Welcome to PHYC90045

Introduction to Quantum Computing

School of Physics, University of Melbourne

Lecturers: Prof. Lloyd Hollenberg, Dr. Charles Hill

PHYC90045 Intro to Quantum Computing

In this subject you will:

- understand the basic elements of quantum computing
- understand quantum logic operations and basic quantum algorithms
- understand how to use the Quantum User Interface (QUI)
- learn about more complex quantum algorithms and applications
- learn how to program quantum computers

Focus is on the logic structure of quantum information processing, i.e. little or no physics…but do brush up on complex numbers and basic linear algebra…

Subject at a glance

Overview:

24 Lectures: Monday 2:15pm, Wednesday 9am
(Opat Seminar Room, 6th floor Physics – David Caro Building)

12 Computer-based Labs: Friday 2:15-5:15pm (G14 Computer Lab, Law Building)
Assessment: 2 projects (80%), 1 hour exam (20%)

Structure:

First half – weeks 1-6: From basics to programming (lectures and labs)
Second half – weeks 7-12: Advanced topics (lectures), projects (labs)

Lecturers: Prof. Lloyd Hollenberg (lloydch@unimelb.edu.au),
Dr. Charles Hill (cdhill@unimelb.edu.au)

LMS: Access lecture notes, bring print-out of lab notes to lab sessions

Suggested reading:

E. Rieffel – "Quantum Computing: A Gentle Introduction"
P. Kaye – "An Introduction to Quantum Computing"
M. Nielsen & I. Chuang – "Quantum Computation and Quantum Information"

PHYC90045 Introduction to Quantum Computing

Week 1

Lecture 1

1.1 Non-technical overview of the quantum world (& QC)

1.2 Qubits: mathematical preliminaries I

Lecture 2

2.1 Qubits: mathematical preliminaries II

2.2 Single qubit logic gates

Lab 1

QUI, Single qubit gates, BB84 communication protocol

PHYC90045 Introduction to Quantum Computing

Lecture 1 overview

In this lecture:

1.1 Non-technical overview of the quantum world (and QC)

- Easy intro to qubits, superposition, entanglement, QC

1.2 Qubits: mathematical preliminaries I

- Superposition and measurements
- Linear algebra and Dirac notation
- Measurement, quantum amplitudes, complex numbers and phase
- Projective operators
- Linear dependence and basis states

- Rieffel, Chapter 3
- Kaye, 2.6
- Nielsen & Chuang, 1.3.2-1.3.4

PHYC90045 Introduction to Quantum Computing

1.1 Non-technical overview of the quantum world (and QC)

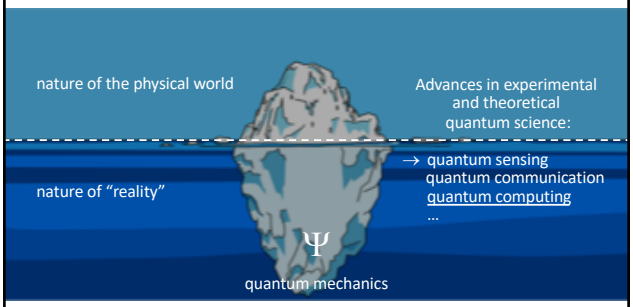
PHYC90045

Lecture 1

PHYC90045 Introduction to Quantum Computing

The Quantum World

Some meta-physics…



PHYC90045 Introduction to Quantum Computing

Key concepts for quantum computing

Quantum superposition:

Systems can be in indeterminate (multiple) states prior to measurement

Quantum measurement:

Result of any given measurement a-priori unknown, system "collapses" to an outcome

Quantum entanglement:

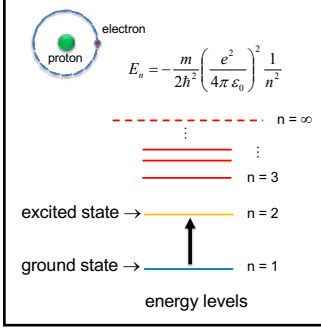
Systems can be linked such that measurement of one part correlates to that of another part

PHYC90045 Introduction to Quantum Computing

Start with a familiar concept – the atom

Planck (1900): postulated that energy is quantised

Bohr (1913): constructed a simple "quantised" model of the atom



Consider lowest two levels

Simply re-label states to a bit notation

→ quantum bit, or "qubit"

(Not to be confused with cubit!)

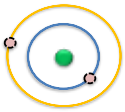
PHYC90045 Introduction to Quantum Computing

Quantum superposition and measurement

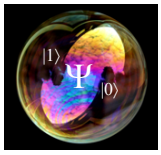
$|1\rangle$

$|0\rangle$

One electron in quantum superposition.



