Quantum Circuits and ZX-Calculus

Renaud Vilmart

Inria, LMF, Université Paris-Saclay

January 19th, 2021

Advantages allowed by quantum computing:

- algorithms (Shor, Grover, ...)
- cryptography
- simulation

Advantages allowed by quantum computing:

- algorithms (Shor, Grover, ...)
- cryptography
- simulation

Develop tools for :

- representing
- analysing/reasoning
- optimising
- verifying

quantum program/protocols.

- Classical bits as vectors: $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

- Arbitrary quantum bits (qubits): $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Arbitrary quantum bits (qubits): $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \xrightarrow{|\alpha|^2} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \xrightarrow[|\beta|^2]{} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ after measurement.

- Classical bits as vectors: $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$

- Arbitrary quantum bits (qubits): $$\begin{tikzcd} & \begin{pmatrix}1\\0\end{pmatrix} \\ \begin{pmatrix}\alpha\\\beta\end{pmatrix} \arrow[ur, "|\alpha|^2"] \arrow[dr, "|\beta|^2"'] & \\ & \begin{pmatrix}0\\1\end{pmatrix} \end{tikzcd}$$ after measurement.

- Larger systems: $q_0 \otimes q_1$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

- Arbitrary quantum bits (qubits): $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{array}{l} \xrightarrow{|\alpha|^2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \xrightarrow[|\beta|^2]{} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array}$ after measurement.

- Larger systems: $q_0 \otimes q_1$

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

- Arbitrary quantum bits (qubits): $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{array}{l} \xrightarrow{|\alpha|^2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \xrightarrow[|\beta|^2]{} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array}$ after measurement.

- Larger systems: $q_0 \otimes q_1$

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$$

- Entangled state cannot be broken down as $q_0 \otimes q_1$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$
- Arbitrary quantum bits (qubits): $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ $\xrightarrow{|\alpha|^2} \begin{pmatrix}1\\0\end{pmatrix}$, $\xrightarrow{|\beta|^2} \begin{pmatrix}0\\1\end{pmatrix}$ after measurement.
- Larger systems: $q_0 \otimes q_1$

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$$

- Entangled state cannot be broken down as $q_0 \otimes q_1$
- Isolated systems evolve unitarily: $|\psi_1\rangle = U|\psi_0\rangle$ with $U^\dagger U = id = UU^\dagger$

- $H := \frac{1}{\sqrt{2}} \begin{array}{cc} & \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{array}{c} |0\rangle \\ |1\rangle \end{array} & \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}$ is unitary

- $H := \frac{1}{\sqrt{2}} \begin{array}{cc} & \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{array}{c} |0\rangle \\ |1\rangle \end{array} & \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}$ is unitary
- $|+\rangle := H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle := H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ (($|0\rangle, |1\rangle$) and ($|+\rangle, |-\rangle$) are bases of $\mathbb{C}^2$)

- $H := \frac{1}{\sqrt{2}} \begin{array}{c c} & \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{array}{c} |0\rangle \\ |1\rangle \end{array} & \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}$ is unitary
- $|+\rangle := H\,|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle := H\,|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ $\quad$ ($(|0\rangle\,, |1\rangle)$ and $(|+\rangle\,, |-\rangle)$ are bases of $\mathbb{C}^2$)
- EPR: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is entangled

- $$H := \frac{1}{\sqrt{2}} \begin{array}{c c} & \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{array}{c} |0\rangle \\ |1\rangle \end{array} & \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}$$ is unitary

- $|+\rangle := H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle := H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ $\qquad$ $\big((|0\rangle, |1\rangle)$ and $(|+\rangle, |-\rangle)$ are bases of $\mathbb{C}^2\big)$

- EPR: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is entangled

- $$\mathrm{QFT}_2 \circ \overbrace{|0+\rangle}^{\substack{\text{state preparation} \\ =|0\rangle\otimes|+\rangle}} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \circ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2\sqrt{2}} \begin{array}{cc} \begin{pmatrix} 2 \\ 1+i \\ 0 \\ 1-i \end{pmatrix} & \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \end{array}$$

measurement $\rightarrow$ 50% $|00\rangle$, 25% $|01\rangle$, 25% $|11\rangle$

Unitarity $\Rightarrow$ reversibility

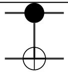
Unitarity $\Rightarrow$ reversibility

Quantum gates:

X or *Not*

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

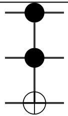
CX or *CNot*



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

$$= |a, b\rangle \mapsto |a, a \oplus b\rangle$$

Toffoli or *CCX* or *CCNot*



$$|a, b, c\rangle \mapsto |a, b, ab \oplus c\rangle$$

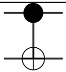
Unitarity $\Rightarrow$ reversibility

Quantum gates:

X or *Not*

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

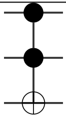
CX or *CNot*



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

$$= |a, b\rangle \mapsto |a, a \oplus b\rangle$$

Toffoli or *CCX* or *CCNot*

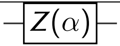


$$|a, b, c\rangle \mapsto |a, b, ab \oplus c\rangle$$

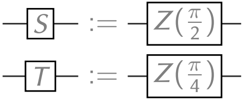
H

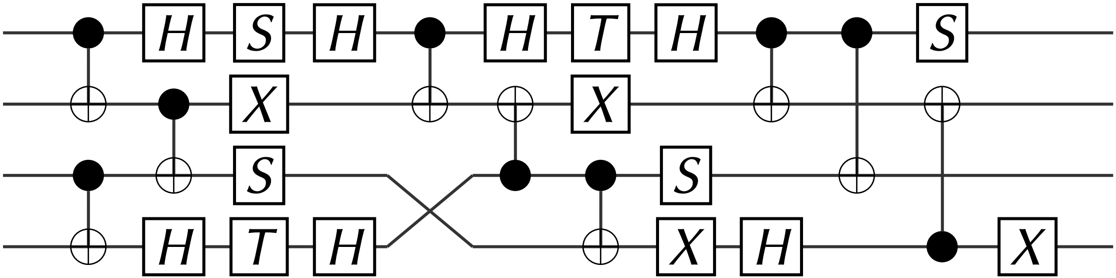
$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

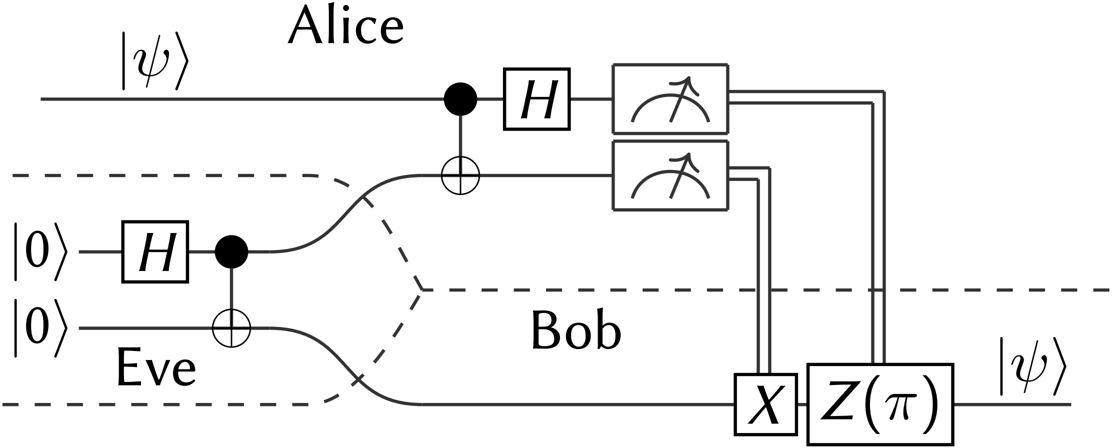
$Z(\alpha)$ or $R_Z(\alpha)$



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




H
S
H
H
T
H
S
X
X
S
S
H
T
H
X
H
X


Alice
$|\psi\rangle$
$|0\rangle$
$|0\rangle$
H
H
Eve
Bob
X
$Z(\pi)$
$|\psi\rangle$

Deferred Measurement Principle[1]

Any measurement can be ”pushed” to the very end of the procedure, without affecting the outcome.

[1] Nielsen, Chuang, *Quantum Computation and Quantum Information*

Deferred Measurement Principle[1]

Any measurement can be ”pushed” to the very end of the procedure, without affecting the outcome.

Usual scheme for quantum computing:

1. Initialise register of qubits
2. Apply unitary gates
3. Measure qubits

[1] Nielsen, Chuang, *Quantum Computation and Quantum Information*

Theorem : Universality[2]

The gate set $\{H, Z(\alpha), CX\}_{\alpha\in\mathbb{R}}$ is universal.

[2] [Barenco *et al.*'95]

[3] Gottesman-Knill theorem, [Gottesman'98]

[4] [Boykin, Mor, Pulver, Roychowdhury, Vatan' 00]

[5] Solovay-Kitaev theorem, [Kitaev'97]

Theorem : Universality[2]

The gate set $\{H, Z(\alpha), CX\}_{\alpha\in\mathbb{R}}$ is universal.

$Z(\alpha) \Rightarrow$ infinite (uncountable) family of gates

$\Rightarrow$ bad for analysis and implementability

[2] [Barenco *et al.*'95]

[3] Gottesman-Knill theorem, [Gottesman'98]

[4] [Boykin, Mor, Pulver, Roychowdhury, Vatan' 00]

[5] Solovay-Kitaev theorem, [Kitaev'97]

Theorem : Universality[2]

The gate set $\{H, Z(\alpha), CX\}_{\alpha\in\mathbb{R}}$ is universal.

