G53NSC and G54NSC
Non-Standard Computation

Dr. Alexander S. Green

9th of February 2010

Introduction

- Last week we looked at reversible computation
- We are able to define reversible computations in terms of circuits
- We introduced a set of gates that is universal for reversible computation
- Today we shall be looking at how to extend this to quantum computation
- First, we shall have a brief look at the history of quantum computation

Part I

A brief history of quantum computation

Before quantum computation

- Quantum Mechanics studies the behaviour of energy and matter at the atomic level
- Matter exhibits both wave-like and particle-like behaviour
  - Wave-particle duality
- The Copenhagen interpretation allows us to describe the state of particles as a wavefunction
  - The amplitudes of a wavefunction correspond to the probabilities of observing a particle in a specific state
- Can we model Quantum Mechanics on a computer?

Quantum Computation

Richard Feynman

- Amongst other things...
- Gave a key-note lecture at the California Institute of Technology in May, 1981
- "Simulating Physics with Computers"
- It was published in the International Journal of Physics in 1982

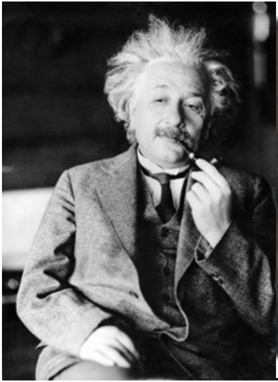
Simulating Physics with Computers

- Feynman set a requirement that any simulator must follow:
  - The number of computer elements required to simulate a large physical system is only to be proportional to the space-time volume of the physical system
  - That is, the simulations cannot be exponential in their number of simulated elements
  - Or, they must relate to feasible computations
- Feynman first looked at classical Physics
- which can be *descretised* and simulated to arbitrary accuracy
- Possible to choose an accuracy that cannot be refuted by experimental evidence
- But what about Quantum Mechanical systems?

Simulating Quantum Mechanics

- The Copenhagen interpretation gives us wavefunctions with complex valued amplitudes
- The state spaces grow exponentially with the number of *elements* in the system
- We cannot simulate this formalism of quantum mechanics on a classical system
- Is this the only formalism of quantum mechanics?
- Is there a way to discretise quantum systems?
- The Copenhagen interpretation gives us a way to model quantum systems based on experimental observations
- but is nature really probabilistic?
- Maybe there is more information than we can currently observe, which would give us the ability to predict the behaviour of quantum systems deterministically

EPR paradox



Albert Einstein

Boris Podolsky

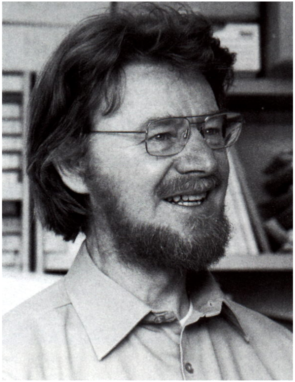
Nathan Rosen

The EPR paradox

What is the EPR paradox?

- A thought experiment introduced in 1935
- arguing that quantum mechanics isn't a complete theory
- Specifically, quantum mechanics can predict a breakdown in locality
- The experiment involves two specially prepared particles that are then seperated by an arbitrarily large distance
- quantum mechanics predicts that measuring one of these particles can instantaneously influence the state of the other particle
- The authors refused to believe this, and presented it as an argument that quantum mechanics is incomplete
- Einstein famously refered to the effect as "spooky action at a distance"

On the EPR paradox



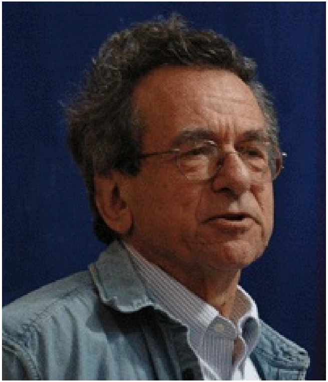
John S. Bell

- Wrote a paper titled "On the Einstein Podolsky Rosen paradox"
- Looking at whether quantum mechanics can be described using local hidden variables
- The paper introduced what is now known as Bell's Theorem

