Nothing Here

Fast Quantum Algorithms

or

How we learned to put our pants on two legs at a time.

Dave Bacon

Institute for Quantum Information

California Institute of Technology

?

A sudden bold and unexpected question doth many times surprise a man and lay him open.

A prudent question is one-half of wisdom.

Iway amway Akespeareshay!

Sir Francis Bacon
(1561-1628)

William Shakespeare
(1568-1623)

“small Latin, less Greek” ?

WarNING

This Talk Under Constant Acceleration

DB and CBSSS assume no responsibility for injuries sustained while zoning out.

Quantum Computers Can Do Amazing Things!

THIS TALK

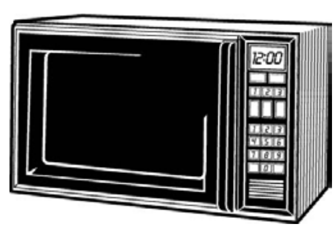
Understanding what makes quantum evolution *different*.

How quantum evolution can used to do something cool.

How quantum evolution can be used to exponentially speed up an oracle problem over classical deterministic algorithms.

How quantum evolution can be used to exponentially speed up an oracle problem over classical probabilistic algorithms.

Randomizing Microwave



Digital Coffee
(Not Java!)

Mystery Markov Microwave

Scalding Hot
H

Freezing Cold
C

Markov

The true method of knowledge is experiment. - William Blake 1788

- Run Experiments To Understand MMM Machine

If you put in C, 70% of the time you get H out
and 30% of the time you get C out
If you put in H, 80% of the time you get H out
and 20% of the time you get C out

- A nice little formalism

$$\text{H} \longrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{C} \longrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$M_{mm} = \begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix}$$

columns sum to 1

0 ≤ matrix entry ≤ 1

$$\begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.8 \\ 0.2 \end{pmatrix}$$

$$\begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0.7 \\ 0.3 \end{pmatrix}$$

Markov Chains



78 % H
22 % C

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.8 \\ 0.2 \end{pmatrix} \qquad \begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix}\begin{pmatrix} 0.8 \\ 0.2 \end{pmatrix} = \begin{pmatrix} 0.78 \\ 0.22 \end{pmatrix}$$

or

$$\begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix}\begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix} = \begin{pmatrix} 0.78 & 0.77 \\ 0.22 & 0.23 \end{pmatrix} \qquad \begin{pmatrix} 0.78 & 0.77 \\ 0.22 & 0.23 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.78 \\ 0.22 \end{pmatrix}$$



52 % H
48 % C

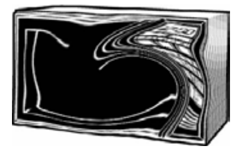
$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.8 \\ 0.2 \end{pmatrix} \qquad \begin{pmatrix} 0.5 & 0.6 \\ 0.5 & 0.4 \end{pmatrix}\begin{pmatrix} 0.8 \\ 0.2 \end{pmatrix} = \begin{pmatrix} 0.52 \\ 0.48 \end{pmatrix}$$

or

$$\begin{pmatrix} 0.5 & 0.6 \\ 0.5 & 0.4 \end{pmatrix}\begin{pmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{pmatrix} = \begin{pmatrix} 0.52 & 0.53 \\ 0.48 & 0.47 \end{pmatrix} \qquad \begin{pmatrix} 0.52 & 0.53 \\ 0.48 & 0.47 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0.52 \\ 0.48 \end{pmatrix}$$

Quantum Microwave

Quantum Digital Coffee



Quantum Microwave (QM)

Scalding Hot **Freezing Cold**

H **C**

What are the rules for the Quantum Microwave?

