

This Week

Lecture 9

Introduction to Grover's algorithm for amplitude amplification,
geometric interpretation

Lecture 10

Amplitude Amplification, Succeeding with Certainty, Quantum
Counting

Lab

Grover's algorithm

Amplitude Amplification

MULT90063 Introduction to Quantum Computing
Lecture 10

Amplitude Amplification

- This lecture: Amplitude amplification
 - Amplitude Amplification
 - Succeeding with certainty
 - Quantum Counting

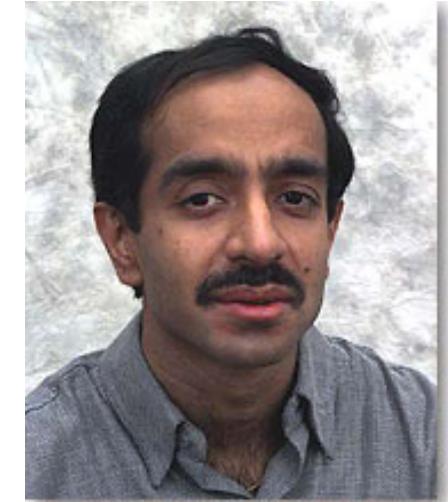
References:

- Rieffel, Chapter 9.1-9.2
- Kaye, Chapter 8.1-8.2
- Nielsen and Chuang, Chapter 6.1-6.2

Grover's Algorithm (1996)

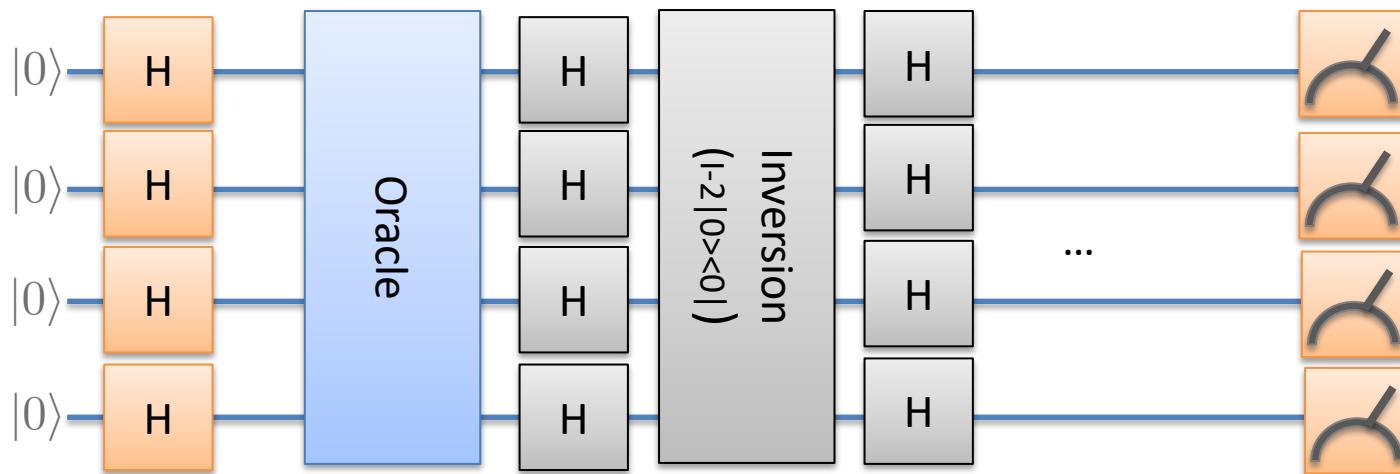
- Unordered search, find one marked item among many
- Classically, this requires $N/2$ queries to the oracle
- Quantum mechanically, requires only $O(\sqrt{N})$ queries.

Simple problem = search for one integer marked by the oracle.

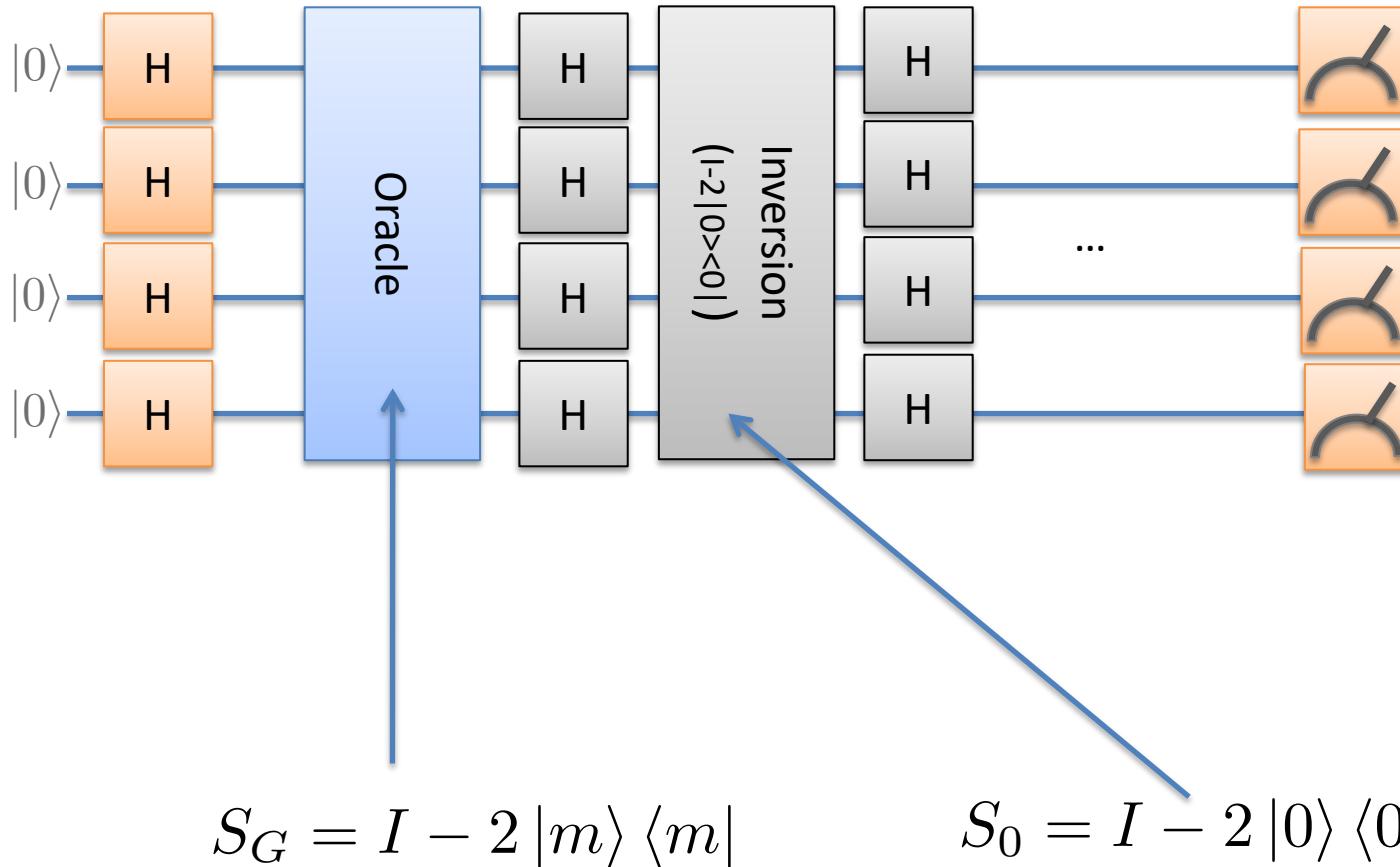


Lov Grover

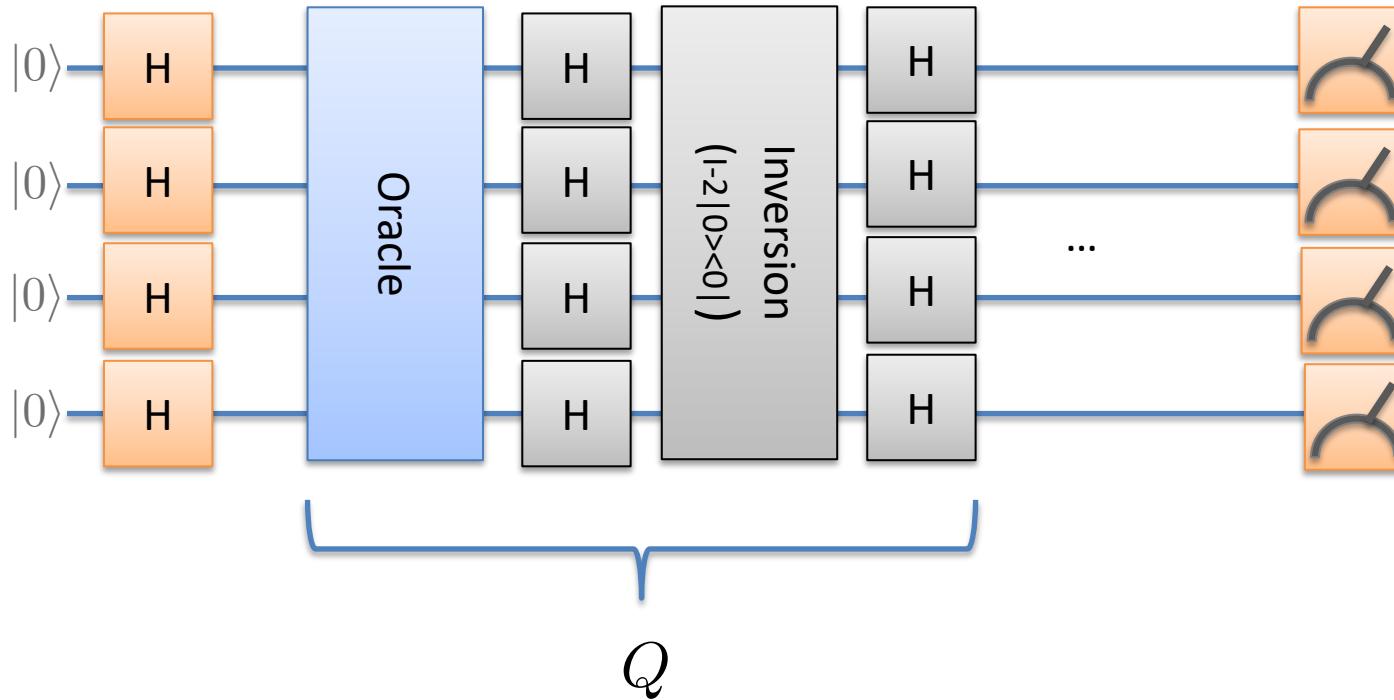
High level structure:



