Amplitude Amplification and Appplications

Peter Høyer

www.cpsc.ucalgary.ca/~hoyer

June 26, 2003, University of Calgary
PIMS-MITACS Summer School on Quantum Information Science

Breathtaking bargain

Work as little as $O(\sqrt{m})^{\star}$

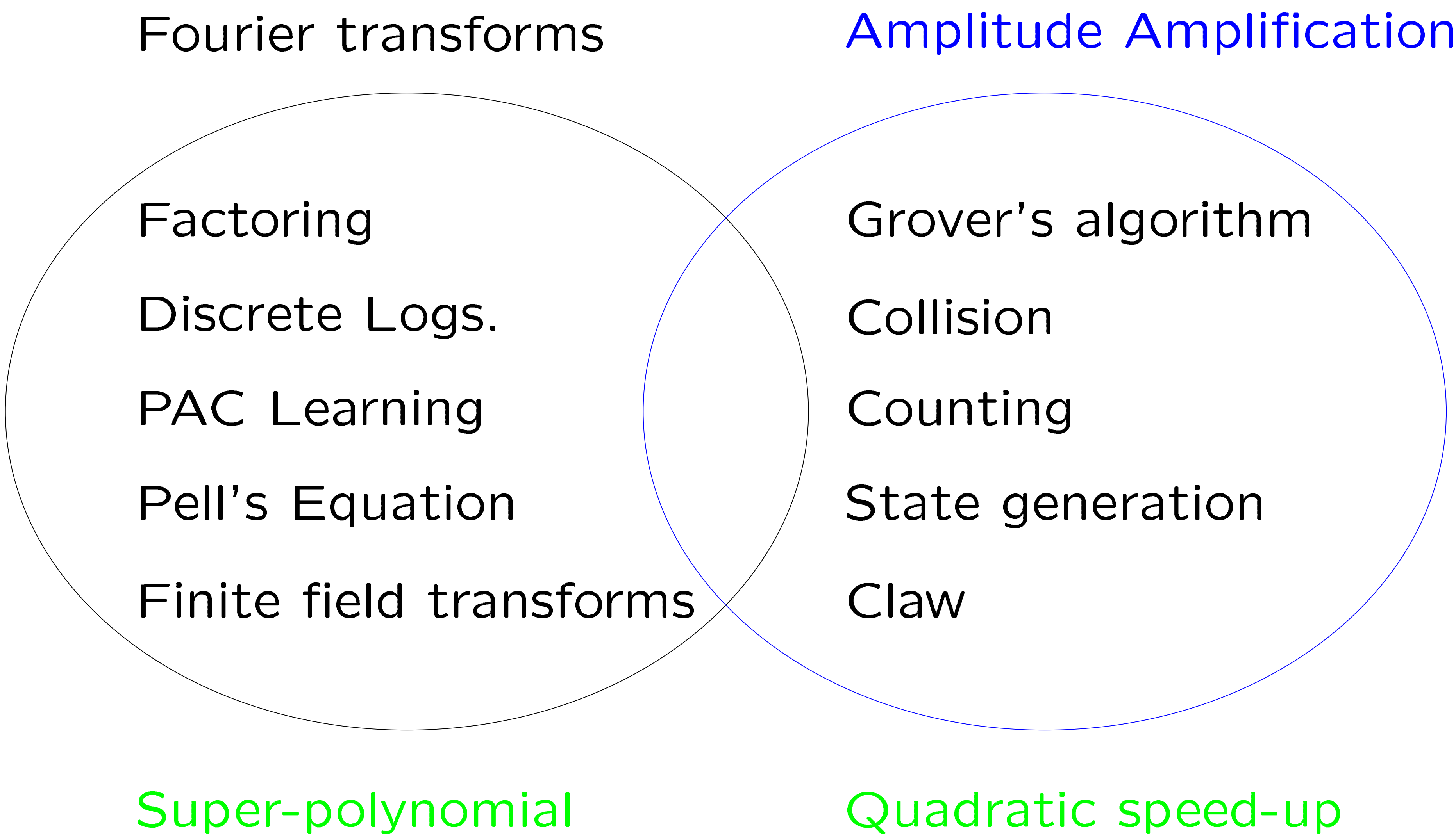
Compare at $O(m)$

Call 1-800-ampl ampl now,

or visit us online at www.amplampl.com.