$Z(\alpha)$ $\Rightarrow$ infinite (uncountable) family of gates
$\Rightarrow$ bad for analysis and implementability

- Clifford fragment : $\alpha \in \frac{\pi}{2}\mathbb{Z}$
  - not universal
  - efficiently simulable on a classical computer[3]

[2] [Barenco *et al.*'95]
[3] Gottesman-Knill theorem, [Gottesman'98]
[4] [Boykin, Mor, Pulver, Roychowdhury, Vatan' 00]
[5] Solovay-Kitaev theorem, [Kitaev'97]

Theorem : Universality[2]

The gate set $\{H, Z(\alpha), CX\}_{\alpha\in\mathbb{R}}$ is universal.

$Z(\alpha) \quad \Rightarrow \quad$ infinite (uncountable) family of gates

$\Rightarrow \quad$ bad for analysis and implementability

- Clifford fragment : $\alpha \in \frac{\pi}{2}\mathbb{Z}$
  - not universal
  - efficiently simulable on a classical computer[3]
- Clifford+T fragment : $\alpha \in \frac{\pi}{4}\mathbb{Z}$
  - approx. universal[4], with efficient approximation[5]

---

2 [Barenco *et al.*'95]

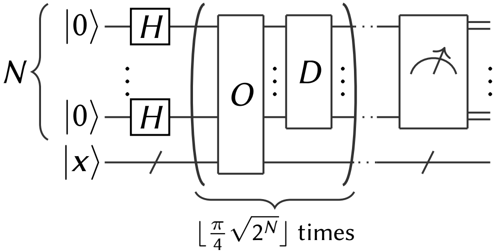
3 Gottesman-Knill theorem, [Gottesman'98]

4 [Boykin, Mor, Pulver, Roychowdhury, Vatan' 00]

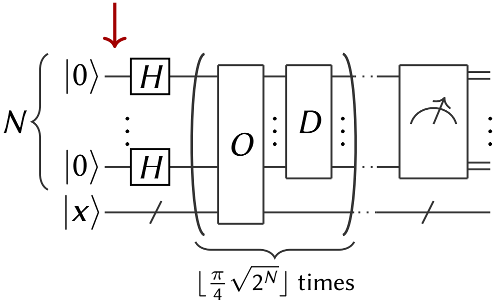
5 Solovay-Kitaev theorem, [Kitaev'97]

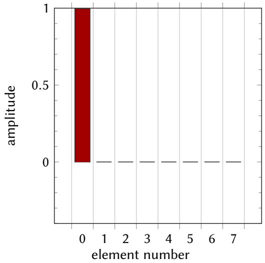
Pb: search of an element x in an unordered array of size 2^N

Pb: search of an element x in an unordered array of size 2^N

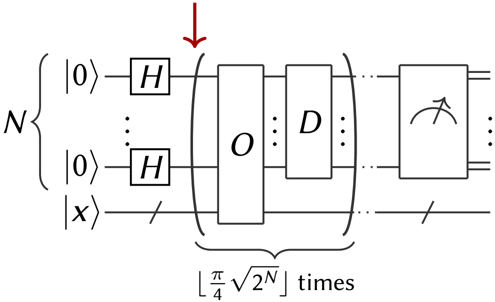


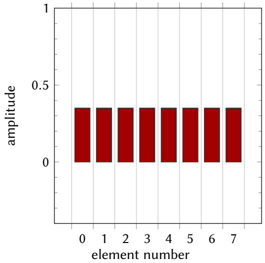
Pb: search of an element x in an unordered array of size 2^N



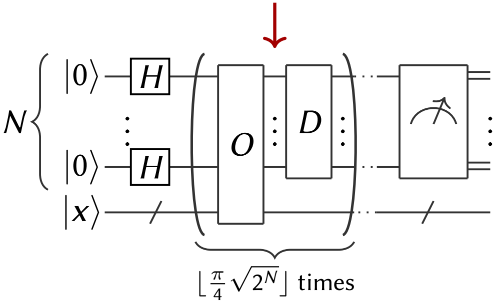


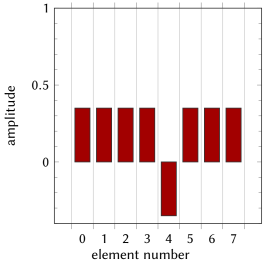
Pb: search of an element x in an unordered array of size 2^N



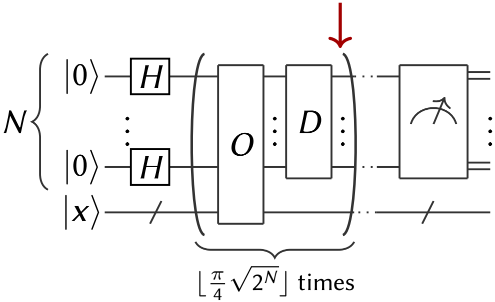


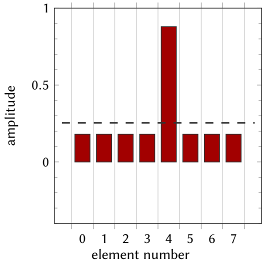
Pb: search of an element x in an unordered array of size 2^N



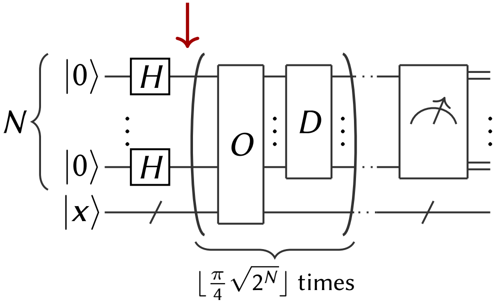


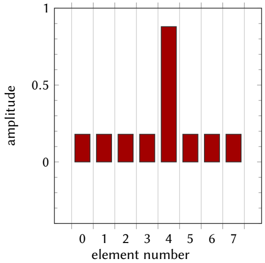
Pb: search of an element x in an unordered array of size 2^N



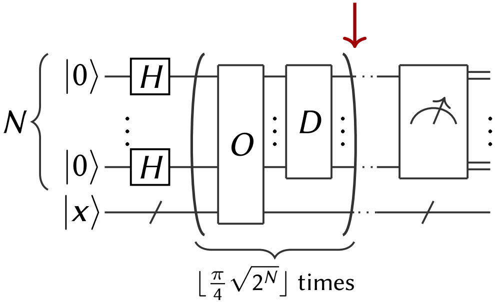


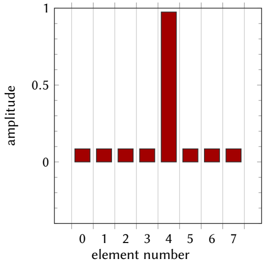
Pb: search of an element x in an unordered array of size 2^N



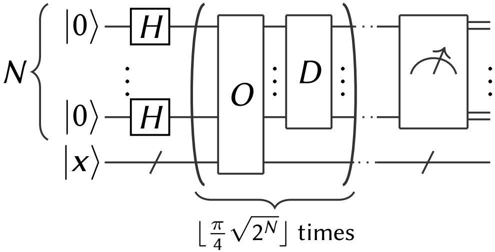


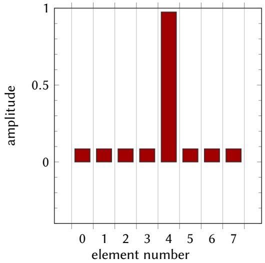
Pb: search of an element x in an unordered array of size 2^N





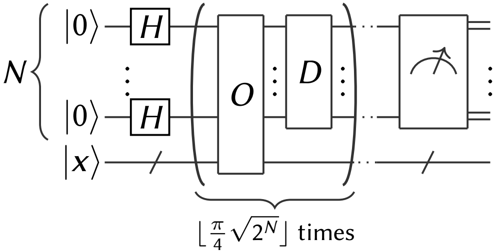
Pb: search of an element x in an unordered array of size 2^N

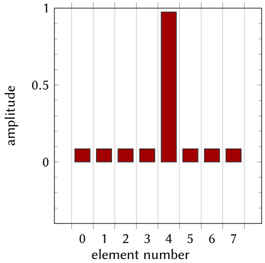




Classically check the result, and repeat if fail

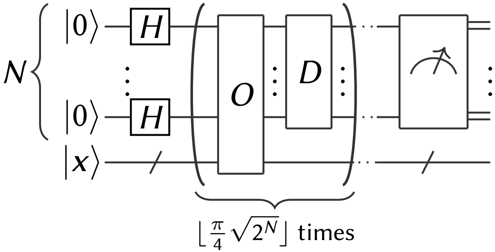
Pb: search of an element x in an unordered array of size 2^N

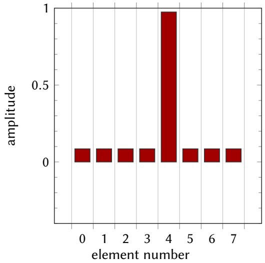




Classically check the result, and repeat if fail
$\Rightarrow$ Quantum part is only a subroutine

Pb: search of an element x in an unordered array of size 2^N





Classically check the result, and repeat if fail

$\Rightarrow$ Quantum part is only a subroutine

Algo in $O(\sqrt{2^N})$ vs. $O(2^N)$ classically

Problem of circuit equivalence

Do two given circuits implement the same operator?

