How to Verify Quantum Processes

Renaud Vilmart

Inria, LMF, Université Paris-Saclay

MOVEP 2022, Aalborg

Plan

- Electronics as the standard support for computers

- Electronics as the standard support for computers

- 1980-1982, Benioff: interaction between computation and quantum mechanics

A Brief History of Quantum Computing

- Electronics as the standard support for computers
- 1980-1982, Benioff: interaction between computation and quantum mechanics
- 1982, Feynman: proposed to use a quantum computer to simulate quantum interactions

- Electronics as the standard support for computers
- 1980-1982, Benioff: interaction between computation and quantum mechanics
- 1982, Feynman: proposed to use a quantum computer to simulate quantum interactions
- 1984, Bennett,Brassard: first quantum cryptography protocol

- Electronics as the standard support for computers
- 1980-1982, Benioff: interaction between computation and quantum mechanics
- 1982, Feynman: proposed to use a quantum computer to simulate quantum interactions
- 1984, Bennett,Brassard: first quantum cryptography protocol
- 1994, Shor: quantum algorithm for prime factorisation ($O(\log^3(n))$)

- 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 bit (qubit):

$$\alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$
- Arbitrary quantum bit (qubit):

$$\alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} \begin{array}{l} \xrightarrow{|\alpha|^2} \begin{pmatrix}1\\0\end{pmatrix} \\ \xrightarrow[|\beta|^2]{} \begin{pmatrix}0\\1\end{pmatrix} \end{array}$$

after (if) measurement.

- Classical bits as vectors: $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Arbitrary quantum bit (qubit):

$$\alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{array}{l} \xrightarrow{|\alpha|^2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \xrightarrow[|\beta|^2]{} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array} \text{ after (if) measurement.}$$

- Isolated systems evolve unitarily: $|\psi_1\rangle = U\,|\psi_0\rangle$ with $\quad U^\dagger U = id = UU^\dagger$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$
- Arbitrary quantum bit (qubit):

$$\alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} \begin{array}{l} \xrightarrow{|\alpha|^2} \begin{pmatrix}1\\0\end{pmatrix} \\ \xrightarrow[|\beta|^2]{} \begin{pmatrix}0\\1\end{pmatrix}\end{array}$$ after (if) measurement.

- Isolated systems evolve unitarily: $|\psi_1\rangle = U|\psi_0\rangle$ with $\overset{U^\dagger = \overline{U}^\intercal}{\overset{\downarrow}{U^\dagger}} U = id = UU^\dagger$

- Classical bits as vectors: $|0\rangle := \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle := \begin{pmatrix}0\\1\end{pmatrix}$
- Arbitrary quantum bit (qubit):

$$\alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \begin{array}{l} \xrightarrow{|\alpha|^2} \begin{pmatrix}1\\0\end{pmatrix} \\[1em] \xrightarrow[|\beta|^2]{} \begin{pmatrix}0\\1\end{pmatrix} \end{array}$$

after (if) measurement.

- Isolated systems evolve unitarily: $|\psi_1\rangle = U\,|\psi_0\rangle$ with $\overset{U^\dagger = \overline{U}^\intercal}{\overset{\downarrow}{U^\dagger}}\,U = id = UU^\dagger$

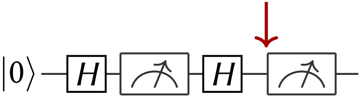
E.g. $H := \frac{1}{\sqrt{2}} \begin{array}{cc} & \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{array}{c} |0\rangle \\ |1\rangle \end{array} & \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{array}$ "quantum coin toss"

Quantum Is More Than Probabilistic

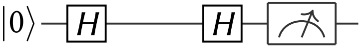
$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$\begin{cases} |0\rangle & 50\% \\ |1\rangle & 50\% \end{cases}$$

$$\begin{cases} \frac{|0\rangle+|1\rangle}{\sqrt{2}} & 50\% \\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} & 50\% \end{cases}$$



$$\begin{cases} |0\rangle & 50\% \\ |1\rangle & 50\% \end{cases}$$



$$\begin{cases} |0\rangle & 50\% \\ |1\rangle & 50\% \end{cases}$$

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

Quantum Is More Than Probabilistic

$$\begin{cases} |0\rangle & 50\% \\ |1\rangle & 50\% \end{cases}$$

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

$$\begin{cases} |0\rangle & 50\% \\ |1\rangle & 50\% \end{cases}$$

$$\begin{cases} |0\rangle & 100\% \\ |1\rangle & 0\% \end{cases}$$

$$\begin{cases} |0\rangle & 50\% \\ |1\rangle & 50\% \end{cases}$$

$$\begin{cases} |0\rangle & 100\% \\ |1\rangle & 0\% \end{cases}$$

- Larger systems: $q_0 \otimes q_1$

- Larger systems: $q_0 \otimes q_1$ where $A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$

- Larger systems: $q_0 \otimes q_1$ where $A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$

  E.g. $|01\rangle := |0\rangle \otimes |1\rangle = \begin{pmatrix} 1\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

- Larger systems: $q_0 \otimes q_1$ where $A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$

  E.g. $|01\rangle := |0\rangle \otimes |1\rangle = \begin{pmatrix} 1\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

- n-qubit state $\Rightarrow$ 2^n-dim vector

- Larger systems: $q_0 \otimes q_1$ where $A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$

  E.g. $|01\rangle := |0\rangle \otimes |1\rangle = \begin{pmatrix} 1\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

- n-qubit state $\Rightarrow$ 2^n-dim vector
- Linear combinations are again allowed:

$$\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$

- Larger systems: $q_0 \otimes q_1$ where $A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots \\ a_{10}B & \ddots & \\ \vdots & & \end{pmatrix}$

  E.g. $|01\rangle := |0\rangle \otimes |1\rangle = \begin{pmatrix} 1\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0\cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

- n-qubit state $\Rightarrow$ 2^n-dim vector
- Linear combinations are again allowed:

  $$\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$

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

- $\langle\psi| := |\psi\rangle^\dagger$

- $\langle\psi| := |\psi\rangle^\dagger$
  E.g. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \;\Rightarrow\; \langle\psi| = \overline{\alpha}\langle 0| + \overline{\beta}\langle 1| = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}$

- $\langle\psi| := |\psi\rangle^\dagger$

  E.g. $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\Rightarrow\; \langle\psi| = \overline{\alpha}\,\langle 0| + \overline{\beta}\,\langle 1| = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}$
- $\left\langle \psi \,\middle|\, \phi \right\rangle = \langle\psi| \circ |\phi\rangle$

- $\langle\psi| := |\psi\rangle^\dagger$

  E.g. $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\;\Rightarrow\;\; \langle\psi| = \overline{\alpha}\,\langle 0| + \overline{\beta}\,\langle 1| = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}$
- $\left\langle\psi\,\middle|\,\phi\right\rangle = \langle\psi| \circ |\phi\rangle$

  E.g. $\left\langle 1\,\middle|\,1\right\rangle = 1$ and $\left\langle 0\,\middle|\,1\right\rangle = 0$

- $\langle\psi| := |\psi\rangle^\dagger$
  E.g. $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\Rightarrow\; \langle\psi| = \overline{\alpha}\,\langle 0| + \overline{\beta}\,\langle 1| = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}$
- $\left\langle\psi\middle|\phi\right\rangle = \langle\psi| \circ |\phi\rangle$
  E.g. $\left\langle 1\middle| 1\right\rangle = 1$ and $\left\langle 0\middle| 1\right\rangle = 0$
- $f = \sum_{\vec{x},\vec{y}} \lambda_{\vec{x},\vec{y}}\,|\vec{y}\rangle\langle\vec{x}|$

- $\langle\psi| := |\psi\rangle^\dagger$

  E.g. $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\;\Rightarrow\;\; \langle\psi| = \overline{\alpha}\,\langle 0| + \overline{\beta}\,\langle 1| = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}$

- $\left\langle\psi\,\middle|\,\phi\right\rangle = \langle\psi| \circ |\phi\rangle$

  E.g. $\left\langle 1\,\middle|\,1\right\rangle = 1$ and $\left\langle 0\,\middle|\,1\right\rangle = 0$

- $f = \sum_{\vec{x},\vec{y}} \lambda_{\vec{x},\vec{y}}\,|\vec{y}\rangle\!\langle\vec{x}|$

$$\text{E.g. } H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} - \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right]$$
$$= \frac{1}{\sqrt{2}}\,|0\rangle\!\langle 0| + \frac{1}{\sqrt{2}}\,|0\rangle\!\langle 1| + \frac{1}{\sqrt{2}}\,|1\rangle\!\langle 0| - \frac{1}{\sqrt{2}}\,|1\rangle\!\langle 1|$$

- $\langle\psi| := |\psi\rangle^\dagger$

  E.g. $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \;\Rightarrow\; \langle\psi| = \overline{\alpha}\,\langle 0| + \overline{\beta}\,\langle 1| = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}$

- $\left\langle\psi\middle|\phi\right\rangle = \langle\psi| \circ |\phi\rangle$

  E.g. $\left\langle 1\middle|1\right\rangle = 1$ and $\left\langle 0\middle|1\right\rangle = 0$

- $f = \sum_{\vec{x},\vec{y}} \lambda_{\vec{x},\vec{y}}\,|\vec{y}\rangle\!\langle\vec{x}|$

$$\text{E.g. } H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} - \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right]$$
$$= \frac{1}{\sqrt{2}}\,|0\rangle\!\langle 0| + \frac{1}{\sqrt{2}}\,|0\rangle\!\langle 1| + \frac{1}{\sqrt{2}}\,|1\rangle\!\langle 0| - \frac{1}{\sqrt{2}}\,|1\rangle\!\langle 1|$$

$$H\,|0\rangle = \tfrac{1}{\sqrt{2}}\left[|0\rangle\left\langle 0\middle|0\right\rangle + |0\rangle\left\langle 1\middle|0\right\rangle + |1\rangle\left\langle 0\middle|0\right\rangle - |1\rangle\left\langle 1\middle|0\right\rangle\right] = \tfrac{|0\rangle+|1\rangle}{\sqrt{2}}$$

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

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

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

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

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

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

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

Unitarity $\Rightarrow$ reversibility

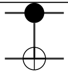
Unitarity $\Rightarrow$ reversibility

Quantum gates:

X or *Not*

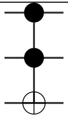
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

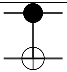
Quantum gates:

X or *Not*

$$-\boxed{X}-$$

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

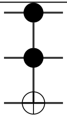
CX or *CNot*



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

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

Toffoli or *CCX* or *CCNot*



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

H

$$-\boxed{H}-$$

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

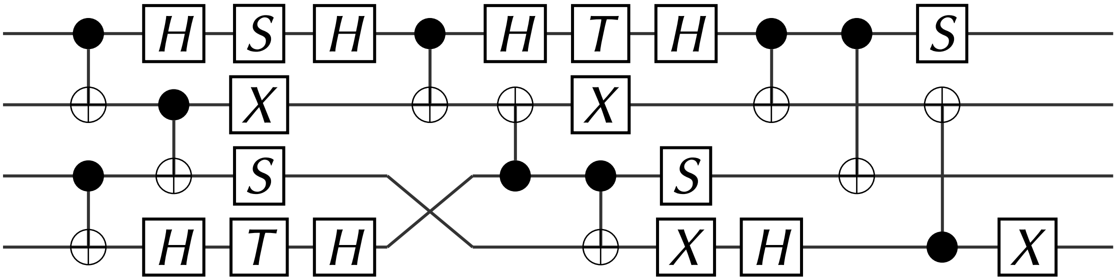
$Z(\alpha)$ or $R_Z(\alpha)$

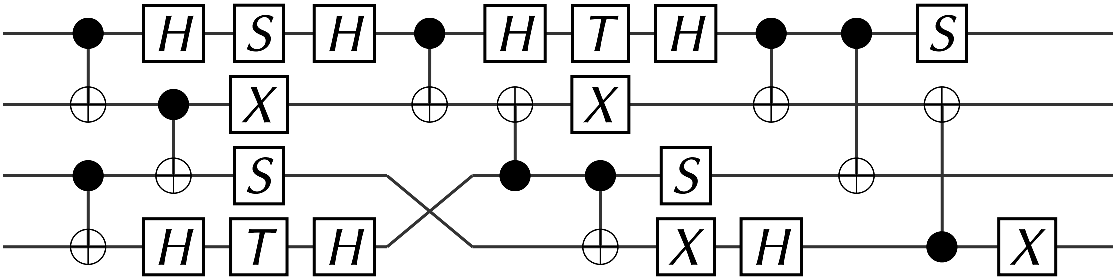
$$-\boxed{Z(\alpha)}-$$

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

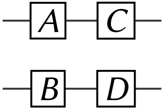
$$-\boxed{S}- := -\boxed{Z(\tfrac{\pi}{2})}-$$

$$-\boxed{T}- := -\boxed{Z(\tfrac{\pi}{4})}-$$


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



NB: make the equation $(C \otimes D)(A \otimes B) = CA \otimes DB$ obvious:



- Qubit initialisation:

Init

$$\boxed{\begin{array}{c} |0\rangle\!-\!\!\!-\!\!\!- \\ \begin{pmatrix}1\\0\end{pmatrix} \end{array}}$$

- Qubit initialisation:

Init

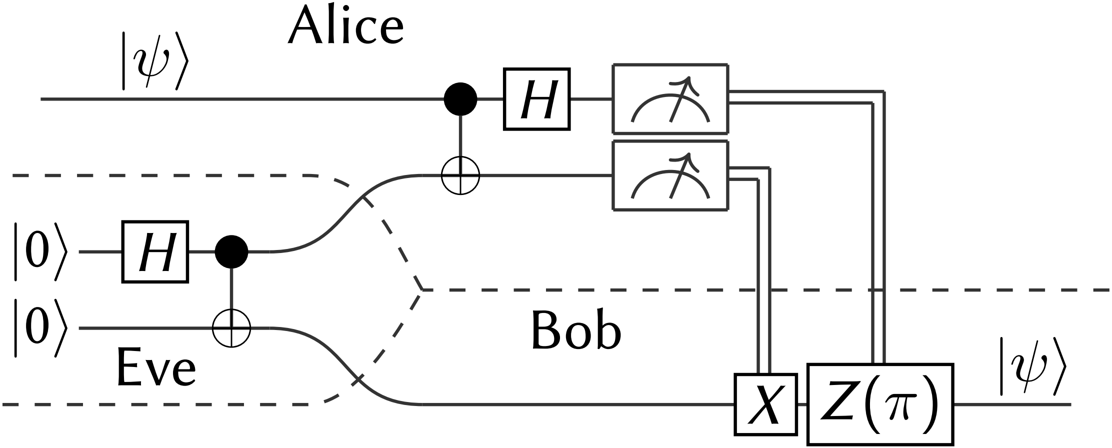
$|0\rangle$

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

- Measurement (effect + classical information):

Meas

$$\left\{\left\langle\begin{pmatrix}1 & 0\end{pmatrix},0\right\rangle,\left\langle\begin{pmatrix}0 & 1\end{pmatrix},1\right\rangle\right\}$$


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

Theorem : Universality[1]

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

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

Theorem : Universality[1]

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

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

Theorem : Universality[1]

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[2]

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

Theorem : Universality[1]

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

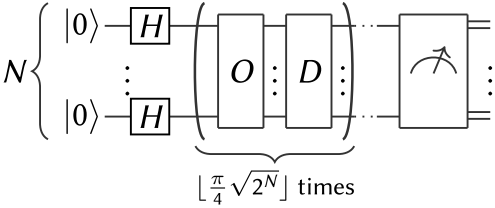
$Z(\alpha)$ $\Rightarrow$ infinite (uncountable) family of gates
$\Rightarrow$ bad for analysis and implementability

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

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

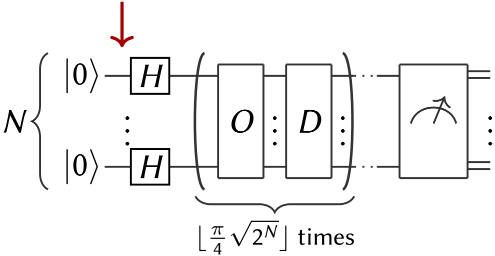
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

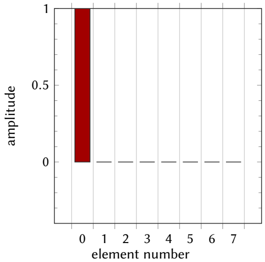
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N



$$O : |\vec{x}\rangle \mapsto (-1)^{\delta_{A[\vec{x}],\vec{y}}} |\vec{x}\rangle$$

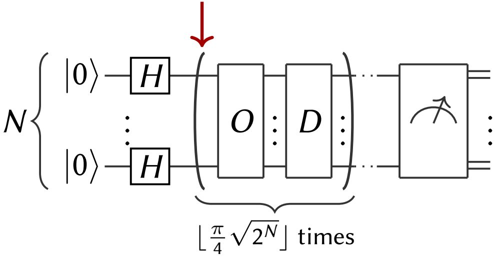
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

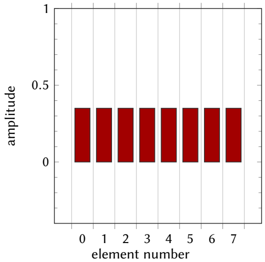




$$O : |\vec{x}\rangle \mapsto (-1)^{\delta_{A[\vec{x}],\vec{y}}} |\vec{x}\rangle$$

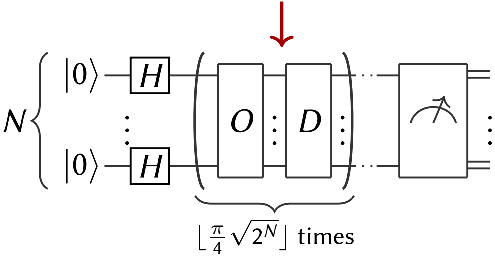
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

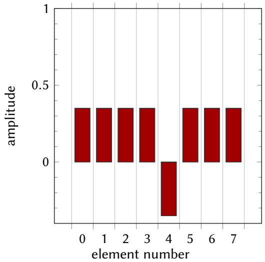




$$O : |\vec{x}\rangle \mapsto (-1)^{\delta_{A[\vec{x}],\vec{y}}} |\vec{x}\rangle$$

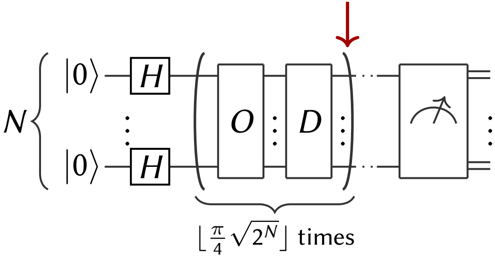
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

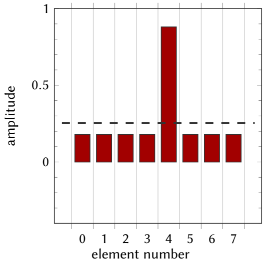




$$O : |\vec{x}\rangle \mapsto (-1)^{\delta_{A[\vec{x}],\vec{y}}} |\vec{x}\rangle$$

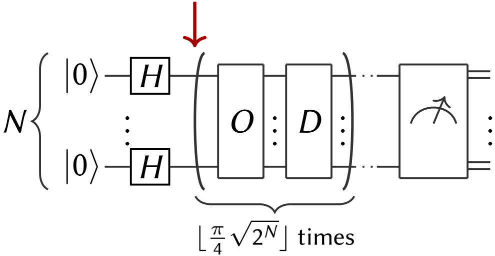
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

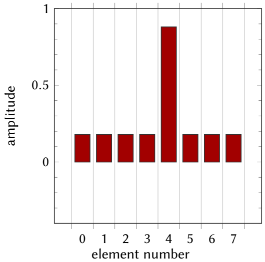




$$O : |\vec{x}\rangle \mapsto (-1)^{\delta_{A[\vec{x}],\vec{y}}} |\vec{x}\rangle$$

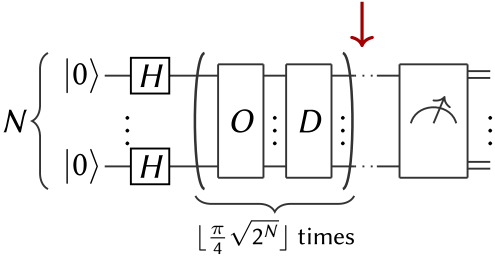
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

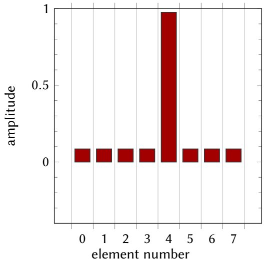




$$O : |\vec{x}\rangle \mapsto (-1)^{\delta_{A[\vec{x}],\vec{y}}} |\vec{x}\rangle$$

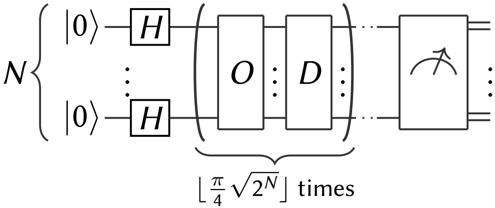
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

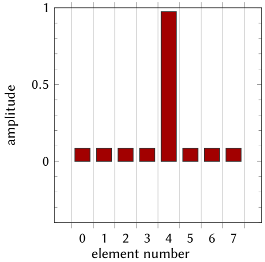




$$O : |\vec{x}\rangle \mapsto (-1)^{\delta_{A[\vec{x}],\vec{y}}} |\vec{x}\rangle$$

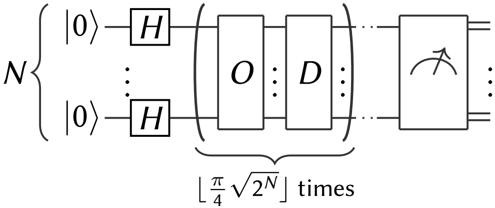
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

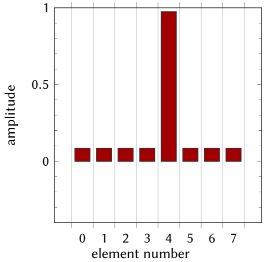




Classically check the result, and repeat if fail

Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N

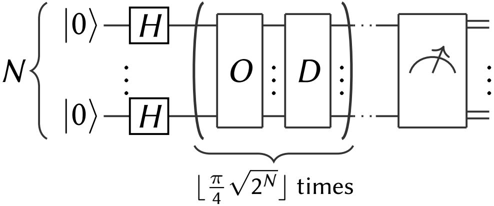


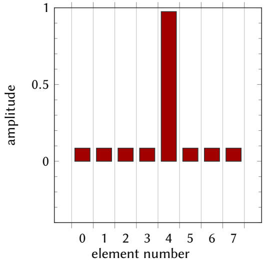


Classically check the result, and repeat if fail

$\Rightarrow$ Quantum part is only a subroutine

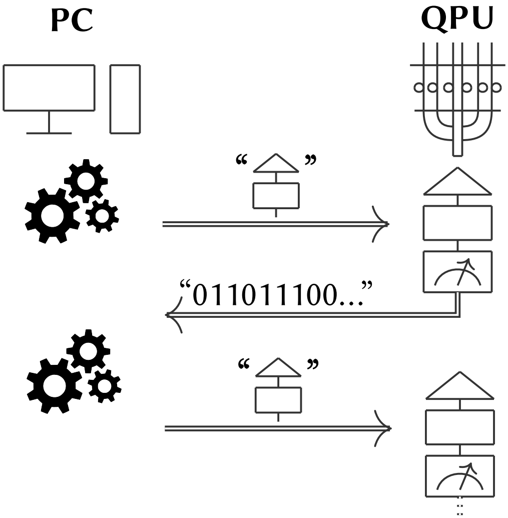
Pb: search of an element $\vec{y}$ in an unordered array A of size 2^N





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

- Quantum counting (quadratic speedup)
- Existence of Hamiltonian cycle (quadratic speedup)
- Shor's prime factorisation (exponential speedup)
- HHL's solution to s-sparse (Hermitian) system of equations (exponential speedup)
- QAOA for combinatorial optimisation
- VQE for ground eigenvalue estimation
- ...


PC
QPU
“011011100...”

Theorem

There is no linear map U such that $\forall \left|\psi\right\rangle,\ U\left|\psi\right\rangle = \left|\psi\right\rangle \otimes \left|\psi\right\rangle$.

Theorem

There is no linear map U such that $\forall \left|\psi\right\rangle,\ U\left|\psi\right\rangle = \left|\psi\right\rangle \otimes \left|\psi\right\rangle$.

Proof for 1 qubit: Suppose such a U exists. Then:

$$U\left|0\right\rangle = \left|00\right\rangle \text{ and } U\left|1\right\rangle = \left|11\right\rangle$$

Theorem

There is no linear map U such that $\forall \left|\psi\right\rangle,\ U\left|\psi\right\rangle = \left|\psi\right\rangle \otimes \left|\psi\right\rangle$.

Proof for 1 qubit: Suppose such a U exists. Then:

$$U\left|0\right\rangle = \left|00\right\rangle \text{ and } U\left|1\right\rangle = \left|11\right\rangle$$

By linearity, for $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$:

$$U\left|\psi\right\rangle = \alpha\left|00\right\rangle + \beta\left|11\right\rangle$$

Theorem

There is no linear map U such that $\forall \left|\psi\right\rangle,\ U\left|\psi\right\rangle = \left|\psi\right\rangle \otimes \left|\psi\right\rangle$.