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

Classification of quantum algorithms



Amplification

A $=$ some algorithm

$p =$ success probability of A

m repetitions $\Rightarrow$ succ. prob. $\approx m \cdot p$

(provided $m \cdot p \leq 2/3$, say)

Amplitude

$\sqrt{}$

Solutions must be verifiable!

Grover (1996)
Brassard, Høyer (1997)
Brassard, Høyer, Mosca, Tapp (1998)
Buhrman, Cleve, de Wolf, Zalka (1999)

Example 1: Grover searching

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

1 $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ N

Suppose t solutions

Success prob. $= p = \frac{t}{N}$

Classically: $\frac{1}{p} = \frac{N}{t}$ queries

Quantumly: $\sqrt{\frac{1}{p}} = \sqrt{\frac{N}{t}}$ queries

General Setting

Quantum alg. A, $\quad \mathsf{A}\,|0\rangle = |\psi_0\rangle = \sum_i \alpha_i\,|i\rangle$

Verifier χ, $\quad \chi : \mathbb{Z} \rightarrow \{\mathsf{Good}, \mathsf{Bad}\}$

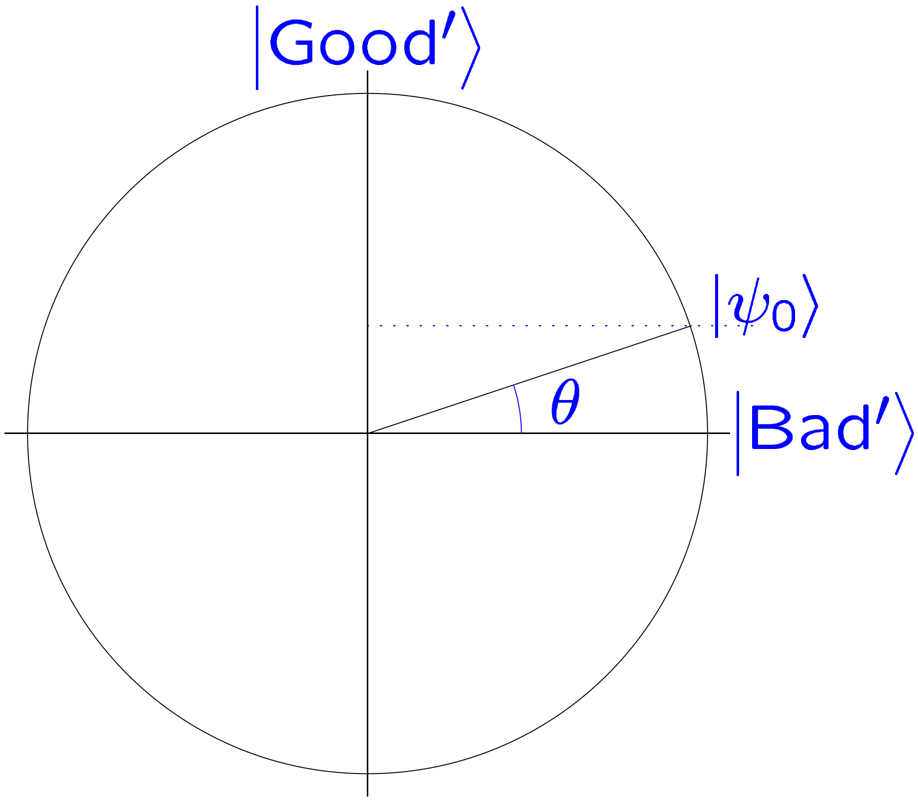
$$\text{Let } |\text{Good}\rangle = \sum_{i:\chi(i)=\text{Good}} \alpha_i |i\rangle$$

$$|\text{Bad}\rangle = \sum_{i:\chi(i)=\text{Bad}} \alpha_i |i\rangle$$

$$\mathsf{A}\,|0\rangle = |\psi_0\rangle = |\mathsf{Good}\rangle + |\mathsf{Bad}\rangle$$