The Amplitude Attitude

H **C**

$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

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

qubit

$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ Complex numbers $(a + bi)$ $\mathbb{C}$

$\alpha|0\rangle + \beta|1\rangle$

If we measure the state then

with probability $|\alpha|^2$ we get H

with probability $|\beta|^2$ we get C

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

For Our Purposes

$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ Real numbers $\mathbb{R}$

$\alpha|0\rangle + \beta|1\rangle$

$-1 \leq \alpha \leq 1$

$-1 \leq \beta \leq 1$

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

If we measure the state then

with probability α^2 we get H

with probability β^2 we get C

Expert Note: Quantum computation with real numbers is equivalent to quantum computation with complex numbers as a consequence of $SU(N) \subseteq SO(2N)$.

Unitary $\neq$ COVENANT OF UNITARIAN UNIVERSALIST PAGANS

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}\frac{\alpha+\beta}{\sqrt{2}}\\ \frac{\alpha-\beta}{\sqrt{2}}\end{pmatrix}$$

$$\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\frac{\alpha+\beta}{\sqrt{2}}\\ \frac{\alpha-\beta}{\sqrt{2}}\end{pmatrix}$$

In general this matrix U must be unitary:

$$UU^{\dagger} = I$$

i.e. the rows U are orthogonal vectors.

For our purposes (real numbers), this becomes

$$UU^{T} = I$$

Matrix entries will be between -1 and 1

Interference

$$\begin{pmatrix}1\\0\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}$$

50 % **H**
50 % **C**

$$\begin{pmatrix}1\\0\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}1\\0\end{pmatrix}$$

100 % **H**
0 % **C**

$$\begin{pmatrix}1\\0\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}$$

50 % **H**
50 % **C**

$$\begin{pmatrix}1\\0\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix} \rightarrow \begin{pmatrix}0\\1\end{pmatrix}$$

0 % **H**
100 % **C**

Deutsch's Problem

(1985)

two qubits

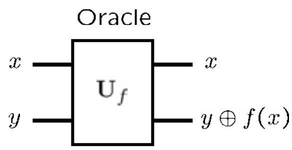
$\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array}$$

David Deutsch

Dr. Falcon

Delphi



$x, y, f(x) \in \{0, 1\}$

Example $f(x) = x$:

$$\mathbf{U}_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Four possible functions $f(x)$:

$$\underbrace{f(x) = 0 \quad f(x) = 1}_{\text{Constant functions}} \; \underbrace{f(x) = x \quad f(x) = \bar{x}}_{\text{Balanced functions}}$$

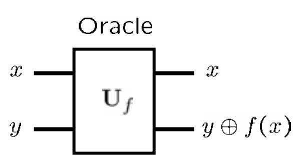
Deutsch's Problem

Determine whether f(x) is constant or balanced using as few queries to the oracle as possible.

Classical Deutsch

Four possible functions $f(x)$:

$$\underbrace{f(x) = 0 \quad f(x) = 1}_{\text{Constant functions}} \; \underbrace{f(x) = x \quad f(x) = \bar{x}}_{\text{Balanced functions}}$$



$x, y, f(x) \in \{0, 1\}$

Query input of x_0 and y_0 only gives information about $f(x_0)$.

Knowing $f(x_0)$ not enough to distinguish constant from balanced.

Classically we need to query the oracle <u>two</u> times to solve Deutsch's Problem

Quantum Deutsch

1. Query oracle with $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
2. Producing the state $\frac{1}{2}\left(|0f(0)\rangle - |0\bar{f}(0)\rangle + |1f(1)\rangle - |1\bar{f}(1)\rangle\right)$

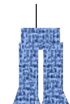
$f(x) = 0$	$f(x) = 1$	$f(x) = x$	$f(x) = \bar{x}$
$\frac{1}{2}(\lvert 00\rangle - \lvert 01\rangle + \lvert 10\rangle - \lvert 11\rangle)$	$\frac{1}{2}(\lvert 01\rangle - \lvert 00\rangle + \lvert 11\rangle - \lvert 10\rangle)$	$\frac{1}{2}(\lvert 00\rangle - \lvert 01\rangle + \lvert 11\rangle - \lvert 10\rangle)$	$\frac{1}{2}(\lvert 01\rangle - \lvert 00\rangle + \lvert 10\rangle - \lvert 11\rangle)$
$\frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}$	$\frac{1}{2}\begin{pmatrix}-1\\1\\-1\\1\end{pmatrix}$	$\frac{1}{2}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}$	$\frac{1}{2}\begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}$

