Deutsch's Algorithm

Dimitrios I. Myrisiotis
MPLA • CoReLab

April 26, 2017

Contents

Introduction

Introduction

Figure : David Deutsch (1953–).

Introduction

Deutsch's Problem.

Input : A black-box U_f for $f : \{0, 1\} \rightarrow \{0, 1\}$.

Output : The value of $\mathrm{XOR}\left(f\left(0\right), f\left(1\right)\right) = f\left(1\right) \oplus f\left(0\right)$.

Introduction

Deutsch's Problem.

Input : A black-box U_f for $f : \{0,1\} \to \{0,1\}$.
Output : The value of $\mathrm{XOR}\left(f(0), f(1)\right) = f(1) \oplus f(0)$.

Classically, we need two queries to U_f.
Quantumly, one query to U_f suffices!

Preliminaries

Preliminaries

$$\underbrace{\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square\;\square}_{16}$$

$$\forall \square : \square \in \{0, 1\}$$

Figure : Our 16-bit computer, with 2^{16} configurations.

Preliminaries

$$p_1 \;\; p_2 \;\; \dots \;\; p_{2^{16}}$$

$$\forall i \in \left\{1, 2, \dots, 2^{16}\right\} : p_i \in \{0, 1\}$$

$$\sum_{i=1}^{2^{16}} p_i = 1 \Leftrightarrow \exists! k : p_k = 1$$

Figure : Communicating a configuration of a **deterministic** computer.

Preliminaries

$$p_1 \;\; p_2 \;\; \dots \;\; p_{2^{16}}$$

$$\forall i \in \left\{1, 2, \dots, 2^{16}\right\} : p_i \in [0, 1]$$

$$\sum_{i=1}^{2^{16}} p_i = 1$$

Figure : Communicating a configuration of a **probabilistic** computer.

Preliminaries

$$c_1 \;\; c_2 \;\; \dots \;\; c_{2^{16}}$$

$$\forall i \in \left\{1, 2, \dots, 2^{16}\right\} : c_i \in \mathbb{C}$$

$$\sum_{i=1}^{2^{16}} |c_i|^2 = 1 \qquad (*)$$

Figure : Communicating a configuration of a **quantum** computer.

Quantum States

Preliminaries: Quantum States

$$\mathcal{B} = \{\mathbf{v}_i\}_{i=1}^{2^{16}}$$

$$\begin{aligned}
\mathbf{v}_1 &= 0\ldots000 \\
\mathbf{v}_2 &= 0\ldots001 \\
&\vdots \\
\mathbf{v}_{2^{16}} &= \underbrace{1\ldots111}_{16}
\end{aligned}$$

Preliminaries: Quantum States

$$\mathcal{B} = \{\mathbf{v}_i\}_{i=1}^{2^{16}}$$

$$\mathbf{v}_1 = \underbrace{0\ldots000}_{16} = \left(\begin{array}{c} 1 \\ 0 \\ \vdots \\ 0 \end{array}\right)\Bigg\} 2^{16}$$

$$\vdots$$

$$\mathbf{v}_{2^{16}} = \underbrace{1\ldots111}_{16} = \left(\begin{array}{c} 0 \\ 0 \\ \vdots \\ 1 \end{array}\right)\Bigg\} 2^{16}$$

Preliminaries: Quantum States

$$\mathcal{B} = \{\mathbf{v}_i\}_{i=1}^{2^{16}}$$

$$\mathcal{H}' = \operatorname{span}(\mathcal{B}, \mathbb{C}) = \left\{ \sum_{i=1}^{2^{16}} c_i \cdot \mathbf{v}_i \mid \forall i : c_i \in \mathbb{C} \text{ and } \mathbf{v}_i \in \mathcal{B} \right\} = \mathbb{C}^{2^{16}}$$

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathbb{C}^{2^{16}} \mid \|\mathbf{q}\|_2 = 1 \right\} \subseteq \mathbb{C}^{2^{16}}$$