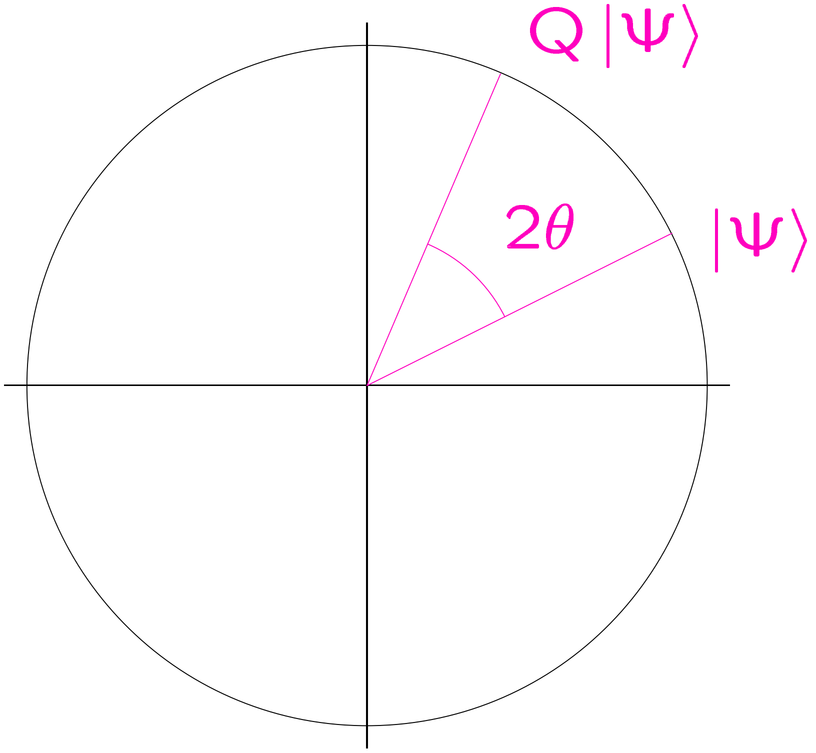
$$\text{Success prob. of A} = p = \langle \mathsf{Good}|\mathsf{Good}\rangle$$