Problem of circuit equivalence

Do two given circuits implement the same operator?

- Decidable: compute the matrices!

Problem of circuit equivalence

Do two given circuits implement the same operator?

- Decidable: compute the matrices!
- But hard: QMA-hard (quantum equivalent of NP-hard)

Problem of circuit equivalence

Do two given circuits implement the same operator?

- Decidable: compute the matrices!
- But hard: QMA-hard (quantum equivalent of NP-hard)
- Other (better?) idea: reason graphically

  $\Rightarrow$ equational theory (e.g. $-\boxed{H}-\boxed{H}- \;=\; \rule{2em}{0.4pt}$)

Problem of circuit equivalence

Do two given circuits implement the same operator?

- Decidable: compute the matrices!
- But hard: QMA-hard (quantum equivalent of NP-hard)
- Other (better?) idea: reason graphically

$\Rightarrow$ equational theory (e.g. $-\boxed{H}-\boxed{H}- \;=\; ——$)

New problem: Completeness

Do we have enough axioms in the equational theory?

Circuit Equivalence

Problem of circuit equivalence

Do two given circuits implement the same operator?

- Decidable: compute the matrices!
- But hard: QMA-hard (quantum equivalent of NP-hard)
- Other (better?) idea: reason graphically
  $\Rightarrow$ equational theory (e.g. $-\boxed{H}-\boxed{H}- \;=\; ——$)

New problem: Completeness

Do we have enough axioms in the equational theory?

- 1-qubit Clifford+T fragment [Backens'14]
- Clifford fragment [Selinger'15]
- $\{CNot, T\}$ [Amy,Chen,Ross'18]
- approx. universal fragment: open

Problem of circuit equivalence

Do two given circuits implement the same operator?

- Decidable: compute the matrices!
- But hard: QMA-hard (quantum equivalent of NP-hard)
- Other (better?) idea: reason graphically
  $\Rightarrow$ equational theory (e.g. $-\boxed{H}-\boxed{H}- \;=\; ——$)

New problem: Completeness

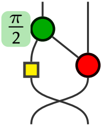
Do we have enough axioms in the equational theory?

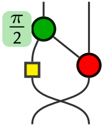
- 1-qubit Clifford+T fragment [Backens'14]
- Clifford fragment [Selinger'15]
- $\{CNot, T\}$ [Amy,Chen,Ross'18]
- approx. universal fragment: open

What if we dropped the unitarity constraint?

- Was introduced by Coecke and Duncan in 2008

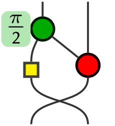
- Was introduced by Coecke and Duncan in 2008
- Is part of the Categorical Quantum Mechanics program (Abramsky&Coecke'04)

- Was introduced by Coecke and Duncan in 2008
- Is part of the Categorical Quantum Mechanics program (Abramsky&Coecke'04)
- Manipulates string diagrams e.g. 

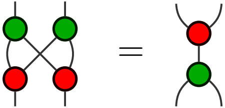
- Was introduced by Coecke and Duncan in 2008
- Is part of the Categorical Quantum Mechanics program (Abramsky&Coecke'04)
- Manipulates string diagrams e.g. 

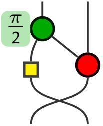
- Describes complementary Frobenius algebras

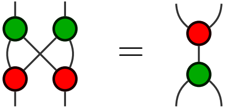
- Was introduced by Coecke and Duncan in 2008
- Is part of the Categorical Quantum Mechanics program (Abramsky&Coecke'04)
- Manipulates string diagrams e.g.



- Describes complementary Frobenius algebras
- Has a powerful equational theory e.g.

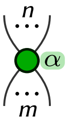


- Was introduced by Coecke and Duncan in 2008
- Is part of the Categorical Quantum Mechanics program (Abramsky&Coecke'04)
- Manipulates string diagrams e.g. 

- Describes complementary Frobenius algebras
- Has a powerful equational theory e.g. 

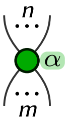
- Represents quantum circuits and more

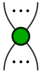
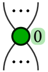
The Generators

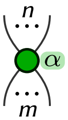
- A spider:  $::$

$$\begin{array}{cc} & \overbrace{\hphantom{1 \quad 0 \quad \cdots \quad \cdots \quad 0}}^{2^n} \\ 2^m \left\{ \vphantom{\begin{matrix}1\\0\\ \vdots\\0\\0\end{matrix}} \right. & \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix} \end{array}$$

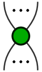
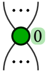
$= |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$

- A spider:  $::$ $$\begin{array}{cc} & \overbrace{\hphantom{\begin{matrix}1 & 0 & \cdots\cdots & 0\end{matrix}}}^{2^n} \\ 2^m\left\{\vphantom{\begin{matrix}1\\0\\ \vdots\\ \vdots \\ 0\end{matrix}}\right. & \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix} \end{array}$$ $$= |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$$

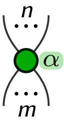
 $:=$ 

- A spider: 

$:: \; 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right.$
$= |0^m\rangle\langle 0^n| + e^{i\alpha} |1^m\rangle\langle 1^n|$

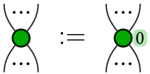
 $:=$ 

- A change of basis:  $:: \; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

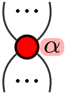
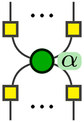
- A spider: 

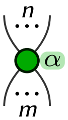
$$:: \; 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha}\end{pmatrix}}^{2^n} \right.$$

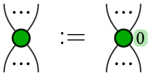
$$= |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$$



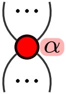
- A change of basis:  $:: \; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

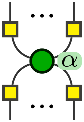
- Another spider:  $:=$  $:: \; |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$

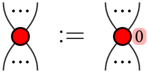
- A spider: 

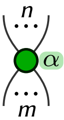
$$:: \; 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha}\end{pmatrix}}^{2^n} \right.$$
$$= |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$$


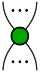
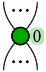
- A change of basis:  $:: \; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- Another spider: 

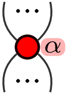
$:=$ 

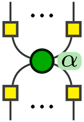
$:: \; |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$


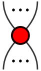
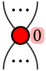
- A spider: 

$$:: \quad 2^m\left\{\overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n}\right. \qquad = |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$$
 $:=$ 

- A change of basis:  $:: \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- Another spider: 

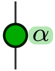
$:=$ 

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

- Wires: $:: \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,  $:: \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,  $:: \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$,  $:: \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}$

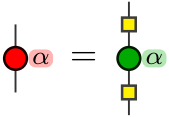
One-qubit Operators

$Z(\alpha)$:
rotation around Z



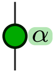
Hadamard:

$X(\alpha)$:
$= HZ(\alpha)H$



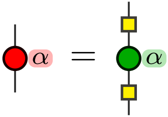
One-qubit Operators

$Z(\alpha)$:
rotation around Z



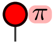
Hadamard: 

$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

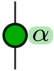
$\sqrt{2}\,|0\rangle$: 

$\sqrt{2}\,|1\rangle$: 

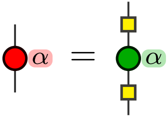
$|00\rangle + |11\rangle$: 

$\langle 00| + \langle 11|$: 

One-qubit Operators

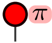
$Z(\alpha)$:
rotation around Z 

Hadamard: 

$X(\alpha)$:
$= HZ(\alpha)H$ 

States and Projectors

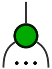
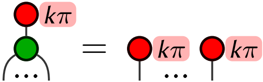
$\sqrt{2}\,|0\rangle$: 

$\sqrt{2}\,|1\rangle$: 

$|00\rangle + |11\rangle$: 

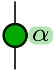
$\langle 00| + \langle 11|$: 

Green Spider

Copy:  s.t. 

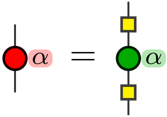
One-qubit Operators

$Z(\alpha)$:
rotation around Z



Hadamard:

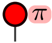
$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

$\sqrt{2}\,|0\rangle$:

$\sqrt{2}\,|1\rangle$:

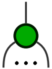


$|00\rangle + |11\rangle$:

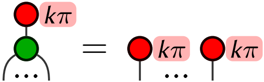
$\langle 00| + \langle 11|$:

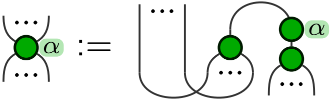
Green Spider

Copy:



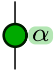
s.t.





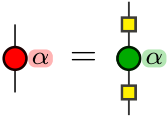
One-qubit Operators

$Z(\alpha)$:
rotation around Z



Hadamard:

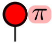
$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

$\sqrt{2}\,|0\rangle$:

$\sqrt{2}\,|1\rangle$:

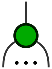


$|00\rangle + |11\rangle$:

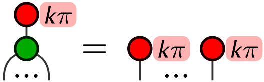
$\langle 00| + \langle 11|$:

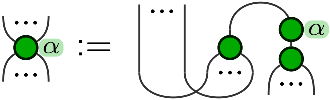
Green Spider

Copy:



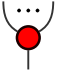
s.t.



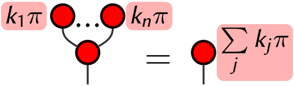


Red Spider

XOR:

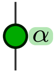


s.t.