Some notation



Some notation



n is the number of input qubits.
 N is the total dimension ($N=2^n$).
 M is the number of solutions.

Oracles for NP-problems

The phone book isn't a great example: Adding in all the names would take $O(N)$ time.

In general though, many problems (specifically those in the class NP) can have easily **checkable** solutions even if it is hard to solve the problem originally. Examples:

- Factoring
- Travelling Salesman with route less than distance d
- Hamiltonian cycle

Straightforward application of Grover's algorithm provides a **polynomial** improvement over random guessing... and potentially a better (but still polynomial speedup) known as **amplitude amplification**.

N	Moose	50427	R	Toyboy	22381
	Mobile.....	23179		Trigger	50560
Morg	Mobile.....	50499		Mobile.....	23738
		22641		Trix	50297
Muff	Mobile.....	50899		Truck.....	23053
		22412		Mobile.....	22678
Mutty					50240
O			S		
			Sarlu	23849	
Nippa		23131	Scotty	22634	
Noon		22246	Scully	23493	
P			Mobile.....	50009	
Onion		23611	Short (Graham)	22236	
Oodie		22289	Short (Nobbs)	22628	
Y			Shorty	22495	
			Mobile.....	50340	
Pash.....		22485	Skeeters	22341	
	Mobile.....	50485	Slack	22559	
Pedro		22455	Slick	22473	
Pelly		22288	Sluggy	50868	
Perko		22536	Smitty	23675	
Philly Foxtel..		22470	Smudgie	22568	
Pinky		22493	Mobile.....	50568	
Pip (Reeves) ..		22649	Snapper	22077	
Pixie		23022	Mobile.....	50963	
	Mobile.....	50666	Snobbles	23026	
Plumber.....		22501	Mobile.....	50350	
Plute		22275	Snoop	22326	
Pooh		50198	Mobile.....	51126	
Pops		23017	Snowy	22558	
Poppa		24228			

© Administration of Norfolk Island

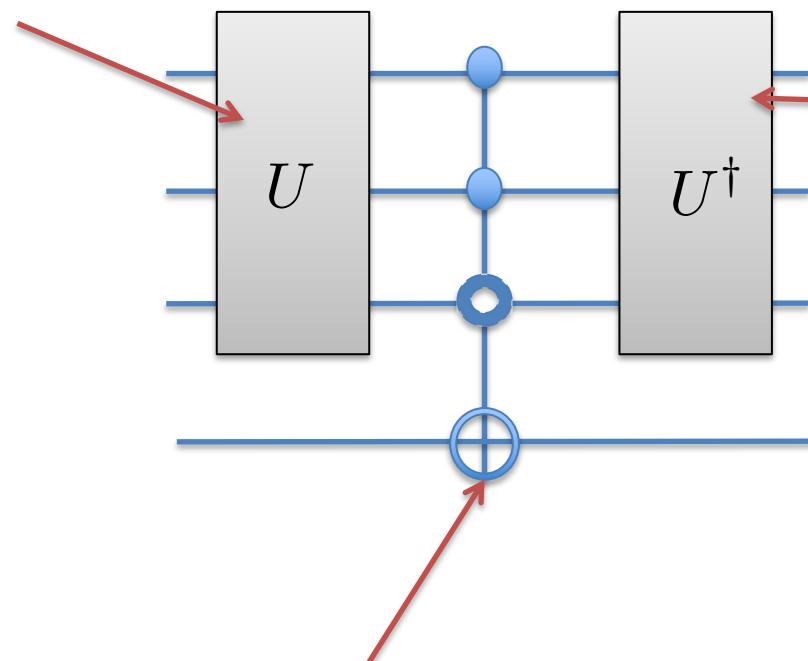
2010-11

Telephone Directory 90

Part of Norfolk Island's telephone book, with people listed by nickname (Photo: Wikicommons)

Oracle for a hash function

A hash function whose output is hard to predict based on the input.

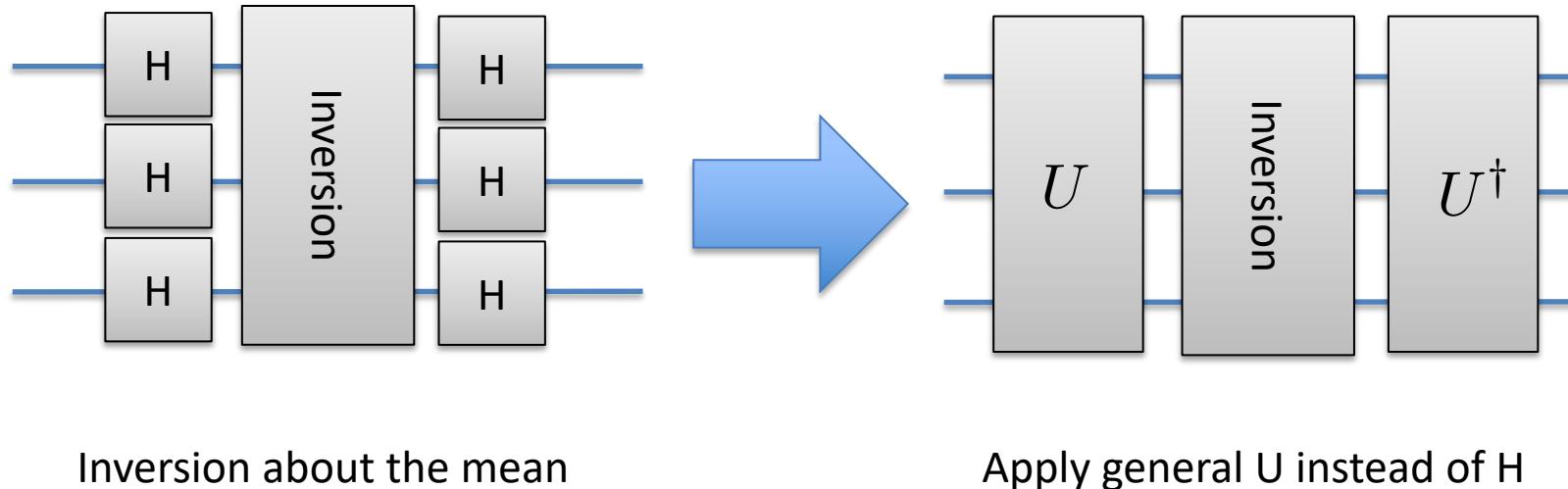


“Uncompute” the hash function – ensures the input register remains unchanged.

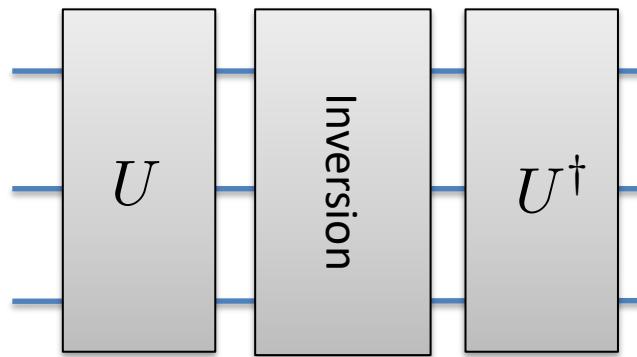
The oracle recognises the ‘correct’ solution, but does not know in advance which input leads to the correct solution

Amplitude amplification

What happens if we replace the Hadamard gates with some other U ?
Perhaps, for example, we can create a U which gives the correct outcome with probability greater than $1/N$. Can we get any advantage?