Bell's Theorem

- Bell proved that the results predicted by quantum mechanics could not be preserved by any theory which preserved locality
- That is, he showed that if you could perform the experiment described in the EPR paradox and you got the results predicted by quantum mechanics then locality can't be true

Bell's Theorem



N. David Mermin

- Author of the course text book...
- and a very accesible paper on Bell's theorem and the EPR thought experiment
- "Bringing home the atomic world: Quantum mysteries for anybody"
- We shall now have a brief look at this proof

Mermin's proof

- The experiment involves a source of particles
- and two identical detectors that measure some aspect of the particles
- When a particle is detected the detector outputs one of two results
- Mermin uses Red and Green lights, but we will use 0 and 1
- We can try running the experiments to learn about what it is that the detector is measuring
- Each of the detectors (A and B) can be in any of three different modes (0, 1, or 2)
- Each mode measures some different aspect of the particles

Mermin's proof

- If we set both detectors to the same setting, and measure the same particle twice then the results will always agree
- If we set the detectors to different settings, this will give results that sometimes agree and sometimes disagree
- At this point we can say that each particle must be in one of eight different states, corresponding to the possible outcomes of measurements in each of the three settings
  - 000,001,010,011,100,101,110,111
- We can now change the experiment, and introduce the concept of locality
- The source is now able to send out two particles in opposite directions
- The detectors are placed such that each one will recieve a single particle from the source

Mermin's proof

- Locality now tells us that once the two particles have left the source, they can no longer influence one another
- First, what happens if both detectors have the same setting?
- In our experiments, we notice that the measurements always agree
- That is, that the source must emit particles that share the same properties
- What happens if the detectors have different settings?
- Can we predict what the outcomes will be?
- Lets look at all possible detector settings, and whether both measurements agree

000

	0	1	2
0	1	1	1
1	1	1	1
2	1	1	1

100

	0	1	2
0	1	0	0
1	0	1	1
2	0	1	1

001

	0	1	2
0	1	1	0
1	1	1	0
2	0	0	1

101

	0	1	2
0	1	0	1
1	0	1	0
2	1	0	1

010

	0	1	2
0	1	0	1
1	0	1	0
2	1	0	1

110

	0	1	2
0	1	1	0
1	1	1	0
2	0	0	1

011

	0	1	2
0	1	0	0
1	0	1	1
2	0	1	1

111

	0	1	2
0	1	1	1
1	1	1	1
2	1	1	1

Mermin's proof

- If we repeat the experiment with random settings on each detector we would expect to have matching measurements with a probability of at least $\frac{5}{9}$
- We can now run the experiment and see if the predictions are correct
- Running the experiment only gives matching measurements with probability $\frac{1}{2}$
- If we can build such a device, then locality doesn't hold
- Can we build such a device?
- Such devices have been built using quantum systems, and these results have been verified
- We will look at this experiment in *QIO* next week

Back to Richard Feynman's talk

- Feynman concluded that quantum mechanical systems can not be simulated on classical computers
- How can we simulate quantum mechanical systems?
- Feynman introduced the concept of a computer that is able to use quantum mechanical phenomena
- Describing a system he called the *universal quantum simulator*
- This is now thought of as the first suggestion of a quantum computer

Quantum computers

- Since Feynman, the field of quantum computation has matured
- In 1985, David Deutsch showed that any quantum mechanical system could be simulated with a collection of two-state quantum systems, along with a set of simple operations
- These two-state quantum systems are now known as quantum bits
  - or Qubits
  - or Qbits in the course text book
- The operations on qubits are now known as quantum gates
- Quantum gates generalise the idea of Boolean logic gates over qubits

Part II

Qubits

Qubits

- So, what are qubits?
- Qubits are a generalisation of classical bits into the quantum realm
- Classical bits can only exist in one of two states
- Qubits can exist in a superposition of the same two states
- or in other words, a linear combination of $|0\rangle$ and $|1\rangle$
- In general, the state of a qubit can be given by

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

- with $\alpha, \beta \in \mathbb{C}$
- and the normalisation condition $|\alpha|^2 + |\beta|^2 = 1$
- The normalisation condition corresponds to the fact that $|\psi\rangle$ is a unit vector in the complex vector space

Dirac notation again

- So, qubit states are represented by unit vectors in the complex vector space
- Lets look at what this means in more detail...
- First, a little bit more linear algebra

Classical states

Euclid

- We can think of the 2-Dimensional vector space, over the real numbers, in terms of geometry
- This extends well to the 3-Dimensional real valued vector space too
- In fact, these type of vector space are known as Euclidean spaces
- But what about the complex vector spaces we need for qubits?