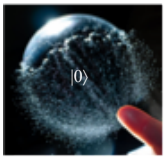
quantum superposition



$|0\rangle$ "and" $|1\rangle$

We write $|\psi\rangle \sim |0\rangle + |1\rangle$

measurement/observation



state collapse → random outcome

Bubble: Brocken Inaglory,commons.wikimedia.org/wiki/File:Soap_bubble_sky.jpg
Bursting bubble: wallpaperswide.com

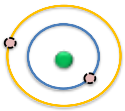
PHYC90045 Introduction to Quantum Computing

Quantum superposition and measurement

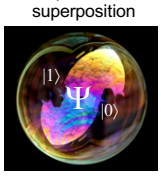
$|1\rangle$

$|0\rangle$

One electron in quantum superposition.



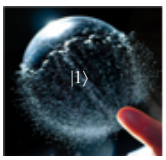
quantum superposition



$|0\rangle$ "and" $|1\rangle$

We write $|\psi\rangle \sim |0\rangle + |1\rangle$

measurement/observation



state collapse → random outcome

Bubble: Brocken Inaglory,commons.wikimedia.org/wiki/File:Soap_bubble_sky.jpg
Bursting bubble: wallpaperswide.com

PHYC90045 Introduction to Quantum Computing

Quantum entanglement

Imagine two qubits. We can prepare two distinct classes of overall state:

a) Separable state: independent quantum superpositions

qubit-1 $\sim |0\rangle + |1\rangle$
qubit-2 $\sim |0\rangle + |1\rangle$

(NB. ignore normalisation for now)

Or we write $|0\rangle + |1\rangle$ x $|0\rangle + |1\rangle \rightarrow |0\rangle\,|0\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle + |1\rangle\,|1\rangle$

Measurement outcomes for each qubit: random and independent

b) An entangled state: e.g. in above notation $|0\rangle\,|1\rangle + |1\rangle\,|0\rangle$

Measurement on qubit-1:
qubit-1 = $|0\rangle$ (random) → qubit-2 = $|1\rangle$
qubit-1 = $|1\rangle$ (random) → qubit-2 = $|0\rangle$

(and vice-versa if we first measured qubit-2)

Measurement outcomes for e.g. qubit-1 are random, but result of qubit-2 depends on qubit-1 outcome → the qubits are somehow connected…

PHYC90045 Introduction to Quantum Computing

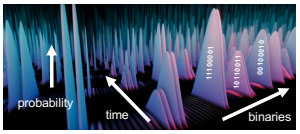
Multiple qubits and binary representation

Basic representation of binaries as quantum information:

Independent quantum superpositions → superposition over *N*-bit binaries |000…0⟩,…, |111…1⟩

Not very useful…measurement of qubits collapses to one random *N*-bit string

Quantum computation: qubits interact to create complex superpositions and entangled states

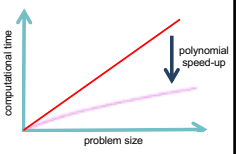


PHYC90045 Introduction to Quantum Computing

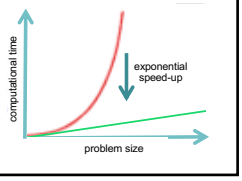
Types of quantum computers

Broadly, there are two classes of quantum computers:

- **Intermediate quantum computers (IQC)**
  - medium-scale system (~1000 qubits)
  - simplified control and error correction
  - potentially polynomial speed-up (e.g. √CPU)
  - optimisation, machine learning, chemistry,…
  - pathway to full-scale universal QC…



- **Full universal quantum computers (UQC)**
  - large-scale system (>>1000 qubits)
  - high redundancy for quantum error correction
  - potentially exponential speed-up for some problems (e.g. Shor's factoring algorithm)
  - large class of problems: financial, data-base analysis, security, bio-molecular simulation
  - polynomial to exponential speed-up



PHYC90045 Introduction to Quantum Computing

Timeline and state of the art

Random QC → simulate with all 2^N binaries: max N = 50 qubits (peta bytes)

Quantum advantage 100-1000 qubits?