New inversion step



Apply general U instead of H

$$|\phi\rangle = U|0\rangle$$

Then we can break this up as:

$$|\phi\rangle = g_0 |\phi_g\rangle + b_0 |\phi_b\rangle$$

Good: In the
subspace spanned
by all solutions

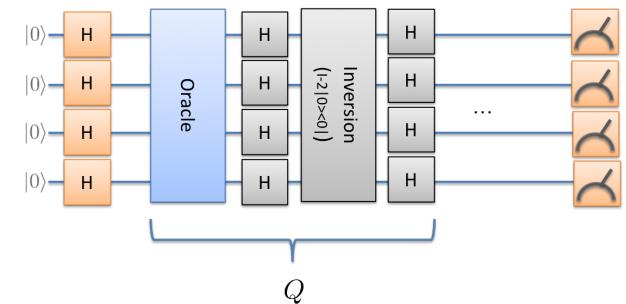
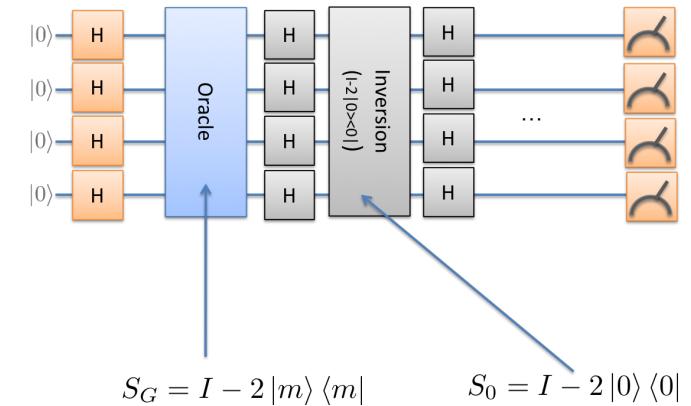
Bad: Not in the subspace
spanned by all solutions

Maths of the Geometric Interpretation

$$\begin{aligned}
 US_0U^\dagger |\psi\rangle &= U(I - 2|0\rangle\langle 0|)U^\dagger |\psi\rangle \\
 &= |\psi\rangle - 2\langle 0|U^\dagger|\psi\rangle U|0\rangle \\
 &= |\psi\rangle - 2\langle\psi|U|0\rangle^*U|0\rangle
 \end{aligned}$$

where $|\phi\rangle = U|0\rangle$
 $|\phi\rangle = g_0|\phi_g\rangle + b_0|\phi_b\rangle$

$$\begin{aligned}
 Q|\phi\rangle_g &= -US_0U^\dagger S_G|\phi_g\rangle \\
 &= US_0U^\dagger|\phi_g\rangle \\
 &= |\phi_g\rangle - 2g_0^*U|0\rangle \\
 &= |\phi_g\rangle - 2g_0^*g_0|\phi_g\rangle - 2g_0^*b_0|\phi_b\rangle \\
 &= (1 - 2t)|\phi_g\rangle - 2\sqrt{t(1-t)}|\phi_b\rangle
 \end{aligned}$$



$t = |g_0|^2$

Maths of Amplitude Amplification

Similarly,

$$Q |\phi_b\rangle = (1 - 2t) |\phi_b\rangle + 2\sqrt{t(1-t)} |\phi_g\rangle$$

And from previous slide: $Q |\phi_g\rangle = (1 - 2t) |\phi_g\rangle - 2\sqrt{t(1-t)} |\phi_b\rangle$

Q recursive step:

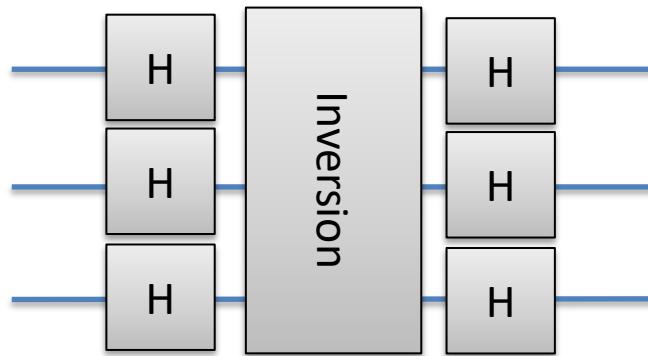
$$Q = \begin{bmatrix} (1 - 2t) & -2\sqrt{t(1-t)} \\ 2\sqrt{t(1-t)} & (1 - 2t) \end{bmatrix}$$

Compare to a rotation matrix:

$$R(2\theta) = \begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}$$

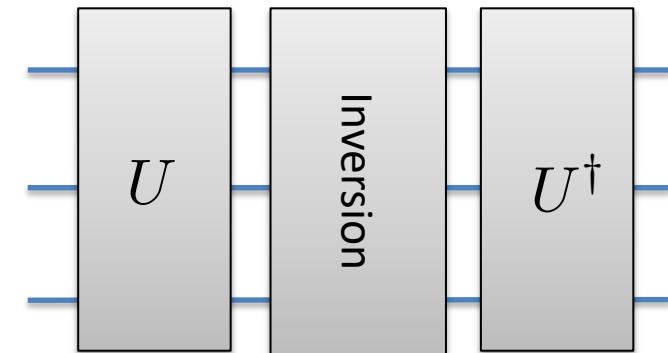
$\sin \theta = \sqrt{t} = g_0$

Grover vs Amplitude Amplification

Grover

Angle of rotation:

$$\sin \theta = \frac{\sqrt{M}}{\sqrt{N}}$$

Amplitude Amplification

Angle of rotation:

$$\sin \theta = \sqrt{t} = g_0$$

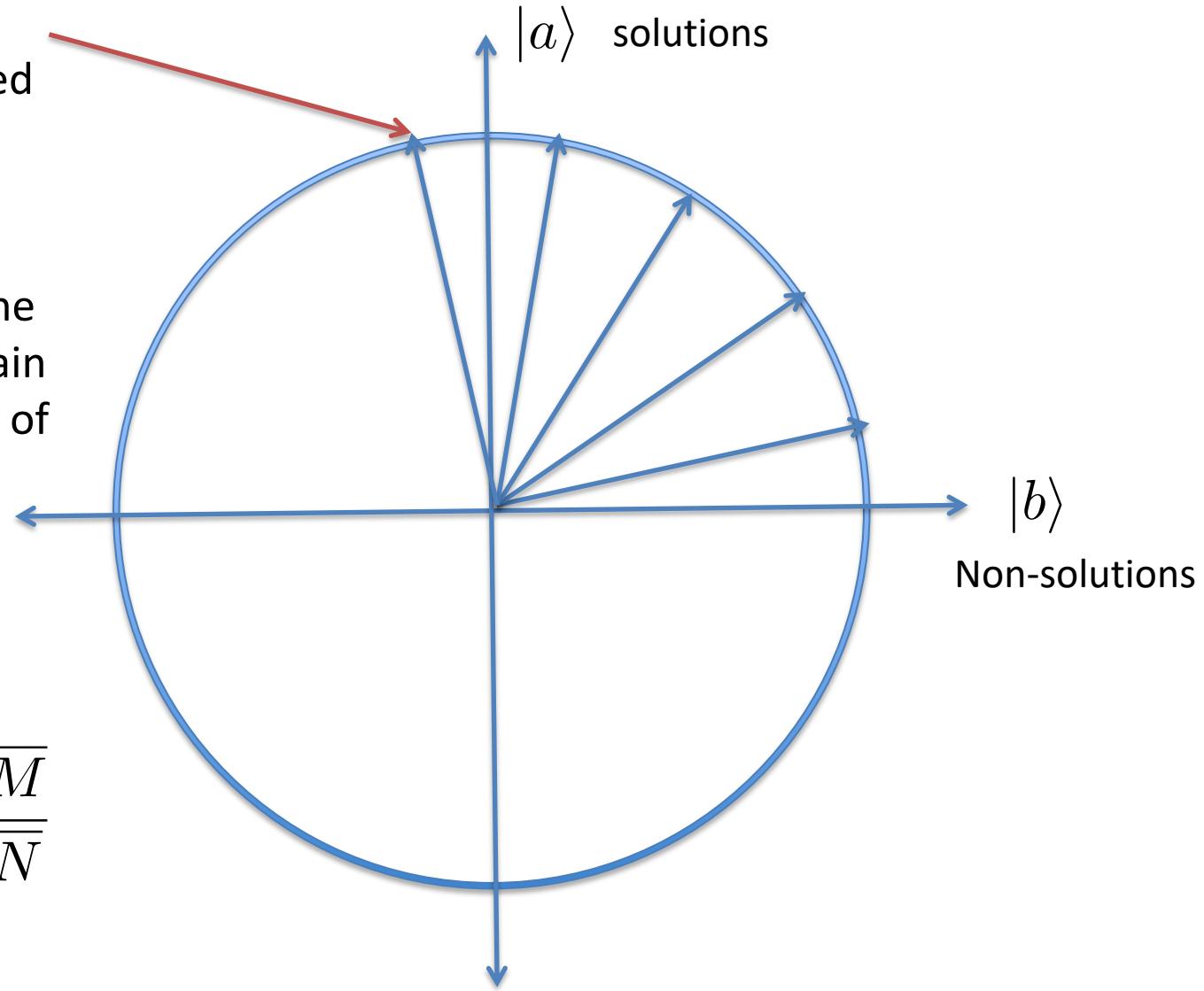
If you can construct a U with a higher probability of success than random guessing $1/N$, then amplitude amplification can help.

