QUANTUM SEARCHING

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

Quadratic speed-up

Cost: was **O(M)**

Now only $O(\sqrt{M})$

* Actual running time on a quantum computer might be incomparable to running time on a classical computer. Availability of quantum computers is limited. Additional error correction not included. Not applicable in conjunction with measurements. Verifier required.

Grover's Problem

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

1 N

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

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

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

Grover's Algorithm

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

1 N

Suppose t solutions (here t=3)

The "classical" algorithm: $A|0\rangle = |\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle$

Success probability = p = t/N

Repetition: 1/p = N/t queries

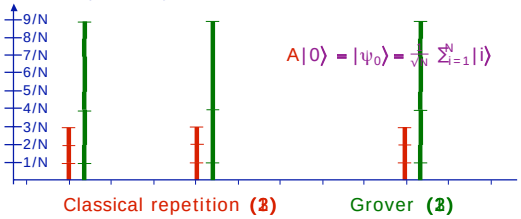
Grover: $\sqrt{1/p} = \sqrt{N/t}$ queries

Standard Analysis

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

1 N

Success probability



Grover's Algorithm

≡

Rotation

Amplification

A = some algorithm
p = success probability of A

m repetitions ⇒ success probability ≈ m·p
(provided m·p ≤ 2/3, say)

Amplitude Amplification

A = some algorithm
p = success probability of A

$\sqrt{m}$ repetitions ⇒ success probability ≈ m·p
(provided m·p ≤ 2/3, say)

(Solutions must be verifiable)

General Setting

Algorithm A, $A|0\rangle = |\psi_0\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$
Verifier f, $f: \{1,2,\ldots,N\} \to \{0,1\}$

Example: Grover

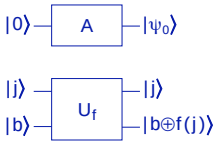
0	1	0	0	1	0	0	0	0	1	0	0

1 N

$A|0\rangle = |\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle$
$f: \{1,2,\ldots,N\} \to \{0,1\}$

General Setting

Algorithm A, $A|0\rangle = |\psi_0\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$
Verifier f, $f: \{1,2,\ldots,N\} \to \{0,1\}$



1 application of A
≡ 1 query to U_f
≡ 1 unit cost

General Setting

Algorithm A, $A|0\rangle = |\psi_0\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$
Verifier f, $f: \{1,2,\ldots,N\} \to \{0,1\}$

Let $|\text{Good}\rangle \sim \sum_{i:f(i)=1} \alpha_i |i\rangle$
$|\text{Bad}\rangle \sim \sum_{i:f(i)=0} \alpha_i |i\rangle$

$A|0\rangle = |\psi_0\rangle = \sin\theta\, |\text{Good}\rangle + \cos\theta\, |\text{Bad}\rangle$
Success prob. of A = p = $\sin^2\theta$

General Setting

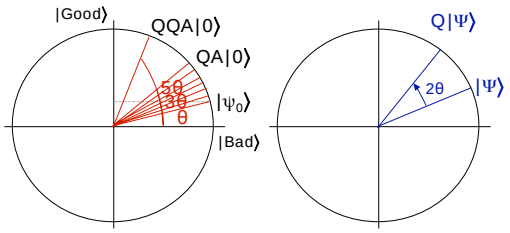
Algorithm A, $A|0\rangle = |\psi_0\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$
Verifier f, $f: \{1,2,\ldots,N\} \to \{0,1\}$

Let $|\text{Good}\rangle \sim \sum_{i:f(i)=1} \alpha_i |i\rangle$
$|\text{Bad}\rangle \sim \sum_{i:f(i)=0} \alpha_i |i\rangle$

$A|0\rangle = |\psi_0\rangle = \sin\theta\, |\text{Good}\rangle + \cos\theta\, |\text{Bad}\rangle$
Success prob. of A = p = $\sin^2\theta$