Proof for 1 qubit: Suppose such a U exists. Then:

$$U\left|0\right\rangle = \left|00\right\rangle \text{ and } U\left|1\right\rangle = \left|11\right\rangle$$

By linearity, for $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$:

$$U\left|\psi\right\rangle = \alpha\left|00\right\rangle + \beta\left|11\right\rangle$$

But:

$$\left|\psi\right\rangle \otimes \left|\psi\right\rangle = \alpha^2\left|00\right\rangle + \alpha\beta(\left|01\right\rangle + \left|10\right\rangle) + \beta^2\left|11\right\rangle$$

- Cannot copy quantum information

Limitations of Usual Debugging

- Cannot copy quantum information
- Measurements are disruptive ($\Rightarrow$ printing value changes the state)

Limitations of Usual Debugging

- Cannot copy quantum information
- Measurements are disruptive ($\Rightarrow$ printing value changes the state)
- Measurement results are probabilistic

Limitations of Usual Debugging

- Cannot copy quantum information
- Measurements are disruptive ($\Rightarrow$ printing value changes the state)
- Measurement results are probabilistic
- Quantum resources are expensive

Limitations of Usual Debugging

- Cannot copy quantum information
- Measurements are disruptive ($\Rightarrow$ printing value changes the state)
- Measurement results are probabilistic
- Quantum resources are expensive
- Errors could be due to noise

- Cannot copy quantum information
- Measurements are disruptive ($\Rightarrow$ printing value changes the state)
- Measurement results are probabilistic
- Quantum resources are expensive
- Errors could be due to noise
- Simulations are very limited ($\sim$40 qubits $\Rightarrow$ supercomputer)

Quantum Lambda Calculus (Lineal [Arrighi,Dowek'06])

- $\mathbf{t} ::= \quad \mathbf{x} \quad | \quad \lambda \mathbf{x}\, \mathbf{t} \quad | \quad \mathbf{t}\ \mathbf{t} \quad | \quad \mathbf{0} \quad | \quad \alpha.\mathbf{t} \quad | \quad \mathbf{t} + \mathbf{t}$

- $\mathbf{t} ::= \quad \mathbf{x} \quad | \quad \lambda \mathbf{x}\, \mathbf{t} \quad | \quad \mathbf{t}\ \mathbf{t} \quad | \quad \mathbf{0} \quad | \quad \alpha.\mathbf{t} \quad | \quad \mathbf{t} + \mathbf{t}$

  E.g. $\mathbf{H} \equiv \lambda \mathbf{y}\, \{\mathbf{y}\, [\frac{\sqrt{2}}{2}.(\mathbf{false} + \mathbf{true})]\, [\frac{\sqrt{2}}{2}.(\mathbf{false} - \mathbf{true})]\}$

- $\mathbf{t} ::= \quad \mathbf{x} \quad | \quad \lambda\mathbf{x}\,\mathbf{t} \quad | \quad \mathbf{t}\ \mathbf{t} \quad | \quad \mathbf{0} \quad | \quad \alpha.\mathbf{t} \quad | \quad \mathbf{t}+\mathbf{t}$

  E.g. $\mathbf{H} \equiv \lambda\mathbf{y}\,\{\mathbf{y}\,[\frac{\sqrt{2}}{2}.(\mathbf{false}+\mathbf{true})]\,[\frac{\sqrt{2}}{2}.(\mathbf{false}-\mathbf{true})]\}$

  $\otimes \equiv \lambda\mathbf{x}\,\lambda\mathbf{y}\,\lambda\mathbf{f}\,(\mathbf{f}\,\mathbf{x}\,\mathbf{y}), \quad \pi_1 \equiv \lambda\mathbf{p}(\mathbf{p}\,\lambda\mathbf{x}\,\lambda\mathbf{y}\,\mathbf{x}), \quad \pi_2 \equiv \lambda\mathbf{p}(\mathbf{p}\,\lambda\mathbf{x}\,\lambda\mathbf{y}\,\mathbf{y}),$

  $\bigotimes \equiv \lambda\mathbf{f}\,\lambda\mathbf{g}\,\lambda\mathbf{x}\left(\otimes\ (\mathbf{f}\,(\pi_1\,\mathbf{x}))\ (\mathbf{g}\,(\pi_2\,\mathbf{x}))\right)$

- $\mathbf{t} ::= \quad \mathbf{x} \quad | \quad \lambda \mathbf{x}\, \mathbf{t} \quad | \quad \mathbf{t}\ \mathbf{t} \quad | \quad \mathbf{0} \quad | \quad \alpha.\mathbf{t} \quad | \quad \mathbf{t} + \mathbf{t}$

  E.g. $\mathbf{H} \equiv \lambda \mathbf{y}\, \{\mathbf{y}\, [\frac{\sqrt{2}}{2}.(\mathbf{false} + \mathbf{true})]\, [\frac{\sqrt{2}}{2}.(\mathbf{false} - \mathbf{true})]\}$

  $\otimes \equiv \lambda \mathbf{x}\, \lambda \mathbf{y}\, \lambda \mathbf{f}\, (\mathbf{f}\, \mathbf{x}\, \mathbf{y}), \quad \pi_1 \equiv \lambda \mathbf{p}(\mathbf{p}\, \lambda \mathbf{x}\, \lambda \mathbf{y}\, \mathbf{x}), \quad \pi_2 \equiv \lambda \mathbf{p}(\mathbf{p}\, \lambda \mathbf{x}\, \lambda \mathbf{y}\, \mathbf{y}),$

  $\bigotimes \equiv \lambda \mathbf{f}\, \lambda \mathbf{g}\, \lambda \mathbf{x} \left(\otimes\ (\mathbf{f}\, (\pi_1\, \mathbf{x}))\ (\mathbf{g}\, (\pi_2\, \mathbf{x})) \right)$

- Restrictions to enforce no-cloning

- $\mathbf{t} ::= \quad \mathbf{x} \quad | \quad \lambda \mathbf{x}\, \mathbf{t} \quad | \quad \mathbf{t}\ \mathbf{t} \quad | \quad \mathbf{0} \quad | \quad \alpha.\mathbf{t} \quad | \quad \mathbf{t} + \mathbf{t}$

  E.g. $\mathbf{H} \equiv \lambda \mathbf{y}\, \{\mathbf{y}\, [\frac{\sqrt{2}}{2}.(\mathbf{false} + \mathbf{true})]\, [\frac{\sqrt{2}}{2}.(\mathbf{false} - \mathbf{true})]\}$

  $\otimes \equiv \lambda \mathbf{x}\, \lambda \mathbf{y}\, \lambda \mathbf{f}\, (\mathbf{f}\, \mathbf{x}\, \mathbf{y}), \quad \pi_1 \equiv \lambda \mathbf{p}(\mathbf{p}\, \lambda \mathbf{x}\, \lambda \mathbf{y}\, \mathbf{x}), \quad \pi_2 \equiv \lambda \mathbf{p}(\mathbf{p}\, \lambda \mathbf{x}\, \lambda \mathbf{y}\, \mathbf{y}),$

  $$\bigotimes \equiv \lambda \mathbf{f}\, \lambda \mathbf{g}\, \lambda \mathbf{x} \left(\otimes\ (\mathbf{f}\, (\pi_1\, \mathbf{x}))\, (\mathbf{g}\, (\pi_2\, \mathbf{x})) \right)$$

- Restrictions to enforce no-cloning

- Rewrite system

- $\mathbf{t} ::= \quad \mathbf{x} \quad | \quad \lambda\mathbf{x}\,\mathbf{t} \quad | \quad \mathbf{t}\ \mathbf{t} \quad | \quad \mathbf{0} \quad | \quad \alpha.\mathbf{t} \quad | \quad \mathbf{t}+\mathbf{t}$

  E.g. $\mathbf{H} \equiv \lambda\mathbf{y}\,\{\mathbf{y}\,[\frac{\sqrt{2}}{2}.(\mathbf{false}+\mathbf{true})]\,[\frac{\sqrt{2}}{2}.(\mathbf{false}-\mathbf{true})]\}$

  $\otimes \equiv \lambda\mathbf{x}\,\lambda\mathbf{y}\,\lambda\mathbf{f}\,(\mathbf{f}\,\mathbf{x}\,\mathbf{y}), \quad \pi_1 \equiv \lambda\mathbf{p}(\mathbf{p}\,\lambda\mathbf{x}\,\lambda\mathbf{y}\,\mathbf{x}), \quad \pi_2 \equiv \lambda\mathbf{p}(\mathbf{p}\,\lambda\mathbf{x}\,\lambda\mathbf{y}\,\mathbf{y}),$

  $\bigotimes \equiv \lambda\mathbf{f}\,\lambda\mathbf{g}\,\lambda\mathbf{x}\left(\otimes\ (\mathbf{f}\,(\pi_1\,\mathbf{x}))\ (\mathbf{g}\,(\pi_2\,\mathbf{x}))\right)$

- Restrictions to enforce no-cloning

- Rewrite system

- Characterisation of vector spaces as model of rewrite system

- $\mathbf{t} ::= \quad \mathbf{x} \quad | \quad \lambda\mathbf{x}\,\mathbf{t} \quad | \quad \mathbf{t}\ \mathbf{t} \quad | \quad \mathbf{0} \quad | \quad \alpha.\mathbf{t} \quad | \quad \mathbf{t}+\mathbf{t}$

  E.g. $\mathbf{H} \equiv \lambda\mathbf{y}\,\{\mathbf{y}\,[\frac{\sqrt{2}}{2}.(\mathbf{false}+\mathbf{true})]\,[\frac{\sqrt{2}}{2}.(\mathbf{false}-\mathbf{true})]\}$

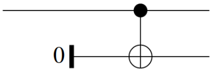
  $\otimes \equiv \lambda\mathbf{x}\,\lambda\mathbf{y}\,\lambda\mathbf{f}\,(\mathbf{f}\,\mathbf{x}\,\mathbf{y}), \quad \pi_1 \equiv \lambda\mathbf{p}(\mathbf{p}\,\lambda\mathbf{x}\,\lambda\mathbf{y}\,\mathbf{x}), \quad \pi_2 \equiv \lambda\mathbf{p}(\mathbf{p}\,\lambda\mathbf{x}\,\lambda\mathbf{y}\,\mathbf{y}),$

  $\bigotimes \equiv \lambda\mathbf{f}\,\lambda\mathbf{g}\,\lambda\mathbf{x}\left(\otimes\ (\mathbf{f}\,(\pi_1\,\mathbf{x}))\ (\mathbf{g}\,(\pi_2\,\mathbf{x}))\right)$

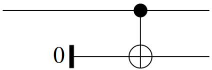
- Restrictions to enforce no-cloning
- Rewrite system
- Characterisation of vector spaces as model of rewrite system
- Confluence

Quipper ([Green,Lumsdaine,Ross,Selinger,Valiron'13])

```
share :: Qubit -> Circ (Qubit, Qubit)
share a = do
  b <- qinit False
  b <- qnot b ‘controlled‘ a
  return (a,b)
```

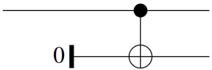


```
share :: Qubit -> Circ (Qubit, Qubit)
share a = do
  b <- qinit False
  b <- qnot b ‘controlled‘ a
  return (a,b)
```



Quipper ([Green,Lumsdaine,Ross,Selinger,Valiron'13])

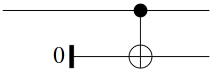
```
share :: Qubit -> Circ (Qubit, Qubit)
share a = do
  b <- qinit False
  b <- qnot b `controlled` a
  return (a,b)
```



- Embedded in Haskell ($\Rightarrow$ functional)

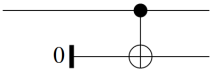
Quipper ([Green,Lumsdaine,Ross,Selinger,Valiron'13])

```
share :: Qubit -> Circ (Qubit, Qubit)
share a = do
  b <- qinit False
  b <- qnot b ‘controlled‘ a
  return (a,b)
```



- Embedded in Haskell ($\Rightarrow$ functional)
- Evaluation of q. circuit by QPU $\Rightarrow$ I/O monad

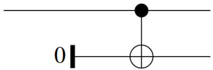
```
share :: Qubit -> Circ (Qubit, Qubit)
share a = do
  b <- qinit False
  b <- qnot b `controlled` a
  return (a,b)
```



- Embedded in Haskell ($\Rightarrow$ functional)
- Evaluation of q. circuit by QPU $\Rightarrow$ I/O monad
- Scalable

Quipper ([Green,Lumsdaine,Ross,Selinger,Valiron'13])

```
share :: Qubit -> Circ (Qubit, Qubit)
share a = do
  b <- qinit False
  b <- qnot b `controlled` a
  return (a,b)
```



- Embedded in Haskell ($\Rightarrow$ functional)
- Evaluation of q. circuit by QPU $\Rightarrow$ I/O monad
- Scalable
- Higher-order

- Proto-Quipper-M [Rios,Selinger'17]
  - Type safety
  - Reduction termination
  - Denotational (categorical) and operational semantics

- Proto-Quipper-M [Rios,Selinger'17]
  - Type safety
  - Reduction termination
  - Denotational (categorical) and operational semantics
- Proto-Quipper-D [Fu,Kishida,Ross,Selinger'20]
  - Dependent types

- Proto-Quipper-M [Rios,Selinger'17]
    - Type safety
    - Reduction termination
    - Denotational (categorical) and operational semantics
- Proto-Quipper-D [Fu,Kishida,Ross,Selinger'20]
    - Dependent types
- Proto-Quipper-Dyn [Fu,Kishida,Ross,Selinger'22]
    - Dynamic lifting

- Qiskit
- Liqui$|\rangle$, Q#
- ProjectQ
- CirQ
- Strawberry Fields
- AQASM
- ...

- Runtime verification $\Rightarrow$ measurement to retrieve information

Projective Measurements for Assertions

- Runtime verification $\Rightarrow$ measurement to retrieve information
- Measurement $\Rightarrow$ disruptive

- Runtime verification $\Rightarrow$ measurement to retrieve information
- Measurement $\Rightarrow$ disruptive

Projective Measurement

$\{P_m\}_m$ with $P_m \circ P_m = P_m$ and $\sum_m P_m = \mathbb{I}$.

- Runtime verification $\Rightarrow$ measurement to retrieve information
- Measurement $\Rightarrow$ disruptive

Projective Measurement

$\{P_m\}_m$ with $P_m \circ P_m = P_m$ and $\sum_m P_m = \mathbb{I}$.
When measured, state $|\psi\rangle$ gives result m with probability $p(m) = \langle\psi| P_m |\psi\rangle$, and collapses to state $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$.

- Runtime verification $\Rightarrow$ measurement to retrieve information
- Measurement $\Rightarrow$ disruptive

Projective Measurement

$\{P_m\}_m$ with $P_m \circ P_m = P_m$ and $\sum_m P_m = \mathbb{I}$.
When measured, state $|\psi\rangle$ gives result m with probability $p(m) = \langle\psi| P_m |\psi\rangle$, and collapses to state $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$.