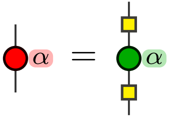
One-qubit Operators

$Z(\alpha)$:
rotation around Z



Hadamard:

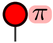
$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

$\sqrt{2}\,|0\rangle$:

$\sqrt{2}\,|1\rangle$:

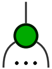


$|00\rangle + |11\rangle$:

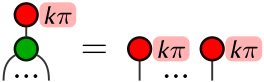
$\langle 00| + \langle 11|$:

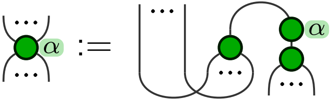
Green Spider

Copy:



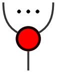
s.t.



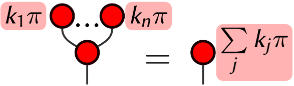


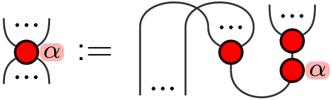
Red Spider

XOR:



s.t.



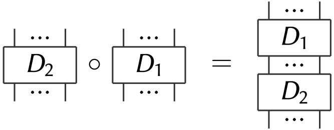


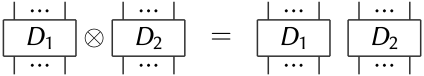
Generators

ZX-Calculus [Coecke,Duncan'08] in Short

Generators

Compositions





Generators

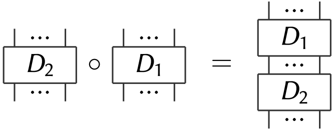
Compositions

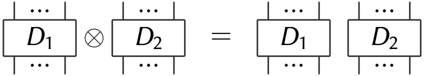
Standard Interpretation

$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

Generators

Compositions

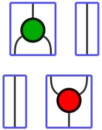




Standard Interpretation

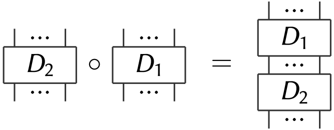
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

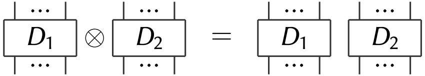
Example



Generators

Compositions

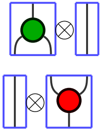




Standard Interpretation

$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

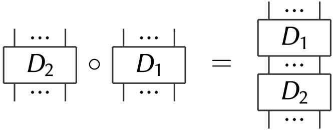
Example

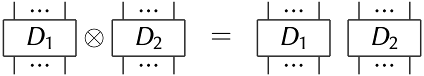


ZX-Calculus [Coecke,Duncan'08] in Short

Generators

Compositions

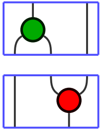




Standard Interpretation

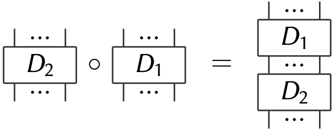
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

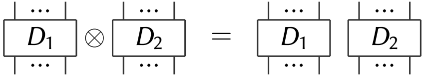
Example



Generators

Compositions

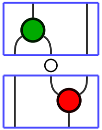




Standard Interpretation

$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

Example



ZX-Calculus [Coecke,Duncan'08] in Short

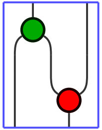
Generators

Compositions

Standard Interpretation

$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

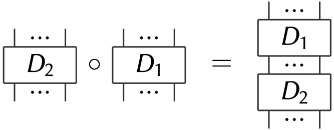
Example

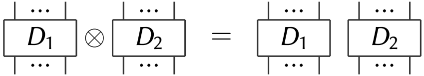


ZX-Calculus [Coecke,Duncan'08] in Short

Generators

Compositions

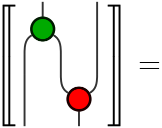




Standard Interpretation

$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

Example



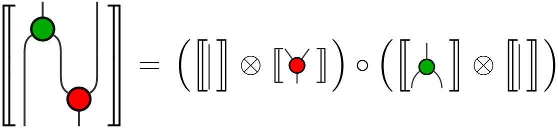
Generators

Compositions

Standard Interpretation

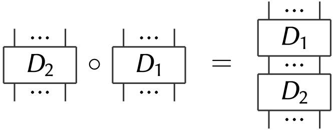
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

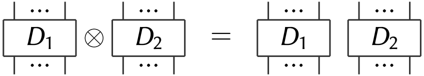
Example



Generators

Compositions

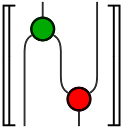




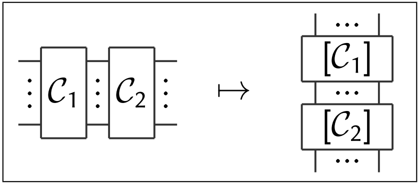
Standard Interpretation

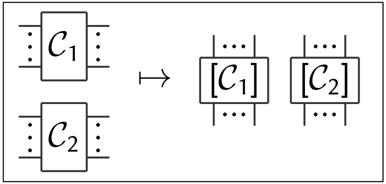
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

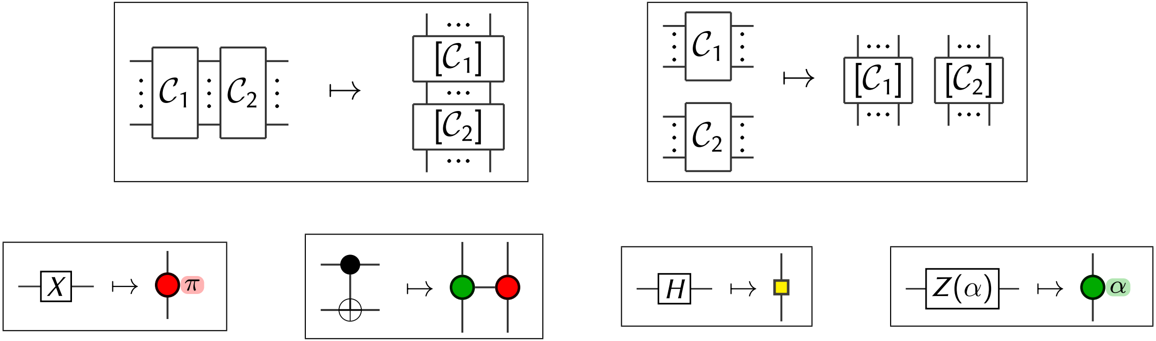
Example

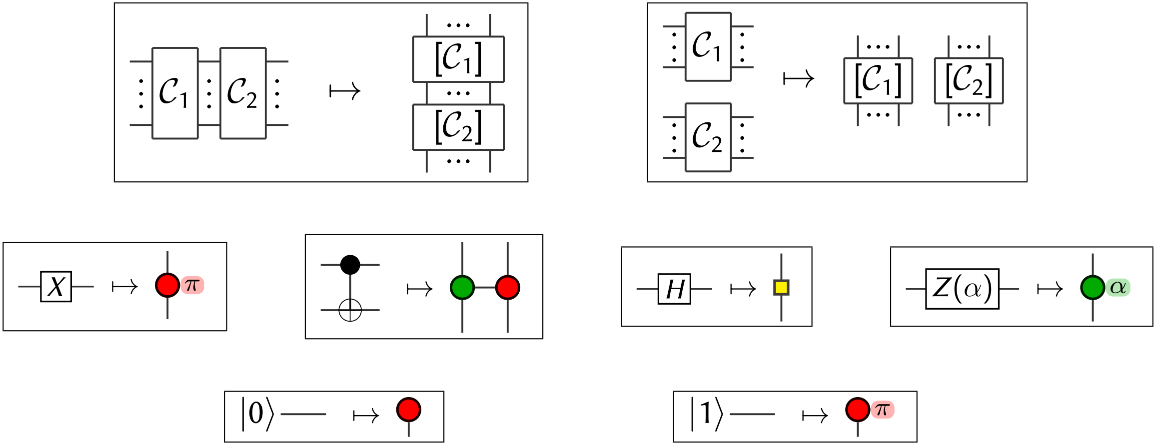


$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$


$\mathcal{C}_1$
$\mathcal{C}_2$
$\mapsto$
$[\mathcal{C}_1]$
$[\mathcal{C}_2]$


$\mathcal{C}_1$
$\mathcal{C}_2$
$\mapsto$
$[\mathcal{C}_1]$
$[\mathcal{C}_2]$


$\mathcal{C}_1$
$\mathcal{C}_2$
$\mapsto$
$[\mathcal{C}_1]$
$[\mathcal{C}_2]$
$\mathcal{C}_1$
$\mathcal{C}_2$
$\mapsto$
$[\mathcal{C}_1]$
$[\mathcal{C}_2]$
X
$\mapsto$
π
$\mapsto$
H
$\mapsto$
$Z(\alpha)$
$\mapsto$
α


C1
C2
[C1]
[C2]
X
π
H
Z(α)
α
|0⟩
|1⟩

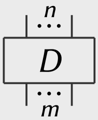
Theorem (Universality)

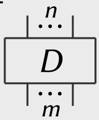
We can represent any quantum operator using ZX-diagrams:

$$\forall f : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m},\ \exists \underset{m}{\overset{n}{\boxed{D}}} \in \mathbf{ZX},\ \left\llbracket \underset{m}{\overset{n}{\boxed{D}}} \right\rrbracket = f$$

