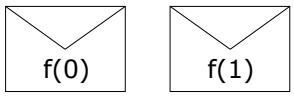
QUANTUM ALGORITHMS

Peter Høyer
www.cpsc.ucalgary.ca/~hoyer

Equips 2006
Sixth Canadian Summer School on Quantum Information Processing
University of Calgary, Canada, August 7-11, 2006

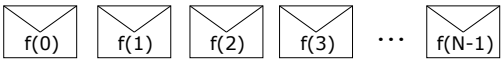
Deutsch's Problem



Is f(0)=f(1)?

Classically: 2 queries
Quantum: 1 query

Grover's Problem



0	1	0	0	1	0	0	0	0	1	0	0

0 N-1

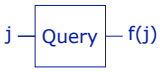
Input: $f:\{0,1,2,\ldots,N-1\}\to\{0,1\}$

Problem: Find integer i such that f(i)=1

You can ask questions of the form: "What is f(j)?"

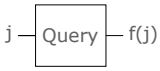
A query

"What is f(j)?"

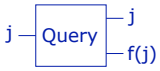


Remember the input

"What is f(j)?"

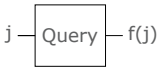


Remember the input:

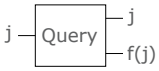


Reversible

"What is f(j)?"



Remember the input:



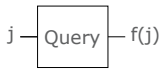
Reversible:

$b \in \{0,1\}$

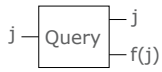
$0\oplus0 = 0$
$0\oplus1 = 1$
$1\oplus0 = 1$
$1\oplus1 = 0$

Unitary query

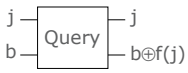
"What is f(j)?"



Remember the input:

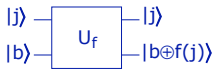


Reversible:



$b \in \{0,1\}$

Unitary:

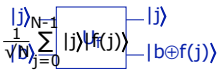


Unitary query

$|j\rangle|b\rangle \mapsto |j\rangle|b\oplus f(j)\rangle$

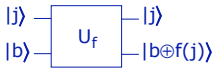
Unitary:

$$\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle|0\rangle \mapsto \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle|f(j)\rangle$$



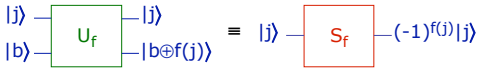
"Apply function f in superposition"

Computational cost

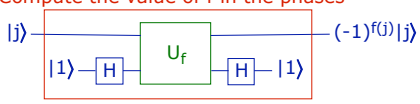


1 query ≡ 1 unit cost

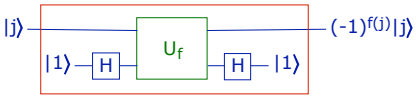
Alternative query model



Proof of ⇒ : "Compute the value of f in the phases"



Equivalence of oracles



$$|j\rangle|1\rangle \xmapsto{H} |j\rangle|0\rangle - |j\rangle|1\rangle$$

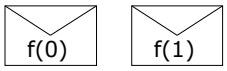
$$\xmapsto{U_f} |j\rangle|f(j)\rangle - |j\rangle|1\oplus f(j)\rangle$$

$$= \begin{cases} |j\rangle|0\rangle - |j\rangle|1\rangle & \text{if } f(j)=0 \\ |j\rangle|1\rangle - |j\rangle|0\rangle & \text{if } f(j)=1 \end{cases}$$

$$= |j\rangle\,(-1)^{f(j)}\,(|0\rangle - |1\rangle)$$

$$\xmapsto{H} (-1)^{f(j)}\,|j\rangle\,|1\rangle \qquad \square$$

Deutsch's Problem in 1 query

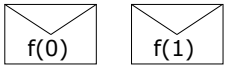


Is f(0)=f(1)?

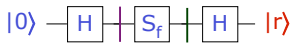
Classical:

Quantum:

Deutsch's Problem in 1 query

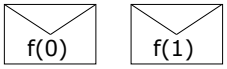


Is f(0)=f(1)?

