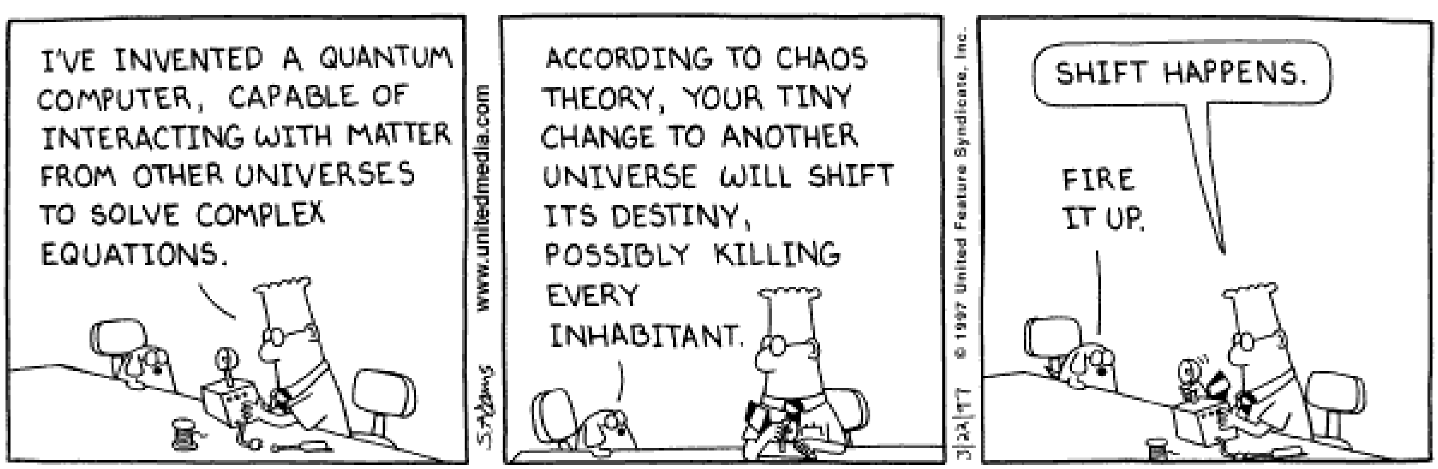
Quantum Computation

Michael A. Nielsen

University of Queensland



What does it mean to compute?

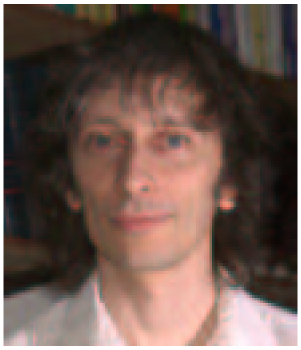
Q: Is there a general algorithm to determine whether a mathematical conjecture is true or false?


Church-Turing:
NO!

Church-Turing thesis: Any algorithmic process can be simulated on a Turing machine.

Ad hoc empirical justification.

Strong Church-Turing thesis: Any algorithmic process can be efficiently simulated on a probabilistic Turing machine.



Deutsch:

Can we justify C-T thesis using laws of physics?

Quantum mechanics seems to be very hard to simulate on a classical computer.

Might it be that computers exploiting quantum mechanics are not efficiently simulatable on a probabilistic Turing machine?

(Violation of strong C-T thesis!)

Might it be that such a computer can solve some computational problems faster than a probabilistic Turing machine?

Candidate universal computer:
quantum computer

Quantum circuit model

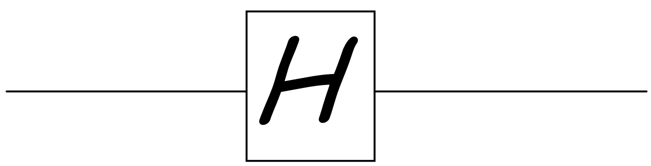
Classical	Quantum
Unit: bit	Unit: qubit
1. Prepare n bit input	1. Prepare n qubit input
2. Logic gates	2. Reversible quantum logic gates
3. Readout value of bits	3. Readout partial information about qubits

Single qubit quantum logic gates

Pauli gates:

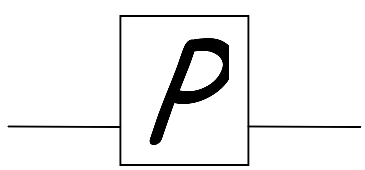
$$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix};\quad Y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix};\quad Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

Hadamard gate:



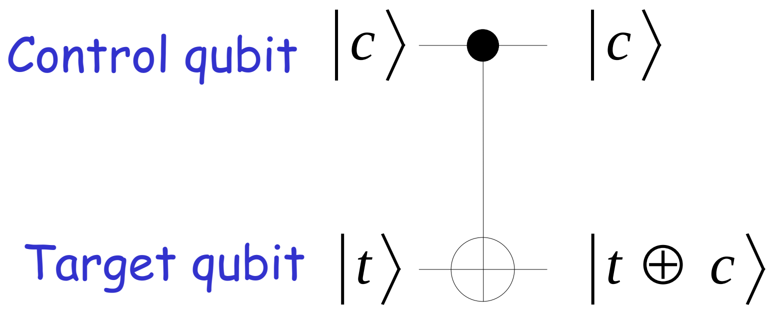
$$H|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}};\quad H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}};\quad H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Phase gate:



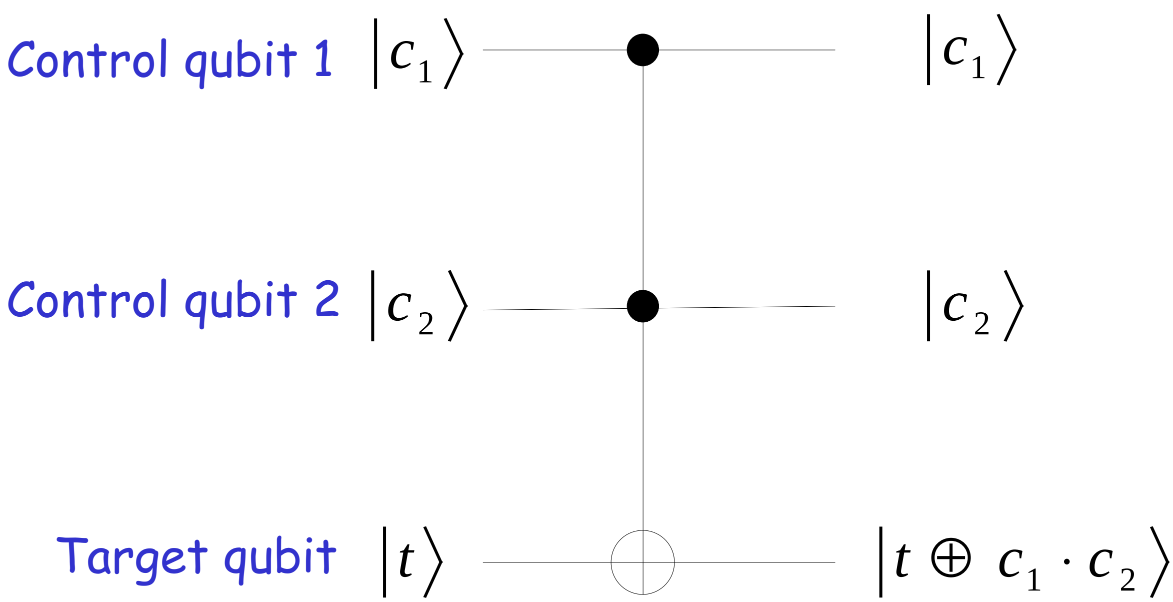
$$P|0\rangle=|0\rangle;\quad P|1\rangle=i|1\rangle$$

Controlled not gate:



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

Toffoli gate



Universal Logic Gates

Suppose U is an arbitrary unitary transformation on n qubits.

