Quantum Algorithms

Class of computations performable using quantum circuits?

Compare with computations performable using classical circuits?

Which task is performed better using a QC than a classical computer?

Can we realise classical algorithms using a quantum circuit?

Yes.

Why?

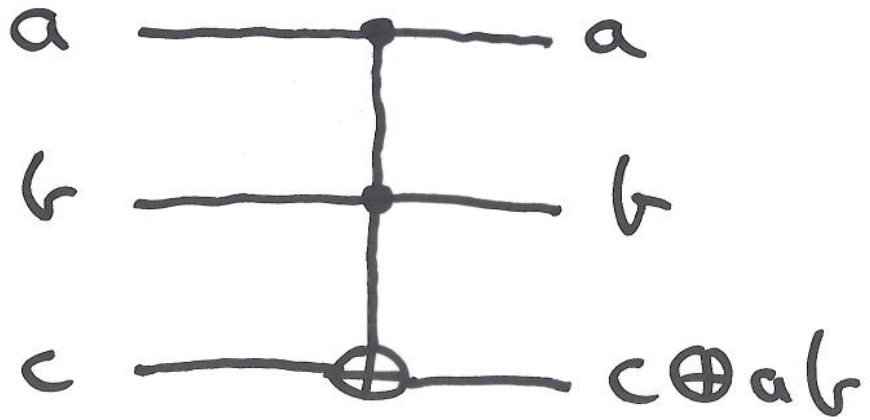
classical $\subset$ quantum

....but... must replace classical components by <u>reversible</u> quantum elements.

Toffoli Gate

$$(a, b, c) \longrightarrow (a, b, c \oplus ab)$$

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



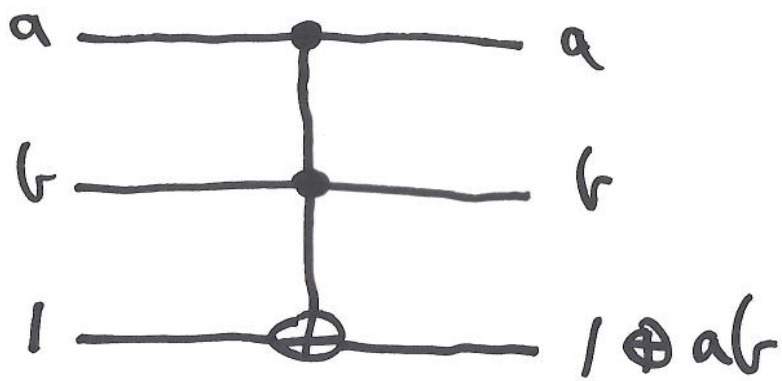
Toffoli Gate is Reversible

Check,

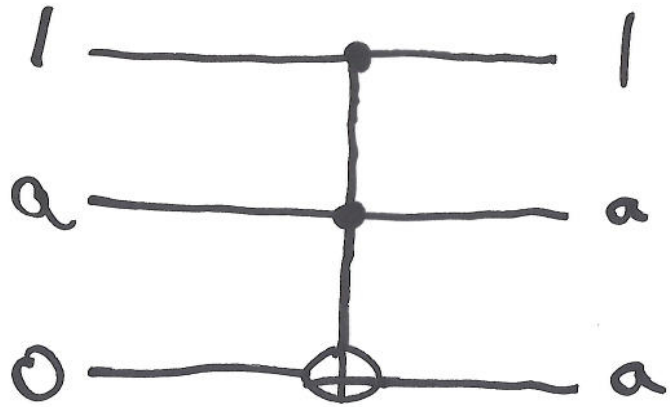
$$(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c \oplus ab \oplus ab)$$

$$U_T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad \text{clearly } U_T U_T = I$$