E.g. on 1 qubit: $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ or $\left\{ \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right\}$

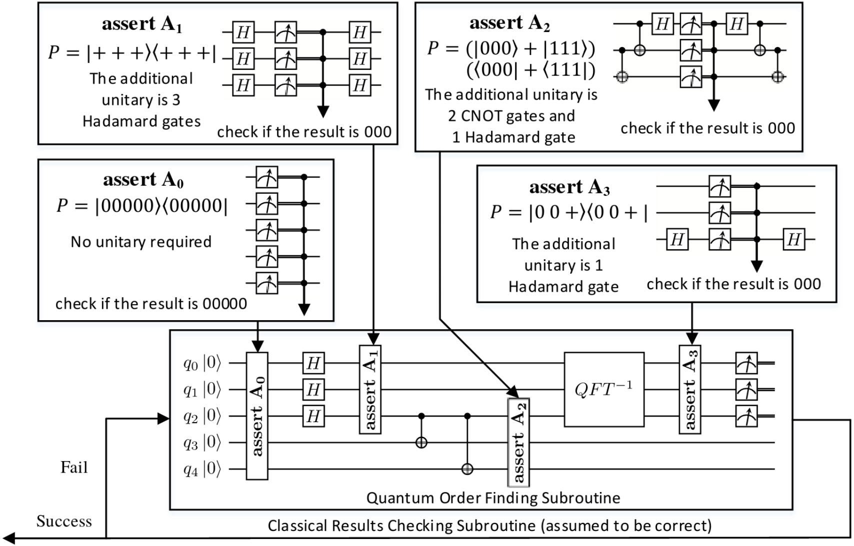
- Runtime verification $\Rightarrow$ measurement to retrieve information
- Measurement $\Rightarrow$ disruptive

Projective Measurement

$\{P_m\}_m$ with $P_m \circ P_m = P_m$ and $\sum_m P_m = \mathbb{I}$.
When measured, state $|\psi\rangle$ gives result m with probability $p(m) = \langle\psi| P_m |\psi\rangle$, and collapses to state $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$.

E.g. on 1 qubit: $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ or $\left\{ \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right\}$

- Projection defines a subspace
  $\Rightarrow$ possible to check if state is in subspace


assert A_1
$P = |+++\rangle\langle+++|$
The additional unitary is 3 Hadamard gates
check if the result is 000
assert A_2
$P = (|000\rangle + |111\rangle)(\langle 000| + \langle 111|)$
The additional unitary is 2 CNOT gates and 1 Hadamard gate
check if the result is 000
assert A_0
$P = |00000\rangle\langle 00000|$
No unitary required
check if the result is 00000
assert A_3
$P = |0\,0\,+\rangle\langle 0\,0\,+|$
The additional unitary is 1 Hadamard gate
check if the result is 000
q_0 $|0\rangle$
q_1 $|0\rangle$
q_2 $|0\rangle$
q_3 $|0\rangle$
q_4 $|0\rangle$
QFT^{-1}
Quantum Order Finding Subroutine
Fail
Success
Classical Results Checking Subroutine (assumed to be correct)

Twist [Yuan,McNally,Carbin'22]

Purity

A state is **pure** when it is separable from (not entangled with) the rest of the program.

Purity

A state is **pure** when it is separable from (not entangled with) the rest of the program.

- $$\begin{aligned} \text{Purity } \pi &::= \mathbf{P} \mid \mathbf{M} \\ \text{Quantum type } \varrho &::= \texttt{qubit} \mid \varrho_1 \,\&\, \varrho_2 \\ \text{Type } \tau &::= \texttt{bool} \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \varrho^\pi \\ \text{Quantum value } q &::= \texttt{ref}[\alpha] \mid [q_1, q_2] \\ \text{Expression } e &::= x \mid f \mid e_1(e_2) \mid (e_1, e_2) \mid \texttt{let } (x, y) = e_1 \texttt{ in } e_2 \mid \texttt{if } e \texttt{ then } e_1 \texttt{ else } e_2 \mid \texttt{T} \mid \texttt{F} \\ &\mid \texttt{qinit } () \mid U(e) \mid U_2(e) \mid \texttt{measure}(e) \mid q^\pi \\ &\mid \texttt{entangle}_\pi(e) \mid \texttt{split}_\pi(e) \mid \texttt{cast}_\pi(e) \end{aligned}$$

Purity

A state is **pure** when it is separable from (not entangled with) the rest of the program.

- $$\begin{aligned} \text{Purity } \pi &::= \mathbf{P} \mid \mathbf{M} \\ \text{Quantum type } \varrho &::= \mathtt{qubit} \mid \varrho_1 \,\&\, \varrho_2 \\ \text{Type } \tau &::= \mathtt{bool} \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \varrho^\pi \\ \text{Quantum value } q &::= \mathtt{ref}[\alpha] \mid [q_1, q_2] \\ \text{Expression } e &::= x \mid f \mid e_1(e_2) \mid (e_1, e_2) \mid \mathtt{let}\ (x,y) = e_1\ \mathtt{in}\ e_2 \mid \mathtt{if}\ e\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \mid \mathtt{T} \mid \mathtt{F} \\ &\mid \mathtt{qinit}\ () \mid U(e) \mid U_2(e) \mid \mathtt{measure}(e) \mid q^\pi \\ &\mid \mathtt{entangle}_\pi(e) \mid \mathtt{split}_\pi(e) \mid \mathtt{cast}_\pi(e) \end{aligned}$$
- Type system (type safety)

Purity

A state is **pure** when it is separable from (not entangled with) the rest of the program.

- $$\begin{aligned}\text{Purity } \pi &::= \mathbf{P} \mid \mathbf{M}\\ \text{Quantum type } \varrho &::= \mathtt{qubit} \mid \varrho_1 \,\&\, \varrho_2\\ \text{Type } \tau &::= \mathtt{bool} \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \varrho^\pi\\ \text{Quantum value } q &::= \mathtt{ref}[\alpha] \mid [q_1, q_2]\\ \text{Expression } e &::= x \mid f \mid e_1(e_2) \mid (e_1, e_2) \mid \mathtt{let}\ (x,y) = e_1\ \mathtt{in}\ e_2 \mid \mathtt{if}\ e\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \mid \mathtt{T} \mid \mathtt{F}\\ &\mid \mathtt{qinit}\ () \mid U(e) \mid U_2(e) \mid \mathtt{measure}(e) \mid q^\pi\\ &\mid \mathtt{entangle}_\pi(e) \mid \mathtt{split}_\pi(e) \mid \mathtt{cast}_\pi(e)\end{aligned}$$
- Type system (type safety)
- Static *and* runtime verification

Define a “lossy” interpretation, much easier to compute, which still provides useful information

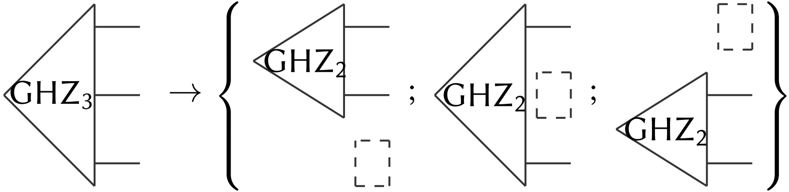
Define a “lossy” interpretation, much easier to compute, which still provides useful information

- [Perdrix’08]: $\mathfrak{Purity}$ check, as partition of the memory

Abstract Interpretation

Define a "lossy" interpretation, much easier to compute, which still provides useful information

- [Perdrix'08]: $\mathfrak{Purity}$ check, as partition of the memory
- [Yu,Palsberg'21]: Decompose states into subspaces



- $S ::= \textbf{skip} \mid \overline{q} := |0\rangle \mid \overline{q} := U\overline{q} \mid S \mid \textbf{measure } M[\overline{q}]\overline{S} \mid \textbf{while } M[\overline{q}] \textbf{ do } \{S\}$

- $S ::= \textbf{skip} \mid \overline{q} := |0\rangle \mid \overline{q} := U\overline{q} \mid S \mid \textbf{measure}\ M[\overline{q}]\overline{S} \mid \textbf{while}\ M[\overline{q}]\ \textbf{do}\ \{S\}$
- Interpretation $[\![.]\!]$ of a program as a function

- $S ::= \textbf{skip} \mid \overline{q} := |0\rangle \mid \overline{q} := U\overline{q} \mid S \mid \textbf{measure } M[\overline{q}]\overline{S} \mid \textbf{while } M[\overline{q}] \textbf{ do } \{S\}$
- Interpretation $[\![.]\!]$ of a program as a function
- Correctness: $\models \{P\}S\{Q\} \iff \mathrm{tr}(P\rho) \leq \mathrm{tr}(Q\,[\![S]\!]\,(\rho)) + \mathrm{tr}(\rho) - \mathrm{tr}([\![S]\!]\,(\rho))$

- $S ::= \textbf{skip} \mid \overline{q} := |0\rangle \mid \overline{q} := U\overline{q} \mid S \mid \textbf{measure } M[\overline{q}]\overline{S} \mid \textbf{while } M[\overline{q}] \textbf{ do } \{S\}$
- Interpretation $[\![.]\!]$ of a program as a function
- Correctness: $\models \{P\}S\{Q\} \iff \mathrm{tr}(P\rho) \leq \mathrm{tr}(Q\,[\![S]\!]\,(\rho)) + \mathrm{tr}(\rho) - \mathrm{tr}([\![S]\!]\,(\rho))$
- $$\{P\}\ \textbf{skip}\ \{P\}$$
  $$\{U^\dagger P U\}\ \overline{q} := U\overline{q}\ \{P\}$$
  $$\frac{\{P\}\ S_1\ \{Q\} \qquad \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1; S_2\ \{R\}}$$
  $$\frac{\{P_m\}\ S_m\ \{Q\} \text{ for all } m}{\{\sum_m {M_m}^\dagger P_m M_m\}\ \textbf{measure } M[\overline{q}] :\ \overline{S}\ \{Q\}}$$
  $$\frac{\{Q\}\ S\ \{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}}{\{M_0^\dagger P M_0 + M_1^\dagger Q M_1\}\ \textbf{while } M[\overline{q}] = 1 \textbf{ do } S\ \{P\}}$$
  $$\frac{P \sqsubseteq P' \quad \{P'\}\ S\ \{Q'\} \quad Q' \sqsubseteq Q}{\{P\}\ S\ \{Q\}}$$

- $S ::= \textbf{skip} \mid \overline{q} := |0\rangle \mid \overline{q} := U\overline{q} \mid S \mid \textbf{measure } M[\overline{q}]\overline{S} \mid \textbf{while } M[\overline{q}] \textbf{ do } \{S\}$
- Interpretation $[\![.]\!]$ of a program as a function
- Correctness: $\models \{P\}S\{Q\} \iff \mathrm{tr}(P\rho) \leq \mathrm{tr}(Q [\![S]\!] (\rho)) + \mathrm{tr}(\rho) - \mathrm{tr}([\![S]\!] (\rho))$
- $$\{P\}\ \textbf{skip}\ \{P\} \qquad \frac{\{P_m\}\ S_m\ \{Q\} \text{ for all } m}{\{\sum_m {M_m}^\dagger P_m M_m\}\ \textbf{measure}\ M[\overline{q}] :\ \overline{S}\ \{Q\}}$$
  $$\{U^\dagger PU\}\ \overline{q} := U\overline{q}\ \{P\} \qquad \frac{\{Q\}\ S\ \{M_0^\dagger PM_0 + M_1^\dagger QM_1\}}{\{M_0^\dagger PM_0 + M_1^\dagger QM_1\}\ \textbf{while}\ M[\overline{q}] = 1\ \textbf{do}\ S\ \{P\}}$$
  $$\frac{\{P\}\ S_1\ \{Q\} \qquad \{Q\}\ S_2\ \{R\}}{\{P\}\ S_1; S_2\ \{R\}} \qquad \frac{P \sqsubseteq P' \quad \{P'\}\ S\ \{Q'\} \quad Q' \sqsubseteq Q}{\{P\}\ S\ \{Q\}}$$
- Löwner order: $P \sqsubseteq P' \iff P' - P$ is positive semi-definite

Example

$$
\begin{array}{l}
q := |0\rangle\ ; \\
q := Hq; \\
\textbf{while } M[q] = 1 \textbf{ do } \{ \\
\quad q := |0\rangle\ ; \\
\quad q := Hq \\
\}
\end{array}
$$

$$
\dfrac{
\dfrac{}{\{\mathbb{I}\}\ q := |0\rangle\ \{|0\rangle\langle 0|\}}
\quad
\dfrac{}{\{|0\rangle\langle 0|\}\ q := Hq\ \{|+\rangle\langle +|\}}
\quad
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\{\mathbb{I}\}\ q := |0\rangle\ \{|0\rangle\langle 0|\}}
\quad
\dfrac{
\dfrac{}{\{|0\rangle\langle 0|\} q := Hq\ \{|+\rangle\langle +|\}}
}{\{|0\rangle\langle 0|\} q := Hq\ \{|0\rangle\langle 0| + |1\rangle\langle 1|\}}
}{\{\mathbb{I}\}\ q := |0\rangle\ ; q := Hq\ \{|0\rangle\langle 0| + |1\rangle\langle 1|\}}
}{\{|0\rangle\langle 0| + |1\rangle\langle 1|\}\ \textbf{while}\ M[q] = 1\ \textbf{do}\ \{q := |0\rangle\ ; q := Hq\}\ \{|0\rangle\langle 0|\}}
}{\{|+\rangle\langle +|\}\ \textbf{while}\ M[q] = 1\ \textbf{do}\ \{q := |0\rangle\ ; q := Hq\}\ \{|0\rangle\langle 0|\}}
}{\{\mathbb{I}\}\ q := |0\rangle\ ; q := Hq;\ \textbf{while}\ M[q] = 1\ \textbf{do}\ \{q := |0\rangle\ ; q := Hq\}\ \{|0\rangle\langle 0|\}}
$$

$$
\dfrac{
\dfrac{}{\{\mathbb{I}\}\ q := |0\rangle\ \{|0\rangle\langle 0|\}}
\quad
\dfrac{}{\{|0\rangle\langle 0|\}\ q := Hq\ \{|+\rangle\langle +|\}}
\quad
\dfrac{
\dfrac{
\dfrac{}{\{\mathbb{I}\}\ q := |0\rangle\ \{|0\rangle\langle 0|\}}
\quad
\dfrac{\dfrac{}{\{|0\rangle\langle 0|\} q := Hq\ \{|+\rangle\langle +|\}}}{\{|0\rangle\langle 0|\} q := Hq\ \{|0\rangle\langle 0| + |1\rangle\langle 1|\}}
}{\{\mathbb{I}\}\ q := |0\rangle\ ;\ q := Hq\ \{|0\rangle\langle 0| + |1\rangle\langle 1|\}}
}{\{|0\rangle\langle 0| + |1\rangle\langle 1|\}\ \textbf{while}\ M[q] = 1\ \textbf{do}\ \{q := |0\rangle\ ;\ q := Hq\}\ \{|0\rangle\langle 0|\}}
}{
\{|+\rangle\langle +|\}\ \textbf{while}\ M[q] = 1\ \textbf{do}\ \{q := |0\rangle\ ;\ q := Hq\}\ \{|0\rangle\langle 0|\}
}
$$

$$
\dfrac{\cdots}{\{\mathbb{I}\}\ q := |0\rangle\ ;\ q := Hq;\ \textbf{while}\ M[q] = 1\ \textbf{do}\ \{q := |0\rangle\ ;\ q := Hq\}\ \{|0\rangle\langle 0|\}}
$$

$$
|0\rangle\langle 0| + |1\rangle\langle 1| - |+\rangle\langle +| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = |-\rangle\langle -|
$$

$$
\Rightarrow \quad |+\rangle\langle +| \sqsubseteq |0\rangle\langle 0| + |1\rangle\langle 1|
$$