Constant functions

Balanced functions

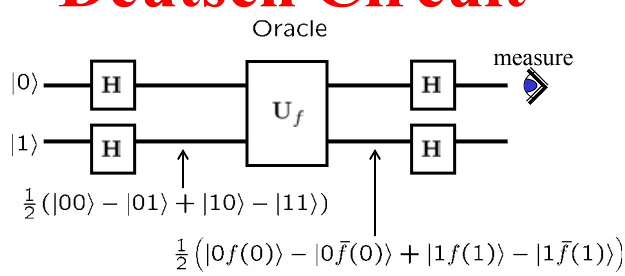
3. Apply the unitary transformation

$$\frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$



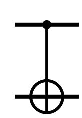
$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\-1\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\-1\end{pmatrix}$
100 % |01⇧	100 % |01⇧	100 % |11⇧	100 % |11⇧

Deutsch Circuit

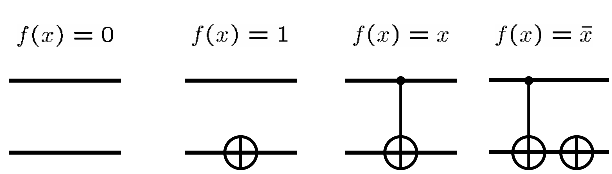


$$\mathbf{H} = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix}$$

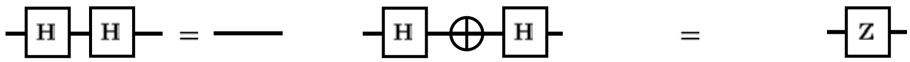
$$\oplus = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$



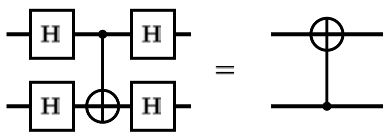
$$= \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$$

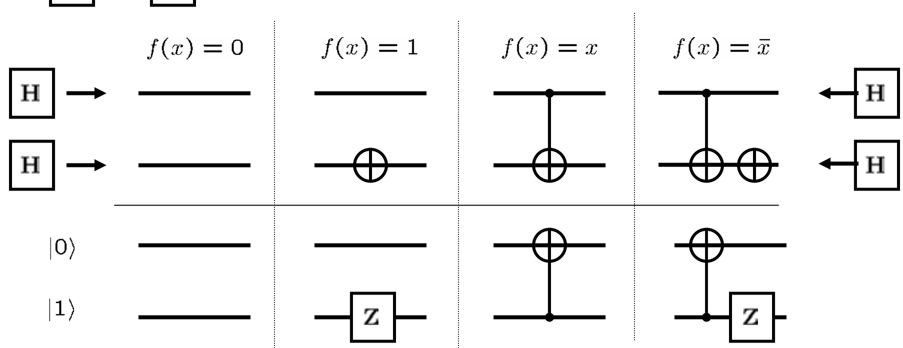


A Different View



$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$





Deutsch In Perspective

Quantum theory allows us to do in a single query what classically requires two queries.

What about problems where the computational complexity is exponentially more efficient?

Deutsch-Jozsa Problem

(1992)

Given a function $f : \{0,1\}^n \to \{0,1\}$

function maps n bit strings to a single bit

f is promised to be either

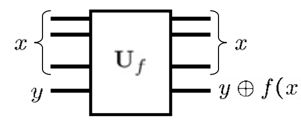
(A) f is constant.

$f(x) = b \ \forall x$

(B) f is balanced.

$f(x) = 1$ if $x \in \mathcal{S}$ otherwise $f(x) = 0$

$\mathcal{S}$ has 2^{n-1} elements.



