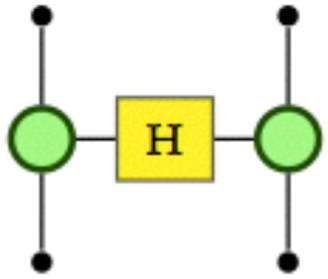
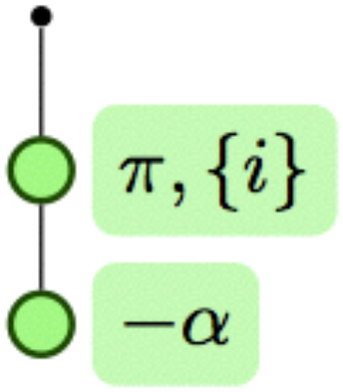
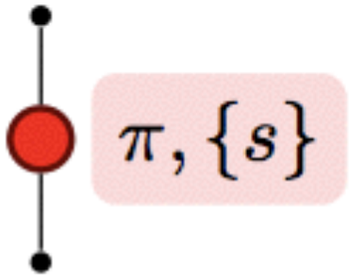
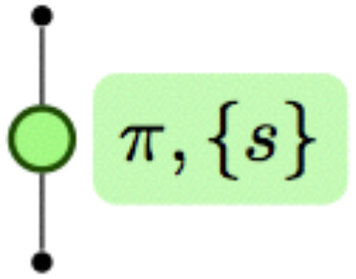
A measurement in the basis: $|+\rangle, |-\rangle$



$$\rho \mapsto \langle +| \rho |+\rangle + \langle +| Z\rho Z |+\rangle$$
$$= \langle +| \rho |+\rangle + \langle -| \rho |-\rangle$$

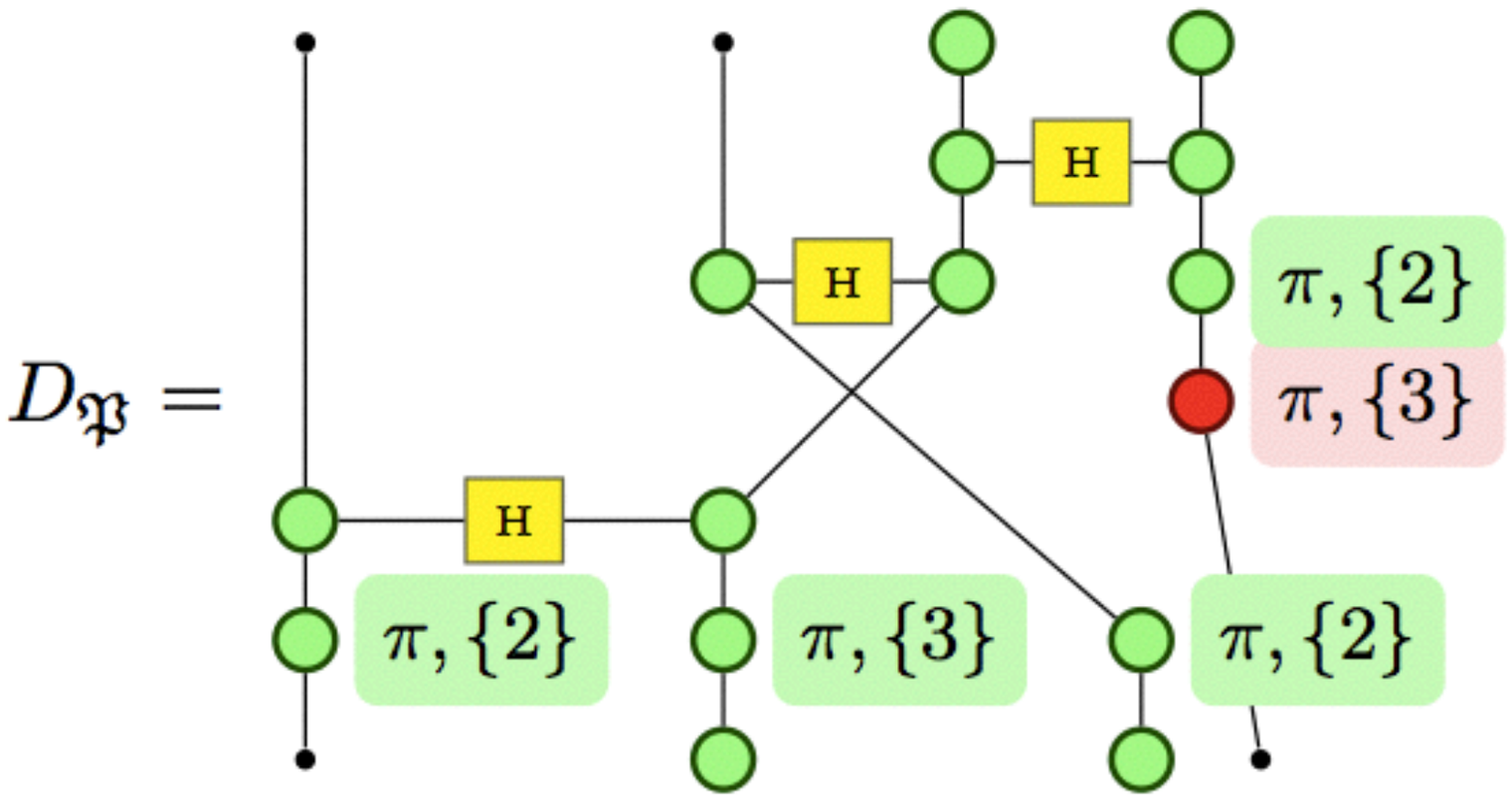
Translation from MC to ZX-calculus

We can translate any measurement pattern to diagram using the table below:

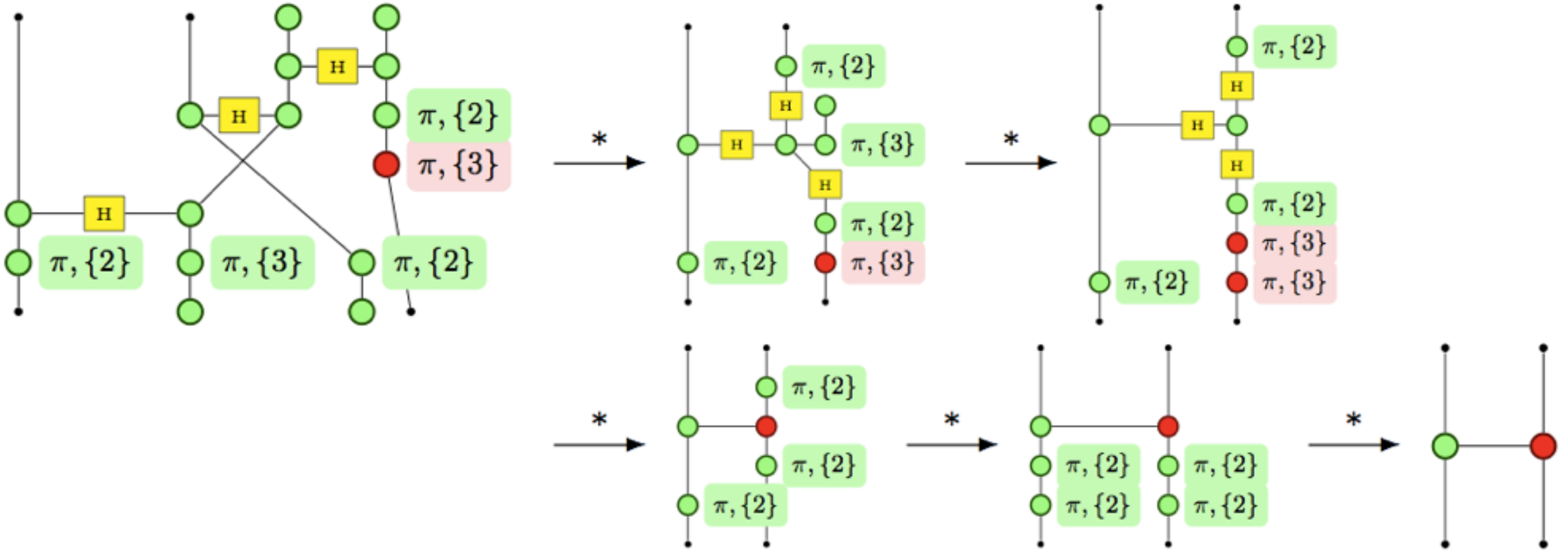
N_i	E_{ij}	M_i^α	X_i^s	Z_i^s
				

Example

CLAIM: this deterministically computes the CNOT of its input



Example Rewrite



We removed all the conditional operations, therefore this **pattern** is deterministic.

Can we do this in general?

Determinism in MBQC

Measurement
Pattern
"low-level program"

Determinism in MBQC

Measurement
Pattern
“low-level program”

implicitly defines

Geometry
“entangled resource”
“graph state”

Determinism in MBQC

Measurement
Pattern
“low-level program”

implicitly defines

Geometry
“entangled resource”
“graph state”

can possess

Flow and GFlow
“correction strategy”

Determinism in MBQC

Measurement Pattern

"low-level program"

implicitly defines

Geometry

"entangled resource"

"graph state"

can possess

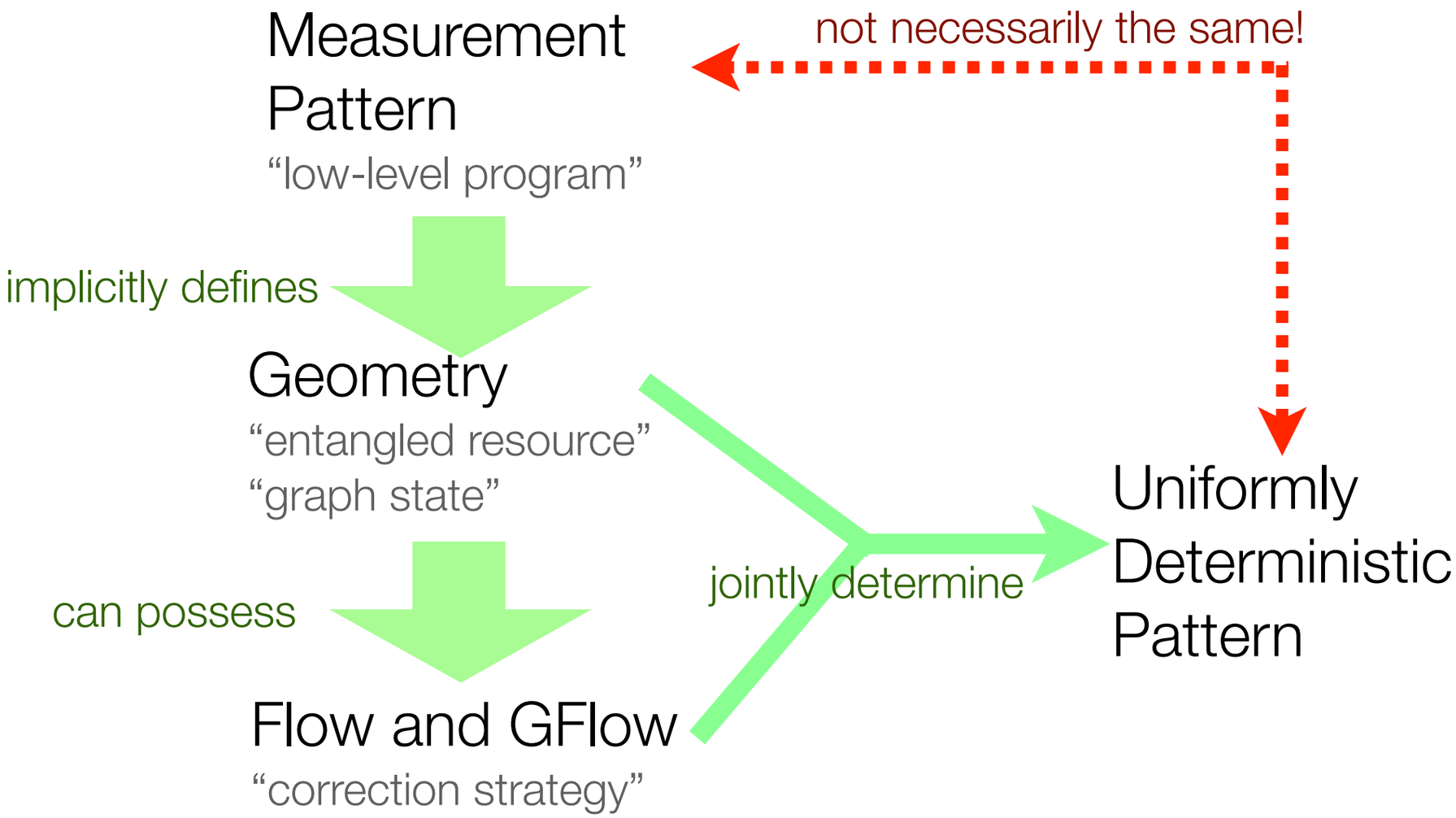
Flow and GFlow

"correction strategy"

