Monday, October 22, 2018 9:17 AM

Deutsch-Jozsa.

We don't expect to be able to show that
$BPP \neq BQP$ → quantum computers are more powerful than classical

This would imply $P \neq PSPACE$
↳ Seems like it should be true but it's a long-standing open problem to prove this.

Instead: Show that quantum computers are more powerful than classical if they both have access to an oracle.

Oracle Model: there is some Boolean function
$f: \{0,1\}^n \to \{0,1\}$

An algorithm can access the oracle by providing an x and getting back $f(x)$.

We want to solve some problem in this model
Usually this involves discovering something about f.

Monday, October 22, 2018 9:17 AM

An algorithm only has black box access to f.
The only way to learn anything about f is to query the oracle.

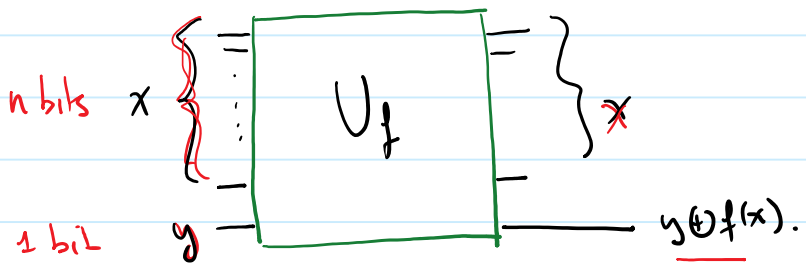
→ Can call the function but not see the code or even know how long it takes.

Usually f is a hard-to-compute function so measure the complexity of an algorithm in terms of the number of calls to f.

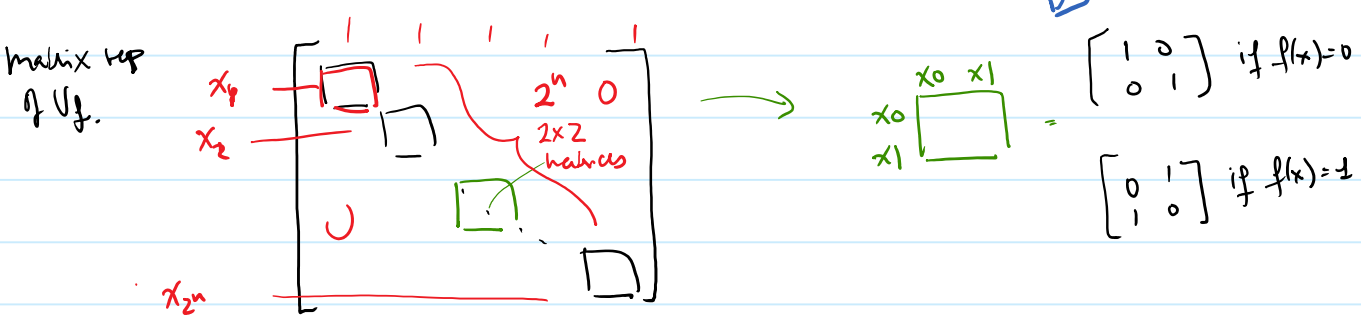
Access to f in the quantum model:

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

x: n-bits, y: 1-bit

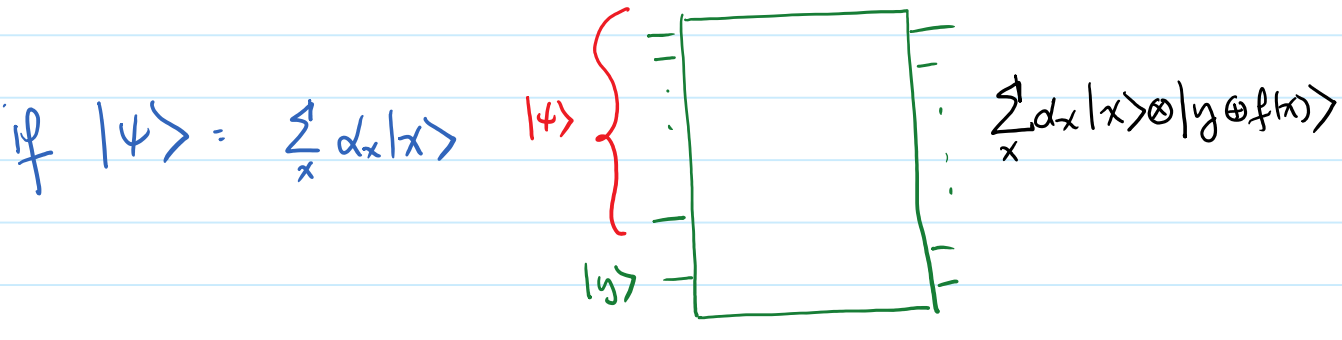


Note:
U_f is unitary.



Monday, October 22, 2018 9:17 AM

Quantum advantage: Can access oracle in superposition.
(Can query f on multiple inputs and have it count as one query).
Limited as to how it can access result by quantum measurement.



