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

Amplitude Amplification

PHYC90045 Introduction to Quantum Computing
Lecture 10

2

Amplitude Amplification

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

References:

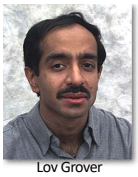
Rieffel, Chapter 9.1-9.2
Kaye, Chapter 8.1-8.2
Nielsen and Chuang, Chapter 6.1-6.2

3

PHYC90045 Introduction to Quantum Computing

Grover's Algorithm (1996)

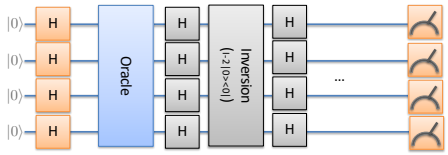
- Unordered search, find one marked item among many
- Classically, this requires N/2 queries to the oracle
- Quantum mechanically, requires only O(√N) queries.



Lov Grover

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

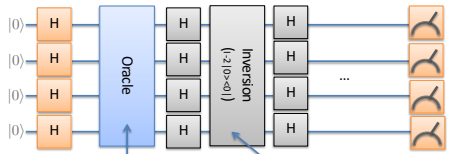
High level structure:



4

PHYC90045 Introduction to Quantum Computing

Some notation

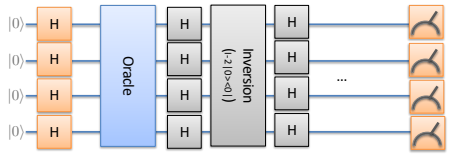


$S_G = I - 2\,|m\rangle\,\langle m|$ $S_0 = I - 2\,|0\rangle\,\langle 0|$

5

PHYC90045 Introduction to Quantum Computing

Some notation



Q

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

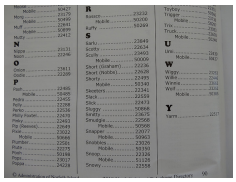
Oracles for NP-problems

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**.



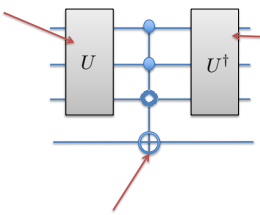
Part of Norfolk Island's telephone book, with people listed by nickname (Photo: Wikicommons)

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.

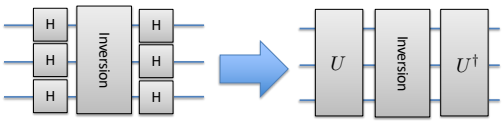
The oracle recognises the 'correct' solution, but does not know in advance which input leads to the correct solution

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?



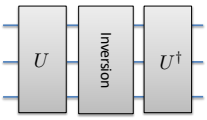
Inversion about the mean

Apply general U instead of H

9

PHYC90045 Introduction to Quantum Computing

New inversion step



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

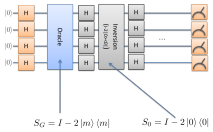
Bad: Not in the subspace spanned by all solutions

10

PHYC90045 Introduction to Quantum Computing

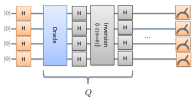
Maths of the Geometric Interpretation

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



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

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



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

$t = |g_0|^2$

11

PHYC90045 Introduction to Quantum Computing

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:

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

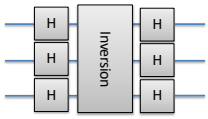
$\sin\theta = \sqrt{t} = g_0$

12

PHYC90045 Introduction to Quantum Computing

Grover vs Amplitude Amplification

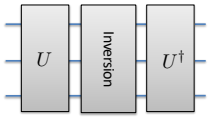
Grover



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.

13

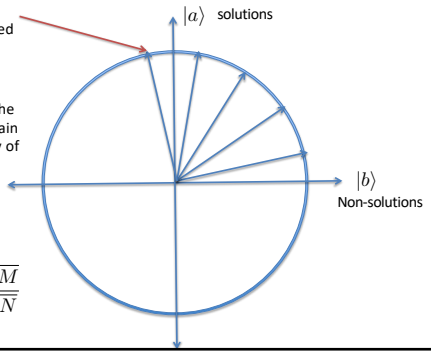
PHYC90045 Introduction to Quantum Computing

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

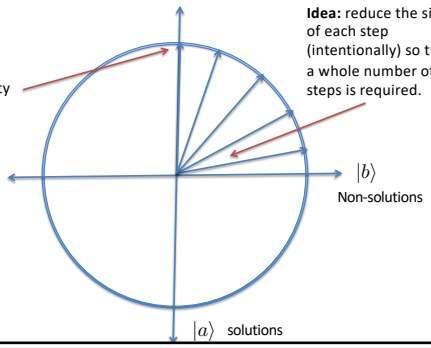
PHYC90045 Introduction to Quantum Computing

Grover with 100% success

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.