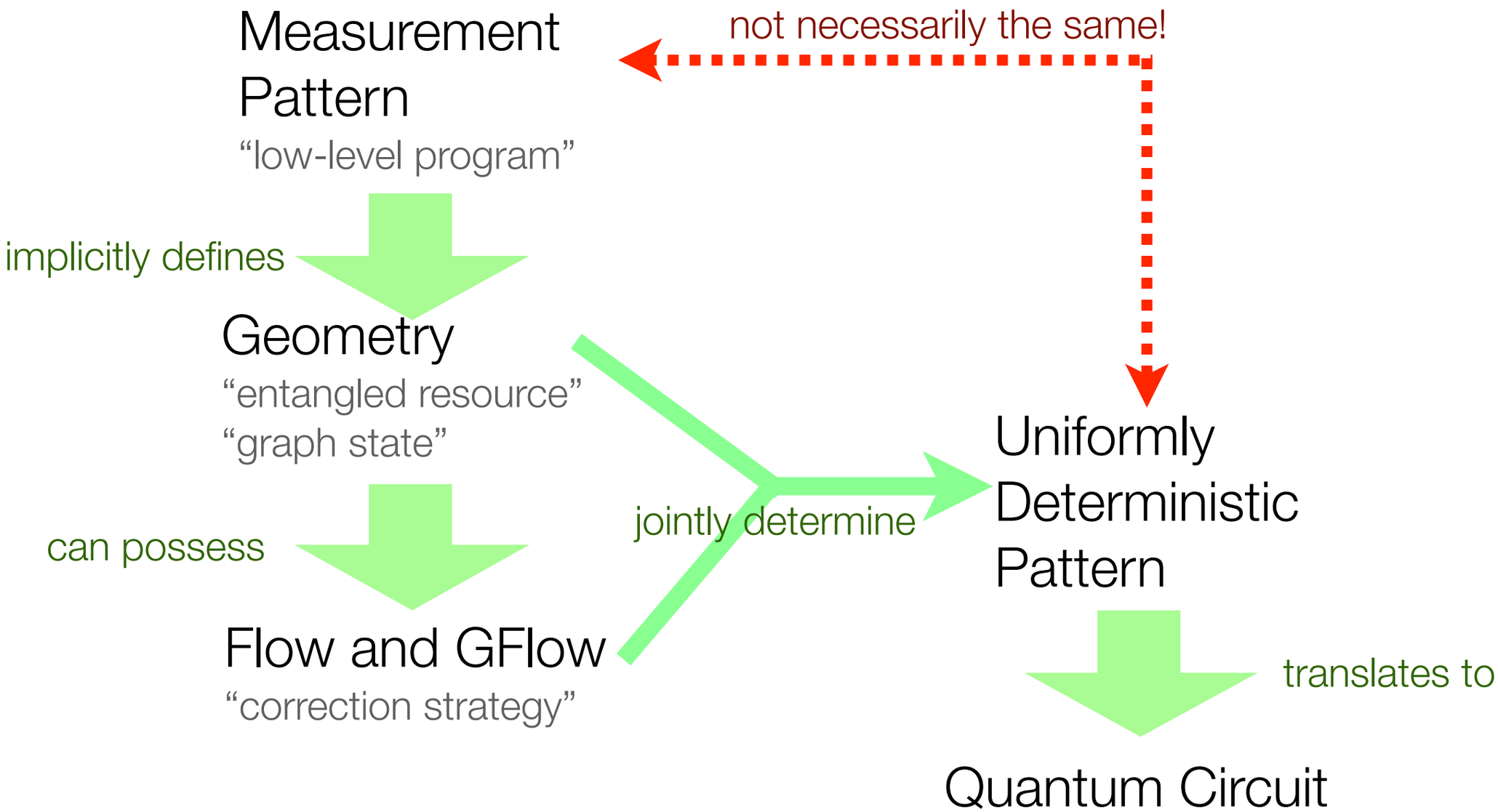
jointly determine

Uniformly Deterministic Pattern

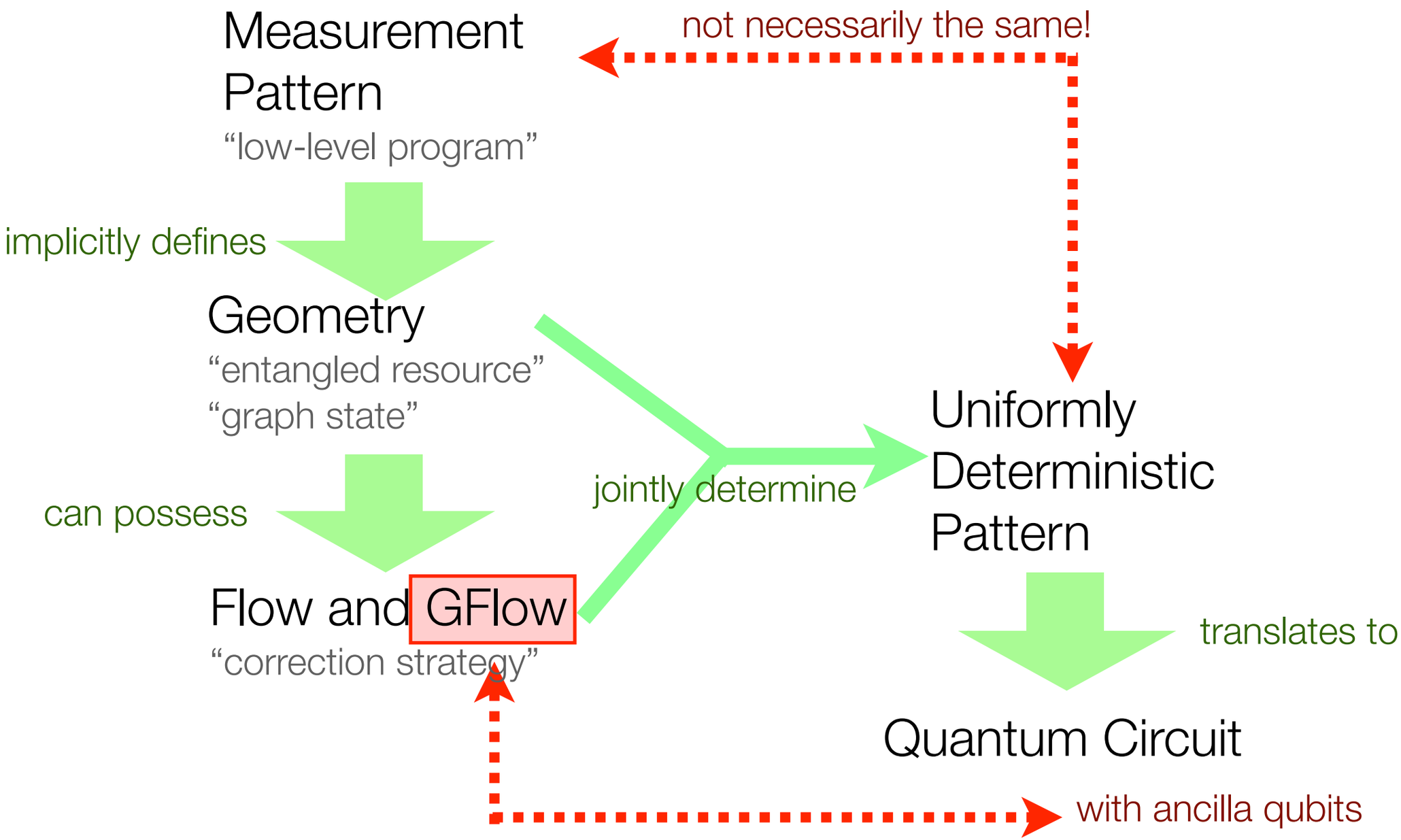
Determinism in MBQC



Determinism in MBQC



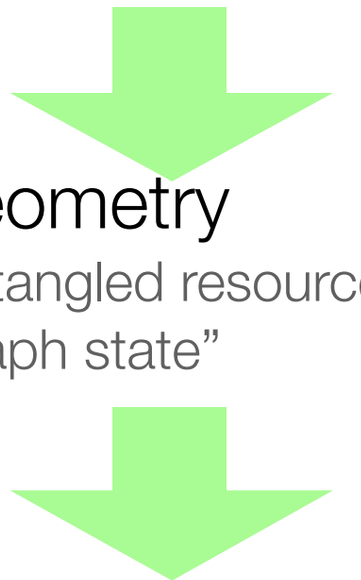
Determinism in MBQC



The plan:

Measurement Pattern

“low-level program”



Geometry

“entangled resource”

“graph state”

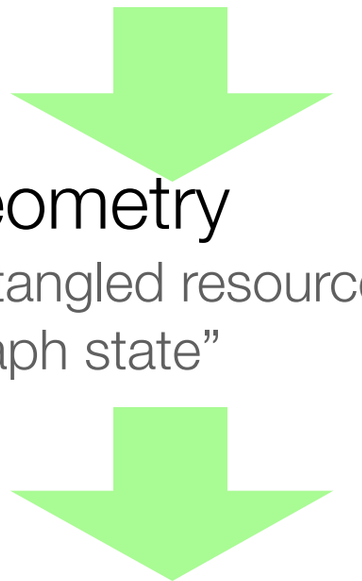
Flow and GFlow

“correction strategy”

The plan:

Measurement Pattern

“low-level program”



Geometry

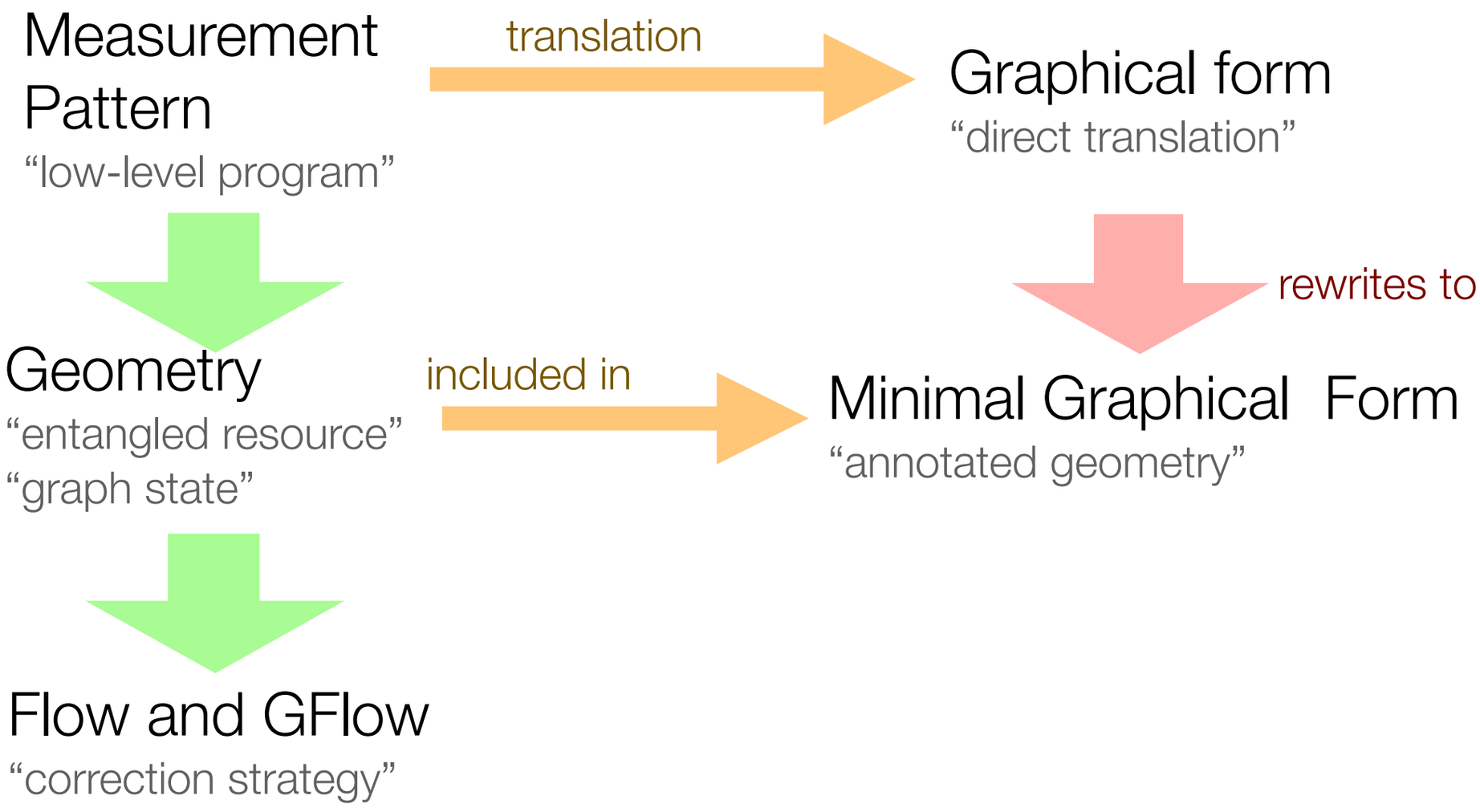
“entangled resource”

“graph state”

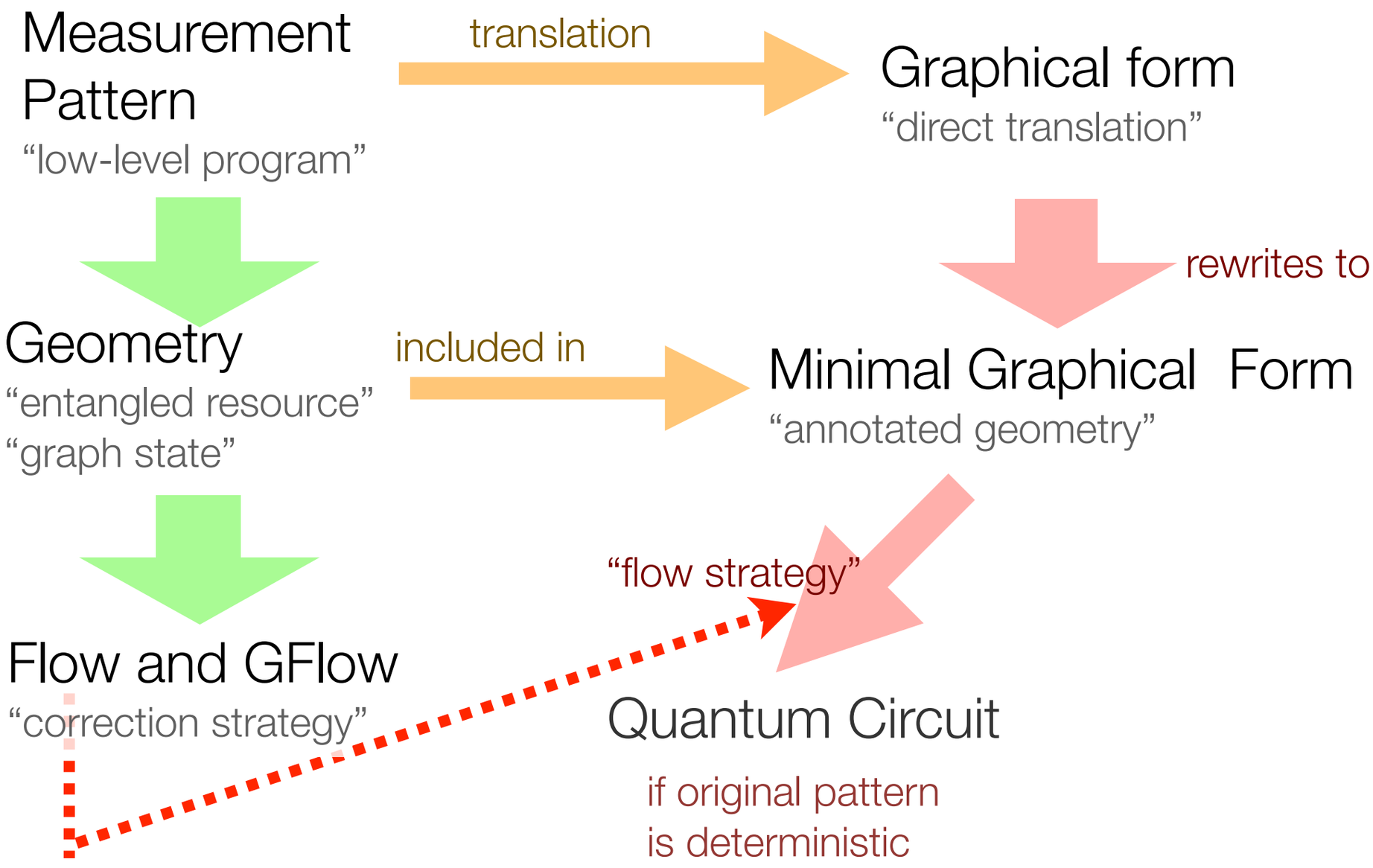
Flow and GFlow

“correction strategy”

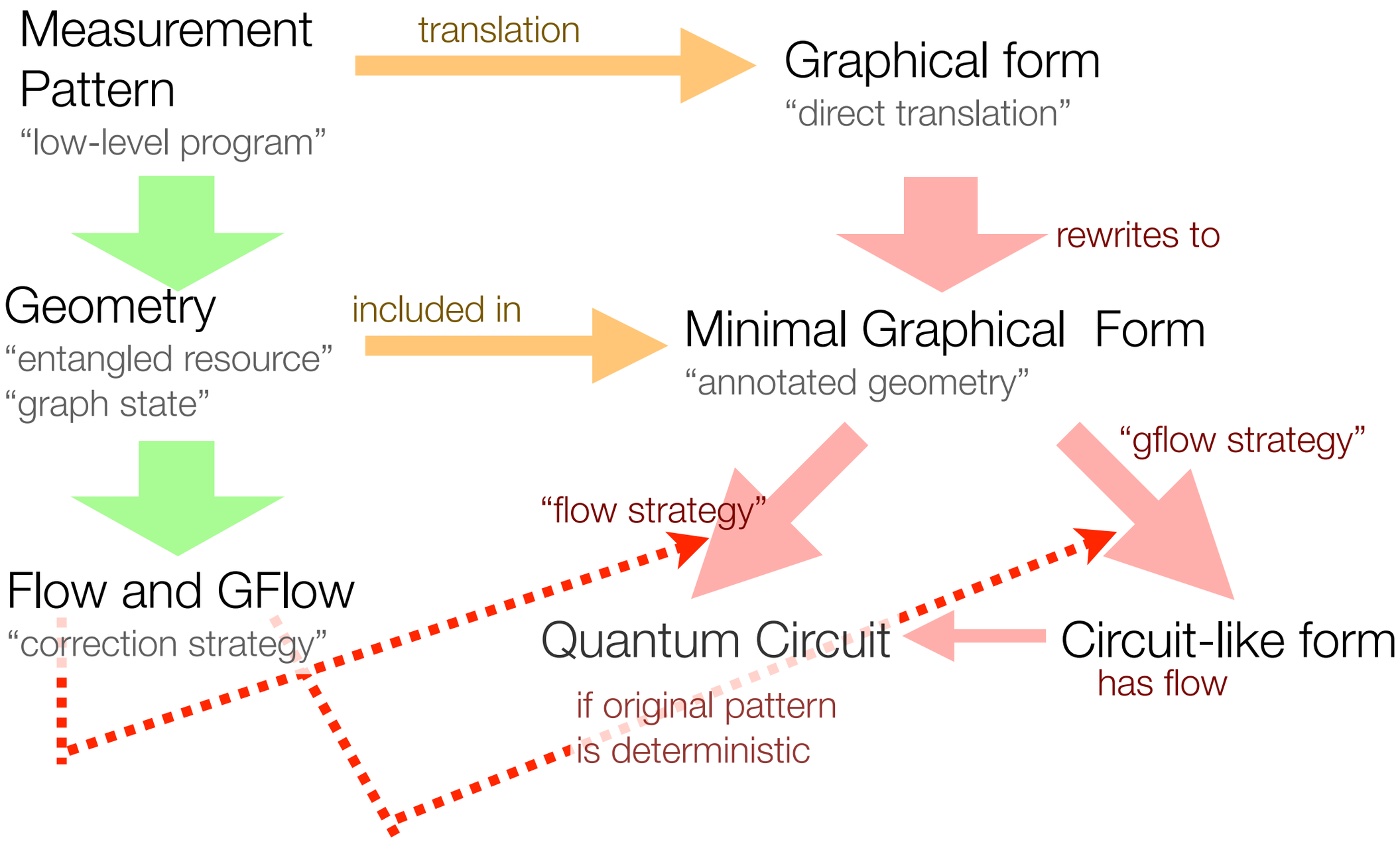
The plan:


Measurement Pattern
"low-level program"
translation
Graphical form
"direct translation"
rewrites to
Geometry
"entangled resource"
"graph state"
included in
Minimal Graphical Form
"annotated geometry"
Flow and GFlow
"correction strategy"

The plan:

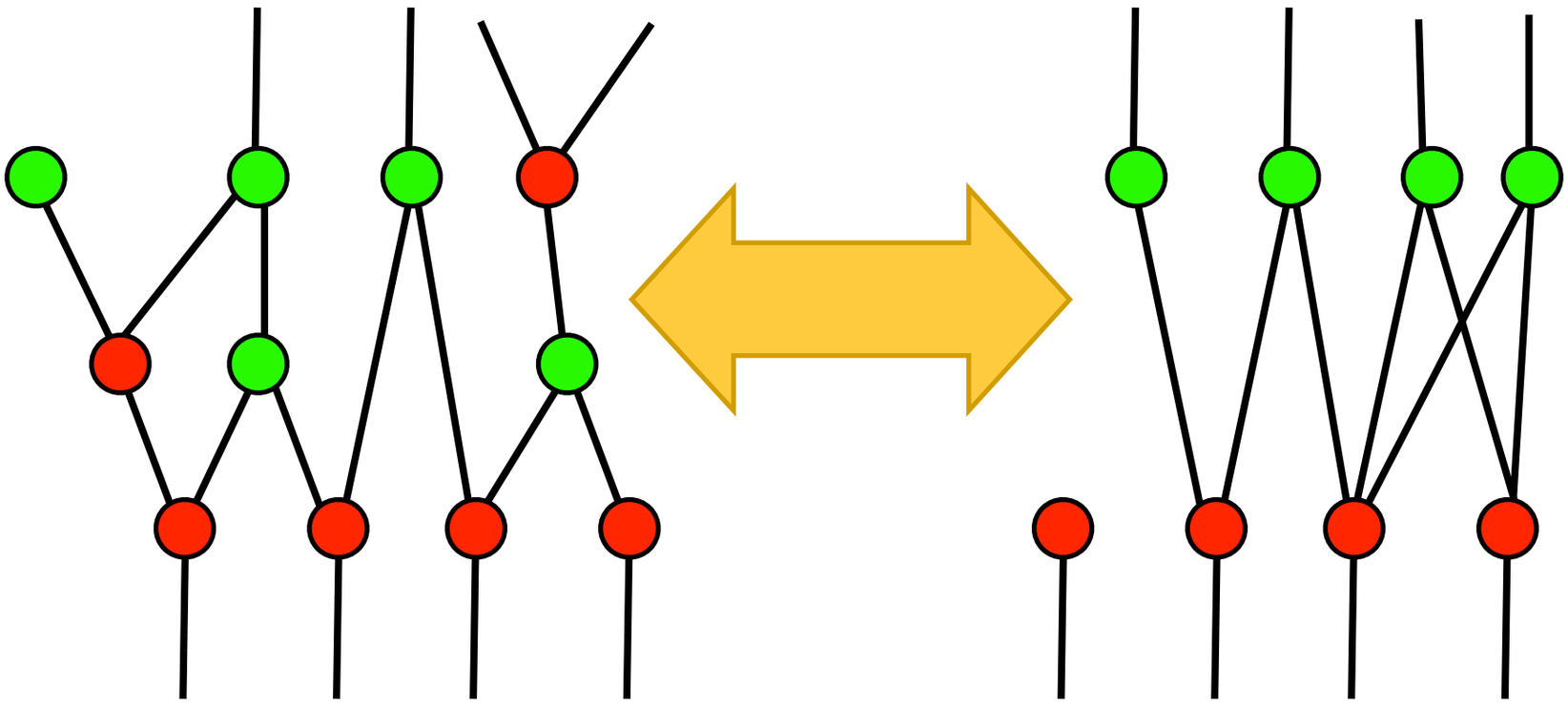

Measurement Pattern
“low-level program”
translation
Graphical form
“direct translation”
rewrites to
Geometry
“entangled resource”
“graph state”
included in
Minimal Graphical Form
“annotated geometry”
“flow strategy”
Flow and GFlow
“correction strategy”
Quantum Circuit
if original pattern
is deterministic

The plan:

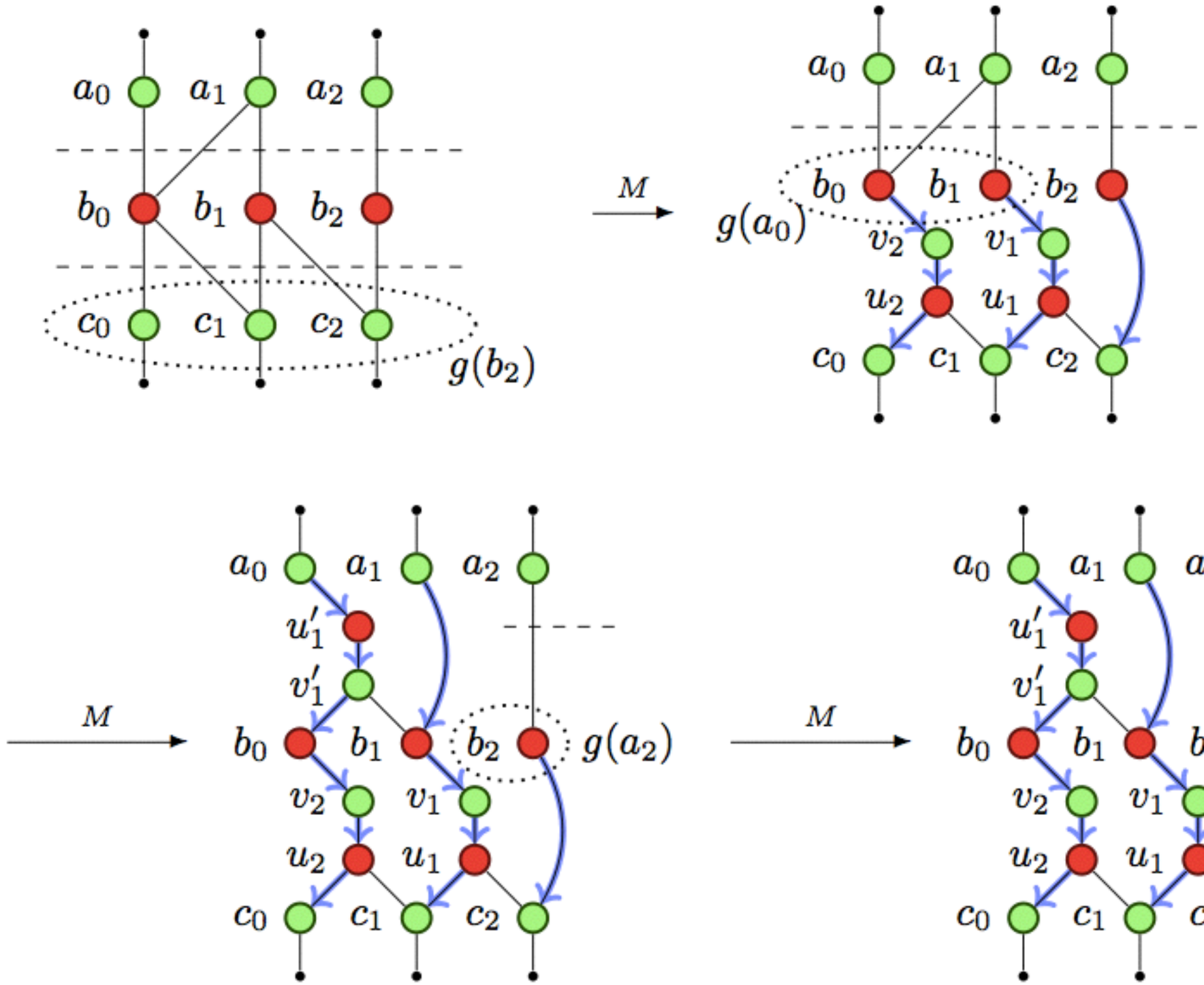

Measurement Pattern
"low-level program"
translation
Graphical form
"direct translation"
rewrites to
Geometry
"entangled resource"
"graph state"
included in
Minimal Graphical Form
"annotated geometry"
"gflow strategy"
"flow strategy"
Flow and GFlow
"correction strategy"
Quantum Circuit
if original pattern
is deterministic
Circuit-like form
has flow

Hopf Algebra Equivalence

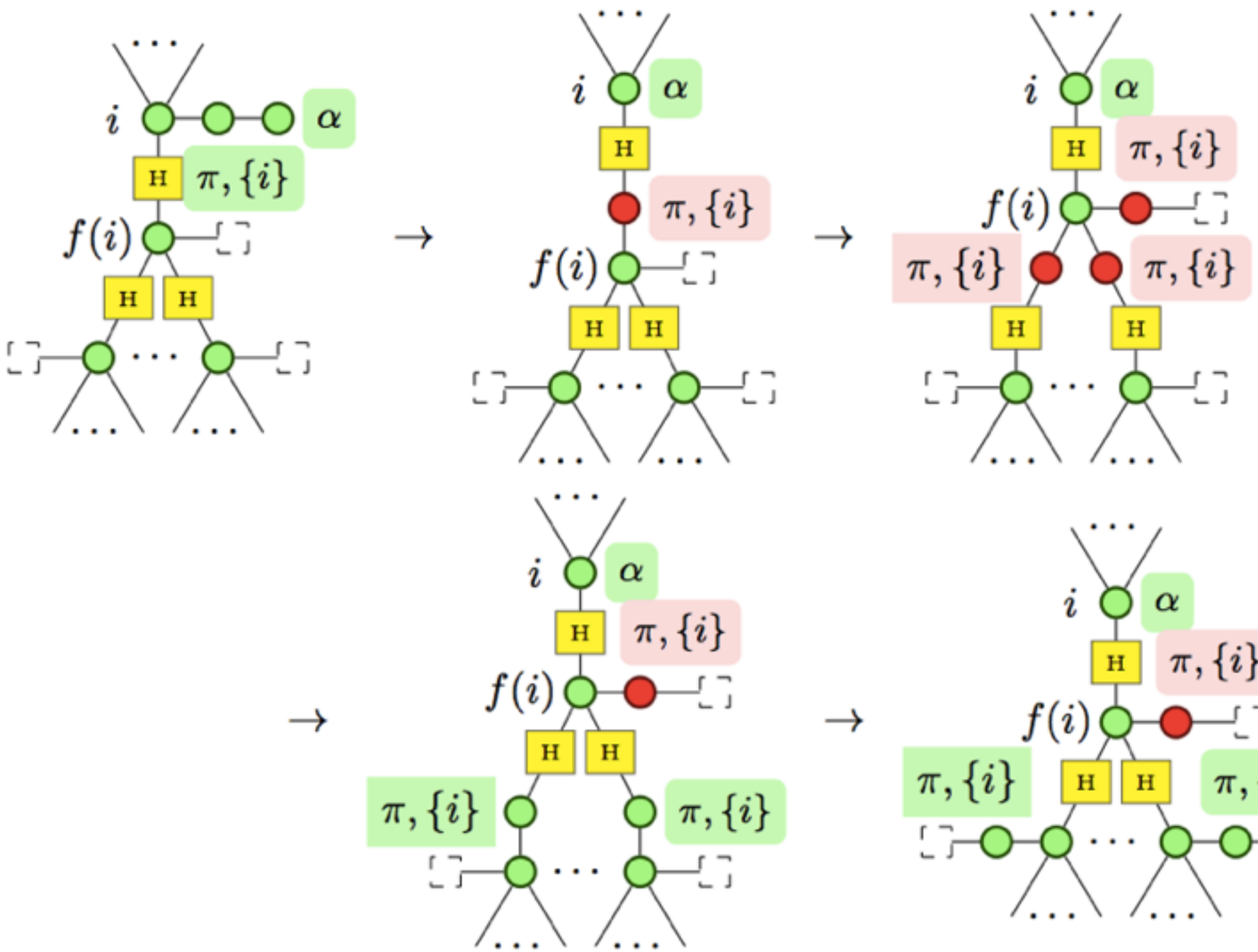
Thm: any Hopf algebra expression can be put into normal form:



GFlow Strategy



Flow Strategy

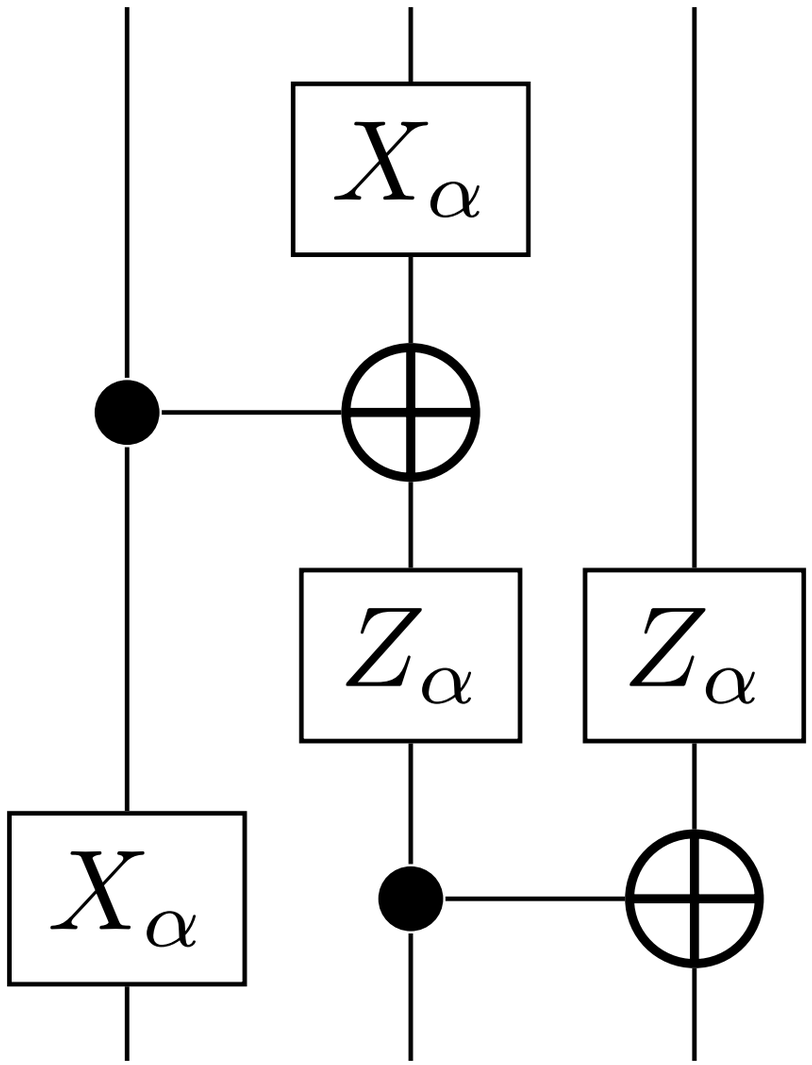


Application 1: MBQC

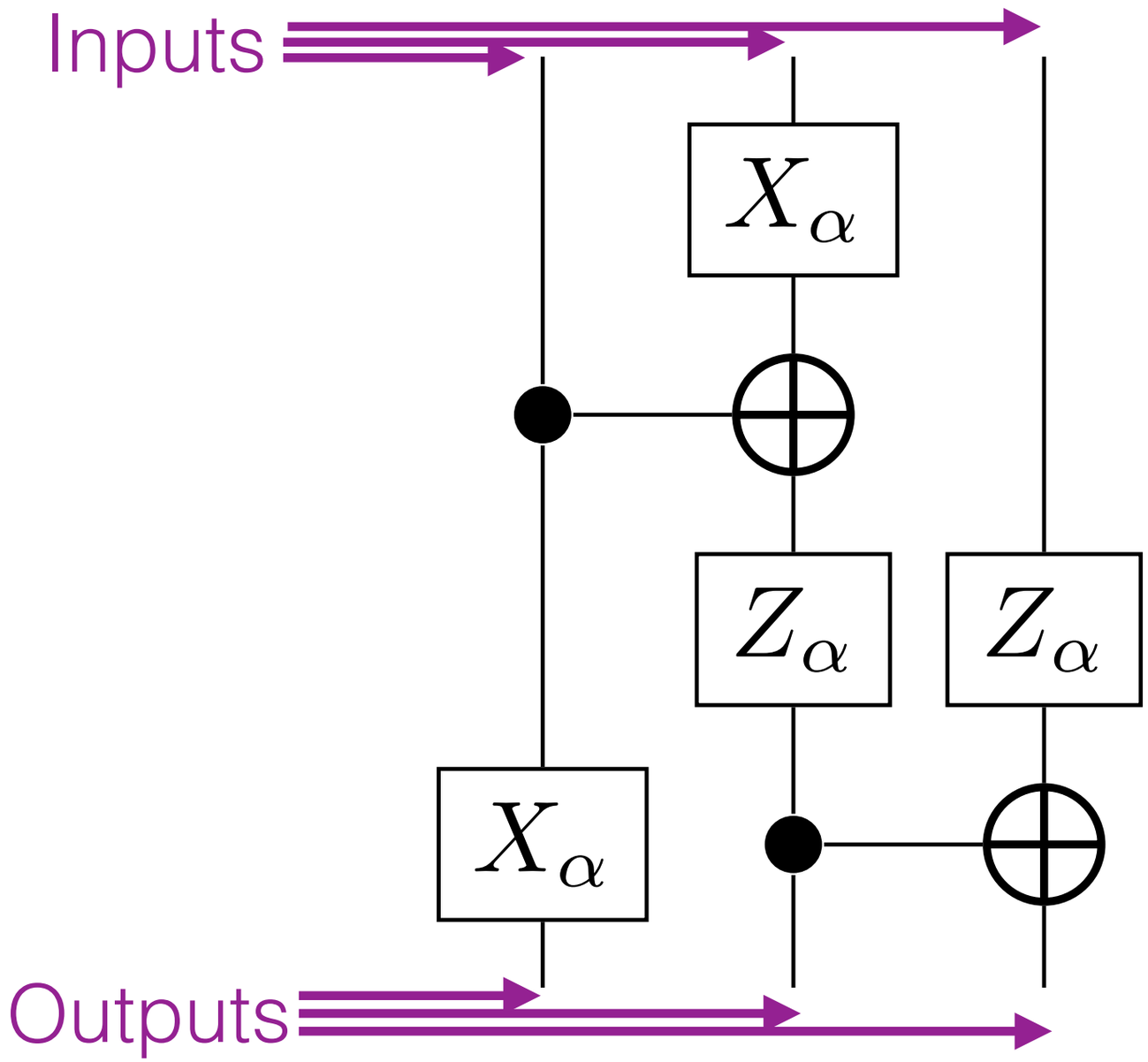
Result: complicated MBQC *implementation* to simpler circuit *specification*.