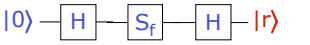


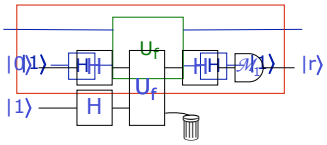
$$|0\rangle \xrightarrow{H} |0\rangle + |1\rangle$$
$$\xrightarrow{S_f} (-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$$
$$= (-1)^{f(0)}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)$$
$$\xrightarrow{H} (-1)^{f(0)}|f(0)\oplus f(1)\rangle \quad \square$$

Deutsch's Problem in 1 query



Is f(0)=f(1)?

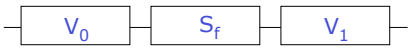




1-query algorithms

Classical:

Quantum:

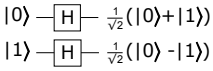


Unitary operators

Unitary ≡ linear, reversible, and preserves probabilities

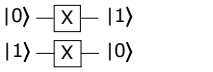
Unitary operators

Hadamard:



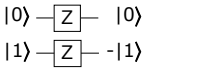
$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Not-gate:



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

Phase-gate:



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

Unitary operators

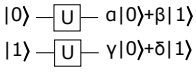
Definition:
Unitary ≡
columns ortho-normal

$1\cdot 1 + 1\cdot(-1) = 0$ $\quad \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

Unitary ≡
orthogonal states
are mapped to
orthogonal states

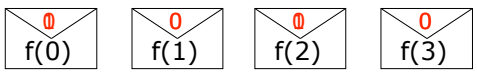
$0\cdot 1 + 1\cdot 0 = 0$ $\quad \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

$1\cdot 0 + 0\cdot(-1) = 0$ $\quad \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$



$\alpha^*\cdot\gamma + \beta^*\cdot\delta = 0$ $\quad \begin{bmatrix}\alpha & \gamma\\ \beta & \delta\end{bmatrix}$

1-out-of-4 in 1 query?



Where is the hidden 1?

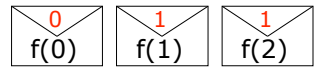
1-out-of-4 in 1 query!

$|0\rangle+|1\rangle+|2\rangle+|3\rangle$ — S_f — $|\psi\rangle$

f	$\lvert\psi\rangle$	
1000	$-\lvert 0\rangle+\lvert 1\rangle+\lvert 2\rangle+\lvert 3\rangle$	$\lvert 0\rangle$
0100	$\lvert 0\rangle-\lvert 1\rangle+\lvert 2\rangle+\lvert 3\rangle$	$\lvert 1\rangle$
0010	$\lvert 0\rangle+\lvert 1\rangle-\lvert 2\rangle+\lvert 3\rangle$	$\lvert 2\rangle$
0001	$\lvert 0\rangle+\lvert 1\rangle+\lvert 2\rangle-\lvert 3\rangle$	$\lvert 3\rangle$

These four states are mutually orthogonal!

These 3 in 1 query?



f = 001 or
f = 011 or
f = 111

Not possible in 1 query!

$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$ — S_f — $|\psi\rangle$

f	$\lvert\psi\rangle$
001	$\alpha\lvert 0\rangle + \beta\lvert 1\rangle - \gamma\lvert 1\rangle$
011	$\alpha\lvert 0\rangle - \beta\lvert 1\rangle - \gamma\lvert 1\rangle$
111	$-\alpha\lvert 0\rangle - \beta\lvert 1\rangle - \gamma\lvert 1\rangle$

NOT possible:
1) These 3 states are mutually orthogonal
2) $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$

1-query algorithms exist?

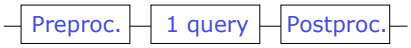
✓ Deutsch's Problem
f∈{00,11} or f∈{01,10}

✓ 1-out-of-4
Which input: 0001, 0010, 0100, or 1000?