Quantum states

David Hilbert

- Hilbert generalised the notion of Euclidean space
- Introducing what are now known as Hilbert spaces
- extending the ideas in $\mathbb{R}^2$ and $\mathbb{R}^3$ to vector spaces of upto infinite dimensions, over real or complex numbers
- We shall be restricting ourselves to finite dimensional Hilbert spaces

Hilbert spaces

Hilbert space

A Hilbert space is a real or complex valued vector space with an inner-product that must satisfy the following conditions:

- $\langle y, x \rangle = \overline{\langle x, y \rangle}$ (conjugate symmetry)
- $\langle ax_1 + bx_2, y \rangle = a \langle x_1, y \rangle + b \langle x_2, y \rangle$ (linear in first argument)
- $\langle x, x \rangle \geqslant 0$ (positive definite)
- Hilbert spaces must also be complete, but this is enforced by restricting ourselves to finite dimensions.

$\mathbb{R}^2$ is a Hilbert space

- Euclidean space, with dot product as the inner product forms a Hilbert space
- $\langle x, y\rangle = x.y = x^T y$
- Conjugate symmetry? $x.y = y.x$
- Linear in first argument? $(ax_1 + bx_2).y = ax_1.y + bx_2.y$
- Positive definite? $x.x \geqslant 0$

$\mathbb{C}^2$ is a Hilbert space

- The 2-Dimensional complex vector space, forms a Hilbert space with the following definition of inner product
- $\langle x, y \rangle = x^* y$
- Conjugate symmetry? Check
- Linear in first argument? Check
- Positive definite? Check

What does Inner product denote?

- Inner product denotes the amplitude of the first state within the second
- For example, if we have the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- we can rewrite this as $|\psi\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- $\langle 0, \psi\rangle = [1, 0] \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha$
- $\langle 1, \psi\rangle = [0, 1] \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \beta$
- How can we visualise the states of a qubit?

The Bloch sphere

Felix Bloch

- A swiss physicist whose work influenced a geometric interpretation of qubit states
- We now call this interpretation the Bloch sphere
- But how can we visualise a qubit as a sphere?

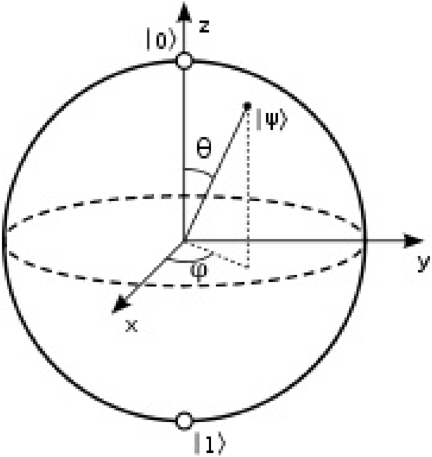
The Bloch sphere

- An arbitrary qubit state, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be rewritten, introducing a global *multiplier* that means the coeffiecient for $|0\rangle$ is real and non-negative
- E.g. The state $\frac{-i}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle = -i(\frac{1}{\sqrt{2}}|0\rangle + \frac{-1}{\sqrt{2}}|1\rangle)$
- This global *multiplier* is known as global phase and it turns out that this doesn't effect measurement outcomes (we'll look more at this next week)
- We are now able to re-write our state $|\psi\rangle = \alpha'|0\rangle + \beta'|1\rangle$ in the form $|\psi\rangle = cos(\frac{\theta}{2})|0\rangle + e^{i\phi}sin(\frac{\theta}{2})|1\rangle$
- $\theta = 2cos^{-1}(\alpha')$
- $\phi = Im(ln(\frac{\beta'}{sin(\frac{\theta}{2})}))$