- Sqir [Hietala,Rand,Hung,Li,Hicks'21]
  - Small but non-trivial syntax
  - Matrix/density operators semantics
  - Proof obligations proven using Coq
  - Verification of Simon, Shor, Grover, ...

- Sqir [Hietala,Rand,Hung,Li,Hicks'21]
  - Small but non-trivial syntax
  - Matrix/density operators semantics
  - Proof obligations proven using Coq
  - Verification of Simon, Shor, Grover, ...
- Voqc [Hietala,Rand,Hung,Wu,Hicks'21]
  - Verified compiler
  - Sqir as intermediate representation

Qbricks [Chareton,Bardin,Bobot,Perrelle,Valiron'21]

- Small but non-trivial syntax

Qbricks [Chareton,Bardin,Bobot,Perrelle,Valiron'21]

- Small but non-trivial syntax
- Circuit description function $\to$ *parameterised* sum-over-paths
  $\Rightarrow$ proofs over *families* of circuits

Qbricks [Chareton,Bardin,Bobot,Perrelle,Valiron'21]

- Small but non-trivial syntax
- Circuit description function $\rightarrow$ *parameterised* sum-over-paths
  $\Rightarrow$ proofs over *families* of circuits
- Proof obligations proven using Why3
  - WhyML
  - external SMT-solvers (Alt-Ergo, CVC3/4, Vampire, Z3, ...)
  - external proof assistants (Coq, Isabelle/HOL)

Qbricks [Chareton,Bardin,Bobot,Perrelle,Valiron'21]

- Small but non-trivial syntax
- Circuit description function $\rightarrow$ *parameterised* sum-over-paths
  $\Rightarrow$ proofs over *families* of circuits
- Proof obligations proven using Why3
  - WhyML
  - external SMT-solvers (Alt-Ergo, CVC3/4, Vampire, Z3, ...)
  - external proof assistants (Coq, Isabelle/HOL)
- Verification of Grover, Shor, ...

Plan

Theorem : Universality[5]

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[6]
- Clifford+T fragment : $\alpha \in \frac{\pi}{4}\mathbb{Z}$
  - approx. universal[7], with efficient approximation[8]

---

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

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)
- Overall trick: try to reduce $\mathcal{C}_2^\dagger \circ \mathcal{C}_1$ to identity

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)
- Overall trick: try to reduce $\mathcal{C}_2^\dagger \circ \mathcal{C}_1$ to identity
- Idea 1: exploit redundancy $\Rightarrow$ Quantum-style decision diagrams

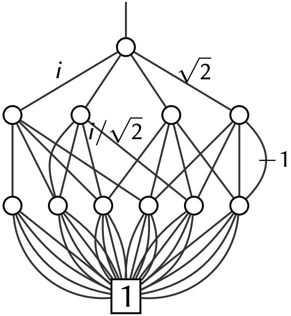
Problem of circuit equivalence

Do two given circuits implement the same operator?

- Decidable: compute the matrices!
- But hard: QMA-hard (quantum equivalent of NP-hard)
- Overall trick: try to reduce $\mathcal{C}_2^\dagger \circ \mathcal{C}_1$ to identity
- Idea 1: exploit redundancy $\Rightarrow$ Quantum-style decision diagrams
- Idea 2: reason graphically / use a rewrite system
  $\Rightarrow$ equational theory (e.g. $-\boxed{H}-\boxed{H}- \;=\; \text{———}$)

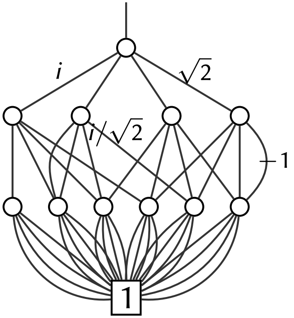
Quantum Multiple-Valued Decision Diagrams (QMDDs) [Wille et al.]

Example:

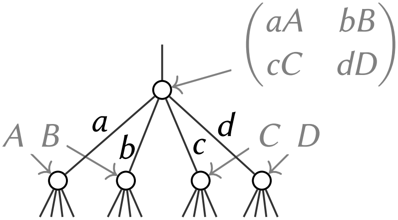


Quantum Multiple-Valued Decision Diagrams (QMDDs) [Wille et al.]

Example:

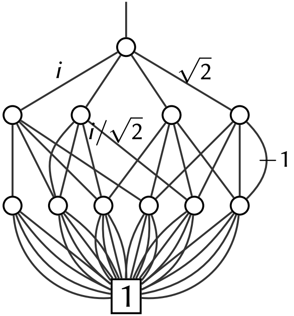


- Interpretation:

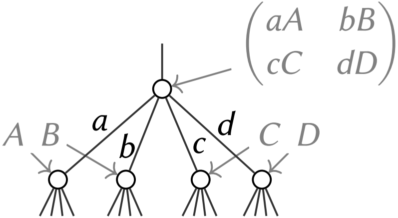


Quantum Multiple-Valued Decision Diagrams (QMDDs) [Wille et al.]

Example:

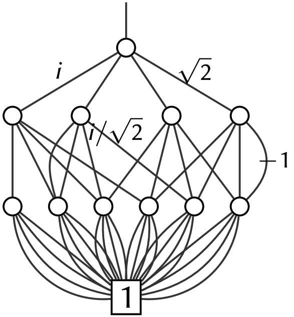


- Interpretation:

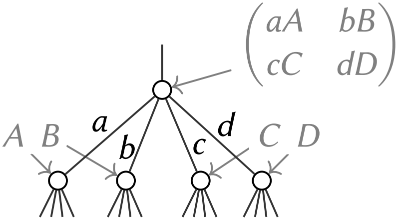


- Reduction: “colinear” nodes are merged

Example:



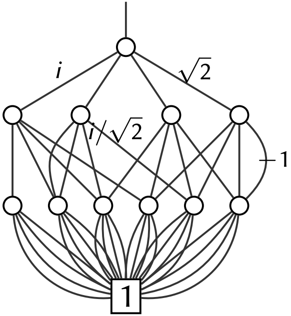
- Interpretation:



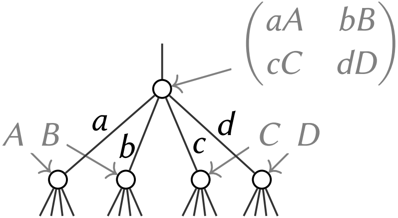
- Reduction: “colinear” nodes are merged
- Uniqueness of reduced QMDD

Quantum Multiple-Valued Decision Diagrams (QMDDs) [Wille et al.]

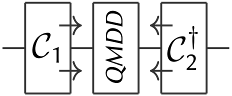
Example:



- Interpretation:



- Reduction: “colinear” nodes are merged
- Uniqueness of reduced QMDD
- Equivalence checking:



- $f := |\vec{x}\rangle \mapsto s \sum_{\vec{y}\in V^k} e^{2i\pi P(\vec{x},\vec{y})} \left|\vec{O}(\vec{x},\vec{y})\right\rangle$

  $s \in \mathbb{R}$, $P \in \mathbb{R}[X_1,\ldots,X_k]$, and $\vec{O} \in (\mathbb{F}_2[X_1,\ldots,X_k])^m$

- $f := |\vec{x}\rangle \mapsto s \sum_{\vec{y}\in V^k} e^{2i\pi P(\vec{x},\vec{y})} \left|\vec{O}(\vec{x},\vec{y})\right\rangle$
  $s \in \mathbb{R}$, $P \in \mathbb{R}[X_1,\ldots,X_k]$, and $\vec{O} \in (\mathbb{F}_2[X_1,\ldots,X_k])^m$

- $id_n := |\vec{x}\rangle \mapsto |\vec{x}\rangle$

- $f := |\vec{x}\rangle \mapsto s \sum_{\vec{y} \in V^k} e^{2i\pi P(\vec{x},\vec{y})} \left| \vec{O}(\vec{x}, \vec{y}) \right\rangle$

  $s \in \mathbb{R}$, $P \in \mathbb{R}[X_1, \ldots, X_k]$, and $\vec{O} \in (\mathbb{F}_2[X_1, \ldots, X_k])^m$

- $id_n := |\vec{x}\rangle \mapsto |\vec{x}\rangle$

- $f \otimes g := \left| \vec{x}_f, \vec{x}_g \right\rangle \mapsto s_f s_g \sum_{\vec{y}_f, \vec{y}_g} e^{2i\pi (P_g + P_f)} \left| \vec{O}_f, \vec{O}_g \right\rangle$

- $f := |\vec{x}\rangle \mapsto s \sum_{\vec{y}\in V^k} e^{2i\pi P(\vec{x},\vec{y})} \left|\vec{O}(\vec{x},\vec{y})\right\rangle$

  $s \in \mathbb{R}$, $P \in \mathbb{R}[X_1,\ldots,X_k]$, and $\vec{O} \in (\mathbb{F}_2[X_1,\ldots,X_k])^m$

- $id_n := |\vec{x}\rangle \mapsto |\vec{x}\rangle$

- $f \otimes g := \left|\vec{x}_f,\vec{x}_g\right\rangle \mapsto s_f s_g \sum_{\vec{y}_f,\vec{y}_g} e^{2i\pi(P_g+P_f)} \left|\vec{O}_f,\vec{O}_g\right\rangle$

- $f \circ g := \left|\vec{x}_g\right\rangle \mapsto s_f s_g \sum_{\vec{y}_f,\vec{y}_g} e^{2i\pi\left(P_g+P_f[\vec{x}_f\leftarrow\vec{O}_g]\right)} \left|\vec{O}_f[\vec{x}_f \leftarrow \vec{O}_g]\right\rangle$

- $f := |\vec{x}\rangle \mapsto s \sum_{\vec{y}\in V^k} e^{2i\pi P(\vec{x},\vec{y})} \left|\vec{O}(\vec{x},\vec{y})\right\rangle$

  $s \in \mathbb{R}$, $P \in \mathbb{R}[X_1,\dots,X_k]$, and $\vec{O} \in (\mathbb{F}_2[X_1,\dots,X_k])^m$

- $id_n := |\vec{x}\rangle \mapsto |\vec{x}\rangle$

- $f \otimes g := \left|\vec{x}_f, \vec{x}_g\right\rangle \mapsto s_f s_g \sum_{\vec{y}_f,\vec{y}_g} e^{2i\pi(P_g+P_f)} \left|\vec{O}_f, \vec{O}_g\right\rangle$

- $f \circ g := \left|\vec{x}_g\right\rangle \mapsto s_f s_g \sum_{\vec{y}_f,\vec{y}_g} e^{2i\pi\left(P_g+P_f[\vec{x}_f\leftarrow\vec{O}_g]\right)} \left|\vec{O}_f[\vec{x}_f \leftarrow \vec{O}_g]\right\rangle$

- $[\![f]\!] := s \sum_{\vec{y},\vec{x}\in\{0,1\}^k} e^{2i\pi P(\vec{x},\vec{y})} \left|\vec{O}(\vec{x},\vec{y})\right\rangle\langle\vec{x}|$

$$H := |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in V} e^{2i\pi \frac{xy}{2}} |y\rangle$$

$$H := |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in V} e^{2i\pi \frac{xy}{2}} |y\rangle$$

$$[\![H]\!] = \frac{1}{\sqrt{2}} \sum_{x,y \in \{0,1\}} e^{2i\pi \frac{xy}{2}} |y\rangle\langle x| = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

$$H := |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in V} e^{2i\pi \frac{xy}{2}} |y\rangle$$

$$[\![H]\!] = \frac{1}{\sqrt{2}} \sum_{x,y \in \{0,1\}} e^{2i\pi \frac{xy}{2}} |y\rangle\langle x| = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

$$H \otimes H = |x_0, x_1\rangle \mapsto \frac{1}{2} \sum_{y_0, y_1 \in V} e^{2i\pi(\frac{x_0 y_0}{2} + \frac{x_1 y_1}{2})} |y_0, y_1\rangle$$

$$H := |x\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{y \in V} e^{2i\pi \frac{xy}{2}} |y\rangle$$

$$[\![H]\!] = \frac{1}{\sqrt{2}} \sum_{x,y \in \{0,1\}} e^{2i\pi \frac{xy}{2}} |y\rangle\langle x| = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

$$H \otimes H = |x_0, x_1\rangle \mapsto \frac{1}{2} \sum_{y_0, y_1 \in V} e^{2i\pi(\frac{x_0 y_0}{2} + \frac{x_1 y_1}{2})} |y_0, y_1\rangle$$

$$\text{CNot} := |x_0, x_1\rangle \mapsto |x_0, x_0 \oplus x_1\rangle$$

3 rewrite rules ($\underset{\mathsf{Clif}}{\longrightarrow}$) in [Amy'18]: reduce the number of variables.