WIP: the converse, optimally.

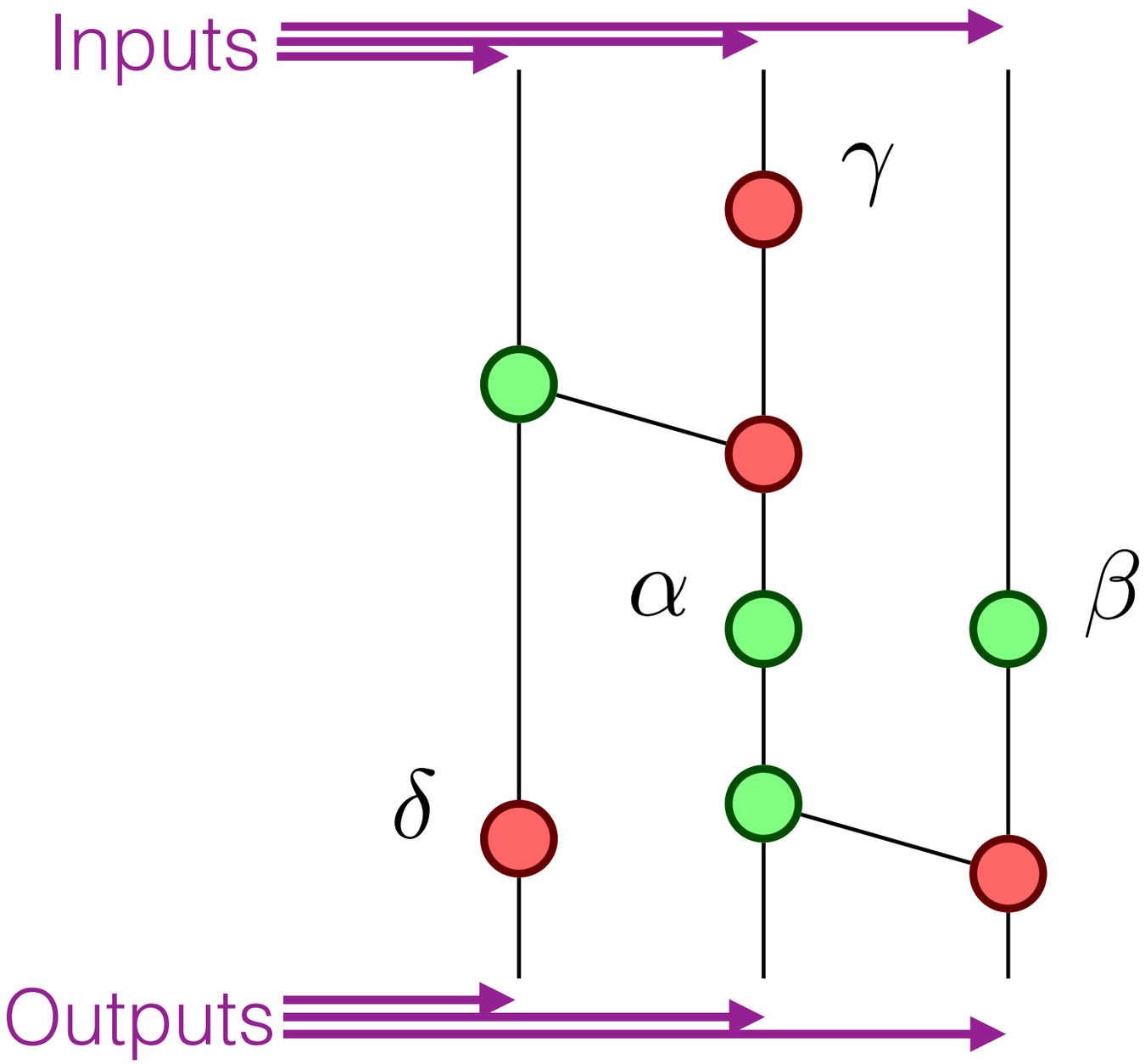
Circuit Perspective



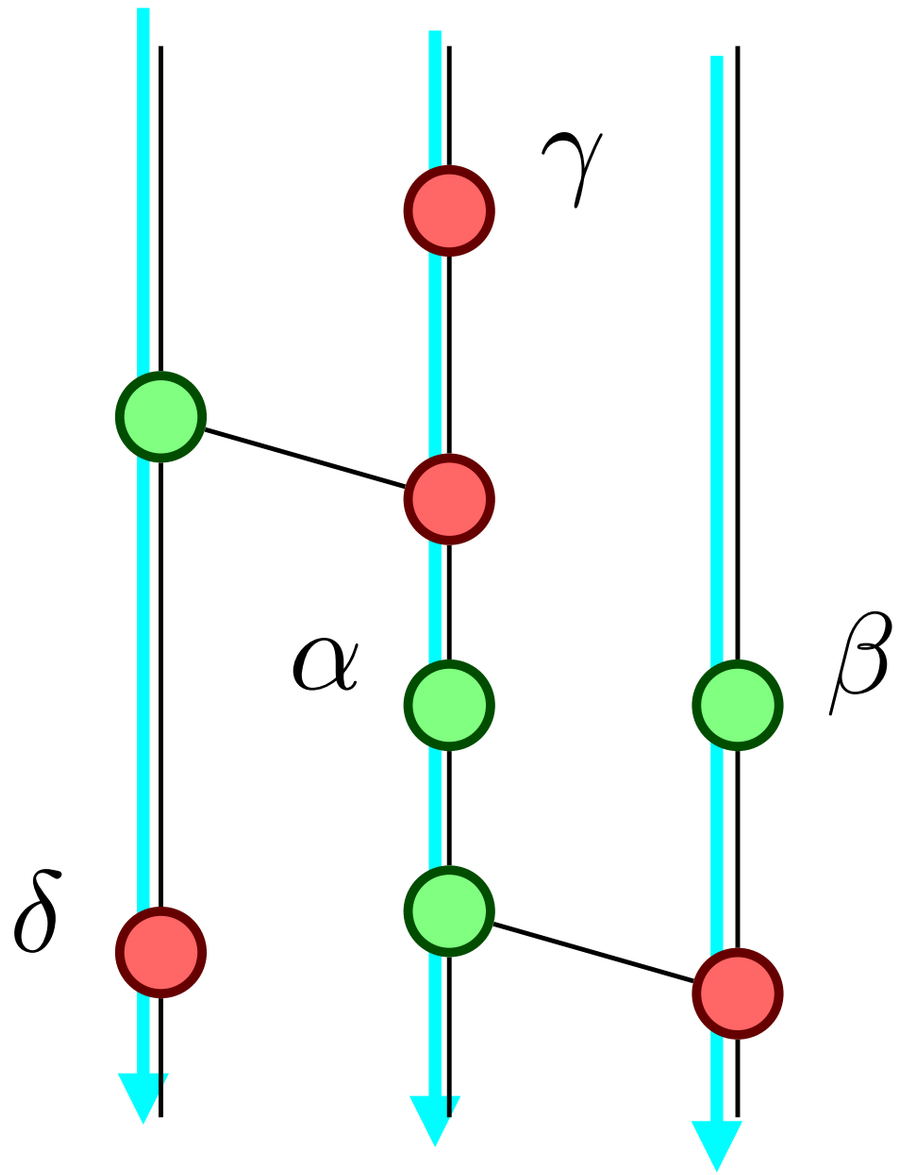
Circuit Perspective



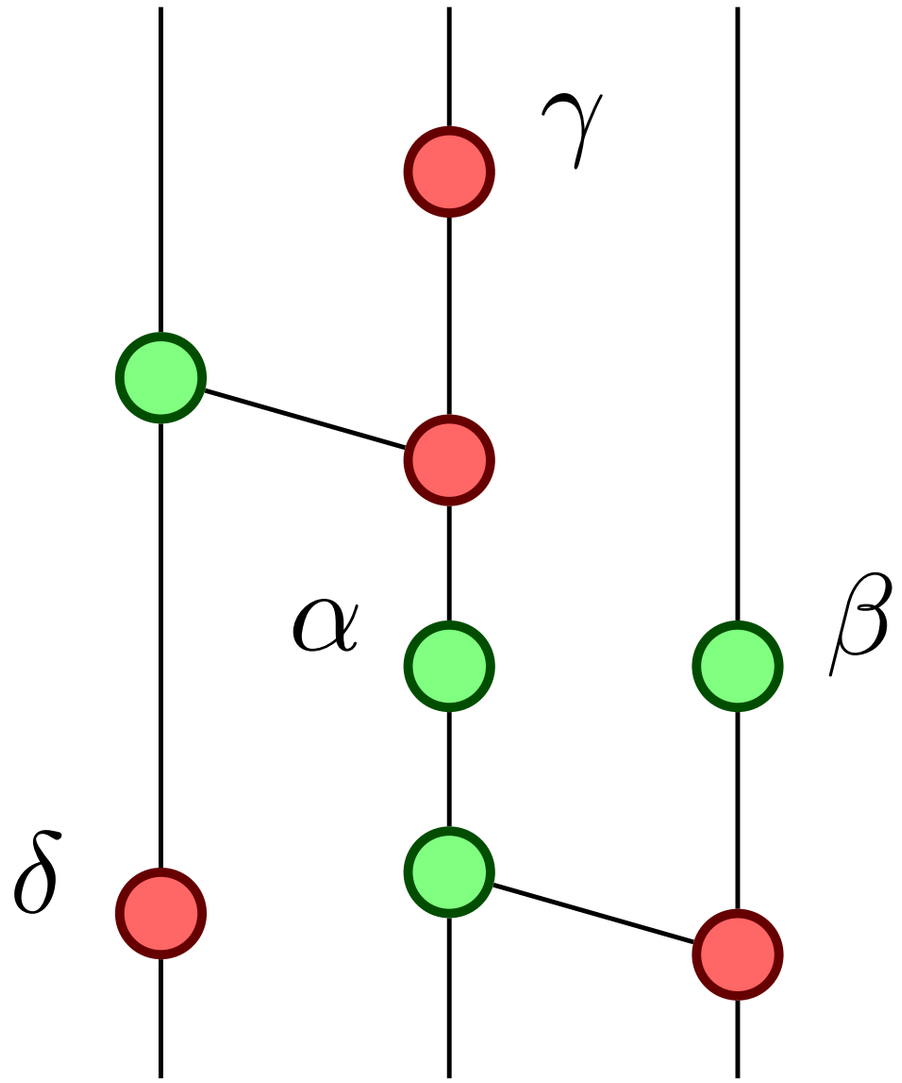
Circuit Perspective



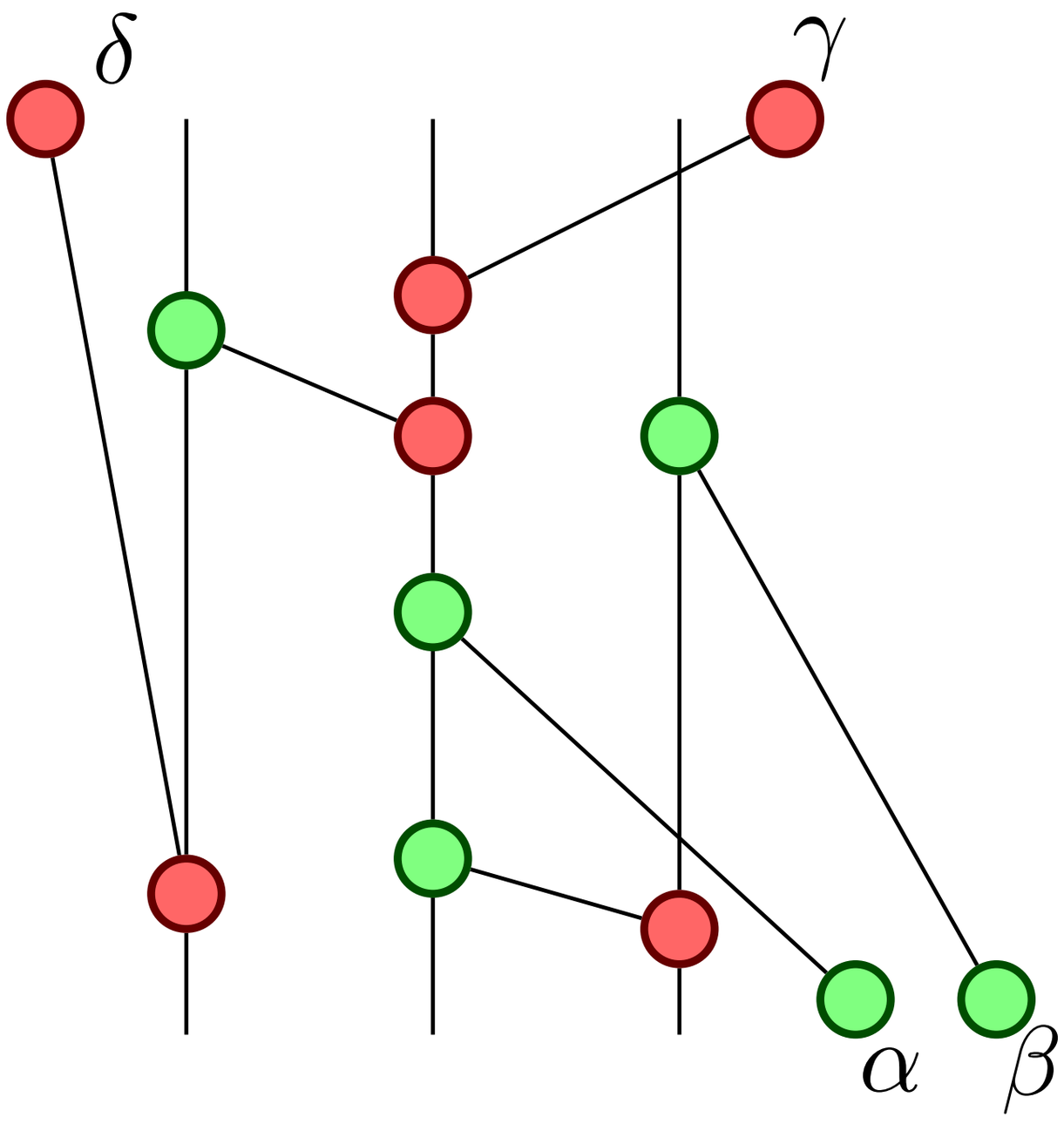
Circuit Perspective



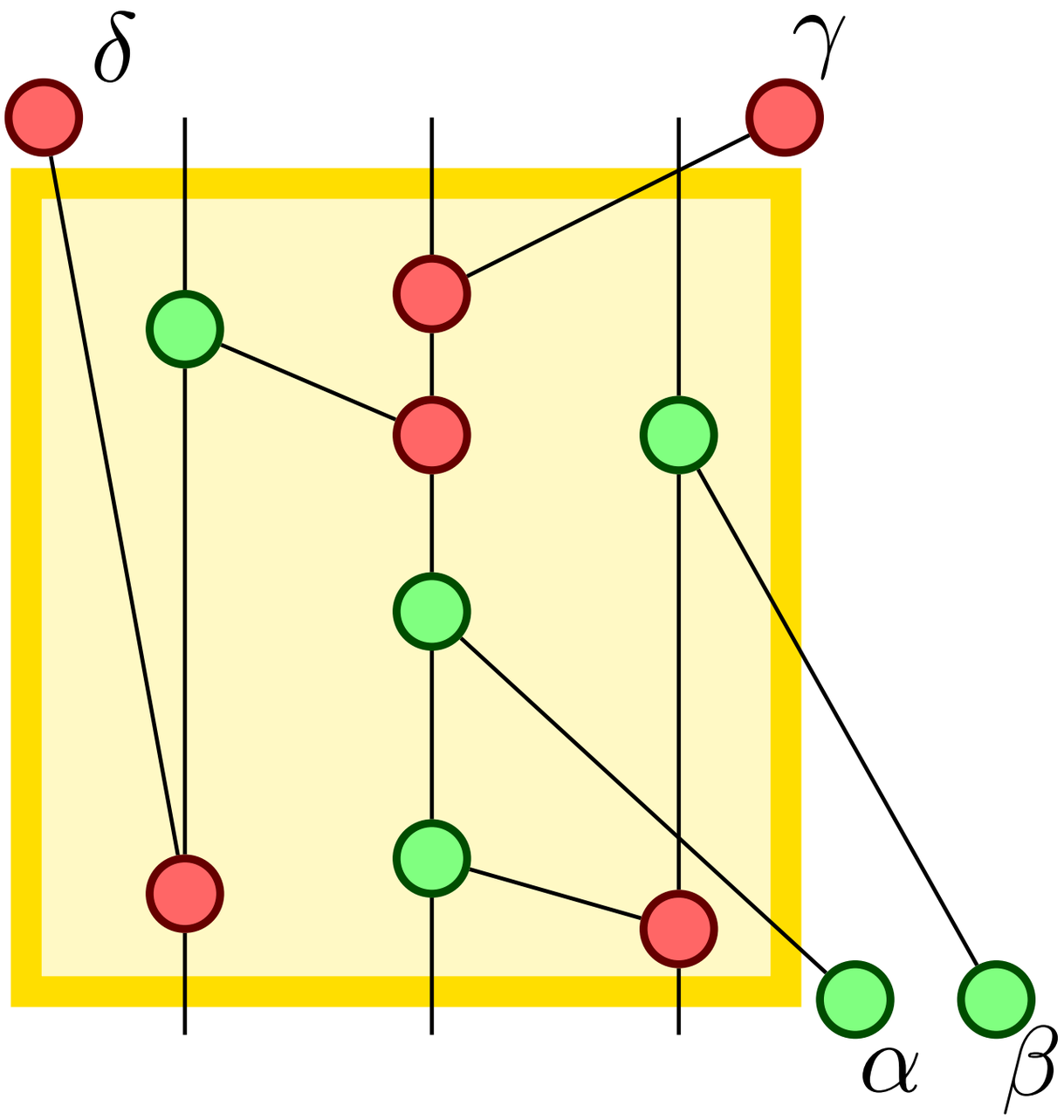
Circuit Perspective



??? Perspective

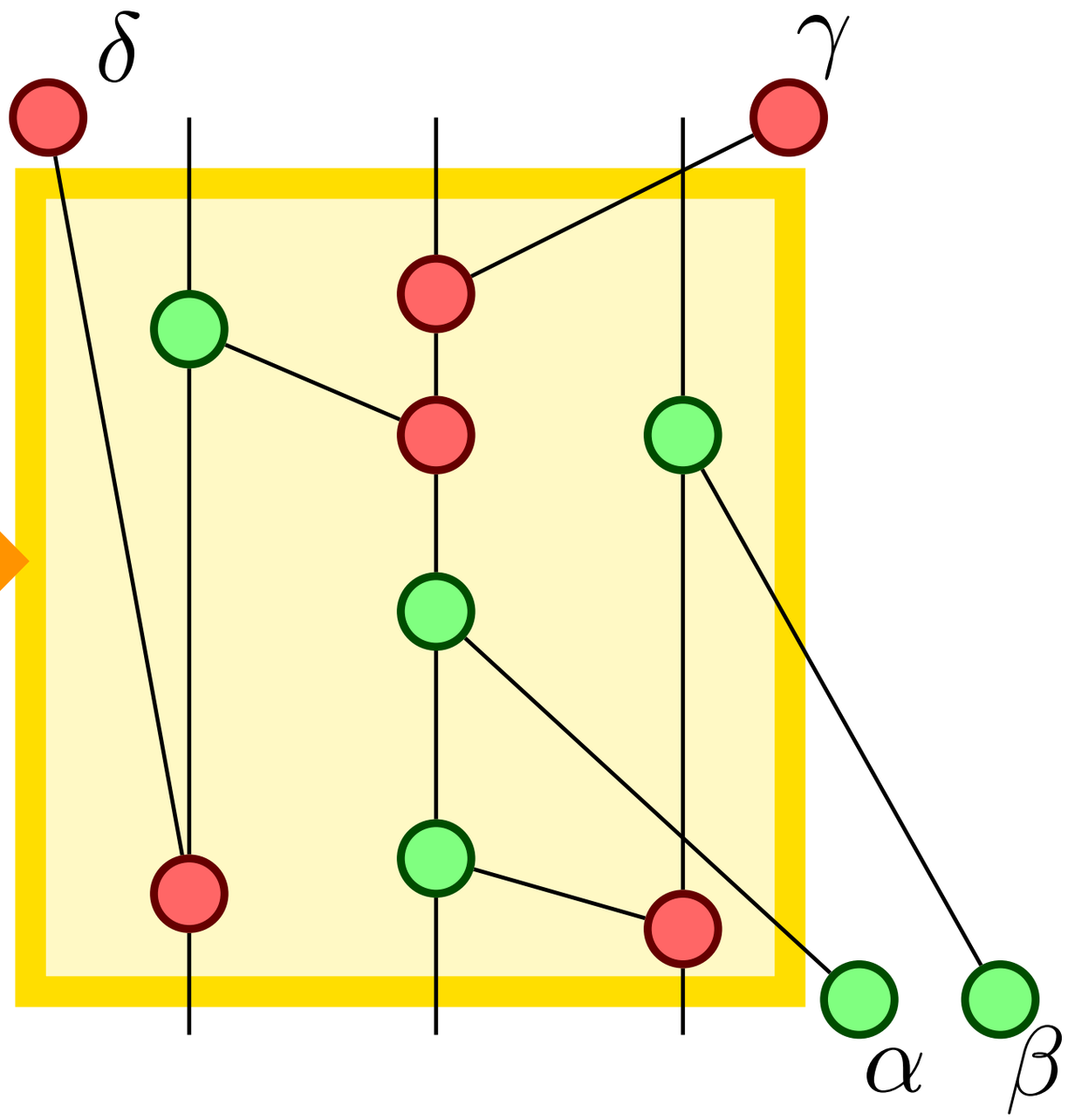


??? Perspective



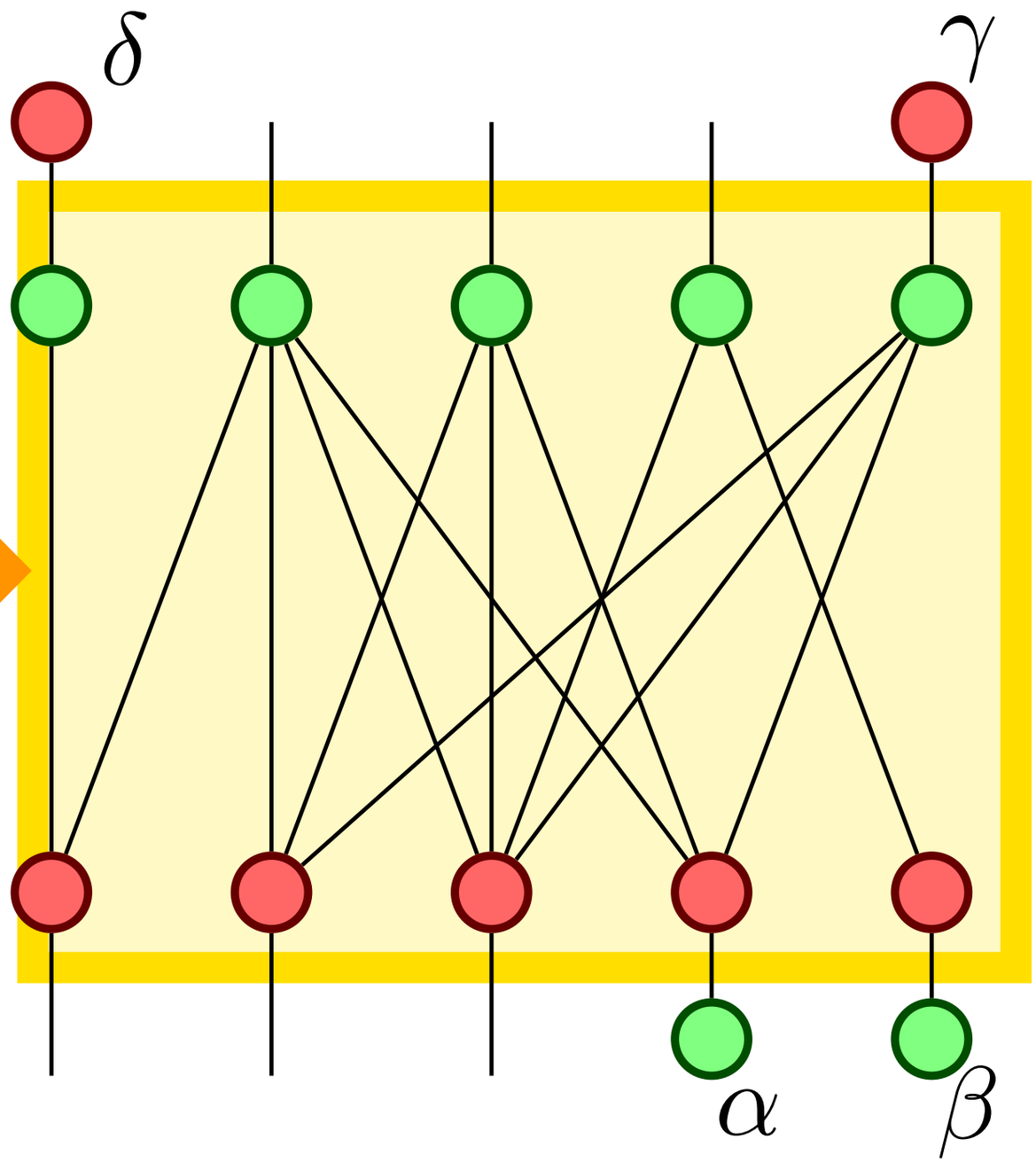