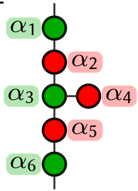
Theorem (Universality)

We can represent any quantum operator using ZX-diagrams:

$\forall f : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m},\ \exists$ 

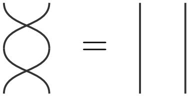
$\in \mathbf{ZX},\ \llbracket$ 

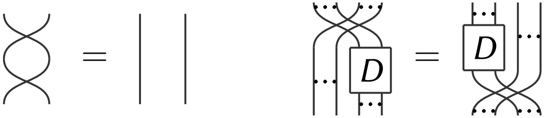
$\rrbracket = f$

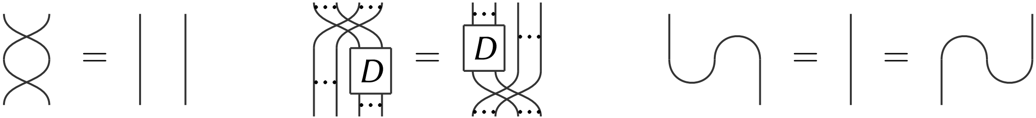
E.g. if $f : \mathbb{C}^2 \to \mathbb{C}^2,\ \exists \alpha_i,\ \llbracket$ 

$\rrbracket = f$

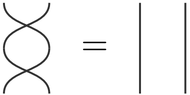
Equational Theory (the Backbone)

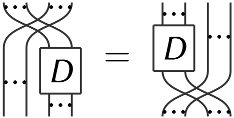


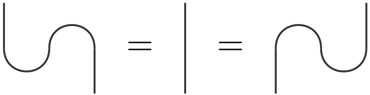

D
D

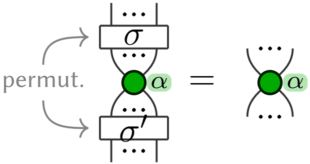

D
D

Equational Theory (the Backbone)

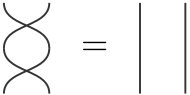


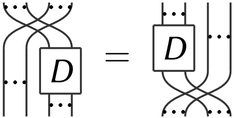


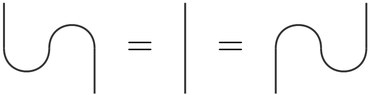


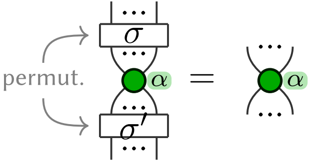


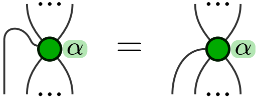
Equational Theory (the Backbone)



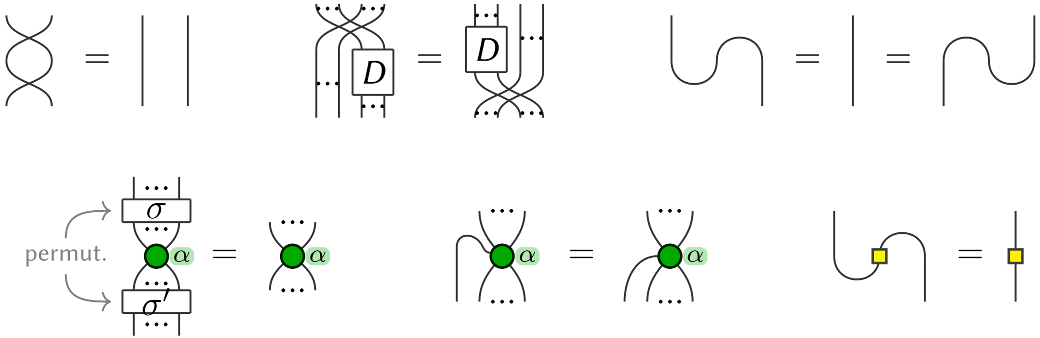




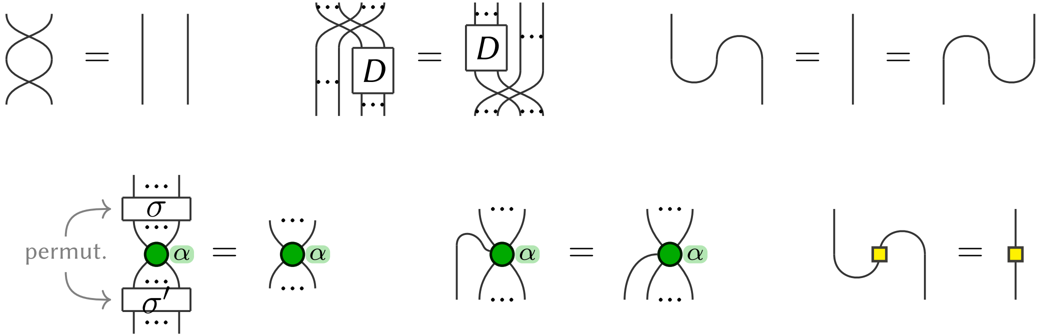




Equational Theory (the Backbone)

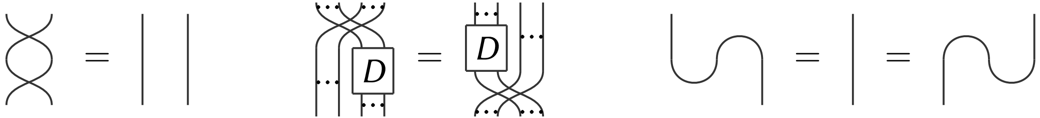


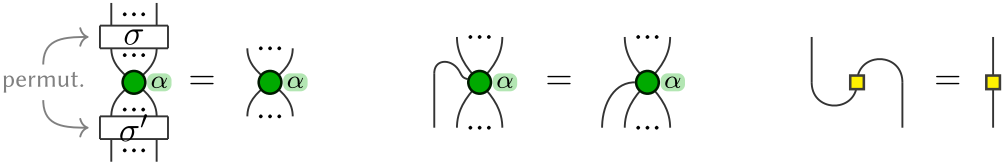
Equational Theory (the Backbone)



Only Connectivity Matters

ZX-diagrams can be seen as open graphs. Any graph isomorphism is a valid derivation in the equational theories.

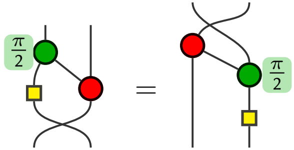




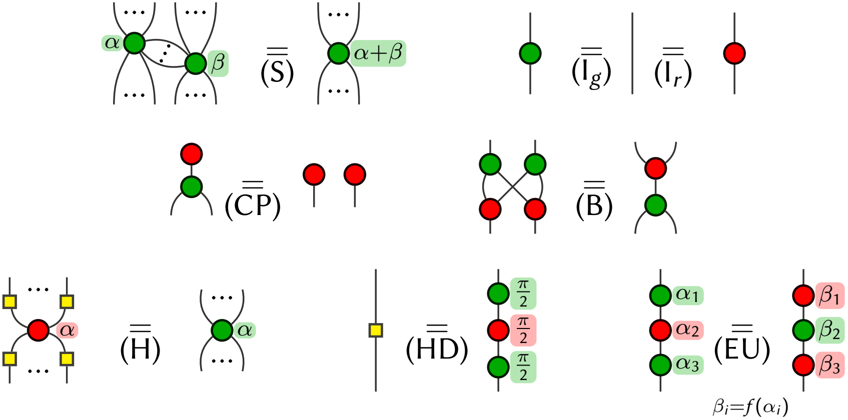
Only Connectivity Matters

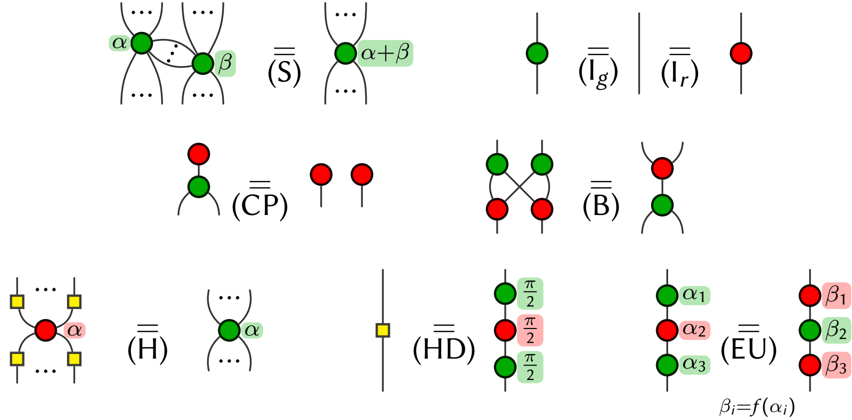
ZX-diagrams can be seen as open graphs. Any graph isomorphism is a valid derivation in the equational theories.

E.g.

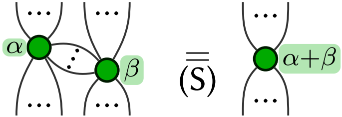


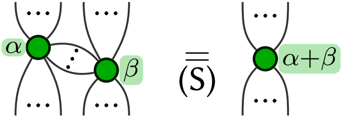
Equational Theory



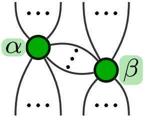


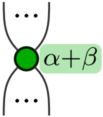
We write ZX $\vdash D_1 = D_2$. Every colour-swapped rule holds.