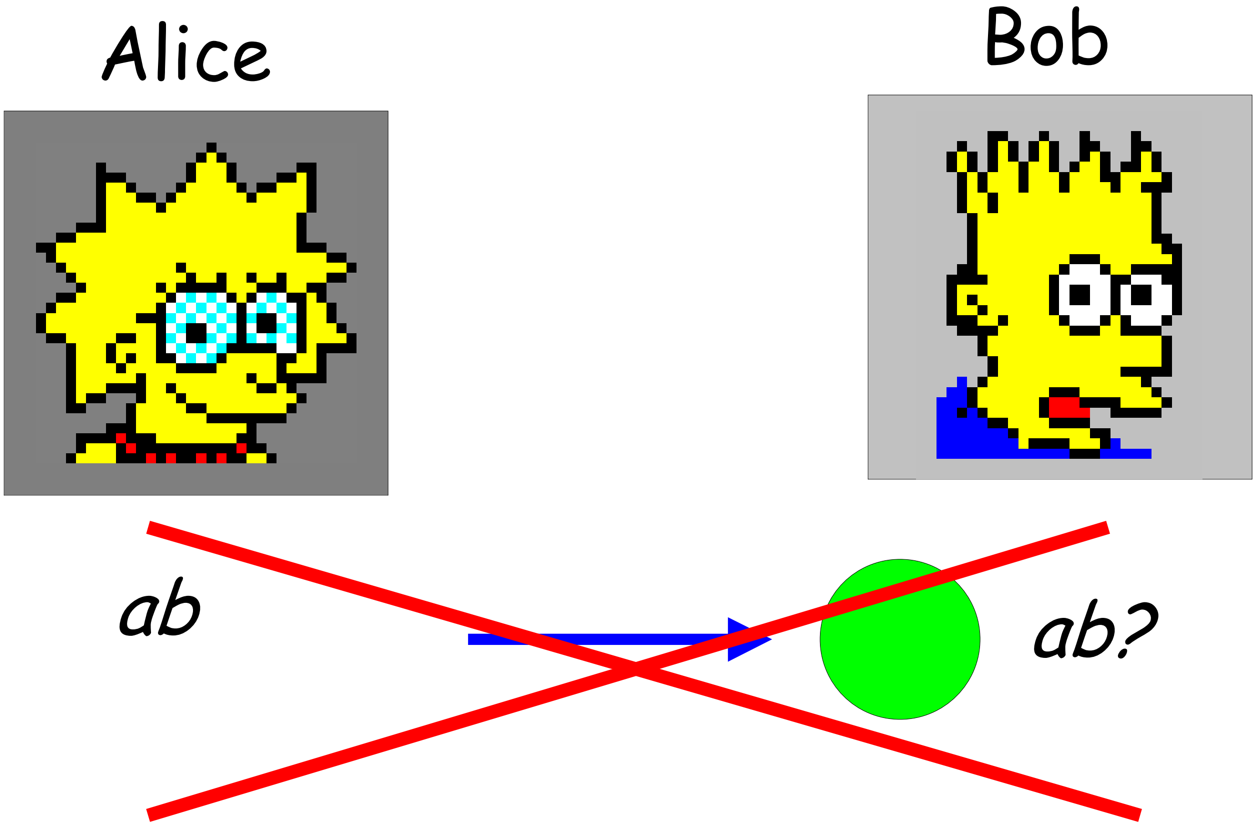
U can be approximated arbitrarily well by a sequence of Hadamard gates, phase gates, controlled not gates, and Toffoli gates.

These gates may all be performed fault-tolerantly, so in principle noise is not a problem.

Quantum circuit model

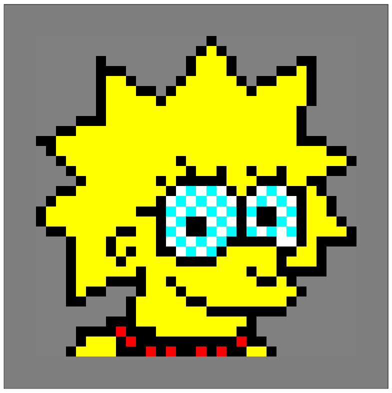
1. Prepare state $|0,0,\ldots,0\rangle$
2. Apply circuit of Hadamard, phase, controlled not and Toffoli gates.
3. Measure in the computational basis.