??? Perspective

Hopf algebra expression

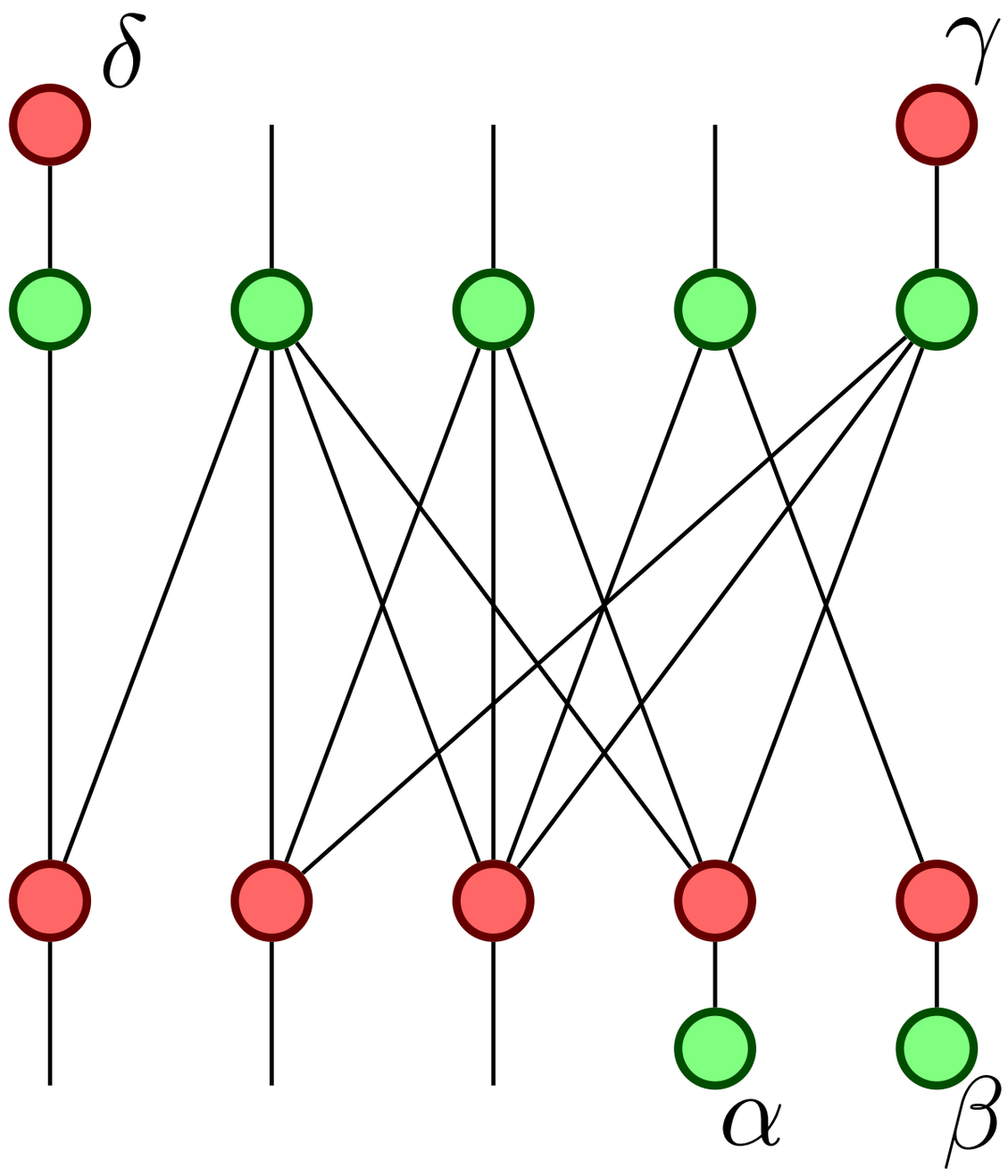


??? Perspective

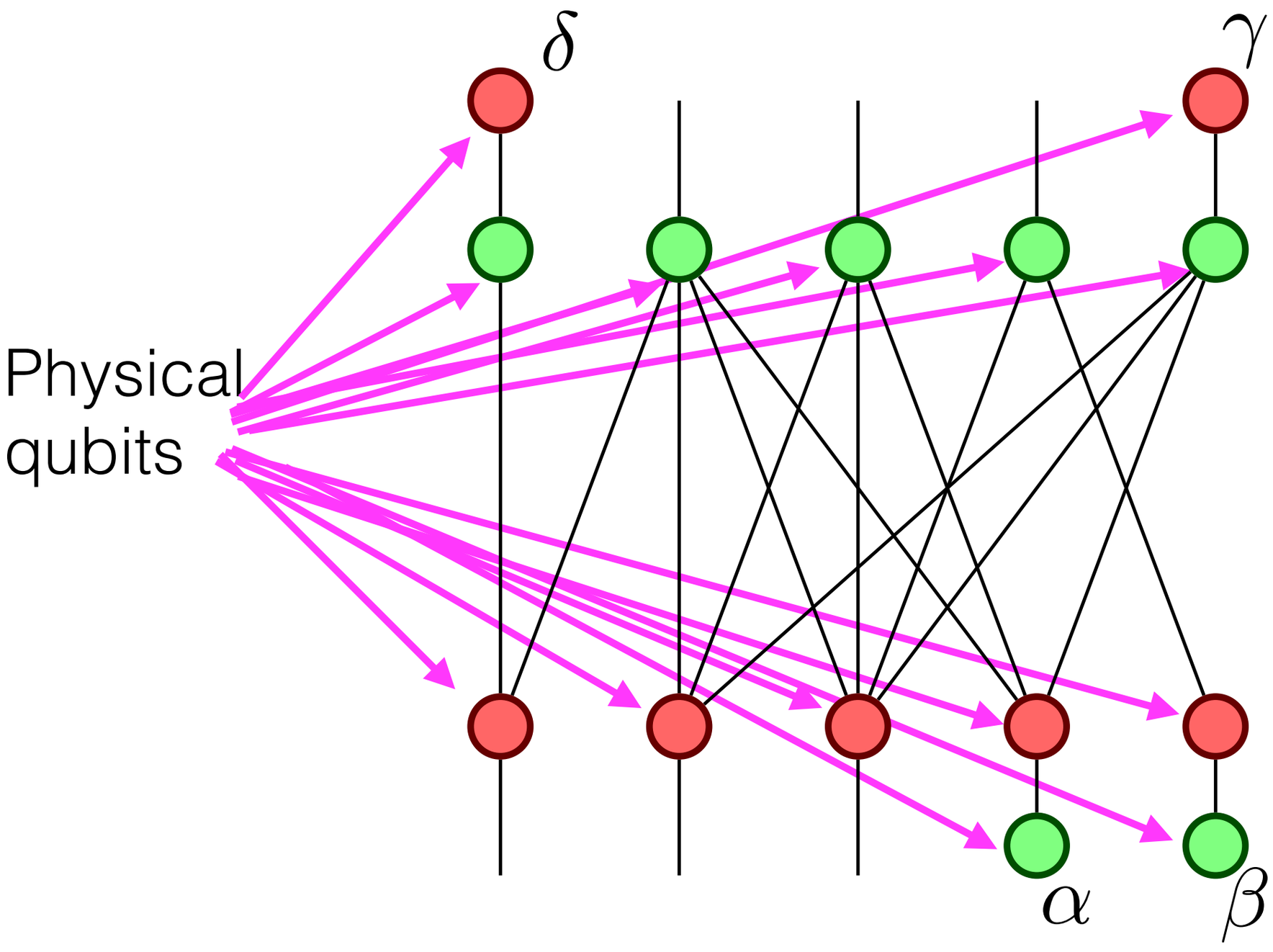
Hopf algebra
normal form



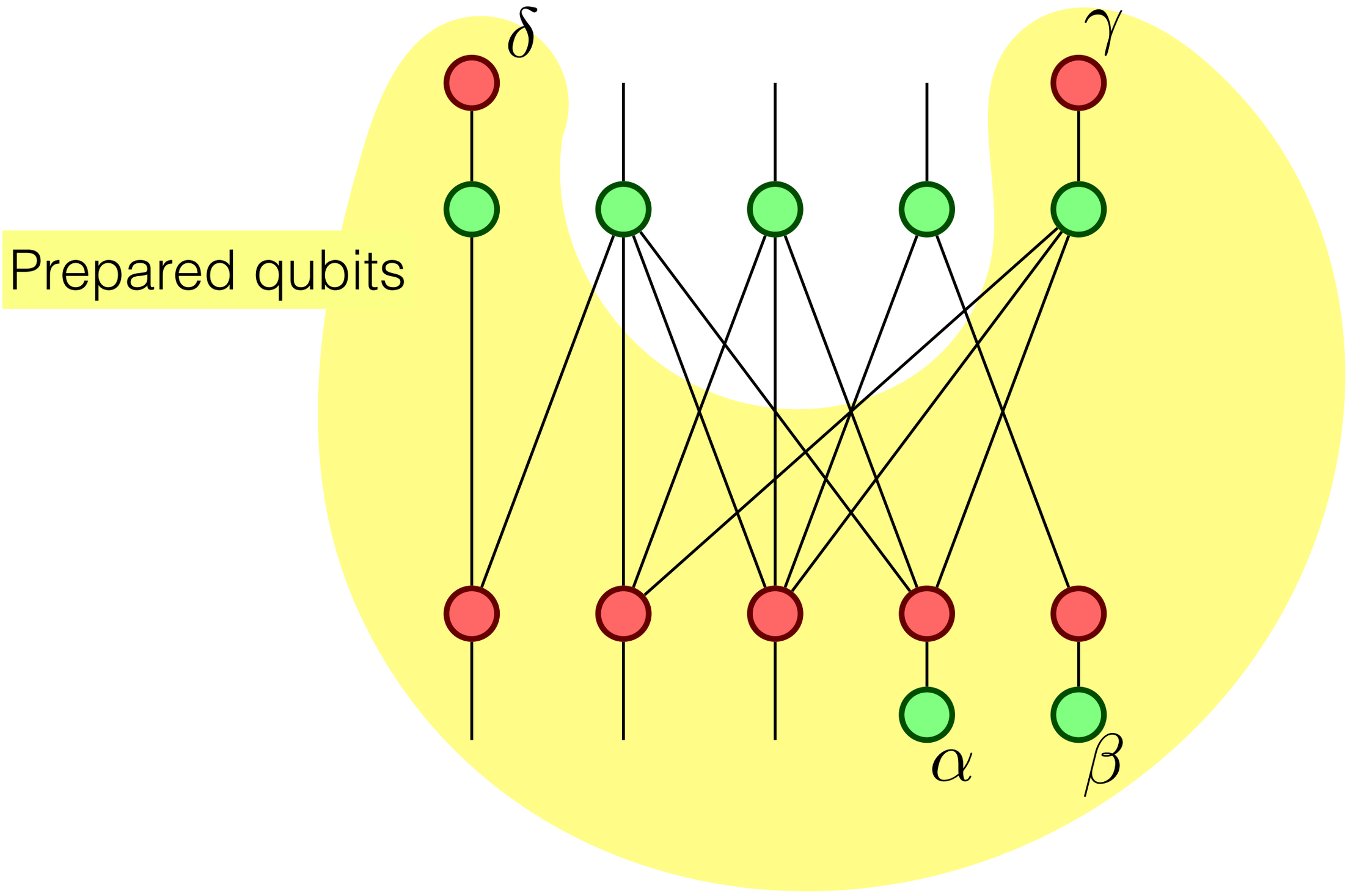
MBQC Perspective



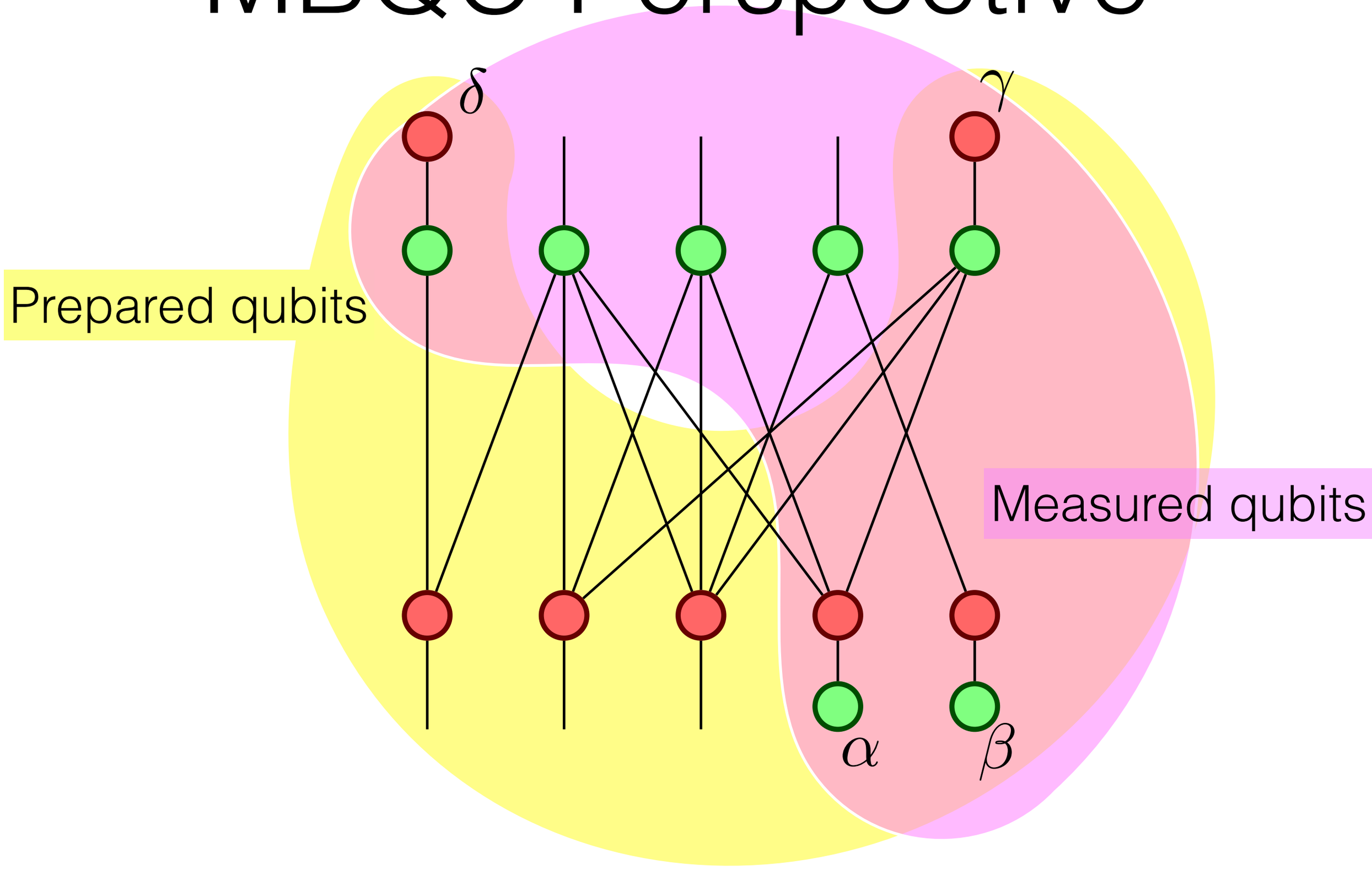
MBQC Perspective



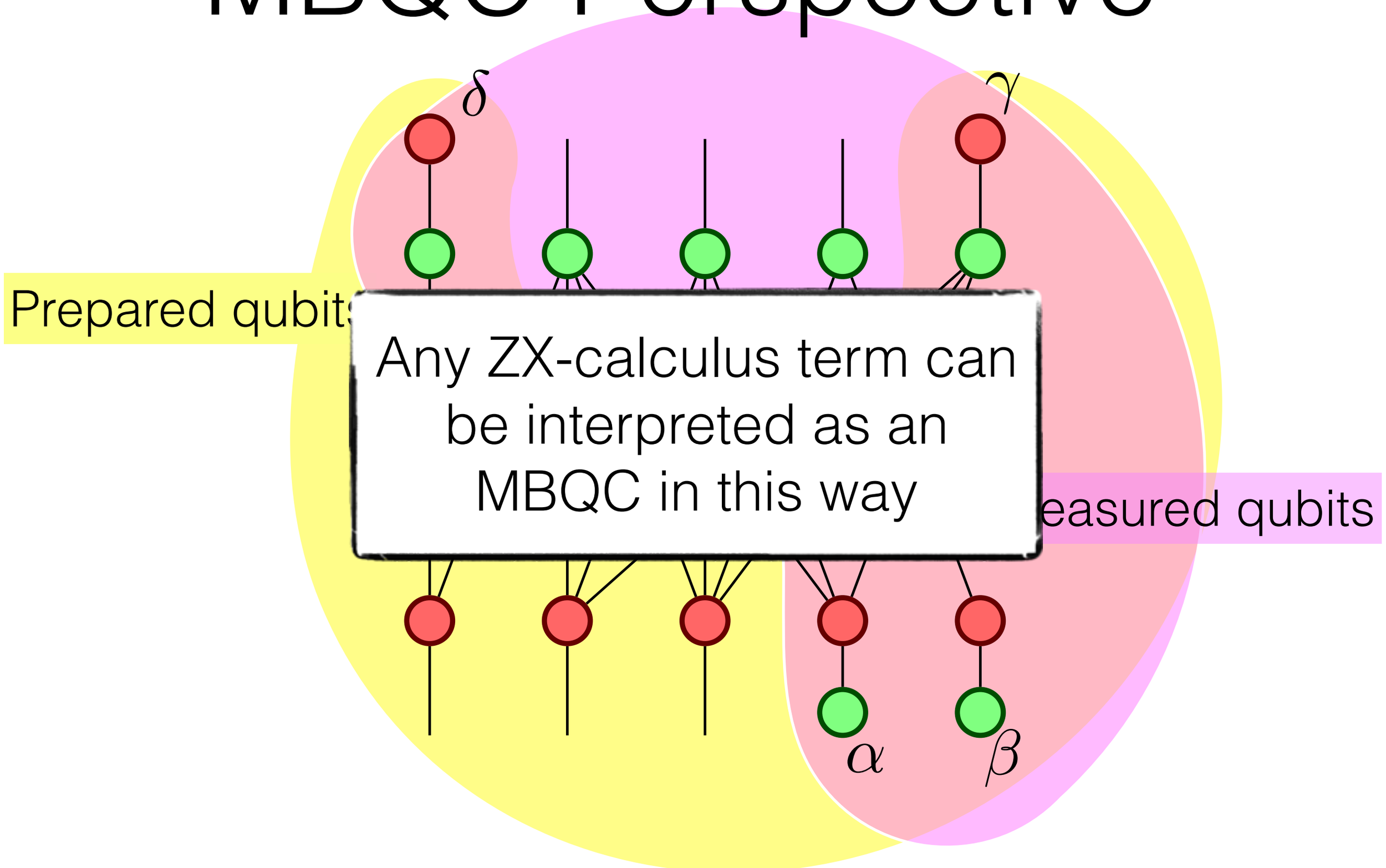
MBQC Perspective



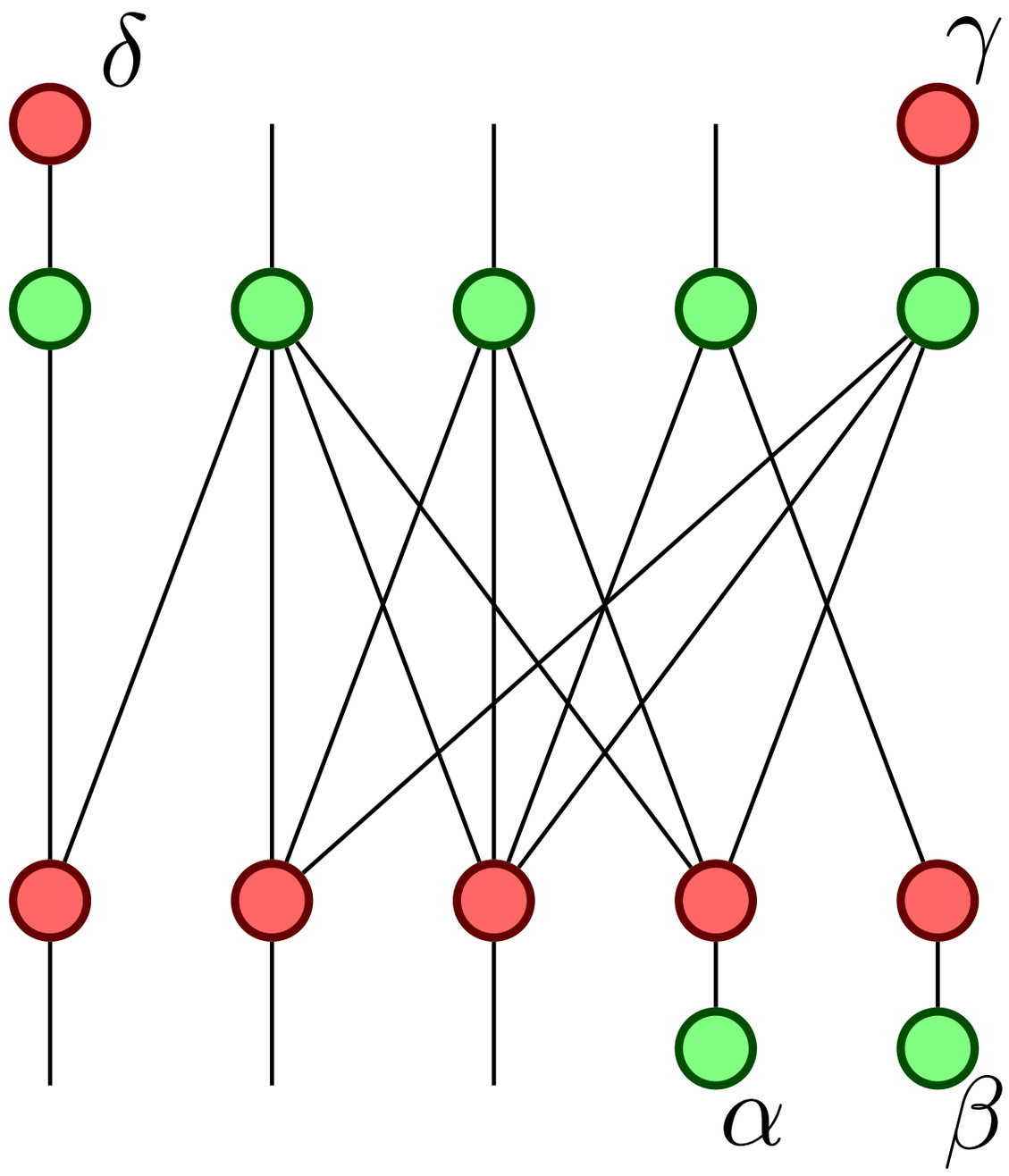
MBQC Perspective



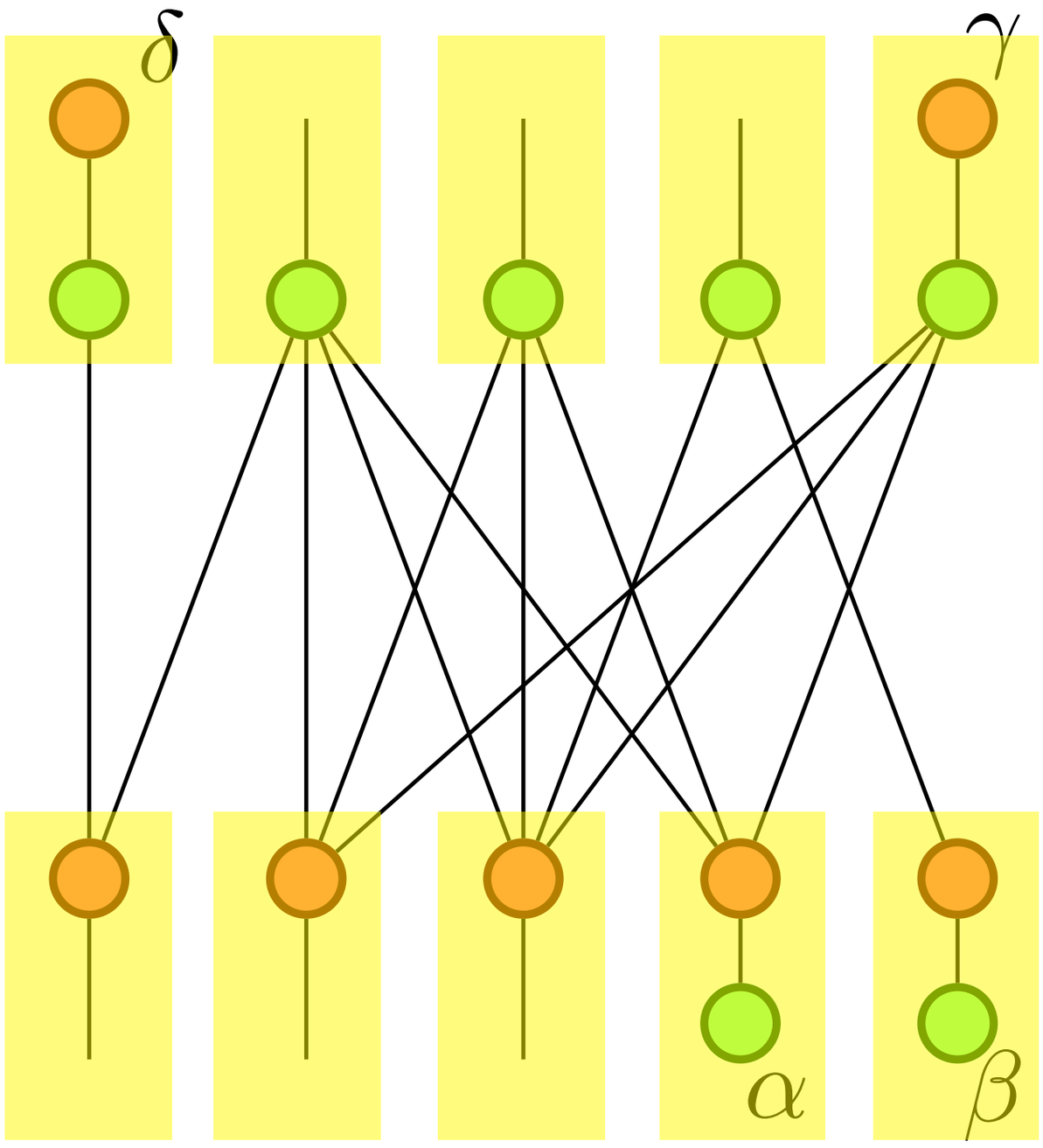