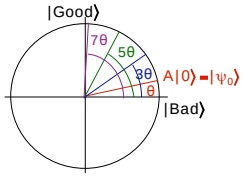
2-dimensional subspace

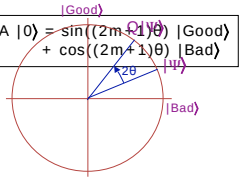
$A|0\rangle = |\psi_0\rangle = \sin\theta\,|Good\rangle + \cos\theta\,|Bad\rangle$



Operator Q rotates by angle 2θ

2-dimensional subspace





$Q^mA\,|0\rangle = \sin((2m+1)\theta)\,|Good\rangle + \cos((2m+1)\theta)\,|Bad\rangle$

$A|0\rangle = \sin\theta\,|Good\rangle + \cos\theta\,|Bad\rangle$

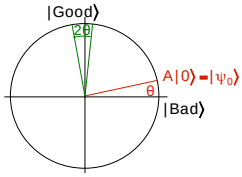
$QA|0\rangle = \sin 3\theta\,|Good\rangle + \cos 3\theta\,|Bad\rangle$

$QQA|0\rangle = \sin 5\theta\,|Good\rangle + \cos 5\theta\,|Bad\rangle$

$QQQA|0\rangle = \sin 7\theta\,|Good\rangle + \cos 7\theta\,|Bad\rangle$

Operator Q rotates by angle 2θ

Maximizing the success prob.



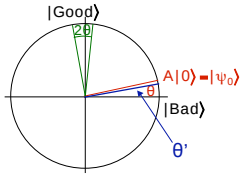
$Q^mA\,|0\rangle = \sin((2m+1)\theta)\,|Good\rangle + \cos((2m+1)\theta)\,|Bad\rangle$

Theorem:
Set $m = \frac{\pi}{4\sqrt{p}}$,
then Prob[Bad] $\le \sin^2\theta = p$

Proof: After m rotations, angle is $(2m+1)\theta$.
We want $(2m+1)\theta \approx \frac{\pi}{2}$.
Since $\sin^2\theta = p$, then $\theta \approx \sqrt{p}$. □

Note: Classically, $m = \frac{1}{p}$. A quadratic speed-up!

"De-randomization" (p known)

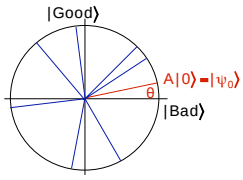


$Q^mA\,|0\rangle = \sin((2m+1)\theta)\,|Good\rangle + \cos((2m+1)\theta)\,|Bad\rangle$

Theorem:
If prob. p is known,
we can "de-randomize".

Proof: If $(2m+1)\theta$ is slightly more than $\frac{\pi}{2}$,
then choose slightly smaller angle $\theta' < \theta$
such that $(2m+1)\theta'$ IS equal to $\frac{\pi}{2}$. □

If p is not known?

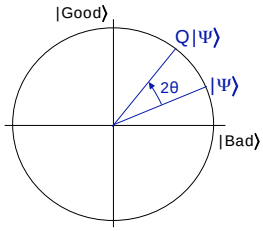


A random vector yields success prob. = 1/2

Solution: obtain a near-random vector
by classically guessing m.

Theorem: Still a quadratic speed-up!

Q ≡ Rotation



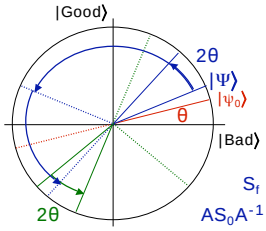
$Q = -AS_0A^{-1}S_f$

$S_0\,|0\rangle = |0\rangle$
$S_0\,|i\rangle = -|i\rangle \quad (i \neq 0)$

$S_f\,|i\rangle = |i\rangle \quad (f(i)=1)$
$S_f\,|i\rangle = -|i\rangle \quad (f(i)=0)$

Q ≡ Rotation

$Q = -AS_0A^{-1}S_f$



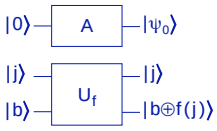
$S_0|0\rangle = |0\rangle$
$S_0|i\rangle = -|i\rangle \quad (i\neq 0)$