How to achieve 100% Success

The optimal, 100% probability of measuring marked can be missed.

Can we modify the algorithm to obtain 100% probability of success?

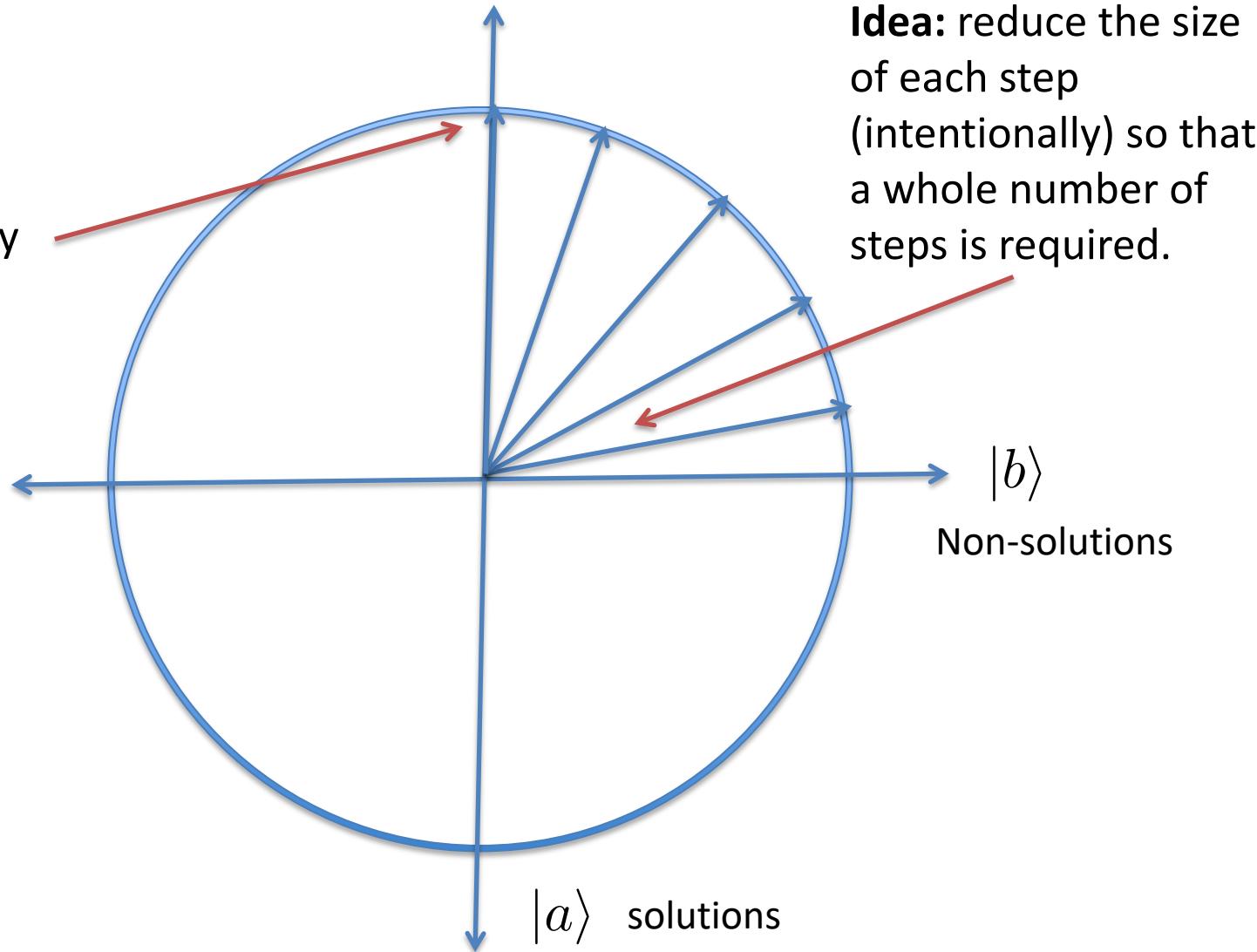
$$\sin \theta = \frac{\sqrt{M}}{\sqrt{N}}$$



Grover with 100% success

Using amplitude amplification

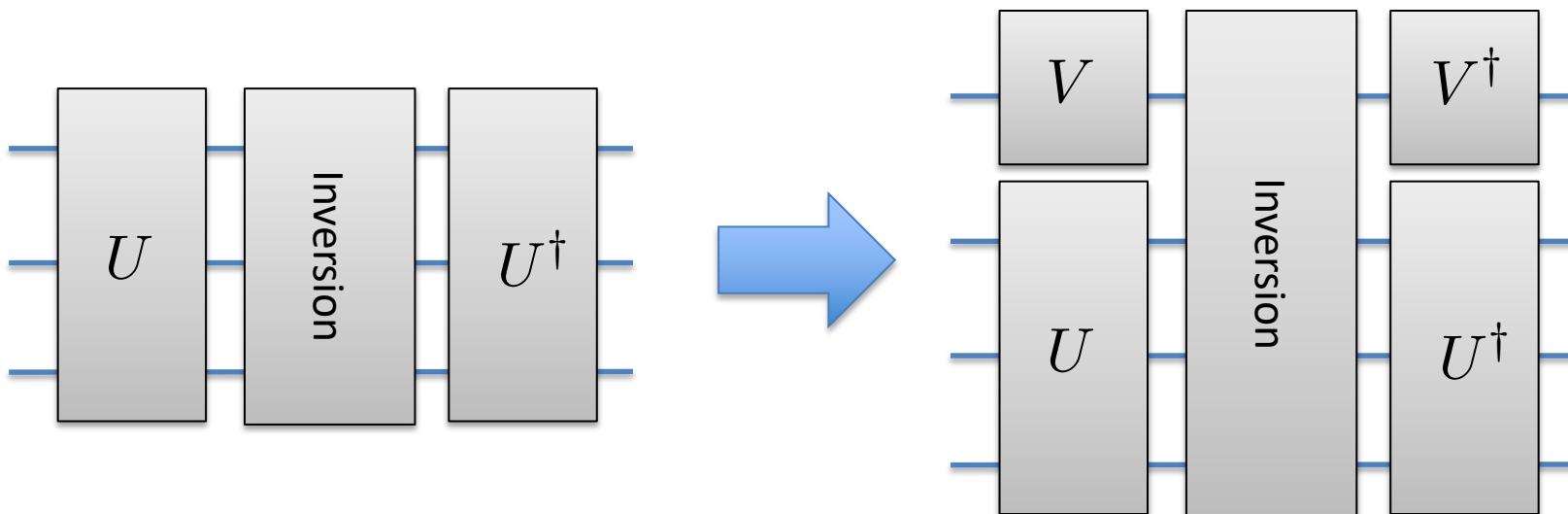
This step gives 100% probability of finding the marked state



Reducing the angle

We want to reduce the angle of rotation in Grover's algorithm/amplitude amplification so that we require a whole number of steps to achieve 100% probability of success.

Trick: Introduce a new qubit.



How much reduction?

Previously:

$$U |0\rangle = g_0 |\phi_g\rangle + b_0 |\phi_b\rangle$$

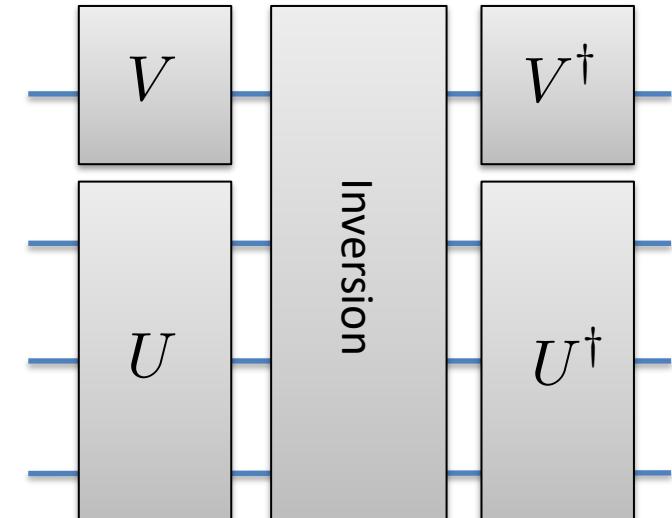
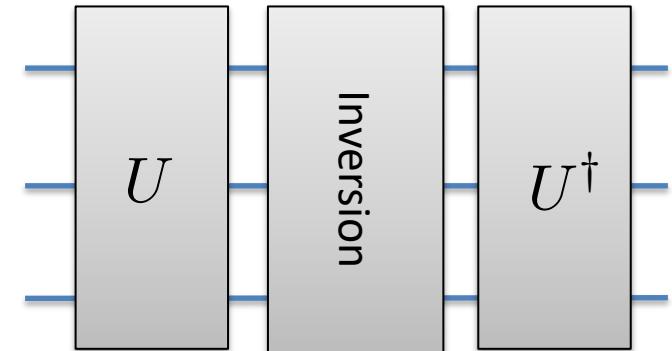
With new qubit:

$$V \otimes U |0\rangle = V |0\rangle \otimes (g_0 |\phi_g\rangle + b_0 |\phi_b\rangle)$$

