Introduction à l'Informatique Quantique

Simon Perdrix

Inria, Mocqua/Loria

ROQ @ Montpellier – 2 Novembre 2021

Why a "quantum" processing of information?

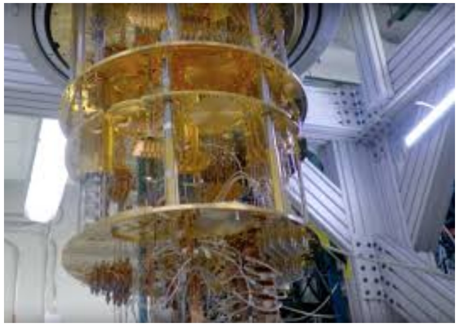
Some problems can be solved much more efficiently using quantum computers

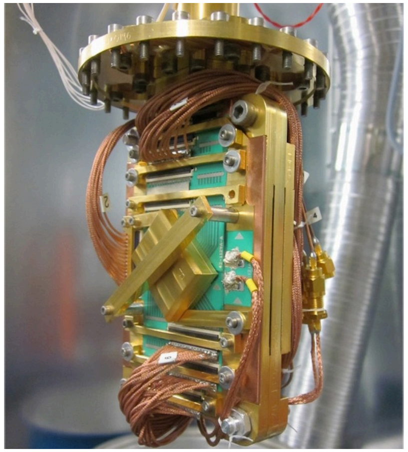
- Factorisation [Shor'94]
- Search [Grover'96]
- Backtracking [Montanaro'15]

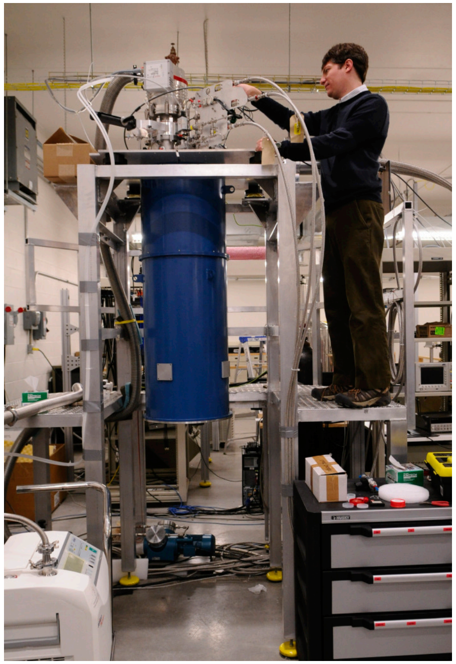
Why a "quantum" processing of information?

Some problems can be solved much more efficiently using quantum computers

- Factorisation [Shor'94]
- Search [Grover'96]
- Backtracking [Montanaro'15]



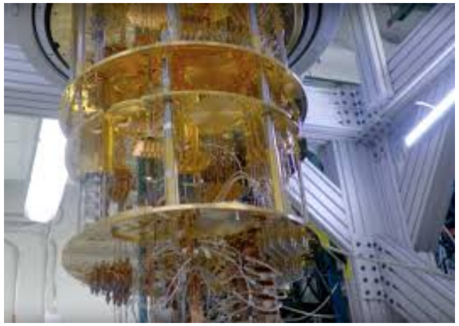


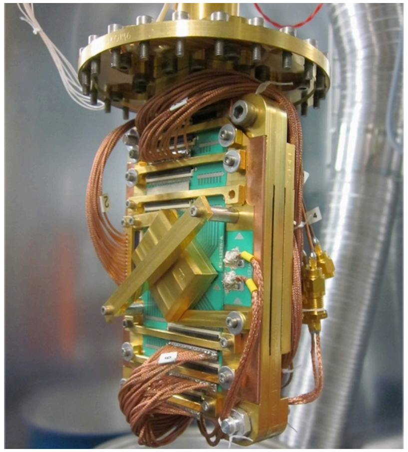


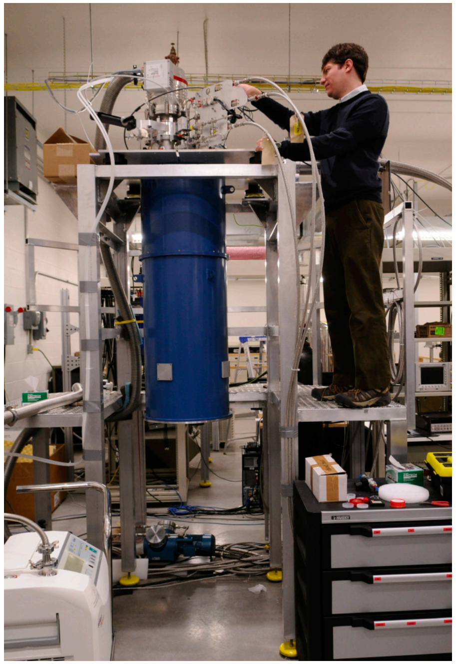
Why a "quantum" processing of information?

Some problems can be solved much more efficiently using quantum computers

- Factorisation [Shor'94]
- Search [Grover'96]
- Backtracking [Montanaro'15]







Main challenges:

- size of the memory (#qubits)
- quality of the qubits.

Towards Fault-Tolerant QC

- Quantum error correcting codes
- Threshold Theorem: correcting errors faster than they are created.

Physics: improve quality of
the quantum memory

CS: develop codes
with smaller threshold

Towards Fault-Tolerant QC

- Quantum error correcting codes

- Threshold Theorem: correcting errors faster than they are created.

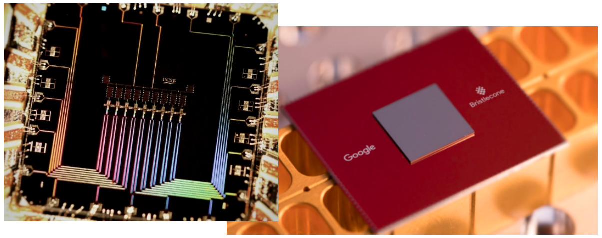
Physics: improve quality of
the quantum memory

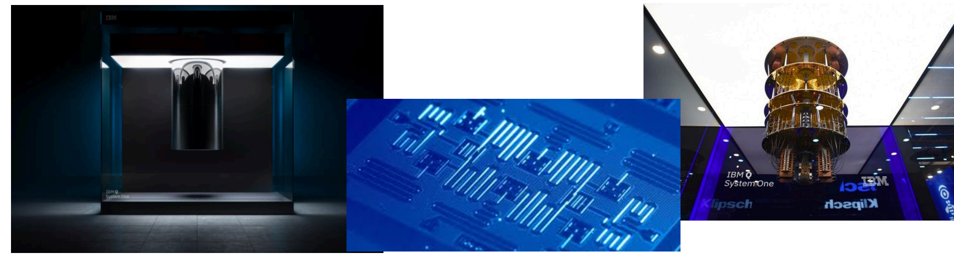
CS: develop codes
with smaller threshold

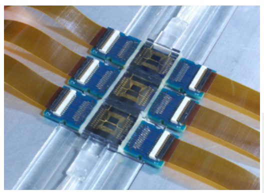
- *when they meet*: Large Scale Quantum computer (**LSQ**)

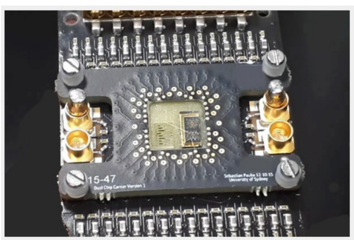
- *now*: Noisy Intermediate-Scale Quantum devices (**NISQ**)

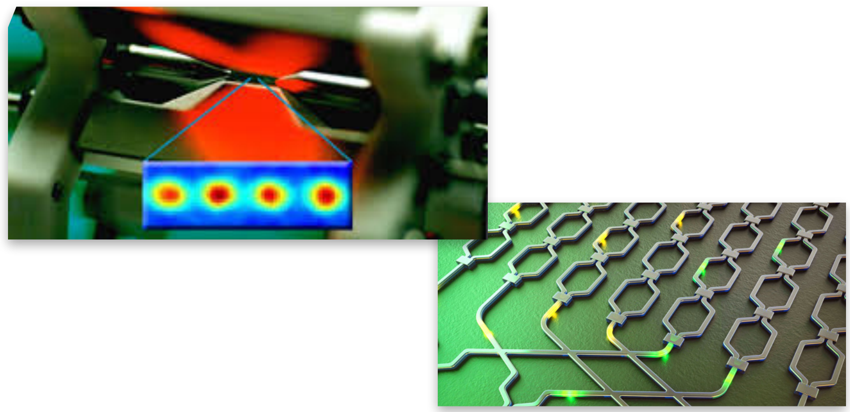
Noisy Intermediate-Scale Quantum (NISQ) devices

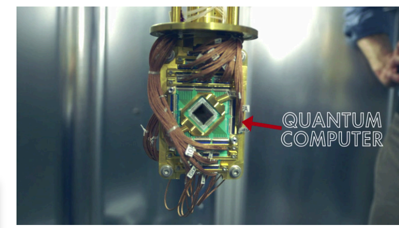








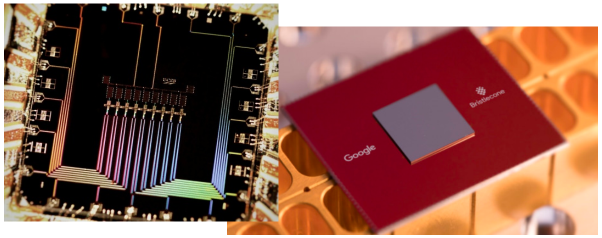


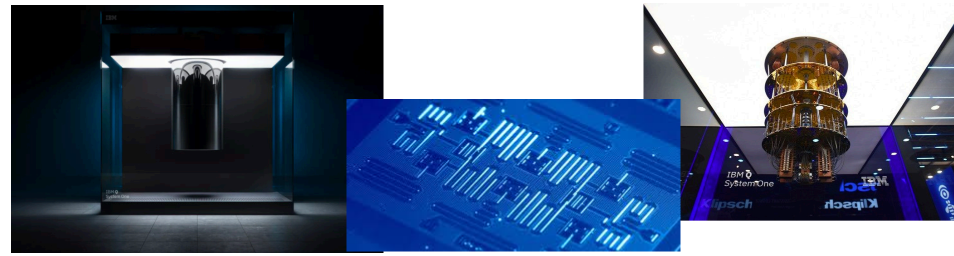


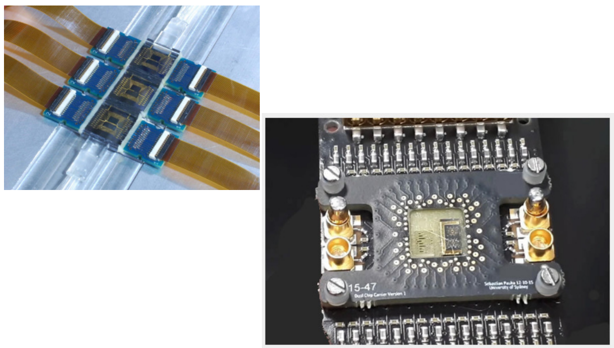
HPC simulation?

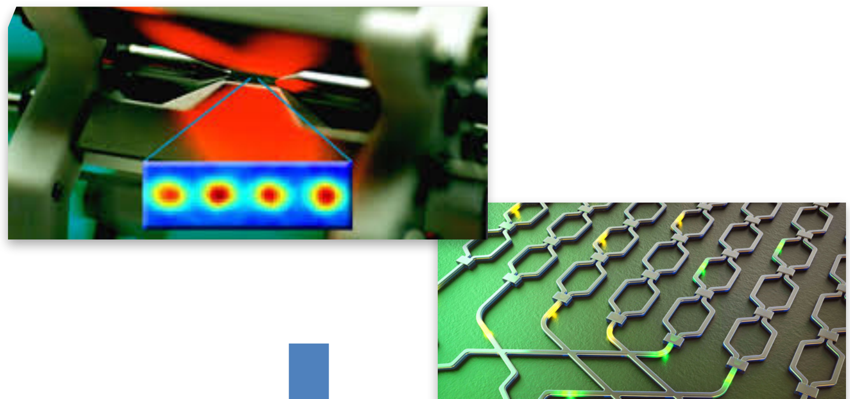
(up to ~50 high quality qubits.)

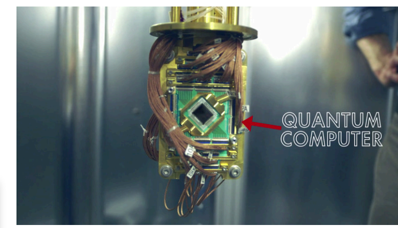
Noisy Intermediate-Scale Quantum (NISQ) devices







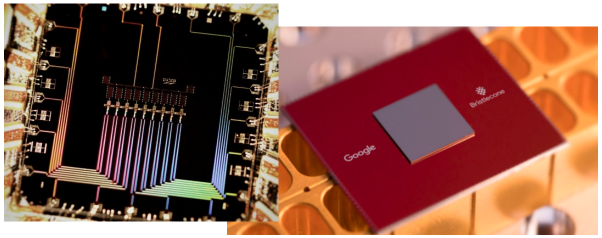


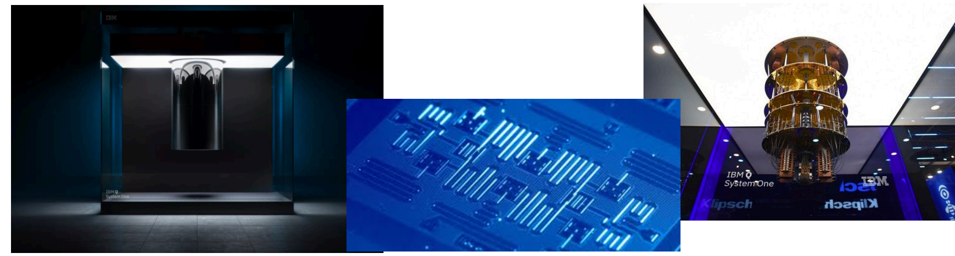


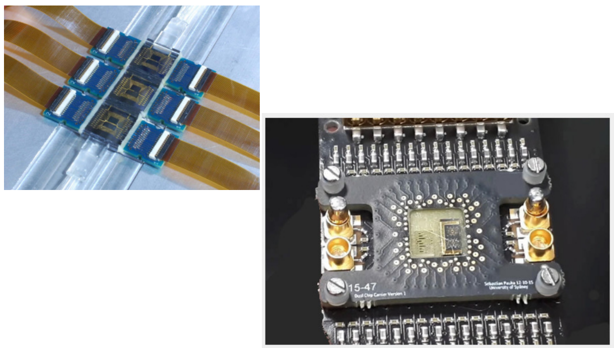
HPC simulation?

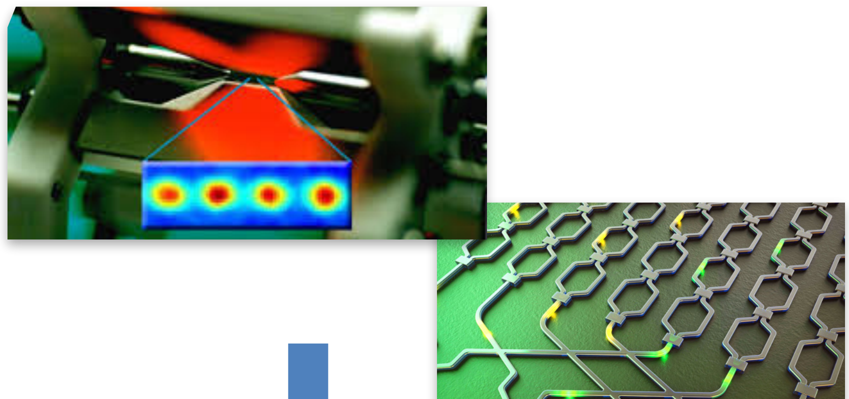
(up to ~50 high quality qubits.)

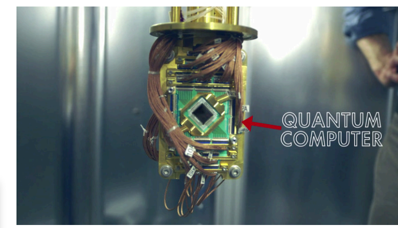
Noisy Intermediate-Scale Quantum (NISQ) devices









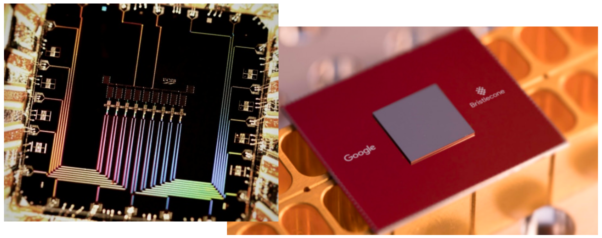


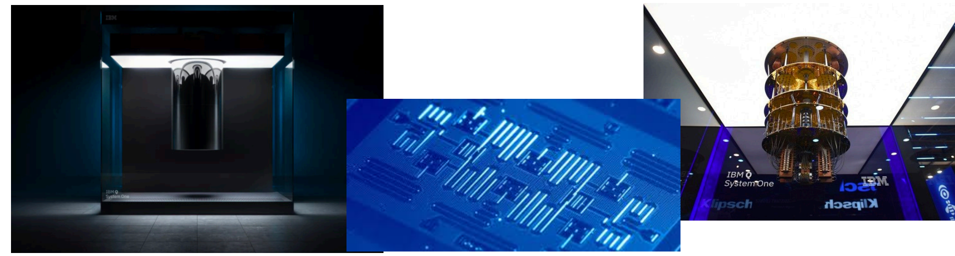
HPC simulation?

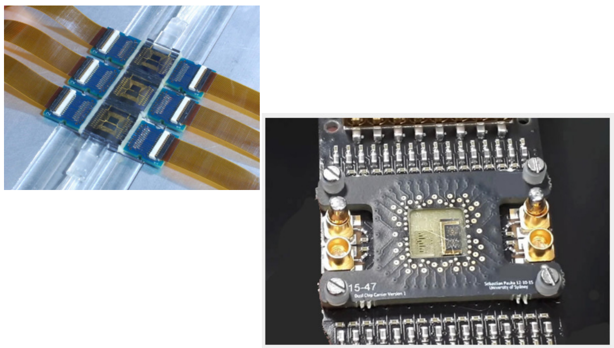
(up to ~50 high quality qubits.)

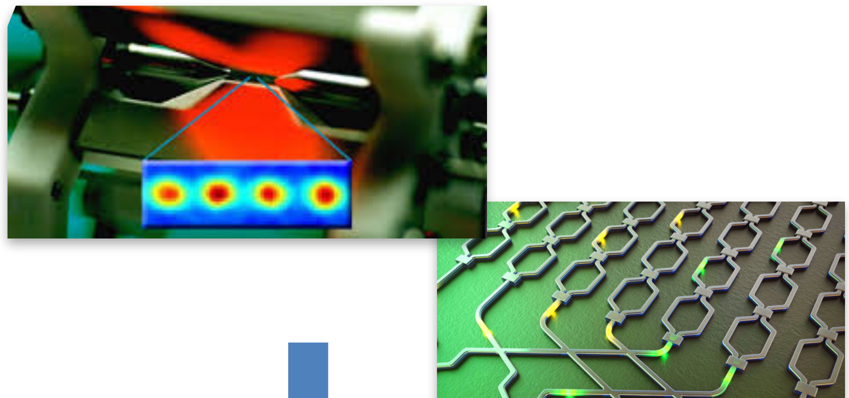
Quantum supremacy:
classical/quantum separation

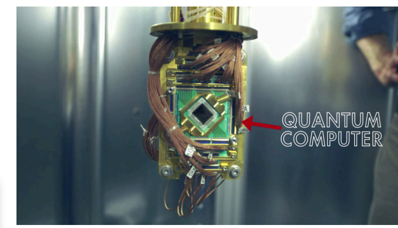
Noisy Intermediate-Scale Quantum (NISQ) devices











HPC simulation?

(up to ~50 high quality qubits.)

Quantum supremacy: classical/quantum separation

Quantum usefulness: beating classical computers in practice.