2-dimensional subspace



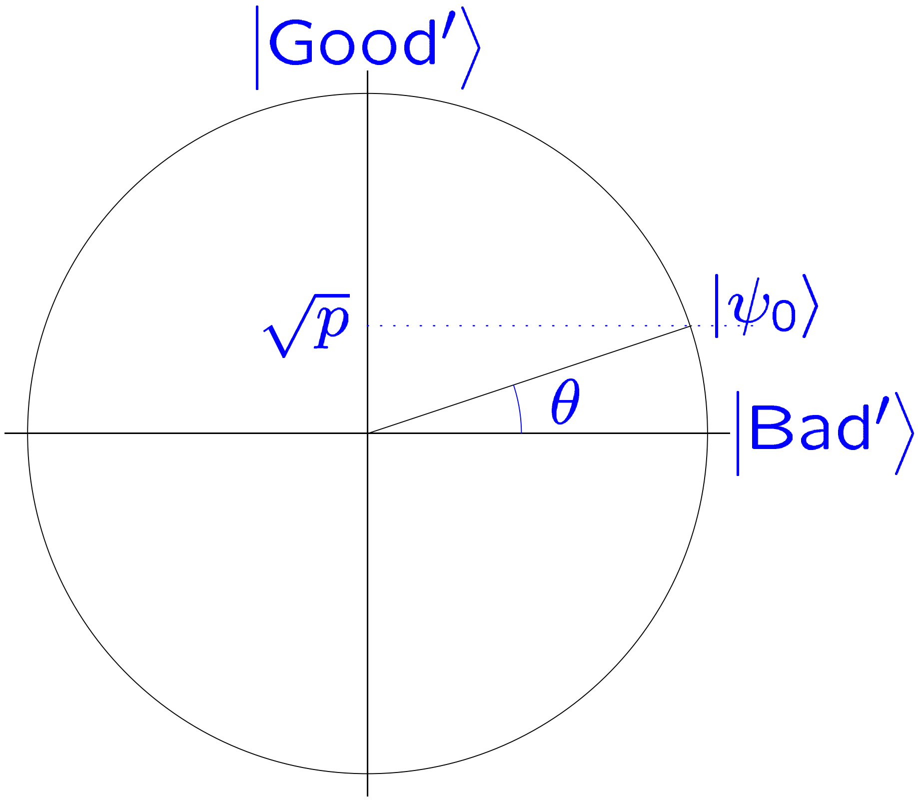
$$\sin^2(\theta) = p$$

Rotation on



Operator Q rotates by angle 2θ

Amplitude Amplification



$$A\,|0\rangle = |\psi_0\rangle$$
$$= |\text{Good}\rangle + |\text{Bad}\rangle$$

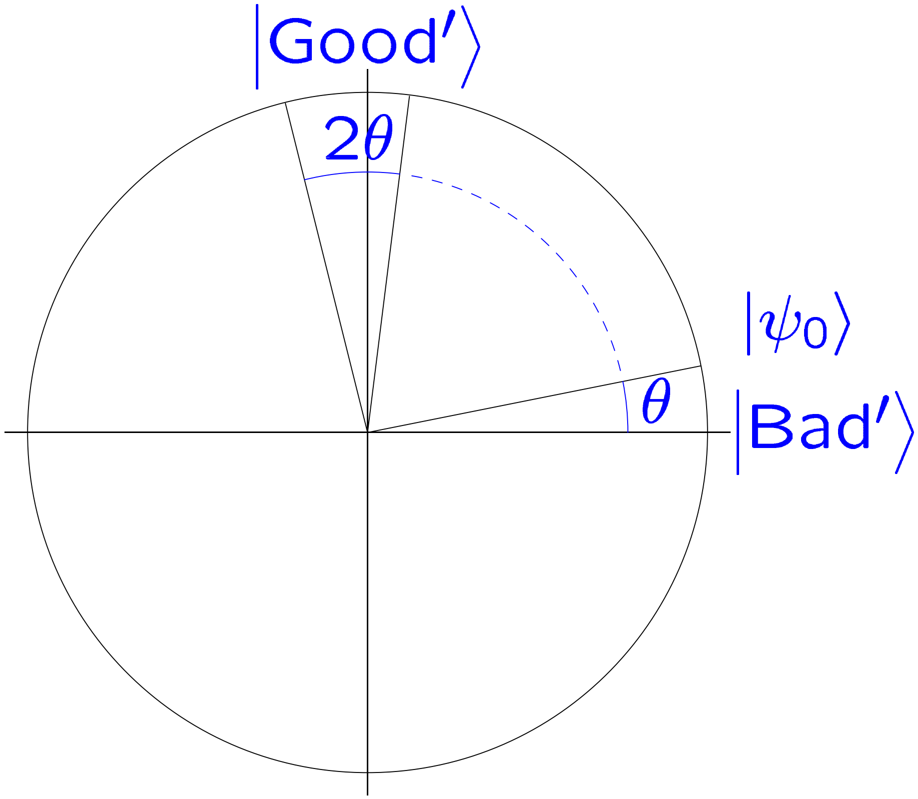
$$\text{Succ. prob} = p$$
$$= \langle \text{Good}|\text{Good}\rangle$$

p unknown:

solution in
expected time $\sqrt{\frac{1}{p}}$

p known:

solution with
certainty in $\sqrt{\frac{1}{p}}$



After m rotations :

state $\mathsf{Q}^m |\psi_0\rangle$

angle $\angle = (2m+1)\theta$

$\sin^2(\theta) = p$

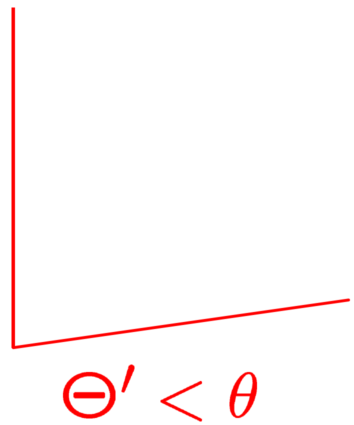
$\theta \approx \sqrt{\frac{1}{p}}$

Maximizing the success prob. (p known)

$(2m+1)\theta \approx \pi/2$, thus $m \approx \frac{\pi}{4}\frac{1}{\theta} \approx \frac{\pi}{4}\sqrt{\frac{1}{p}}$

Then $\text{Prob}[\text{Bad}] \leq \sin^2(\theta) = p$

De-randomization (p known)