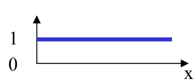
$x \in \{0,1\}^n$

$y, f(x) \in \{0,1\}$

Deutsch-Jozsa Problem

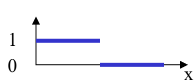
Determine whether f(x) is constant or balanced using as few queries to the oracle as possible.

Classical DJ



(A) f is constant.

$f(x) = b \ \forall x$



(B) f is balanced.

$f(x) = 1$ if $x \in \mathcal{S}$ otherwise $f(x) = 0$

$\mathcal{S}$ has 2^{n-1} elements.

If we never want to be wrong:

Worst case we need $2^{n-1} + 1$ querries

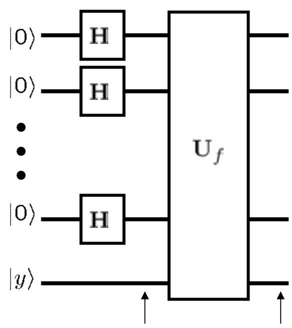
If we allow a failure probability of ϵ, then

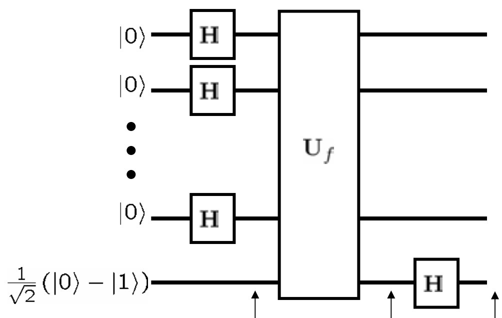
Randomly choose k different x_k to query.

$k = O\left(log\left(\frac{1}{\epsilon}\right)\right)$ (question on website!)

Determinstically hard, probabilistically easy.

Quantum DJ





$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|y\rangle \quad \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|y \oplus f(x)\rangle$$

$$|x\rangle = |x_n x_{n-1}\ldots x_1\rangle$$

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

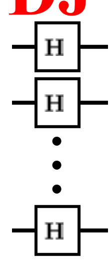
$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|f(x)\rangle - |\bar{f}(x)\rangle\right)$$

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle|1\rangle$$

Quantum DJ

Information about $f(x)$ is in the phase

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle|1\rangle$$



$= \mathbf{H}^{\otimes n}$

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

$$= \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle \qquad x\cdot y = x_n y_n + x_{n-1}y_{n-1} + \cdots + x_1 y_1 \text{ mod } 2$$

All matrix elements of $\mathbf{H}^{\otimes n}$ are $\pm\frac{1}{\sqrt{2^n}}$

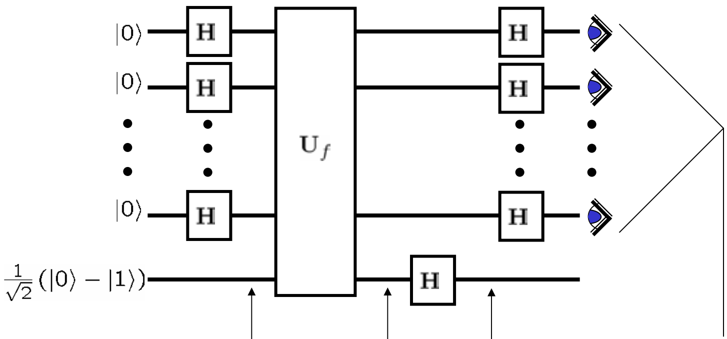
First row of $\mathbf{H}^{\otimes n}$ has all elements $+\frac{1}{\sqrt{2^n}}$

Other rows have equal number $\pm\frac{1}{\sqrt{2^n}}$ elements.

If $f(x)$ is constant, applying $\mathbf{H}^{\otimes n}$ to $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$ always gives $|0\rangle$.

If $f(x)$ is balanced, applying $\mathbf{H}^{\otimes n}$ to $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$ always gives a superposition without $|0\rangle$.