$S_f|i\rangle = |i\rangle \quad (f(i)=1)$
$S_f|i\rangle = -|i\rangle \quad (f(i)=0)$

S_f ≡ reflection about $|Good\rangle$
AS_0A^{-1} ≡ reflection about $|\psi_0\rangle$

∴ Q ≡ rotation by 2θ

Cost of Q



1 application of A
≡ 1 query to U_f
≡ 1 unit cost

$Q = -AS_0A^{-1}S_f$

1 application of Q ≡ 1 applications of S_f
+ 2 applications of A
+ 1 application of S_0
≡ 4 units cost

The Recipe

Algorithm A, $A|0\rangle = |\psi_0\rangle = \sum_{i=1}^{N} \alpha_i|i\rangle$
Verifier f, $f:\{1,2,\ldots,N\}\rightarrow\{0,1\}$

Define reflections:

$S_0|0\rangle = -|0\rangle$ $\quad S_f|i\rangle = -|i\rangle \quad (f(i)=1)$
$S_0|i\rangle = |i\rangle \quad (i\neq 0)$ $\quad S_f|i\rangle = |i\rangle \quad (f(i)=0)$

Amplitude Amplification operator:

$Q = -AS_0A^{-1}S_f$

Repeated apply Q on state $A|0\rangle$

Complete Grover

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

1 $\quad f:\{1,2,\ldots,N\}\rightarrow\{0,1\}$ $\quad$ N

$A|0\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N}|i\rangle$

$Q = -AS_0A^{-1}S_f$

$S_0|0\rangle = |0\rangle$
$S_0|i\rangle = -|i\rangle \quad (i\neq 0)$
$S_f|i\rangle = |i\rangle \quad (f(i)=1)$
$S_f|i\rangle = -|i\rangle \quad (f(i)=0)$

Grover's algorithm:

1) Apply A on $|0\rangle$, gives $|\psi\rangle$
2) Repeat $O(\sqrt{N})$ times:
   Apply Q on $|\psi\rangle$
3) Measure $|\psi\rangle$
4) Return outcome $|i\rangle$

Theorem: $Prob[f(i)=1] \geq 2/3$

The Recipe

Algorithm A, $A|0\rangle = |\psi_0\rangle = \sum_{i=1}^{N} \alpha_i|i\rangle$
Verifier f, $f:\{1,2,\ldots,N\}\rightarrow\{0,1\}$

Define reflections:

$S_0|0\rangle = -|0\rangle$ $\quad S_f|i\rangle = -|i\rangle \quad (f(i)=1)$
$S_0|i\rangle = |i\rangle \quad (i\neq 0)$ $\quad S_f|i\rangle = |i\rangle \quad (f(i)=0)$

Amplitude Amplification operator:

$Q = -AS_0A^{-1}S_f$

Repeated apply Q on state $A|0\rangle$

Appendix A

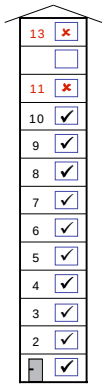
The next slides discuss how to guess m randomly if p is unknown.

Our goal is to have m of order square-root of (1/p).

Bizarre example

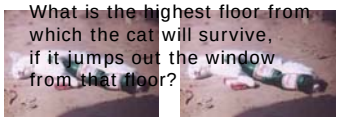
Viewer discretion is advised...

Kiil, the cat

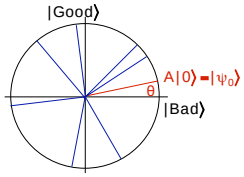


1 cat ≡ 11 trials
2 cats ≡ 7 trials

What is the highest floor from which the cat will survive, if it jumps out the window from that floor?