Preliminaries: Quantum States

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathbb{C}^{2^{16}} \mid \|\mathbf{q}\|_2 = 1 \right\}$$

$$= \text{where 16-register quantum computers live}$$

$$\subseteq \mathbb{C}^{2^{16}}$$

Preliminaries: Quantum States

$$\begin{aligned}\mathcal{H} &= \left\{\mathbf{q} \in \mathbb{C}^{2^n} \mid \|\mathbf{q}\|_2 = 1\right\} \\ &= \text{where } n\text{-register quantum computers live} \\ &\subseteq \mathbb{C}^{2^n}\end{aligned}$$

Preliminaries: Quantum States

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathbb{C}^{2^n} \mid \|\mathbf{q}\|_2 = 1 \right\}$$

$$\mathbf{q} = \left(\sum_{i=1}^{2^{16}} c_i \cdot \mathbf{v}_i \right) \in \mathcal{H} \Leftrightarrow \|\mathbf{q}\|_2 = 1 \Leftrightarrow \sum_{i=1}^{2^n} |c_i|^2 = 1 \qquad (*)$$

Preliminaries: Quantum States

$$|\psi\rangle$$

Preliminaries: Quantum States

$$|\psi\rangle \in \mathcal{H} \subseteq \mathbb{C}^{2^n}$$

Preliminaries: Quantum States

$$
\begin{aligned}
|\psi\rangle &= \text{a ket} \\
&= \text{a column vector in } \mathcal{H}
\end{aligned}
$$

$$
\begin{aligned}
\langle\psi| &= \text{a bra} \\
&= \text{a row vector in } \mathcal{H}^\dagger \\
&= \text{the dual of } |\psi\rangle \\
&= |\psi\rangle^\dagger \\
&= \left(|\psi\rangle^*\right)^T = \left(|\psi\rangle^T\right)^*
\end{aligned}
$$

Preliminaries: Quantum States

$$\mathcal{B} = \{\mathbf{v}_i\}_{i=1}^{2^{16}}$$

$$\begin{aligned} \mathbf{v}_1 &= 0\ldots000 \\ \mathbf{v}_2 &= 0\ldots001 \\ &\vdots \\ \mathbf{v}_{2^{16}} &= 1\ldots111 \end{aligned}$$

Preliminaries: Quantum States

$$\mathcal{B} = \{|v_i\rangle\}_{i=1}^{2^{16}}$$

$$\begin{aligned} |v_1\rangle &= |0\ldots000\rangle \\ |v_2\rangle &= |0\ldots001\rangle \\ &\vdots \\ |v_{2^{16}}\rangle &= |1\ldots111\rangle \end{aligned}$$

Preliminaries: Quantum States

$$\mathcal{B} = \{|v_i\rangle\}_{i=1}^{2^{16}}$$

$$\begin{aligned} |v_1\rangle &= |0\ldots000\rangle = |1\rangle \\ |v_2\rangle &= |0\ldots001\rangle = |2\rangle \\ &\vdots \qquad\qquad\quad \vdots \\ |v_{2^{16}}\rangle &= |1\ldots111\rangle = \left|2^{16}\right\rangle \end{aligned}$$

Preliminaries: Quantum States

$$\begin{aligned}\mathcal{I}\left(\left|\psi\right\rangle, \left|\phi\right\rangle\right) &= \text{inner product} \\ &= \left\langle\psi\right| \cdot \left|\phi\right\rangle \\ &= \langle\psi|\phi\rangle \in \mathbb{C}\end{aligned}$$

$$\begin{aligned}\mathcal{O}\left(\left|\psi\right\rangle, \left|\phi\right\rangle\right) &= \text{outer product} \\ &= \left|\psi\right\rangle \cdot \left\langle\phi\right| \\ &= |\psi\rangle\langle\phi| \in \mathbb{C}^{2^n \times 2^n}\end{aligned}$$

Unitary Evolution

Preliminaries: Unitary Evolution

$$U \left| q_{\text{old}} \right\rangle = \left| q_{\text{new}} \right\rangle$$

$$U^{-1} = U^{\dagger} = (U^{*})^{T} = \left(U^{T}\right)^{*}$$

Preliminaries: Unitary Evolution

$$|q_{\text{initial}}\rangle \in \mathcal{H}$$

Preliminaries: Unitary Evolution

$$U_1 \left| q_{\text{initial}} \right\rangle \in \mathcal{H}$$

Preliminaries: Unitary Evolution

$$U_2 U_1 \left| q_{\text{initial}} \right\rangle \in \mathcal{H}$$

Preliminaries: Unitary Evolution

$$m \in \mathbb{N}$$

$$U_m \cdots U_2 U_1 \left| q_{\text{initial}} \right\rangle \in \mathcal{H}$$

Preliminaries: Unitary Evolution

$$m \in \mathbb{N}$$

$$|q_{\text{final}}\rangle = U_m \cdots U_2 U_1 \, |q_{\text{initial}}\rangle \in \mathcal{H}$$

