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

THE UNIVERSITY OF MELBOURNE

Amplitude Amplification

PHYC90045 Introduction to Quantum Computing

Lecture 10

Amplitude Amplification

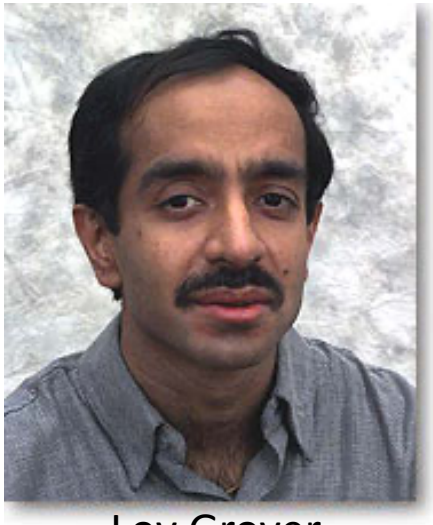
- This lecture: Amplitude amplificaiton
  - Amplitude Amplification
  - Succeeding with certainty
  - Quantum Counting

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)

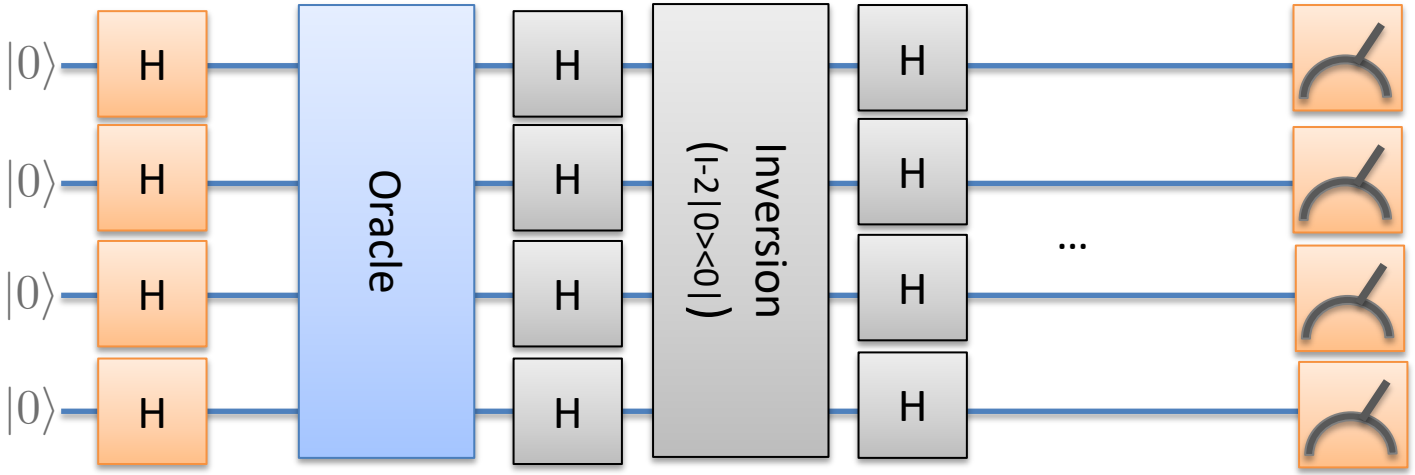
- Unordered search, find one marked item among many
- Classically, this requires N/2 queries to the oracle
- Quantum mechanically, requires only O(√N) queries.



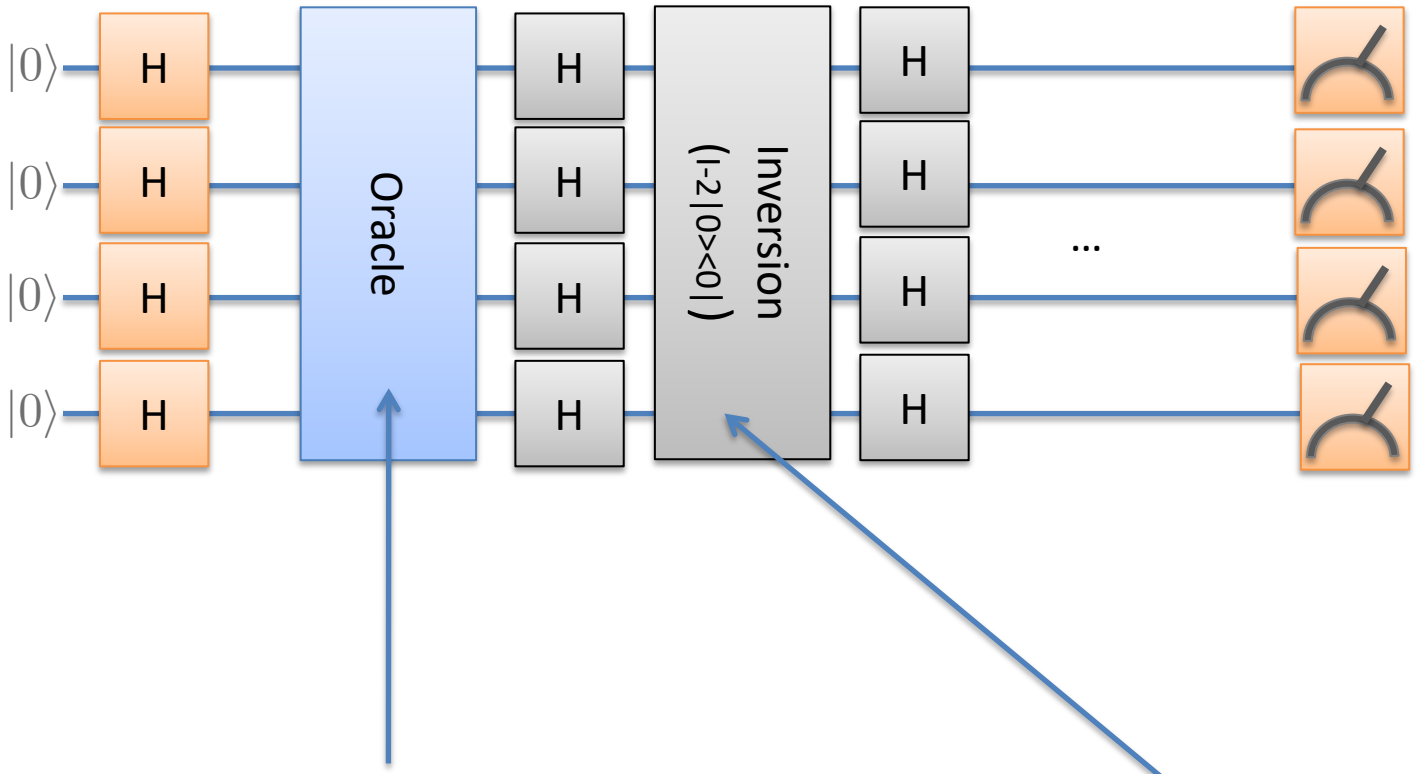
Lov Grover

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

High level structure:



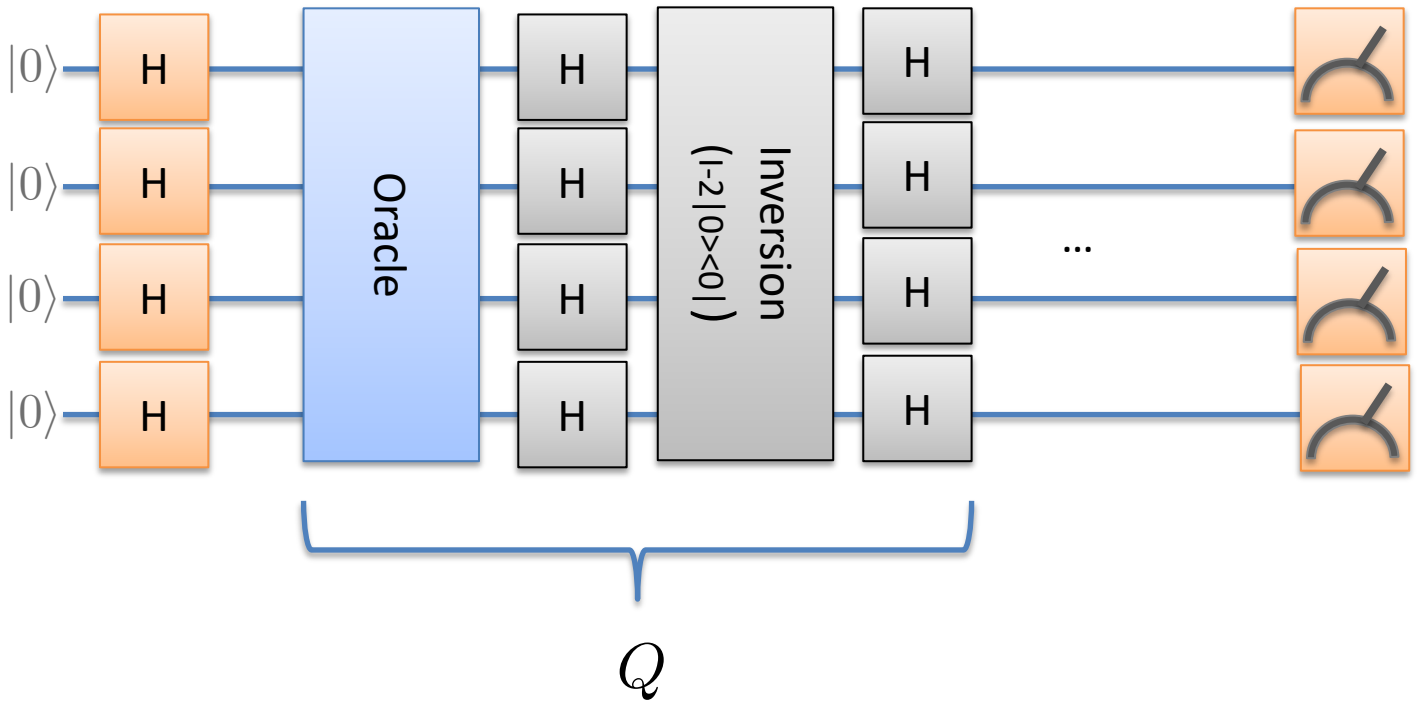
Some notation



$$S_G = I - 2\left|m\right\rangle\left\langle m\right|$$

$$S_0 = I - 2\left|0\right\rangle\left\langle 0\right|$$

Some notation



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

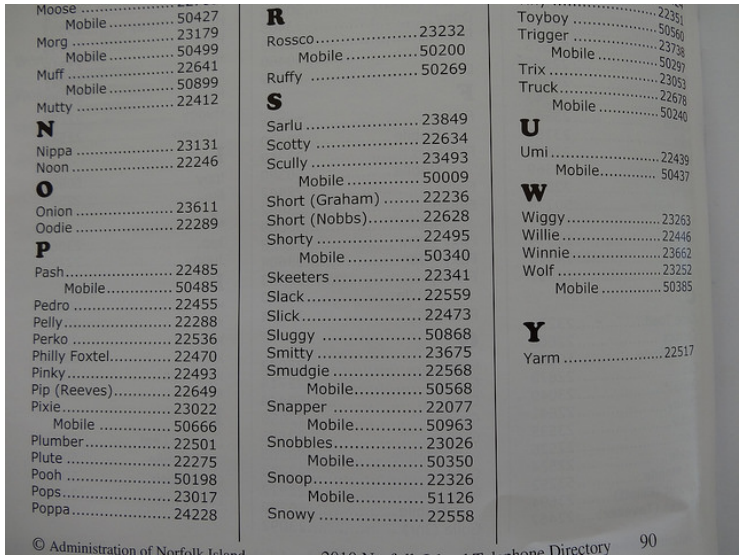
Oracles for NP-problems

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

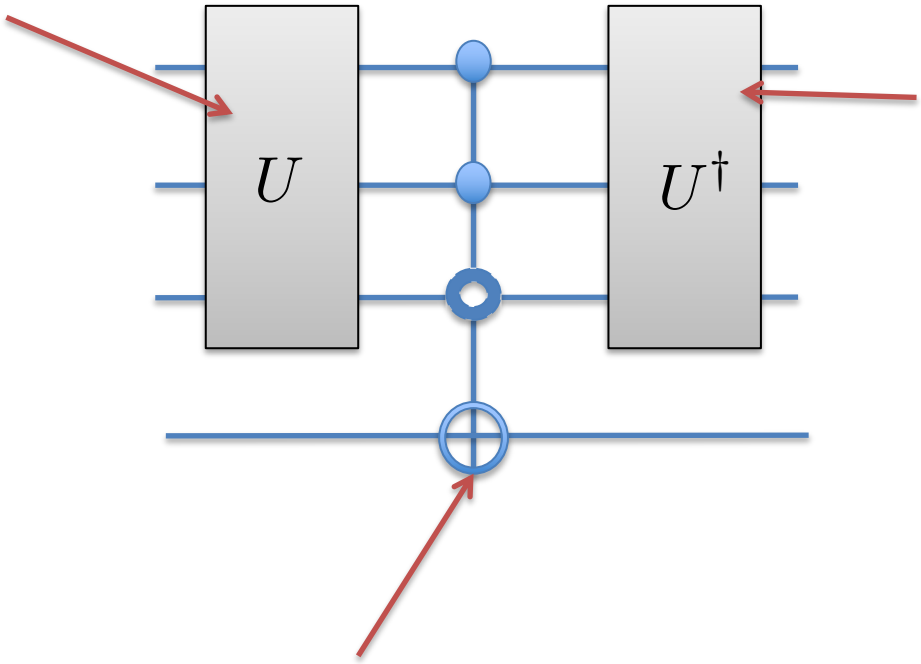
Straightforward application of Grover's algorithm provides a **polynomial** improvement over random guessing… and potentially a better (but still polynomial speedup) known as **amplitude amplication**.


Moose
Mobile 50427
Morg 23179
Mobile 50499
Muff 22641
Mobile 50899
Mutty 22412
N
Nippa 23131
Noon 22246
O
Onion 23611
Oodie 22289
P
Pash 22485
Mobile 50485
Pedro 22455
Pelly 22288
Perko 22536
Philly Foxtel 22470
Pinky 22493
Pip (Reeves) 22649
Pixie 23022
Mobile 50666
Plumber 22501
Plute 22275
Pooh 50198
Pops 23017
Poppa 24228
R
Rossco 23232
Mobile 50200
Ruffy 50269
S
Sarlu 23849
Scotty 22634
Scully 23493
Mobile 50009
Short (Graham) 22236
Short (Nobbs) 22628
Shorty 22495
Mobile 50340
Skeeters 22341
Slack 22559
Slick 22473
Sluggy 50868
Smitty 23675
Smudgie 22568
Mobile 50568
Snapper 22077
Mobile 50963
Snobbles 23026
Mobile 50350
Snoop 22326
Mobile 51126
Snowy 22558
Toyboy 22351
Trigger 50560
Mobile 23738
Trix 50297
Truck 23053
Mobile 22678
U
Umi 50240
Mobile 22439
W
Wiggy 50437
Willie 23263
Winnie 22446
Wolf 23662
Mobile 23252
Y
Yarm 50385
22517
© Administration of Norfolk Island
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.

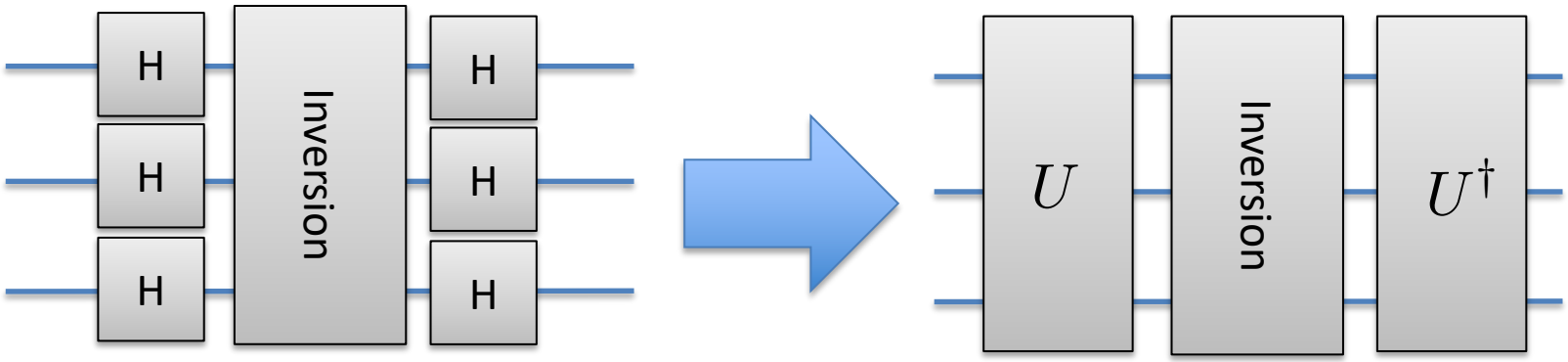


"Uncompute" the hash function – ensures the input register remains unchanged.

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

Amplitude amplification

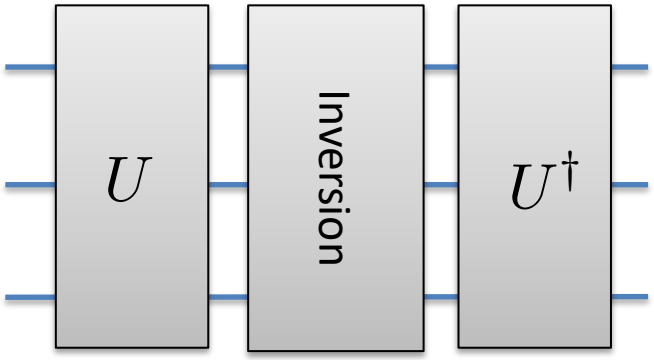
What happens if we replace the Hadamard gates with some other U? Perhaps, for example, we can create a U which gives the correct outcome with probability greater than 1/N. Can we get any advantage?