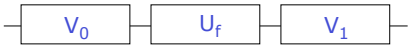
× Sorted inputs
Which input: 001, 011, or 111?

The query model

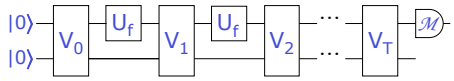
Classical:



Quantum:

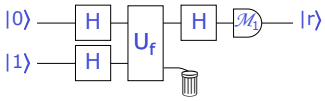


Many queries:



Highlights

Deutsch: f(0) = f(1)?



QUANTUM ALGORITHMS

(Part 2: Fourier Transforms)

Peter Høyer

www.cpsc.ucalgary.ca/~hoyer

Equips 2006

Sixth Canadian Summer School on Quantum Information Processing

University of Calgary, Canada, August 7-11, 2006

Hadamard gate

$$|b_0\rangle \;\boxed{H}\; |0\rangle + (-1)^{b_0}|1\rangle = \sum_{r_0\in\{0,1\}} (-1)^{b_0 r_0}\,|r_0\rangle$$

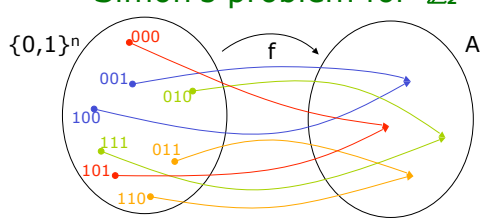
$$|b_0 b_1\rangle \xrightarrow{H^{\otimes 2}} \sum_{r_0 r_1\in\{0,1\}^2} (-1)^{b_0 r_0 + b_1 r_1}\,|r_0 r_1\rangle$$

$$|b\rangle \xrightarrow{H^{\otimes n}} \sum_{r\in\{0,1\}^n} (-1)^{b\bullet r}\,|r\rangle$$

$$|b_1\rangle \;\boxed{H}\; |0\rangle + (-1)^{b_1}|1\rangle$$

$b\in\{0,1\}^n$ $\qquad b\bullet r = \sum_{i=0} b_i r_i$

Simon's problem for $\mathbb{Z}_2^n$



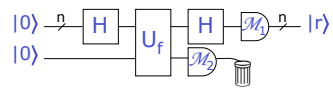
Given: $f:\{0,1\}^n \to A$

Promise: f is 2-to-1

$\exists s\in\{0,1\}^n$: $f(x)=f(x\oplus s)$ for all x

Problem: find s

Simon's algorithm



$$|0\rangle|0\rangle \xrightarrow{H} \sum_{x\in\{0,1\}^n} |x\rangle\,|0\rangle \xrightarrow{U_f} \sum_{x\in\{0,1\}^n} |x\rangle\,|f(x)\rangle$$

$$\xrightarrow{\mathcal{M}_2} |x\rangle + |x\oplus s\rangle$$

$$\xrightarrow{H} \sum_{r\in\{0,1\}^n} (-1)^{r\bullet x}|r\rangle + \sum_{r\in\{0,1\}^n} (-1)^{r\bullet(x\oplus s)}|r\rangle$$

$$= \sum_{r\in\{0,1\}^n} (-1)^{r\bullet x}\,(1+(-1)^{r\bullet s})\,|r\rangle$$

$\exists s\in\{0,1\}^n$: $f(x)=f(x\oplus s)$ for all x

$\xrightarrow{\mathcal{M}_1}$ random r such that $r\bullet s=0$ □

Simon's algorithm

Goal: Find hidden $s\in\{0,1\}^n$

Routine produces:
a random r such that $r\bullet s=0$

Eg. n=5:

$$\begin{array}{l} r^1 = \\ r^2 = \\ r^3 = \\ r^4 = \end{array} \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} s^1 \\ s^2 \\ s^3 \\ s^4 \\ s^5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

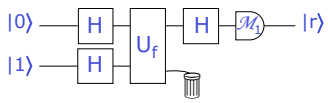
Simon's theorem

Theorem:
Using 3n queries, we can find the hidden s with error $< 1/2^n$.