If we arrange so that:

$$V |0\rangle = \sqrt{1 - \left(\frac{g'_0}{g_0}\right)^2} |0\rangle + \frac{g'_0}{g_0} |1\rangle$$

e.g. Y-rotation by an angle: $\cos \frac{\alpha}{2} = \frac{g'_0}{g}$



New rotation angle

$$V \otimes U |0\rangle = V |0\rangle \otimes (g_0 |\phi_g\rangle + b_0 |\phi_b\rangle)$$

$$V |0\rangle = \sqrt{1 - \left(\frac{g'_0}{g_0}\right)^2} |0\rangle + \frac{g'_0}{g_0} |1\rangle$$

Gives:

$$V \otimes U |0\rangle = g'_0 |1\rangle |\phi_g\rangle + \dots$$

We can choose the initial amplitude to be anything value less than the original

Our new “good” states, but now have a preceding “1” on the extra qubit we added

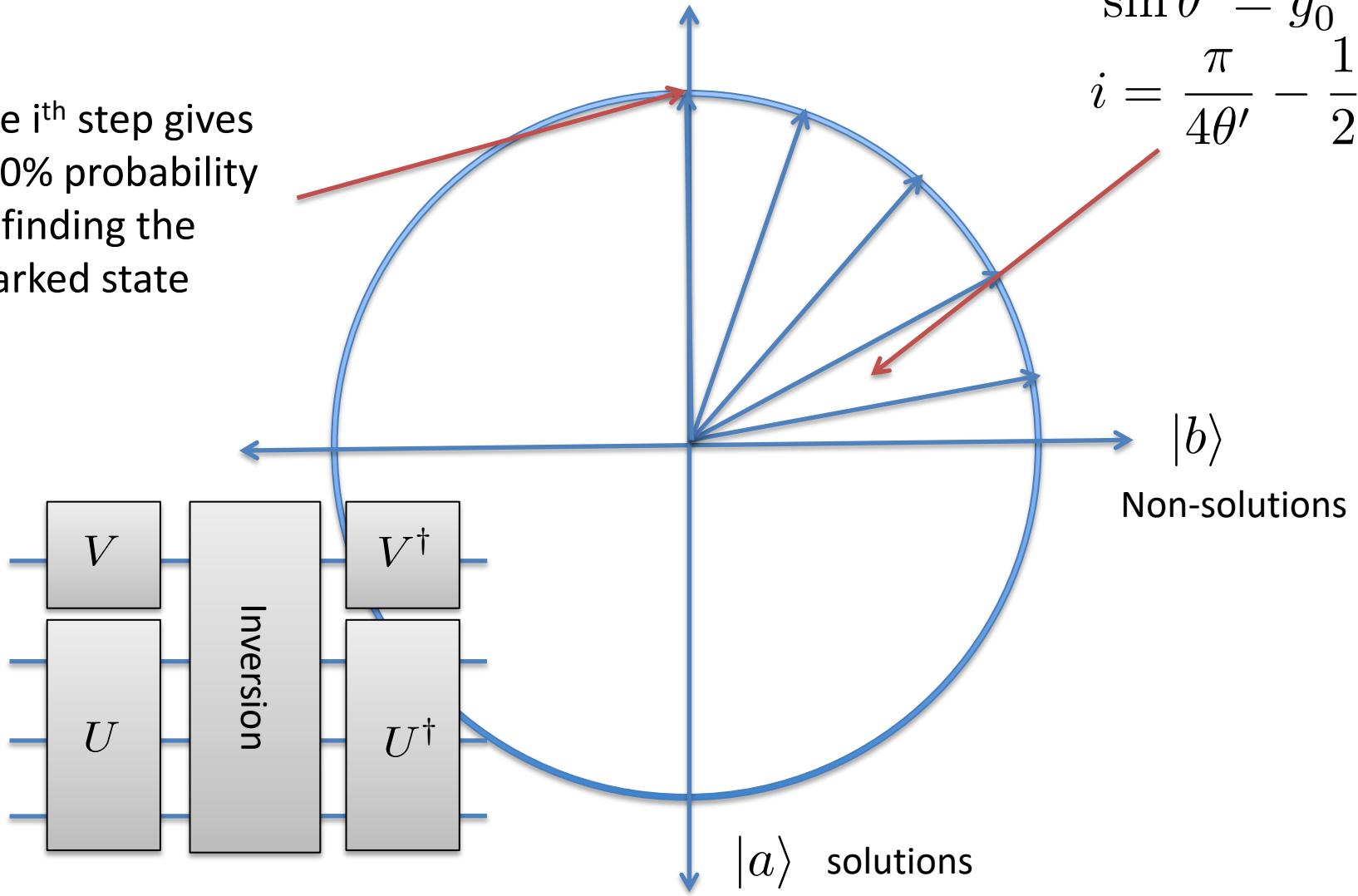
Choose g'_0 s.t. $i = \frac{\pi}{4\theta'} - \frac{1}{2}$ is a whole number

100% success

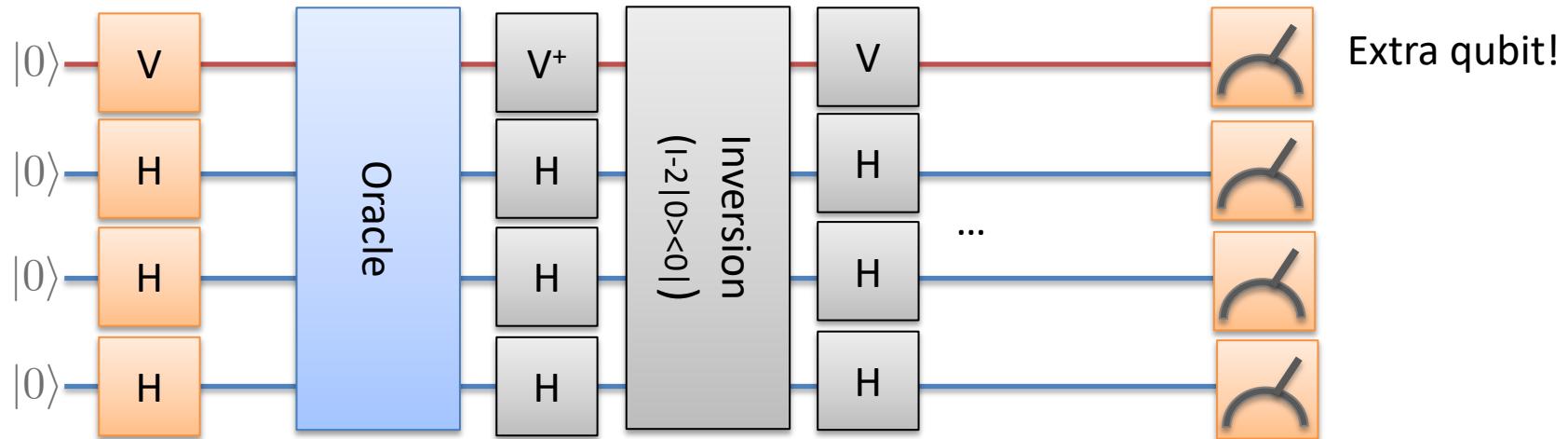
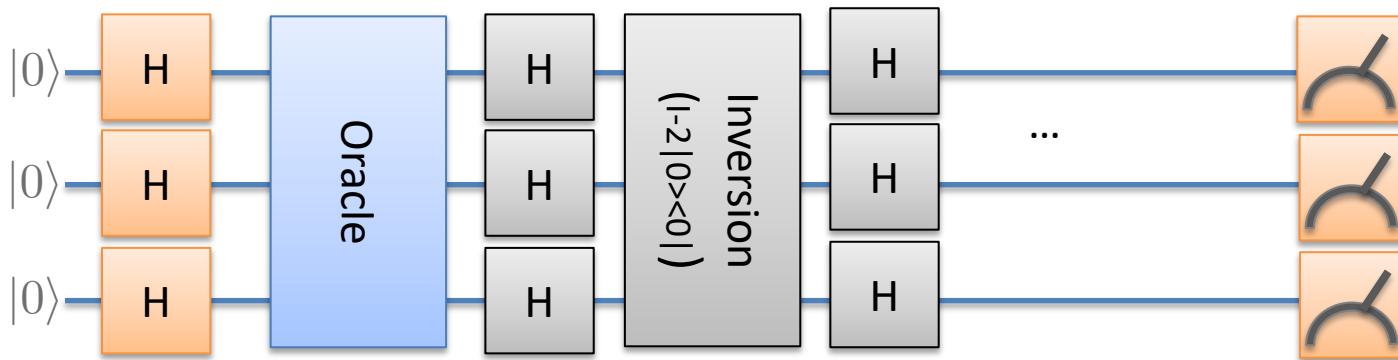
Using amplitude amplification