3 rewrite rules ($\xrightarrow[\text{Clif}]{}$) in [Amy'18]: reduce the number of variables.E.g.:

$$\begin{array}{c} |\vec{x}\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{y_0}{2}(y_0'+\widehat{Q})+R\right)} \left|\vec{O}\right\rangle \\ \Big\downarrow \quad \begin{array}{l} y_0 \notin \mathrm{Var}(R, Q, \vec{O}) \\ y_0' \notin \mathrm{Var}(Q) \end{array} \\ |\vec{x}\rangle \mapsto 2 \sum_{\vec{y}\setminus\{y_0,y_0'\}} e^{2i\pi\left(R\left[y_0'\leftarrow\widehat{Q}\right]\right)} \left|\vec{O}\left[y_0' \leftarrow Q\right]\right\rangle \end{array} \tag{HH}$$

3 rewrite rules ($\xrightarrow[\text{Clif}]{}$) in [Amy'18]: reduce the number of variables.E.g.:

$$\begin{array}{c} |\vec{x}\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{y_0}{2}(y_0'+\widehat{Q})+R\right)} \left|\vec{O}\right\rangle \\ \Big\downarrow \quad \begin{array}{l} y_0 \notin \mathrm{Var}(R, Q, \vec{O}) \\ y_0' \notin \mathrm{Var}(Q) \end{array} \\ |\vec{x}\rangle \mapsto 2 \sum_{\vec{y}\setminus\{y_0,y_0'\}} e^{2i\pi\left(R[y_0'\leftarrow\widehat{Q}]\right)} \left|\vec{O}\left[y_0' \leftarrow Q\right]\right\rangle \end{array} \tag{HH}$$

Weak Completeness for Clifford

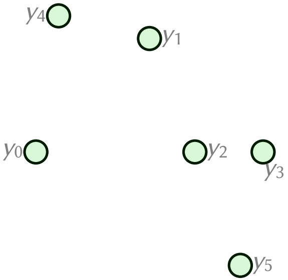
If t_0 and t_1 are unitary Clifford terms such that $[\![t_0]\!] = [\![t_1]\!]$, then $t_0 \circ t_1^\dagger \xrightarrow[\text{Clif}]{}^* id$.

$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0 + \frac{1}{2}y_4y_0 + \frac{1}{8}y_5y_0y_1 + \frac{3}{4}y_1y_2y_3 + \frac{1}{2}y_0y_3\right)} |0, 1\oplus y_0 \oplus y_4y_2, y_5\rangle$$

$$\downarrow$$

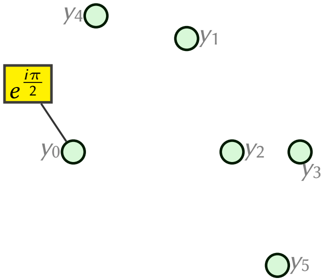
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)} |0, 1\oplus y_0\oplus y_4y_2, y_5\rangle$$

$$\downarrow$$



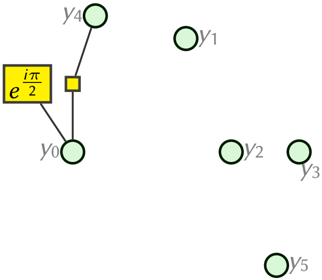
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)}\,|0, 1\oplus y_0\oplus y_4y_2, y_5\rangle$$

$$\downarrow$$



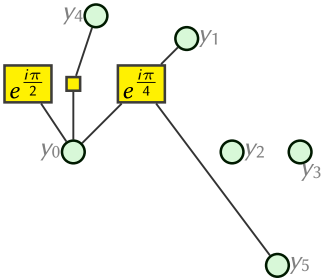
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0 + \frac{1}{2}y_4y_0 + \frac{1}{8}y_5y_0y_1 + \frac{3}{4}y_1y_2y_3 + \frac{1}{2}y_0y_3\right)} |0, 1\oplus y_0 \oplus y_4y_2, y_5\rangle$$

$\downarrow$



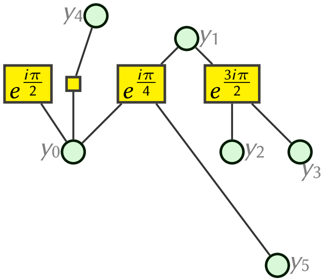
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)}\,|0, 1\oplus y_0\oplus y_4y_2, y_5\rangle$$

$$\downarrow$$



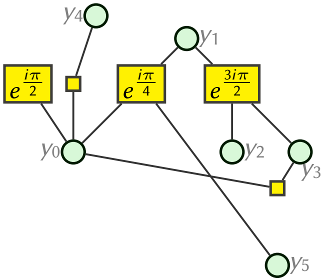
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0 + \frac{1}{2}y_4y_0 + \frac{1}{8}y_5y_0y_1 + \frac{3}{4}y_1y_2y_3 + \frac{1}{2}y_0y_3\right)} |0, 1\oplus y_0 \oplus y_4y_2, y_5\rangle$$

$$\downarrow$$



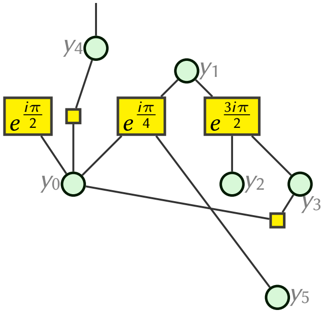
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)}|0, 1\oplus y_0\oplus y_4y_2, y_5\rangle$$

$$\downarrow$$



$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)}|0, 1\oplus y_0\oplus y_4y_2, y_5\rangle$$

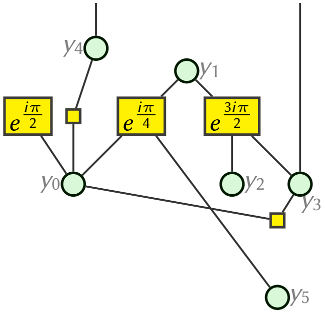
$$\downarrow$$



A Visualisation of SOP Terms With ZX Diagrams

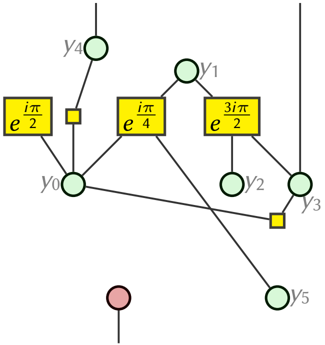
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)} |0,\, 1\oplus y_0\oplus y_4y_2,\, y_5\rangle$$

$$\downarrow$$



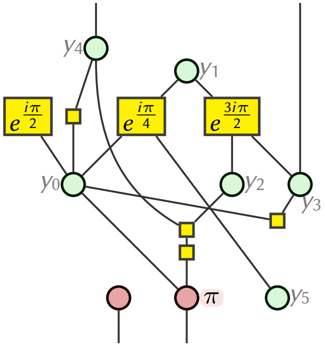
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)}\,|0,\ 1\oplus y_0\oplus y_4y_2,\ y_5\rangle$$

$$\downarrow$$



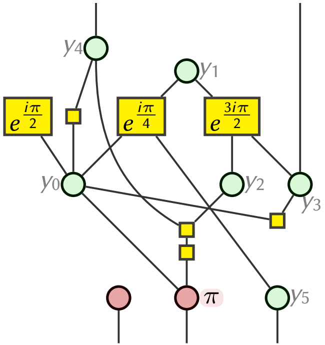
$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)} |0, 1\oplus y_0\oplus y_4y_2, y_5\rangle$$

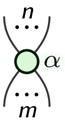
$$\downarrow$$



$$|y_4, y_3\rangle \mapsto \sum_{\vec{y}} e^{2i\pi\left(\frac{1}{4}y_0+\frac{1}{2}y_4y_0+\frac{1}{8}y_5y_0y_1+\frac{3}{4}y_1y_2y_3+\frac{1}{2}y_0y_3\right)}\,|0,\ 1\oplus y_0\oplus y_4y_2,\ y_5\rangle$$

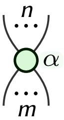
$$\downarrow$$



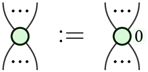
- A spider: 

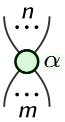
$$:: \quad 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right.$$

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

- A spider: 

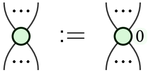
$$:: \quad 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right. = |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$$



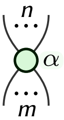
- A spider: 

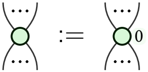
$:: \; 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right.$

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

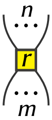


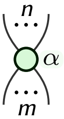
- A change of basis:  $:: \; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

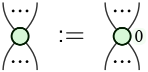
- A spider:  $:: \quad 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right. \quad = |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$

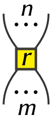


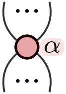
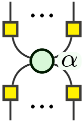
- A change of basis:  $:: \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

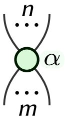
generalised to  $:: \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \cdots & \cdots & 1 \\ \vdots & \ddots & & \vdots \\ \vdots & & 1 & 1 \\ 1 & \cdots & 1 & r \end{pmatrix}$

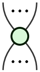
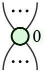
- A spider:  $:: \quad 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right.$
  $= |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$

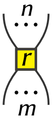


- A change of basis:  $:: \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ generalised to  $:: \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \cdots & \cdots & 1 \\ \vdots & \ddots & & \vdots \\ \vdots & & 1 & 1 \\ 1 & \cdots & 1 & r \end{pmatrix}$

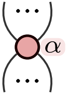
- Another spider:  $:=$  $:: \quad |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$

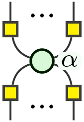
- A spider: 

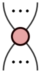
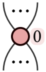
$$:: \quad 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & 0 & 0 \\ 0 & \cdots & \cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right.$$
$$= |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$$
 $:=$ 

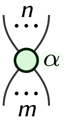
- A change of basis:  $:: \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ generalised to 

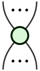
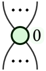
$:: \ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \cdots & \cdots & 1 \\ \vdots & \ddots & & \vdots \\ \vdots & & 1 & 1 \\ 1 & \cdots & 1 & r \end{pmatrix}$

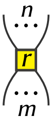
- Another spider: 

$:=$ 

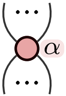
$:: \ |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$
 $:=$ 

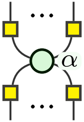
- A spider: 

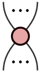
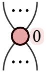
$:: \; 2^m \left\{ \overbrace{\begin{pmatrix} 1 & 0 & \cdots\cdots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \vdots \\ \vdots & & 0 & 0 \\ 0 & \cdots\cdots & 0 & e^{i\alpha} \end{pmatrix}}^{2^n} \right. = |0^m\rangle\langle 0^n| + e^{i\alpha}|1^m\rangle\langle 1^n|$
 $:=$ 

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

$:: \; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \cdots & \cdots & 1 \\ \vdots & \ddots & & \vdots \\ \vdots & & 1 & 1 \\ 1 & \cdots & 1 & r \end{pmatrix}$

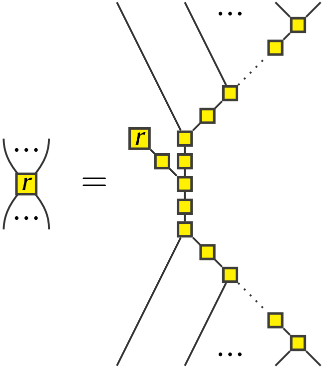
- Another spider: 

$:=$ 

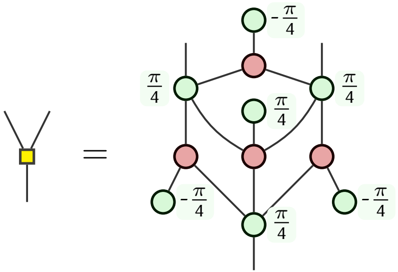
$:: \; |+^m\rangle\langle +^n| + e^{i\alpha}\,|-^m\rangle\langle -^n|$
 $:=$ 

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

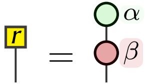
Getting Rid of the H-Spider



and

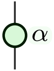


and



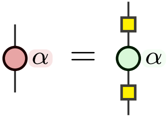
One-qubit Operators

$Z(\alpha)$:
rotation around Z



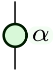
Hadamard:

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



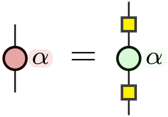
One-qubit Operators

$Z(\alpha)$:
rotation around Z



Hadamard:

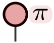
$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

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

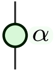
$\sqrt{2}\,|1\rangle$:



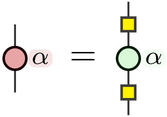
$|00\rangle + |11\rangle$:

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

One-qubit Operators

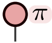
$Z(\alpha)$:
rotation around Z 

Hadamard: 

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

States and Projectors

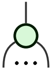
$\sqrt{2}\,|0\rangle$: 

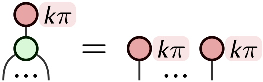
$\sqrt{2}\,|1\rangle$: 

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

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

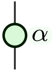
Green Spider

Copy: 

s.t. 

