PHYC90045 Introduction to Quantum Computing

This Week

Lecture 1
Quantum search – introduction to Grover's algorithm for amplitude amplification, geometric interpretation

Lecture 2
Optimality, Succeeding with Certainty, Quantum Counting

Lab
Grover's algorithm

PHYC90045 Introduction to Quantum Computing

Grover's Algorithm

Physics 90045
Lecture 7

PHYC90045 Introduction to Quantum Computing

Introduction to Grover's algorithm

- This lecture: Grover's search algorithm
  - Grover's algorithm
  - Worked Example
  - Geometric interpretation

References:

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

Reminder: Outer Product

For two quantum states $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, \ |\phi\rangle = \begin{bmatrix} c \\ d \end{bmatrix}$

We can define an outer product between them:

$$|\psi\rangle\langle\phi| = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c^* & d^* \end{bmatrix}$$

$$= \begin{bmatrix} ac^* & ad^* \\ bc^* & bd^* \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$|1\rangle\langle 2|$

For number basis states, this specifies a matrix with a single "1" in the location 1,2. In general:

$|\mathrm{row}\rangle\langle\mathrm{column}|$

Unordered Search

Grover's algorithm performs a similar* problem to this: You are given *a telephone book*

And a phone number: *23675*

Your task:
Find the name which goes with that number…

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

* Not all that similar, better examples later….

Quantum search – Grover's problem

Given an black box (oracle), U_f, which computes the function:

$$f: \{0,1\}^n \rightarrow \{0,1\}$$

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

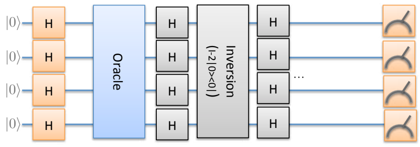
Grover's Algorithm (1996)

- 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

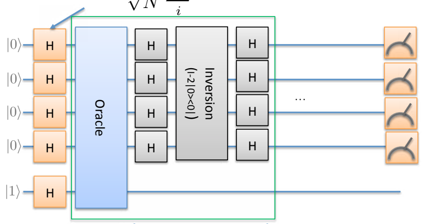
Simple problem = search for one integer marked by the oracle.

High level structure:



Two basic steps in Grover's algorithm

Quantum database: $|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_i |i\rangle$ (i.e. all integers 0 to N-1)



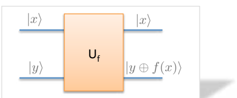
The "oracle" Identifies a particular marked state, m

$I - 2\,|\Phi\rangle\langle\Phi|$ "Inversion about the mean"

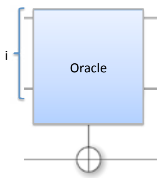
Repeat these two operations O(√N) times

The Oracle

The task of recognizing the correct solution goes to the "oracle".



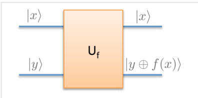
Binary function, or "oracle" Identifying a marked state, m



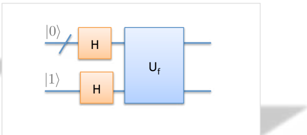
Designed to flip the last bit if the input, i, is a solution

The oracle is just a Boolean function (as seen in previous lectures)

Phase kickback for Boolean function



Binary function, or "oracle"



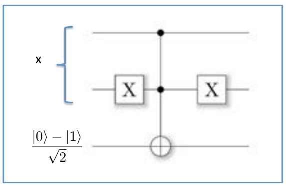
After the function has been applied:

Target qubit remains the same

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

If the oracle function evaluates to "1" then the target qubit is flipped, and we pick up a phase (associated with the control qubit state). Otherwise, there is no phase applied. This is a simple way to write that.

Example: Oracle recognizing the state "2 = |10>"



<u>Phase kickback</u>

$$\begin{aligned} |00\rangle &\rightarrow \ \ |00\rangle \\ |01\rangle &\rightarrow \ \ |01\rangle \\ |10\rangle &\rightarrow -|10\rangle \\ |11\rangle &\rightarrow \ \ |11\rangle \end{aligned}$$

The effect on each of the 4 states in the 2-qubit control register, x:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I - 2|10\rangle\langle 10|$$

The marked state

Initially in Grover's algorithm, we will be searching for a *single (integer) solution*, ***m***. In that case the effect of the oracle on the control register is:

$$I - 2|m\rangle\langle m|$$ (in decimal ket notation)

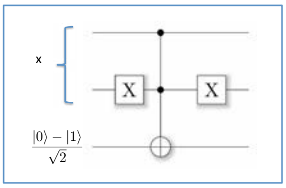
As a matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

-1 in the m^{th} position

Here, as in future slides, we are only writing out the control qubits (in this case 2 qubits only).