Full Quantum DJ



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

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|f(x)\rangle - |\bar{f}(x)\rangle\right)$$

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle|1\rangle$$

If all bits are 0, then f is constant.

If all bits are not 0, then f is balanced.

Solves DJ with a SINGLE query vs $2^{n-1}+1$ classical deterministic!!!!!!!!!

Simon's Problem

(is that no one does what "Simon says"?) (1994)

Given a function $f : \{0,1\}^n \to \{0,1\}^n$

function maps n bit strings to a n bit strings

f is promised to satisfy either

(A) f is distinct on all inputs.

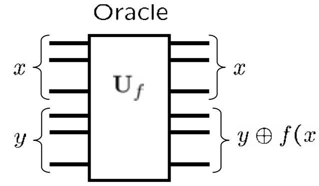
$$f(x) \neq f(y) \quad \forall x \neq y$$

(B) f is distinct up to an XOR mask s

$$f(x) = f(x \oplus s)\ \forall x \qquad (s \text{ is unkown and } \neq 0)$$

$$f(x) \neq f(x \oplus t)\ \forall t \neq s$$

Oracle



$x, y, f(x) \in \{0,1\}^n$

Simon's Problem

Determine whether f(x) has is distinct on an XOR mask or distinct on all inputs using the fewest queries of the oracle. (Find s)

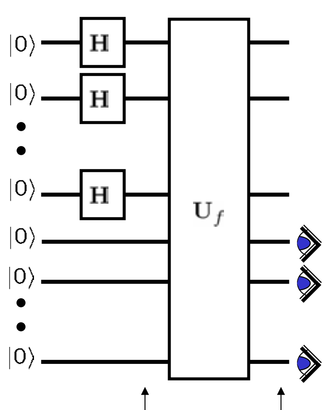
Classical Simon

Now both determinsitcally and probabilistically an exponential number of queries is required.

Left as an exercise for those who are asleep.

Make sure to tell the sleepers that they missed a cameo appearance by my good friend Robin Williams.

Quantum Simon

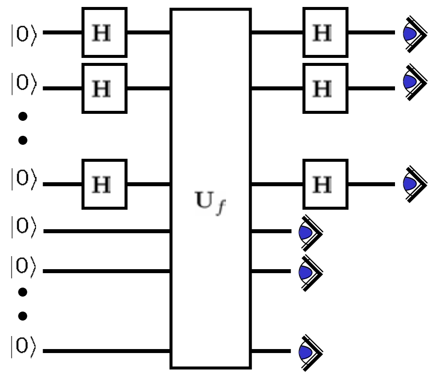


$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle \qquad \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

If $f(x)$ is distinct, then first register will be random $|x\rangle$.

If $f(x)$ is distinct on an XOR map s, then first register will be $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$ for a random x.

Quantum Simon



Quantum Simon

$$\mathbf{H}^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \longleftarrow$$ Equal amplitude and uniform over all y

$$\mathbf{H}^{\otimes n} \frac{1}{\sqrt{2}} (|x\rangle + |x \oplus s\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} \left((-1)^{x \cdot y} |y\rangle + (-1)^{(x \oplus s) \cdot y} |y\rangle \right)$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} (1 + (-1)^{s \cdot y}) |y\rangle \; (1)$$

$\uparrow$

Equal amplitude and uniform over all y such that $y \cdot s = 0$.

If we get $n-1$ linearly independent y's such that $y \cdot s = 0$ we can determine s.

Claim: with probability at most $\frac{1}{4}$, $n-1$ random vectors y such that $y \cdot s = 0$ are linearly independent.

An Open Question

(you could be famous!)

