Quantum Computing
Lecture 1

Bits and Qubits

Maris Ozols

What is Quantum Computing?

Aim: *use quantum mechanical phenomena that have no counterpart in classical physics for computational purposes.*

(Classical = not quantum)

Two central research directions:

- *Experimental*
  - building devices with a specified quantum behaviour
- *Theoretical*
  - **quantum algorithms:** designing algorithms that use quantum mechanical phenomena for computation
  - **quantum information:** designing protocols for transmitting and processing quantum information

Mediating experiments and theory is a *mathematical model* of quantum computation.

Why look at Quantum Computing?

- *The physical world is quantum*
  - information is physical
  - classical computation provides only a crude level of abstraction

  Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.
  – Richard Feynman (1982)
- *Devices are getting smaller*
  - Moore's law
  - on very small scale, the classical laws of physics break down
- *Exploit quantum phenomena*
  - using quantum phenomena may allow to perform computational and cryptographic tasks that are otherwise not efficient or even possible
  - understand the world and discover new physics

Course Outline

A total of eight lecturers:

1. *Bits and Qubits* (this lecture)
2. *Linear Algebra*
3. *Quantum Mechanics*
4. *Model of Quantum Computation*
5. *Quantum Information Protocols*
6. *Search Algorithm*
7. *Factoring*
8. *Complexity*

Useful Resources

Bookzz.org:

Each of these books covers the basic material very well:

- Kaye P., Laflamme R., Mosca M., *An Introduction to Quantum Computing*
- Hirvensalo M., *Quantum Computing*
- Mermin N.D., *Quantum Computer Science: An Introduction*

This is a comprehensive reference (covers the basics too):

- Nielsen M.A., Chuang I.L., *Quantum Computation and Quantum Information*

Papers:

- Braunstein S.L., Quantum computation [`link`]
- Aharonov D., Quantum computation [`arXiv:quant-ph/9812037`]
- Steane A., Quantum computing [`arXiv:quant-ph/9708022`]

Other lecture notes:

- Umesh Vazirani (UC Berkeley) [`link`] – basics and beyond
- John Preskill (Caltech) [`link`] – basics and beyond
- Andrew Childs (U of Maryland) [`link`] – quantum algorithms
- John Watrous (U of Waterloo) [`link`] – quantum information

Course website: `http://www.cl.cam.ac.uk/teaching/1617/QuantComp/`

Bits

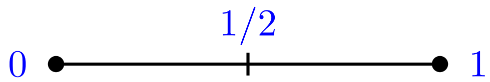
A building block of classical computational devices is a two-state system or a classical bit:

$0 \bullet \qquad\qquad \bullet 1$

Indeed, any system with a finite set of discrete and stable states, with controlled transitions between them, will do:

Probabilistic bits

When you don't know the state of a system exactly but only have partial information, you can use probabilities to describe it:



It is convenient to represent system's state using vectors:

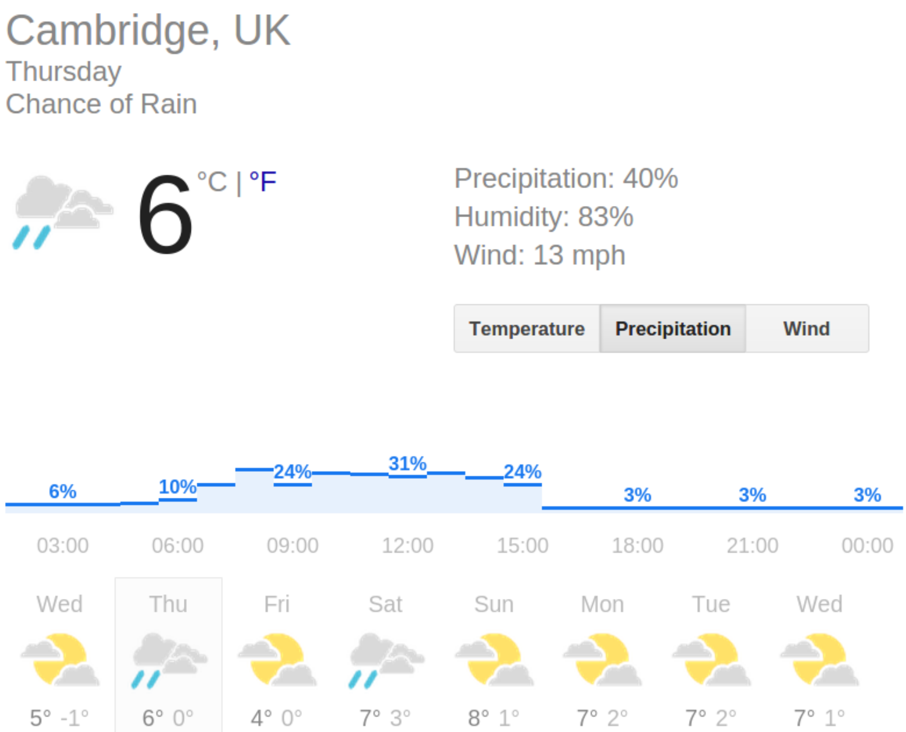
 $= \begin{pmatrix}1\\0\end{pmatrix}$  $= \begin{pmatrix}0\\1\end{pmatrix}$