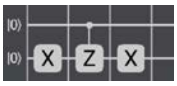
Example: Oracle recognizing the state "2 = |10>"



Phase kickback

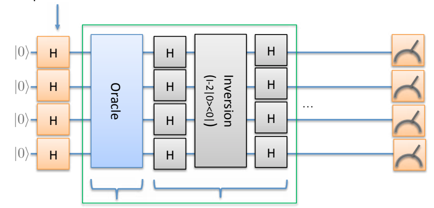
$$|00\rangle \to \quad |00\rangle$$
$$|01\rangle \to \quad |01\rangle$$
$$|10\rangle \to -|10\rangle$$
$$|11\rangle \to \quad |11\rangle$$

In practice we can implement the oracle without the check qubit using a controlled-Z gate (ex. Show the circuit right marks the state |10>, i.e. |m=2>).



Two steps to Grover's algorithm

Set up "data base"



$I - 2|m\rangle\langle m|$ $\quad$ $I - 2|\Phi\rangle\langle\Phi|$

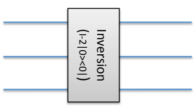
The oracle $\quad$ "Inversion about the mean"

Repeat these two operations O(√N) times

One iteration of Grover where $|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_i |i\rangle$

Unpicking the details: "Inversion" operation

The "Inversion" part is just applying a phase to the zero state:



$$I - 2|0\rangle\langle 0| = \begin{bmatrix} -1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

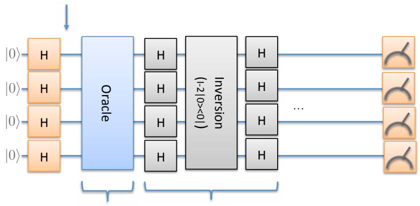
How? Recall outer product etc: $|\psi\rangle\langle\phi| = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c^* & d^* \end{bmatrix} = \begin{bmatrix} ac^* & ad^* \\ bc^* & bd^* \end{bmatrix}$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \otimes (10\dots0) = \begin{pmatrix} 10\dots0 \\ 00\dots0 \\ \vdots \end{pmatrix} \qquad I = \begin{pmatrix} 100\dots0 \\ 010\dots0 \\ 001\dots0 \\ \vdots \end{pmatrix}$$

$$I - 2|0\rangle\langle 0| = \begin{pmatrix} 100\dots0 \\ 010\dots0 \\ 001\dots0 \\ \vdots \end{pmatrix} - 2\begin{pmatrix} 10\dots0 \\ 00\dots0 \\ \vdots \end{pmatrix} = \begin{bmatrix} -1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

Inversion about the mean

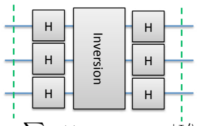
$$|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_i |i\rangle$$ Set up "data base"



$$I - 2|\Phi\rangle\langle\Phi|$$

"Inversion about the mean"…let's see how that works.

Apply inversion about the mean to general state



$$|\Psi\rangle = \sum_i a_i |i\rangle \qquad |\Psi'\rangle$$

Applying Hadamards both sides:

$$I - 2H^{\otimes n}|0\rangle\langle 0| H^{\otimes n}$$
$$= I - 2|\Phi\rangle\langle\Phi|$$

$$|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_i |i\rangle$$

Equal superposition

$$|\Psi\rangle = \sum_i a_i|i\rangle \rightarrow |\Psi'\rangle = (I - 2|\Phi\rangle\langle\Phi|)\sum_i a_i|i\rangle$$
$$= \sum_i a_i|i\rangle - 2\frac{1}{\sqrt{N}}\sum_k |k\rangle \frac{1}{\sqrt{N}}\sum_j \langle j| \sum_i a_i|i\rangle$$
$$= \sum_i a_i|i\rangle - 2\sum_k |k\rangle\left(\frac{1}{N}\sum_j a_j\right)$$
$$= \sum_i (a_i - 2A)|i\rangle$$

General state

$$A \equiv \left(\frac{1}{N}\sum_j a_j\right)$$

Average amplitude in state $|\Psi\rangle$

Inversion about the mean

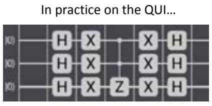
Consider a general state. The resulting amplitude from the "Inversion about the mean" step is:

$$\sum_i a_i|i\rangle \rightarrow \sum_i (a_i - 2A)|i\rangle$$

Original amplitude

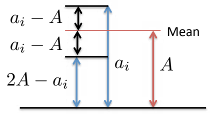
Average amplitude

In practice on the QUI…



Inversion about the mean

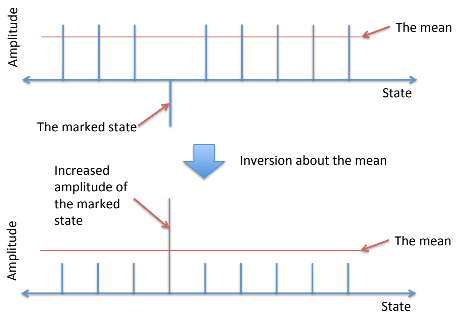
Amplitudes of the state, before and after:



When the state undergoes this transformation:

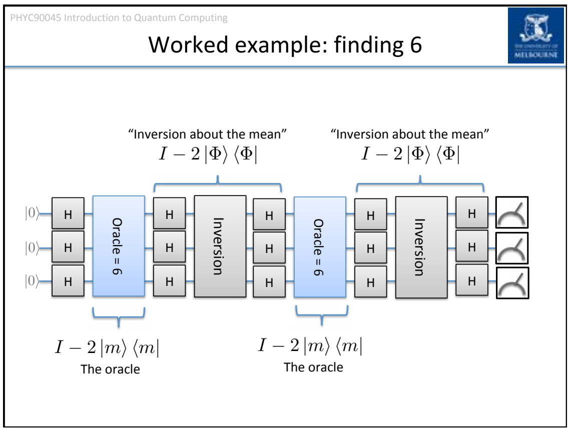
$$\sum_i a_i |i\rangle \rightarrow -\sum_i (2A - a_i)\,|i\rangle$$

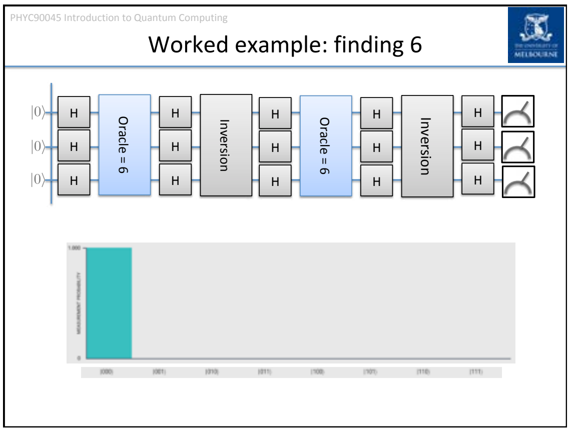
Effect of inversion about the mean

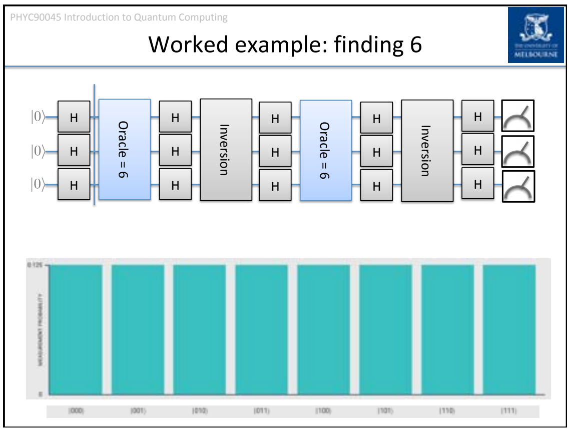


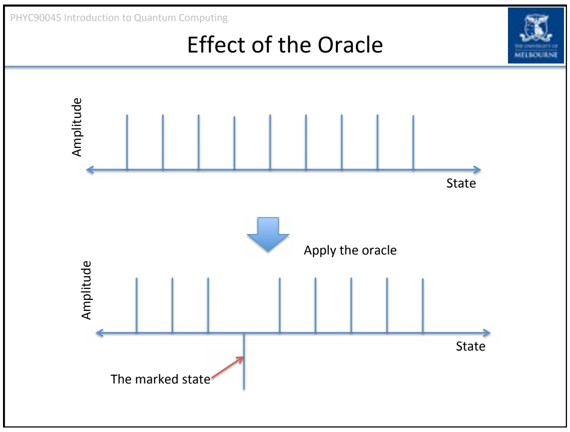
Interactive Example

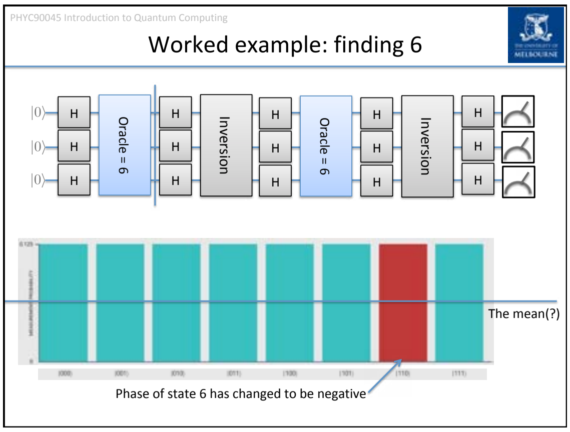
https://codepen.io/samtonetto/full/BVOGmW