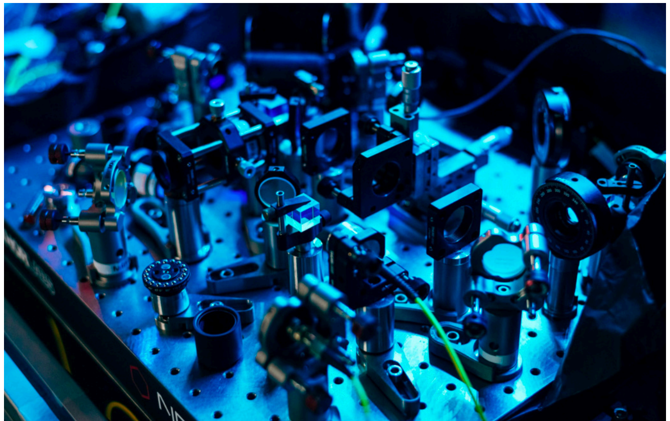
Why a "quantum" processing of information?

Some problems can be solved much more efficiently using quantum computers

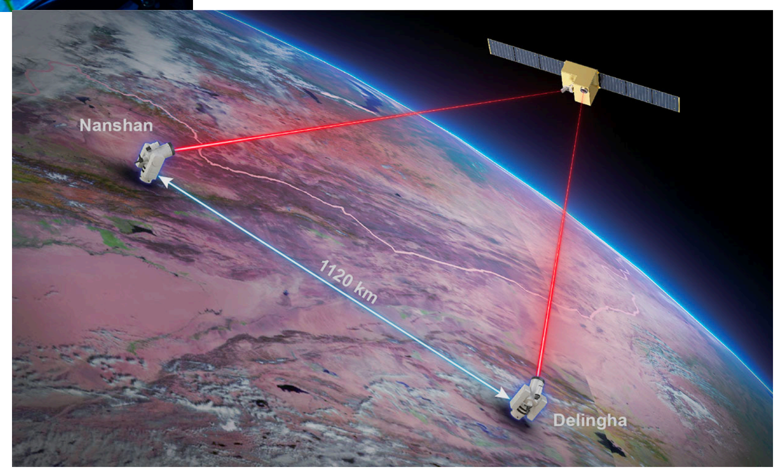
- Factorisation [Shor’94]
- Search [Grover’96]
- Backtracking [Montanaro’15]

Quantum Cryptography: unconditionally secured communications

- Quantum key distribution [BB84]




IDQ


Nanshan
1120 km
Delingha

Outline

Postulates

Quantum Circuits

1st Algo: Detecting fake coins with a quantum scale

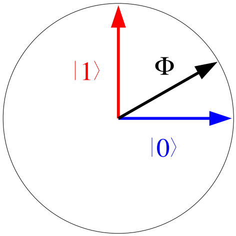
2nd Algo: Deutsch-Jozsa

Postulate 1: Quantum states

- Classical bit: $b \in \{0, 1\}$
- Quantum bit (**qubit**): $|\varphi\rangle \in \mathbb{C}^2$,

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

with $|\alpha|^2 + |\beta|^2 = 1$



Examples:

$$|0\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$$

Register of qubits

Definition. The state of a n-qubit register is a unit vector of $\mathbb{C}^{2^n}$.

$$|\varphi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \text{ with } || \, |\varphi\rangle \, ||^2 = \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$$

Examples:

$$\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$

$$\frac{1}{\sqrt{3}}(|00\rangle + i\,|01\rangle + |11\rangle)$$

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Postulate 2: composed system

Definition. Let $|\varphi_1\rangle$ be a n-qubit state and $|\varphi_2\rangle$ be a m-qubit state, the $(n+m)$-qubit state of the composed system is

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

where $\cdot \otimes \cdot$ is bilinear and $\forall x \in \{0,1\}^n$, $\forall y \in \{0,1\}^m$, $|x\rangle \otimes |y\rangle = |xy\rangle$.

Examples:

1. $|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle\otimes|0\rangle - |0\rangle\otimes|1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$
2. $\frac{|01\rangle + |11\rangle}{\sqrt{2}} \quad = \quad ? \otimes ?$
3. $\frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad = \quad ? \otimes ?$

Postulate 2: composed system

Definition. Let $|\varphi_1\rangle$ be a n-qubit state and $|\varphi_2\rangle$ be a m-qubit state, the $(n+m)$-qubit state of the composed system is

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

where $\cdot \otimes \cdot$ is bilinear and $\forall x \in \{0,1\}^n$, $\forall y \in \{0,1\}^m$, $|x\rangle \otimes |y\rangle = |xy\rangle$.

Examples:

1. $|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$
2. $\frac{|01\rangle + |11\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle$
3. $\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \; ? \otimes ?$

Postulate 2: composed system

Definition. Let $|\varphi_1\rangle$ be a n-qubit state and $|\varphi_2\rangle$ be a m-qubit state, the $(n+m)$-qubit state of the composed system is

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

where $\cdot \otimes \cdot$ is bilinear and $\forall x \in \{0,1\}^n$, $\forall y \in \{0,1\}^m$, $|x\rangle \otimes |y\rangle = |xy\rangle$.

Examples:

1. $|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$
2. $\frac{|01\rangle + |11\rangle}{\sqrt{2}} \quad = \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle$
3. $$\begin{aligned} \frac{|00\rangle + |11\rangle}{\sqrt{2}} &= (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) \\ &= ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \\ &\quad \Longrightarrow\ ad = 0 \ \Longrightarrow\ ac = 0 \text{ or } bd = 0 \quad \text{impossible} \end{aligned}$$

Postulate 2: composed system

Definition. Let $|\varphi_1\rangle$ be a n-qubit state and $|\varphi_2\rangle$ be a m-qubit state, the $(n+m)$-qubit state of the composed system is

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

where $\cdot \otimes \cdot$ is bilinear and $\forall x \in \{0,1\}^n$, $\forall y \in \{0,1\}^m$, $|x\rangle \otimes |y\rangle = |xy\rangle$.

Examples:

1. $|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$
2. $\frac{|01\rangle + |11\rangle}{\sqrt{2}} \quad = \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle$
3. $$\begin{aligned} \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad &\neq \quad (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) \\ &= \quad ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \\ &\quad \implies ad = 0 \implies ac = 0 \text{ or } bd = 0 \quad \text{impossible} \end{aligned}$$

Postulate 2: composed system

Definition. Let $|\varphi_1\rangle$ be a n-qubit state and $|\varphi_2\rangle$ be a m-qubit state, the $(n+m)$-qubit state of the composed system is

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

where $\cdot \otimes \cdot$ is bilinear and $\forall x \in \{0,1\}^n$, $\forall y \in \{0,1\}^m$, $|x\rangle \otimes |y\rangle = |xy\rangle$.

Examples:

1. $|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle\otimes|0\rangle - |0\rangle\otimes|1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$
2. $\frac{|01\rangle + |11\rangle}{\sqrt{2}} \quad = \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle$
3. $$\begin{aligned} \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad &\neq \quad (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) \\ &= \quad ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \\ &\quad \implies ad = 0 \implies ac = 0 \text{ or } bd = 0 \quad \text{impossible} \end{aligned}$$

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ **is an entangled state.**

Postulate 3: Measurement

$$\alpha |0\rangle + \beta |1\rangle \xrightarrow{|\alpha|^2} |0\rangle \quad \textit{with classical outcome } 0$$

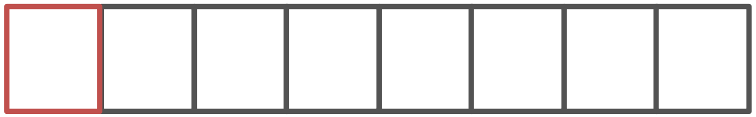
$$\alpha |0\rangle + \beta |1\rangle \xrightarrow{|\beta|^2} |1\rangle \quad \textit{with classical outcome } 1$$

Measurement is **probabilistic** and **irreversible**.

Measure $\Longrightarrow$ Interaction $\Longrightarrow$ Transformation

Partial Measurement

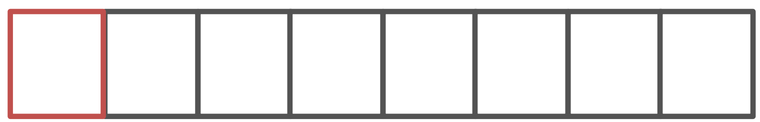
$$
\begin{aligned}
|\varphi\rangle &= \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = \sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |0x\rangle + \sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |1x\rangle \\
&= |0\rangle \otimes \left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |x\rangle \right) + |1\rangle \otimes \left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |x\rangle \right)
\end{aligned}
$$



$\frac{1}{2}$

Partial Measurement

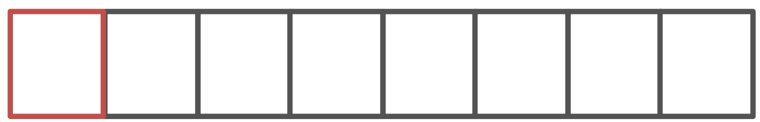
$$
\begin{aligned}
|\varphi\rangle &= \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = \sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |0x\rangle + \sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |1x\rangle \\
&= |0\rangle \otimes \left(\underbrace{\sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |x\rangle}_{\alpha|\varphi_0\rangle} \right) + |1\rangle \otimes \left(\underbrace{\sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |x\rangle}_{\beta|\varphi_1\rangle} \right)
\end{aligned}
$$



$\frac{1}{2}$

Partial Measurement

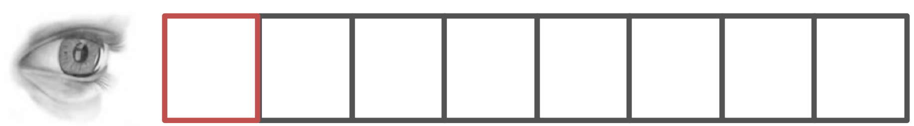
$$
\begin{aligned}
|\varphi\rangle &= \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = \sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |0x\rangle + \sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |1x\rangle \\
&= |0\rangle \otimes \underbrace{\left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |x\rangle \right)}_{\alpha|\varphi_0\rangle} + |1\rangle \otimes \underbrace{\left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |x\rangle \right)}_{\beta|\varphi_1\rangle} = \alpha|0\rangle \otimes |\varphi_0\rangle + \beta|1\rangle \otimes |\varphi_1\rangle
\end{aligned}
$$



$\frac{1}{2}$

Partial Measurement

$$
\begin{aligned}
|\varphi\rangle &= \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = \sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |0x\rangle + \sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |1x\rangle \\
&= |0\rangle \otimes \underbrace{\left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{0x} |x\rangle \right)}_{\alpha|\varphi_0\rangle} + |1\rangle \otimes \underbrace{\left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{1x} |x\rangle \right)}_{\beta|\varphi_1\rangle} = \alpha|0\rangle \otimes |\varphi_0\rangle + \beta|1\rangle \otimes |\varphi_1\rangle
\end{aligned}
$$



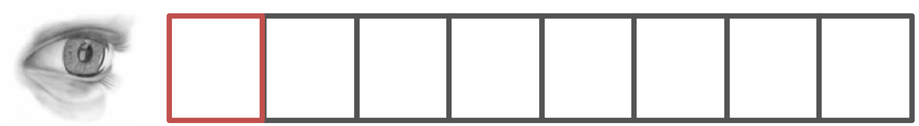
$$
\alpha|0\rangle \otimes |\varphi_0\rangle + \beta|1\rangle \otimes |\varphi_1\rangle \xrightarrow{|\alpha|^2} |0\rangle \otimes |\varphi_0\rangle \quad \textit{classical outcome } 0
$$

$$
\alpha|0\rangle \otimes |\varphi_0\rangle + \beta|1\rangle \otimes |\varphi_1\rangle \xrightarrow{|\beta|^2} |1\rangle \otimes |\varphi_1\rangle \quad \textit{classical outcome } 1
$$

Partial Measurement

$$|\varphi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = \sum_{x\in\{0,1\}^{n-1}} \alpha_{0x}|0x\rangle + \sum_{x\in\{0,1\}^{n-1}} \alpha_{1x}|1x\rangle$$

$$= |0\rangle \otimes \underbrace{\left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{0x}|x\rangle\right)}_{\alpha|\varphi_0\rangle} + |1\rangle \otimes \underbrace{\left(\sum_{x\in\{0,1\}^{n-1}} \alpha_{1x}|x\rangle\right)}_{\beta|\varphi_1\rangle} = \alpha|0\rangle\otimes|\varphi_0\rangle + \beta|1\rangle\otimes|\varphi_1\rangle$$



$$\alpha|0\rangle\otimes|\varphi_0\rangle + \beta|1\rangle\otimes|\varphi_1\rangle \xrightarrow{|\alpha|^2} |0\rangle\otimes|\varphi_0\rangle$$ *classical outcome* 0

$$\alpha|0\rangle\otimes|\varphi_0\rangle + \beta|1\rangle\otimes|\varphi_1\rangle \xrightarrow{|\beta|^2} |1\rangle\otimes|\varphi_1\rangle$$ *classical outcome* 1

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}} \xrightarrow{\frac{1}{2}} |0\rangle\otimes|0\rangle$$ *classical outcome* 0

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}} \xrightarrow{\frac{1}{2}} |1\rangle\otimes|1\rangle$$ *classical outcome* 1

Postulate 4: Closed System, a Unitary Evolution

Definition. An isolated system evolves

- linearly i.e., $U(\alpha\,|\varphi\rangle + \beta\,|\psi\rangle) = \alpha U(|\varphi\rangle) + \beta U(|\psi\rangle)$
- preserving the normalisation condition i.e., $||U(|\varphi\rangle)|| = ||\,|\varphi\rangle\,||$

Example:

$$\begin{array}{cccc} H & : & |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ & & |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

$H(H(|0\rangle)) =$

Postulate 4: Closed System, a Unitary Evolution

Definition. An isolated system evolves

- linearly i.e., $U(\alpha|\varphi\rangle + \beta|\psi\rangle) = \alpha U(|\varphi\rangle) + \beta U(|\psi\rangle)$
- preserving the normalisation condition i.e., $||U(|\varphi\rangle)|| = ||\,|\varphi\rangle\,||$

Example:

$$\begin{array}{rclcl} H & : & |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ & & |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

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

Postulate 4: Closed System, a Unitary Evolution

Definition. An isolated system evolves

- linearly i.e., $U(\alpha|\varphi\rangle + \beta|\psi\rangle) = \alpha U(|\varphi\rangle) + \beta U(|\psi\rangle)$
- preserving the normalisation condition i.e., $||U(|\varphi\rangle)|| = || \, |\varphi\rangle \, ||$

Example:

$$\begin{array}{cccc} H & : & |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ & & |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

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

Postulate 4: Closed System, a Unitary Evolution

Definition. An isolated system evolves

- linearly i.e., $U(\alpha\,|\varphi\rangle + \beta\,|\psi\rangle) = \alpha U(|\varphi\rangle) + \beta U(|\psi\rangle)$
- preserving the normalisation condition i.e., $||U(|\varphi\rangle)|| = ||\,|\varphi\rangle\,||$

Example:

$$\begin{array}{ccccc} H & : & |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ & & |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

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

Postulate 4: Closed System, a Unitary Evolution

Definition. An isolated system evolves

- linearly i.e., $U(\alpha\,|\varphi\rangle + \beta\,|\psi\rangle) = \alpha U(|\varphi\rangle) + \beta U(|\psi\rangle)$
- preserving the normalisation condition i.e., $||U(|\varphi\rangle)|| = ||\,|\varphi\rangle\,||$

Example:

$$
\begin{array}{cccccc}
H & : & |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
 & & |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}}
\end{array}
$$

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

Postulate 4: Closed System, a Unitary Evolution

Definition. An isolated system evolves

- linearly i.e., $U(\alpha\,|\varphi\rangle + \beta\,|\psi\rangle) = \alpha U(|\varphi\rangle) + \beta U(|\psi\rangle)$
- preserving the normalisation condition i.e., $||U(|\varphi\rangle)|| = ||\,|\varphi\rangle\,||$

Example:

$$\begin{array}{cccc} H & : & |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ & & |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

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

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

More Unitary Evolutions

$$X : \begin{array}{rcl} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{array}$$

$$Z : \begin{array}{rcl} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{array}$$

$$H : \begin{array}{rcl} |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

$$R_z(\theta) : \begin{array}{rcl} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & e^{i\theta}|1\rangle \end{array}$$

$$CNot : \begin{array}{rcl} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$$

Parallel Composition

If U is applied to a subregister, and V is applied on the rest of the register, the overall evolution is $U \otimes V$ with:

$$(U \otimes V)(|\varphi\rangle \otimes |\psi\rangle) = (U |\varphi\rangle) \otimes (V |\psi\rangle)$$

Example:
$(H \otimes H) |01\rangle =$

When the state is entangled, one can use linearity:

$$\begin{aligned} (U \otimes V)\frac{|00\rangle+|11\rangle}{\sqrt{2}} &= \frac{(U\otimes V)|00\rangle+(U\otimes V)|11\rangle}{\sqrt{2}} \\ &= \frac{(U|0\rangle)\otimes(V|0\rangle)+(U|1\rangle)\otimes(V|1\rangle)}{\sqrt{2}} \end{aligned}$$

Parallel Composition

If U is applied to a subregister, and V is applied on the rest of the register, the overall evolution is $U \otimes V$ with:

$$(U \otimes V)(|\varphi\rangle \otimes |\psi\rangle) = (U\,|\varphi\rangle) \otimes (V\,|\psi\rangle)$$

Example:
$(H \otimes H)\,|01\rangle = (H\,|0\rangle) \otimes (H\,|1\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2}$

When the state is entangled, one can use linearity:

$$\begin{aligned} (U \otimes V)\frac{|00\rangle+|11\rangle}{\sqrt{2}} &= \frac{(U\otimes V)|00\rangle+(U\otimes V)|11\rangle}{\sqrt{2}} \\ &= \frac{(U|0\rangle)\otimes(V|0\rangle)+(U|1\rangle)\otimes(V|1\rangle)}{\sqrt{2}} \end{aligned}$$

Parallel Composition

If U is applied to a subregister, and V is applied on the rest of the register, the overall evolution is $U \otimes V$ with:

$$(U \otimes V)(|\varphi\rangle \otimes |\psi\rangle) = (U|\varphi\rangle) \otimes (V|\psi\rangle)$$

Example:
$(H \otimes H)|01\rangle = (H|0\rangle) \otimes (H|1\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2}$

When the state is entangled, one can use linearity:

$$\begin{aligned}(U \otimes V)\tfrac{|00\rangle+|11\rangle}{\sqrt{2}} &= \tfrac{(U\otimes V)|00\rangle+(U\otimes V)|11\rangle}{\sqrt{2}} \\ &= \tfrac{(U|0\rangle)\otimes(V|0\rangle)+(U|1\rangle)\otimes(V|1\rangle)}{\sqrt{2}}\end{aligned}$$

Matrix Notations

- $\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \qquad \leftrightarrow \qquad \begin{bmatrix} \alpha_{0\ldots 0} \\ \vdots \\ \alpha_{1\ldots 1} \end{bmatrix}$
- A matrix U is unitary iff $U^\dagger U = UU^\dagger = I$, where $U^\dagger$ is the adjoint of U
- $\begin{bmatrix} a & c \\ b & d \end{bmatrix} \otimes U = \begin{bmatrix} aU & cU \\ bU & dU \end{bmatrix}$

Dirac Notations

The state space of a quantum system is a Hilbert space $\mathcal{H}$ equipped with a inner product $\langle ., . \rangle$

A Hilbert space $\mathcal{H}$ of finite dimension d is isomorphic to $\mathbb{C}^d$ equipped with the canonical inner product $\langle \vec{\varphi}, \vec{\psi} \rangle = \vec{\varphi}^\dagger \vec{\psi} = \begin{bmatrix} \varphi_1^* & \dots & \varphi_d^* \end{bmatrix} . \begin{bmatrix} \psi_1 \\ \vdots \\ \psi_d \end{bmatrix}$

$\langle \varphi | := | \varphi \rangle^\dagger$

'bra'

$|\psi\rangle$

'ket'

Outline

Postulates

Quantum Circuits

1st Algo: Detecting fake coins with a quantum scale

2nd Algo: Deutsch-Jozsa

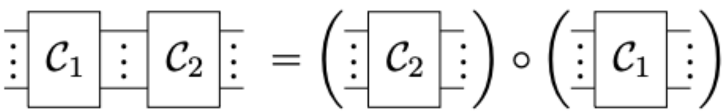
Representing quantum evolutions

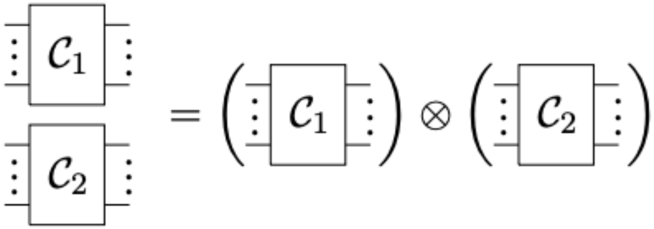
$$\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\right) \circ \left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) \circ \left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}\right)$$