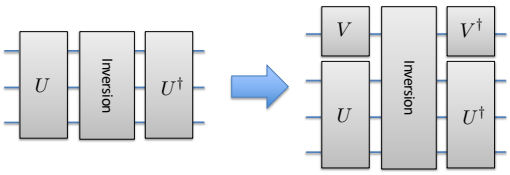
15

PHYC90045 Introduction to Quantum Computing

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.



16

PHYC90045 Introduction to Quantum Computing

How much reduction?

Previously:

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

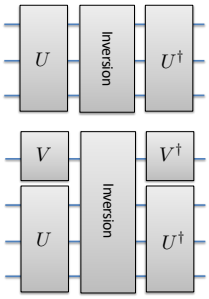
With new qubit:

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

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



17

PHYC90045 Introduction to Quantum Computing

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:

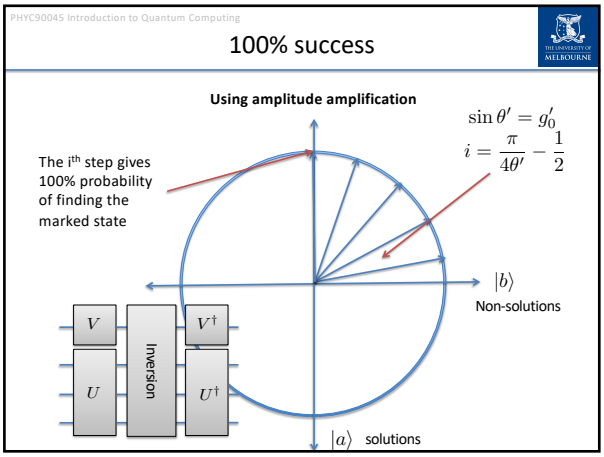
$$V \otimes U|0\rangle = g_0'|1\rangle|\phi_g\rangle + \ldots$$

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

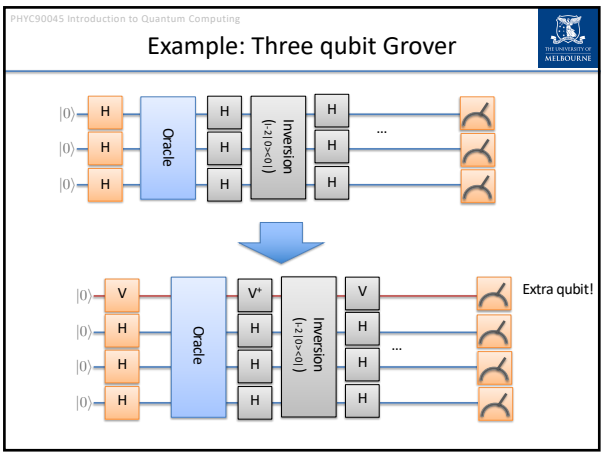
Our new "good" states, but now have a preceding "1" on the extra qubit we added

Choose g_0' s.t. $i = \frac{\pi}{4\theta'} - \frac{1}{2}$ is a whole number

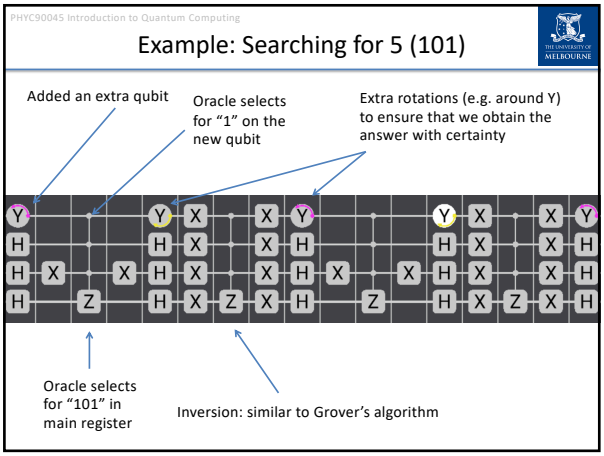
18


PHYC90045 Introduction to Quantum Computing
100% success
Using amplitude amplification
The i^th step gives 100% probability of finding the marked state
$\sin\theta' = g_0'$
$i = \frac{\pi}{4\theta'} - \frac{1}{2}$
$|b\rangle$
Non-solutions
$|a\rangle$ solutions
V
U
Inversion
$V^\dagger$
$U^\dagger$