Inversion about the mean

Apply general U instead of H

New inversion step



Apply general U instead of H

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

Then we can break this up as:

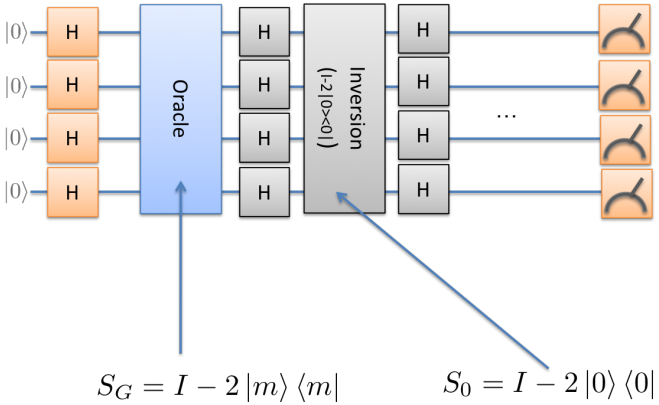
$$|\phi\rangle = g_0\,|\phi_g\rangle + b_0\,|\phi_b\rangle$$

Good: In the subspace spanned by all solutions

Bad: Not in the subspace spanned by all solutions

Maths of the Geometric Interpretation

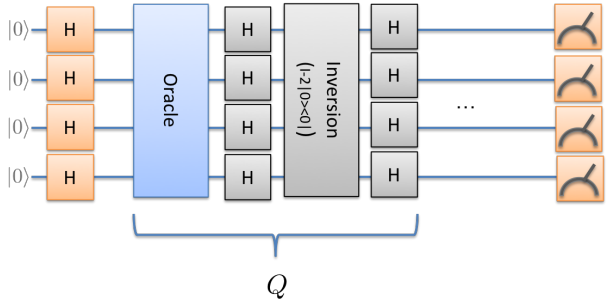
$$
\begin{aligned}
US_0U^\dagger |\psi\rangle &= U(I - 2|0\rangle\langle 0|)U^\dagger |\psi\rangle \\
&= |\psi\rangle - 2\langle 0| U^\dagger |\psi\rangle U|0\rangle \\
&= |\psi\rangle - 2\langle \psi| U|0\rangle^* U|0\rangle
\end{aligned}
$$



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

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

Q recursive step:

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

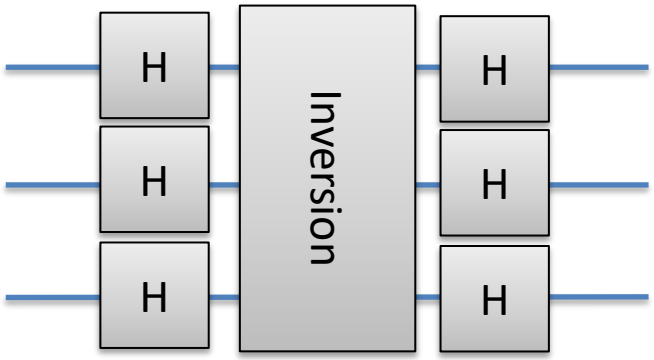
Compare to a rotation matrix:

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

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

Grover vs Amplitude Amplification

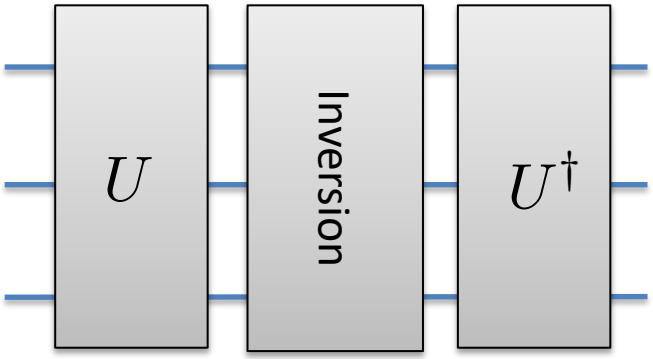
Grover



Angle of rotation:

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

Amplitude Amplification



Angle of rotation:

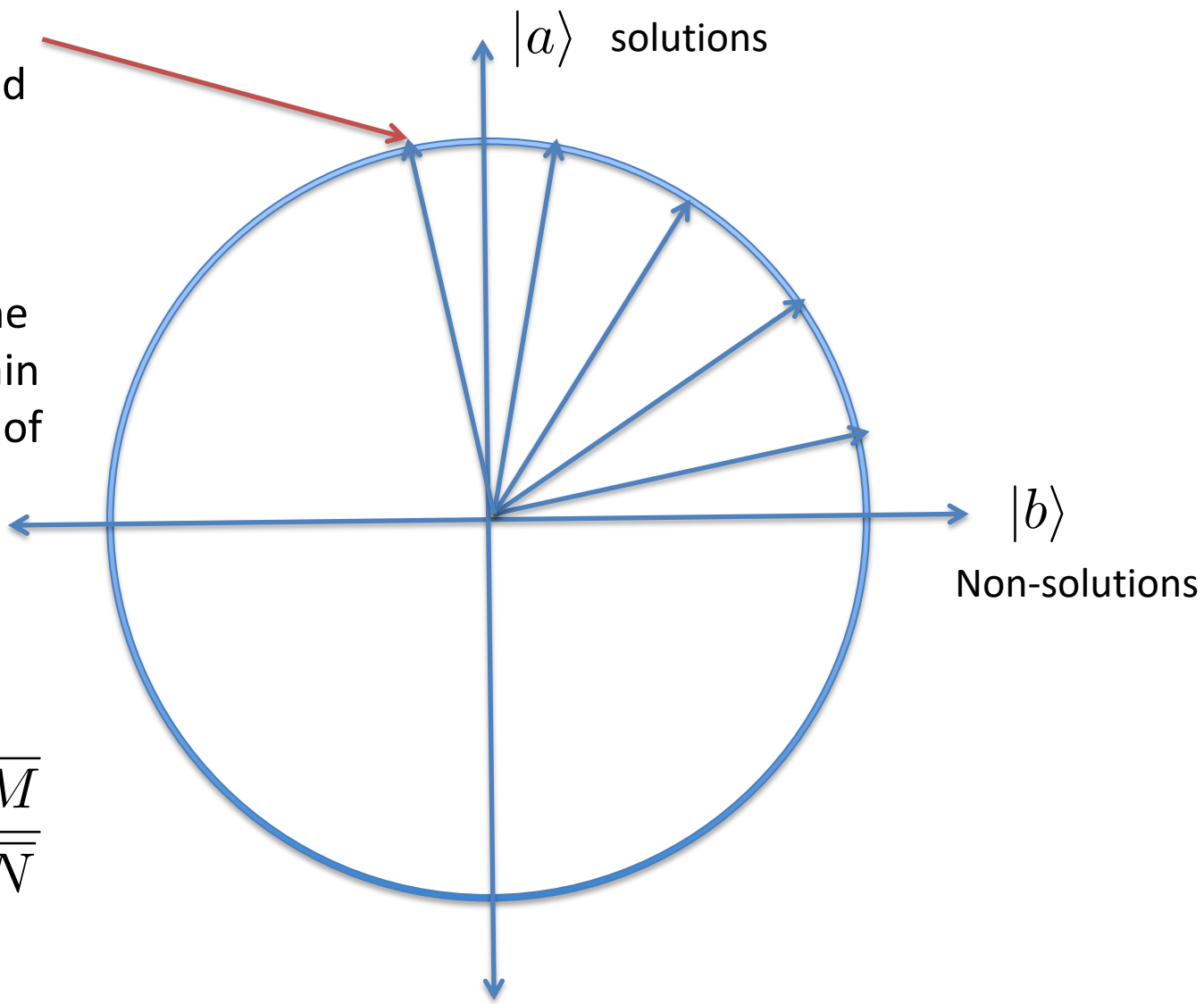
$$\sin\theta = \sqrt{t} = g_0$$

If you can construct a U with a higher probability of success than random guessing 1/N, then amplitude amplificaton 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?



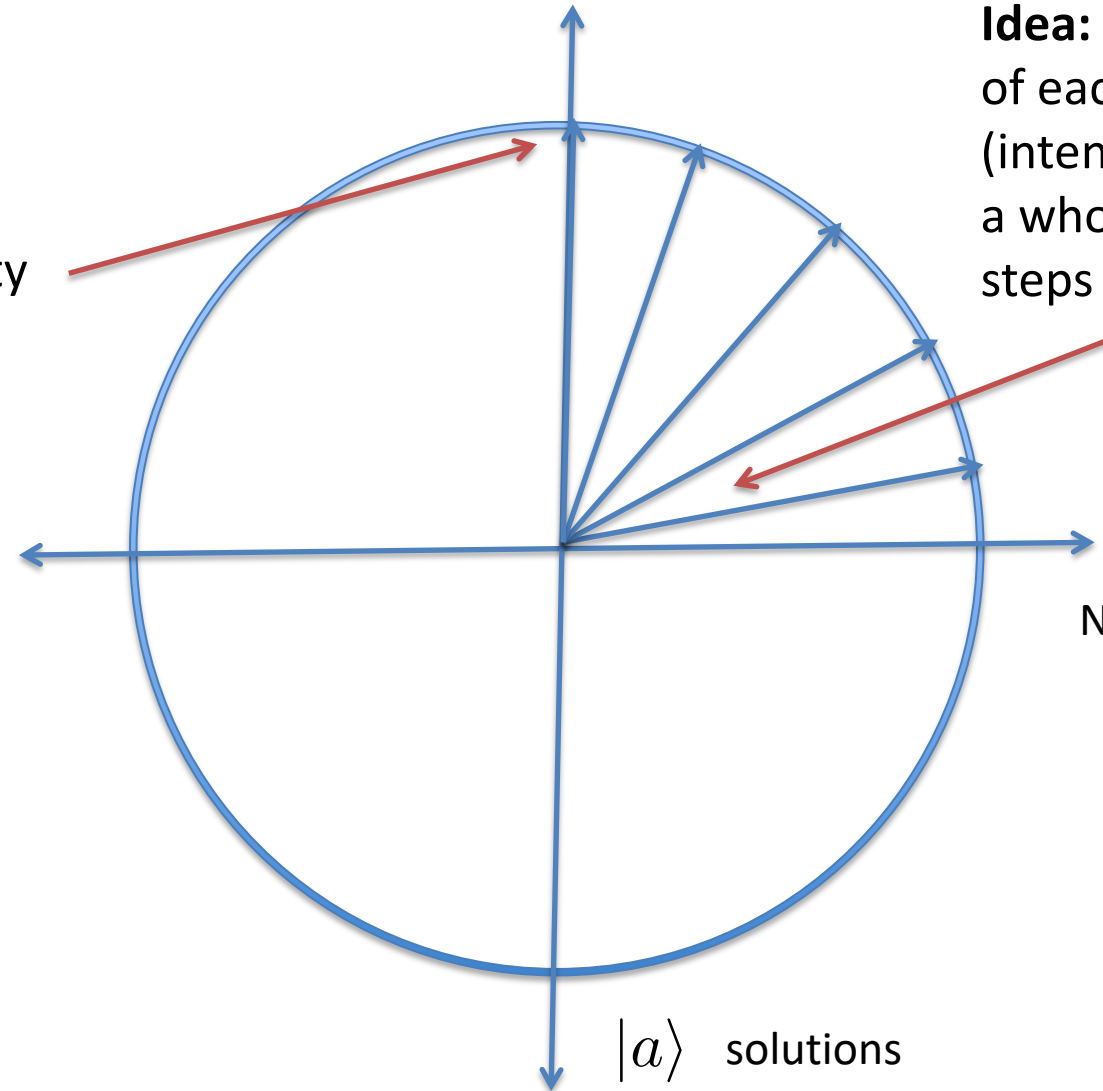
$$\sin\theta = \frac{\sqrt{M}}{\sqrt{N}}$$