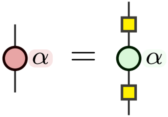
One-qubit Operators

$Z(\alpha)$:
rotation around Z



Hadamard:

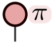
$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

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

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

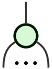


$|00\rangle + |11\rangle$:

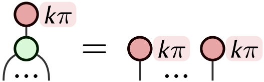
$\langle 00| + \langle 11|$:

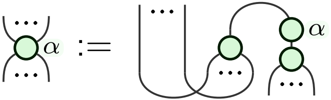
Green Spider

Copy:



s.t.

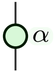




Intuition Behind the Generators

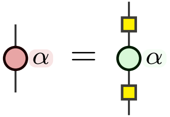
One-qubit Operators

$Z(\alpha)$:
rotation around Z



Hadamard:

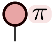
$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

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

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

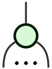


$|00\rangle + |11\rangle$:

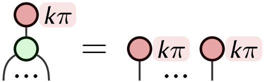
$\langle 00| + \langle 11|$:

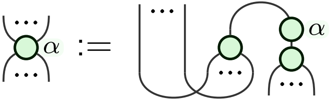
Green Spider

Copy:



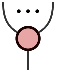
s.t.



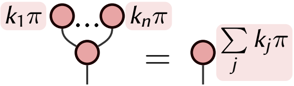


Red Spider

XOR:

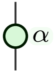


s.t.



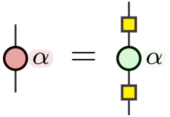
One-qubit Operators

$Z(\alpha)$:
rotation around Z



Hadamard:

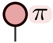
$X(\alpha)$:
$= HZ(\alpha)H$



States and Projectors

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

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

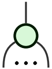


$|00\rangle + |11\rangle$:

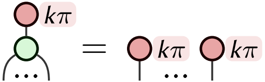
$\langle 00| + \langle 11|$:

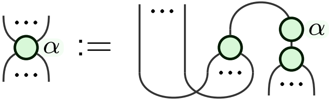
Green Spider

Copy:



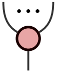
s.t.



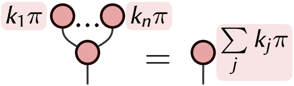


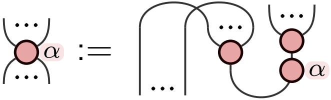
Red Spider

XOR:



s.t.

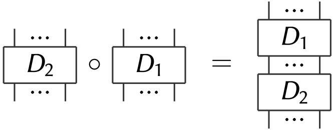


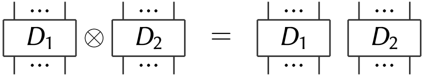


Generators

Generators

Compositions





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

Generators

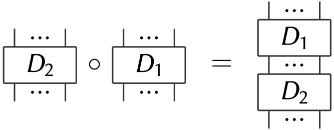
Compositions

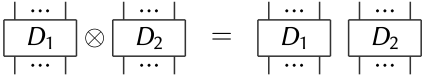
Standard Interpretation

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

Generators

Compositions

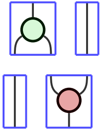




Standard Interpretation

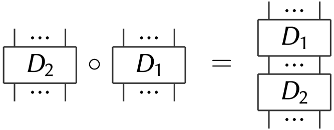
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

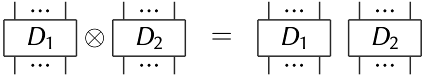
Example



Generators

Compositions

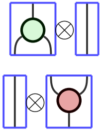




Standard Interpretation

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

Example



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

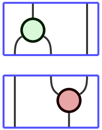
Generators

Compositions

Standard Interpretation

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

Example



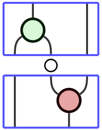
Generators

Compositions

Standard Interpretation

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

Example



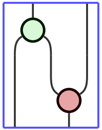
Generators

Compositions

Standard Interpretation

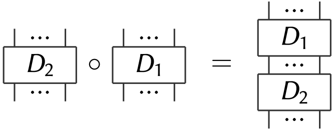
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

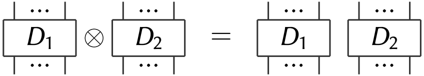
Example



Generators

Compositions

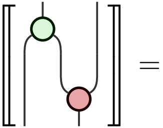




Standard Interpretation

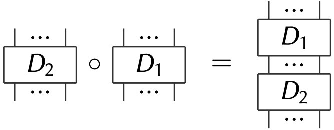
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

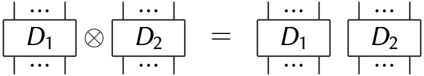
Example



Generators

Compositions

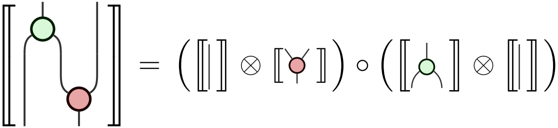




Standard Interpretation

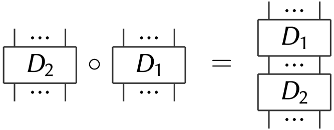
$$[\![.]\!] : \mathbf{ZX} \to \mathcal{M}(\mathbb{C})$$

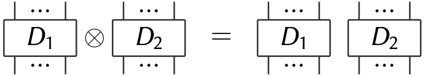
Example



Generators

Compositions

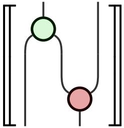




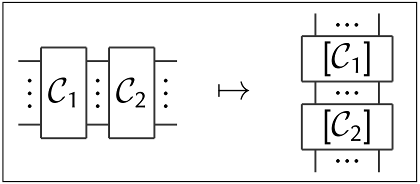
Standard Interpretation

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

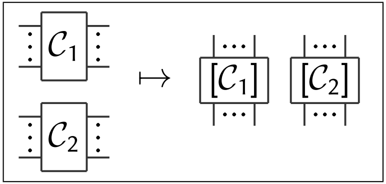
Example



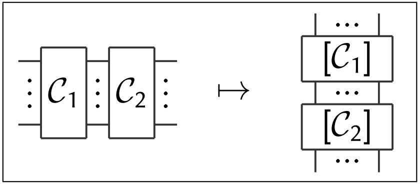
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



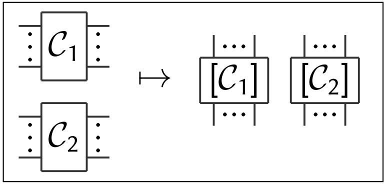
$\mathcal{C}_1$
$\mathcal{C}_2$
$\mapsto$
$[\mathcal{C}_1]$
$[\mathcal{C}_2]$



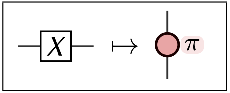
$\mathcal{C}_1$
$\mathcal{C}_2$
$\mapsto$
$[\mathcal{C}_1]$
$[\mathcal{C}_2]$



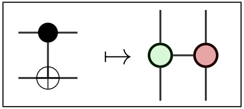
C1
C2
[C1]
[C2]

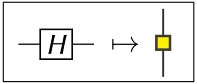


C1
C2
[C1]
[C2]

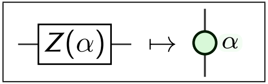


X
π

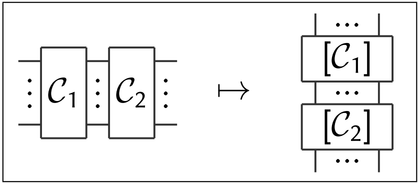


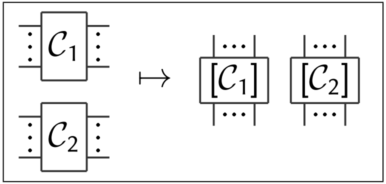


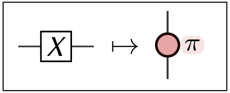
H

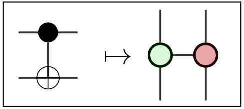


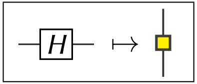
Z(α)
α

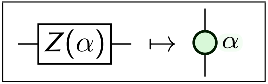

$\mathcal{C}_1$ $\mathcal{C}_2$ $\mapsto$ $[\mathcal{C}_1]$ $[\mathcal{C}_2]$

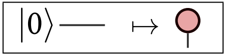

$\mathcal{C}_1$ $\mathcal{C}_2$ $\mapsto$ $[\mathcal{C}_1]$ $[\mathcal{C}_2]$

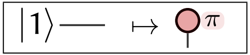

X $\mapsto$ π


$\mapsto$


H $\mapsto$


$Z(\alpha)$ $\mapsto$ α


$|0\rangle$ $\mapsto$


$|1\rangle$ $\mapsto$ π

Theorem (Universality)

We can represent any quantum operator using ZX-diagrams:

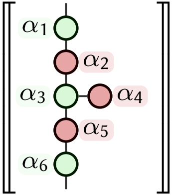
$$\forall f : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m},\ \exists \overset{n}{\underset{m}{\boxed{D}}} \in \mathbf{ZX},\ \left[\!\left[\overset{n}{\underset{m}{\boxed{D}}} \right]\!\right] = f$$

Theorem (Universality)

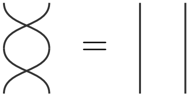
We can represent any quantum operator using ZX-diagrams:

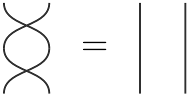
$$\forall f : \mathbb{C}^{2^n} \to \mathbb{C}^{2^m},\ \exists \overset{n}{\underset{m}{\boxed{D}}} \in \mathbf{ZX},\ [\![\overset{n}{\underset{m}{\boxed{D}}}]\!] = f$$

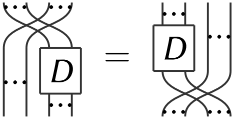
E.g. if $f : \mathbb{C}^2 \to \mathbb{C}^2$, $\exists \alpha_i$,



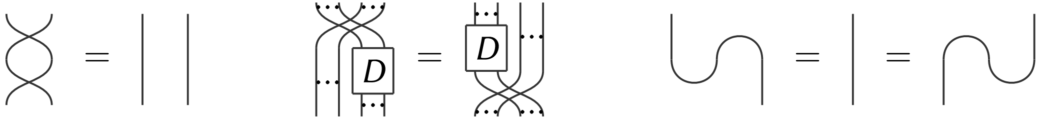
$= f$

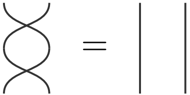


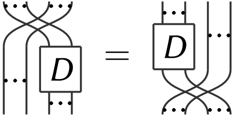


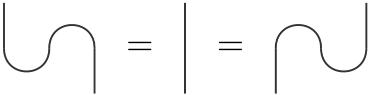

D
D

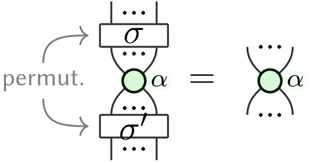
Equational Theory (the Backbone)

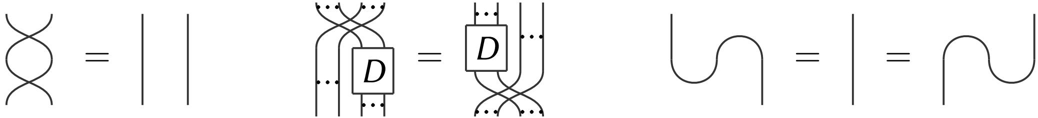


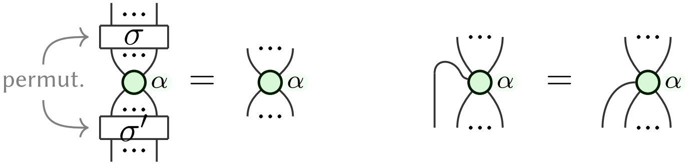



D
=
D

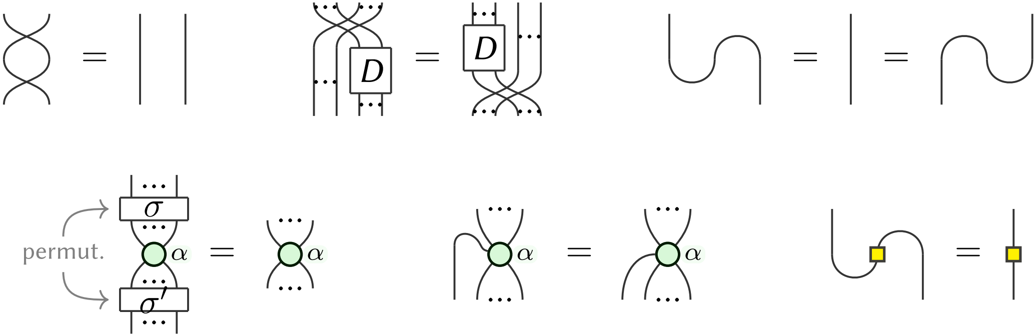


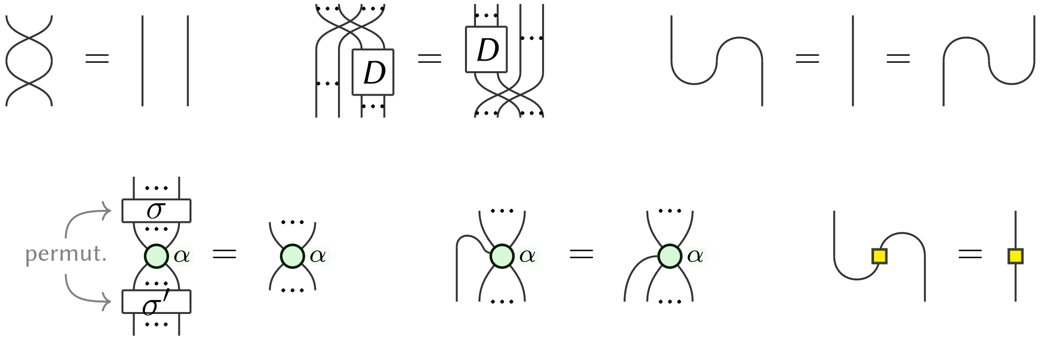

permut.
σ
α
σ'
=
α


=
D
=
D
=
=


permut.
σ
α
σ′
=
α
α
=
α

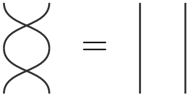
Equational Theory (the Backbone)

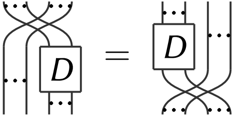


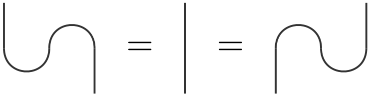


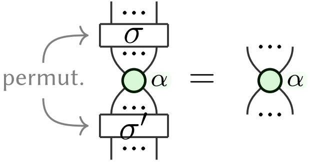
Only Connectivity Matters

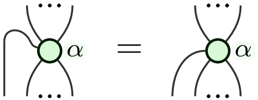
ZX-diagrams can be seen as open graphs. Any graph isomorphism is a valid derivation in the equational theories.