The i^{th} step gives 100% probability of finding the marked state

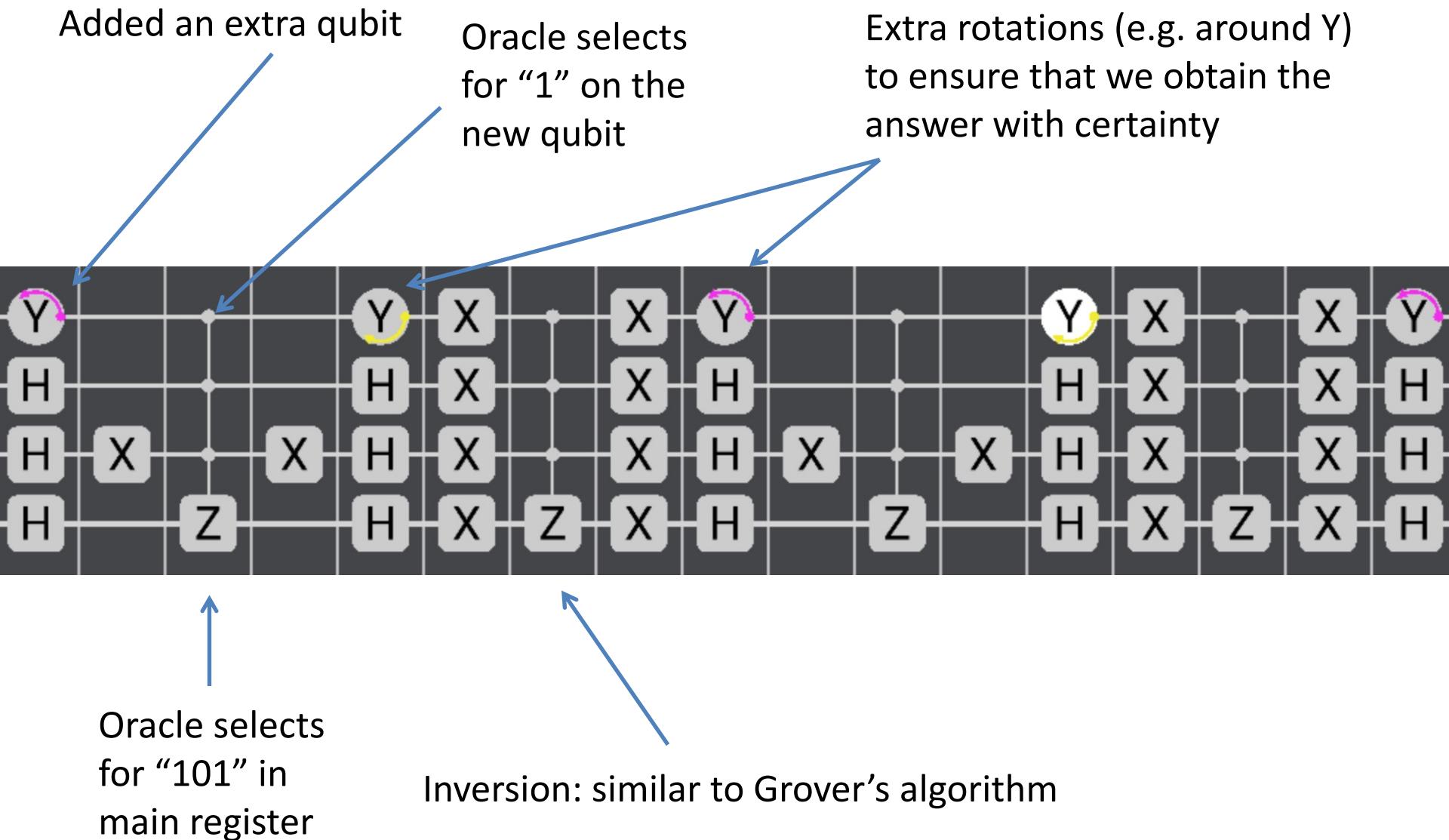
$$\begin{aligned}\sin \theta' &= g'_0 \\ i &= \frac{\pi}{4\theta'} - \frac{1}{2}\end{aligned}$$



Example: Three qubit Grover



Example: Searching for 5 (101)



Example: Searching for 5 (101)



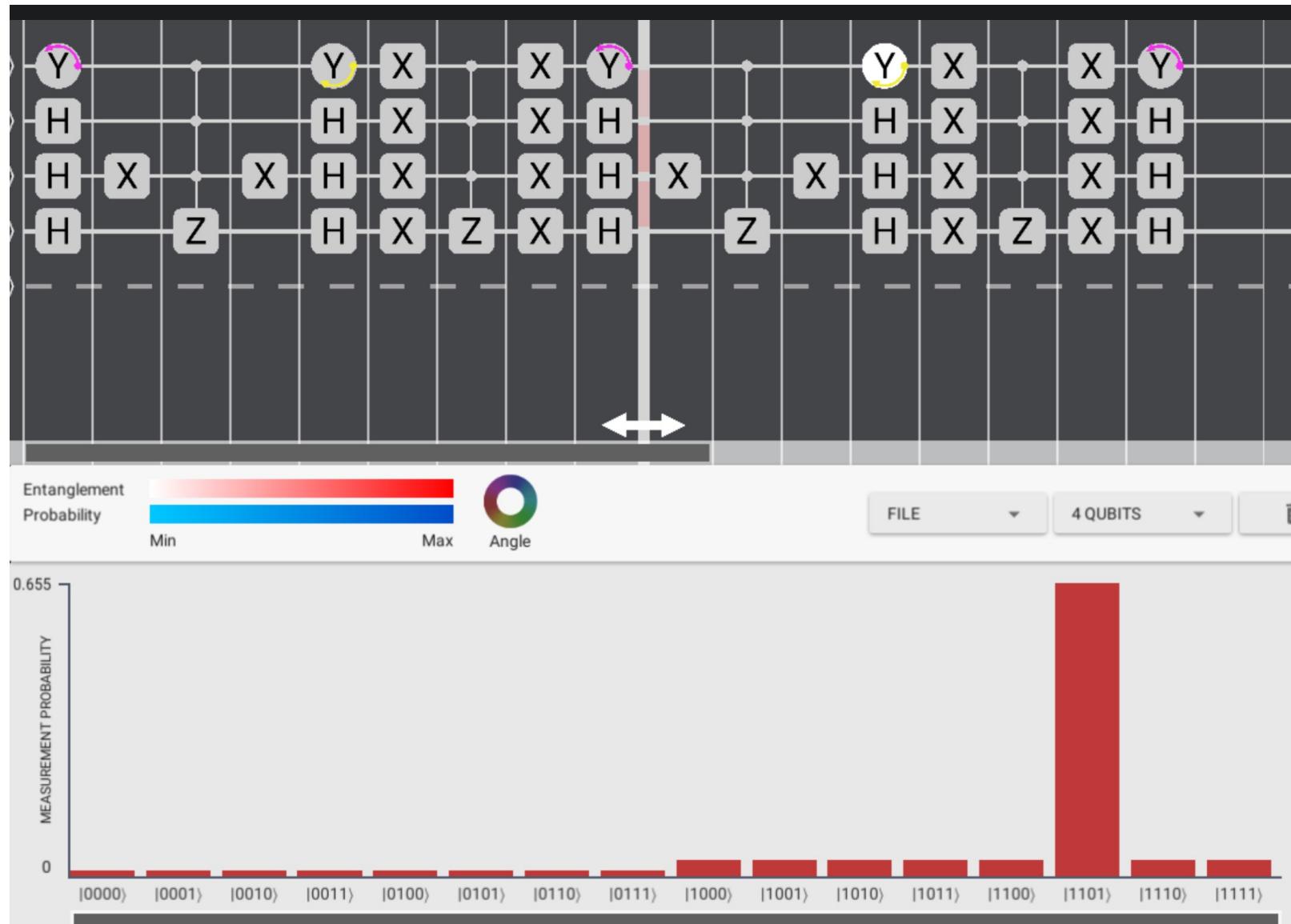
Example: Searching for 5 (101)



Example: Searching for 5 (101)



Example: Searching for 5 (101)



Example: Searching for 5 (101)



Example: Searching for 5 (101)

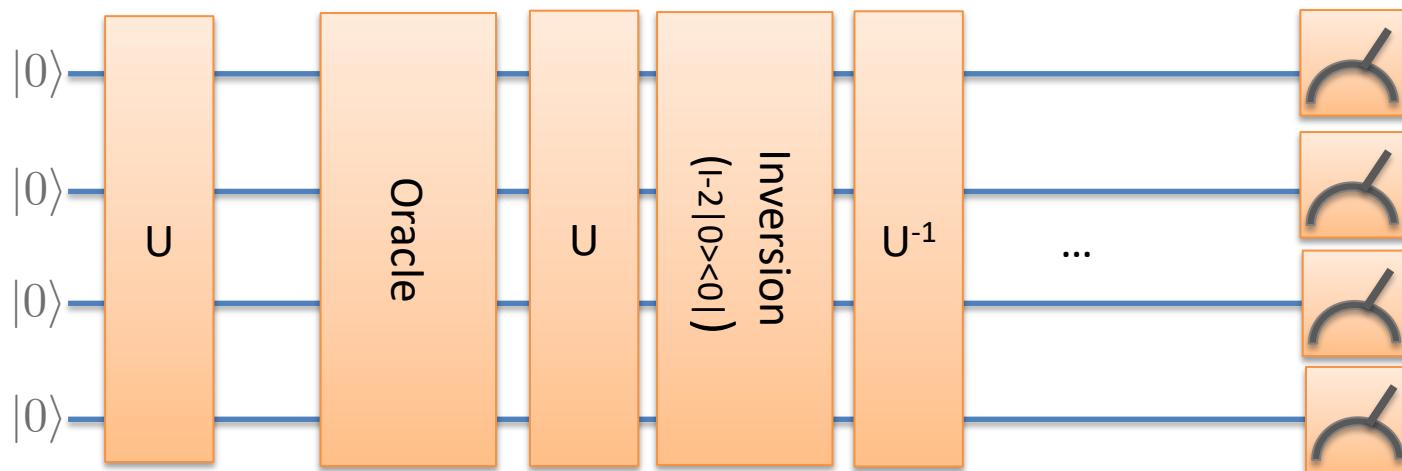


Amplitude Amplification

Given a black box (oracle), U_f , which computes the function $f: \{0,1\}^n \rightarrow \{0,1\}$

Find an x s.t. $f(x) = 1$

- Unordered search, generalisation of Grover's algorithm
- Classically, this requires $N/2$ uses of the oracle
- Quantum mechanically, requires only $O(\sqrt{N})$.