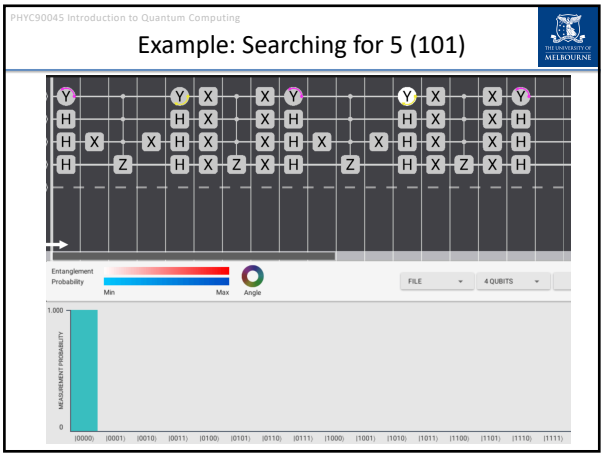
19


PHYC90045 Introduction to Quantum Computing
Example: Three qubit Grover
|0⟩
H
Oracle
Inversion (|+⟩⟨+| - |0⟩⟨0|)
...
V
V+
Extra qubit!

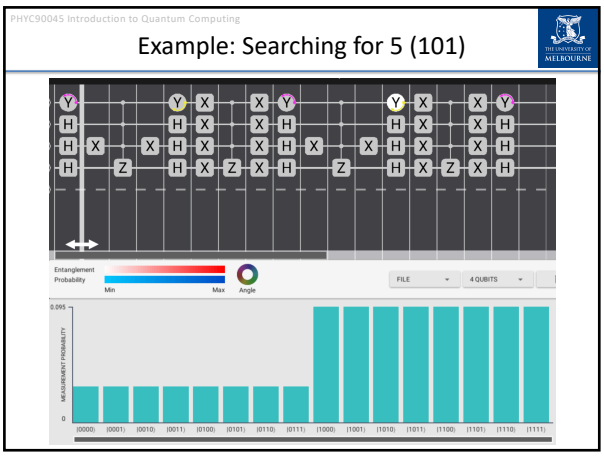
20


PHYC90045 Introduction to Quantum Computing
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

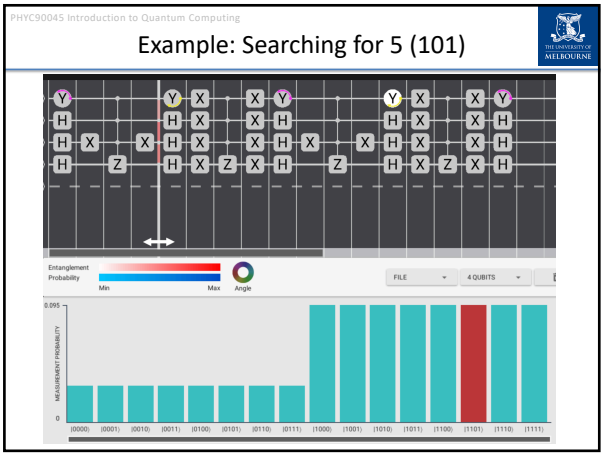
21


PHYC90045 Introduction to Quantum Computing
Example: Searching for 5 (101)
THE UNIVERSITY OF MELBOURNE
Entanglement Probability
Min
Max
Angle
FILE
4 QUBITS
MEASUREMENT PROBABILITY
1.000
0
|0000⟩ |0001⟩ |0010⟩ |0011⟩ |0100⟩ |0101⟩ |0110⟩ |0111⟩ |1000⟩ |1001⟩ |1010⟩ |1011⟩ |1100⟩ |1101⟩ |1110⟩ |1111⟩

22


PHYC90045 Introduction to Quantum Computing
Example: Searching for 5 (101)
THE UNIVERSITY OF MELBOURNE
Entanglement Probability
Min
Max
Angle
FILE
4 QUBITS
MEASUREMENT PROBABILITY
0.095
0
|0000⟩ |0001⟩ |0010⟩ |0011⟩ |0100⟩ |0101⟩ |0110⟩ |0111⟩ |1000⟩ |1001⟩ |1010⟩ |1011⟩ |1100⟩ |1101⟩ |1110⟩ |1111⟩

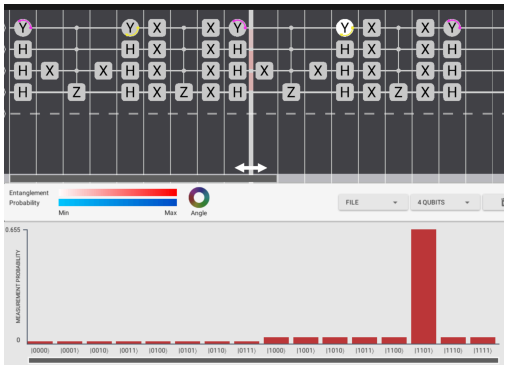
23


PHYC90045 Introduction to Quantum Computing
Example: Searching for 5 (101)
THE UNIVERSITY OF MELBOURNE
Entanglement Probability
Min
Max
Angle
FILE
4 QUBITS
MEASUREMENT PROBABILITY
0.095
0
|0000⟩ |0001⟩ |0010⟩ |0011⟩ |0100⟩ |0101⟩ |0110⟩ |0111⟩ |1000⟩ |1001⟩ |1010⟩ |1011⟩ |1100⟩ |1101⟩ |1110⟩ |1111⟩

