

PHYC90045 Introduction to Quantum Computing

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



1

PHYC90045 Introduction to Quantum Computing

Amplitude Amplification

PHYC90045 Introduction to Quantum Computing
Lecture 10



2

PHYC90045 Introduction to Quantum Computing

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



3

PHYC90045 Introduction to Quantum Computing

Grover's Algorithm (1996)

The University of Melbourne

- 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.

High level structure:

4

PHYC90045 Introduction to Quantum Computing

Some notation

The University of Melbourne

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

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

5

PHYC90045 Introduction to Quantum Computing

Some notation

The University of Melbourne

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

6

PHYC90045 Introduction to Quantum Computing

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**.

Part of Norfolk Island's telephone book, with people listed by nickname (Photo: [Willcommens](#))

7

PHYC90045 Introduction to Quantum Computing

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

8

PHYC90045 Introduction to Quantum Computing

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

9

PHYC90045 Introduction to Quantum Computing

New inversion step

The diagram illustrates a quantum circuit segment. It consists of three rectangular boxes representing quantum gates, arranged horizontally. The first box is labeled U , the second is labeled "Inversion", and the third is labeled U^\dagger . Each gate is flanked by two blue horizontal lines, which represent the qubits passing through the circuit. Below this circuit, the text "Apply general U instead of H" is displayed.

Apply general U instead of H

$$|\phi\rangle = U |\psi\rangle$$

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

10

PHYS90045 Introduction to Quantum Computing

Maths of the Geometric Interpretation

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

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

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

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

$t = |g_0|^2$

11

PHYC90045 Introduction to Quantum Computing



 THE UNIVERSITY OF
 MELBOURNE

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:

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

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

12

PHYC90045 Introduction to Quantum Computing

Grover vs Amplitude Amplification

The diagram illustrates two quantum circuit models side-by-side:

- Grover:** A circuit with four horizontal lines representing qubits. The first three lines pass through three Hadamard (H) gates each. The fourth line passes through four H gates. Between the second and third qubit lines is a large gray rectangle labeled "Inversion".
- Amplitude Amplification:** A circuit with four horizontal lines representing qubits. The first three lines pass through three unitary operations (U) each. The fourth line passes through three inverse unitary operations (U^\dagger). Between the second and third qubit lines is a large gray rectangle labeled "Inversion".

Angle of rotation:

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

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.

13

PHYC90045 Introduction to Quantum Computing

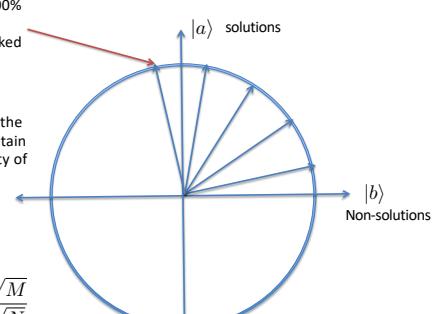


 THE UNIVERSITY OF
 MELBOURNE

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?



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

14

Using amplitude amplification

This step gives 100% probability of finding the marked state

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

15

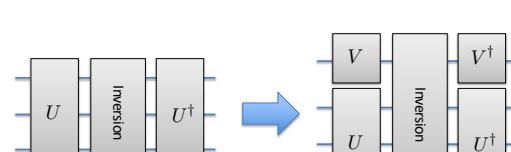
PHYC90045 Introduction to Quantum Computing

THE UNIVERSITY OF
MELBOURNE

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.



The diagram illustrates a quantum circuit transformation. On the left, three horizontal lines represent qubits. The first qubit passes through a gray rectangular box labeled U . The second qubit passes through a gray rectangular box labeled "Inversion". The third qubit passes through a gray rectangular box labeled U^\dagger . A large blue arrow points to the right, indicating the transformation. On the right, the circuit is modified. The first qubit now passes through a gray rectangular box labeled V . The second qubit passes through a gray rectangular box labeled "Inversion". The third qubit passes through a gray rectangular box labeled U^\dagger . This modification effectively reduces the total rotation angle for the second qubit, as it now undergoes an inversion followed by a unitary operation, which together result in a full π rotation.

16

PHYC90045 Introduction to Quantum Computing



 THE UNIVERSITY OF
 MELBOURNE

How much reduction?