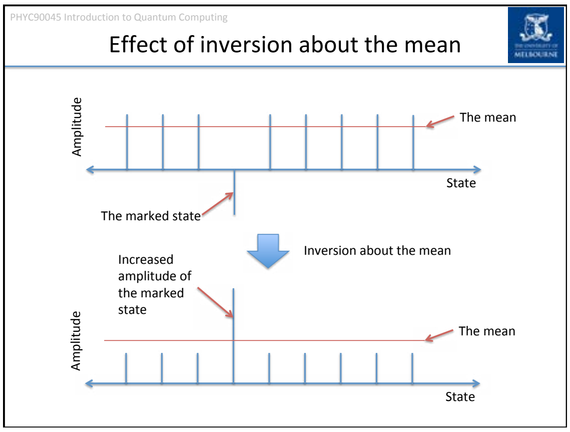

PHYC90045 Introduction to Quantum Computing
Worked example: finding 6
"Inversion about the mean"
$I - 2|\Phi\rangle\langle\Phi|$
"Inversion about the mean"
$I - 2|\Phi\rangle\langle\Phi|$
$|0\rangle$
$|0\rangle$
$|0\rangle$
H
Oracle = 6
Inversion
$I - 2|m\rangle\langle m|$
The oracle
$I - 2|m\rangle\langle m|$
The oracle

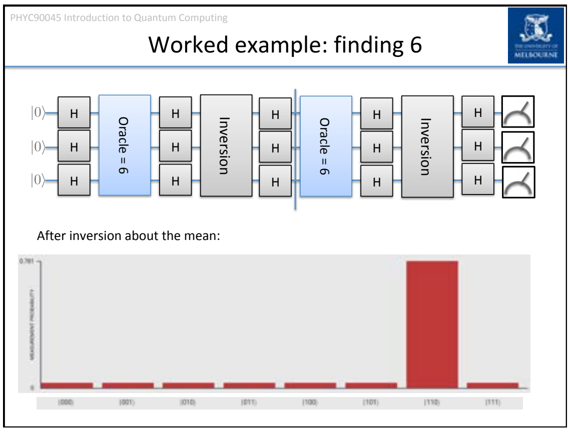

PHYC90045 Introduction to Quantum Computing
Worked example: finding 6
$|0\rangle$
$|0\rangle$
$|0\rangle$
H
Oracle = 6
Inversion

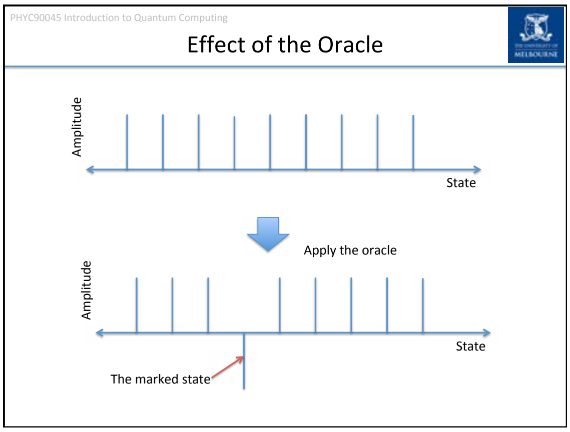

PHYC90045 Introduction to Quantum Computing
Worked example: finding 6
$|0\rangle$
$|0\rangle$
$|0\rangle$
H
Oracle = 6
Inversion


PHYC90045 Introduction to Quantum Computing
Effect of the Oracle
Amplitude
State
Apply the oracle
Amplitude
State
The marked state


PHYC90045 Introduction to Quantum Computing
Worked example: finding 6
|0⟩
|0⟩
|0⟩
H
Oracle = 6
Inversion
Oracle = 6
Inversion
The mean(?)
Phase of state 6 has changed to be negative


PHYC90045 Introduction to Quantum Computing
Effect of inversion about the mean
Amplitude
The mean
State
The marked state
Inversion about the mean
Increased amplitude of the marked state
Amplitude
The mean
State

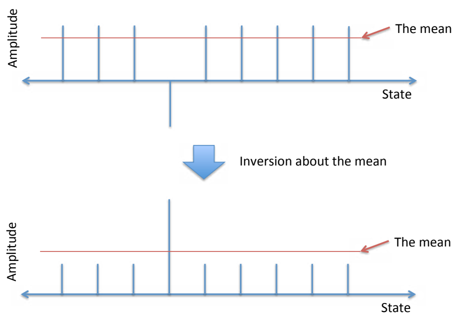

PHYC90045 Introduction to Quantum Computing
Worked example: finding 6
|0⟩
|0⟩
|0⟩
H
Oracle = 6
Inversion
After inversion about the mean:


PHYC90045 Introduction to Quantum Computing
Effect of the Oracle
Amplitude
State
Apply the oracle
Amplitude
State
The marked state


PHYC90045 Introduction to Quantum Computing
Worked example: finding 6
|0⟩
|0⟩
|0⟩
H
Oracle = 6
Inversion
After the second oracle:

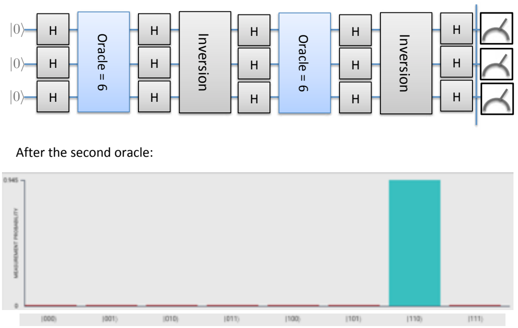
PHYC90045 Introduction to Quantum Computing