If $(2m+1)\theta$ is slightly more than $\pi/2$,
then choose slightly smaller angle Θ' such that
$(2m+1)\Theta'$ IS equal to $\pi/2$

Example 2: 100% success prob

Have:

$$A \; : \; |000\rangle \longmapsto \frac{1}{\sqrt{3}}\big(\,|000\rangle + |010\rangle + |111\rangle\,\big)$$

Want:

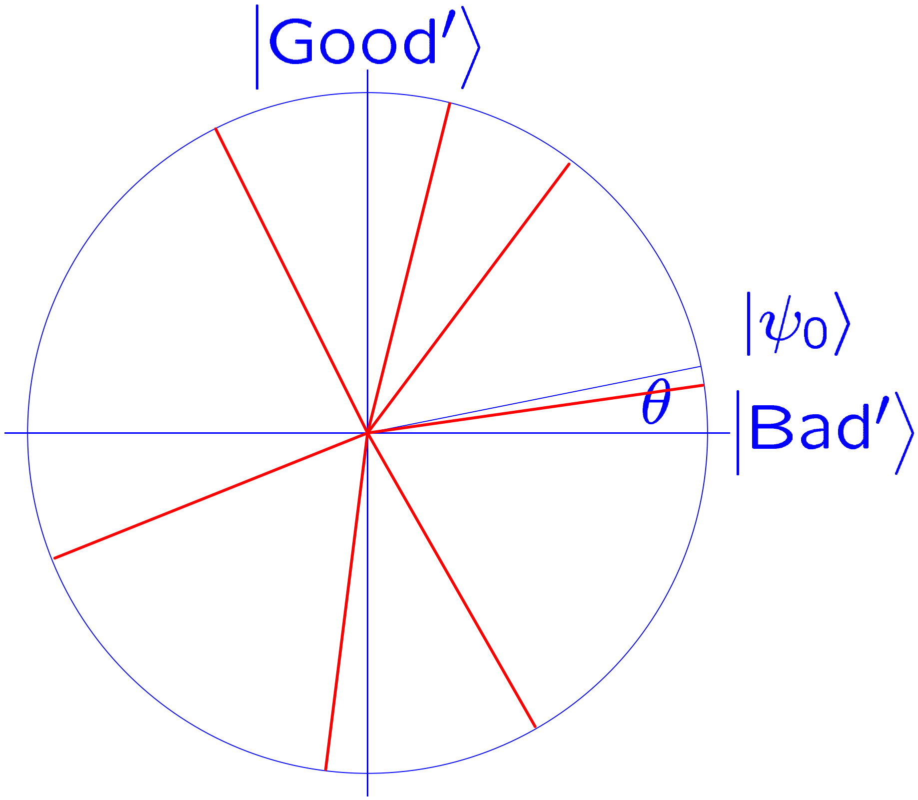
$$D \; : \; |000\rangle \longmapsto \frac{1}{\sqrt{2}}\big(\,|000\rangle + |111\rangle\,\big)$$

Example 3: State generation

1) $$\frac{1}{\sqrt{K}}\sum_{i=0}^{K-1}|i\rangle$$ $K > 0$ any integer

2) $$\sum_{\substack{i=0\\ \gcd(i,K)=1}}^{K-1}|i\rangle$$

Guessing when succ. prob p is UNKNOWN



After m rotations :