Previously:

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

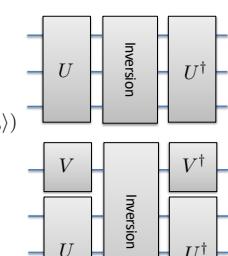
With new qubit:

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

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: $\cos \frac{\alpha}{2} = \frac{g'_0}{g_0}$



17

PHYS90045 Introduction to Quantum Computing



 THE UNIVERSITY OF
 MELBOURNE

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:

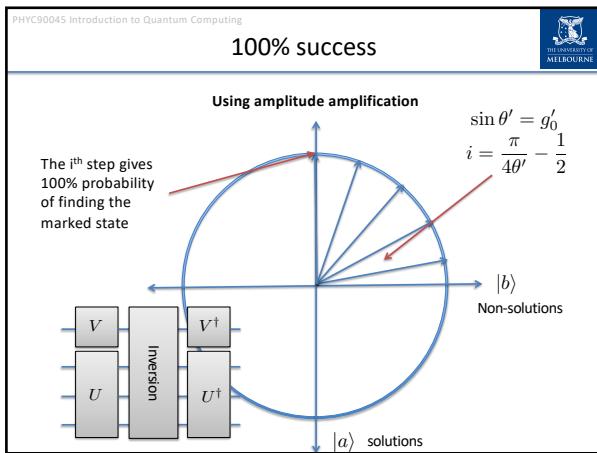
$$V \otimes U |0\rangle = g'_0 |1\rangle |\phi_g\rangle + \dots$$

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

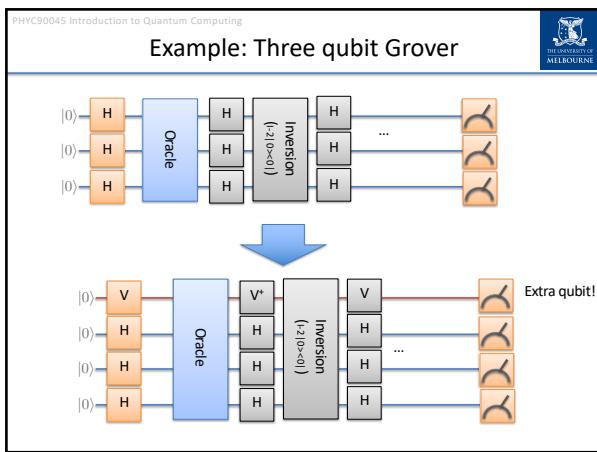
Our new "good" states, but now have a preceding "1" on the extra qubit we added