Toffoli Gate can simulate NAND and FANOUT



NAND



FANOUT

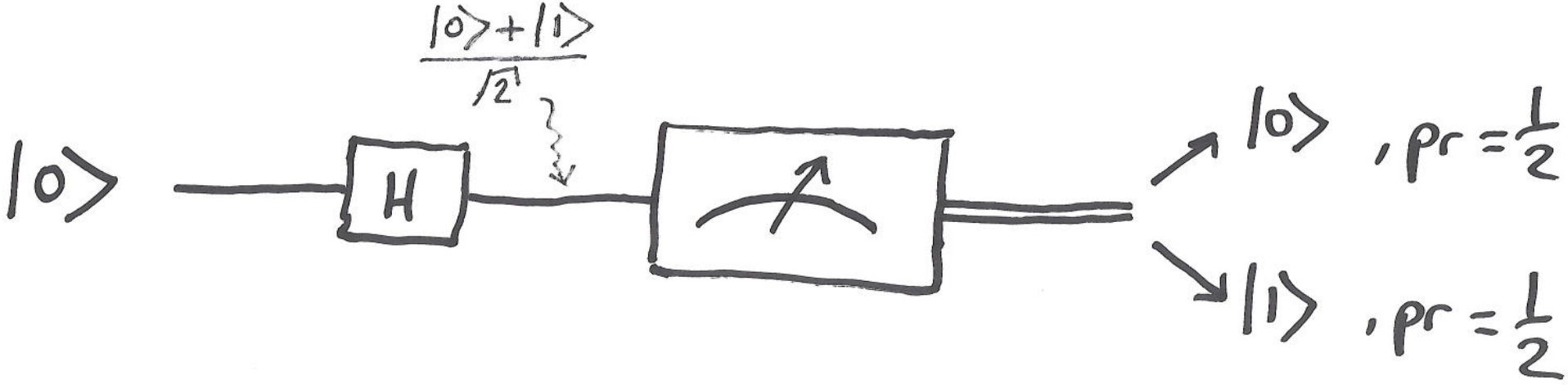
Therefore,

classical universality is ensured.

Classical Non-Deterministic?

i.e. can quantum circuit generate random classical bits?

YES.



Quantum Parallism

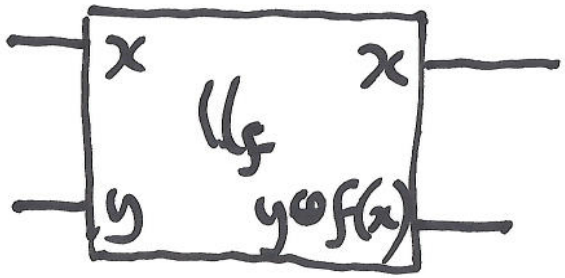
QCs evaluate a function $f(x)$ for many different values of x simultaneously,

.... Sort of...

$f(x) : \{0,1\} \rightarrow \{0,1\}$ on a QC?

$$|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$$

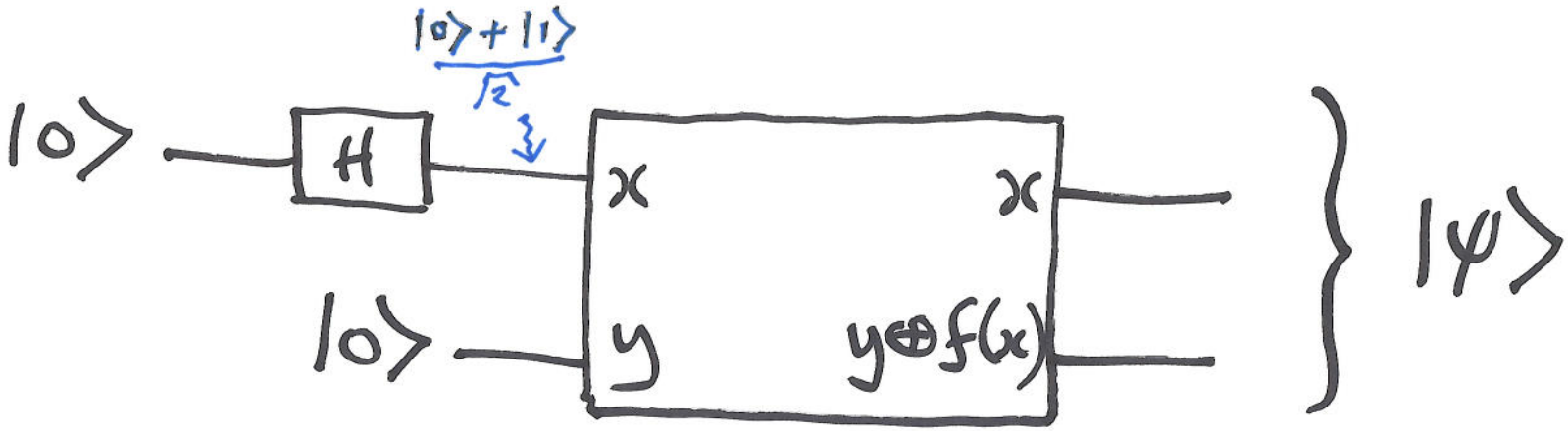
i.e.