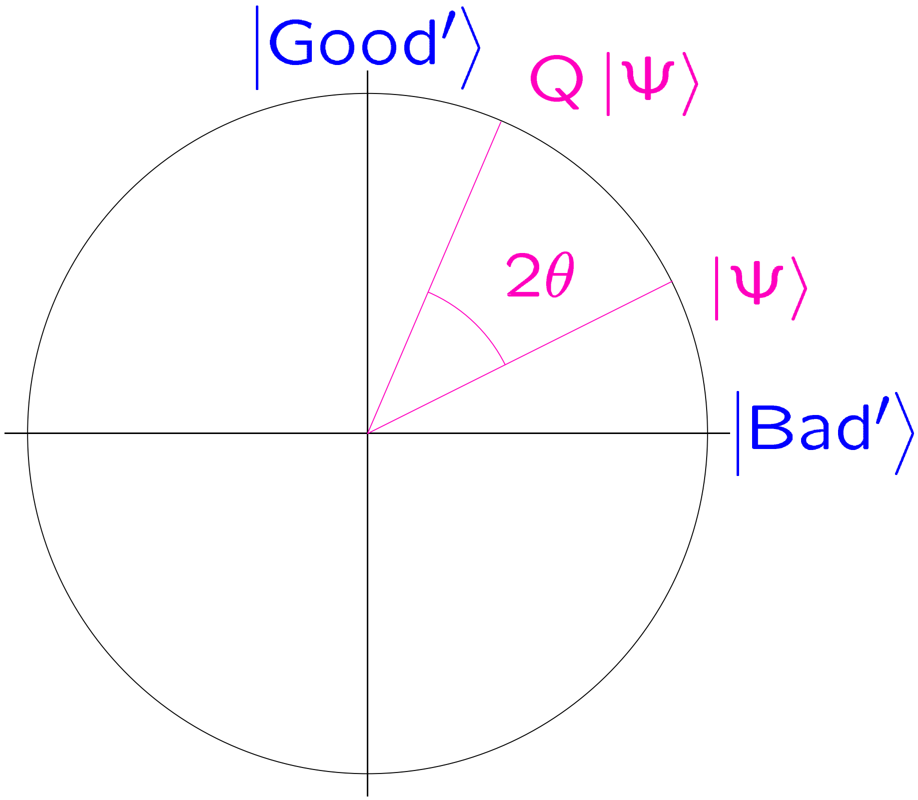
state $\mathrm{Q}^m |\psi_0\rangle$

angle $\angle = (2m+1)\theta$

A random vector yields succ. prob $= \frac{1}{2}$

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

Rotation on 2-dimensional subspace



$$\boxed{Q = -AS_0A^{-1}S_\chi}$$

$$\begin{aligned} S_0\,|0\rangle &= -\,|0\rangle \\ S_0\,|i\rangle &= \;\;\,|i\rangle \quad (i \neq 0) \end{aligned}$$

$$\begin{aligned} S_\chi\,|i\rangle &= -\,|i\rangle \quad (\chi(i) = 1) \\ S_\chi\,|i\rangle &= \;\;\,|i\rangle \quad (\chi(i) = 0) \end{aligned}$$

$$\begin{aligned} S_\chi &\equiv \text{reflection around } |\text{Good}'\rangle \\ -AS_0A^{-1} &\equiv \text{reflection around } |\psi_0\rangle \end{aligned}$$

$$\therefore \; Q \equiv \text{rotates by angle } 2\theta$$

Example 4: quantum algorithm for Claw

f	6	15	42	1	17	21	3	21	27	7	57	18
g	10	2	37	33	14	53	21	5	19	42	33	2
	1											N

Claw = A pair of indices (i, j) such that

$$f(i) = g(j).$$

Classically: $N \log N$

Quantumly: $N^{3/4} \log N$

Steps 1–4,   Claw algorithm

f	6		42				3				57	
g	10	2	37	33	14	53	21	5	19	42	33	2

1. Pick $B \subseteq_R \{1, 2, \ldots, N\}$ of size $\sqrt{N}$

2–4. Find claw in $f(B) \times g(\{1, 2, \ldots, N\})$ using $O(\sqrt{N} \log N)$ comparisons

$$\text{Success prob.} \geq p = \frac{|B|}{N} = \frac{1}{\sqrt{N}}$$

Amplitude amplification: $\frac{1}{\sqrt{p}}$ iterations

$$O(\sqrt{N} \log N \times N^{1/4}) = O(N^{3/4} \log N)$$

Step 1, Claw algorithm

f	6		42				3				57	
g	10	2	37	33	14	53	21	5	19	42	33	2

1. Pick $B \subseteq_R \{1, 2, \ldots, N\}$ of size $\sqrt{N}$

Step 2, Claw algorithm

f	3	6	42	57								
g	10	2	37	33	14	53	21	5	19	42	33	2

1. Pick $B \subseteq_R \{1, 2, \ldots, N\}$ of size $\sqrt{N}$
2. Sort B wrt. f-values

$|B| \log |B|$

Step 3, Claw algorithm

f	3	6	42	57								
g	10	2	37	33	14	53	21	5	19	42	33	2
h	0	0	0	0	0	0	0	0	0	1	0	0

1. Pick $B \subseteq_R \{1, 2, \ldots, N\}$ of size $\sqrt{N}$
2. Sort B wrt. f-values
3. Define $h : \{1, 2, \ldots, N\} \to \{0, 1\}$

   by $h(i) = 1$ *iff* $g(i) \in f(B)$

   (Evaluating $h(i)$ takes $\log |B|$ compar.)