Effect of inversion about the mean



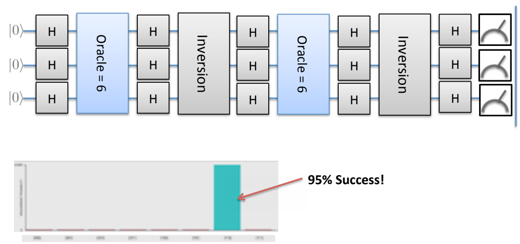
PHYC90045 Introduction to Quantum Computing

Worked example: finding 6



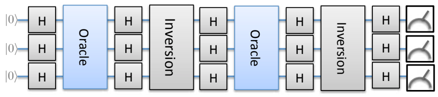
PHYC90045 Introduction to Quantum Computing

Grover's algorithm



Finally, we measure the marked state after 2 applications of the oracle, and find the marked state, 6 with 95% probability

Geometric interpretation of Grover's algorithm



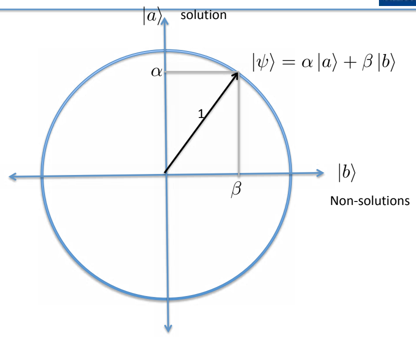
A very useful basis:

$$|a\rangle = |m\rangle$$ Solution!

$$|b\rangle = \frac{1}{\sqrt{N-1}} \sum_{i \notin \text{solutions}} |i\rangle$$ Non-solutions...

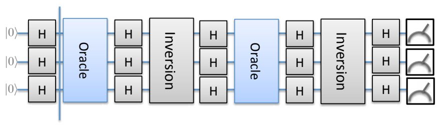
We only need to consider the amplitude of these two states in Grover's algorithm.
Every operation is also real, so we can plot on a circle.

Geometric Interpretation



Every state in Grover's algorithm can be expressed as a superposition of these vectors

Equal superposition



Equal superposition state:

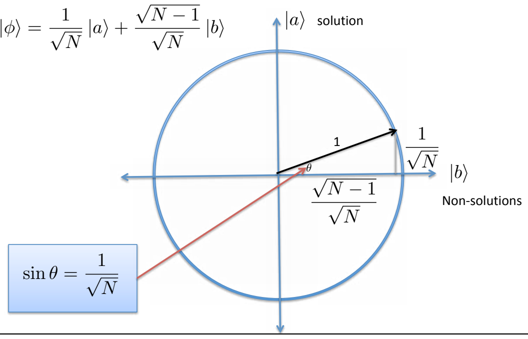
$$|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_i |i\rangle$$
$$= \frac{1}{\sqrt{N}} |a\rangle + \frac{\sqrt{N-1}}{\sqrt{N}} |b\rangle$$

$$|a\rangle = |m\rangle \qquad |b\rangle = \frac{1}{\sqrt{N-1}} \sum_{i \notin \text{solutions}} |i\rangle$$

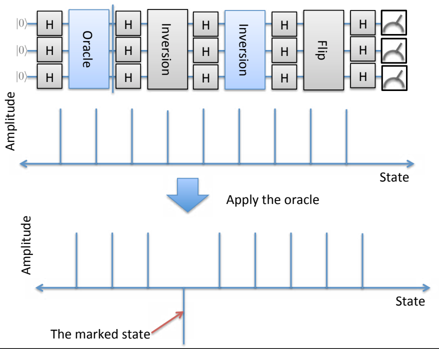
Equal Superposition

Consider the equal superposition:

$$|\phi\rangle = \frac{1}{\sqrt{N}}|a\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|b\rangle$$

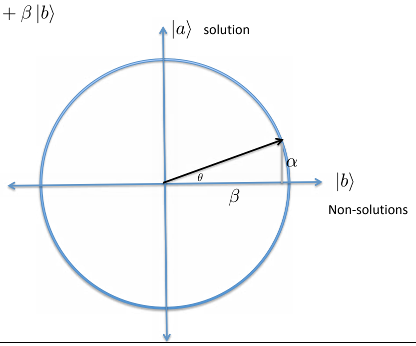


Effect of the Oracle



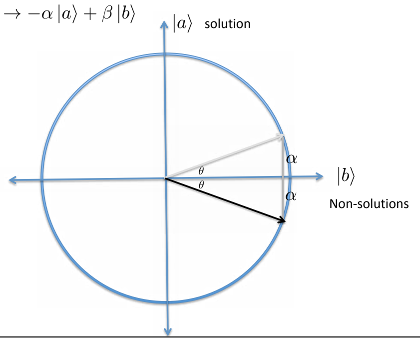
Geometric Effect of Oracle

$\alpha|a\rangle + \beta|b\rangle$

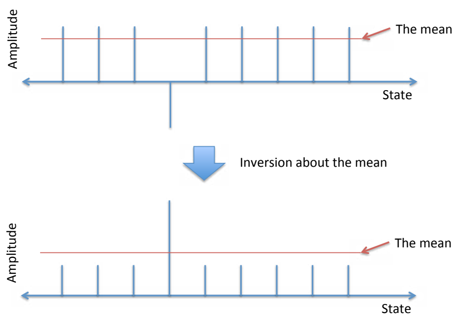


Geometric Effect of Oracle

$$\alpha\,|a\rangle + \beta\,|b\rangle \to -\alpha\,|a\rangle + \beta\,|b\rangle$$