MBQC Perspective



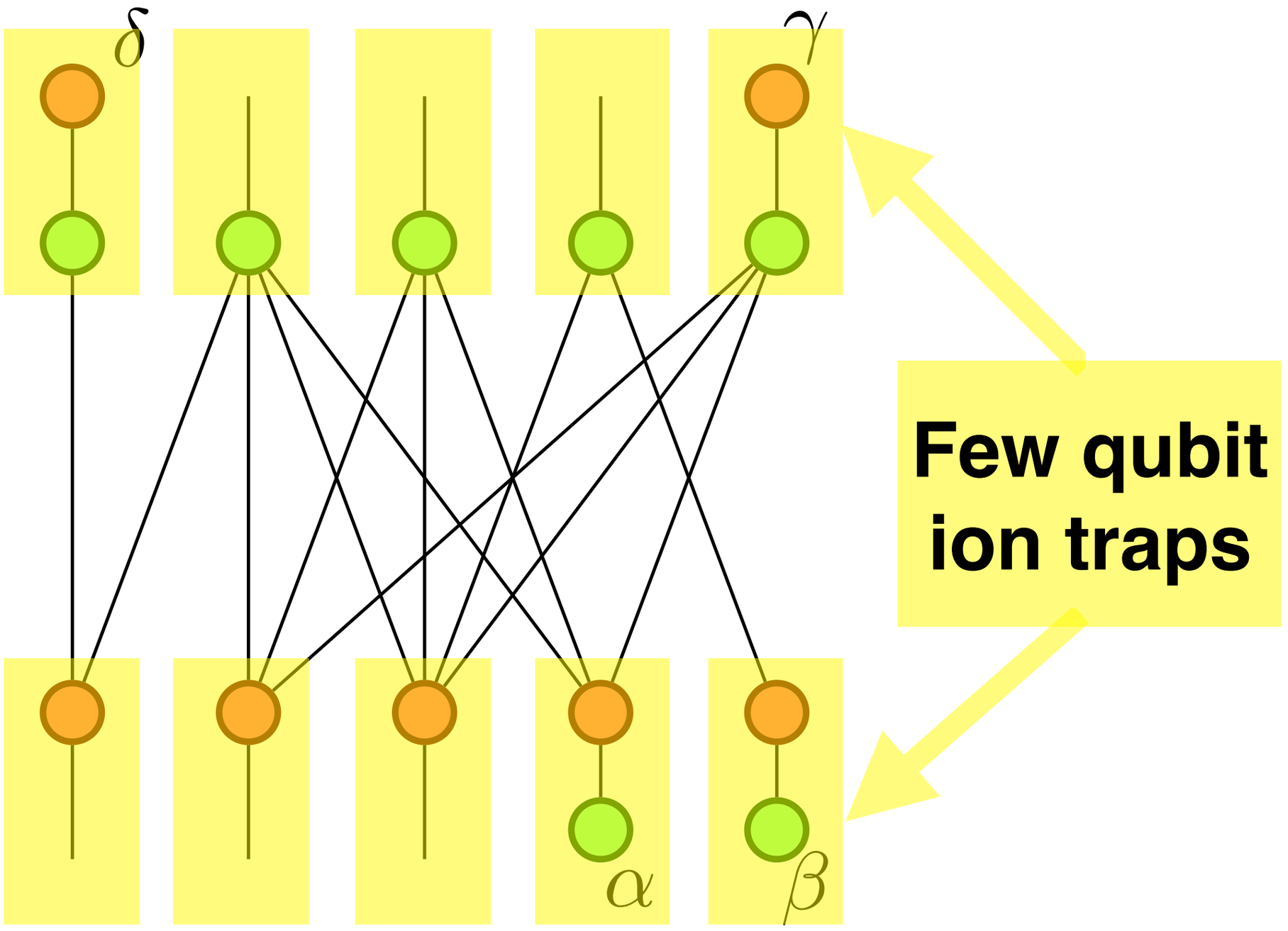
NQIT Perspective



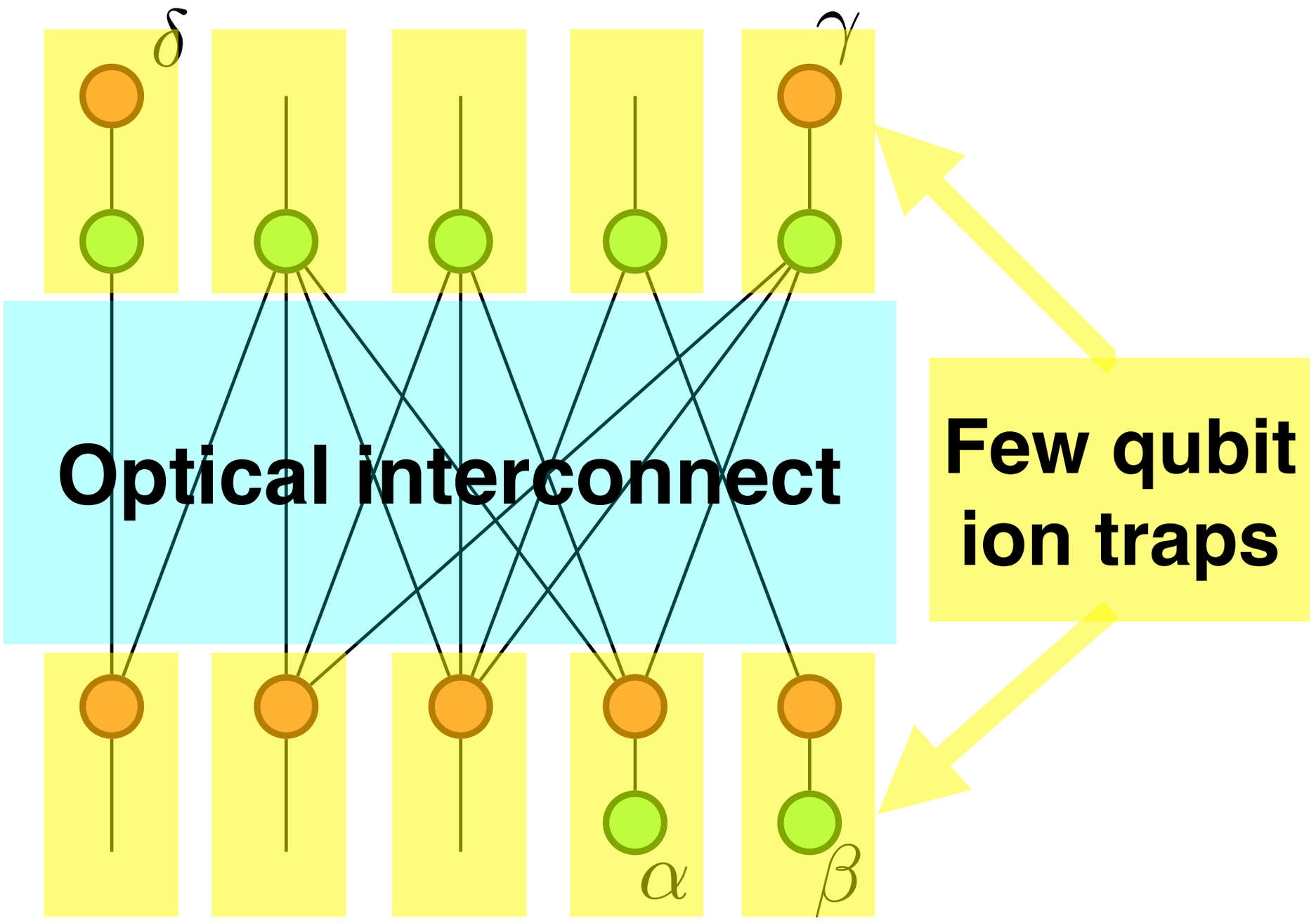
NQIT Perspective



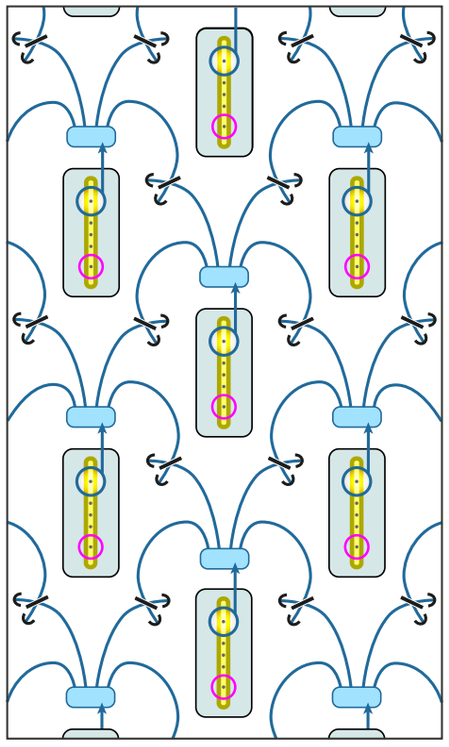
NQIT Perspective

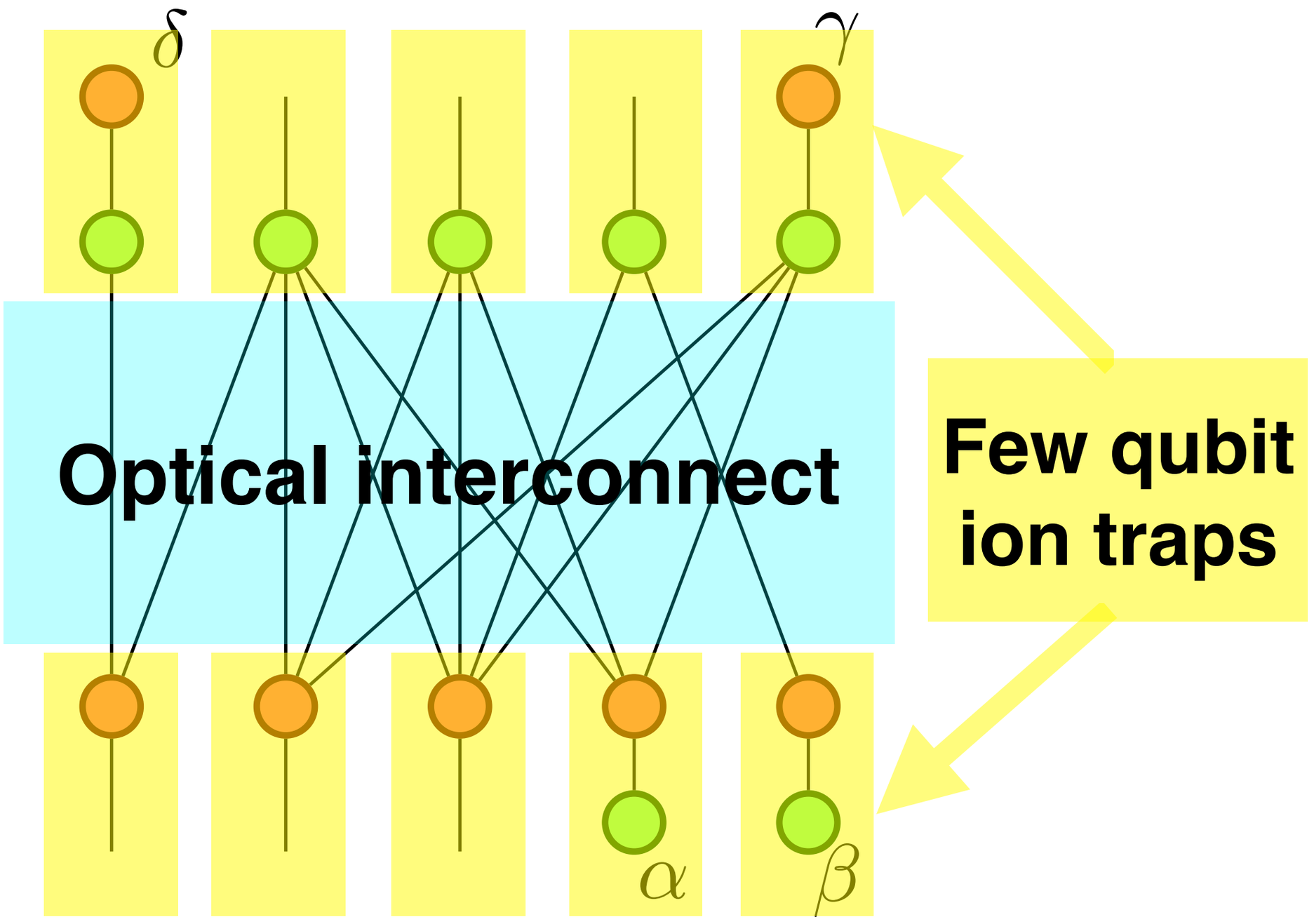


NQIT Perspective



NQIT Perspective





5.

Prospectus

I did not talk about:

- Mixed states, CP-maps, probabilities
- Causality
- Contextuality, Non-locality
- Infinite dimensional spaces

I did not talk about:

- Mixed states, CP-maps, probabilities

doi : 10.1016/j.entcs.2006.12.018

- Causality

arXiv:1107.6019

- Contextuality, Non-locality

arXiv:1203.4988

- Infinite dimensional spaces

arXiv:1011.6123
arXiv:1605.04305

I did not talk about:

- Algorithms: Deutsch-Josza, Grover, Hidden Subgroup (Vicary, Zeng, Gogioso, Kissinger)

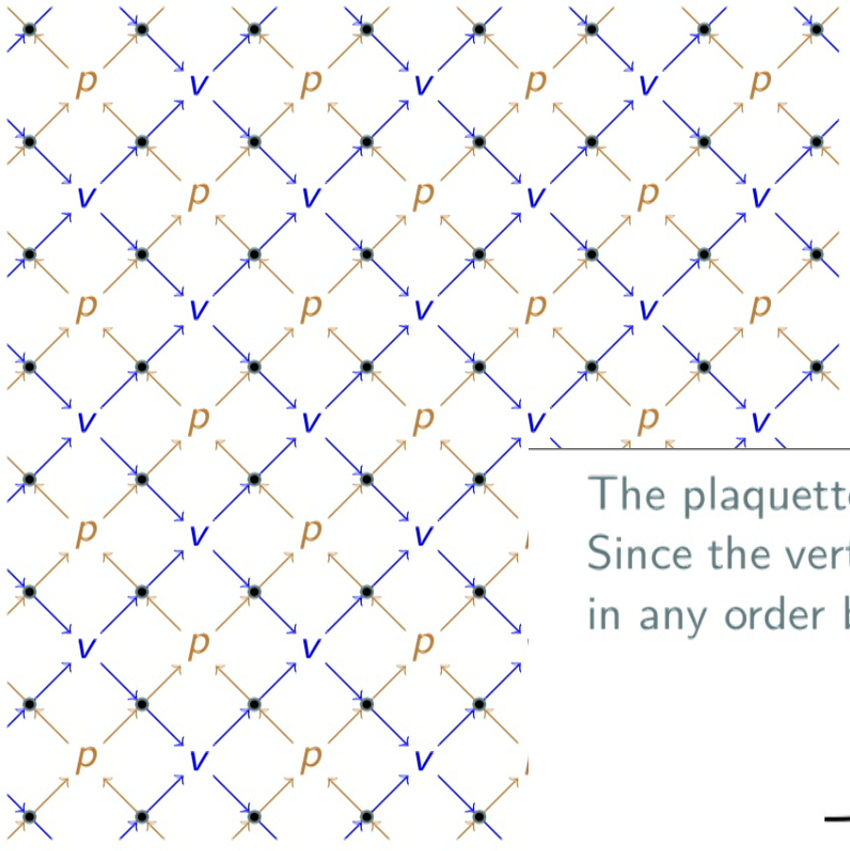
- Quantum Key Distribution (Hillebrand, Kissinger, Tull, Westerbaan)

- Error Correction (RD, Horsman et al)