Superdense coding

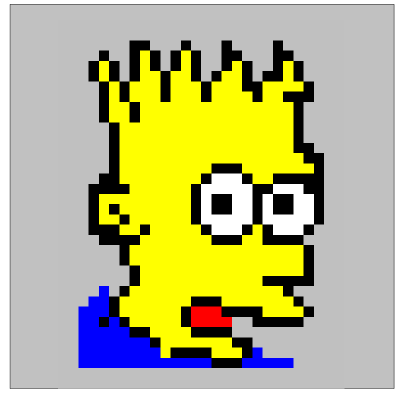


Superdense coding

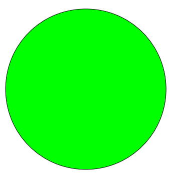
Alice

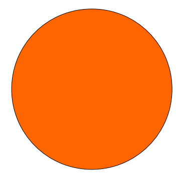


Bob



ab

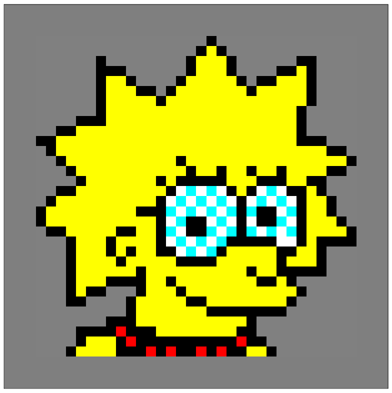


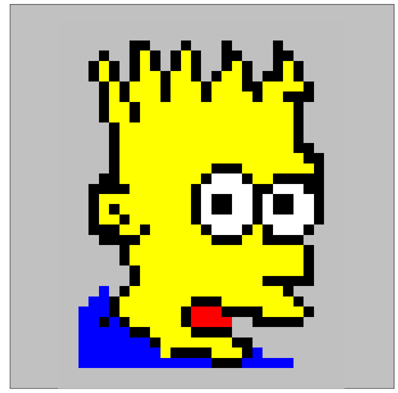


Superdense coding

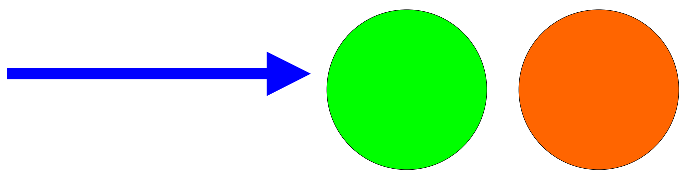
Alice

Bob



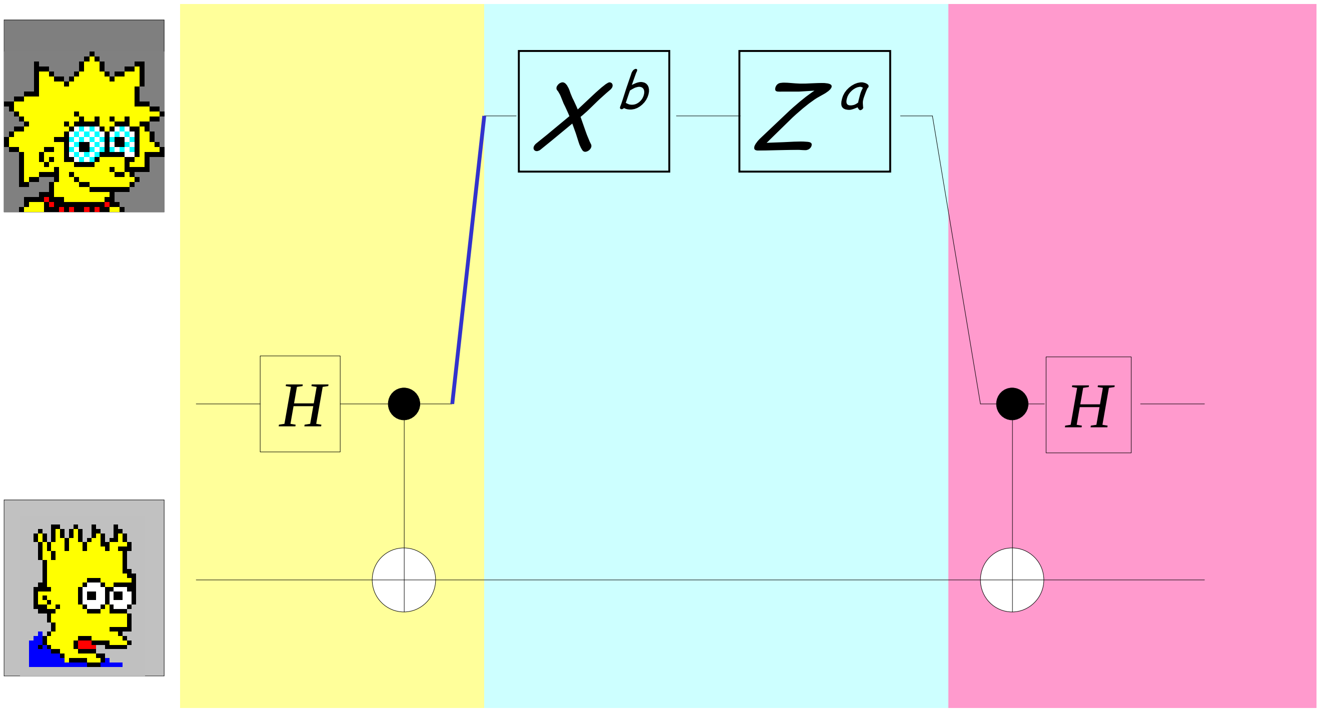


ab



ab?

Superdense coding



$$00 \to 00 + 10 \to 00 + 11$$

$$00 + 11$$

$b = 0$: $00 + 11$ $b = 1$: $10 + 01$