U_f is always unitary, i.e. U_f is reversible
(input is stored at the output)

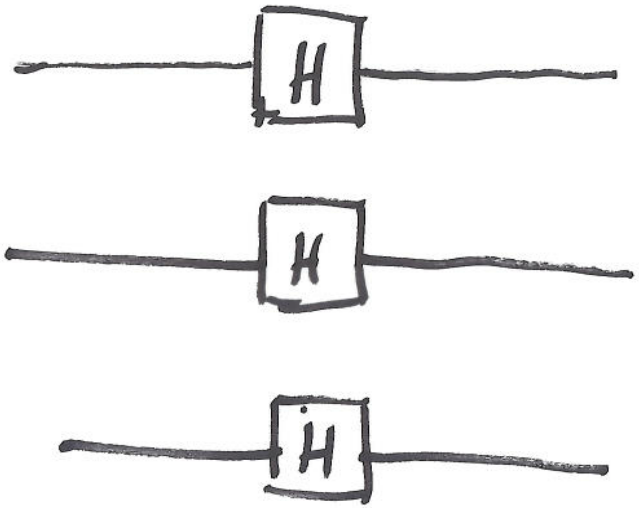
When $y=0$, then second qubit stores $f(x)$.

Computing Everything at Once



f(0) and f(1) are evaluated simultaneously!

Hadamard Transform



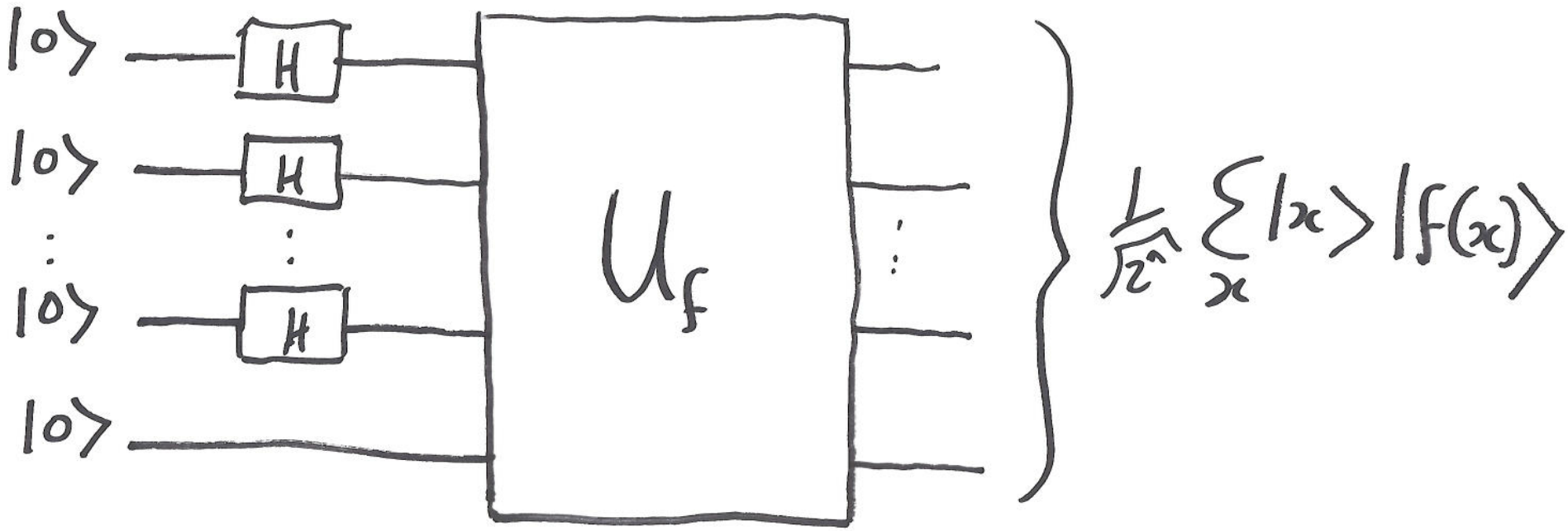
$$H^{\otimes n} = H \otimes H \otimes \ldots H,$$

where $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle = H^{\otimes n} |0\rangle$$