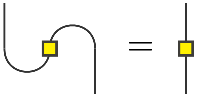








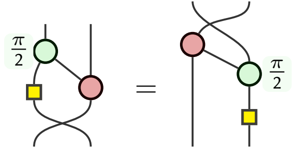


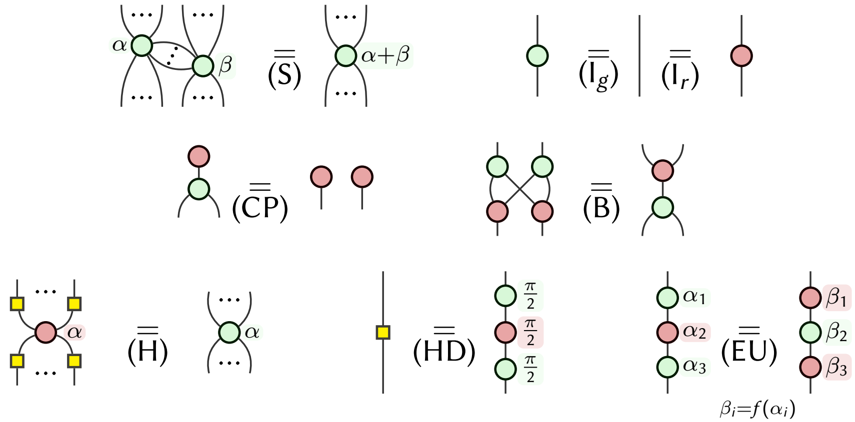


Only Connectivity Matters

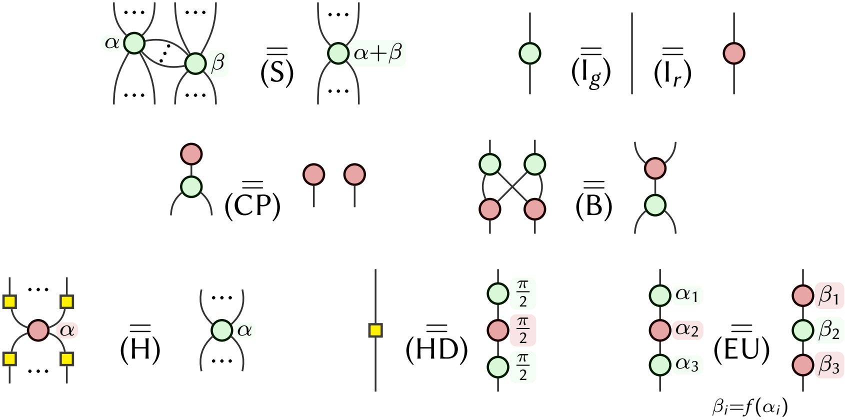
ZX-diagrams can be seen as open graphs. Any graph isomorphism is a valid derivation in the equational theories.

E.g.





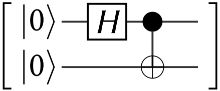
α
β
(S)
α+β
(I_g)
(I_r)
(CP)
(B)
α
(H)
α
(HD)
π/2
π/2
π/2
α1
α2
α3
(EU)
β1
β2
β3
βi=f(αi)



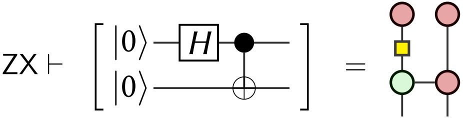
We write $\mathrm{ZX} \vdash D_1 = D_2$. Every colour-swapped rule holds.

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

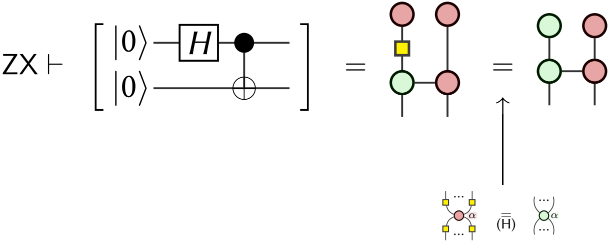
ZX $\vdash$



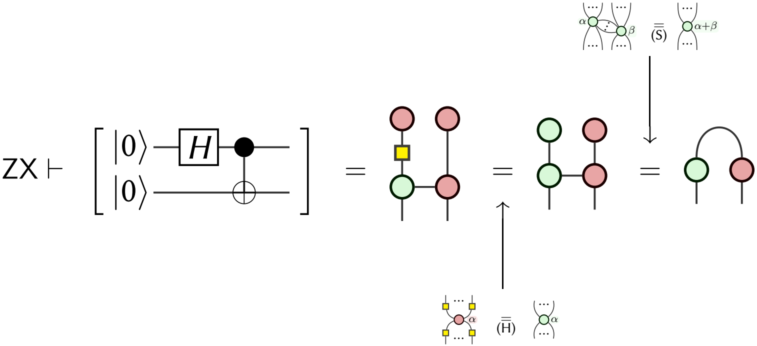
The EPR state: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$



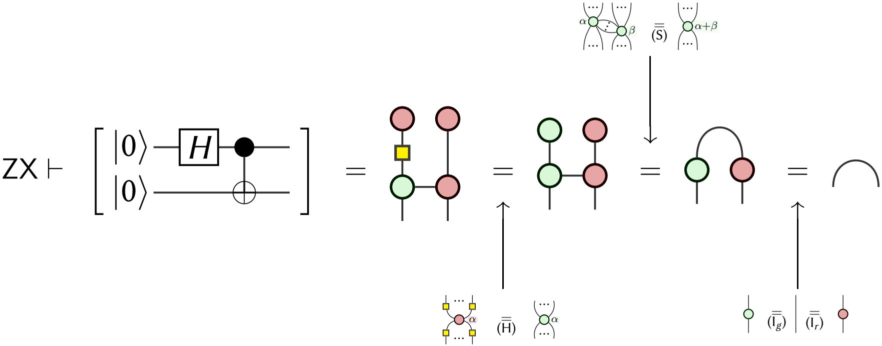
The EPR state: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$



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*:

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

Theorem [V.'19]

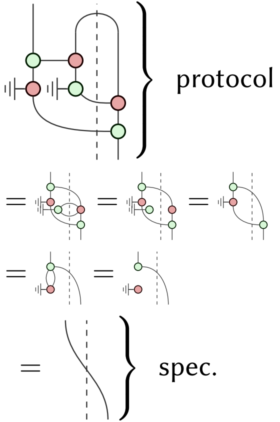
The language is *complete*:

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

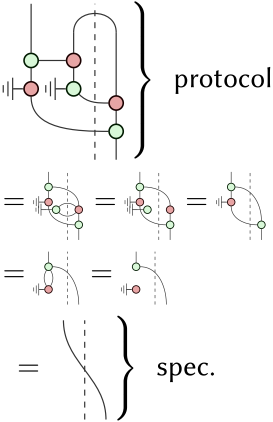
Previous/other completeness results:

- $\frac{\pi}{2}$-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]

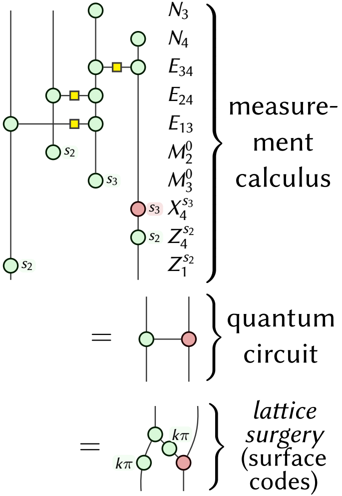
Verification



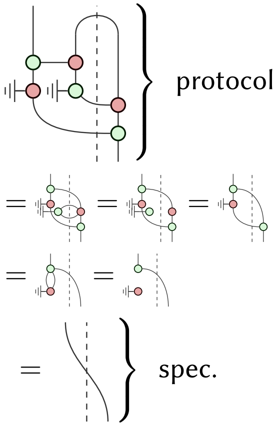
Verification



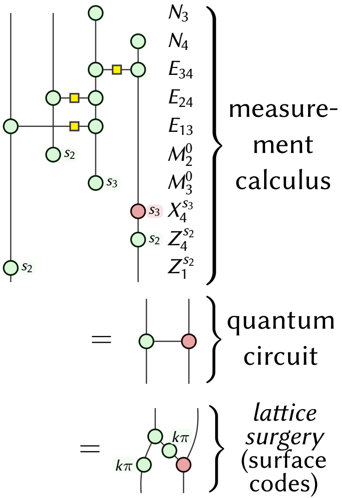
Unification



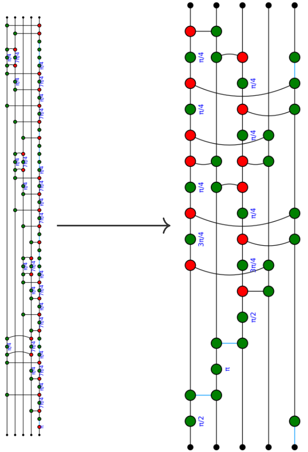
Verification



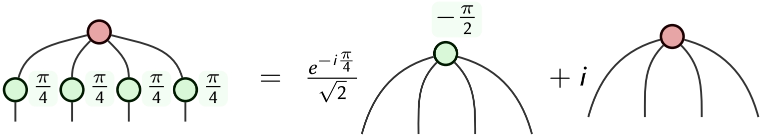
Unification

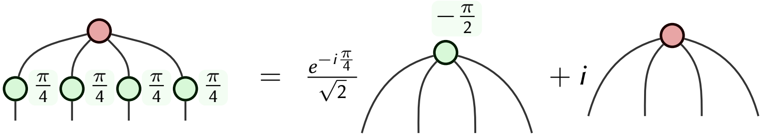


Optimisation

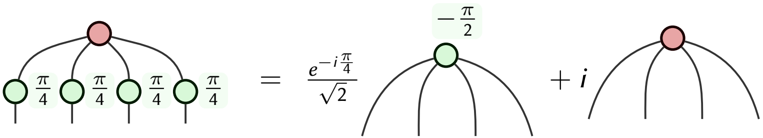


- Optimisation strategy
  - reduces Clifford diagrams to a (pseudo) normal form efficiently
  - can still be used in larger fragments

- Optimisation strategy
  - reduces Clifford diagrams to a (pseudo) normal form efficiently
  - can still be used in larger fragments
- 

- Optimisation strategy
  - reduces Clifford diagrams to a (pseudo) normal form efficiently
  - can still be used in larger fragments
- 

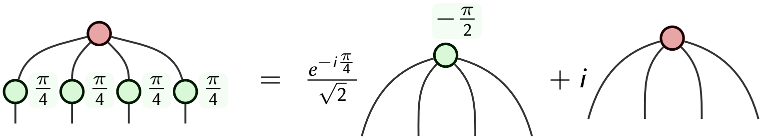
- Interleaving of optimisation and decomposition

- Optimisation strategy
  - reduces Clifford diagrams to a (pseudo) normal form efficiently
  - can still be used in larger fragments
- 

- Interleaving of optimisation and decomposition
- Scales exponentially with #non-Clifford spiders
- Scales polynomially with #qubits

Simulation [Kissinger,Wetering,V.'22]

- Optimisation strategy
  - reduces Clifford diagrams to a (pseudo) normal form efficiently
  - can still be used in larger fragments

- 

- Interleaving of optimisation and decomposition

- Scales exponentially with #non-Clifford spiders
- Scales polynomially with #qubits

- Simulation of non-trivial medium-scale circuits

- Quantum and probabilist effects $\Rightarrow$ hard to use usual debugging techniques

- Quantum and probabilist effects $\Rightarrow$ hard to use usual debugging techniques
- Formal methods to the rescue

- Quantum and probabilist effects $\Rightarrow$ hard to use usual debugging techniques
- Formal methods to the rescue
- Usual techniques may be adapted but come with new caveats

Conclusion

- Quantum and probabilist effects $\Rightarrow$ hard to use usual debugging techniques
- Formal methods to the rescue
- Usual techniques may be adapted but come with new caveats
- Interestingly possible to classically verify a quantum program

- Quantum and probabilist effects $\Rightarrow$ hard to use usual debugging techniques
- Formal methods to the rescue
- Usual techniques may be adapted but come with new caveats
- Interestingly possible to classically verify a quantum program
- *Formal methods for quantum algorithms: A Survey* [Chareton,Bardin,Lee,Valiron,V.,Xu'21]