Universal QC: (millions of qubits) poly to exponential speed-up on various problems

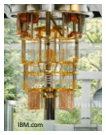
increasing # qubits and quality

Largest simulation of a QC: quantum factoring for 60 qubits (exa → tera bytes)*

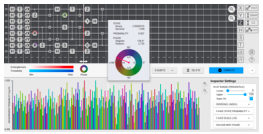
Hardware race: IBM, Google, Intel, D-Wave, Rigetti, Microsoft, SQC,…

*A. Dang et al, arXiv:1712.07311

DWave: 2000 "qubits analogue "QC"



IBM-Q: 50 qubits digital QC



In the meantime, the era of quantum software and app development has begun…

PHYC90045 Introduction to Quantum Computing

1.2 Qubits: mathematical preliminaries I

PHYC90045
Lecture 1

PHYC90045 Introduction to Quantum Computing

Superposition, stochastic measurements

Recap: unlike bits which are in a definite state (0 or 1), a qubit can be a *superposition*

e.g. an atom in both "0" and "1" even though still only <u>one</u> electron

If we measure which state qubit is in, we will get a *probabilistic* outcome of "0" or "1".

e.g. If we prepare a qubit in an **equal** (50:50) superposition and measure:

Prepare/repeat same qubit many times → { 50% of the time, "1" will be measured; 50% of the time, "0" will be measured

Superpositions are not always equal. Another state could lead to different probabilities, eg.

{ 80% of the time, "1" will be measured (prob = 0.8); 20% of the time, "0" will be measured (prob = 0.2)

Here we will briefly develop the **mathematical framework** to describe qubits.

PHYC90045 Introduction to Quantum Computing

Linear Algebra and Dirac notation

- A lot of quantum mechanics comes down to linear algebra (matrices and vectors), but uses a slightly different notation introduced by Dirac:

$|\psi\rangle$ ← A "ket" is a member of a **linear vector space** which represents *the state* of a qubit.

We write the general state of a qubit in ket notation as:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$$

where a_0 and a_1 are in general complex amplitudes.

PHYC90045 Introduction to Quantum Computing

Linear Algebra and Dirac notation

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$$

For qubits we can use column vectors to represent a convenient basis for kets:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Computational basis states

$$a_0 |0\rangle + a_1 |1\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

$$a_0, a_1 \in \mathbb{C}$$

General qubit state
a_0 and a_1 are "amplitudes"

PHYC90045 Introduction to Quantum Computing

Dual vectors

$\langle\psi|$ A "bra" is a **row vector** .

For a qubit state,

$$|\psi\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \quad a_0, a_1 \in \mathbb{C}$$

we define the corresponding *dual vector* to be:

$$\langle\psi| = [\, a_0^* \quad a_1^* \,]$$

PHYC90045 Introduction to Quantum Computing

Measurement and quantum amplitudes

- In quantum mechanics the outcomes of measurements are probabilistic
- Qubits can be in **superpositions**

$$a_0 |0\rangle + a_1 |1\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

- If we were to measure (in the computational basis) we would randomly measure "0" with probability:

$$|a_0|^2$$

or "1" with probability,

$$|a_1|^2$$

- Since probabilities must sum to 1, all qubit states are normalised:

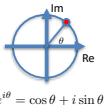
$$|a_0|^2 + |a_1|^2 = 1$$

PHYC90045 Introduction to Quantum Computing

Recap: amplitudes in the QUI

Quantum mechanics represents the *wave function.* Complex numbers represent the amplitude *and phase* of this wave.

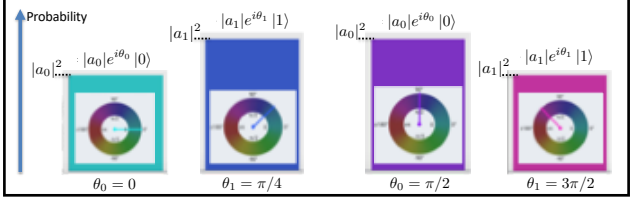
$$|\psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle \;\rightarrow |\psi\rangle = |a_0|e^{i\theta_0}\,|0\rangle + |a_1|e^{i\theta_1}\,|1\rangle$$



Recall: $a = \mathrm{Re}[a] + i\,\mathrm{Im}[a] = |a|e^{i\theta} \rightarrow \begin{matrix} |a| = \sqrt{\mathrm{Re}[a]^2 + \mathrm{Im}[a]^2} \\ \theta = \tan^{-1}(\mathrm{Im}[a]/\mathrm{Re}[a]) \end{matrix}$

$e^{i\theta} = \cos\theta + i\sin\theta$

In the QUI, phase is represented using the phase wheel colour map, and probability by histogram, e.g. two different single-qubit states:



PHYC90045 Introduction to Quantum Computing

Inner Product

$\langle\psi|\phi\rangle$ A "braket" is an **inner product** (analogous to dot product for vectors in 3D)

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

We can define an inner product between them

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

PHYC90045 Introduction to Quantum Computing

Outer Product

$|\psi\rangle\langle\phi|$ is an **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 inner product between them:

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

PHYC90045 Introduction to Quantum Computing

Orthogonality

Two states are *orthogonal* if their inner product is zero

$$\langle\psi|\phi\rangle = 0$$

"Z-basis" (computational basis)