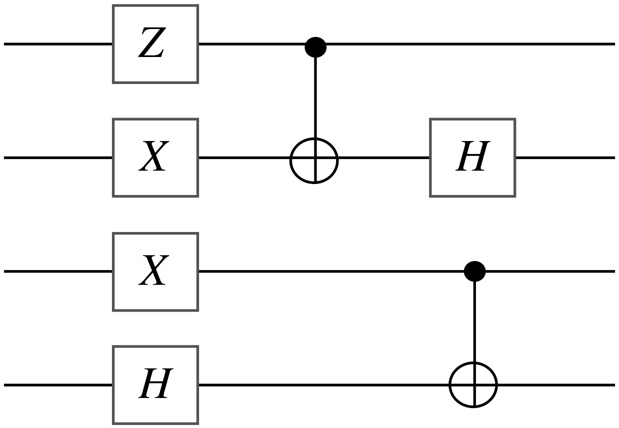
Representing quantum evolutions

$$(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}) \circ (\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) \circ (\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix})$$

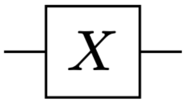
Quantum circuits: 2D representation







Quantum Gates

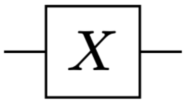


$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

$$|x\rangle \mapsto |1 - x\rangle$$

Quantum Gates

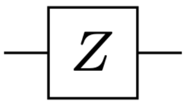


$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

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

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

$$|x\rangle \mapsto |1-x\rangle$$



$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$|0\rangle \mapsto |0\rangle$$

$$|1\rangle \mapsto -|1\rangle$$

$$|x\rangle \mapsto (-1)^x|x\rangle$$

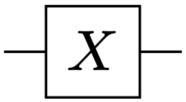
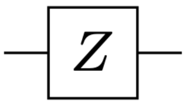
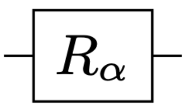
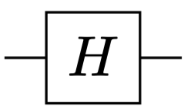
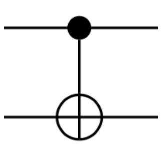
Quantum Gates

$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\vert 0\rangle \mapsto \vert 1\rangle$ $\vert 1\rangle \mapsto \vert 0\rangle$	$\vert x\rangle \mapsto \vert 1-x\rangle$
$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\vert 0\rangle \mapsto \vert 0\rangle$ $\vert 1\rangle \mapsto -\vert 1\rangle$	$\vert x\rangle \mapsto (-1)^x \vert x\rangle$
$-\boxed{R_\alpha}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$	$\vert 0\rangle \mapsto \vert 0\rangle$ $\vert 1\rangle \mapsto e^{i\alpha}\vert 1\rangle$	$\vert x\rangle \mapsto e^{ix\alpha}\vert x\rangle$

Quantum Gates

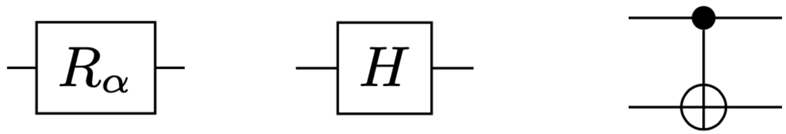
$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\lvert 0\rangle \mapsto \lvert 1\rangle$ $\lvert 1\rangle \mapsto \lvert 0\rangle$	$\lvert x\rangle \mapsto \lvert 1-x\rangle$
$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\lvert 0\rangle \mapsto \lvert 0\rangle$ $\lvert 1\rangle \mapsto -\lvert 1\rangle$	$\lvert x\rangle \mapsto (-1)^x\lvert x\rangle$
$-\boxed{R_\alpha}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$	$\lvert 0\rangle \mapsto \lvert 0\rangle$ $\lvert 1\rangle \mapsto e^{i\alpha}\lvert 1\rangle$	$\lvert x\rangle \mapsto e^{ix\alpha}\lvert x\rangle$
$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$\lvert 0\rangle \mapsto \frac{\lvert 0\rangle + \lvert 1\rangle}{\sqrt{2}}$ $\lvert 1\rangle \mapsto \frac{\lvert 0\rangle - \lvert 1\rangle}{\sqrt{2}}$	$\lvert x\rangle \mapsto \frac{\lvert 0\rangle + (-1)^x\lvert 1\rangle}{\sqrt{2}}$

Quantum Gates

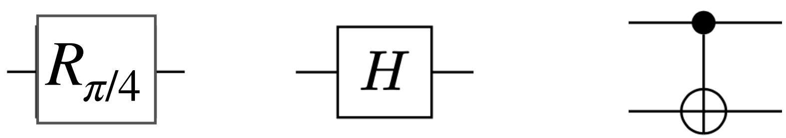
	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\lvert 0\rangle \mapsto \lvert 1\rangle$ $\lvert 1\rangle \mapsto \lvert 0\rangle$	$\lvert x\rangle \mapsto \lvert 1-x\rangle$
	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\lvert 0\rangle \mapsto \lvert 0\rangle$ $\lvert 1\rangle \mapsto -\lvert 1\rangle$	$\lvert x\rangle \mapsto (-1)^x\lvert x\rangle$
	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$	$\lvert 0\rangle \mapsto \lvert 0\rangle$ $\lvert 1\rangle \mapsto e^{i\alpha}\lvert 1\rangle$	$\lvert x\rangle \mapsto e^{ix\alpha}\lvert x\rangle$
	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$\lvert 0\rangle \mapsto \frac{\lvert 0\rangle + \lvert 1\rangle}{\sqrt{2}}$ $\lvert 1\rangle \mapsto \frac{\lvert 0\rangle - \lvert 1\rangle}{\sqrt{2}}$	$\lvert x\rangle \mapsto \frac{\lvert 0\rangle + (-1)^x\lvert 1\rangle}{\sqrt{2}}$
	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	$\lvert 00\rangle \mapsto \lvert 00\rangle$ $\lvert 01\rangle \mapsto \lvert 01\rangle$ $\lvert 10\rangle \mapsto \lvert 11\rangle$ $\lvert 11\rangle \mapsto \lvert 10\rangle$	$\lvert x, y\rangle \mapsto \lvert x, x \oplus y\rangle$ XOR

Universality

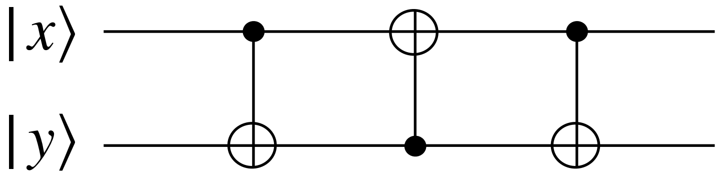
Universality: Any unitary transformation acting on a finite number of qubits can be represented by a quantum circuit which gates are :



Approx. Universality: Any unitary transformation acting on a finite number of qubits can be approximated by a quantum circuit which gates are :

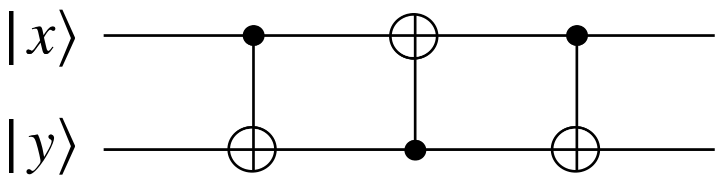


Quantum Circuits — Examples



$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

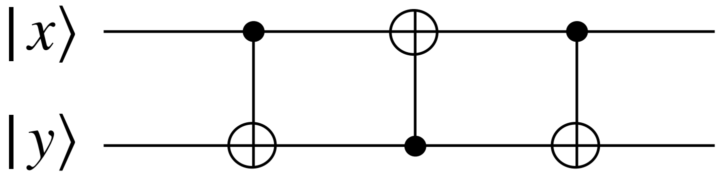
Quantum Circuits — Examples



$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$|x, y\rangle \mapsto |x, x \oplus y\rangle$$

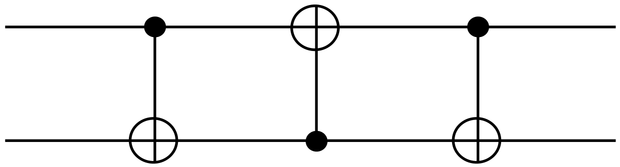
Quantum Circuits — Examples



$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$\begin{aligned} |x, y\rangle &\mapsto |x, x \oplus y\rangle \\ &\mapsto |x \oplus (x \oplus y), x \oplus y\rangle = |y, x \oplus y\rangle \end{aligned}$$

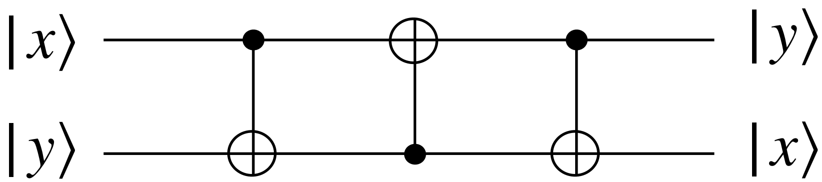
Quantum Circuits — Examples

$$\begin{array}{c} |x\rangle \\ |y\rangle \end{array}$$ 

$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$\begin{aligned} |x, y\rangle &\mapsto |x, x \oplus y\rangle \\ &\mapsto |x \oplus (x \oplus y), x \oplus y\rangle = |y, x \oplus y\rangle \\ &\mapsto |y, y \oplus (x \oplus y)\rangle = |y, x\rangle \end{aligned}$$

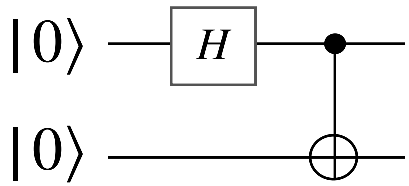
Quantum Circuits — Examples



$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$\begin{aligned}
|x, y\rangle &\mapsto |x, x \oplus y\rangle \\
&\mapsto |x \oplus (x \oplus y), x \oplus y\rangle = |y, x \oplus y\rangle \\
&\mapsto |y, y \oplus (x \oplus y)\rangle = |y, x\rangle
\end{aligned}$$

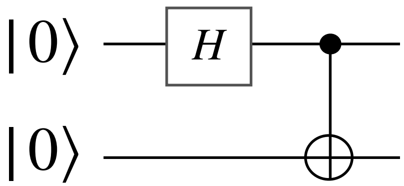
Quantum Circuits — Examples



$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$H = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$$

Quantum Circuits — Examples

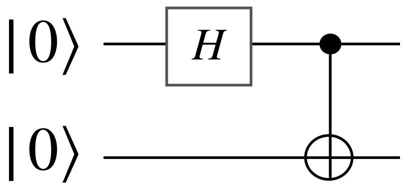


$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$H = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$$

$$|00\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

Quantum Circuits — Examples



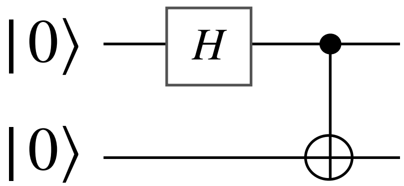
$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$H = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$$

$$|00\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$\mapsto \frac{CNot\,|00\rangle + CNot\,|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Quantum Circuits — Examples



$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

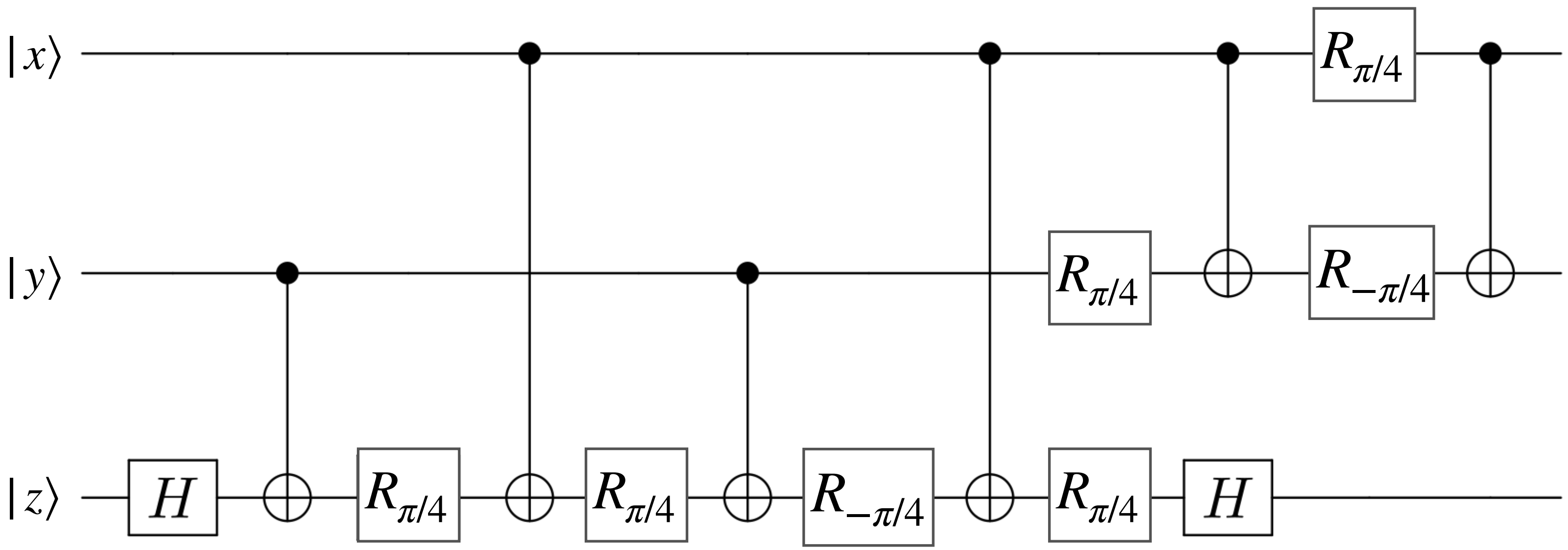
$$CNot = |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$H = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$$

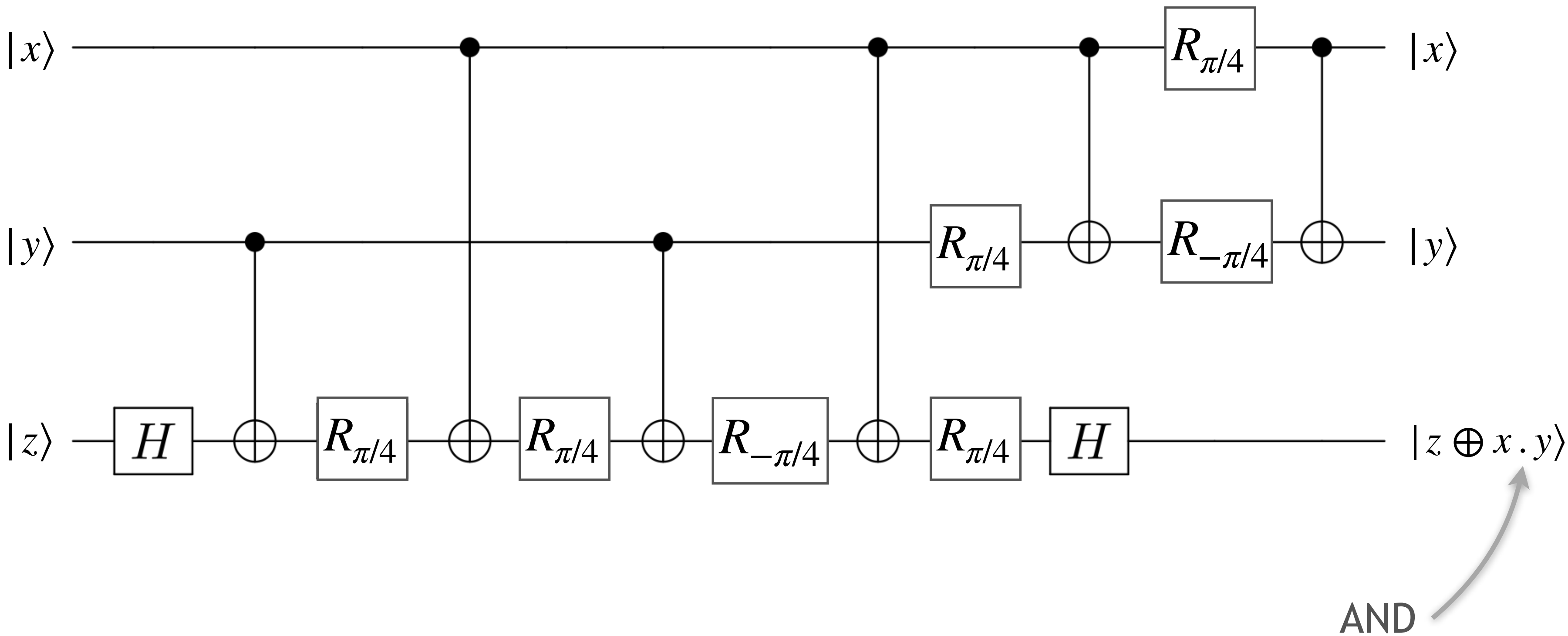
$$|00\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$\mapsto \frac{CNot\,|00\rangle + CNot\,|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

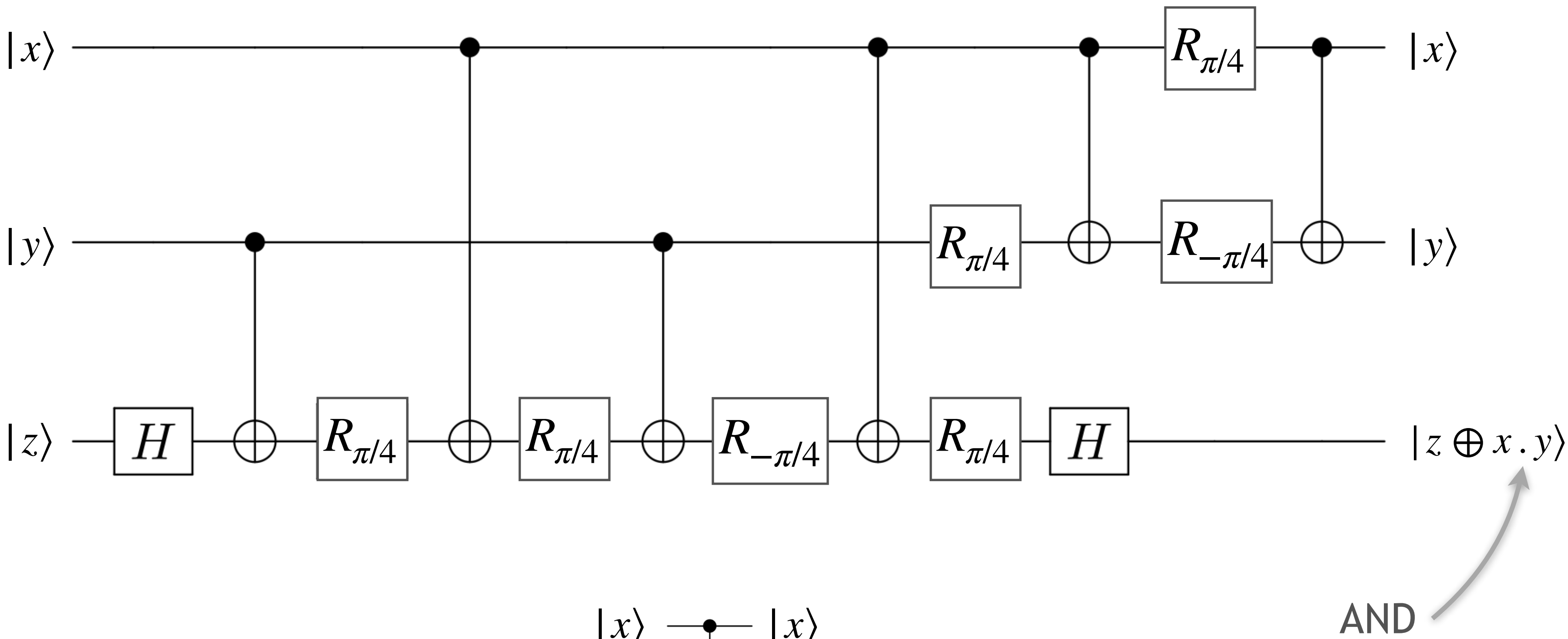
Quantum Circuits - Toffoli



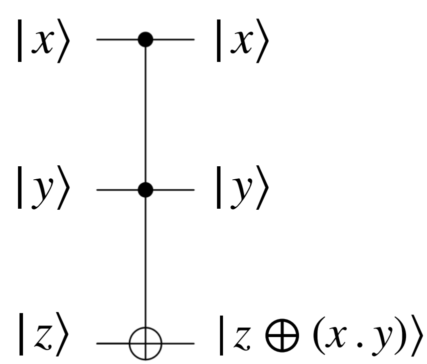
Quantum Circuits - Toffoli



Quantum Circuits - Toffoli

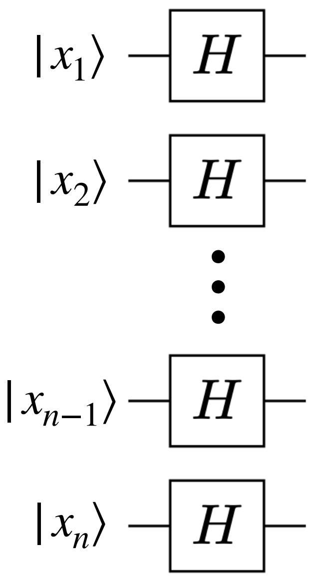


Toffoli gate:

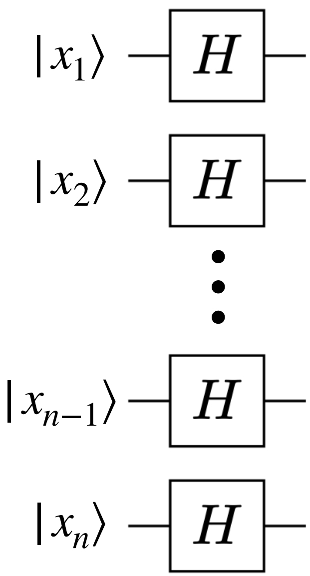


Quantum Circuits - Hadamard

$$H_n|0\ldots0\rangle = (H|0\rangle) \otimes \ldots \otimes (H|0\rangle)$$



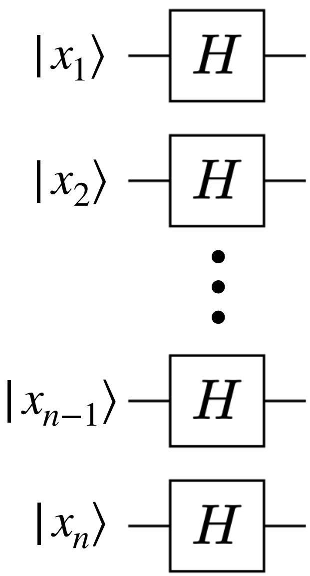
Quantum Circuits - Hadamard



$$H_n|0\ldots0\rangle = (H|0\rangle) \otimes \ldots \otimes (H|0\rangle)$$

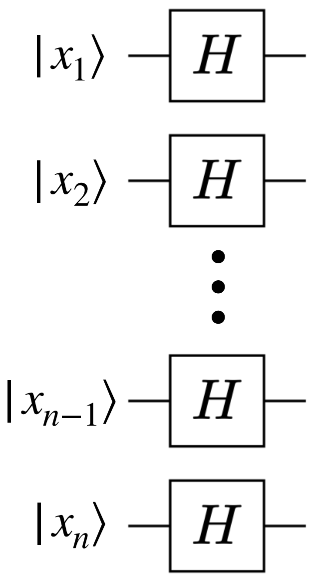
$$= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Quantum Circuits - Hadamard



$$
\begin{aligned}
H_n|0\ldots 0\rangle &= (H|0\rangle) \otimes \ldots \otimes (H|0\rangle) \\
&= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_1,\ldots y_n \in \{0,1\}} |y_1 \ldots y_n\rangle
\end{aligned}
$$

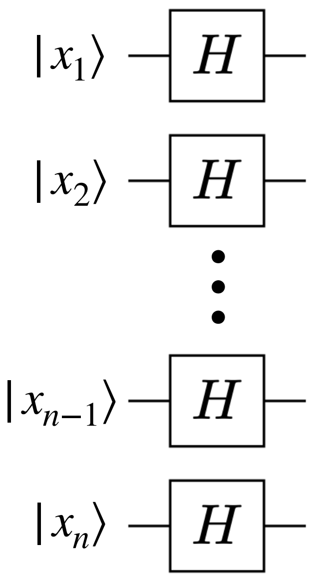
Quantum Circuits - Hadamard



$$
\begin{aligned}
H_n|0\ldots0\rangle &= (H|0\rangle)\otimes\ldots\otimes(H|0\rangle)\\
&= \frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\ldots\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}\\
&= \frac{1}{\sqrt{2^n}}\sum_{y_1,\ldots y_n\in\{0,1\}}|y_1\ldots y_n\rangle
\end{aligned}
$$

$$H_n|x_1\ldots x_n\rangle = (H|x_1\rangle)\otimes\ldots\otimes(H|x_n\rangle)$$

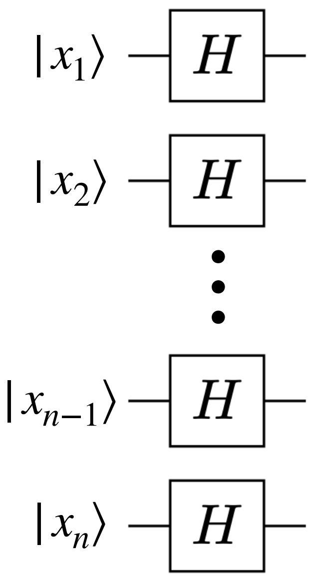
Quantum Circuits - Hadamard



$$\begin{aligned} H_n|0\ldots0\rangle &= (H|0\rangle)\otimes\ldots\otimes(H|0\rangle) \\ &= \frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\ldots\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ &= \frac{1}{\sqrt{2^n}}\sum_{y_1,\ldots y_n\in\{0,1\}}|y_1\ldots y_n\rangle \end{aligned}$$

$$\begin{aligned} H_n|x_1\ldots x_n\rangle &= (H|x_1\rangle)\otimes\ldots\otimes(H|x_n\rangle) \\ &= \frac{|0\rangle+(-1)^{x_1}|1\rangle}{\sqrt{2}}\otimes\ldots\otimes\frac{|0\rangle+(-1)^{x_n}|1\rangle}{\sqrt{2}} \end{aligned}$$

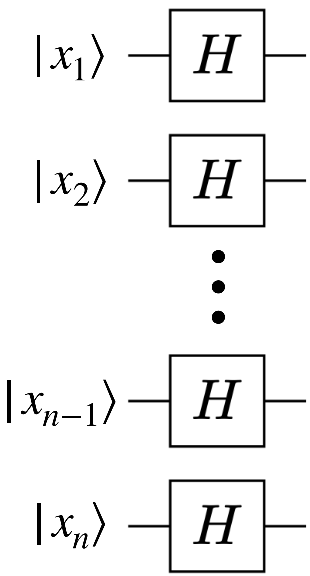
Quantum Circuits - Hadamard



$$
\begin{aligned}
H_n|0\ldots 0\rangle &= (H|0\rangle) \otimes \ldots \otimes (H|0\rangle) \\
&= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_1,\ldots y_n \in \{0,1\}} |y_1 \ldots y_n\rangle
\end{aligned}
$$

$$
\begin{aligned}
H_n|x_1\ldots x_n\rangle &= (H|x_1\rangle) \otimes \ldots \otimes (H|x_n\rangle) \\
&= \frac{|0\rangle + (-1)^{x_1}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + (-1)^{x_n}|1\rangle}{\sqrt{2}} \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_1,\ldots y_n \in \{0,1\}} (-1)^{\sum_i x_i y_i} |y_1 \ldots y_n\rangle
\end{aligned}
$$

Quantum Circuits - Hadamard



$$H_n|0\ldots0\rangle = (H|0\rangle)\otimes\ldots\otimes(H|0\rangle)$$

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

$$= \frac{1}{\sqrt{2^n}}\sum_{y_1,\ldots y_n\in\{0,1\}}|y_1\ldots y_n\rangle$$

$$H_n|x_1\ldots x_n\rangle = (H|x_1\rangle)\otimes\ldots\otimes(H|x_n\rangle)$$

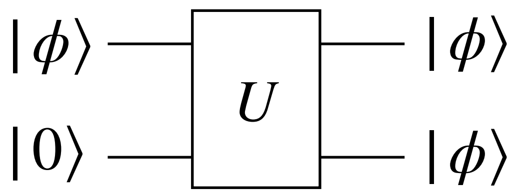
$$= \frac{|0\rangle+(-1)^{x_1}|1\rangle}{\sqrt{2}}\otimes\ldots\otimes\frac{|0\rangle+(-1)^{x_n}|1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^n}}\sum_{y_1,\ldots y_n\in\{0,1\}}(-1)^{\sum_i x_iy_i}|y_1\ldots y_n\rangle$$

$$\boxed{H_n|\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}}\sum_{\mathbf{y}\in\{0,1\}^n}(-1)^{\mathbf{x}\bullet\mathbf{y}}|\mathbf{y}\rangle \text{ where } \mathbf{x}\bullet\mathbf{y} = \sum_i x_iy_i}$$

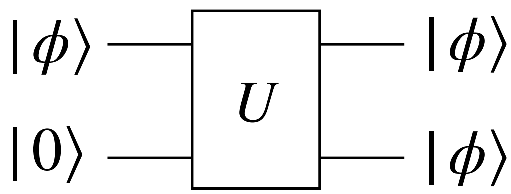
No Cloning

THM: There is no unitary transformation U such that $\forall |\phi\rangle$



No Cloning

THM: There is no unitary transformation U such that $\forall |\phi\rangle$

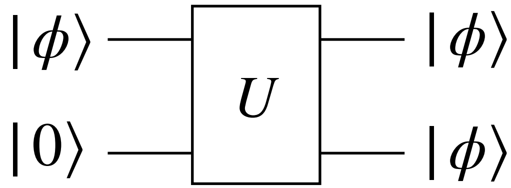


Proof: Assume U exists

$$U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

No Cloning

THM: There is no unitary transformation U such that $\forall |\phi\rangle$



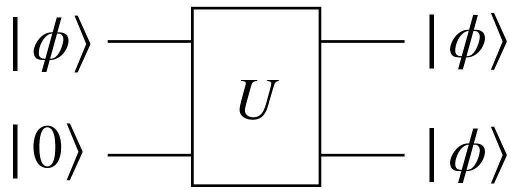
Proof: Assume U exists

$$U\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|0\rangle\right)=\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle+|1\rangle}{\sqrt{2}}=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$$

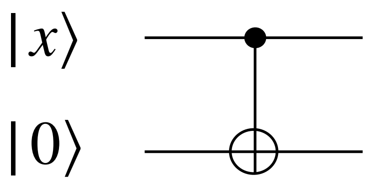
$$U\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|0\rangle\right)=U\left(\frac{|00\rangle+|10\rangle}{\sqrt{2}}\right)=\frac{U|00\rangle+U|10\rangle}{\sqrt{2}}=\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

No Cloning

THM: There is no unitary transformation U such that $\forall |\phi\rangle$

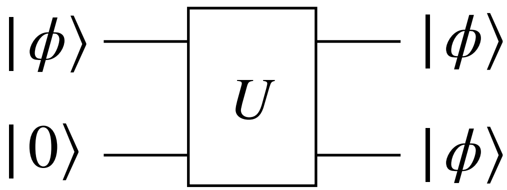


But, one can copy the basis states:

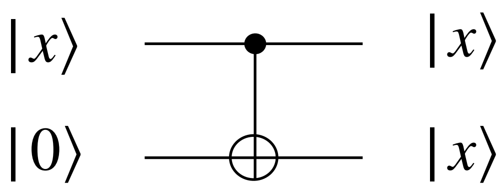


No Cloning

THM: There is no unitary transformation U such that $\forall |\phi\rangle$

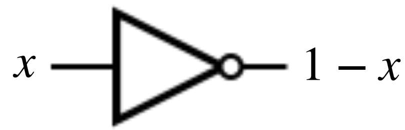


But, one can copy the basis states:



Classical versus Quantum Circuits

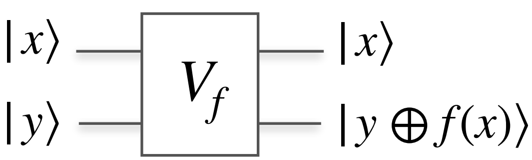
Classical universality: Any boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ can be implemented by a (AND, NOT)-circuit.



Classical versus Quantum Circuits

Classical universality: Any boolean function $f : \{0,1\}^n \to \{0,1\}$ can be implemented by a (AND, NOT)-circuit.

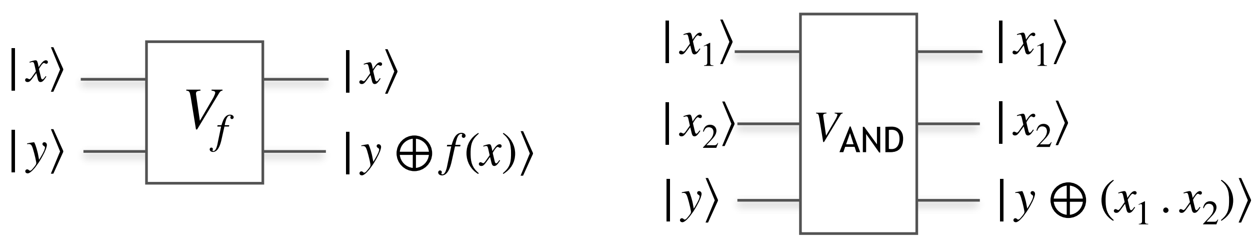
Quantum extension: The quantum extension of a boolean function $f : \{0,1\}^n \to \{0,1\}$ is the unitary transformation $V_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$



Classical versus Quantum Circuits

Classical universality: Any boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ can be implemented by a (AND, NOT)-circuit.

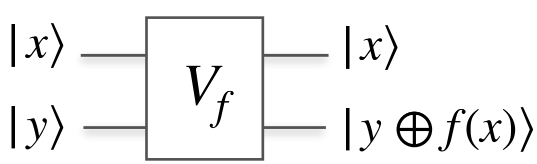
Quantum extension: The quantum extension of a boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ is the unitary transformation $V_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$

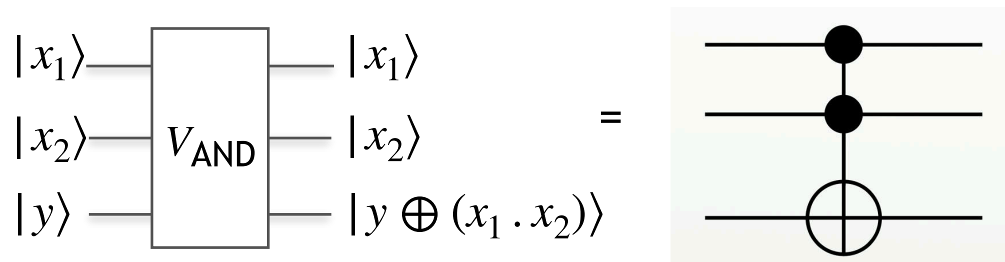


Classical versus Quantum Circuits

Classical universality: Any boolean function $f:\{0,1\}^n \to \{0,1\}$ can be implemented by a (AND, NOT)-circuit.

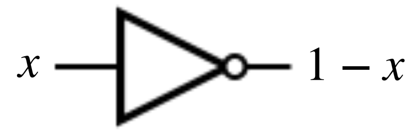
Quantum extension: The quantum extension of a boolean function $f:\{0,1\}^n \to \{0,1\}$ is the unitary transformation $V_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$



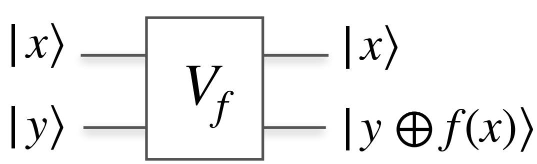


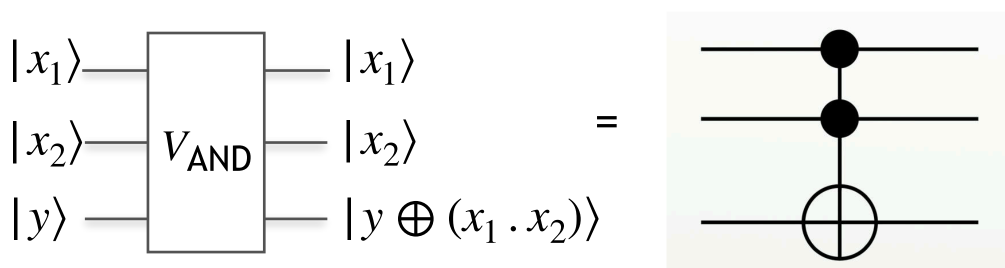
Classical versus Quantum Circuits

Classical universality: Any boolean function $f : \{0,1\}^n \to \{0,1\}$ can be implemented by a (AND, NOT)-circuit.



Quantum extension: The quantum extension of a boolean function $f : \{0,1\}^n \to \{0,1\}$ is the unitary transformation $V_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$

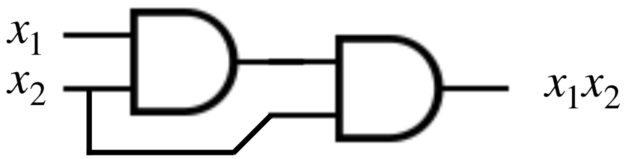




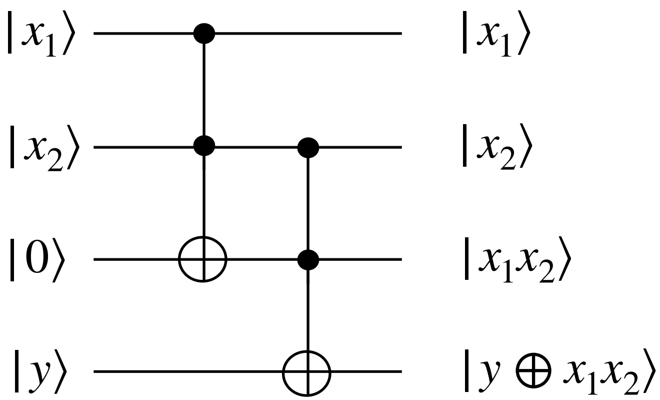
THM: if a boolean function $f : \{0,1\}^n \to \{0,1\}$ can be implemented by a boolean circuit of size s then V_f can be implemented by a quantum circuit of size $O(s)$.