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

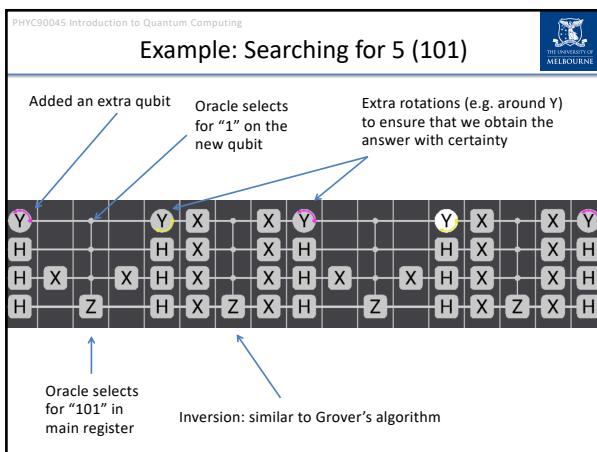
18



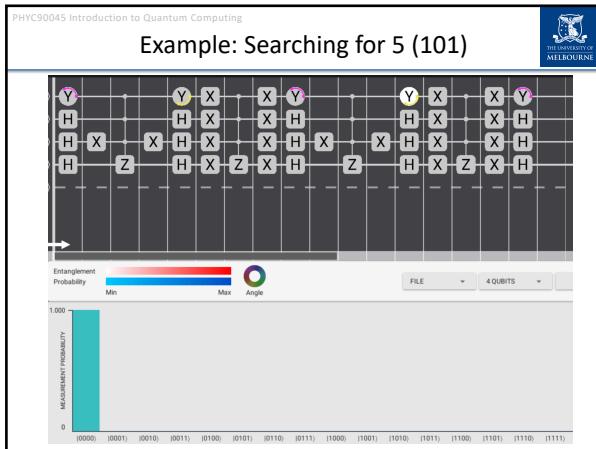
19



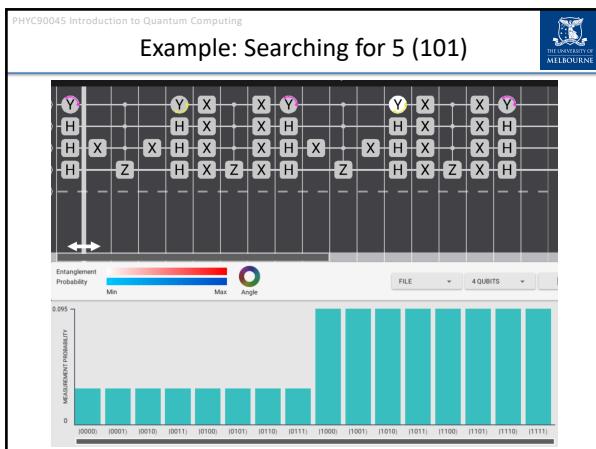
20



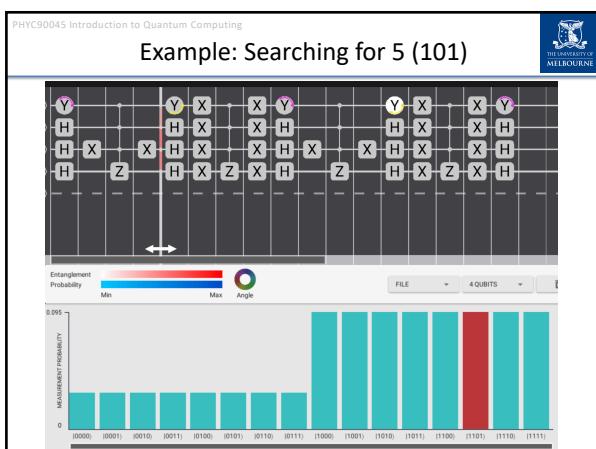
21



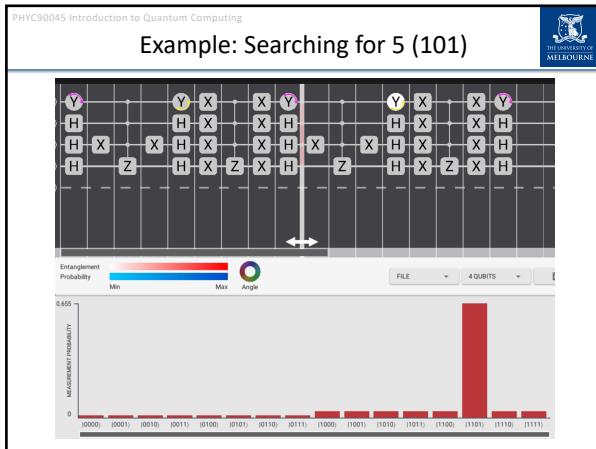
22



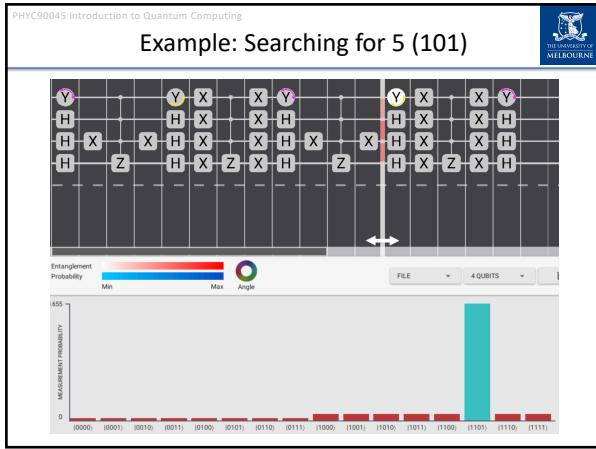
23



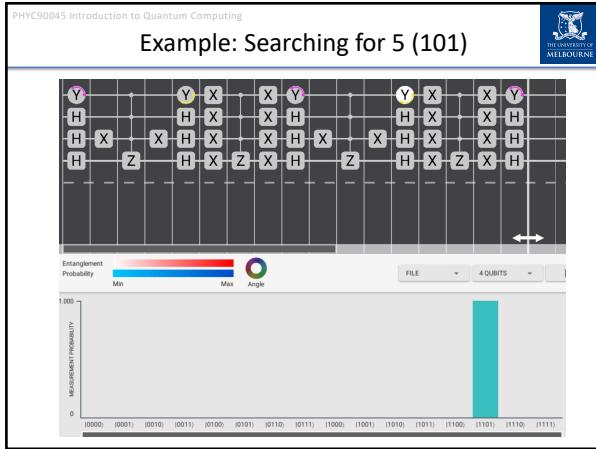
24



25



26



27

PHYC90045 Introduction to Quantum Computing



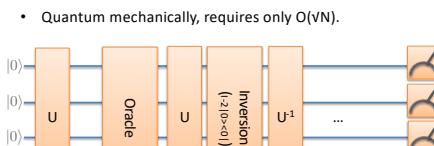
 THE UNIVERSITY OF
 MELBOURNE

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 $O(\sqrt{N})$.