Grover with 100% success

Using amplitude amplification

Idea: reduce the size of each step (intentionally) so that a whole number of steps is required.

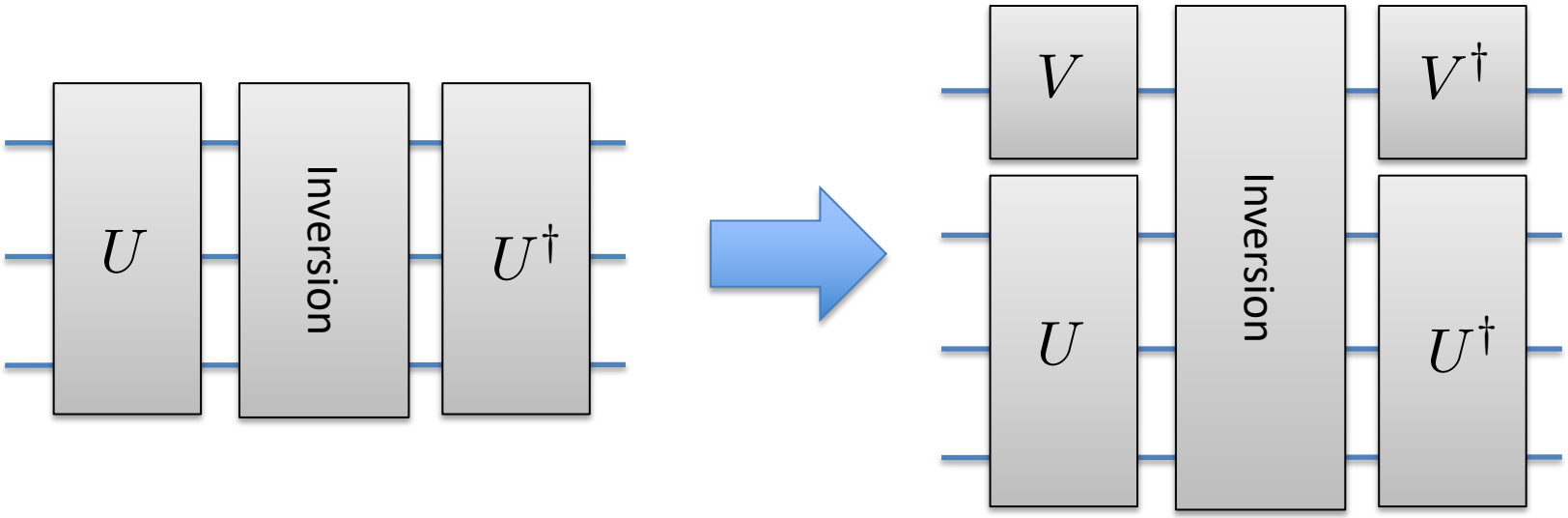
This step gives 100% probability of finding the marked state



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:

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

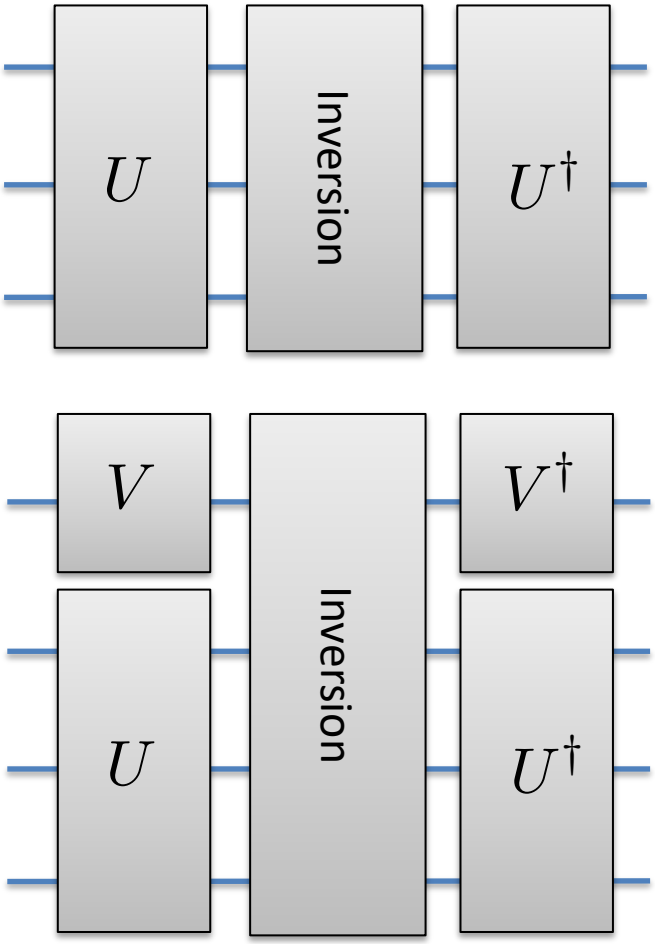
With new qubit:

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

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:

$$V \otimes U |0\rangle = g_0' |1\rangle|\phi_g\rangle + \ldots$$

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

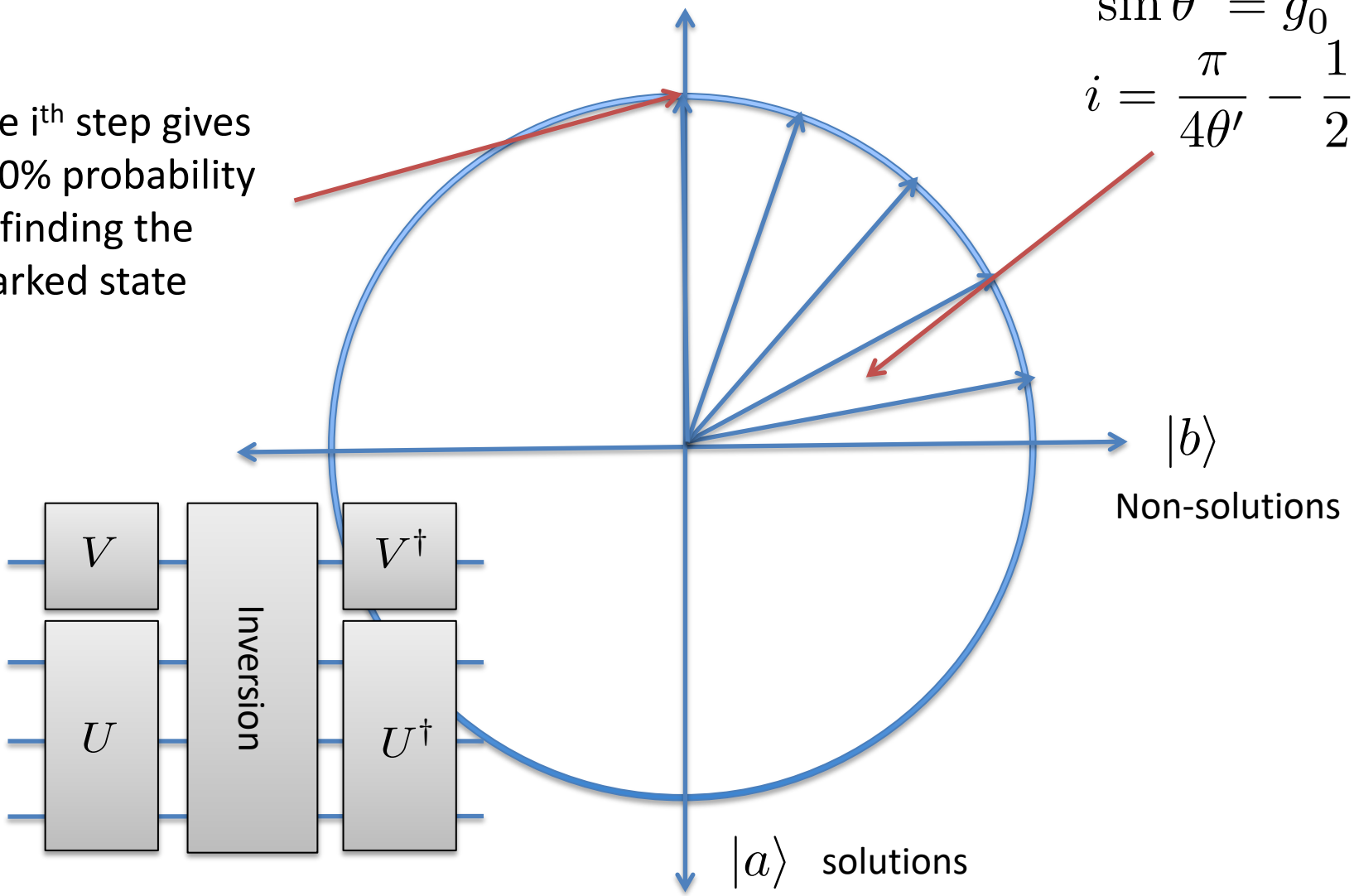
100% success

Using amplitude amplification

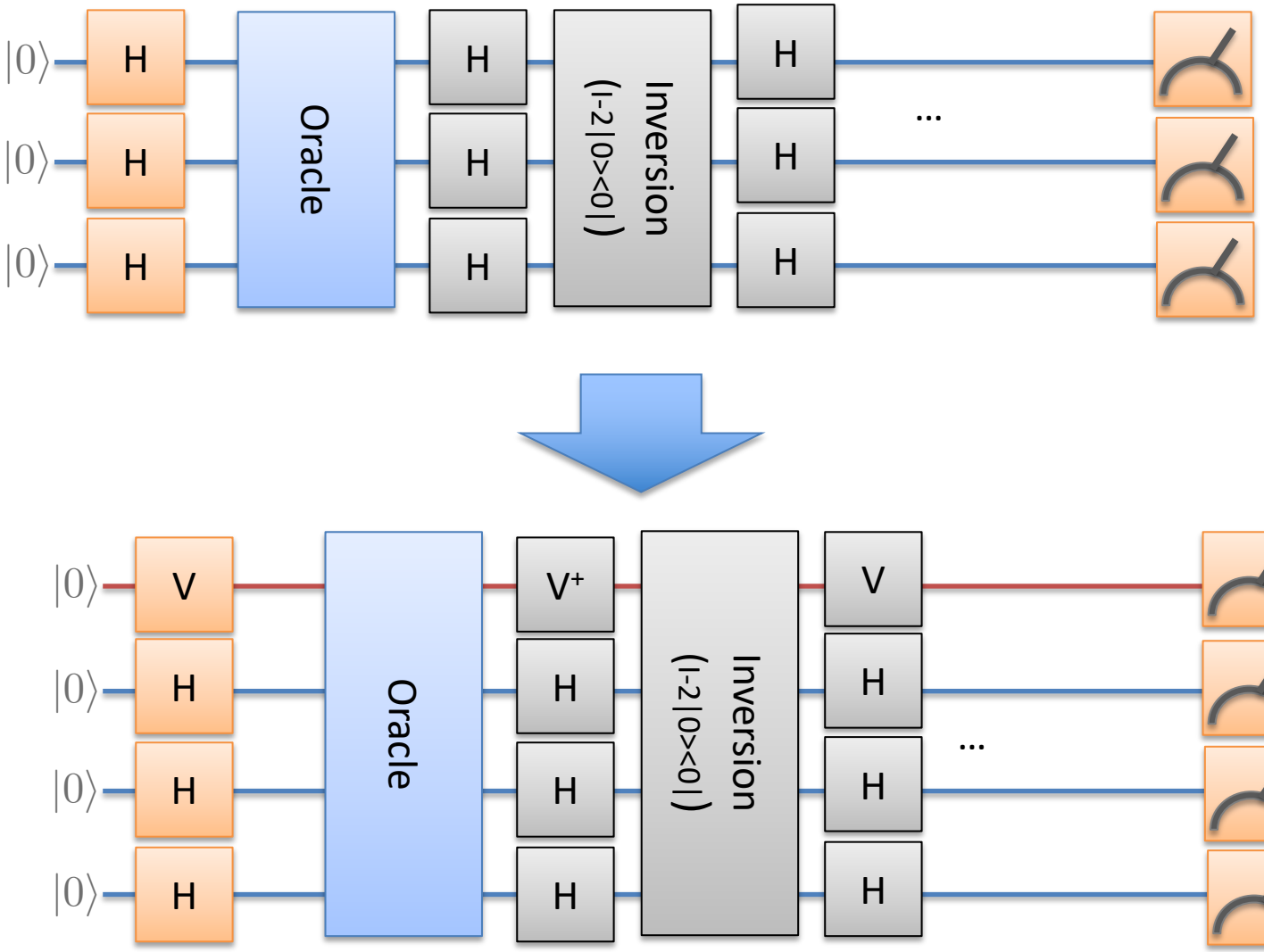
$$\sin\theta' = g_0'$$

$$i = \frac{\pi}{4\theta'} - \frac{1}{2}$$

The i[th] step gives 100% probability of finding the marked state



Example: Three qubit Grover



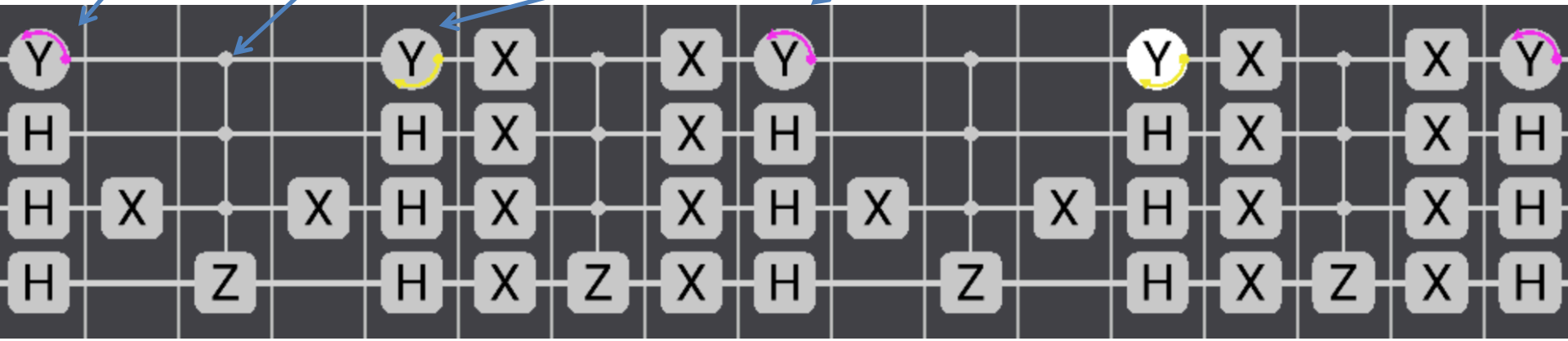
Extra qubit!

Example: Searching for 5 (101)

Added an extra qubit

Oracle selects for “1” on the new qubit

Extra rotations (e.g. around Y) to ensure that we obtain the answer with certainty