Example

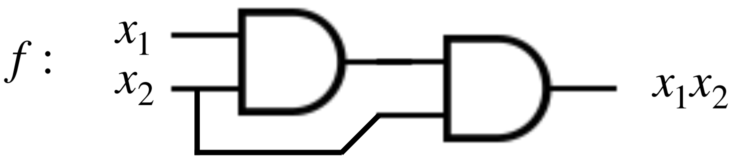
$f:$



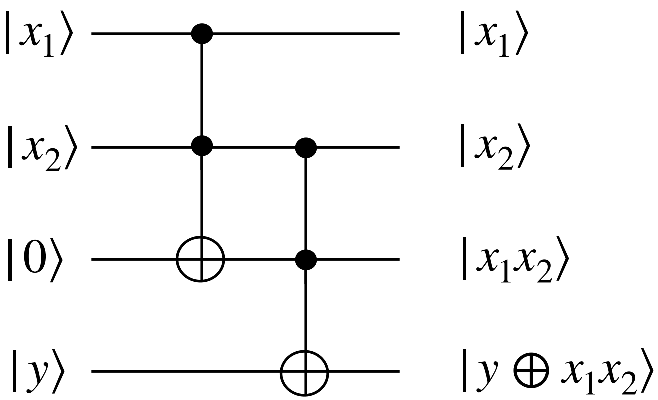
$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus xy\rangle$$



Example

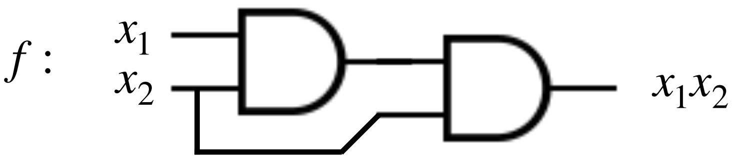


$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus x_1 x_2\rangle$$

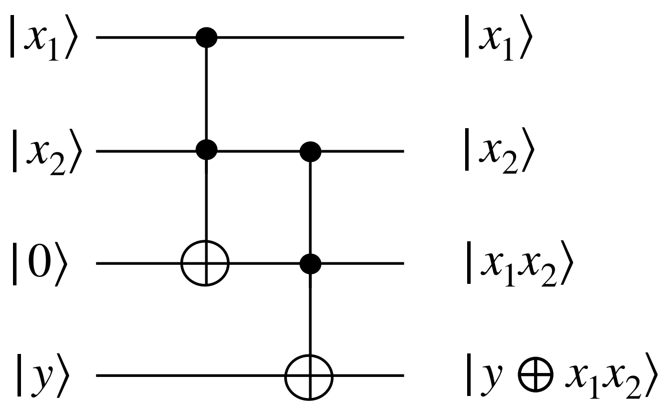


$$C : |x_1, x_2, y\rangle \mapsto |x_1, x_2, \mathbf{x_1 x_2}, y \oplus x_1 x_2\rangle$$

Example



$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus x_1 x_2\rangle$$

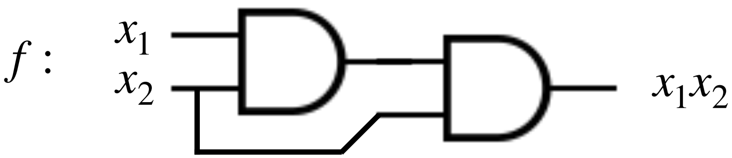


$$C : |x_1, x_2, y\rangle \mapsto |x_1, x_2, \mathbf{x_1 x_2}, y \oplus x_1 x_2\rangle$$

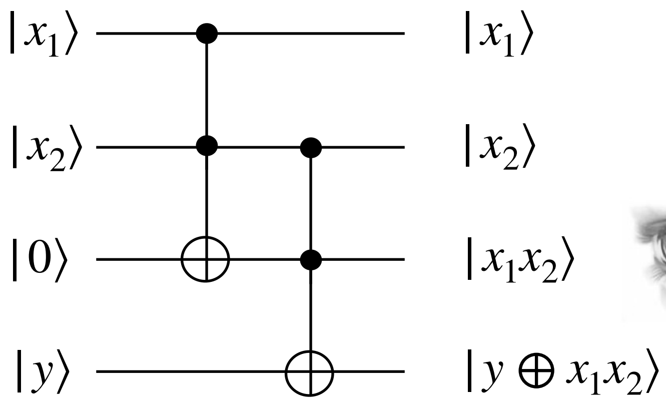
$$V_f\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |y\rangle\right) = \frac{V_f|00y\rangle + V_f|11y\rangle}{\sqrt{2}} = \frac{|00y\rangle + |11(y \oplus 1)\rangle}{\sqrt{2}}$$

$$C\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |y\rangle\right) = \frac{C|00y\rangle + C|11y\rangle}{\sqrt{2}} = \frac{|00\mathbf{0}y\rangle + |11\mathbf{1}(y \oplus 1)\rangle}{\sqrt{2}}$$

Example



$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus x_1x_2\rangle$$



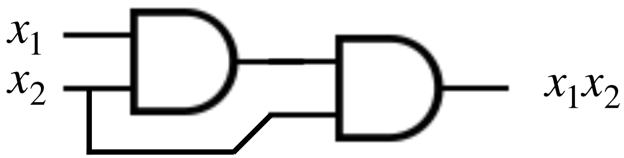
$$C : |x_1, x_2, y\rangle \mapsto |x_1, x_2, \mathbf{x_1x_2}, y \oplus x_1x_2\rangle$$

$$V_f\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |y\rangle\right) = \frac{V_f|00y\rangle + V_f|11y\rangle}{\sqrt{2}} = \frac{|00y\rangle + |11(y \oplus 1)\rangle}{\sqrt{2}}$$

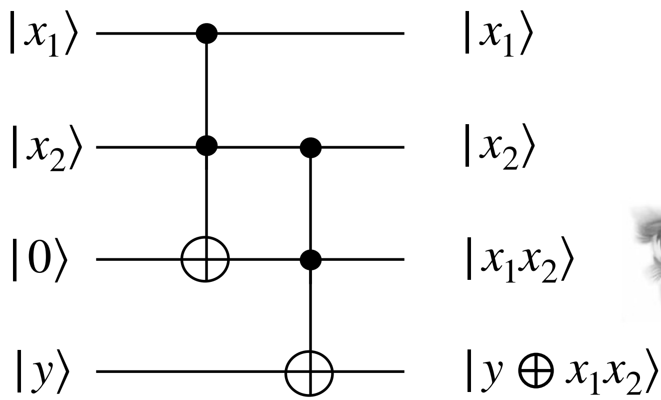
$$C\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |y\rangle\right) = \frac{C|00y\rangle + C|11y\rangle}{\sqrt{2}} = \frac{|00\mathbf{0}y\rangle + |11\mathbf{1}(y \oplus 1)\rangle}{\sqrt{2}}$$

Example

$f:$



$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus x_1x_2\rangle$$



$$C : |x_1, x_2, y\rangle \mapsto |x_1, x_2, \mathbf{x_1x_2}, y \oplus x_1x_2\rangle$$

$$V_f\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |y\rangle\right) = \frac{V_f|00y\rangle + V_f|11y\rangle}{\sqrt{2}} = \frac{|00y\rangle + |11(y \oplus 1)\rangle}{\sqrt{2}}$$

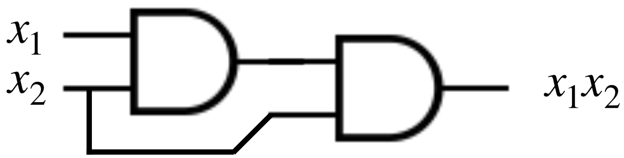
$$C\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |y\rangle\right) = \frac{C|00y\rangle + C|11y\rangle}{\sqrt{2}} = \frac{|00\mathbf{0}y\rangle + |11\mathbf{1}(y \oplus 1)\rangle}{\sqrt{2}}$$

$|00\mathbf{0}y\rangle$

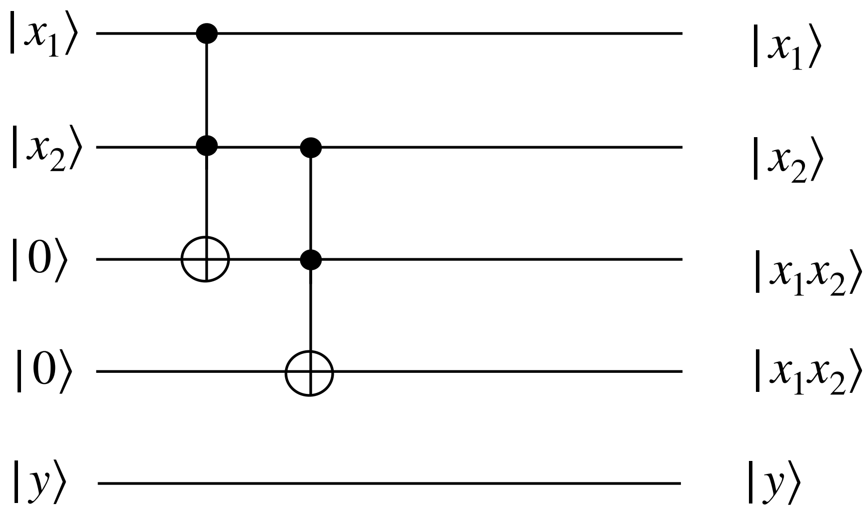
$|00\mathbf{1}(y \oplus 1)\rangle$

Example

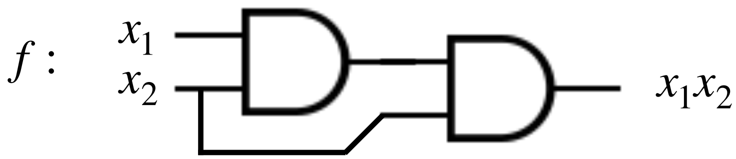
$f:$



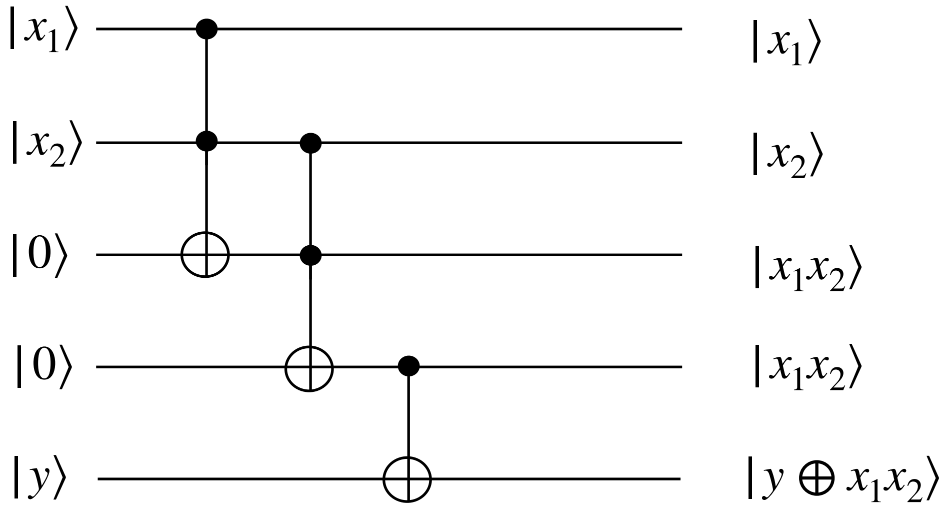
$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus xy\rangle$$



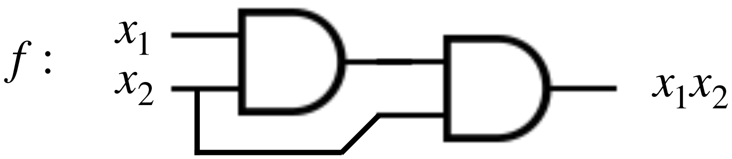
Example



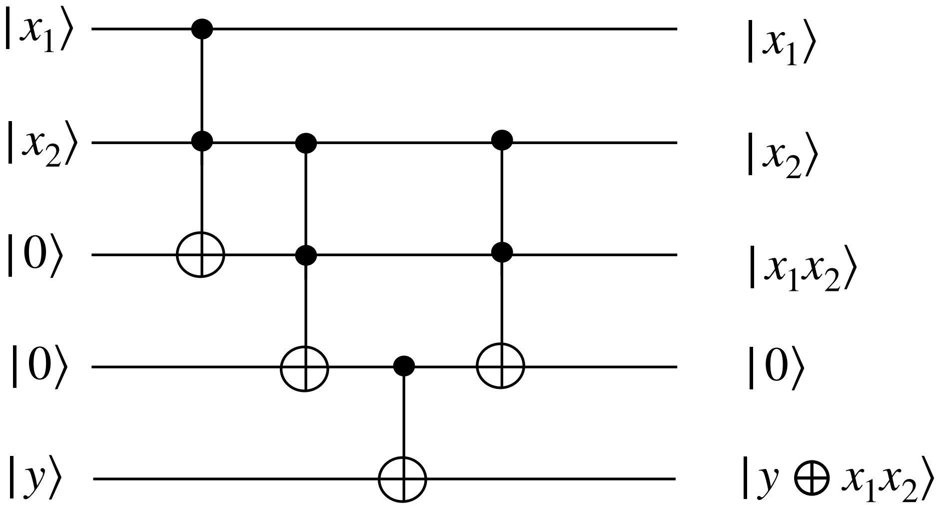
$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus xy\rangle$$



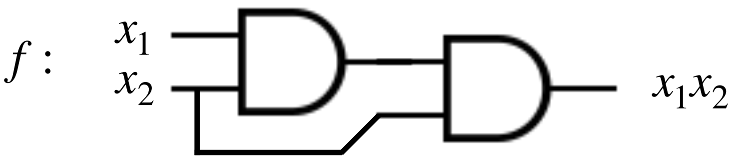
Example



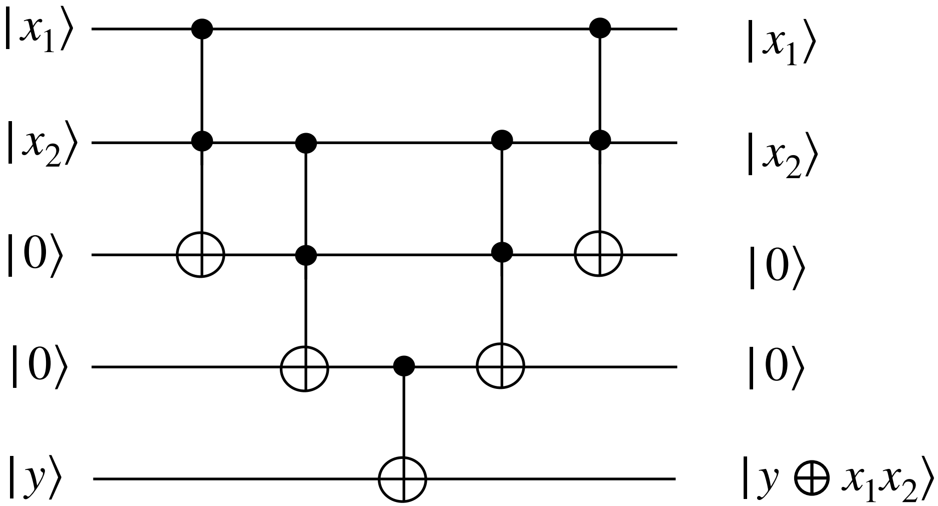
$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus xy\rangle$$



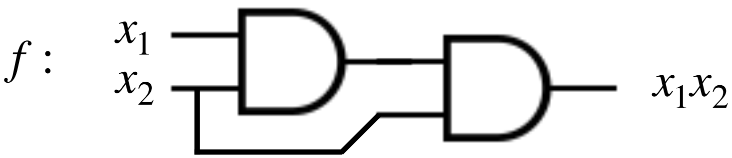
Example



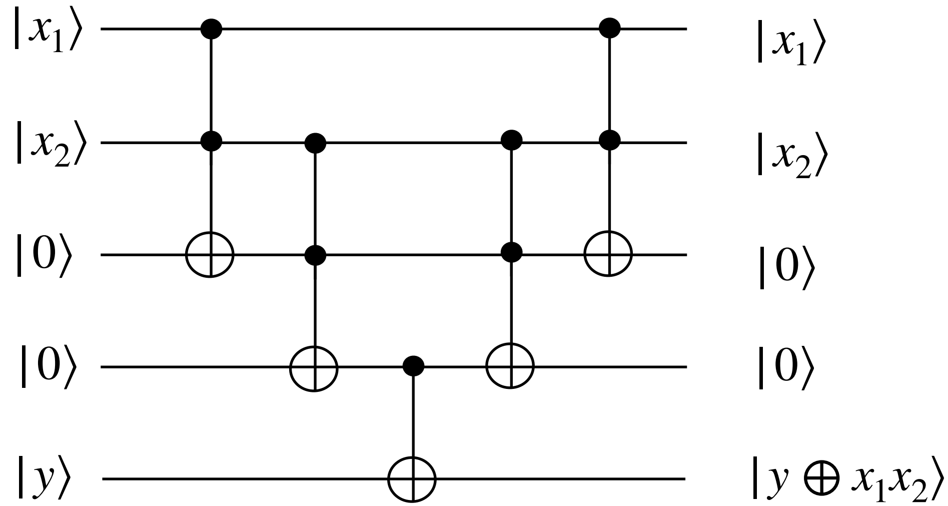
$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus xy\rangle$$



Example



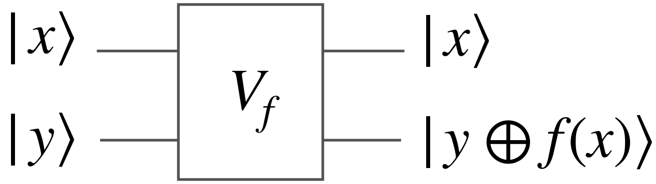
$$V_f : |x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus xy\rangle$$

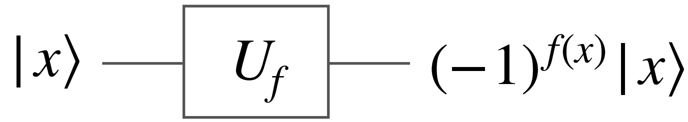


This circuit is an implementation of V_f

Another quantum extension

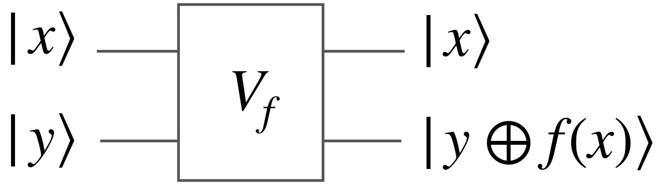
Quantum extensions of a boolean function $f : \{0,1\}^n \to \{0,1\}$:

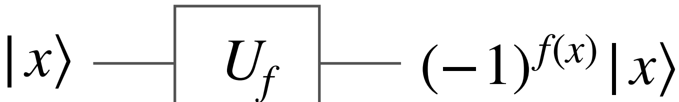


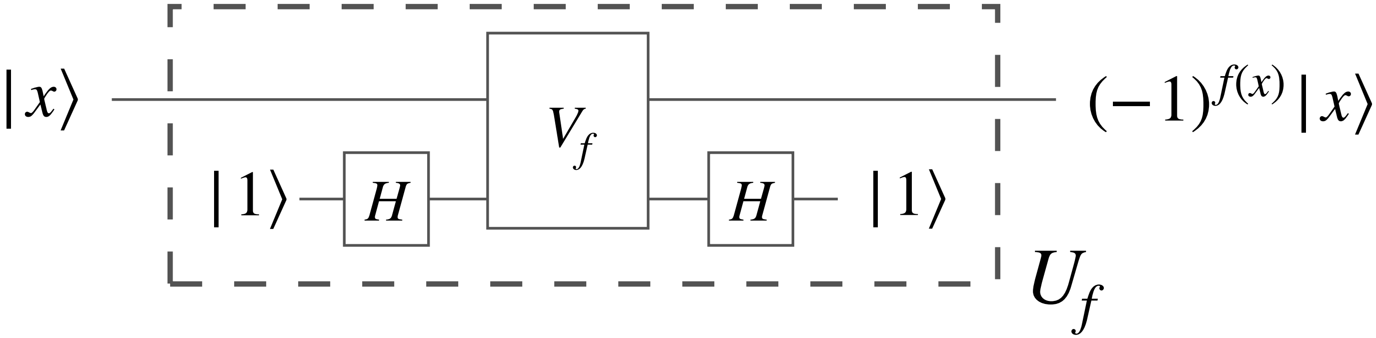


Another quantum extension

Quantum extensions of a boolean function $f : \{0,1\}^n \to \{0,1\}$:

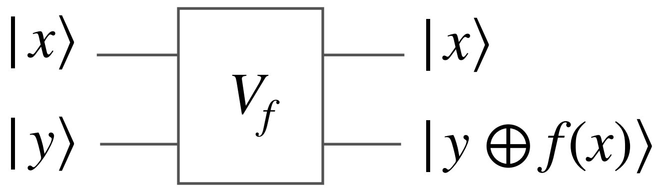


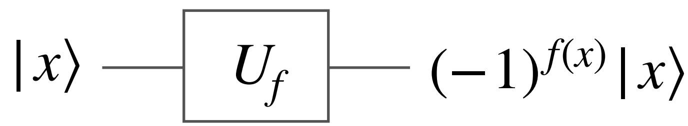


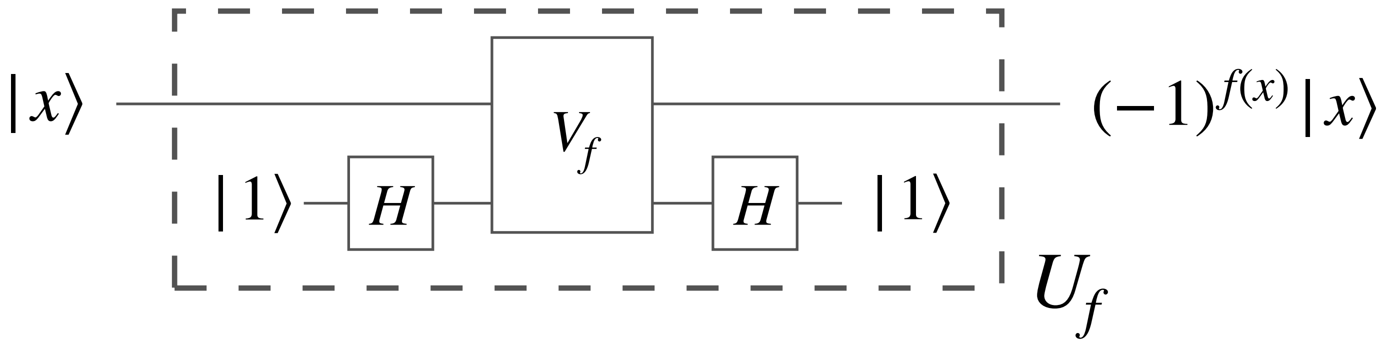


Another quantum extension

Quantum extensions of a boolean function $f : \{0,1\}^n \to \{0,1\}$:





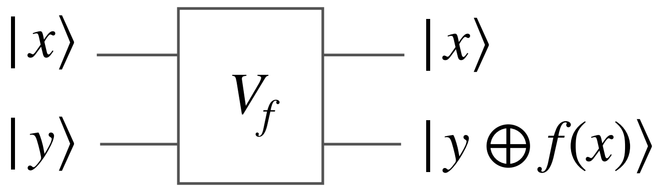


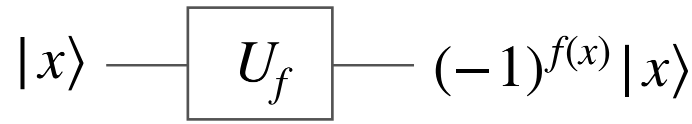
$$|x,1\rangle \overset{H}{\mapsto} \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}} \overset{V_f}{\mapsto} \frac{|x,0 \oplus f(x)\rangle - |x,1 \oplus f(x)\rangle}{\sqrt{2}}$$

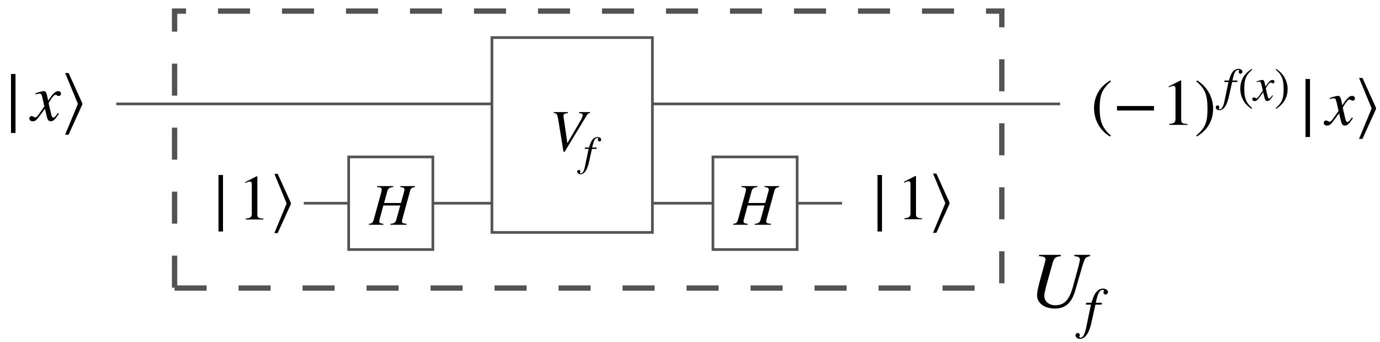
$$H = |y\rangle \mapsto \frac{|0\rangle + (-1)^y|1\rangle}{\sqrt{2}}$$

Another quantum extension

Quantum extensions of a boolean function $f : \{0,1\}^n \to \{0,1\}$:







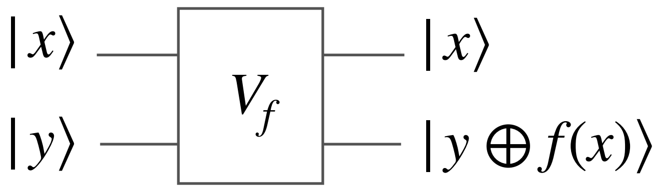
$$|x,1\rangle \overset{H}{\mapsto} \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}} \overset{V_f}{\mapsto} \frac{|x,0 \oplus f(x)\rangle - |x,1 \oplus f(x)\rangle}{\sqrt{2}}$$

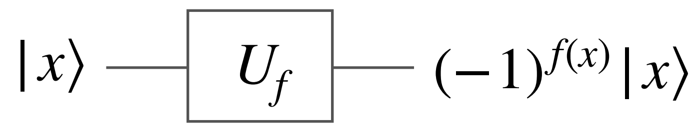
$$\boxed{H = |y\rangle \mapsto \frac{|0\rangle + (-1)^y|1\rangle}{\sqrt{2}}}$$

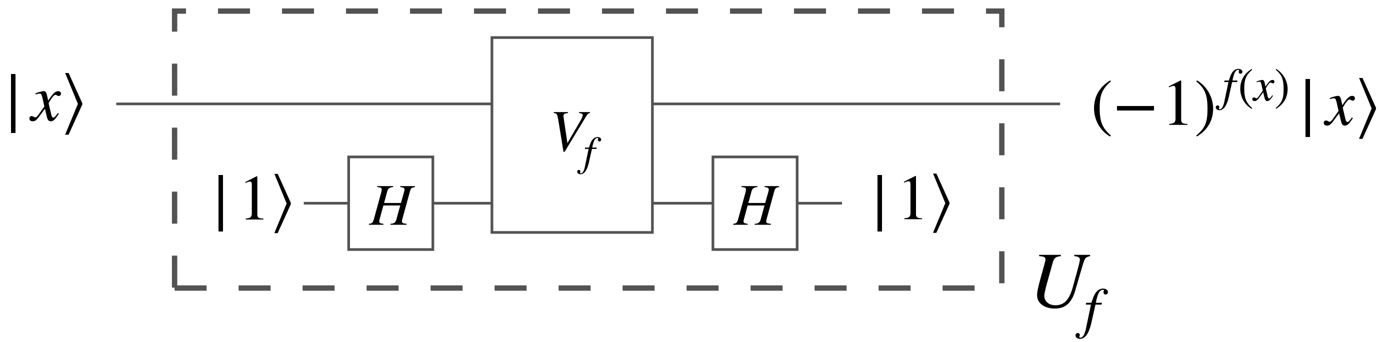
$$\overset{H}{\mapsto} \frac{|x,0\rangle + (-1)^{f(x)}|x,1\rangle - (|x,0\rangle + (-1)^{1 \oplus f(x)}|x,1\rangle)}{2}$$

Another quantum extension

Quantum extensions of a boolean function $f : \{0,1\}^n \to \{0,1\}$:







$$|x,1\rangle \overset{H}{\mapsto} \frac{|x,0\rangle - |x,1\rangle}{\sqrt{2}} \overset{V_f}{\mapsto} \frac{|x,0 \oplus f(x)\rangle - |x,1 \oplus f(x)\rangle}{\sqrt{2}}$$

$$\boxed{H = |y\rangle \mapsto \frac{|0\rangle + (-1)^y|1\rangle}{\sqrt{2}}}$$

$$\overset{H}{\mapsto} \frac{|x,0\rangle + (-1)^{f(x)}|x,1\rangle - (|x,0\rangle + (-1)^{1\oplus f(x)}|x,1\rangle)}{2}$$

$$= \frac{|x,0\rangle + (-1)^{f(x)}|x,1\rangle - |x,0\rangle + (-1)^{f(x)}|x,1\rangle)}{2} = (-1)^{f(x)}|x,1\rangle$$

Outline

Postulates

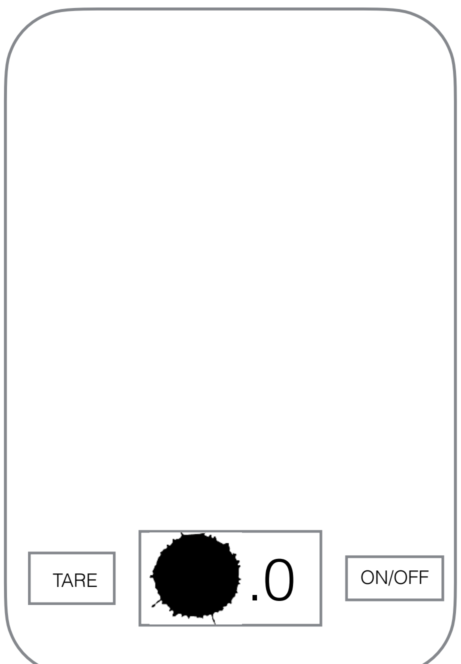
Quantum Circuits

1st Algo: Detecting fake coins with a quantum scale

2nd Algo: Deutsch-Jozsa

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.



Detecting fake coins

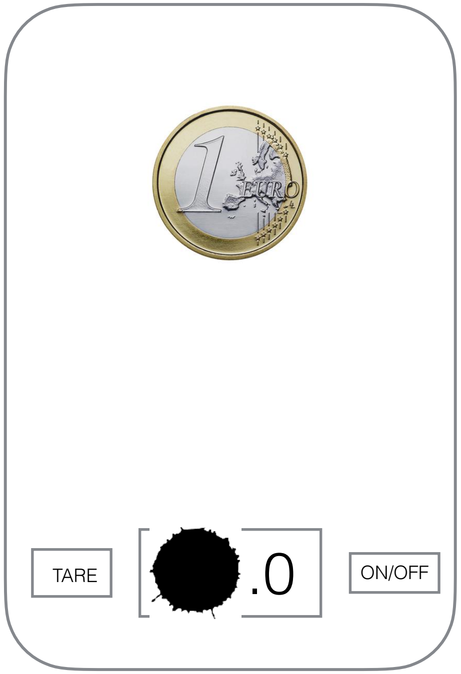
A true coin weighs 8g,
a fake 7.5g.

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.



Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

Detecting fake coins

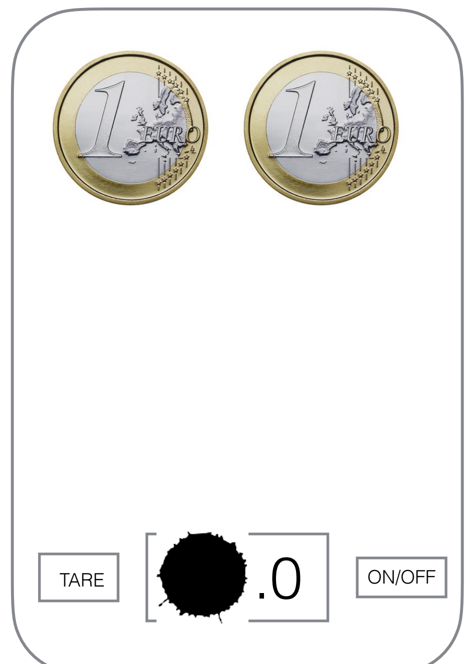
A true coin weighs 8g,
a fake 7.5g.

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.



Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

odd number of fake coins

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

odd number of fake coins

Detecting fake coins

A true coin weighs 8g,
a fake 7.5g.

Mathematical modelling

 $\leftrightarrow$ 0 1 0 0 1 0

A subset of n coins $\leftrightarrow$ a binary word of size n

Let $a \in \{0,1\}^n$ be the set of **fake** coins

Mathematical modelling

$\leftrightarrow$ 0 1 0 0 1 0

A subset of n coins $\leftrightarrow$ a binary word of size n

Let $a \in \{0,1\}^n$ be the set of **fake** coins

A weighing is described by a function $f_a : \{0,1\}^n \to \{0,1\}$ which associates with every subset x of coins, the parity $f_a(x)$ of fake coins in x.

$$f_a(x) = \sum_{i=1}^{n} x_i a_i \bmod 2 = x \bullet a$$

How to (classically) identify the fake coins among n?

- Greedy algorithm:
    -> Weighing coins one by one: **n Weighings**

- Better algorithm?

How to (classically) identify the fake coins among n?

- Greedy algorithm:
  -> Weighing coins one by one: **n Weighings**

- Better algorithm?

No, the greedy algorithm is optimal

How to (classically) identify the fake coins among n?

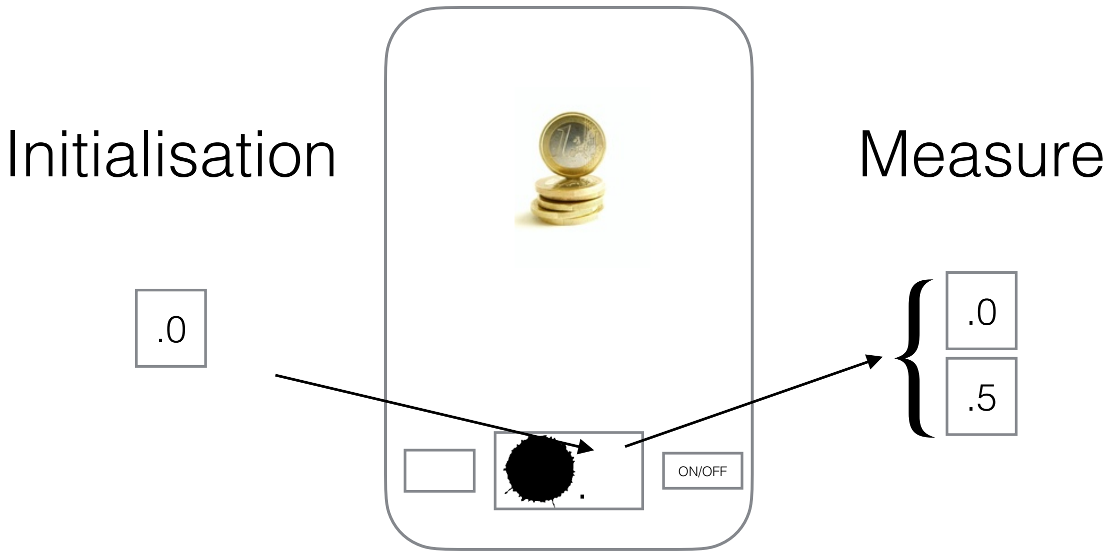
- Greedy algorithm:
  -> Weighing coins one by one: **n Weighings**
- Better algorithm?

No, the greedy algorithm is optimal

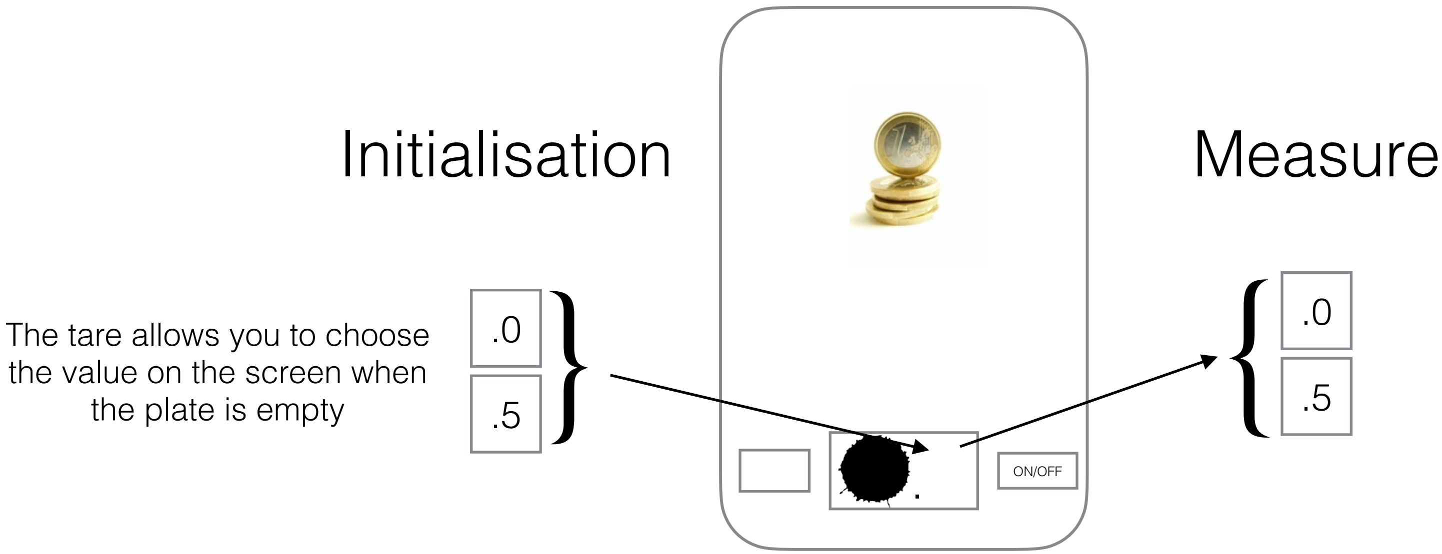
Intuition:

- Need (at least) n bits to describe the solution (because 2^n possible answers).
- Each weighing gives a single bit of information (".0" or ".5")
- So at least n weighing are necessary