..... produces "quantum superposition"

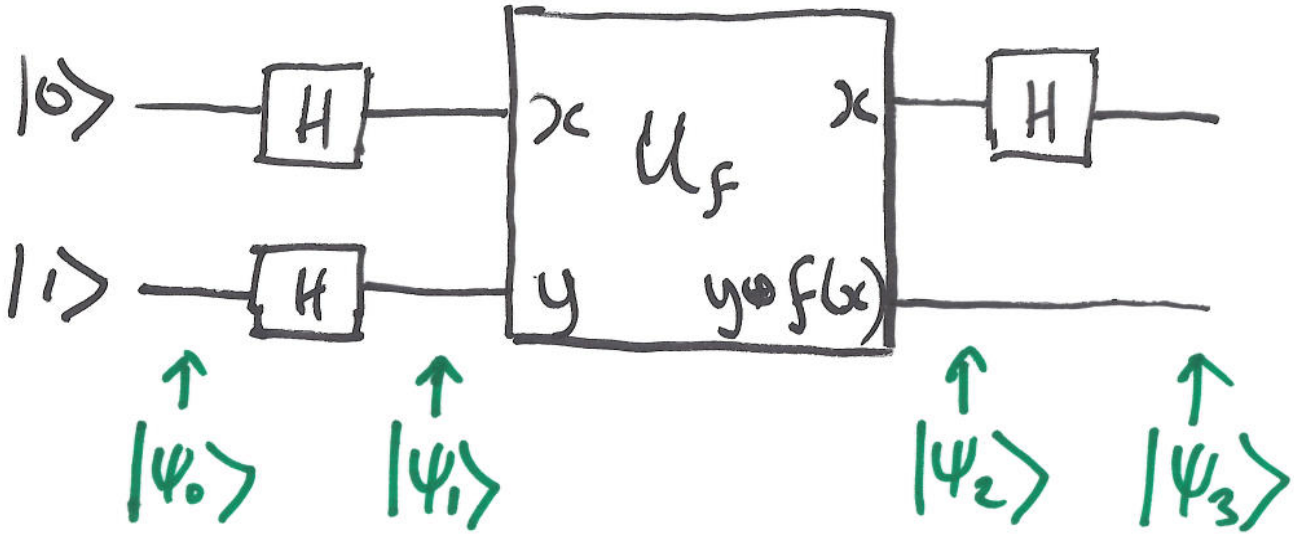
Everything Computed at Once



....the catch...

measurement of output only gives us one of the values, $f(x)$, for a single value of x.

Deutsch's Algorithm



$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|x\rangle\left(|0\rangle - |1\rangle\right)/\sqrt{2} \longrightarrow (-1)^{f(x)}|x\rangle\left(|0\rangle - |1\rangle\right)/\sqrt{2}$$

$$\Rightarrow$$

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

$$\Rightarrow$$

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1) \end{cases}$$

$$\Rightarrow |\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Quantum Speed-Up - global information about f obtained