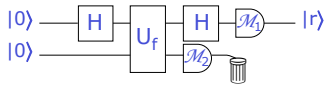
random r such that $r\bullet s=0$

Highlights

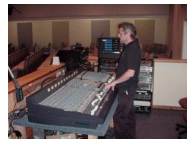
Deutsch: f(0) = f(1)?

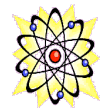


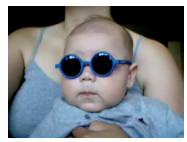
Simon: f(x) = f(x⊕s)



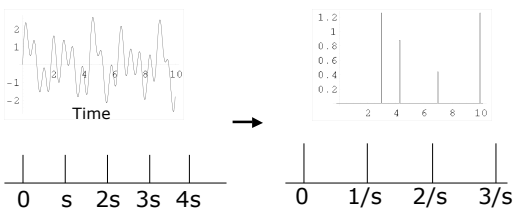
Frequency analysis







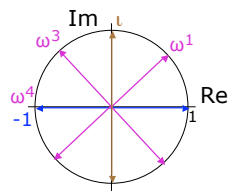
Discrete fourier transforms



Period s

Frequency 1/s
(and higher orders)

Roots of unity



$X^2=1 \Leftrightarrow X\in\{+1,-1\}$

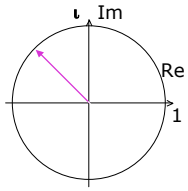
$X^4=1 \Leftrightarrow X\in\{+1,\iota,-1,-\iota\}$

$X^8=1 \Leftrightarrow$
$X\in\{\omega^0,\omega^1,\omega^2,\omega^3,\omega^4,\omega^5,\omega^6,\omega^7\}$

where $\omega = \omega_8 = \exp(2\pi\iota/8)$

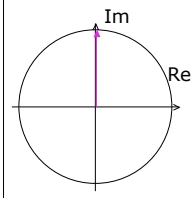
Def: n^{th} principal root is $\omega_n = \exp(2\pi\iota/n)$

Rotating vector



$f_2 = 1, \iota, -1, -\iota, 1, \iota, -1, -\iota$

Rotating vector

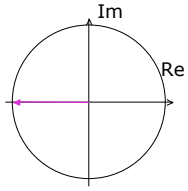


TIME

f_2	1	ι	-1	-ι	1	ι	-1	-ι

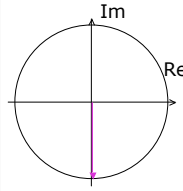
Vector rotating with constant speed

Rotating vector



f_2	1	ι	-1	-ι	1	ι	-1	-ι
f_4	1	-1	1	-1	1	-1	1	-1

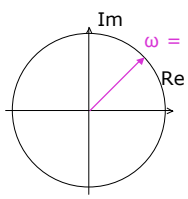
Rotating vector



FREQUENCY

f_2	1	ι	-1	-ι	1	ι	-1	-ι
f_4	1	-1	1	-1	1	-1	1	-1
f_6	1	-ι	-1	ι	1	-ι	-1	ι

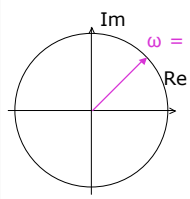
Rotating vector



$\omega = \exp(2\pi\iota/8)$

f_1	1	ω						
f_2	1	ι	-1	-ι	1	ι	-1	-ι
f_4	1	-1	1	-1	1	-1	1	-1
f_6	1	-ι	-1	ι	1	-ι	-1	ι