Preliminaries: Unitary Evolution

$$m \in \mathbb{N}$$

$$|q_{\text{final}}\rangle = U_m \cdots U_2 U_1 |q_{\text{initial}}\rangle \in \mathcal{H}$$

Figure : Our first quantum algorithm.

Measurements

Preliminaries: Measurements

$$|\psi\rangle = \sum_{i=1}^{2^n} c_i \cdot |v_i\rangle \in \mathcal{H}$$

$$\sum_{i=1}^{2^n} |c_i|^2 = 1 \qquad (*)$$

Preliminaries: Measurements

$$|\psi\rangle = \sum_{i=1}^{2^n} c_i \cdot |v_i\rangle \overset{\text{Measurement}}{\Rightarrow} \exists j : |\psi'\rangle = |v_j\rangle$$

$$\Pr\left[\text{The outcome is } j.\right] = |c_j|^2$$

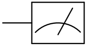
Preliminaries: Measurements

$$|\psi\rangle = \sum_{i=1}^{2^n} c_i \cdot |v_i\rangle \overset{\text{Measurement}}{\Rightarrow} \exists j : \left|\psi'\right\rangle = |v_j\rangle$$

$$\overset{\text{Measurement}}{\Rightarrow} \left|\psi''\right\rangle = |v_j\rangle$$

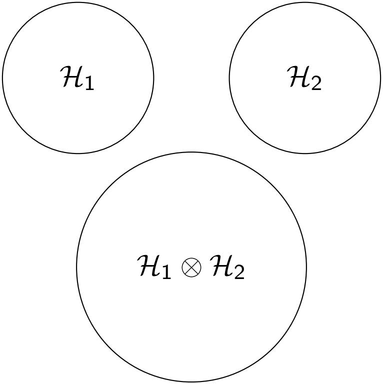
$$\begin{aligned} \Pr\left[\text{The outcome is } j.\right] &= |1|^2 \\ &= 1 \end{aligned}$$