Then a uniformly random bit is represented by

 $= \frac{1}{2}$  $+ \frac{1}{2}$  $= \frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix}$

Using probabilities to represent information (or lack of it. . .) is more useful than you might think!

Weather forecast



Source: Google / Weather.com

Party planning

Name	Coming?	Chances?
John	Y	0.1
Sarah	N	0.1
Peter	-	0.8
Anna	-	0.5
Tom	N	0.0
Rebecca	Y	1.0
Andy	-	0.6
Kathy	-	0.3
Richard	-	0.7
Total:	2-7	4.1

Probability as a stock price

Quantum superposition...

In nature, the state of an actual physical system is more uncertain than we are used to in our daily lives...

© Charles Addams, The New York Times

That's why complex amplitudes rather than probabilities are used in quantum mechanics!

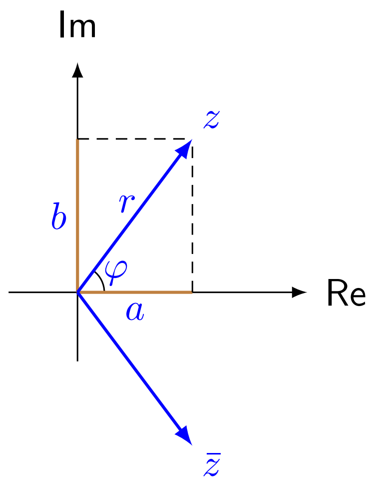
Complex numbers ($i^2 = -1$)

Representations:

- algebraic: $z = a + ib$
- exponential: $z = re^{i\varphi} = r(\cos\varphi + i\sin\varphi)$

Operations:

- addition and subtraction:
  $(a + ib) \pm (c + id) = (a \pm c) + i(b \pm d)$
- multiplication:
  $(a + ib) \cdot (c + id) = (ac - bd) + i(ad + bc)$
  $re^{i\varphi} \cdot r'e^{i\varphi'} = rr'e^{i(\varphi+\varphi')}$
- complex conjugate: $z^* = \bar{z} = a - ib = re^{-i\varphi}$
- absolute value:
  $|z| = \sqrt{a^2 + b^2} = r$, $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$
- absolute value squared: $|z|^2 = a^2 + b^2 = r^2$
  important: $|z|^2 = z\bar{z}$
- inverse: $1/z = \bar{z}/|z|^2$



Classical vs quantum bits

Classical

Recall that a random bit can be described by a probability vector:

p  $+\, q$  $= p\begin{pmatrix}1\\0\end{pmatrix} + q\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}p\\q\end{pmatrix}$

where $p, q \in \mathbb{R}$ such that $p, q \geq 0$ and $p + q = 1$.

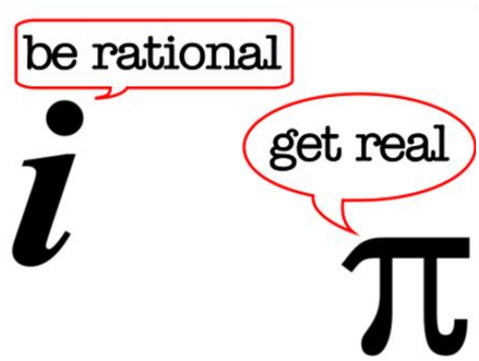
Quantum

A quantum bit (or qubit for short) is described by a quantum state:

$$\alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

where $\alpha, \beta \in \mathbb{C}$ are called amplitudes and satisfy $|\alpha|^2 + |\beta|^2 = 1$. Here $|0\rangle, |1\rangle$ are used as place-holders for the two discernible states of a coin (or any other physical system for that matter).