α
β
(S)
α+β



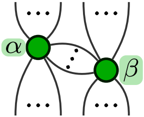
: comes from the study of †-Frobenius algebras in $\mathbb{C}^2$.

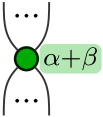


$\underset{(\mathrm{S})}{=}$


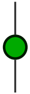
: comes from the study of †-Frobenius algebras in $\mathbb{C}^2$.


$\underset{(\mathrm{I}_g)}{=}$ | $\underset{(\mathrm{I}_r)}{=}$

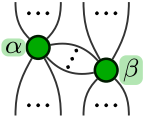



$\underset{(S)}{=}$


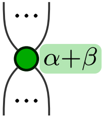
: comes from the study of †-Frobenius algebras in $\mathbb{C}^2$.

rotation of angle 0 $\rightarrow$  $\underset{(I_g)}{=}$ $\underset{(I_r)}{=}$  $\leftarrow$ rotation of angle 0

Understanding the Rules: the Spiders

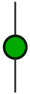


$\overset{(\mathrm{S})}{=}$



: comes from the study of †-Frobenius algebras in $\mathbb{C}^2$.

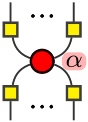
rotation of angle 0 $\rightarrow$



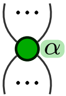
$\overset{(\mathrm{I}_g)}{=}$

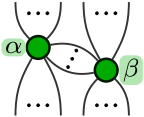
$\overset{(\mathrm{I}_r)}{=}$

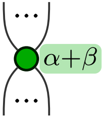
$\leftarrow$ rotation of angle 0



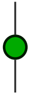
$\overset{(\mathrm{H})}{=}$



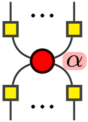


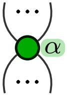
$\overset{(\mathrm{S})}{=}$


: comes from the study of †-Frobenius algebras in $\mathbb{C}^2$.

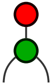
rotation of angle 0 $\to$

$\overset{(\mathrm{I}_g)}{=}$ | $\overset{(\mathrm{I}_r)}{=}$

$\leftarrow$ rotation of angle 0

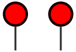


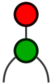
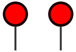
$\overset{(\mathrm{H})}{=}$


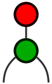
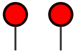
: change of basis

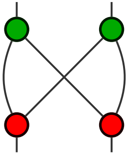
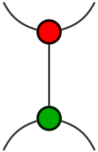


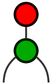
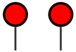
$\overset{(CP)}{=}$

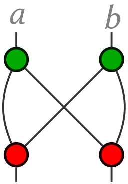


 $\overset{}{\underset{\text{(CP)}}{=}}$  : copy of classical 0.

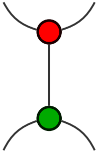
 $\overset{=}{\text{(CP)}}$  : copy of classical 0.

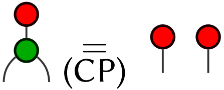
 $\overset{=}{\text{(B)}}$ 

 $\underset{(CP)}{=}$  : copy of classical 0.

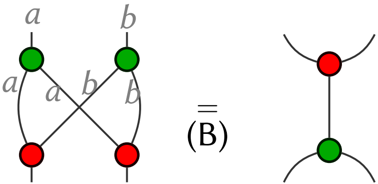


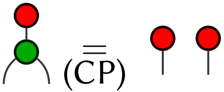
$\underset{(B)}{=}$



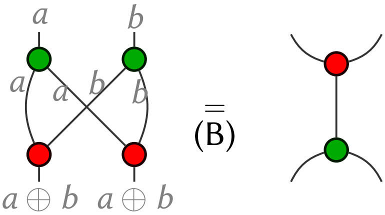


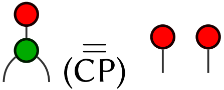
: copy of classical 0.



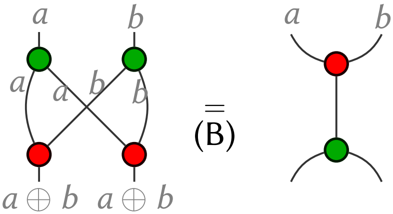


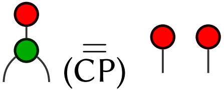
: copy of classical 0.



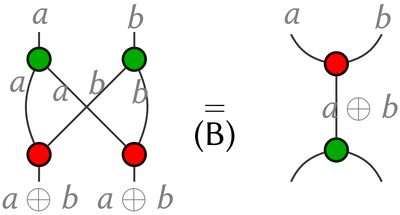


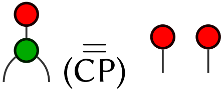
: copy of classical 0.



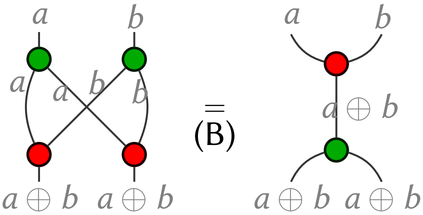


: copy of classical 0.





: copy of classical 0.

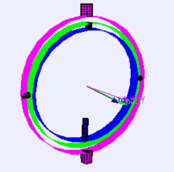


Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$

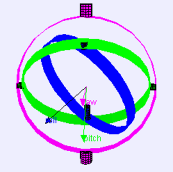
Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$



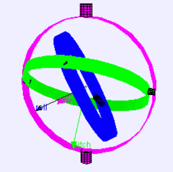
Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$



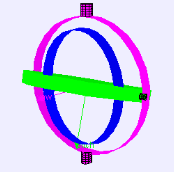
Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$



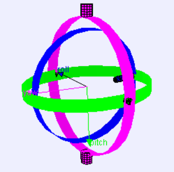
Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$



Rotations in $\mathbb{R}^3$:

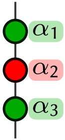
$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$



Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$

Also true for $U(2)$ i.e. any 1-qubit unitary can be decomposed as:

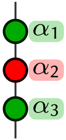


Understanding the Rules: Euler Angles

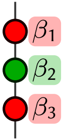
Rotations in $\mathbb{R}^3$:

$$\forall \theta,\ \exists \alpha_i,\quad R_?(\theta) = R_x(\alpha_3) \circ R_y(\alpha_2) \circ R_x(\alpha_1)$$

Also true for $U(2)$ i.e. any 1-qubit unitary can be decomposed as:



or

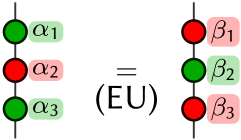


Understanding the Rules: Euler Angles

Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$

Also true for $U(2)$ i.e. any 1-qubit unitary can be decomposed as:

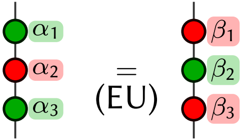


with $\beta_i = f(\alpha_i)$

Rotations in $\mathbb{R}^3$:

$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$

Also true for $U(2)$ i.e. any 1-qubit unitary can be decomposed as:



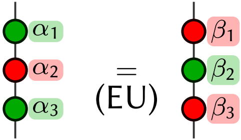
with $\beta_i = f(\alpha_i)$

 represents a 1-qubit unitary:

Rotations in $\mathbb{R}^3$:

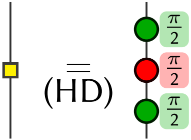
$$\forall\theta,\ \exists\alpha_i,\quad R_?(\theta) = R_x(\alpha_3)\circ R_y(\alpha_2)\circ R_x(\alpha_1)$$

Also true for $U(2)$ i.e. any 1-qubit unitary can be decomposed as:

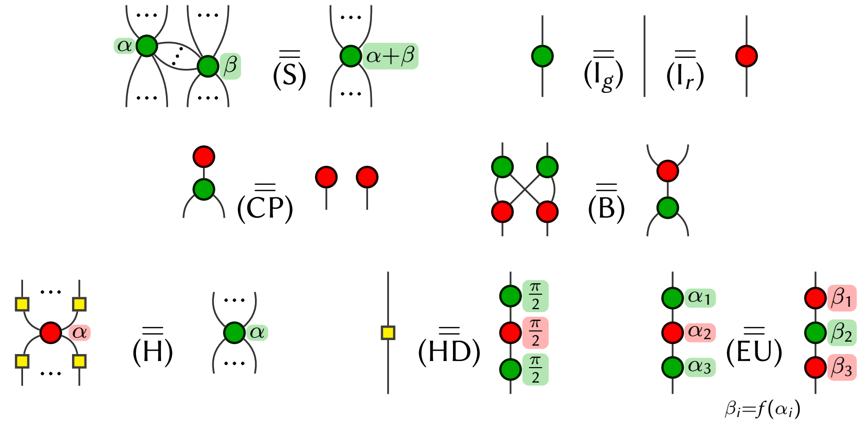


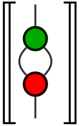
with $\beta_i = f(\alpha_i)$

represents a 1-qubit unitary:

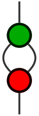
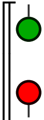


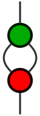
Equational Theory

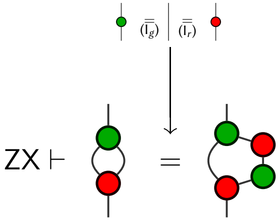




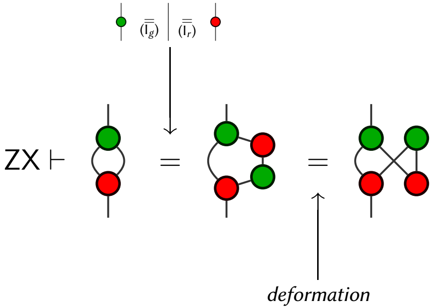
$$= \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$\llbracket$  $\rrbracket = \begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix} = \begin{pmatrix}1\\ 0\end{pmatrix} \circ \begin{pmatrix}1 & 1\end{pmatrix} = \llbracket$  $\rrbracket$