Preliminaries: Measurements

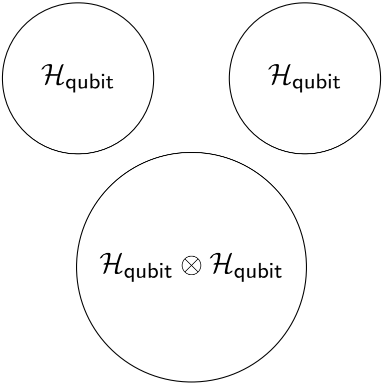


Composition

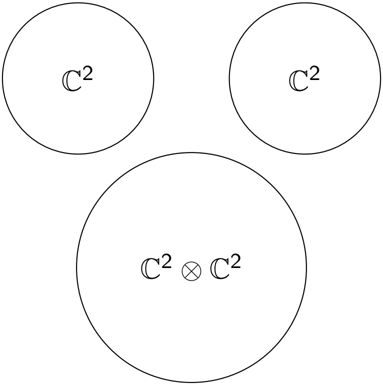
Preliminaries: Composition



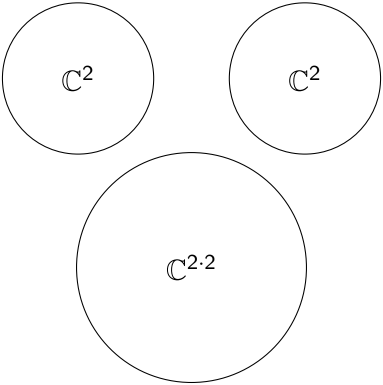
Preliminaries: Composition



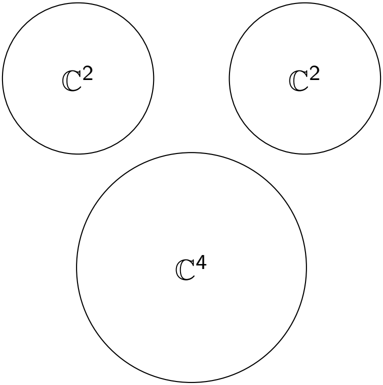
Preliminaries: Composition



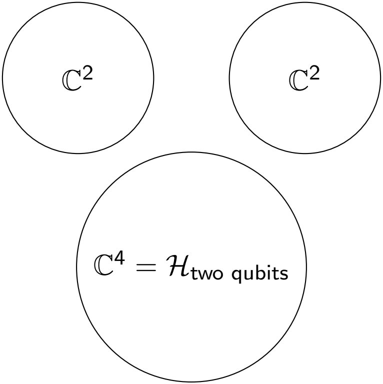
Preliminaries: Composition



Preliminaries: Composition



Preliminaries: Composition



Preliminaries: Composition

A useful property:

$$\underbrace{(U_1 \otimes U_2)}_{U}(|x\rangle \otimes |y\rangle) = U_1 |x\rangle \otimes U_2 |y\rangle .$$

A Comparison

Preliminaries: A Comparison

Table : Quantum mechanics and probability theory.

Probability Theory	Quantum Mechanics
Real numbers in $[0, 1]$	Complex numbers
Real numbers that sum to 1	Complex numbers that the squares of their magnitudes sum to 1
The *sum* is equal to 1	The *Euclidean norm* is equal to 1
The *sum* is preserved	The *Euclidean norm* is preserved
The L_1-norm is preserved	The L_2-norm is preserved
Use of stochastic matrices	Use of unitary matrices

The Algorithm

The Algorithm

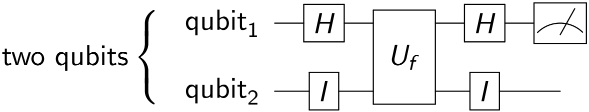
Deutsch's Problem.

Input : A black-box U_f for $f : \{0,1\} \to \{0,1\}$.

Output : The value of $\mathrm{XOR}\left(f\left(0\right), f\left(1\right)\right) = f\left(1\right) \oplus f\left(0\right)$.

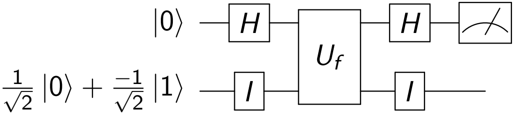
Classically, we need two queries to U_f.
Quantumly, one query to U_f suffices!

The Algorithm

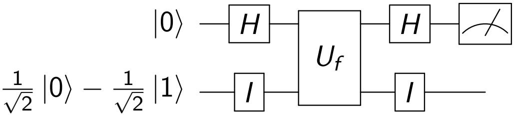


$$|\text{two qubits}\rangle = |\text{qubit}_1\rangle \otimes |\text{qubit}_2\rangle$$

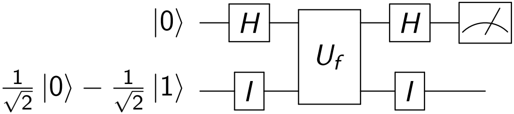
The Algorithm



The Algorithm

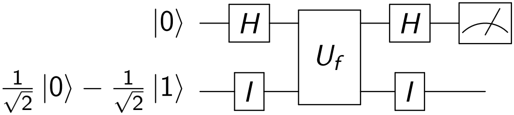


The Algorithm



$$|\psi_0\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$
$$|\psi_1\rangle = U_1 |\psi_0\rangle = (H \otimes I)|\psi_0\rangle$$
$$|\psi_2\rangle = U_2 |\psi_1\rangle = U_f |\psi_1\rangle$$
$$|\psi_3\rangle = U_3 |\psi_2\rangle = (H \otimes I)|\psi_2\rangle$$
$$|\psi_4\rangle = \text{the state after we measure the first qubit of } |\psi_3\rangle$$

The Algorithm



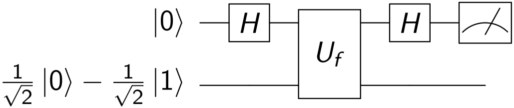
$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