Result is,

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

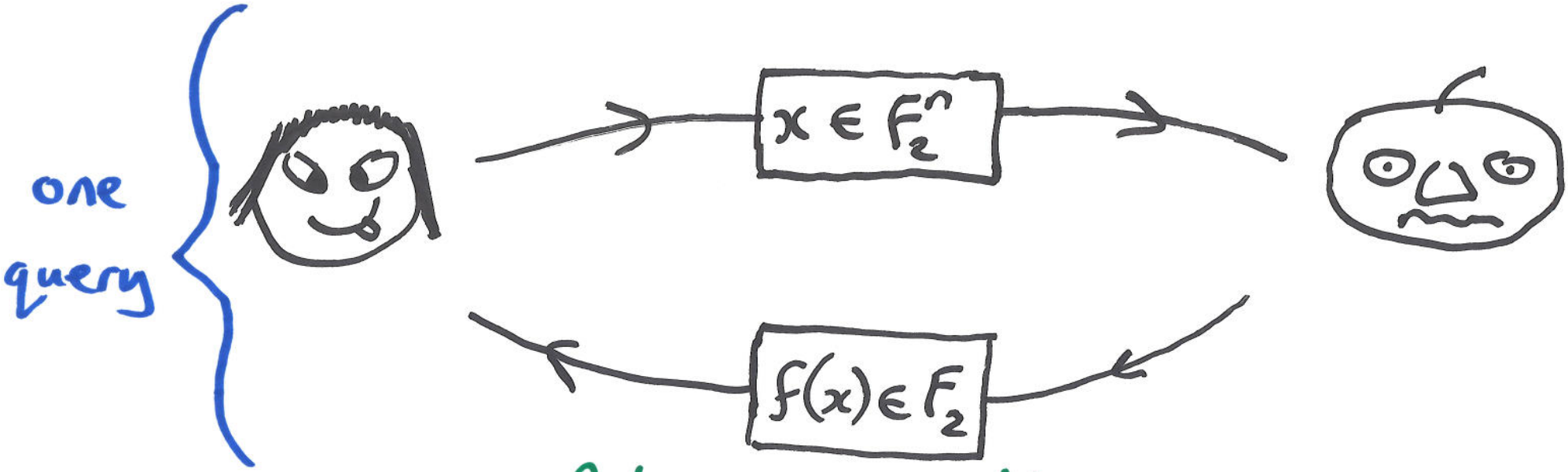
Therefore,

measuring first qubit allows us to determine,

$$f(0) \oplus f(1)$$

classical apparatus would require at least two evaluations.

Deutsch-Josza Algorithm



Bob's promise to Alice:
f is constant or balanced

Alice's Challenge:

Determine with certainty whether Bob has chosen a constant or balanced function. Use minimum correspondence

Classical case

Worst-case : $2^{n-1}+1$ queries

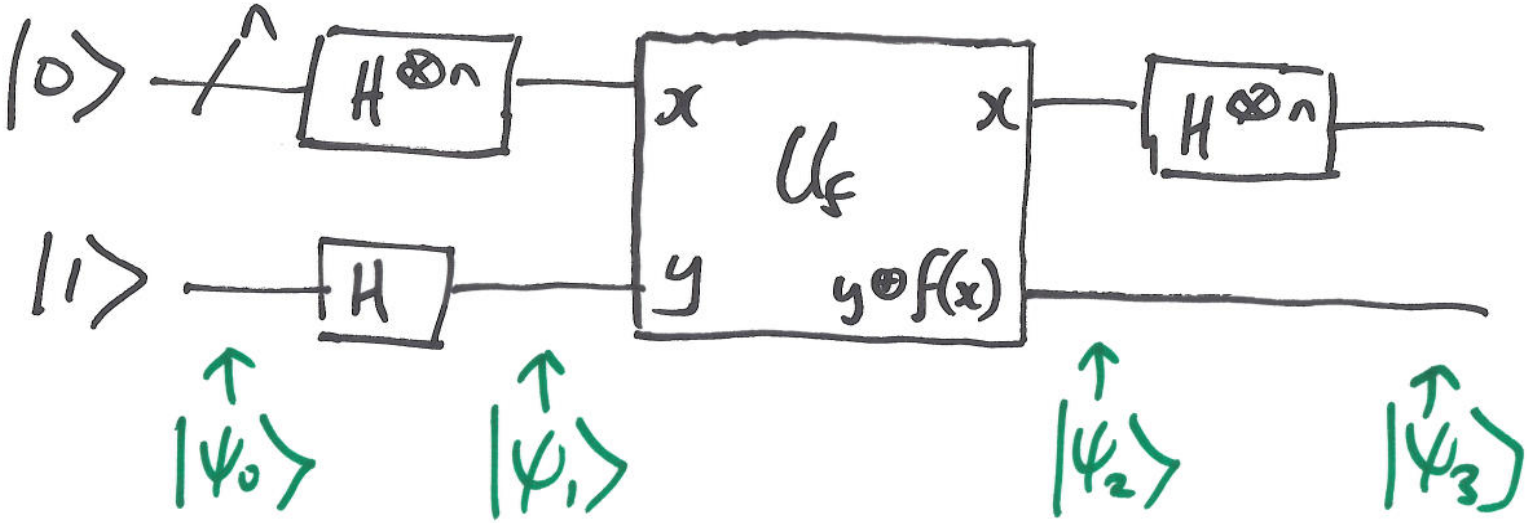
.... each query requires Alice → Bob n bits
Bob → Alice 1 bit

Quantum case

One query required.