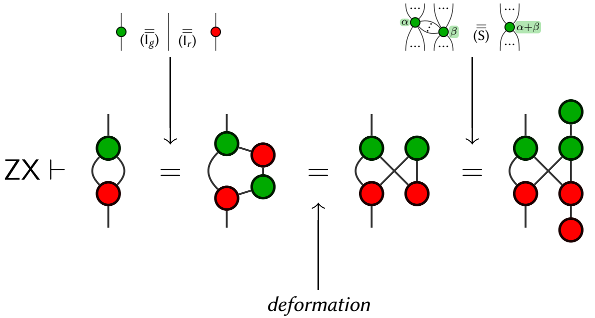
ZX ⊢ 

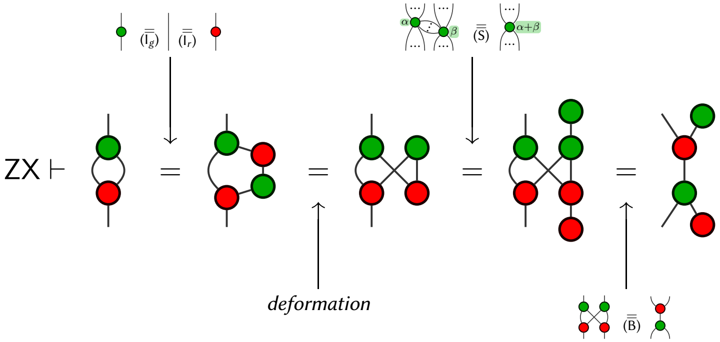

ZX ⊢
$(\overline{\overline{\mathrm{I}}}_g)$
$(\overline{\overline{\mathrm{I}}}_r)$
=

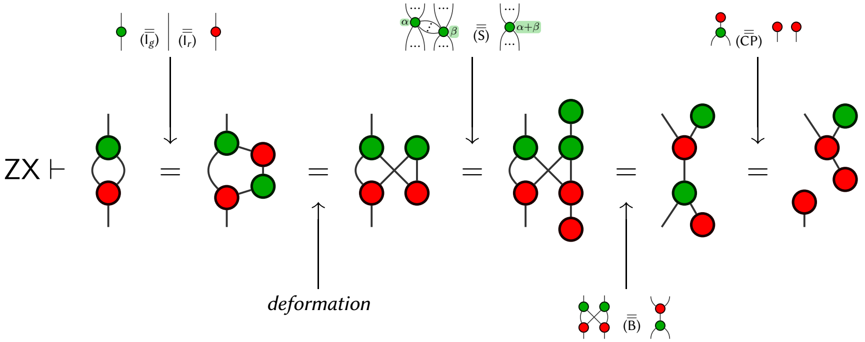
Using the Rules: the Hopf Law



Using the Rules: the Hopf Law

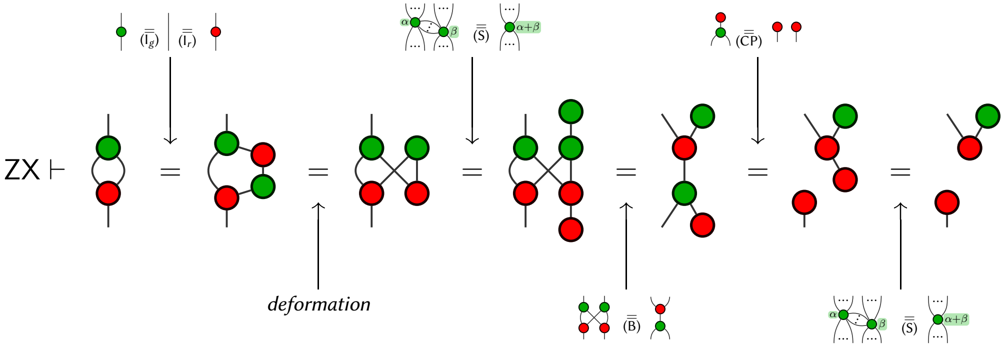


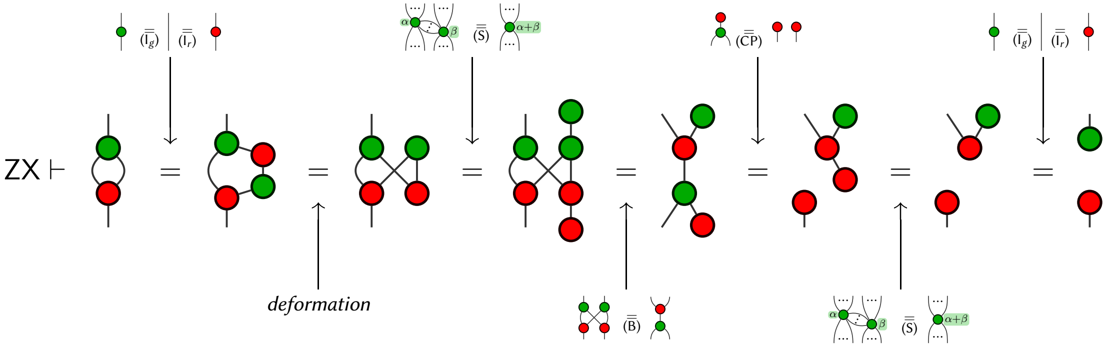

ZX ⊢
=
=
=
=
$(\overline{\overline{\mathrm{I}_g}})$
$(\overline{\overline{\mathrm{I}_r}})$
α
β
$(\overline{\overline{\mathrm{S}}})$
$\alpha+\beta$
deformation
$(\overline{\overline{\mathrm{B}}})$



ZX ⊢
$(\overline{\overline{\mathrm{I}_g}})$
$(\overline{\overline{\mathrm{I}_r}})$
α
β
$(\overline{\overline{\mathrm{S}}})$
$\alpha+\beta$
$(\overline{\overline{\mathrm{CP}}})$
deformation
$(\overline{\overline{\mathrm{B}}})$

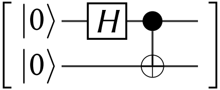
Using the Rules: the Hopf Law




ZX ⊢
$\overset{=}{(\mathrm{I}_g)}$
$\overset{=}{(\mathrm{I}_r)}$
deformation
α
β
$\overset{=}{(\mathrm{S})}$
$\alpha+\beta$
$\overset{=}{(\mathrm{B})}$
$\overset{=}{(\mathrm{CP})}$
$\overset{=}{(\mathrm{S})}$
$\overset{=}{(\mathrm{I}_g)}$
$\overset{=}{(\mathrm{I}_r)}$

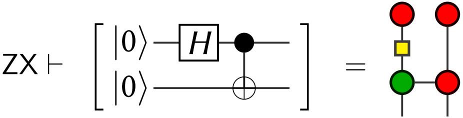
The EPR state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$

ZX $\vdash$

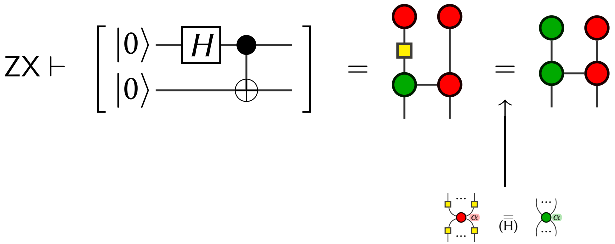


Using the Rules: The EPR Pair

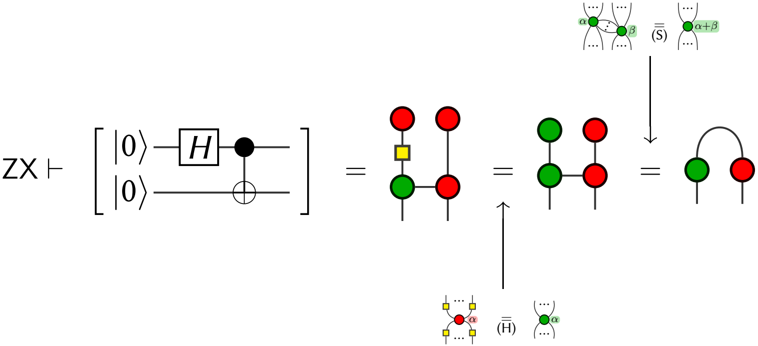
The EPR state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$



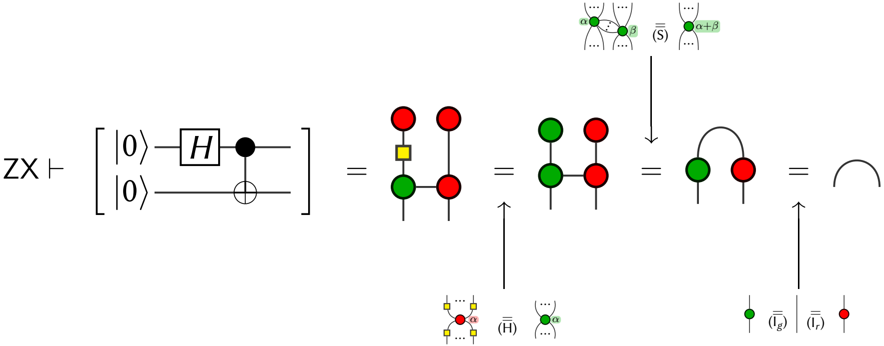
The EPR state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$