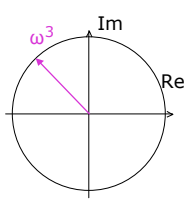
Rotating vector



$\omega = \exp(2\pi\iota/8)$

f_1	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
f_2	1	ι	-1	-ι	1	ι	-1	-ι
f_4	1	-1	1	-1	1	-1	1	-1
f_6	1	-ι	-1	ι	1	-ι	-1	ι

Rotating vector



$\omega = \exp(2\pi\iota/8)$

f_0	1	1	1	1	1	1	1	1
f_1	1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
f_2	1	ι	-1	-ι	1	ι	-1	-ι
f_3	1	ω^3	ω^6	ω	ω^4	ω^7	ω^2	ω^5
f_4	1	-1	1	-1	1	-1	1	-1
f_5	1	ω^5	ω^2	ω^7	ω^4	ω	ω^6	ω^3
f_6	1	-ι	-1	ι	1	-ι	-1	ι
f_7	1	ω^7	ω^6	ω^5	ω^4	ω^3	ω^2	ω

Fourier transform

$F_M = \sum_{i,j=0}^{M-1} \omega^{ij} |i\rangle\langle j| =$

1	1	1	1	1	1	1	1
1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
1	ω^2	ω^4	ω^6	ω^0	ω^2	ω^4	ω^6
1	ω^3	ω^6	ω	ω^4	ω^7	ω^2	ω^5
1	ω^4	ω^0	ω^4	ω^0	ω^4	ω^0	ω^4
1	ω^5	ω^2	ω^7	ω^4	ω	ω^6	ω^3
1	ω^6	ω^4	ω^2	ω^0	ω^6	ω^4	ω^2
1	ω^7	ω^6	ω^5	ω^4	ω^3	ω^2	ω

$\omega = \exp(2\pi i/M)$

- Unitary: $\sum_j \omega^{-j}\omega^{2j} = 0$
- $F_M |0\rangle = \sum_j |j\rangle = F_M^{-1}|0\rangle$
- Computable in time $O(\log^2 M)$

Computable in $O(\log^2 M)$

1	1	1	1
1	ω^2	ω^4	ω^6
1	ω^4	ω^0	ω^4
1	ω^6	ω^4	ω^2

1	1	1	1	1	1	1	1
1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
1	ω^2	ω^4	ω^6	ω^0	ω^2	ω^4	ω^6
1	ω^3	ω^6	ω	ω^4	ω^7	ω^2	ω^5
1	ω^4	ω^0	ω^4	ω^0	ω^4	ω^0	ω^4
1	ω^5	ω^2	ω^7	ω^4	ω	ω^6	ω^3
1	ω^6	ω^4	ω^2	ω^0	ω^6	ω^4	ω^2
1	ω^7	ω^6	ω^5	ω^4	ω^3	ω^2	ω

Computable in $O(\log^2 M)$

1	1	1	1
1	ω^2	ω^4	ω^6
1	ω^4	ω^0	ω^4
1	ω^6	ω^4	ω^2

1	ω	ω^2	ω^3
1	ω^3	ω^6	ω
1	ω^5	ω^2	ω^7
1	ω^7	ω^6	ω^5

1	1	1	1	1	1	1	1
1	ω	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7
1	ω^2	ω^4	ω^6	ω^0	ω^2	ω^4	ω^6
1	ω^3	ω^6	ω	ω^4	ω^7	ω^2	ω^5
1	ω^4	ω^0	ω^4	ω^0	ω^4	ω^0	ω^4
1	ω^5	ω^2	ω^7	ω^4	ω	ω^6	ω^3
1	ω^6	ω^4	ω^2	ω^0	ω^6	ω^4	ω^2
1	ω^7	ω^6	ω^5	ω^4	ω^3	ω^2	ω

$F_4 = F_4 \cdot \mathrm{diag}(\boxed{1 \mid \omega \mid \omega^2 \mid \omega^3})$

$T(M) = T(M/2) + \log M \quad \Rightarrow \quad T(M) = \log^2 M$

Simon's Problem for $\mathbb{Z}_M$

Given: function $f: \mathbb{Z}_M \to A$ (Arbitrary set)