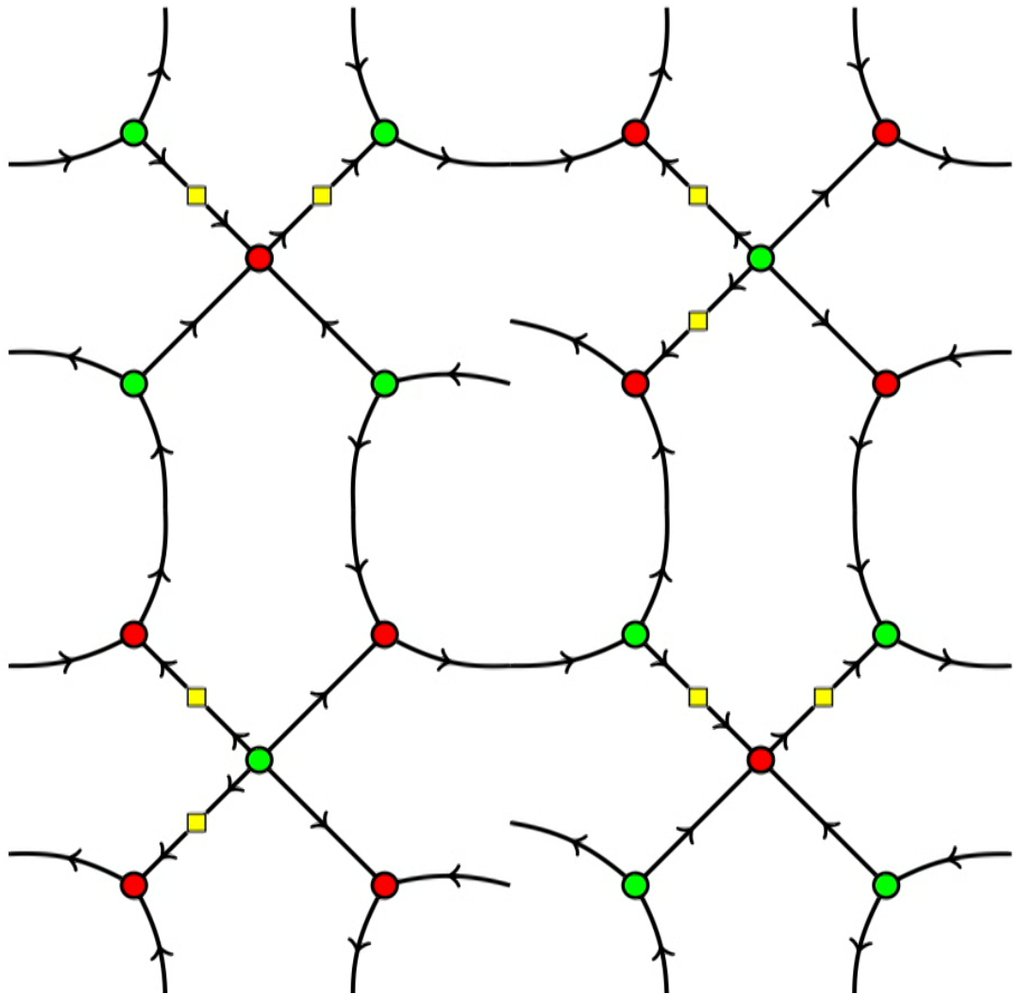
- Secret sharing (Gogioso, Perdrix)

- Topological Quantum Computing (Horsman, de Beaudrap)

Now let's take a ~~ribbon graph~~dual pair of graphs underlying the Kitaev model on a surface:



The plaquette operators are the same, but with the colours reversed. Since the vertex and plaquette operators commute, we can compose them in any order by matching up the external terminals. For example like this:



Tobias Fritz — recent talk available on PIRSA

What next?

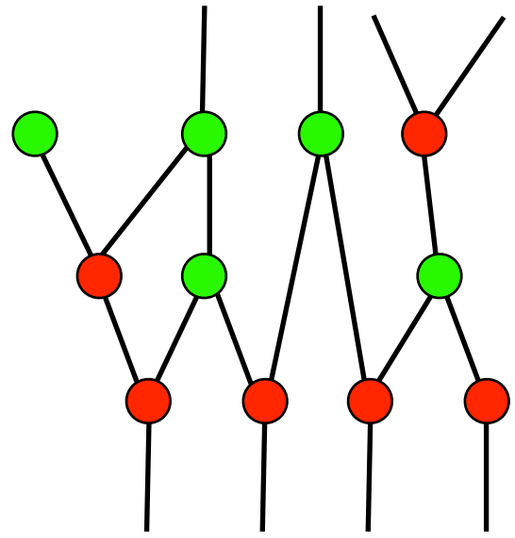
- “ZX-like” theories exist for any quantum system (including codeword spaces!)

- ZX-calculus has no commitment to architecture or causal structure

- ZX-calculus encodes quantum theory “below the gate level”

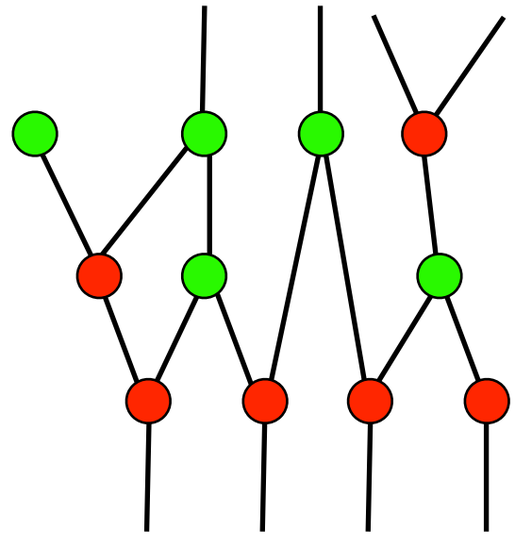
Extensional / Denotational

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

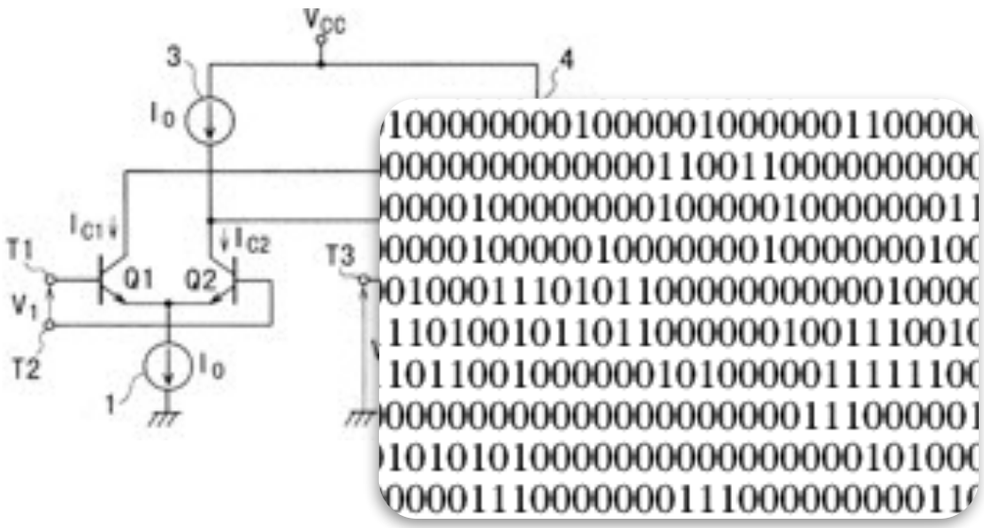


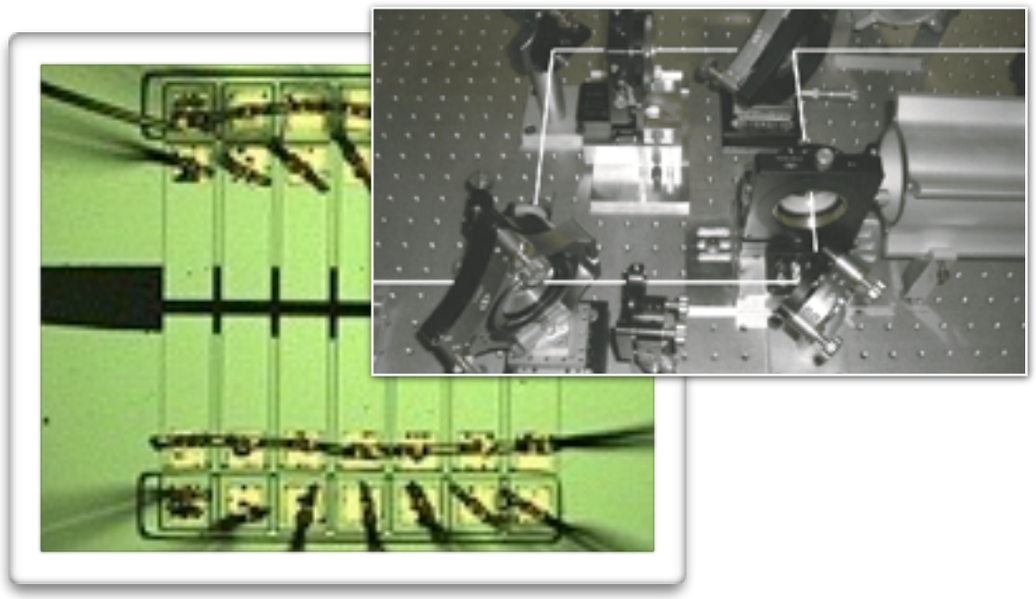
Extensional / Denotational

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



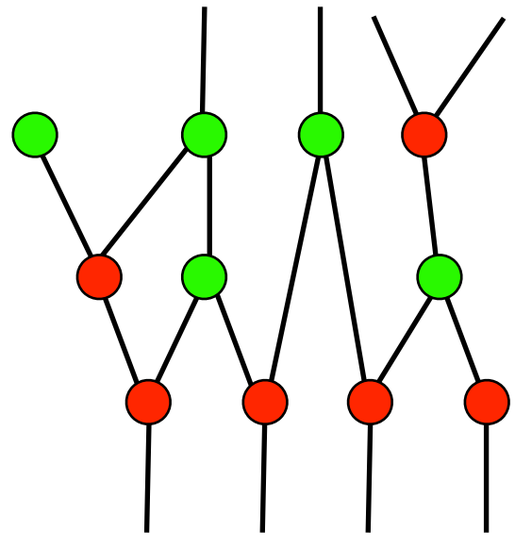
Intensional / Operational





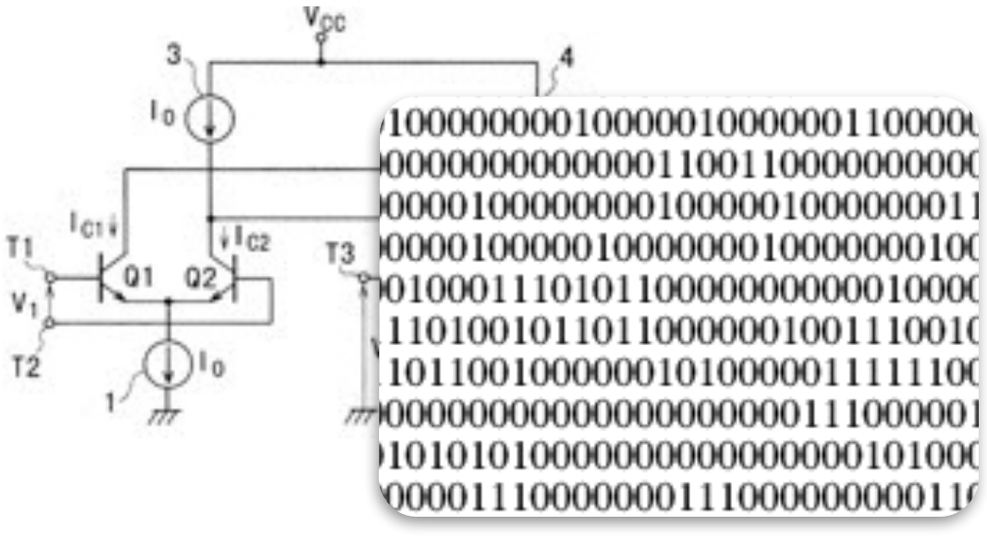
Extensional / Denotational

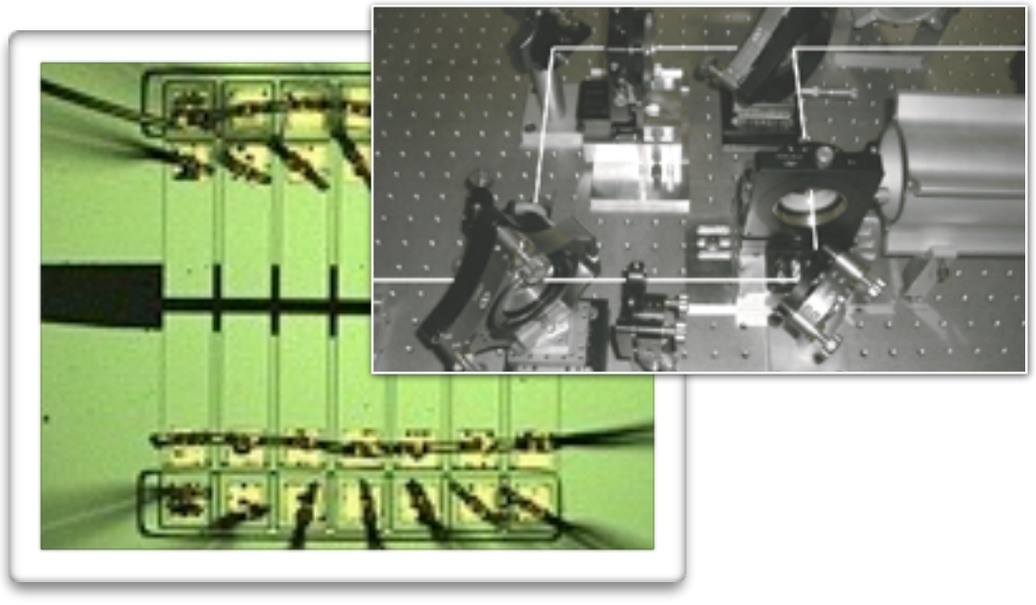
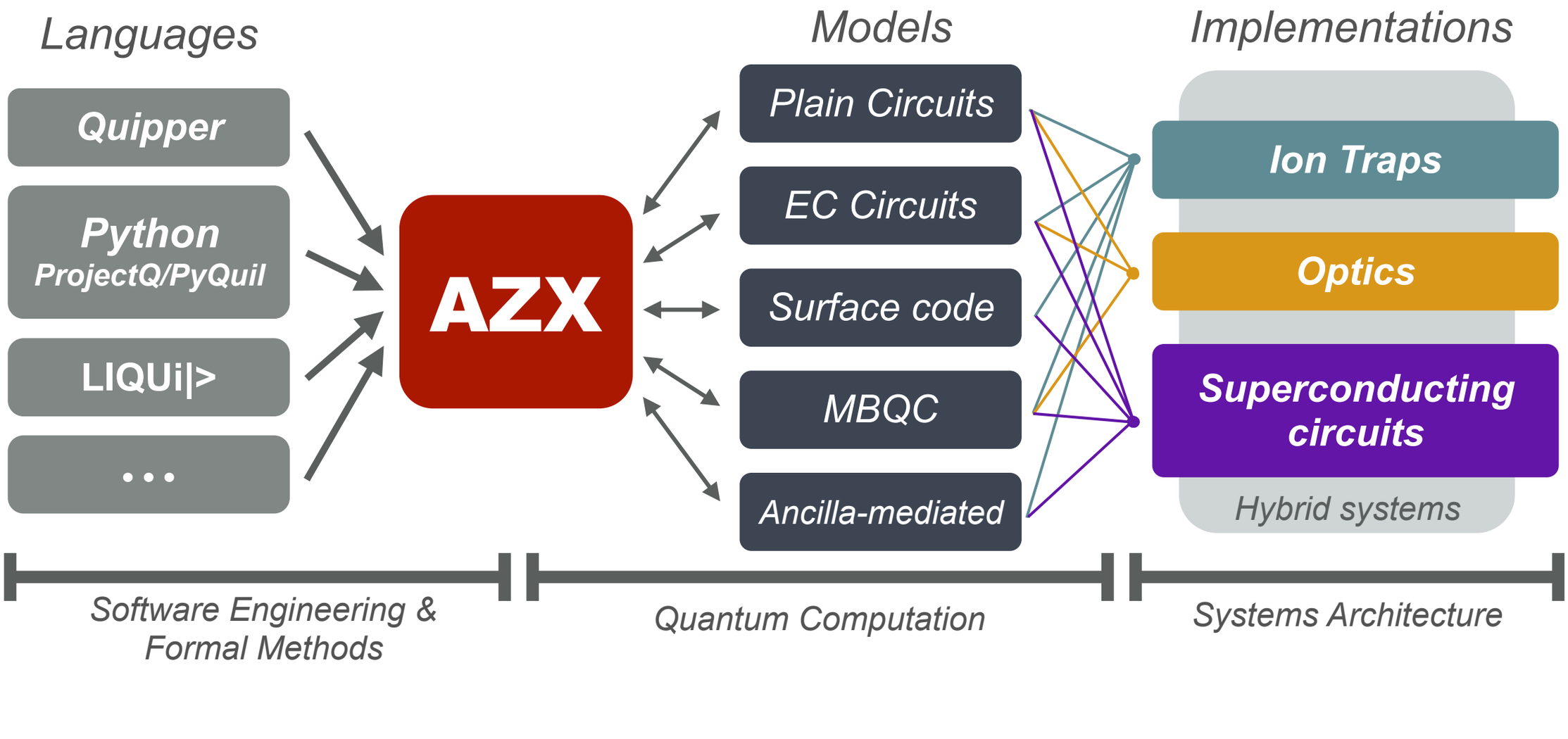
$$\lambda x.\lambda y.\lambda z.xz(yz)$$



Compilation

Intensional / Operational





The Next Step