Any system that can exist in states $|0\rangle$ and $|1\rangle$ can also exist in a superposition $\alpha|0\rangle + \beta|1\rangle$, according to quantum mechanics!



Can I buy $4.1 + 2.8i$ bottles of wine?

Measurement

Classical

Observing a random coin

p  $+\, q$ 

results in heads with probability p and tails with probability q.

Quantum

Measuring the quantum state

$$\alpha|0\rangle + \beta|1\rangle$$

results in $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$.

Important:

- After the measurement, the system is in the measured state, so repeating the measurement will always yield the same value!
- We can only extract one bit of information from a single copy of a random bit or a qubit!

Global and relative phases

Phase

If $re^{i\varphi}$ is a complex number, $e^{i\varphi}$ is called phase.

Global phase

The following states differ only by a global phase:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad e^{i\varphi}|\psi\rangle = e^{i\varphi}\alpha|0\rangle + e^{i\varphi}\beta|1\rangle$$

These states are indistinguishable! Why? Because $|\alpha|^2 = |e^{i\varphi}\alpha|^2$ and $|\beta|^2 = |e^{i\varphi}\beta|^2$ so it makes no difference during measurements.

Relative phase

These states differ by a relative phase:

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Are they also indistinguishable? No! (Measure in a *different basis*.)

Remember: global phase does not matter, relative phase matters!

Qubit states: the Bloch sphere

Any qubit state can be written as

$$|\psi\rangle = \underbrace{\cos\tfrac{\theta}{2}}_{\alpha}|0\rangle + \underbrace{e^{i\varphi}\sin\tfrac{\theta}{2}}_{\beta}|1\rangle$$

for some angles $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi)$.

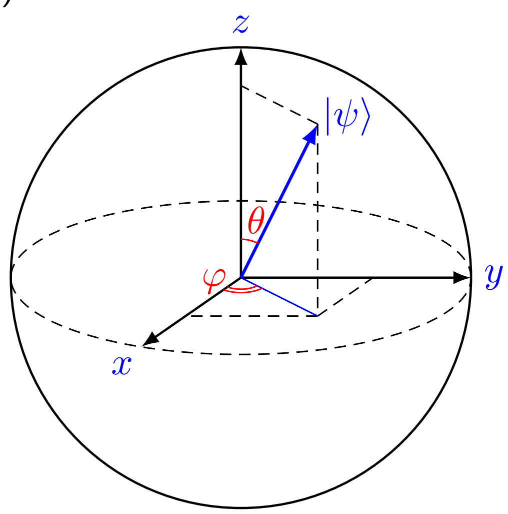
There is a one-to-one correspondence between qubit states and points on a unit sphere (also called Bloch sphere):

Bloch vector of $|\psi\rangle$ in spherical coordinates:

$$\begin{cases} x = \sin\theta\cos\varphi \\ y = \sin\theta\sin\varphi \\ z = \cos\theta \end{cases}$$

Measurement probabilities:

$$|\alpha|^2 = (\cos\tfrac{\theta}{2})^2 = \tfrac{1}{2} + \tfrac{1}{2}\cos\theta$$
$$|\beta|^2 = (\sin\tfrac{\theta}{2})^2 = \tfrac{1}{2} - \tfrac{1}{2}\cos\theta$$



Summary

- **Quantum computing** = quantum physics + computers + math
- **Complex numbers:** $i^2 = -1$, if $z = a + ib$ then $\bar{z} = a - ib$ and $|z|^2 = z\bar{z} = a^2 + b^2$, Euler's identity: $e^{i\varphi} = \cos\varphi + i\sin\varphi$
- **Classical probabilities:** $p, q \geq 0$ and $p + q = 1$
- **Quantum amplitudes:** $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$
- **Qubit state:** $\binom{\alpha}{\beta} = \alpha|0\rangle + \beta|1\rangle$ where α, β are as above
- **Measurement:** get 0 with probability $|\alpha|^2$ and 1 with prob. $|\beta|^2$
- **Phases:** global phase $e^{i\varphi}|\psi\rangle$ does not matter, relative phase matters
- **Bloch sphere:** $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$