Digression : Tare weight



Digression : Tare weight

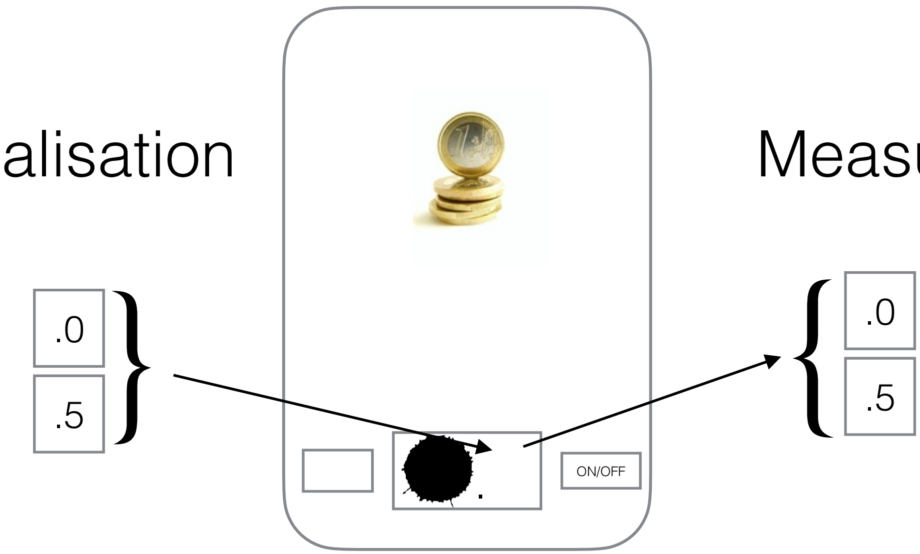


Digression : Tare weight

Initialisation

Measure

The tare allows you to choose the value on the screen when the plate is empty



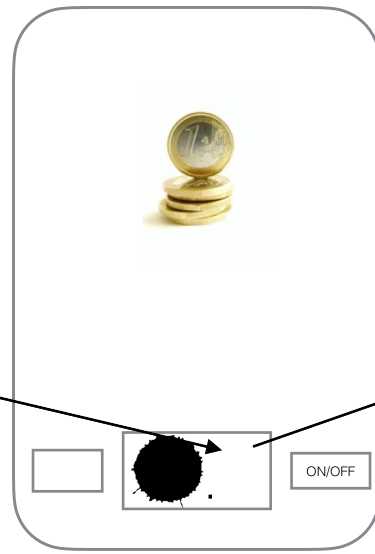
- **even** number of fake coins

.0 → .0

.5 → .5

Digression : Tare weight

Initialisation



Measure

The tare allows you to choose the value on the screen when the plate is empty

.0
.5

.0
.5

- **even** number of fake coins

Screen does **not** change

.0	→	.0
.5	→	.5

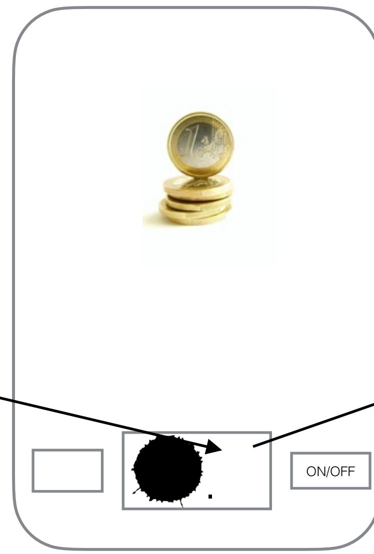
Digression : Tare weight

Initialisation

The tare allows you to choose the value on the screen when the plate is empty

.0

.5



Measure

.0

.5

- **even** number of fake coins

Screen does not change

.0 → .0

.5 → .5

- **odd** number of fake coins

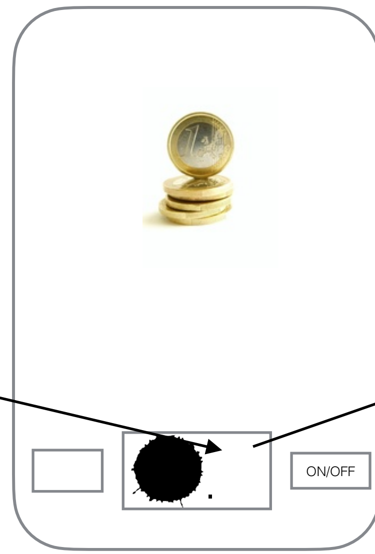
.0 → .5

.5 → .0

Digression : Tare weight

Initialisation

Measure



The tare allows you to choose the value on the screen when the plate is empty

.0
.5

.0
.5

- **even** number of fake coins

Screen does **not** change

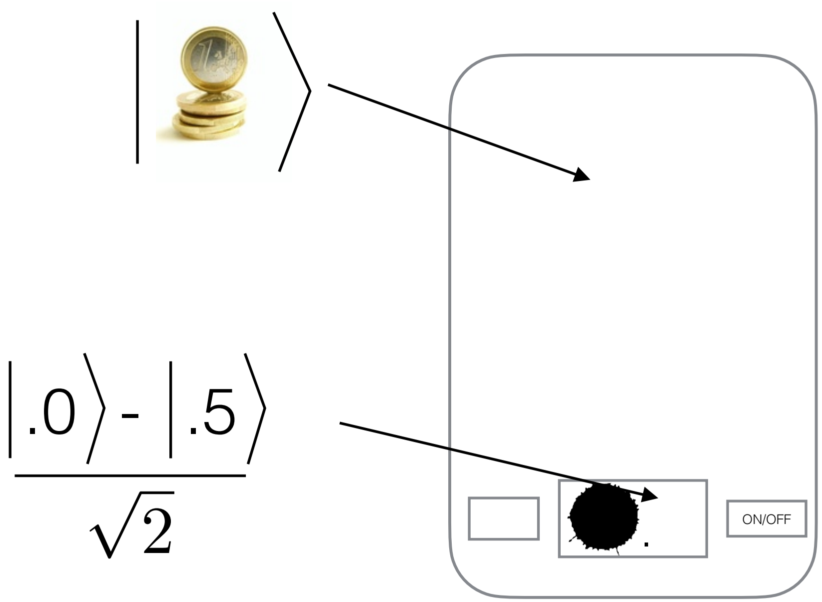
.0 → .0
.5 → .5

- **odd** number of fake coins

Screen does change

.0 → .5
.5 → .0

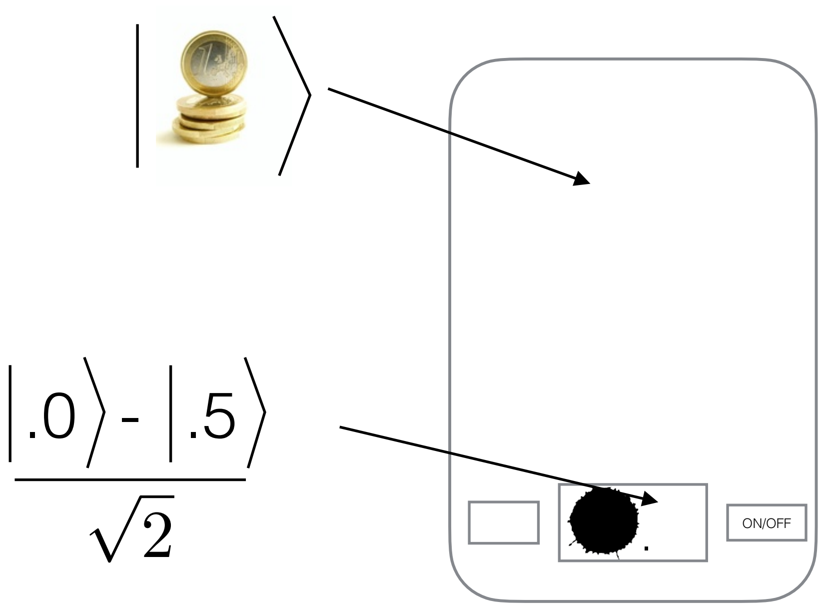
Quantum scale (disclaimer: this is a thought experiment)



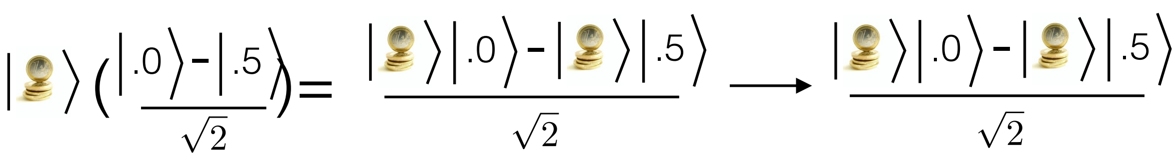
- if **even** number of fake coins:

$|$$\rangle \left(\frac{|.0\rangle - |.5\rangle}{\sqrt{2}} \right) =$ ($|$$\rangle |.0\rangle - |$$\rangle |.5\rangle$) $/ \sqrt{2} \longrightarrow$

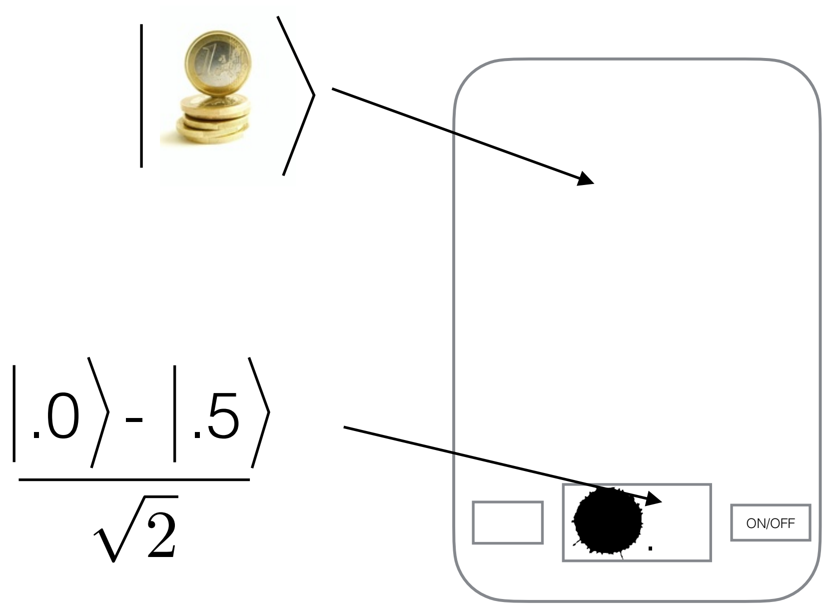
Quantum scale (disclaimer: this is a thought experiment)



- if **even** number of fake coins:



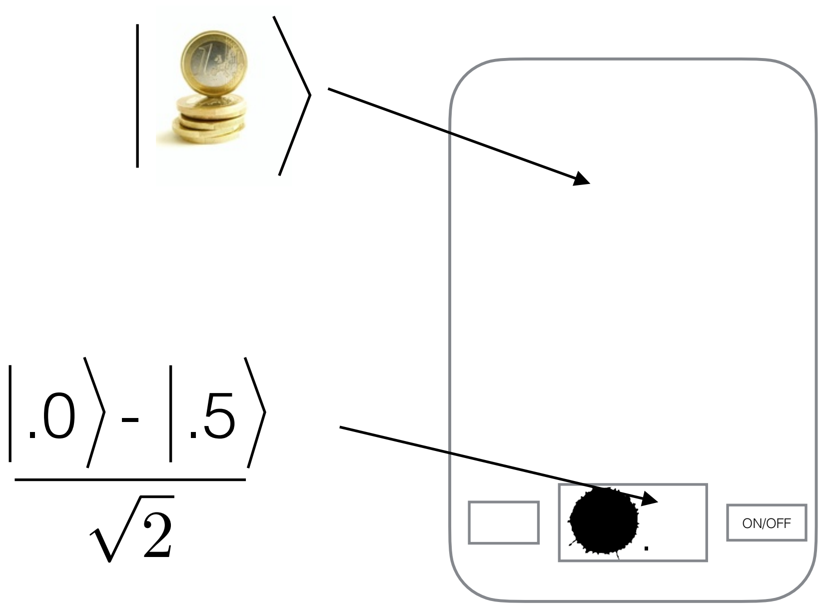
Quantum scale (disclaimer: this is a thought experiment)



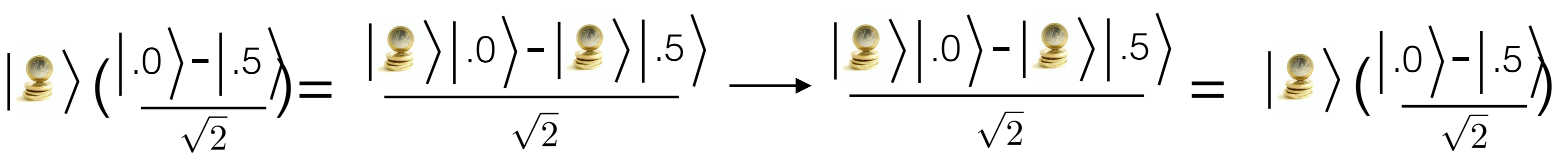
- if **even** number of fake coins:

$|$$\rangle \left(\frac{|.0\rangle - |.5\rangle}{\sqrt{2}} \right) =$ $\Big($ $|$$\rangle|.0\rangle - |$$\rangle|.5\rangle$ $\Big) / \sqrt{2}$ $\longrightarrow$ $\Big($ $|$$\rangle|.0\rangle - |$$\rangle|.5\rangle$ $\Big) / \sqrt{2}$ $=$ $|$$\rangle \left(\frac{|.0\rangle - |.5\rangle}{\sqrt{2}} \right)$

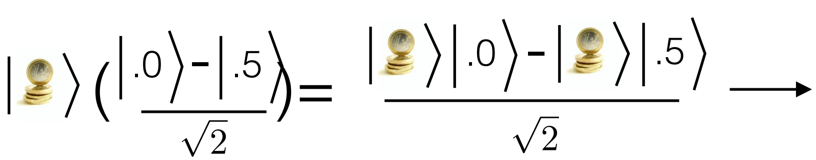
Quantum scale (disclaimer: this is a thought experiment)



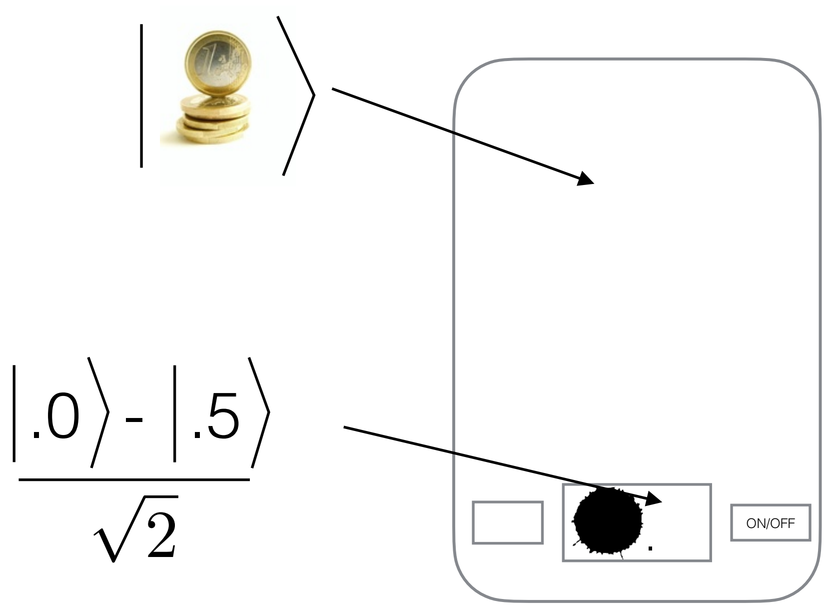
- if **even** number of fake coins:



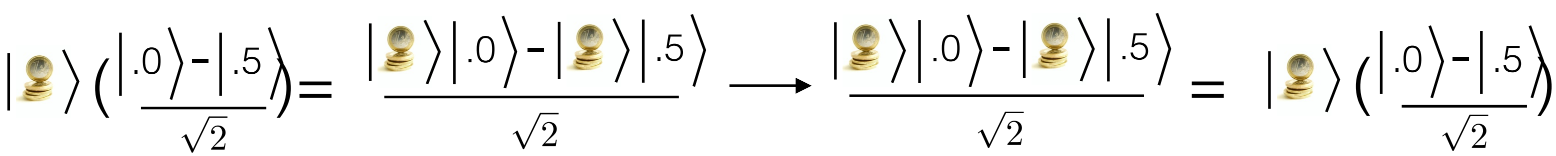
- if **odd** number of fake coins:



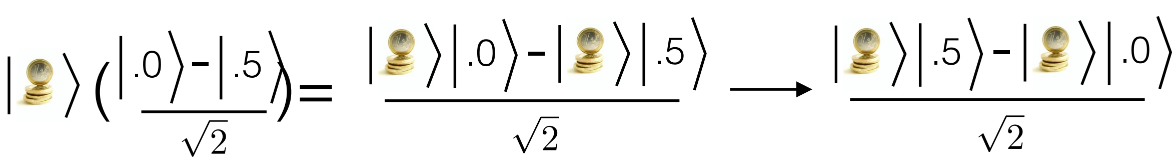
Quantum scale (disclaimer: this is a thought experiment)



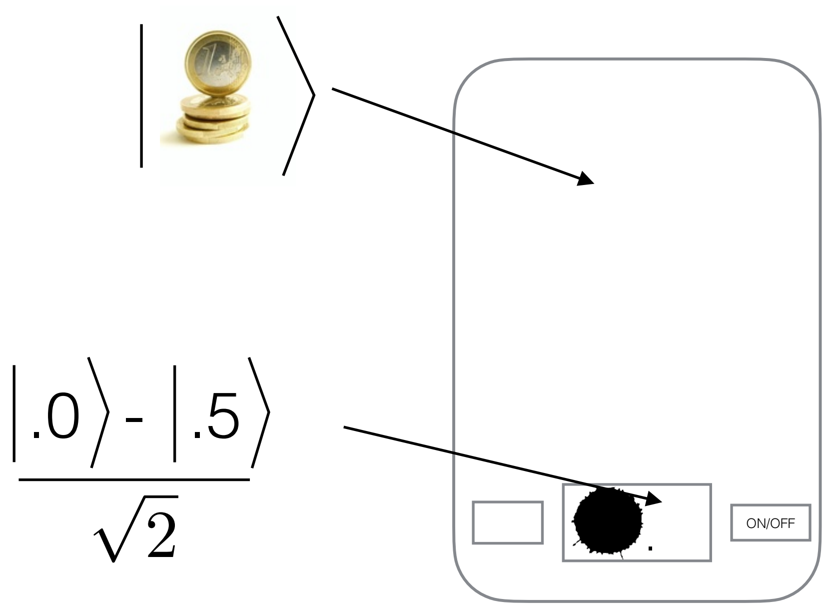
- if **even** number of fake coins:



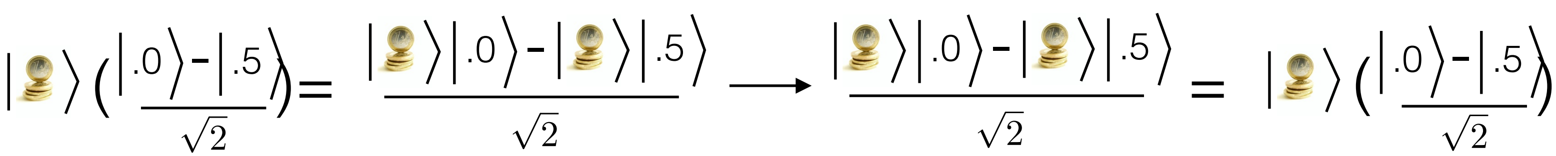
- if **odd** number of fake coins:



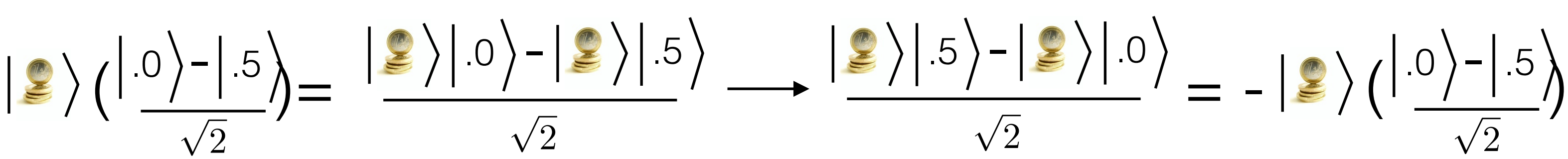
Quantum scale (disclaimer: this is a thought experiment)



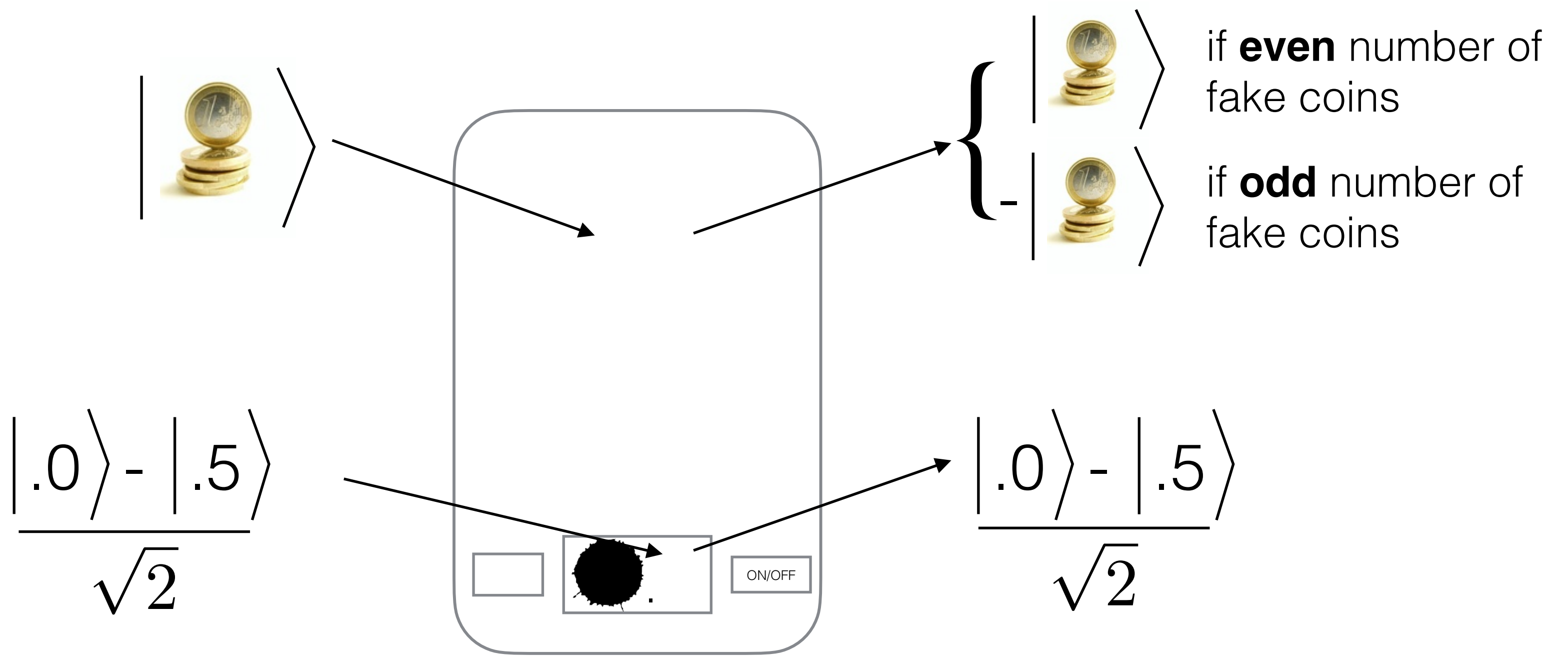
- if **even** number of fake coins:



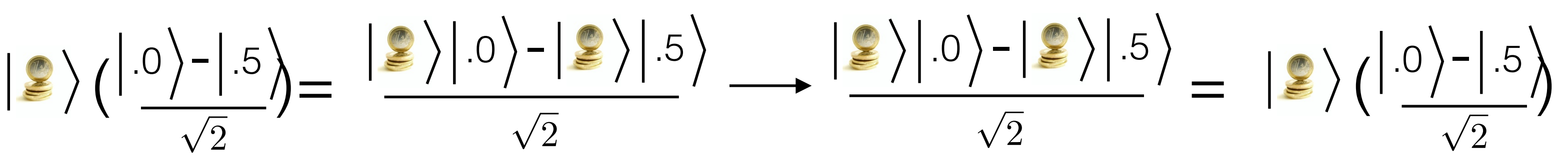
- if **odd** number of fake coins:



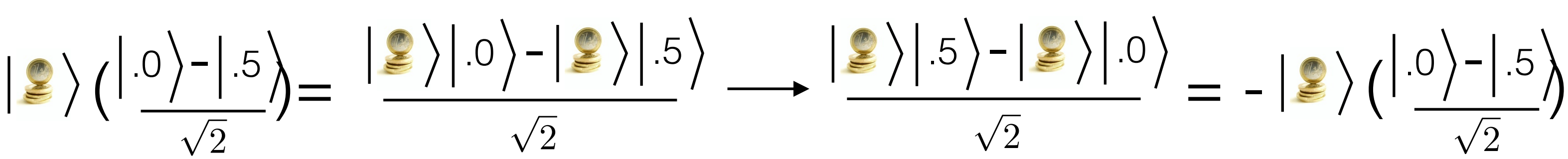
Quantum scale (disclaimer: this is a thought experiment)



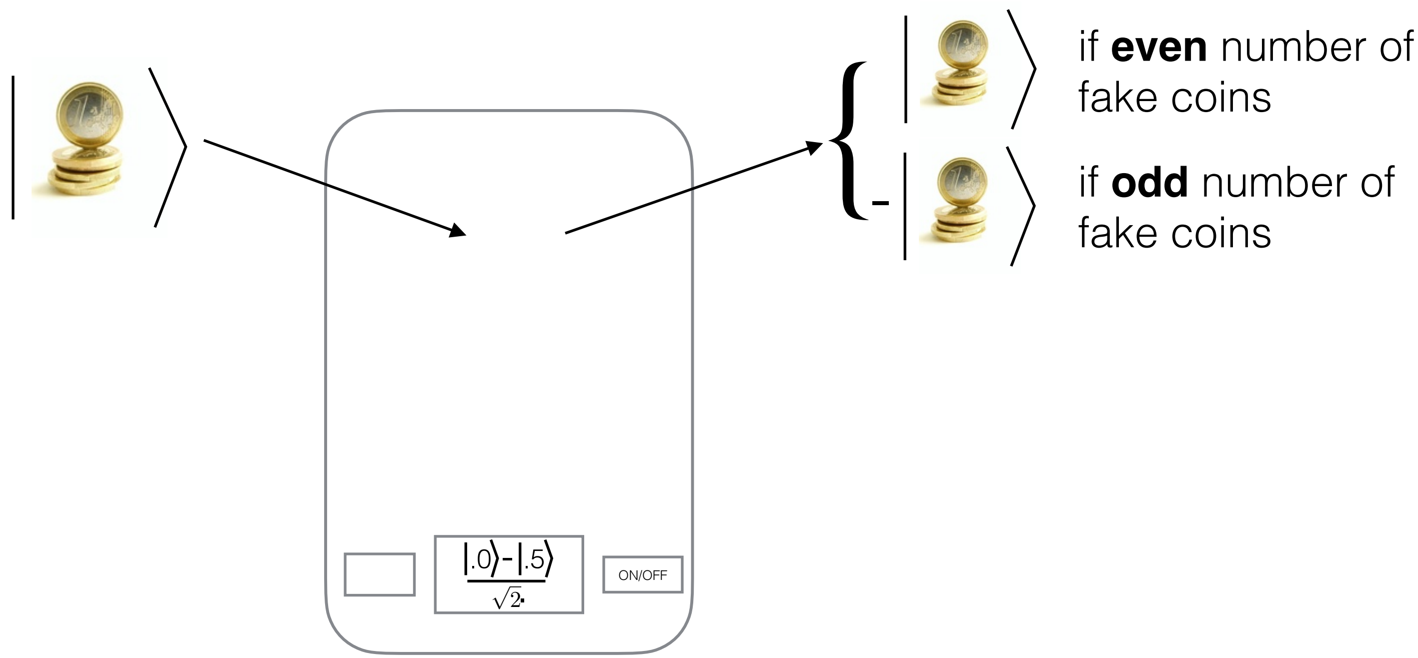
- if **even** number of fake coins:



- if **odd** number of fake coins:

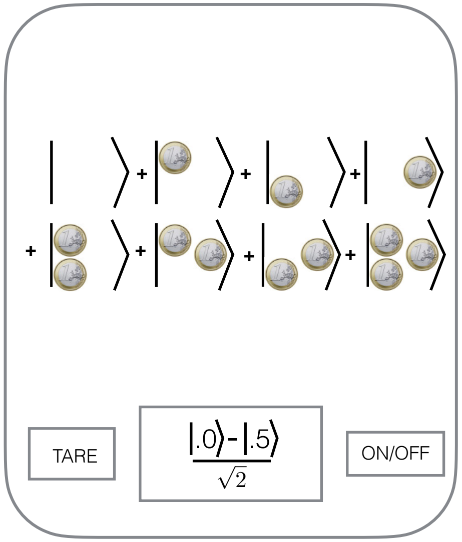


Quantum scale (disclaimer: this is a thought experiment)



$$|x\rangle \mapsto (-1)^{f_a(x)}|x\rangle = (-1)^{x \bullet a}|x\rangle$$

Bernstein-Vazirani Algorithm



$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

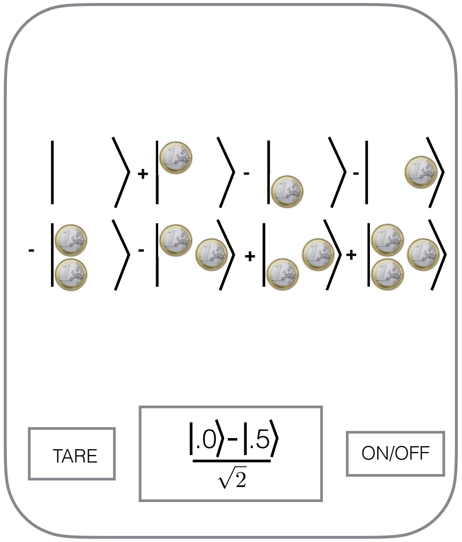
weigh. $U_{f_a} : |x\rangle \mapsto (-1)^{x\bullet a}|x\rangle$

Hadamard $H_n : |y\rangle \mapsto \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{x\bullet y}|x\rangle$

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$$

$$H_n \circ H_n = I$$

Bernstein-Vazirani Algorithm



weighing

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \quad \mapsto \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet a}|x\rangle$$

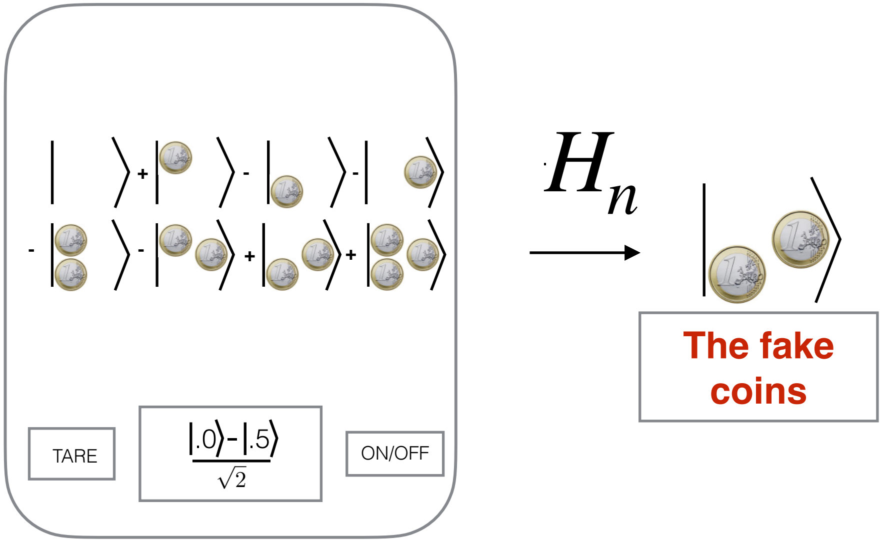
weigh. $U_{f_a} : |x\rangle \mapsto (-1)^{x\bullet a}|x\rangle$

Hadamard $H_n : |y\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet y}|x\rangle$

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$H_n \circ H_n = I$$

Bernstein-Vazirani Algorithm



weighing

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \quad \mapsto \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet a}|x\rangle$$

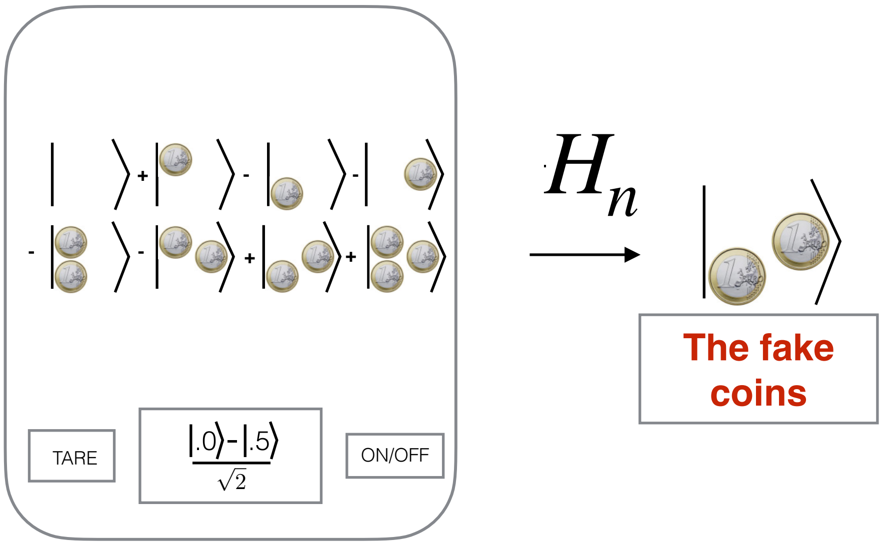
weigh. $U_{f_a} : |x\rangle \mapsto (-1)^{x\bullet a}|x\rangle$

Hadamard $H_n : |y\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet y}|x\rangle$

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$H_n \circ H_n = I$$

Bernstein-Vazirani Algorithm



weighing

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \;\mapsto\; \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet a}|x\rangle \;=\; H_n|a\rangle$$

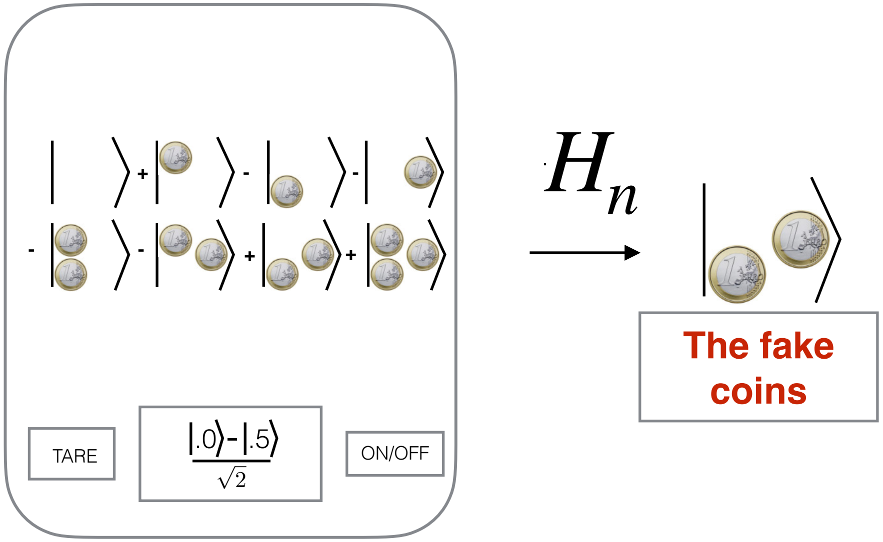
weigh. $U_{f_a} : |x\rangle \mapsto (-1)^{x\bullet a}|x\rangle$

Hadamard $H_n : |y\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet y}|x\rangle$

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$H_n \circ H_n = I$$

Bernstein-Vazirani Algorithm



weighing

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \;\mapsto\; \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet a}|x\rangle \;=\; H_n|a\rangle \;\overset{H_n}{\mapsto}\; = H_nH_n|a\rangle = |a\rangle$$

weigh. $U_{f_a} : |x\rangle \mapsto (-1)^{x\bullet a}|x\rangle$

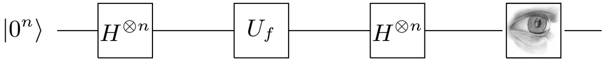
Hadamard $H_n : |y\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet y}|x\rangle$

$$H_n|0\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$H_n \circ H_n = I$$

Detecting Fake Coins: Bernstein-Vazirani

Promise: $f : \{0,1\}^n \rightarrow \{0,1\}$ s.t. $\exists a \in \{0,1\}^n, f(x) = x \bullet a = \sum_{i=1}^{n} x_i a_i \bmod 2$.
Problem: Find $a \in \{0,1\}^n$.
Classical algorithm: n calls to f are necessary and sufficient.
Quantum algorithm: 1 call to U_f.



Outline

Postulates

Quantum Circuits

1st Algo: Detecting fake coins with a quantum scale

2nd Algo: Deutsch-Jozsa

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm:
Quantum algorithm:

0	0	0	0	0	0	0	0	$\to$	constant
1	1	1	1	1	1	1	1	$\to$	constant
0	1	0	0	1	1	0	1	$\to$	balanced
0	0	0	0	1	1	1	1	$\to$	balanced

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm:
Quantum algorithm:

0		0	0				0	$\to$	?
0		0	0			**0**	0	$\to$	constant
0		0	0			**1**	0	$\to$	balanced

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2+1$ calls to f with $N=2^n$
Quantum algorithm:

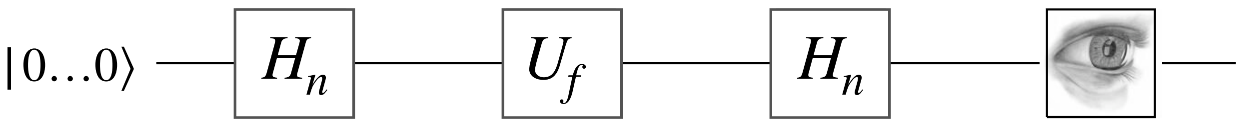
0		0	0				0	$\to$	?
0		0	0			**0**	0	$\to$	constant
0		0	0			**1**	0	$\to$	balanced

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2+1$ calls to f with $N=2^n$
Quantum algorithm: 1 call to U_f.

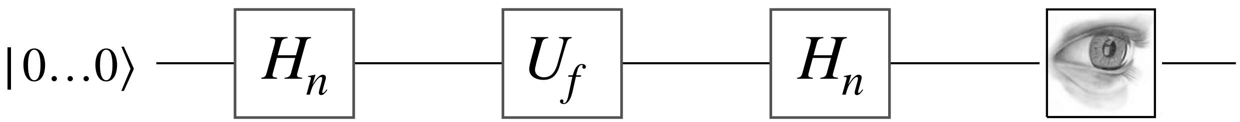
Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \rightarrow \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2{+}1$ calls to f with $N{=}2^n$
Quantum algorithm: 1 call to U_f.



Deutsch-Jozsa Algorithm

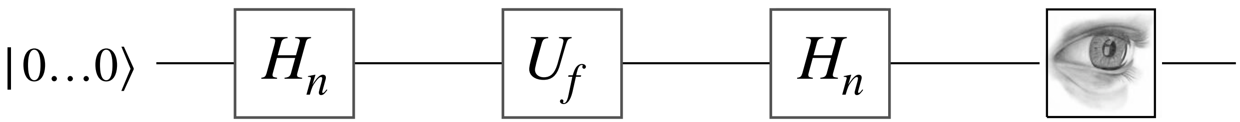
Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2{+}1$ calls to f with $N{=}2^n$
Quantum algorithm: 1 call to U_f.



$$
\begin{aligned}
|0^n\rangle \quad & \mapsto^{H_n} \quad \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} |x\rangle \\
& \mapsto^{U_f} \\
& \mapsto^{H_n}
\end{aligned}
$$

Deutsch-Jozsa Algorithm

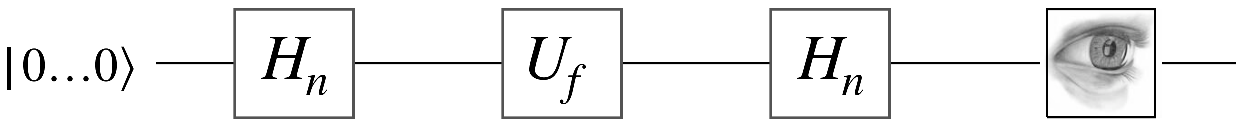
Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2{+}1$ calls to f with $N{=}2^n$
Quantum algorithm: 1 call to U_f.



$$
\begin{aligned}
|0^n\rangle \quad &\mapsto^{H_n} \quad \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \\
&\mapsto^{U_f} \quad \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \\
&\mapsto^{H_n}
\end{aligned}
$$

Deutsch-Jozsa Algorithm

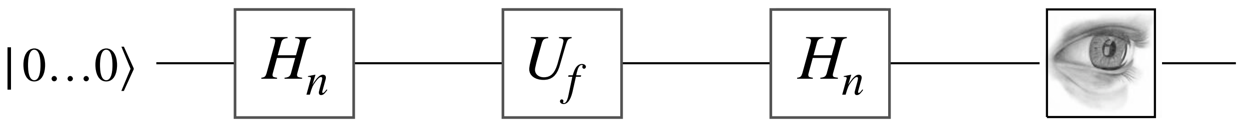
Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2+1$ calls to f with $N=2^n$
Quantum algorithm: 1 call to U_f.



$$
\begin{aligned}
|0^n\rangle \quad &\mapsto^{H_n} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\mapsto^{U_f} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \\
&\mapsto^{H_n} \quad \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)} (-1)^{x\cdot y} |y\rangle
\end{aligned}
$$

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2{+}1$ calls to f with $N{=}2^n$
Quantum algorithm: 1 call to U_f.

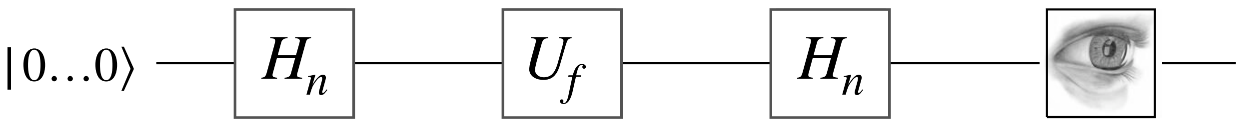


$$\begin{aligned}
|0^n\rangle \quad &\mapsto^{H_n} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\mapsto^{U_f} \quad \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\,|x\rangle \\
&\mapsto^{H_n} \quad \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)}(-1)^{x\cdot y}\,|y\rangle
\end{aligned}$$

Amplitude of $|0^n\rangle$ is $\alpha_0 = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}$

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced ($|f^{-1}(0)| = |f^{-1}(1)|$)
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2{+}1$ calls to f with $N{=}2^n$
Quantum algorithm: 1 call to U_f.



$$
\begin{aligned}
|0^n\rangle \quad & \mapsto^{H_n} \quad \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} |x\rangle \\
& \mapsto^{U_f} \quad \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \\
& \mapsto^{H_n} \quad \tfrac{1}{2^n} \textstyle\sum_{x,y\in\{0,1\}^n} (-1)^{f(x)} (-1)^{x\cdot y} |y\rangle
\end{aligned}
$$

Amplitude of $|0^n\rangle$ is $\alpha_0 = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$

– If f is balanced, $\alpha_0 = 0 \implies$ never measure 0^n.
– Si f est constante, $\alpha_0 = \pm 1 \implies$ always measure 0^n.

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2{+}1$ calls to f with $N{=}2^n$
Quantum algorithm: 1 call to U_f.
Bounded error algorithm:

0	1	0	0	1	1	0	1

1	1	1	1	1	1	1	1

Deutsch-Jozsa Algorithm

Promise: $f : \{0,1\}^n \to \{0,1\}$ is either constant or balanced $(|f^{-1}(0)| = |f^{-1}(1)|)$
Problem: decide whether f is constant or balanced.
Classical algorithm: requires $N/2+1$ calls to f with $N=2^n$
Quantum algorithm: 1 call to U_f.
Bounded error algorithm: $O(1)$ calls to f.

0	1	0	0	1	1	0	1

1	1	1	1	1	1	1	1