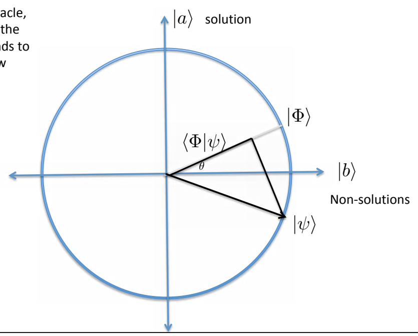


Effect of inversion about the mean



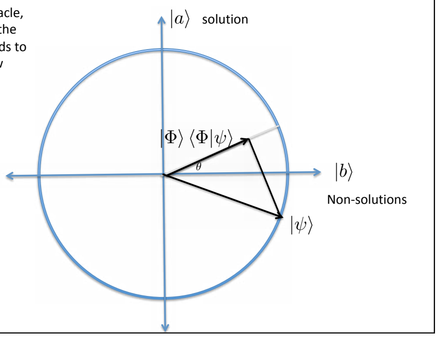
Inversion about the mean

Similar to the oracle, inversion about the mean corresponds to a reflection. Now about **equal superposition**.



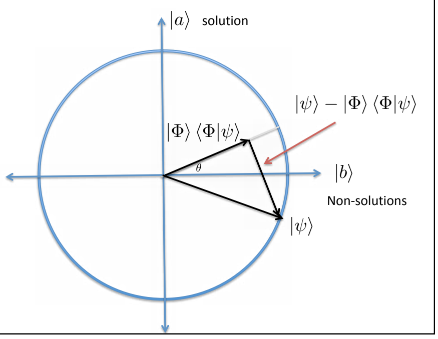
Inversion about the mean

Similar to the oracle, inversion about the mean corresponds to a reflection. Now about **equal superposition**.



PHYC90045 Introduction to Quantum Computing

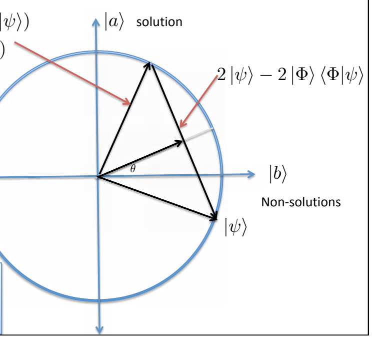
Inversion about the mean



PHYC90045 Introduction to Quantum Computing

Inversion about the mean

$$|\psi\rangle - (2|\psi\rangle - 2|\Phi\rangle\langle\Phi|\psi\rangle)$$
$$= -(|\psi\rangle - 2|\Phi\rangle\langle\Phi|\psi\rangle)$$

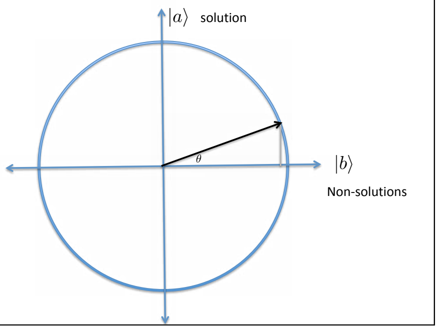


Reflection about the mean reflects around the equal superposition state

PHYC90045 Introduction to Quantum Computing

Geometric Effect of both Oracle and Inversion

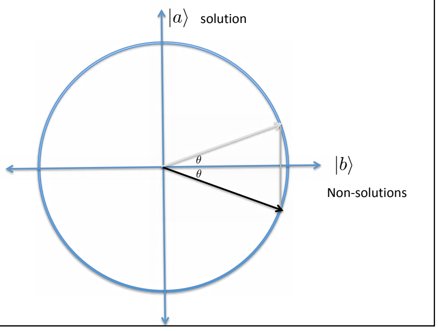
Combining both effects:



PHYC90045 Introduction to Quantum Computing

Geometric Effect of both Oracle and Inversion

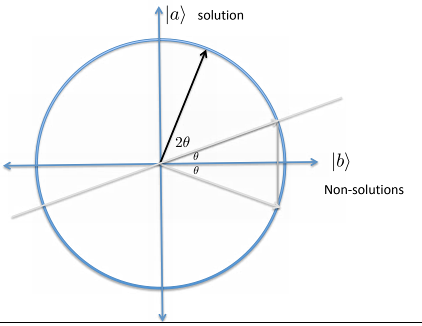
Combining both effects:



PHYC90045 Introduction to Quantum Computing

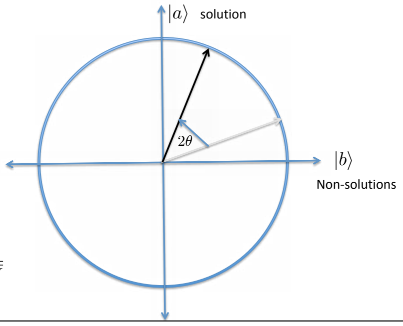
Geometric Effect of both Oracle and Inversion

Combining both effects:



Total effect of one Grover iteration

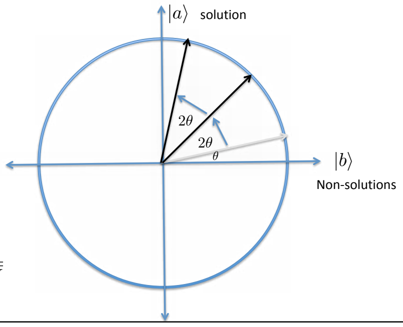
Product of two reflections is a rotation.



$$\sin\theta = \frac{1}{\sqrt{N}}$$

Many Grover iterations

Product of two reflections is a rotation.



$$\sin\theta = \frac{1}{\sqrt{N}}$$

How many iterations required?

$$\sin\theta = \frac{1}{\sqrt{N}}$$

For small angles,

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

After n iterations, we rotate to have only marked solutions:

$$(2n+1)\theta = \frac{\pi}{2}$$

$$n \approx \frac{\pi}{4}\sqrt{N}$$

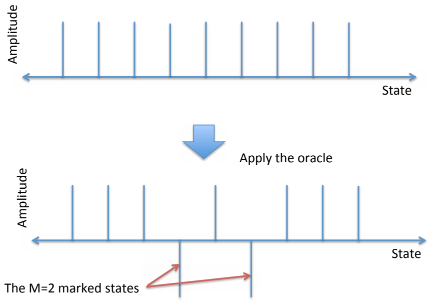
The number of steps, *n*, required scales as O(√N), and not with N as it would classically.

This is a "polynomial" rather than an "exponential" speedup.

PHYC90045 Introduction to Quantum Computing

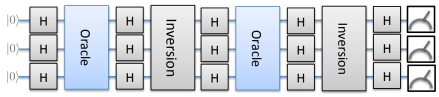
Multiple Solutions

There can be more than one solution to a problem.



PHYC90045 Introduction to Quantum Computing

Geometric interpretation of Grover's algorithm



A very useful basis:

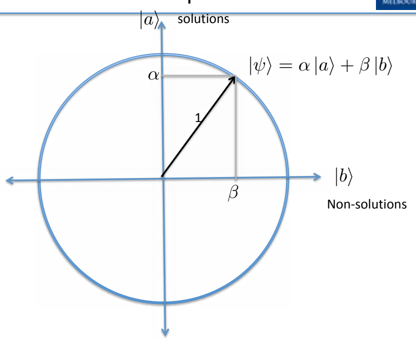
$$|a\rangle = \frac{1}{\sqrt{M}} \sum_{i \in \text{solutions}} |i\rangle$$ Solutions!

$$|b\rangle = \frac{1}{\sqrt{N-M}} \sum_{i \notin \text{solutions}} |i\rangle$$ Non-solutions...

We only need to consider the amplitude of these two states in Grover's algorithm. Every operation is also real, so we can plot on a circle.

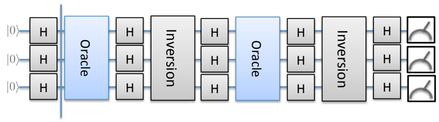
PHYC90045 Introduction to Quantum Computing

Geometric Interpretation



Every state in Grover's algorithm can be expressed as a superposition of these vectors

Equal superposition



Equal superposition state:

$$|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_i |i\rangle$$

$$|\Phi\rangle = \frac{\sqrt{M}}{\sqrt{N}}|a\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|b\rangle$$

$$|a\rangle = \frac{1}{\sqrt{M}}\sum_{i\in\text{solutions}}|i\rangle$$

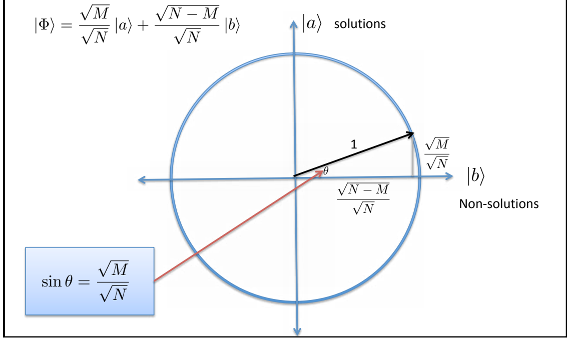
$$|b\rangle = \frac{1}{\sqrt{N-M}}\sum_{i\notin\text{solutions}}|i\rangle$$