Catch: qubits exchanged
f computed using U_f

Deutsch-Josza Algorithm



$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_3\rangle = \sum_z \sum_x (-1)^{x \cdot z + f(x)} |z\rangle / 2^n \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Observe:

$$H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$$

$$\Rightarrow H^{\otimes n}|x_1,\ldots x_n\rangle = \sum_{z_1\ldots z_n} (-1)^{x_1z_1+\ldots+x_nz_n}\frac{|z_1,\ldots z_n\rangle}{\sqrt{2^n}}$$

$$\Rightarrow H^{\otimes n}|x\rangle = \sum_z \frac{(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}$$

... So...

$$|\psi_3\rangle = H^{\otimes n}|\psi_2\rangle = H^{\otimes n}\sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$= \sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{2^n}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Alice measures query register (leftmost n qubits)

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}}{2^n} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

For f constant:

assume measurement result is $|00\ldots0\rangle$. Then $x\cdot z = 0$ for all x, and coefficient of $|00\ldots0\rangle$ is 1. Then the coefficient for all other values of $|z\rangle$ is 0 (by Parseval's theorem). Therefore measurement yields $|z\rangle = |00\ldots0\rangle$ with probability 1.

For f balanced:

assume measurement result is $|00\ldots0\rangle$. Then $(-1)^{x\cdot z + f(x)}$ is 1 for $2^n/2$ values of x, and -1 for $2^n/2$ values of x. Therefore the coefficient of $|00\ldots0\rangle$ is zero.

$|z\rangle = |00\ldots0\rangle$ is measured with probability 0.

Summary - Deutsch-Josza - deterministic

Inputs: (1) Black box, U_f,
(2) Promise: f is constant or balanced.

Outputs: $|00\ldots0\rangle$ if and only if f is constant.

Runtime: One evaluation of U_f.

Procedure:

1. Initialize state to $|0\rangle^{\otimes n}|1\rangle$
2. Create superposition: $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
3. Evaluate U_f: $\sum_x (-1)^{f(x)}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
4. Perform Hadamard transform: $\sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$
5. Measure to obtain z.

Probabilistic Classical Algorithm

- Class exercise

What is the performance of the best classical algorithm to distinguish between a constant and balanced function with error probability

$$\varepsilon < \frac{1}{2} ?$$

Deutsch-Josza algorithm is a simplified version of linear cryptanalysis

Let $f(x)$ be a Boolean function which is "close" to an affine function, $a(x) = a_0 + a_1 x_1 + a_2 x_2 + \ldots$

Then, using the Deutsch-Josza set-up, with high probability,

$$z = (a_0, a_1, \ldots a_n)$$

will be measured.

Why?

There are three known classes of quantum algorithm which provide an advantage over known classical algorithms

1. Quantum versions of the Fourier transform (e.g. Deutsch-Josa)
2. Quantum search
3. Quantum simulation

Quantum algorithms based on the Fourier transform

DFT:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j$$

Quantum version:

Define U such that,

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle = U|j\rangle$$

U is unitary.

The Quantum Fourier Transform

$$\sum_{k=0}^{2^n-1} y_k |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi i jk/2^n} x_j \right] |k\rangle = U\left(\sum_{j=0}^{2^n-1} x_j |j\rangle \right)$$

. . . . . subtle implementation . . .

How Fast Can a Fourier Transform be Computed?

for $N = 2^n$.

Classically

$$\simeq N \log(N) = n 2^n,$$

Quantum

$$\simeq \log^2(N) = n^2$$

exponential advantage.

The Catch

The output spectral coefficients are hidden.

Measurement only yields the index to <u>one</u> spectral coefficient from this vector,

(probably the index with highest or (near)-highest magnitude).

Hidden Subgroup Problem - generalization

....solvable by the "QFT"

Let f be a function from a finitely generated group, G, to a finite set, X, such that f is constant on the cosets of a subgroup, K, and distinct on each coset.

Given a quantum black box for performing the unitary transform,

$$U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle, \quad g \in G,\ h \in X$$

where "$\oplus$" is an appropriately chosen binary operation on X, find a generating set for K.

Quantum Search Algorithms

– discovered by Grover.

Given a search space of size N, and no prior knowledge as to the structure of the space, how long does it take to find an element in the search space satisfying a given property?

Classically : N operations

Quantum : $\sqrt{N}$ operations

Quantum Simulation

Problem:

Simulate quantum mechanical system with n components

Classical : c^n memory bits

Quantum : kn qubits

... but result is "hidden"

Moore's Law

QCs keep pace with Moore's Law if a single qubit is added to the QC every two years.