The diagram illustrates a quantum circuit for amplitude amplification. It consists of six horizontal lines representing qubits. The first five qubits are initialized to $|0\rangle$. The circuit is composed of several orange rectangular boxes representing operations:

- A single U gate acts on the first qubit.
- An **Oracle** gate acts on the second qubit.
- A single U gate acts on the third qubit.
- An **Inversion** gate, labeled $(I_{2^k} - |0\rangle\langle 0|)$, acts on the fourth qubit.
- A U^{-1} gate acts on the fifth qubit.
- Ellipses indicate that the sequence continues for the remaining qubits.
- Final measurement symbols are shown at the end of each line, indicating the state of each qubit after the circuit has been run.

28

PHYC90045 Introduction to Quantum Computing


THE UNIVERSITY OF
MELBOURNE

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.

29

PHYC90045 Introduction to Quantum Computing


THE UNIVERSITY OF
MELBOURNE

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. $f(x) = 1$?

30

PHYC90045 Introduction to Quantum Computing

Equivalent question

What angle rotation does Q make?

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

31

PHYC90045 Introduction to Quantum Computing

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

32

PHYC90045 Introduction to Quantum Computing

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)

33

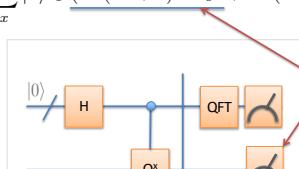
PHYC90045 Introduction to Quantum Computing



 THE UNIVERSITY OF
 MELBOURNE

Finding the period of a periodic function

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



The diagram shows a quantum circuit with two horizontal lines representing qubits. The top qubit starts in state $|0\rangle$ and passes through a Hadamard gate (H). It then enters a box labeled "QFT" (Quantum Fourier Transform). The bottom qubit starts in an unknown state and passes through a box labeled Q^x . Both qubits then enter a second box labeled "QFT". A red arrow points from the text "If we measure the second register" to the second QFT box.

If we measure the second register

34

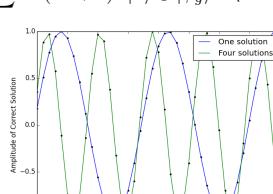
PHYC90045 Introduction to Quantum Computing



 THE UNIVERSITY OF
 MELBOURNE

After measurement of the second register

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



The graph plots the Amplitude of Correct Solution (y-axis, ranging from -1.0 to 1.0) against the Steps of Grover's Algorithm (x-axis, ranging from 0 to 40). Two curves are shown: a blue curve labeled "One solution" and a green curve labeled "Four solutions". The blue curve has a single peak at step 0 with amplitude 1.0. The green curve has four peaks at steps 0, 10, 20, and 30, each with amplitude 1.0. Between these peaks, the amplitude drops to -1.0 at steps 5, 15, 25, and 35 respectively.

Steps of Grover's Algorithm	Amplitude (One solution)	Amplitude (Four solutions)
0	1.0	-0.5
5	0.0	-1.0
10	0.0	1.0
15	0.0	-1.0
20	0.0	1.0
25	0.0	-1.0
30	0.0	1.0
35	0.0	-1.0
40	0.0	0.0

Next step: Use Quantum Fourier Transformation to find the period

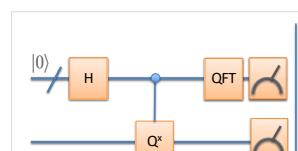
35

PHYC90045 Introduction to Quantum Computing



 THE UNIVERSITY OF
 MELBOURNE

After the Fourier transformation



The diagram illustrates a quantum circuit for preparing a periodic function and performing a Fourier transform. The circuit consists of two horizontal lines representing qubits. The top qubit starts with an initial state $|0\rangle$, followed by a Hadamard gate (H). This is followed by a Quantum Fourier Transform block (QFT) and a meter. The bottom qubit starts with a Quantum Fourier Transform block (QF^\dagger) and ends with a meter. A red arrow points from the text "One solution, Four solutions" to the meter on the bottom qubit.

Dimension: N'

Dimension: N

After Fourier transforming a periodic function, we get a good approximation to the theta. If we measure value “!”:

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

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

36

PHYC90045 Introduction to Quantum Computing

Phase Estimation and HSP Problems

The diagram shows a quantum circuit starting with a qubit in state $|0\rangle$. It passes through a Hadamard gate (**H**), followed by a control point, then a Quantum Fourier Transform gate (**QFT**). The circuit then splits into two parallel paths. The top path contains a phase estimation block, which includes a controlled phase gate (indicated by a box with a curved arrow) and a control point. The bottom path also contains a phase estimation block with a similar controlled phase gate and control point. Both paths converge back onto a single qubit line.

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.

37

PHYC90045 Introduction to Quantum Computing

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

38