Amplitude Amplification is optimal

Proof in your textbooks.

Grover's algorithm is optimal in terms of the number of applications of the oracle.

For many oracle problems the required number of uses of the oracle scales like:

$$O(\sqrt{N})$$

This means that for a broad range of problems the best speedup we can achieve using a quantum computer is **not** exponential, but polynomial (which can be quite significant).

For problems with identifiable structure, we might hope for more speedup.
More on this next week.

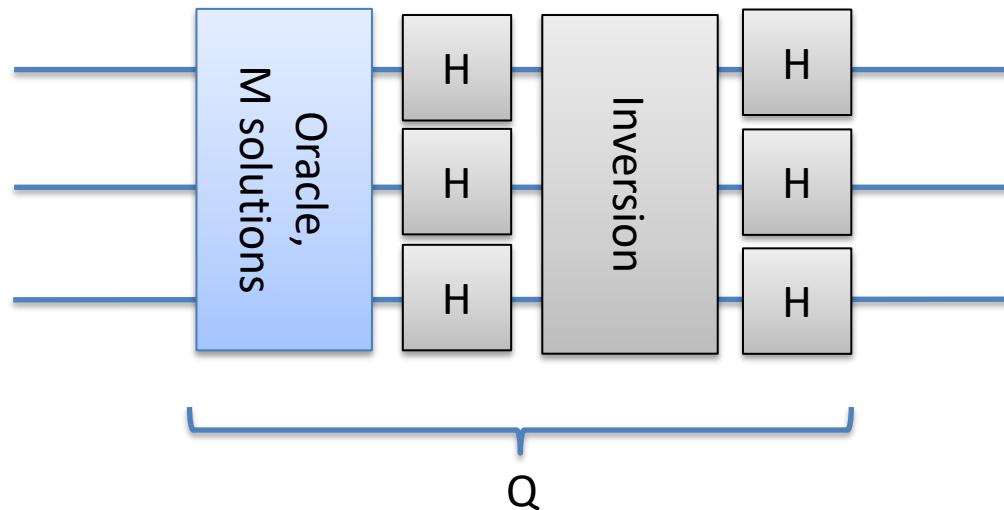
Quantum Counting

Will show you this algorithm now, but will leave some of the details until after next week's lectures/lab.

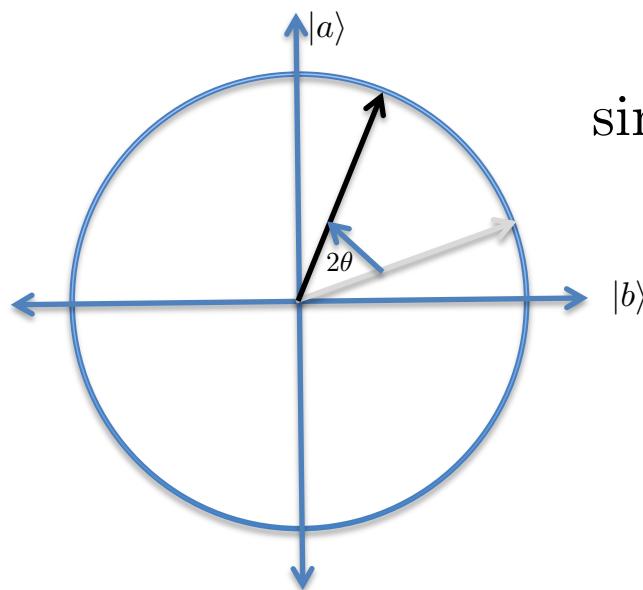
Given an black box (oracle), U_f , which computes the function $f: \{0,1\}^n \rightarrow \{0,1\}$

How many x s.t. $f(x) = 1$?

Equivalent question



What angle rotation does Q make?



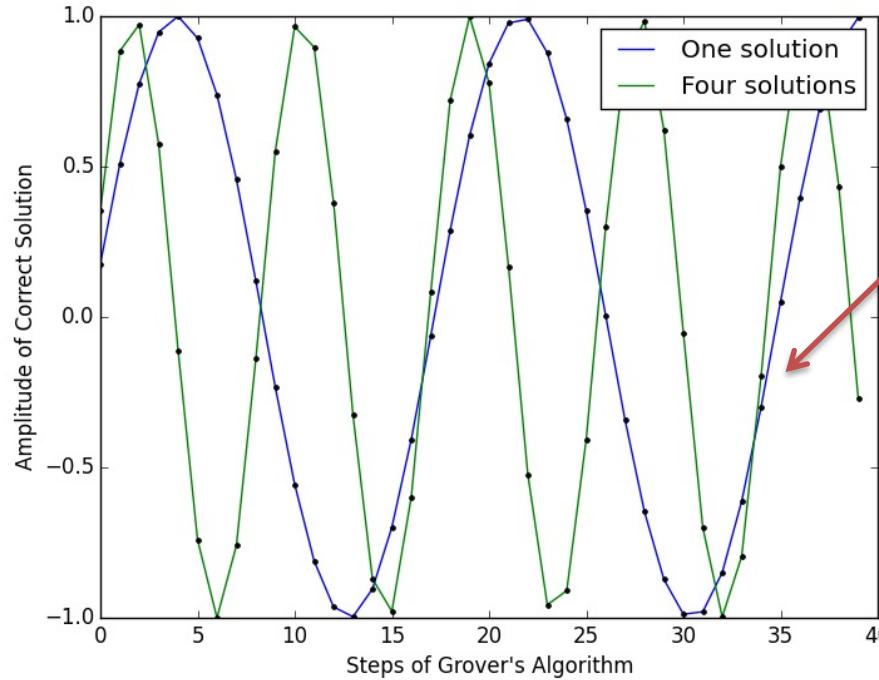
$$\sin \theta = \frac{\sqrt{M}}{\sqrt{N}}$$

Plotting amplitude as function of step number

After k steps:

$$\theta_k = (2k + 1)\theta$$

$$\sin \theta = \frac{\sqrt{M}}{\sqrt{N}}$$



Number of solutions
is reflected in the
period/frequency

Incorrect solutions
would follow cosine,
rather than sin

Amplitude at step 'k' is:

$$g_k = \sin(2k + 1)\theta$$

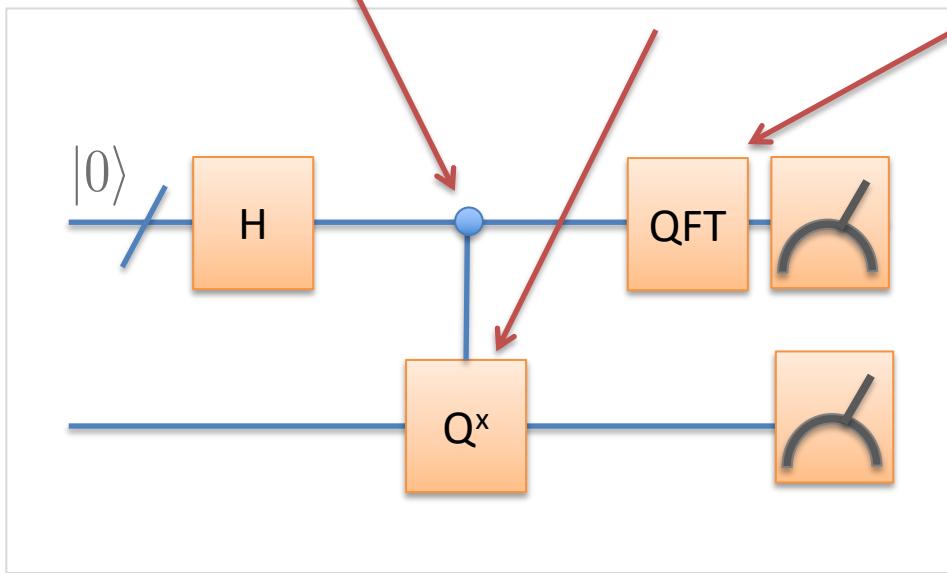
Finding the period of a periodic function