24

PHYC90045 Introduction to Quantum Computing

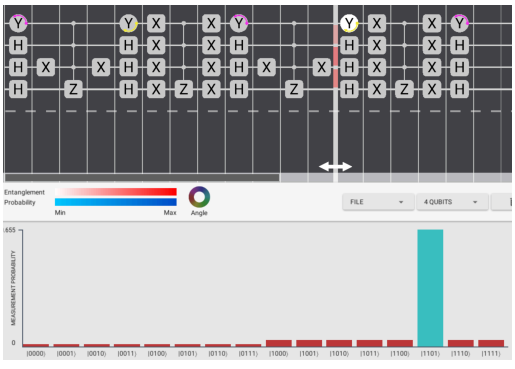
Example: Searching for 5 (101)



25

PHYC90045 Introduction to Quantum Computing

Example: Searching for 5 (101)



26

PHYC90045 Introduction to Quantum Computing

Example: Searching for 5 (101)

27

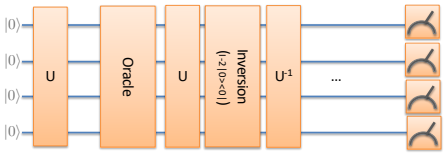
PHYC90045 Introduction to Quantum Computing

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).



28

PHYC90045 Introduction to Quantum Computing

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

Quantum Counting

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

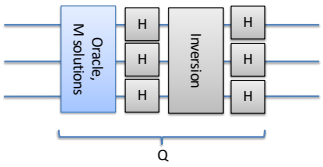
Given an black box (oracle), U_f, which computes the function $f:\{0,1\}^n \rightarrow \{0,1\}$

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

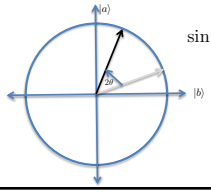
30

PHYC90045 Introduction to Quantum Computing

Equivalent question



What angle rotation does Q make?



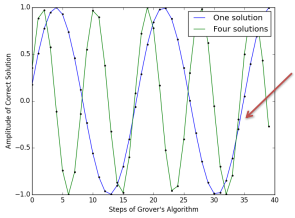
$$\sin\theta = \frac{\sqrt{M}}{\sqrt{N}}$$

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

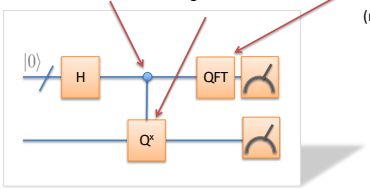
Finding the period of a periodic function

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

Control register, x

x steps of Grover's algorithm

Quantum Fourier Transform (next week)

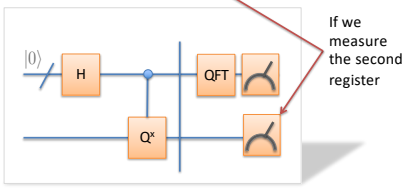


33

PHYC90045 Introduction to Quantum Computing

Finding the period of a periodic function

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



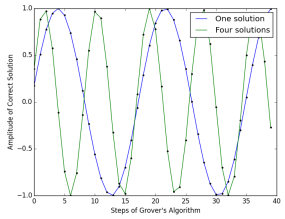
If we measure the second register

34

PHYC90045 Introduction to Quantum Computing

After measurement of the second register

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

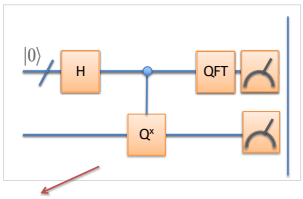


Next step: Use Quantum Fourier Transformation to find the period

35

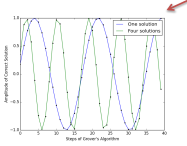
PHYC90045 Introduction to Quantum Computing

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":

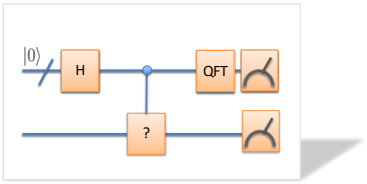
$$\theta = \frac{j\pi}{N'} \qquad \sin\theta = \frac{\sqrt{M}}{\sqrt{N}}$$

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

36

PHYC90045 Introduction to Quantum Computing

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.

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