Given a quantum oracle which produces either

(A) $|x\rangle$

(B) $\frac{1}{\sqrt{2}}(|x\rangle + |x+l\rangle)$ l is unkown

$x, l \in \{0, 2^n - 1\}$

both for uniform random $x \in \{0, 2^n - 1\}$

Distinguishing between (A) and (B) using only a polynomial number of queries to the quantum oracle and with an efficient quantum circuit solves the

Dihydral hidden subgroup problem

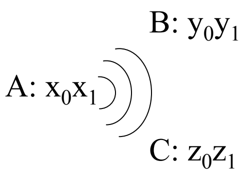
which is a big step towards solving

Graph Isomorphism

Shor Type Algorithms

1985 Deutsch's algorithm	demonstrates task quantum computer can perform in one shot that classically takes two shots.
1992 Deutsch-Jozsa algorithm	demonstrates an exponential separation between classical deterministic and quantum algorithms.
1993 Bernstein-Vazirani algorithm	demonstrates a superpolynomial separation between probabilistic and quantum algorithms.
1994 Simon's algorithm	demonstrates an exponential separation between probabilistic and quantum algorithms.
1994 Shor's algorithm	demonstrates that quantum computers can efficiently factor numbers.

Sample Quantum Communication Complexity



Three parties A, B, C given inputs x,y,z

Want to compute f(x,y,z) via a set protocol of communication.

Ability to "broadcast" information to other two parties. cost=# bits broadcast

SAMPLE WHERE PRESHARED ENTANGLEMENT LOWERS COST

A, B, C each given a two bit string.

guarantee: $x_0y_0z_0 \in \{000, 011, 101, 110\}$, $x_1y_1z_1$ unrestricted

$f(x,y,z) = x_1 \oplus y_1 \oplus z_1 \oplus (x_0 \vee y_0 \vee z_0)$ ($\oplus$ is XOR, $\vee$ is OR)

Quantum: each party has one part of a tripartite entangled state:

$$|\psi\rangle = \tfrac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle) \qquad |abc\rangle = \underset{A}{|a\rangle} \otimes \underset{B}{|b\rangle} \otimes \underset{C}{|c\rangle}$$

Protocol: Hadamard $\equiv H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

1. For each given party, if first bit (x_0,y_0, or z_0) is 1, then apply the Hadamard gate to given part of $|\psi\rangle$

2. Next, measure the respective qubit. Denote the given parties output as a,b,c respectively.

If $x_0y_0z_0$=000, then $|\psi\rangle$ unchanged, $a \oplus b \oplus c = 0$

If $x_0y_0z_0$=110, then $|\psi\rangle \rightarrow \tfrac{1}{2}(|010\rangle - |001\rangle + |111\rangle + |100\rangle)$, $a \oplus b \oplus c = 1$ (etc)

$$a \oplus b \oplus c = x_0 \vee y_0 \vee z_0$$

3. Parties broadcast- A: $(x_1 \oplus a)$ B: $(y_1 \oplus b)$ C: $(z_1 \oplus c)$

Each party can now compute

$$(x_1 \oplus a) \oplus (y_1 \oplus b) \oplus (z_1 \oplus c) = x_1 \oplus y_1 \oplus z_1 \oplus (x_0 \vee y_0 \vee z_0)$$

f(x,y,z) with 3 bits classical result requires: 4 bits

Buhrman, Cleve, Tapp 1997

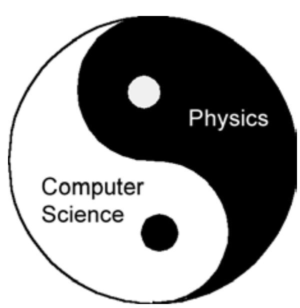
Quantum Communication Complexity

Less communication needed to compute certain functions if either (a) qubit used to communicate or (b) shared entangled quantum states are available.

How much less communciation?

Exponentially less: Ran Raz "Exponential Separation of Quantum and Classical Communication Complexity", 1998

A final word from my sponsors



Physics says to computer science, "your information carriers should be quantum mechanical" and out pops quantum computation!

What can computer science tell us about physics?!?!

Dave Bacon, 156 Jorgensen, dabacon@cs.caltech.edu