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

$$H^{-1} = H$$

$$I|x\rangle = |x\rangle$$

The Algorithm



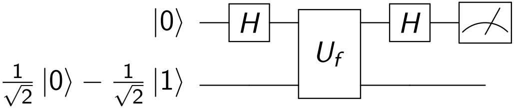
$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

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

$$H^{-1} = H$$

$$I|x\rangle = |x\rangle$$

The Algorithm



$$|\psi_0\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right)$$

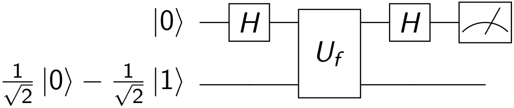
$$|\psi_1\rangle = (H \otimes I) |\psi_0\rangle = \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right)$$

$$= \frac{1}{2} (|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle)$$

$$|\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{2} (|0\rangle \otimes |0 \oplus f(0)\rangle - |0\rangle \otimes |1 \oplus f(0)\rangle + \dots)$$

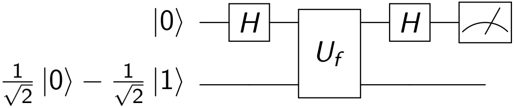
$$\stackrel{*}{=} \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(0) \oplus f(1)}}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}} |1\rangle \right)$$

The Algorithm



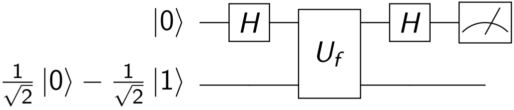
$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(0) \oplus f(1)}}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}} |1\rangle \right)$$

The Algorithm



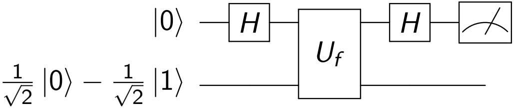
$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{1}}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

The Algorithm



$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

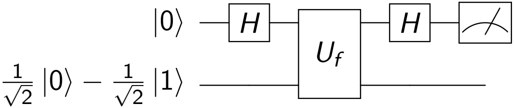
The Algorithm



$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_3\rangle = (H \otimes I)|\psi_2\rangle = |1\rangle \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

The Algorithm

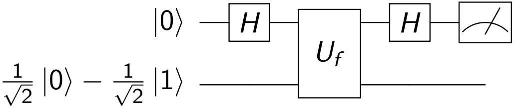


$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_3\rangle = (H \otimes I)|\psi_2\rangle = |1\rangle \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

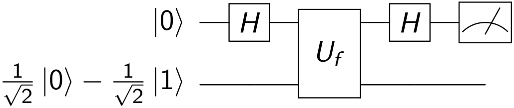
$$= |f(0) \oplus f(1)\rangle \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

The Algorithm



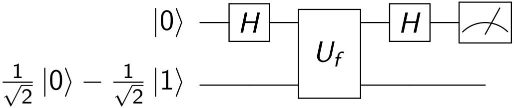
$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(0) \oplus f(1)}}{\sqrt{2}} |1\rangle \right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}} |1\rangle \right)$$

The Algorithm



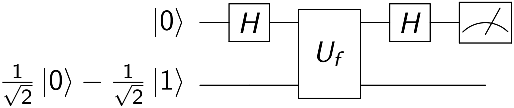
$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{0}}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

The Algorithm



$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

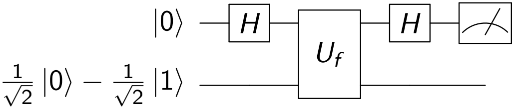
The Algorithm



$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_3\rangle = (H \otimes I)|\psi_2\rangle = |0\rangle \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

The Algorithm



$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

$$|\psi_3\rangle = (H \otimes I)|\psi_2\rangle = |0\rangle \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

$$= |f(0) \oplus f(1)\rangle \otimes \left(\frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle - \frac{(-1)^{f(0)}}{\sqrt{2}}|1\rangle\right)$$

The Algorithm

:D

Misc.

Misc.: Where to start?/References

- *An Introduction to Quantum Computing* (2009), by Kaye, Laflamme, and Mosca.
- *Quantum Computing Since Democritus* (2013), by Aaronson.

Thank you!