Promise: with period s: $f(x)=f(x+s)=f(x+2s)=\ldots$
f is unique within each period
s is a divisor of M

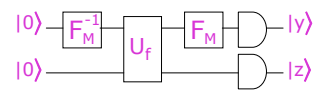
Goal: find s

Example of f with M=15 and period s = 5:

0														14
20	17	3	10	9	20	17	3	10	9	20	17	3	10	9

This problem is a simplification of Shor's quantum algorithm for Integer Factorization

Quantum algorithm

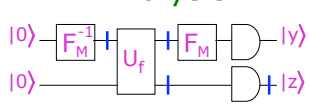


Theorem: $y \in_{random} \{0, M/s, 2M/s, \ldots, (s-1)M/s\}$

Corollary: We can find period s using only 10 queries

- Repeat 10 times. Obtain $y_1, y_2, \ldots, y_{10}$.
- Compute $d = GCD(y_1, y_2, \ldots, y_{10})$.
  Then with high prob., d = M/s.
- Output M/d.

Analysis



$|0\rangle \to \sum_{j=0}^{M-1} |j\rangle \to \sum_{j=0}^{M-1} |j\rangle\,|f(j)\rangle \to \sum_{r=0}^{M/s-1} |k+rs\rangle\,|z\rangle$

$|\psi_k\rangle := \sum_{r=0}^{M/s-1} |k+rs\rangle$

Lemma: $F_M\,|\psi_k\rangle = \sum_{t=0}^{s-1} \omega_s^{tk}\,|t\,M/s\rangle$

Main proof

$|\psi_k\rangle := \sum_{r=0}^{M/s-1} |k+rs\rangle$

Lemma: $F_M\,|\psi_k\rangle = \sum_{t=0}^{s-1} \omega_s^{tk}\,|t\,M/s\rangle$

Pf: $F_M\,|\psi_k\rangle = \sum_{i,j=0}^{M-1} \omega_M^{ij}\,|i\rangle\langle j|\,\sum_{r=0}^{M/s-1} |k+rs\rangle$

$= \sum_{i=0}^{M-1} |i\rangle \left(\sum_{r=0}^{M/s-1} \sum_{j=0}^{M-1} \omega_M^{ij} \langle j|k+rs\rangle\right)$

$= \sum_{i=0}^{M-1} |i\rangle \left(\sum_{r=0}^{M/s-1} \omega_M^{i(k+rs)}\right)$

$= \sum_{i=0}^{M-1} \omega_M^{ik}\,|i\rangle \left(\sum_{r=0}^{M/s-1} \omega_M^{irs}\right)$

$= \sum_{i=0}^{M-1} \omega_M^{ik}\,|i\rangle \left(\sum_{r=0}^{M/s-1} \omega_{M/s}^{ir}\right)$

$= \sum_{i=tM/s} \omega_M^{ik}\,|i\rangle$ □

Simon's Problem for $\mathbb{Z}_M$

Given: function f: $\mathbb{Z}_M \rightarrow A$ (Arbitrary set)
Promise: with period s: f(x)=f(x+s)=f(x+2s)=…
f is unique within each period
s is a divisor of M
Goal: find s

Theorem: We can find s with only 10 queries to f, with probability at least 2/3.

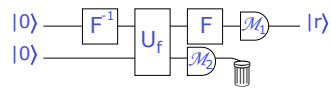
Example of f with M=15 and period s = 5:

0														14
20	17	3	10	9	20	17	3	10	9	20	17	3	10	9

Highlights

$F_M = \sum_{i,j=0} \omega_M^{ij} |i\rangle\langle j|$

Deutsch: f(0) = f(1)?
Simon: f(x) = f(x⊕s)
Shor-like: f(x) = f(x+s) = f(x+2s)=…



Very fast quantum algorithms ≡ finding periodicities