PHYC90045 Introduction to Quantum Computing

Equal Superposition

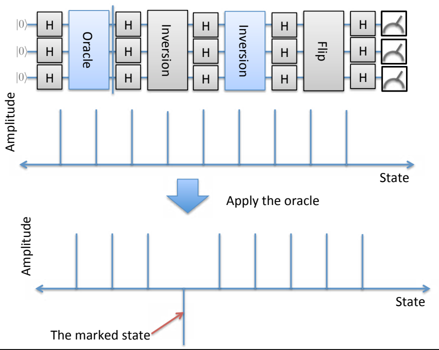
Consider the equal superposition:

$$|\Phi\rangle = \frac{\sqrt{M}}{\sqrt{N}}|a\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|b\rangle$$



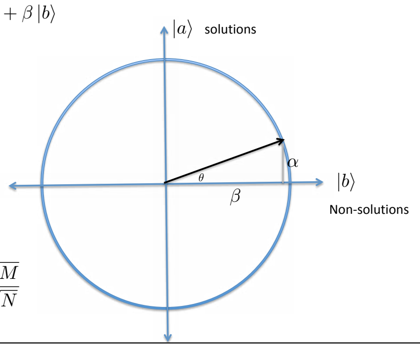
PHYC90045 Introduction to Quantum Computing

Effect of the Oracle



Geometric Effect of Oracle

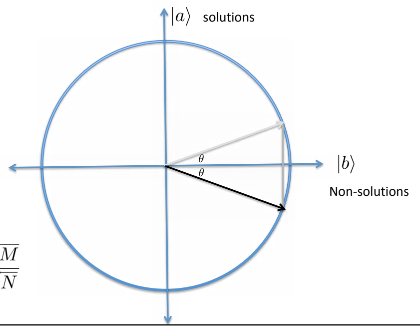
$\alpha\,|a\rangle + \beta\,|b\rangle$



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

Geometric Effect of both Oracle and Inversion

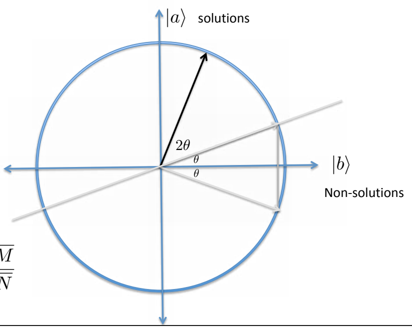
Combining both effects:



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

Geometric Effect of both Oracle and Inversion

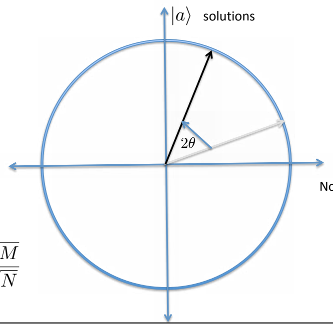
Combining both effects:



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

Total effect of one Grover iteration

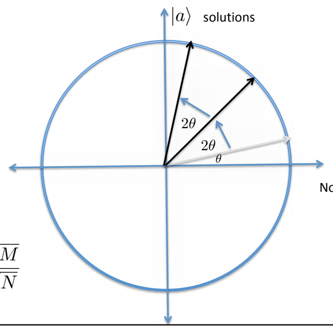
Product of two reflections is a rotation.



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

Many Grover iterations

Product of two reflections is a rotation.



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

How many iterations required?

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

For small angles,

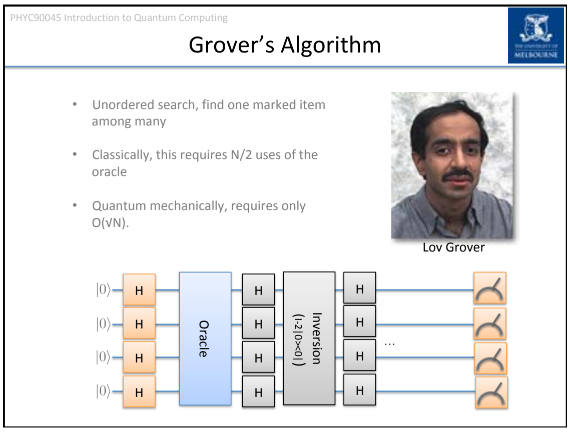
$$\theta \approx \frac{\sqrt{M}}{\sqrt{N}}$$

After n iterations, we rotate to have only marked solutions:

$$(2n+1)\theta = \frac{\pi}{2}$$

$$n \approx \frac{\pi\sqrt{N}}{4\sqrt{M}}$$

Having multiple solutions is faster than searching for a single marked solution.


PHYC90045 Introduction to Quantum Computing
Grover's Algorithm
Unordered search, find one marked item among many
Classically, this requires N/2 uses of the oracle
Quantum mechanically, requires only O(√N).
Lov Grover
|0⟩
H
Oracle
Inversion (I-2|0⟩⟨0|)
…