We will show two examples showing that quantum computation is provably more powerful than quantum in this model.

Although a bit contrived they did lead to more interesting applications.

Monday, October 22, 2018 9:17 AM

Deutsch-Jozsa

in this problem, we are promised that f is either:

all 0: $f(x) = 0 \quad \forall x$

balanced: $f(x) = 1$ for exactly half of $x \in \{0,1\}^n$.

Problem: determine which one is the case.

Classical complexity:

Deterministic $\geq \frac{2^n}{2} + 1$ queries required in the worst case.

Worst case: the first $2^n/2$ x's queried have $f(x) = 0$.

Randomized: best strategy is to query k random locations $x_1, \ldots, x_k$.

output:

If $f(x_i) = 1$ for some i $\Rightarrow$ Balanced

If $f(x_i) = 0$ for all i $\Rightarrow$ all 0.

Only possible error:

f is balanced + $f(x_i) = 0 \ \forall i$.

probability of error $= 1/2^k$.

If balanced, a random guess $f(x) = 0$ w.p. $1/2$.

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

$\left(\frac{1}{\sqrt{2}}\right)^2(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Quantum protocol will get the correct answer in 2 queries with 0 probability of error.

Start with $|0\rangle^n|0\rangle$

Apply H to the first n qubits to get:

$$|+\rangle^n|0\rangle = \frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes|0\rangle$$

$$H^{\otimes n}\otimes I_{n+1}\,|0\rangle^n|0\rangle = |+\rangle^n|0\rangle$$

$$= \left[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right]^{\otimes n}|0\rangle = \left(\frac{1}{\sqrt{2}}\right)^n\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle$$

n bits, 1-bit.

Monday, October 22, 2018 9:17 AM

Now apply U_f: $\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$

$U_f : |x\rangle|y\rangle \to |x\rangle|y\oplus f(x)\rangle$ (n, 1)

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

Apply Z to the last qubit to get: $\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle(-1)^{f(x)}$

Apply U_f again $\quad (f(x)\oplus f(x) = 0)$

$$\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle(-1)^{f(x)}|0\rangle$$

f(x) now only stored in the phase.

We won't use the last qubit again, so we'll drop it.

Deutsch-Jozsa - page 6

Monday, October 22, 2018 9:17 AM

$|\phi_{f'}\rangle = \sum_x |x\rangle (-1)^{f'(x)}$ $\quad f' \equiv 0.$

Define $\Rightarrow |\phi_f\rangle = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle.$

If f is 0 and f' is balanced (or vice versa) then

$f' \equiv 0$ f balanced.

$\langle \phi_f | \phi_{f'} \rangle = 0$

$\sum_x (-1)^{f(x)} (-1)^{f'(x)} \langle x | x \rangle$

if f is all 0's $= \sum_x (-1)^{f'(x)}$

half $+1$, half -1

Still true for $U|\phi_f\rangle$ $U|\phi_{f'}\rangle$ where U is unitary.

The unitary we will choose is $H^{\otimes n}$

If $f \equiv 0$ $\quad |\phi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle = (|+\rangle)^n$ $\quad \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^n$

$H^{\otimes n} |\phi_f\rangle = H(|+\rangle)^n = |0\rangle^n$

If f is balanced $H|\phi_f\rangle$ is orthogonal to $|0\rangle^n$

$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$ $\quad \alpha_{\vec{0}} = 0$

Deutsch-Jozsa - page 6.5

Wednesday, October 24, 2018 2:13 PM

$|\phi_f\rangle = \sum_x (-1)^{f(x)} |x\rangle$ f balanced.

$|\phi_{f'}\rangle = \sum_x (-1)^{f'(x)} |x\rangle$ $f' \equiv 0$

$\langle \phi_f | \phi_{f'} \rangle = \left[\sum_y (-1)^{f(y)} \langle y| \right] \left[\sum_x |x\rangle \right]$

$\sum_{xy} (-1)^{f(y)} \langle y|x\rangle = \sum_{x \in \{0,1\}^3} (-1)^{f(x)} = 0.$

$(y_1 + \cdots + y_n)(x_1 + \cdots + x_n) = \sum_{ij} y_i x_j$

Monday, October 22, 2018 10:48 AM

$\Rightarrow f \equiv 0$: $H^{\otimes n} |\phi_f\rangle = |0\rangle^n$

$\Rightarrow$ f balanced : $H^{\otimes n} |\phi_f\rangle$ orthogonal to $|0\rangle^n$

↳ when expressed in the standard basis, amplitude of $|00\cdots0\rangle$ is 0.

Measure all the qubits:

If $\geq$ one 1 then balanced.

If all 0's then $f \equiv 0$.

Applied U_f 2 x

Or: Compute the AND of all the qubits and measure the 1-qubit result.

A little unsatisfying because the randomized classical algorithm for this problem is still pretty good.

$n \longleftrightarrow 2^n$

quantum (classical rand.