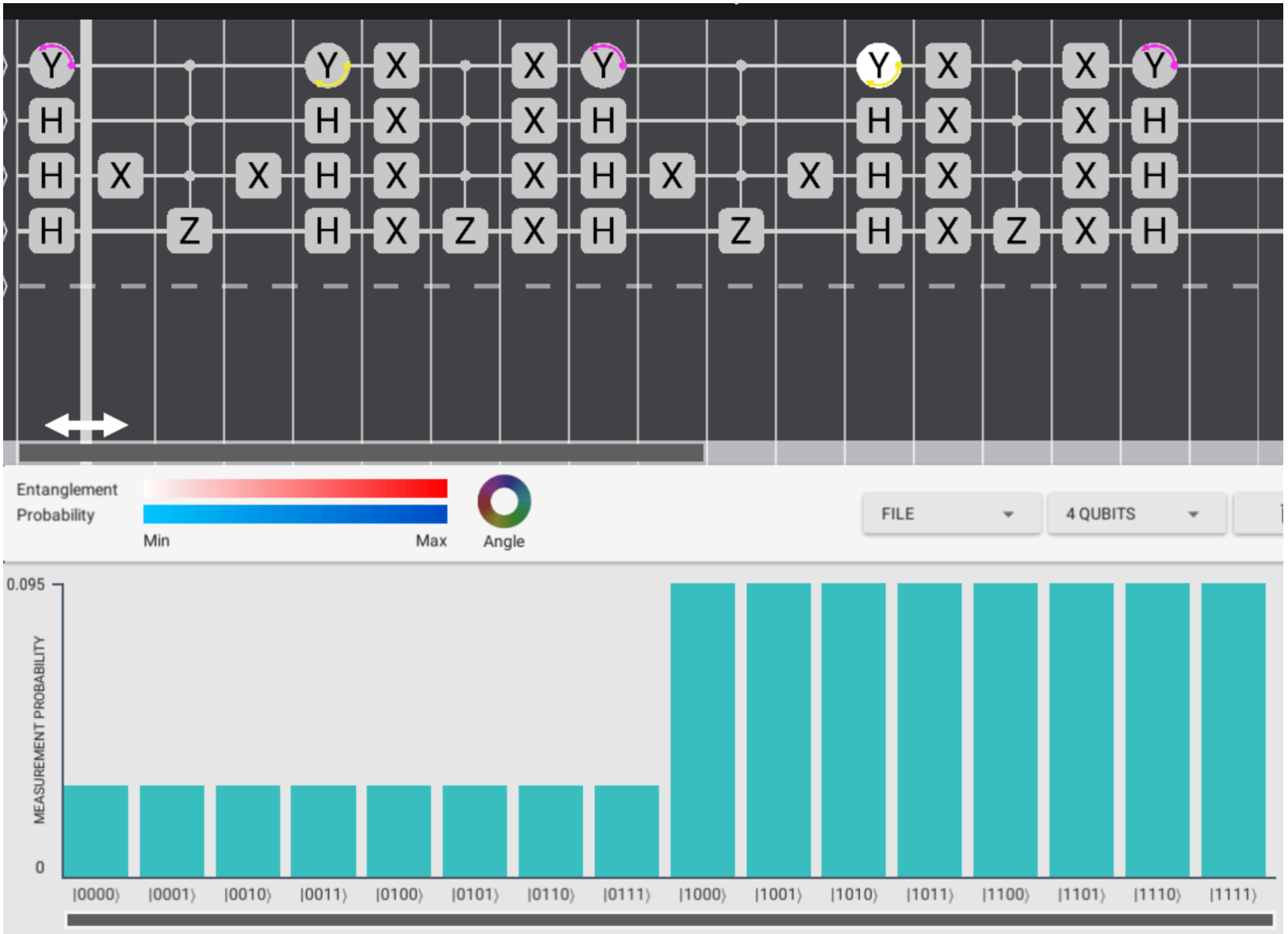


Oracle selects for “101” in main register

Inversion: similar to Grover’s algorithm

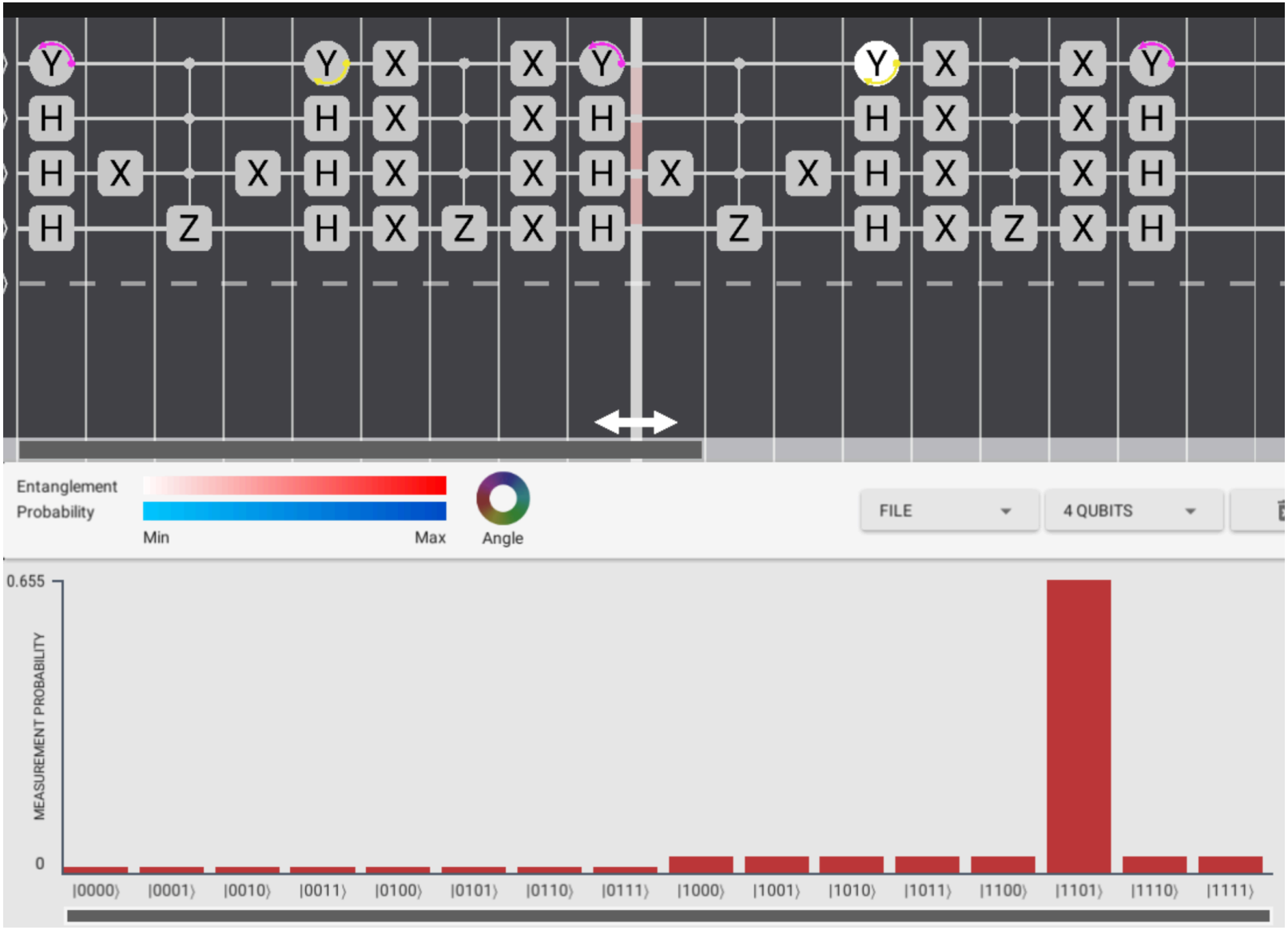
Example: Searching for 5 (101)

Example: Searching for 5 (101)

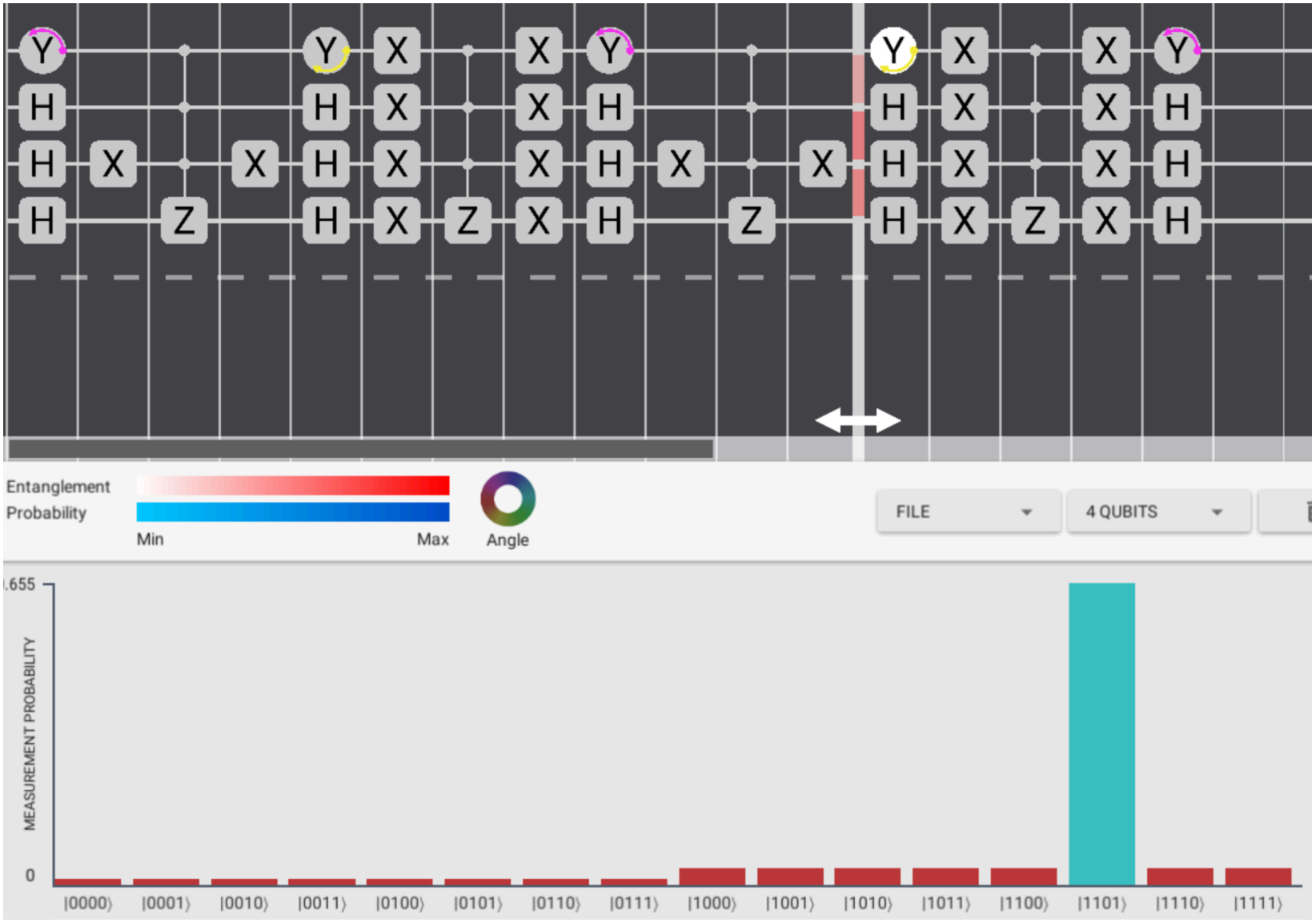


Example: Searching for 5 (101)