Guessing when p unknown



Algorithm:

1) Set M=1, λ=1.99
2) Repeat forever:
   - Set M=λM
   - Let m∈R[1,M]
   - Do $Q^m A|0\rangle$
   - Measure, say $|i\rangle$
   - If f(i)=1, then break
3) Output i

Appendix B

The next slides discuss generalizations of the amplitude amplification methods we have seen in this talk.

General rotation

$Q = -AS_0A^{-1}S_f$

$\Phi_s, \Phi_f \in C^*$

$S_0|0\rangle = \Phi_s|0\rangle$
$S_0|i\rangle = |i\rangle \quad (i\neq 0)$
$S_f|i\rangle = \Phi_f|i\rangle \quad (f(i)=1)$
$S_f|i\rangle = |i\rangle \quad (f(i)=0)$

Suitable choices of phases:

- $\Phi_s = \Phi_f = -1$
- $\Phi_s = \Phi_f = i = \sqrt{-1}$
- $\Phi_s = \Phi_f = e^{\pi i/3}$
- $\Phi_s = \Phi_f$ such that $\mathrm{Re}(\Phi_s)>0$

General Analysis

$$A|0\rangle = \sin\theta\,|Good\rangle + \cos\theta\,|Bad\rangle$$
$$Q(\Phi_s,\Phi_f)A|0\rangle = \alpha\sin\theta\,|Good\rangle + \beta\cos\theta\,|Bad\rangle$$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}-\Phi_s\Phi_f & 1-\Phi_s-\Phi_f\\ -1+\Phi_f-\Phi_s\Phi_f & -\Phi_s\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

General Analysis

$$A|0\rangle = \sin\theta\,|Good\rangle + \cos\theta\,|Bad\rangle$$
$$Q(\Phi_s,\Phi_f)A|0\rangle = \alpha\sin\theta\,|Good\rangle + \beta\cos\theta\,|Bad\rangle$$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}-\Phi_s\Phi_f & 1-\Phi_s-\Phi_f\\ -1+\Phi_f-\Phi_s\Phi_f & -\Phi_s\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

$\Phi_s = \Phi_f = -1$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}-1 & 3\\ -3 & 1\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

General Analysis

$$A|0\rangle = \sin\theta\,|Good\rangle + \cos\theta\,|Bad\rangle$$
$$Q(\Phi_s,\Phi_f)A|0\rangle = \alpha\sin\theta\,|Good\rangle + \beta\cos\theta\,|Bad\rangle$$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}-\Phi_s\Phi_f & 1-\Phi_s-\Phi_f\\ -1+\Phi_f-\Phi_s\Phi_f & -\Phi_s\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

$\Phi_s = \Phi_f = i$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}1 & 1-2i\\ i & -i\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

General Analysis

$$A|0\rangle = \sin\theta\,|Good\rangle + \cos\theta\,|Bad\rangle$$
$$Q(\Phi_s,\Phi_f)A|0\rangle = \alpha\sin\theta\,|Good\rangle + \beta\cos\theta\,|Bad\rangle$$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}-\Phi_s\Phi_f & 1-\Phi_s-\Phi_f\\ -1+\Phi_f-\Phi_s\Phi_f & -\Phi_s\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

$\Phi_s = \Phi_f = e^{\pi i/3}$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}-e^{2\pi i/3} & 1-2e^{\pi i/3}\\ 0 & -e^{\pi i/3}\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

General Analysis

$$A|0\rangle = \sin\theta\,|Good\rangle + \cos\theta\,|Bad\rangle$$
$$Q(\Phi_s,\Phi_f)A|0\rangle = \alpha\sin\theta\,|Good\rangle + \beta\cos\theta\,|Bad\rangle$$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}-\Phi_s\Phi_f & 1-\Phi_s-\Phi_f\\ -1+\Phi_f-\Phi_s\Phi_f & -\Phi_s\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$

$\Phi_s = \Phi_f$ such that $Re(\Phi_s) > 0$

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}? & ?\\ <1 & ?\end{bmatrix}\begin{bmatrix}\sin^2\theta\\ \cos^2\theta\end{bmatrix}$$