For $|0\rangle$ and $|1\rangle$

$$\langle 0|1\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0$$

Computational basis states are orthogonal

"X-basis" (+/- states)

For

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

These states are also orthogonal

PHYC90045 Introduction to Quantum Computing

Qubit state after measurement

Measurements in quantum mechanics necessarily *disturb the measured system.*

If we make a measurement in quantum mechanics, we disturb the system, and have to update the wave function:

$$|\psi\rangle \rightarrow |\psi'\rangle$$

If measure the state "0", the wave function becomes

$$|\psi'\rangle = |0\rangle$$

If measure the state "1", the wave function becomes

$$|\psi'\rangle = |1\rangle$$

This dramatic change of the state is known as wave function "collapse". In the first Lab we will see how we can use this fact to detect an eavesdropper.

PHYC90045 Introduction to Quantum Computing

Projective Operators

Consider a qubit in the state: $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$

In the computational basis, we can define two projectors:

$$P_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$P_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

The projection operators separate out the basis state in question, e.g.:

$$P_0|\psi\rangle = |0\rangle\langle 0|(a_0|0\rangle + a_1|1\rangle) = a_0|0\rangle\langle 0|0\rangle + a_1|0\rangle\langle 0|1\rangle = a_0|0\rangle$$

($\langle 0|0\rangle = 1$, $\langle 0|1\rangle = 0$)

Or in matrix representation: $P_0|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} a_0 \\ 0 \end{pmatrix}$

PHYC90045 Introduction to Quantum Computing

Projective Measurement

The probability of measurement outcome in terms of projection operators is:

$$p(0) = \langle\psi| P_0 |\psi\rangle = a_0^* a_0 = |a_0|^2 \qquad p(1) = \langle\psi| P_1 |\psi\rangle = a_1^* a_1 = |a_1|^2$$

The state after measurement 'collapses' to: $|\psi'\rangle = \dfrac{P_m |\psi\rangle}{\sqrt{p(m)}}$

Consider measurement on a state $|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle \rightarrow |\psi'\rangle$

If "0" is measured, the resulting state is: $|\psi'\rangle = \dfrac{P_0 |\psi\rangle}{|a_0|} = \dfrac{a_0 |0\rangle}{|a_0|} = |0\rangle$

If "1" is measured, the resulting state is: $|\psi'\rangle = \dfrac{P_1 |\psi\rangle}{|a_1|} = \dfrac{a_1 |0\rangle}{|a_1|} = |1\rangle$

(up to global phase)

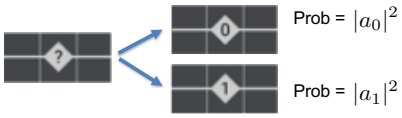
PHYC90045 Introduction to Quantum Computing

QUI: measurement operation

In the QUI the measurement operation looks like this:

By default, measurements are made in the computational basis (ie. 0 or 1).

When you run the circuit, the QUI will randomly select a measurement outcome based on the amplitudes of the state at that point:

$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$  Prob = $|a_0|^2$

Prob = $|a_1|^2$

In some circuit diagrams notation is:  (but we like the spinning lottery)

PHYC90045 Introduction to Quantum Computing

Linear Dependence

A set of vectors is *linearly dependent* if you can write

$$a_1|\psi_1\rangle + a_2|\psi_2\rangle + \ldots = 0$$

with $a_1 \neq 0, a_2 \neq 0, \ldots$

A set of vectors is *linearly independent* if they are not linearly dependent.

$\left\{|0\rangle, |1\rangle, \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right\}$ are linearly dependent

$\{|0\rangle, |1\rangle\}$ are linearly independent

$\left\{\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}, \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$ are also linearly independent

PHYC90045 Introduction to Quantum Computing

Basis states

Every possible qubit state can be expressed as a linear combination of *two* linearly independent vectors.

Every vector space is spanned by *d* linearly independent vectors. This set of vectors is known as a **basis**. d is the **dimension** of the vector space.

$\{|0\rangle, |1\rangle\}$ The computational, or "Z basis"

$\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$ The Hadamard (+/-) or "X basis"

Every qubit state can be expressed in Z-basis as: $a_0 |0\rangle + a_1 |1\rangle$

Or in the X-basis as as: $a_+ \frac{|0\rangle + |1\rangle}{\sqrt{2}} + a_- \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

PHYC90045 Introduction to Quantum Computing

Week 1

Lecture 1

1.1 Non-technical overview of the quantum world (& QC)

1.2 Qubits: mathematical preliminaries I

Lecture 2

2.1 Qubits: mathematical preliminaries II

2.2 Single qubit logic gates

Lab 1

QUI, Single qubit gates, BB84 communication protocol