Example: Searching for 5 (101)



Example: Searching for 5 (101)



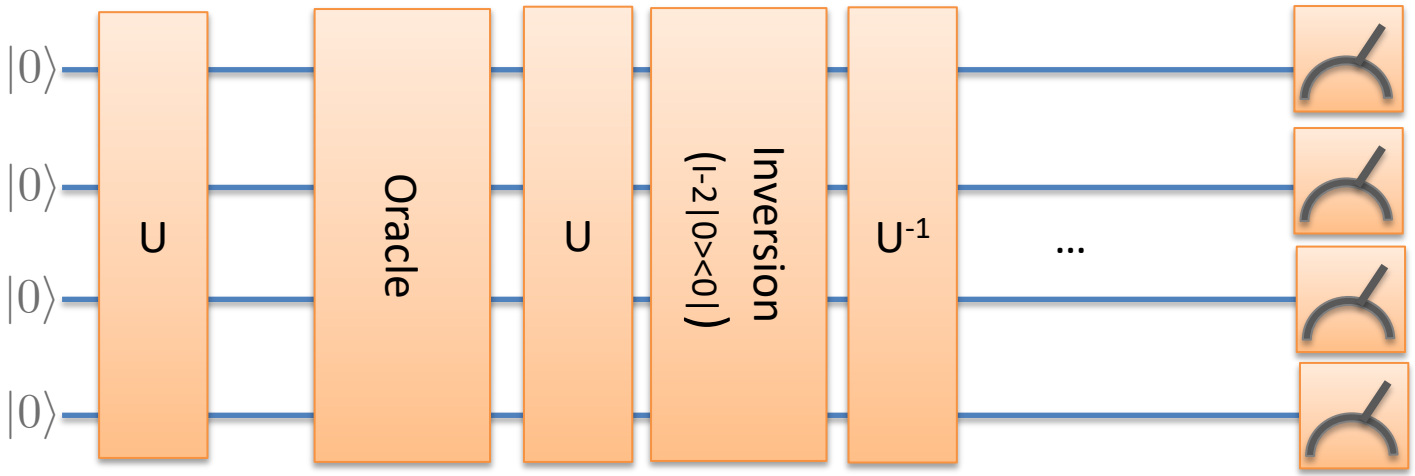
Example: Searching for 5 (101)

Amplitude Amplification

Given an 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(√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.

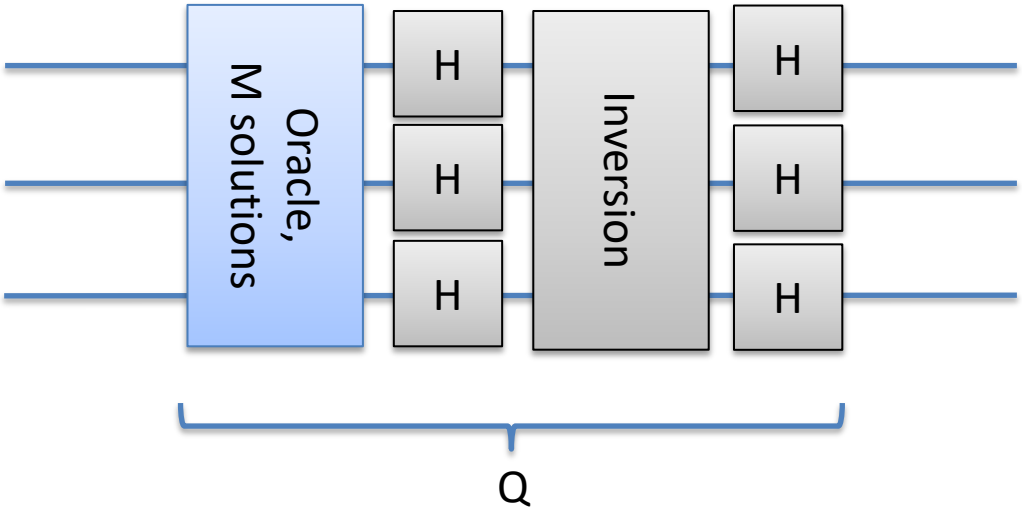
Quantum Counting

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

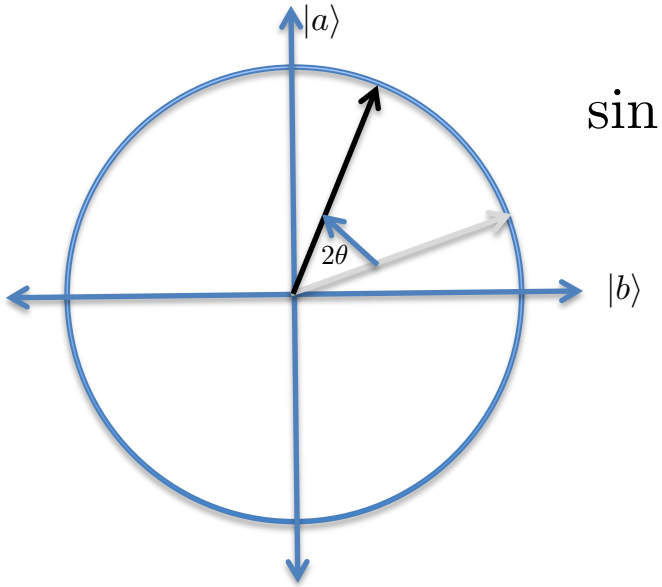
Given an black box (oracle), U_f, which computes the function $f: \{0,1\}^n \rightarrow \{0,1\}$

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

Equivalent question



What angle rotation does Q make?

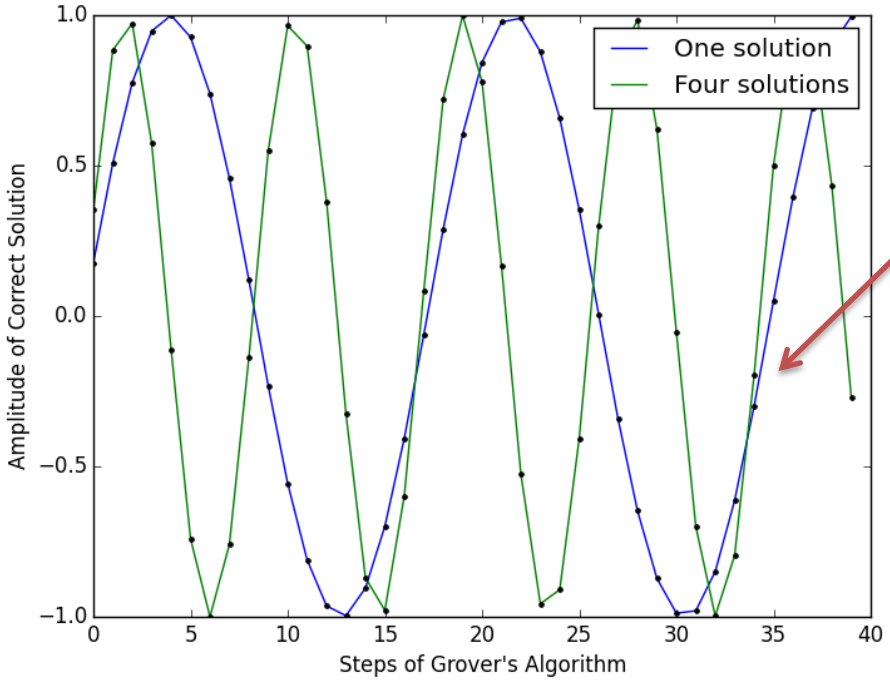


$$\sin\theta = \frac{\sqrt{M}}{\sqrt{N}}$$

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:

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

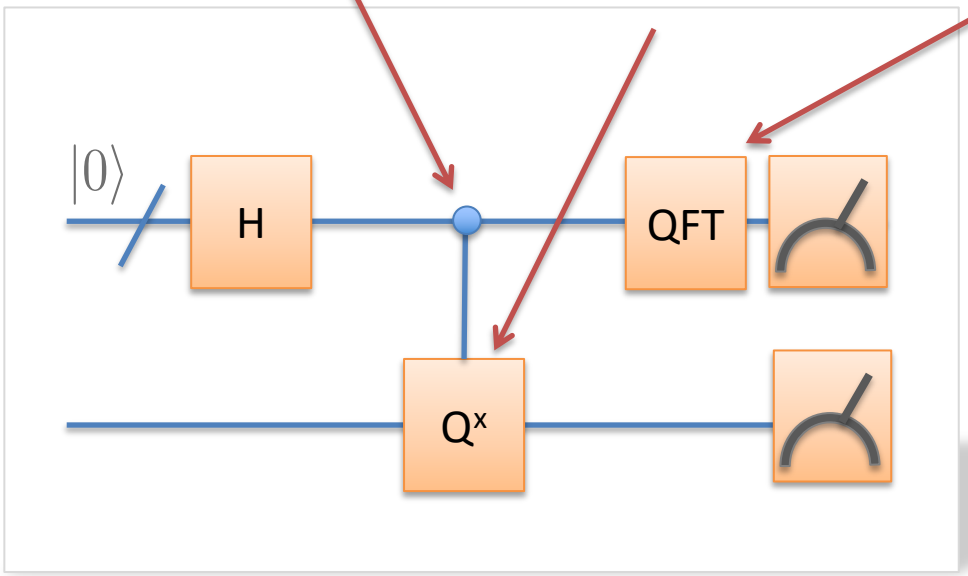
Finding the period of a periodic function