$|B| \log |B|$

Step 4, Claw algorithm

f	3	6	42	57								
g	10	2	37	33	14	53	21	5	19	42	33	2
h	0	0	0	0	0	0	0	0	0	1	0	0

1. Pick $B \subseteq_R \{1, 2, \ldots, N\}$ of size $\sqrt{N}$
2. Sort B wrt. f-values
3. Define $h : \{1, 2, \ldots, N\} \to \{0, 1\}$

   by $h(i) = 1$ *iff* $g(i) \in f(B)$
4. Compute Grover(h)

$$|B| \log |B| + \sqrt{N} \log |B| \;\in\; O(\sqrt{N} \log N)$$

Algorithms using amplitude amplification

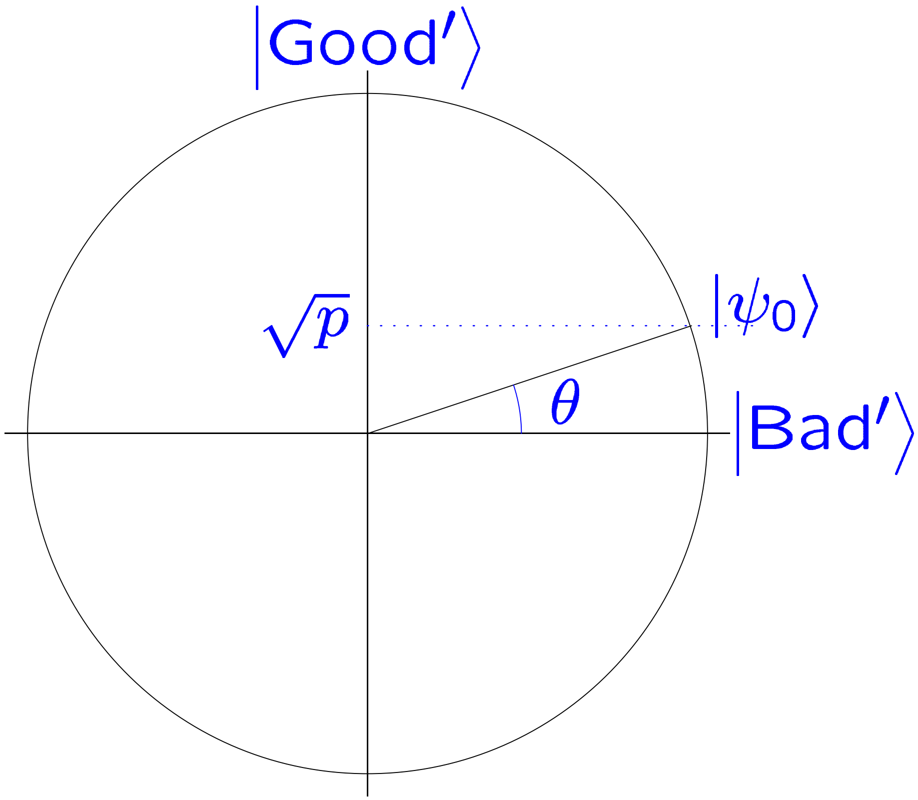
Computational Geometry
Communication Complexitity

Grover's algorithm
OR
Threshold$_S$
Elem. Distinctness
Claw

Median
Majority
Counting
Integration
Pattern Matching

Derandomization
...

Amplitude Amplification



$$\mathsf{A}\,|0\rangle = |\psi_0\rangle$$
$$= |\mathsf{Good}\rangle + |\mathsf{Bad}\rangle$$

$$\mathsf{Q} = -\mathsf{A}\mathsf{S}_0\mathsf{A}^{-1}\mathsf{S}_\chi$$

$$\text{Succ. prob} = p$$

p unknown:

solution in expected time $\sqrt{\frac{1}{p}}$

p known:

solution with certainty in $\sqrt{\frac{1}{p}}$