$a = 0$: $00 + 11$ $a = 1$: $00 - 11$ $a = 0$: $10 + 01$ $a = 1$: $-10 + 01$

$$00 + 11 \quad 00 - 11 \quad 10 + 01 \quad -10 + 01$$

$$ab = 01: \; 10 + 01 \to 11 + 01 \to 01$$

Example: Deutsch's problem

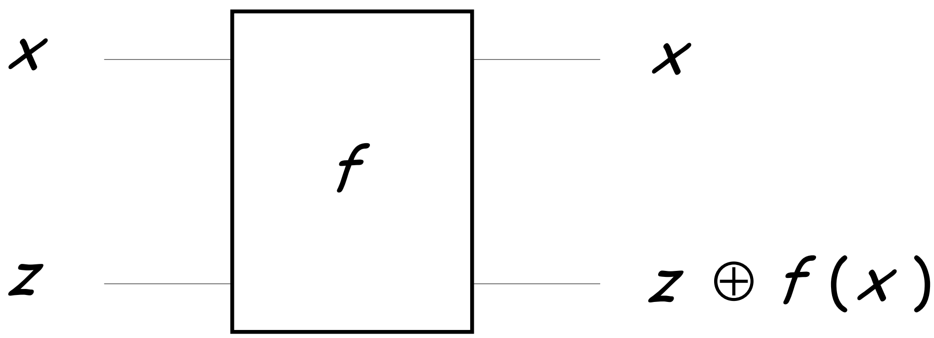
Given a black box computing a function $f:\{0,1\} \to \{0,1\}$

Our task is to determine whether f is constant or balanced?

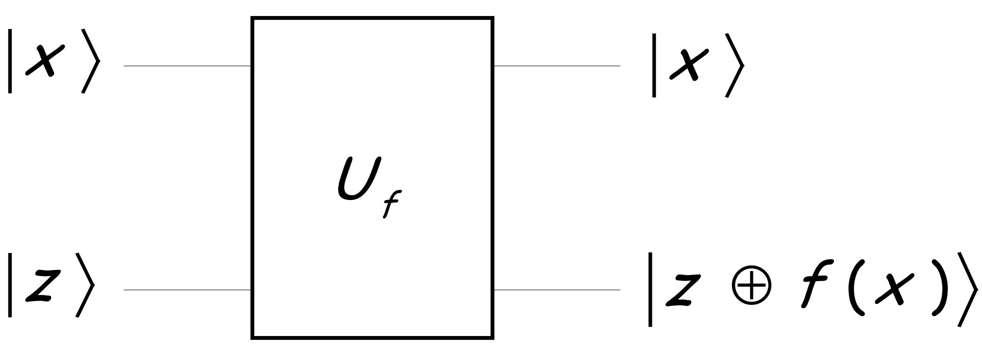
Classically we need to evaluate both $f(0)$ and $f(1)$.

Quantumly we need only use the black box for $f(\bullet)$ once!