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

Control register, x

x steps of Grover's algorithm

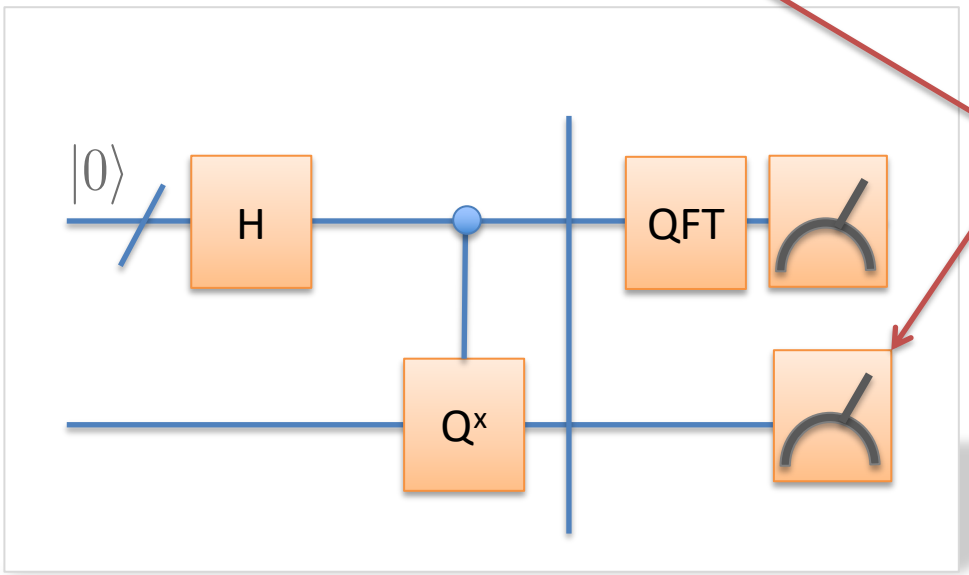
Quantum Fourier Transform (next week)



Finding the period of a periodic function

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

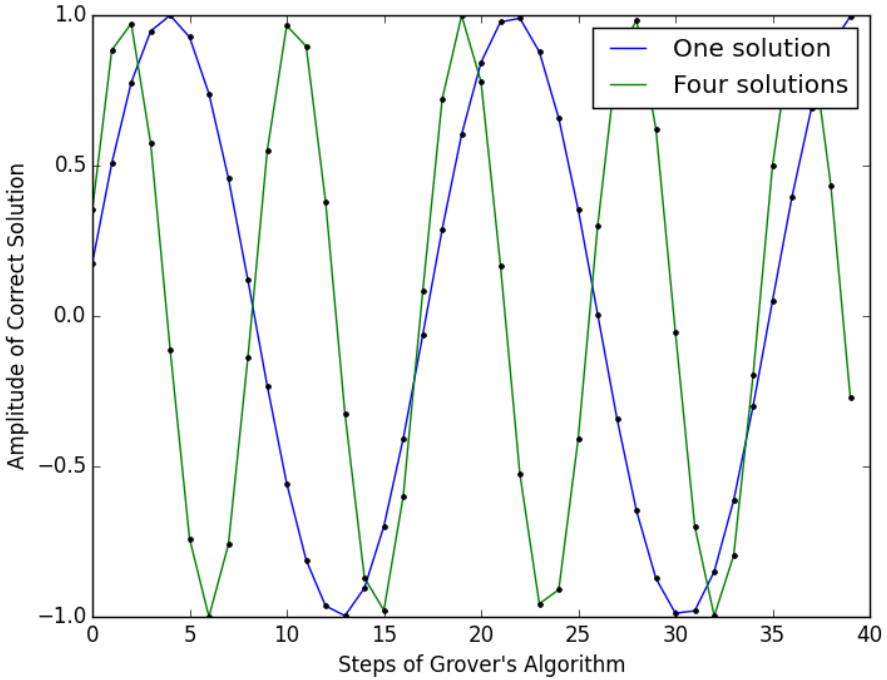
$$= \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes (\sin(2x+1)\theta \, |\phi_g\rangle + \cos(2x+1)\theta \, |\phi_b\rangle)$$



If we measure the second register

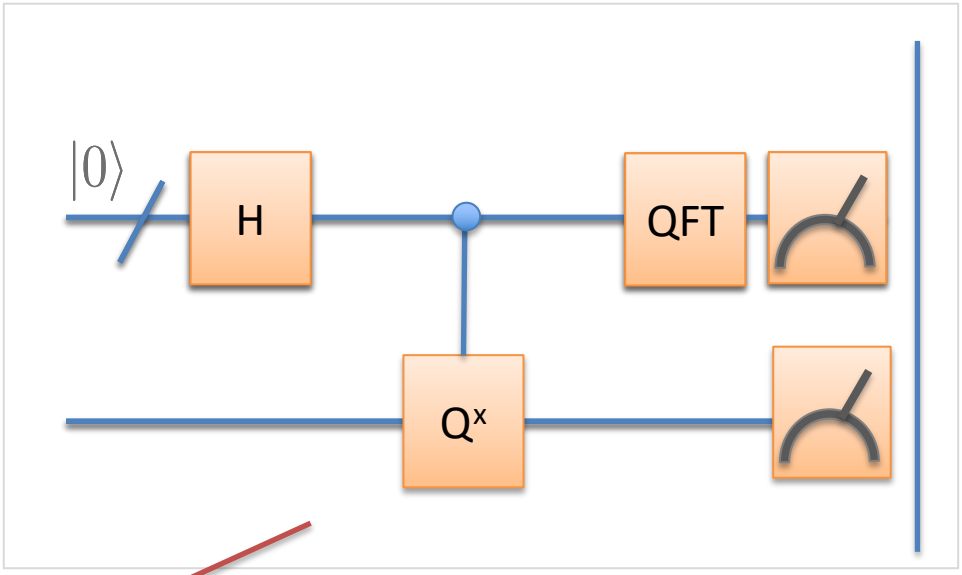
After measurement of the second register

$$|\psi\rangle = \sum_i \sin(2x+1)\theta\,|x\rangle \otimes |\psi_g\rangle$$ (not normalized)



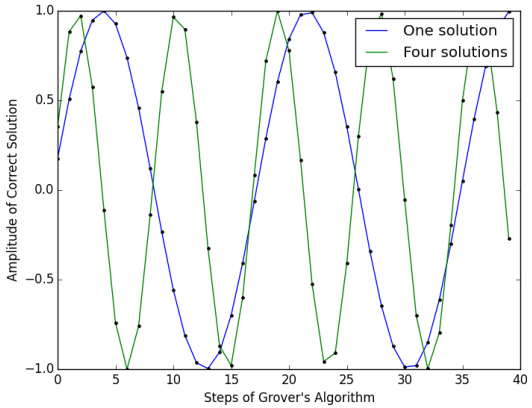
Next step: Use Quantum Fourier Transformation to find the period

After the Fourier transformation



Dimension: N'

Dimension: N

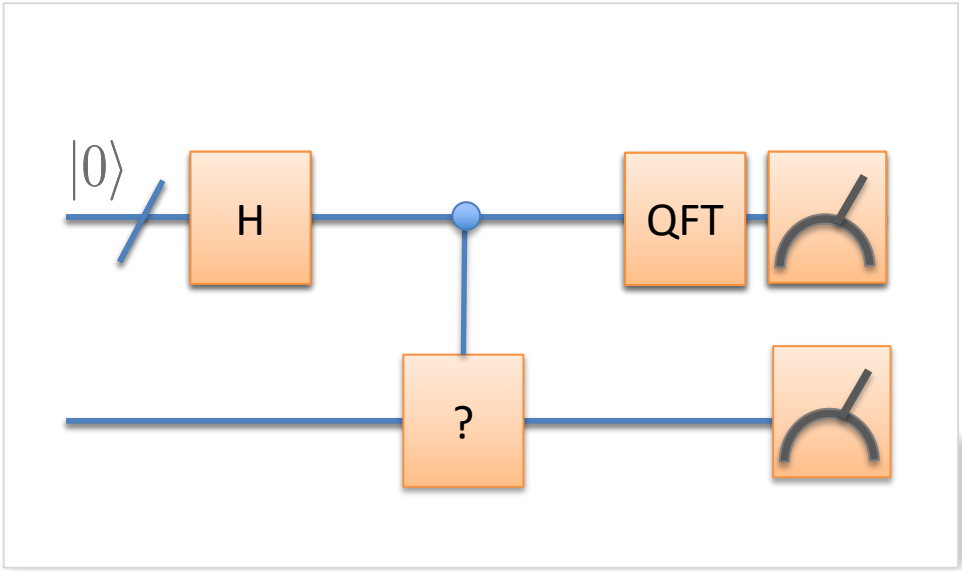


After Fourier transforming a periodic function, we get a good approximation to theta. If we measure value "j":

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

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

Phase Estimation and HSP Problems



The Hadamard and Fourier transform part is a 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