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes Q^x |0\rangle$$

Control
register, x

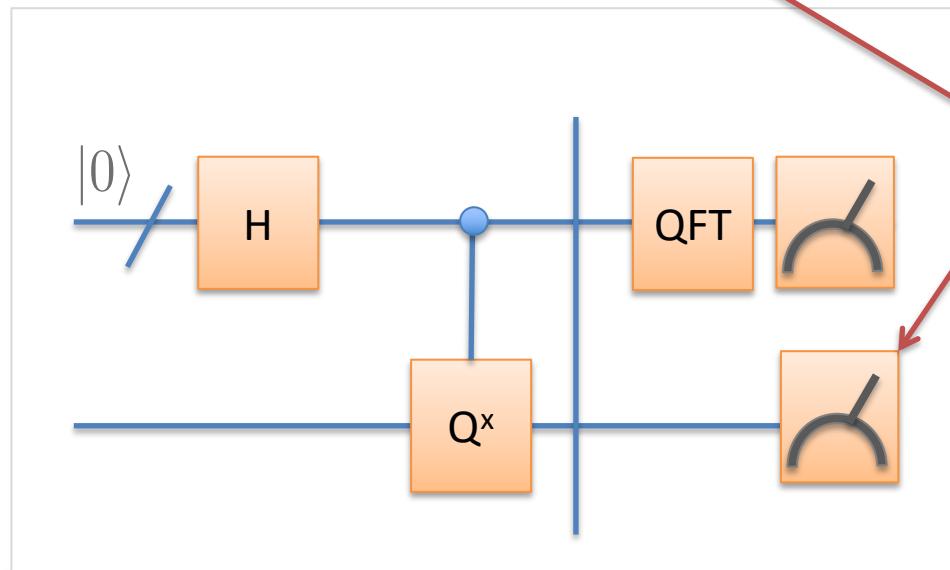
x steps of Grover's
algorithm

Quantum
Fourier
Transform
(next week)



Finding the period of a periodic function

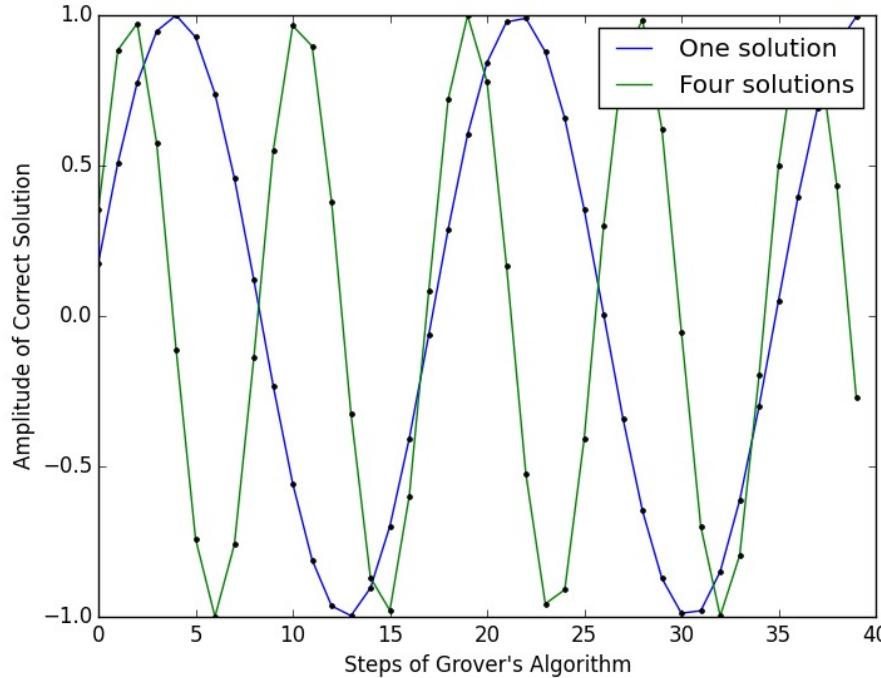
$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes Q^x |0\rangle \\ &= \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes (\underbrace{\sin(2x+1)\theta |\phi_g\rangle + \cos(2x+1)\theta |\phi_b\rangle}_\text{Periodic function}) \end{aligned}$$



If we measure the second register

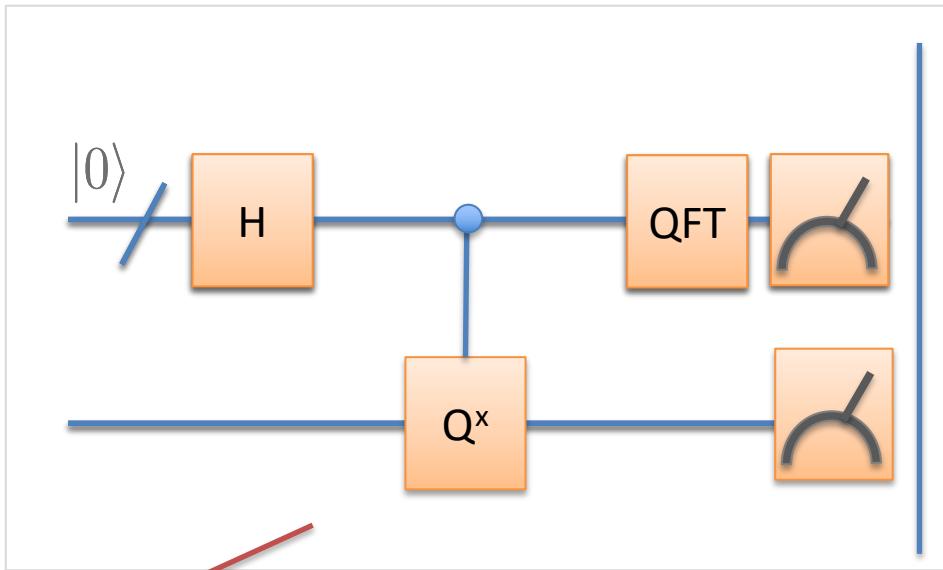
After measurement of the second register

$$|\psi\rangle = \sum \sin(2x + 1)\theta |x\rangle \otimes |\psi_g\rangle \quad (\text{not normalized})$$



Next step: Use Quantum Fourier Transformation to find the period

After the Fourier transformation

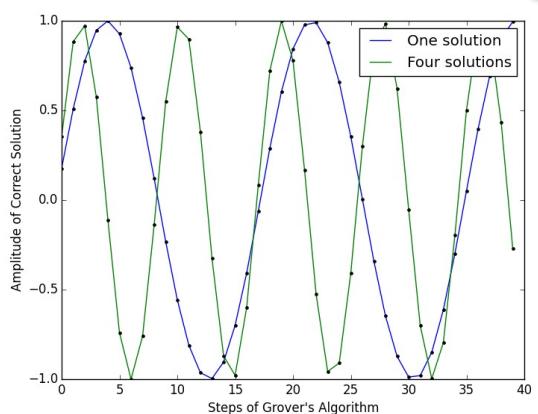


Dimension: N'

Dimension: N

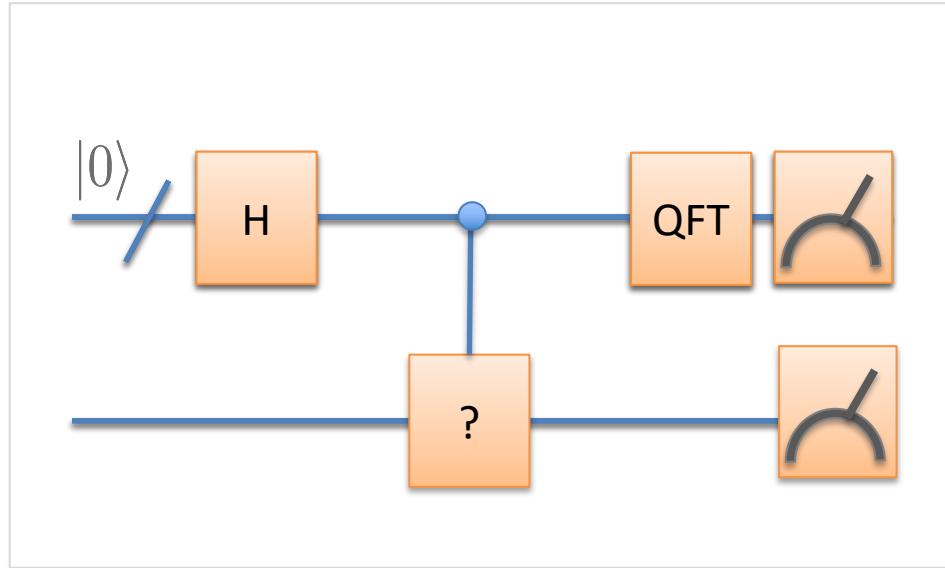
After Fourier transforming a periodic function, we get a good approximation to theta. If we measure value "j":

$$\theta = \frac{j\pi}{N'} \quad \sin \theta = \frac{\sqrt{M}}{\sqrt{N}}$$



Which we can solve to obtain the number of solutions, M

Phase Estimation and HSP Problems



The Hadamard and Fourier transform part is known as **phase estimation**, and extremely useful for period functions (and eigenvalues which are periodic).

As we will see in the next lecture, this pattern is often repeated.

This Week

Lecture 9

Introduction to Grover's algorithm for amplitude amplification,
geometric interpretation

Lecture 10

Amplitude Amplification, Succeeding with Certainty, Quantum
Counting

Lab

Grover's algorithm