The EPR state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$



The EPR state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$



Theorem [V.'19]

The language is *complete*:

$$\forall D_1, D_2 \in \mathbf{ZX},\ [\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZX} \vdash D_1 = D_2$$

Theorem [V.'19]

The language is *complete*:

$$\forall D_1, D_2 \in \mathbf{ZX},\ [\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZX} \vdash D_1 = D_2$$

Previous/other completeness results:

- $\frac{\pi}{2}$-fragment [Backens'14]
- π-fragment [Duncan,Perdrix'14]
- 1-qubit $\frac{\pi}{4}$-fragment [Backens'14]
- $\frac{\pi}{4}$-fragment [Jeandel,Perdrix,V.'18]
- full ZX (modified) [Hadzihasanovic,Ng,Wang'18]
- full ZX [Jeandel,Perdrix,V.'18]

- Main idea: notion of controlled state:

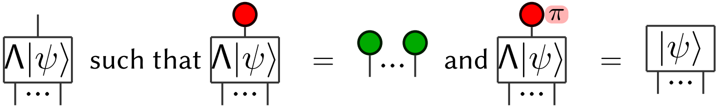
- Main idea: notion of controlled state:

$$\Lambda|\psi\rangle := \sqrt{2}^n\,|+^n\rangle\langle 0| + |\psi\rangle\langle 1| = \begin{pmatrix} 1 & \psi_0 \\ \vdots & \vdots \\ 1 & \psi_{2^n-1} \end{pmatrix} \text{ i.e.:}$$

Sketch of (a) proof: Normal Forms

- Main idea: notion of controlled state:

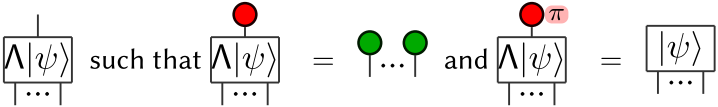
$$\Lambda|\psi\rangle := \sqrt{2}^n \, |+^n\rangle\langle 0| + |\psi\rangle\langle 1| = \begin{pmatrix} 1 & \psi_0 \\ \vdots & \vdots \\ 1 & \psi_{2^n-1} \end{pmatrix} \text{ i.e.:}$$



Sketch of (a) proof: Normal Forms

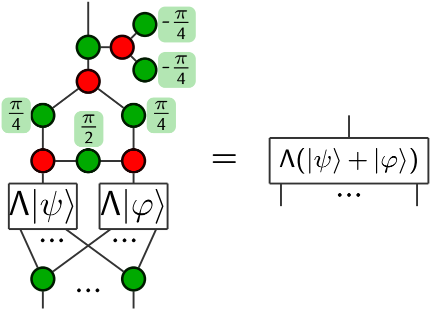
- Main idea: notion of controlled state:

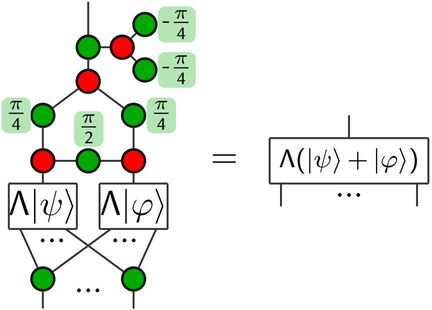
$$\Lambda|\psi\rangle := \sqrt{2}^n \,|+^n\rangle\langle 0| + |\psi\rangle\langle 1| = \begin{pmatrix} 1 & \psi_0 \\ \vdots & \vdots \\ 1 & \psi_{2^n-1} \end{pmatrix} \text{ i.e.:}$$

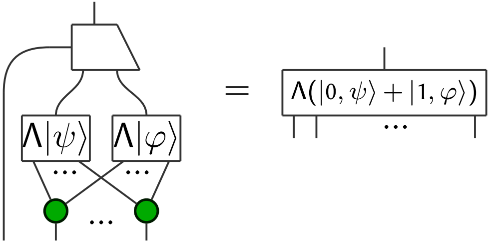


- Base case: controlled scalar:

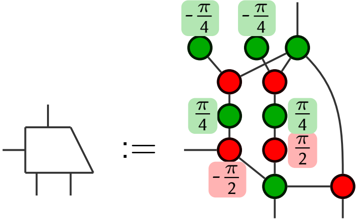
$$\Lambda x = \langle 0| + x\,\langle 1| = \begin{pmatrix} 1 & x \end{pmatrix}$$

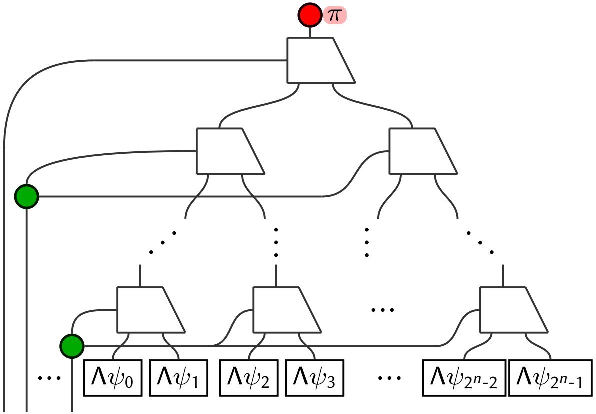

$-\frac{\pi}{4}$
$-\frac{\pi}{4}$
$\frac{\pi}{4}$
$\frac{\pi}{2}$
$\frac{\pi}{4}$
$\Lambda|\psi\rangle$
$\Lambda|\varphi\rangle$
$=$
$\Lambda(|\psi\rangle + |\varphi\rangle)$





with





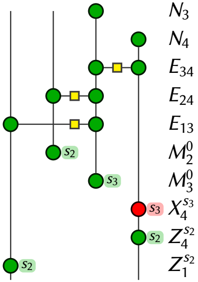
- Generators can be put in NF
- Compositions of states in NF can be put in NF
- Completeness on controlled scalars

$\Downarrow$

Completeness!

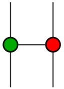
Plan

Unification



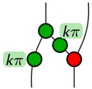
measure-ment calculus

$=$



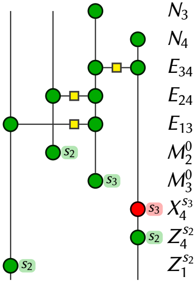
quantum circuit

$=$

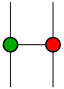


lattice surgery (surface codes)

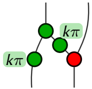
Unification



measure-ment calculus

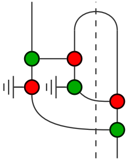
$=$ 

quantum circuit

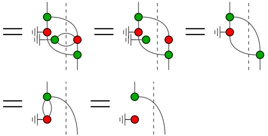
$=$ 

lattice surgery (surface codes)

Verification



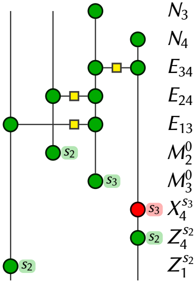
protocol



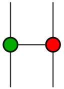
$=$ 

spec.

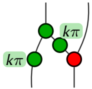
Unification



measure-ment calculus

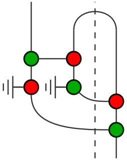
$=$ 

quantum circuit

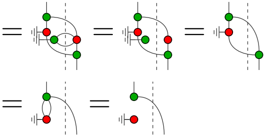
$=$ 

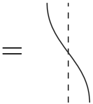
lattice surgery (surface codes)

Verification



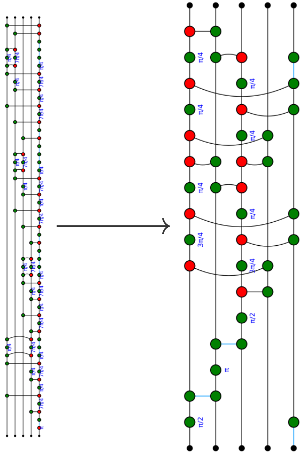
protocol



$=$ 

spec.

Optimisation



- Graphical language

- Graphical language
  - visualises information flow

- Graphical language
  - visualises information flow
  - laxer than circuits

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory
- Universal

Conclusion

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory
- Universal
- Several completeness results

Conclusion

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory
- Universal
- Several completeness results
- Cousin languages ZW and ZH

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory
- Universal
- Several completeness results
- Cousin languages ZW and ZH
- Unifies different models of quantum computation

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory
- Universal
- Several completeness results
- Cousin languages ZW and ZH
- Unifies different models of quantum computation
  - Gaining traction as the default language for describing quantum processes

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory
- Universal
- Several completeness results
- Cousin languages ZW and ZH
- Unifies different models of quantum computation
  - Gaining traction as the default language for describing quantum processes
- Used for optimisation (PyZX)

- Graphical language
  - visualises information flow
  - laxer than circuits
  - powerful & intuitive equational theory
- Universal
- Several completeness results
- Cousin languages ZW and ZH
- Unifies different models of quantum computation
  - Gaining traction as the default language for describing quantum processes
- Used for optimisation (PyZX)
- Used for verification (Quantomatic)