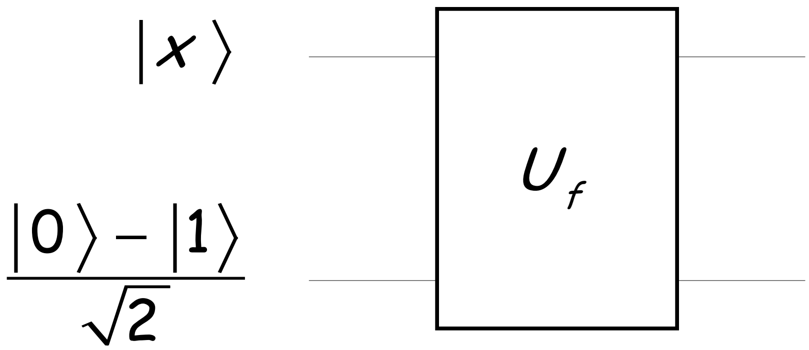
Classical black box



Quantum black box



Putting information in the phase



$f(x) = 0:$

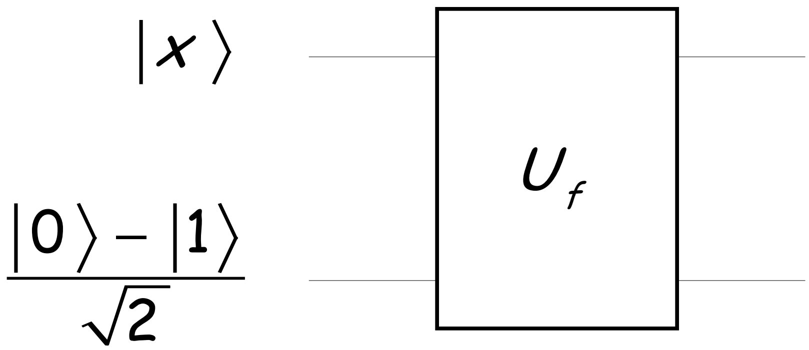
$$|x\rangle(|0\rangle - |1\rangle) \rightarrow |x\rangle(|0\rangle - |1\rangle)$$

$f(x) = 1:$

$$|x\rangle(|0\rangle - |1\rangle) \rightarrow |x\rangle(|1\rangle - |0\rangle)$$
$$= -|x\rangle(|0\rangle - |1\rangle)$$

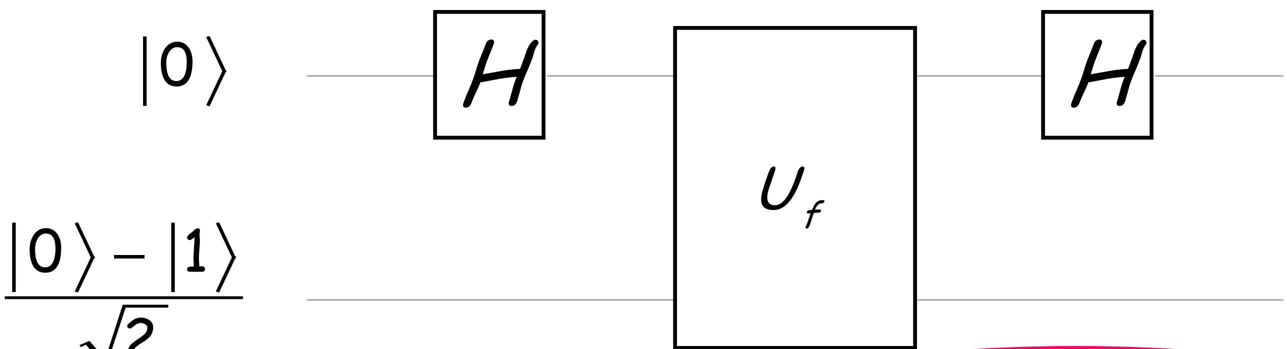
$$|x\rangle(|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Putting information in the phase



$$|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$$

Quantum algorithm for Deutsch's problem



Quantum parallelism

$$|0\rangle \to |0\rangle + |1\rangle$$

$$\to (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$

$$\to (-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)$$

$$= \left[(-1)^{f(0)} + (-1)^{f(1)}\right]|0\rangle + \left[(-1)^{f(0)} - (-1)^{f(1)}\right]|1\rangle$$

f const. $\Rightarrow$ all amplitude in $|0\rangle$.

f balan. $\Rightarrow$ all amplitude in $|1\rangle$.

[redacted]