The Boch sphere

- Except for the vectors $|0\rangle$ and $|1\rangle$ we are left with unique θ and ϕ with $0 \leqslant \theta \leqslant \pi$ and $0 \leqslant \phi \leqslant 2\pi$
- These *angles* represent a unique point on the unit sphere
- Let try it for $\frac{1}{\sqrt{2}} |0\rangle + \frac{-1}{\sqrt{2}} |1\rangle$
- $\theta = 2cos^{-1}(\frac{1}{\sqrt{2}}) = \frac{\pi}{2}$
- $\phi = Im(ln(\frac{\frac{1}{\sqrt{2}}}{sin(\frac{\pi}{4})})) = \pi$

The Bloch sphere



Measurement

- Unfortunately, there is now way to measure the state of an arbitrary qubit
- Why is this?
- Born's rule tells us that measuring a quantum system collapses the wave function!
- What does this mean?
- If we look at, or measure, the state of a qubit then we only ever get see one of the base states, $|0\rangle$ or $|1\rangle$
- and, the qubit is collapsed into that state!
- Fortunately, we can use the amplitudes of a qubit to give us the probabilities of measuring either state

Measurement

- If we measure a qubit in an arbitrary super-position $\psi = \alpha\,|0\rangle + \beta\,|1\rangle$ we are left with $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$
- For example, if we have the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ then we will measure $|0\rangle$ ot $|1\rangle$ both with probability $\frac{1}{2}$
- $|+\rangle$ is said to be in an equal super-position
- What else can we do with qubits, that doesn't collapse their wave function?

What else can we do with Qubits?

- So, the states of a qubit can be thought of as a point on Bloch sphere
- Single qubit gates can be thought of as rotations about the Bloch sphere
- As the state space of a qubit is continuous, this means there are an infinte number of possible one-qubit gates
- Any complex valued unitary 2x2 matrix represents a single qubit gate
- A set of gates is said to be universal if it can *simulate* any gate upto an arbitrary accuracy
- We'll look now at some popular gates...

Hadamard rotation

- The Hadamard gate is named in honour of French mathematician Jacques Hadamard
- It is an important gate as it takes the base states $|0\rangle$ and $|1\rangle$ into equal super-positions
- The Hadamard gate is given by $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- $|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- It also has the property that it is its own inverse

Pauli rotations

Wolfgang Pauli

- Came up with an important set of gates
- Known as the Pauli-X, Pauli-Y and Pauli-Z gates
- or X, Y and Z for short
- They are all self inverse, and correspond to rotations about the axis they are named after

Pauli rotations

- $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- X corresponds to the classical negation operation
- $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
- $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Qubits in *QIO*

- Operations on single qubits aren't that interesting
- We shall look at multiple-qubit gates next week
- and introduce the concept of Entanglement
- The labs this week will involve using *QIO* to define some single qubit quantum computations, so we shall have a brief look now at *QIO*
- We have already seen how we can use the classical subset of *QIO* and this extends nicely into the quantum realm.
- Quantum computations consist of the same three steps as reversible computations:
  - Initialise any qubits that are required
  - Perform unitary operations on these qubits
  - Measure any qubits that form part of the result

Initialisation

- We initialise qubits in the same way as we initialised bits for the reversible computations
- Now, *mkQbit False* returns a qubit initialised to $|0\rangle$
- and *mkQbit True* returns a qubit initialised to $|1\rangle$

Unitary operations

- We shall be looking at unitary operations on single qubits in this weeks labs
- The exercise sheet shall introduce new members of the U data-type that can be used within Quantum computations
- We will be implementing all the rotations described previously.
- Applying a unitary is still done with the *applyU* function.

Measurement

- Measurement is also done in a simlar manner as for reversible computation
- *measQbit q* returns a Boolean that represents the base state that the qubit q has collapsed into
- Measurements are probabilistic, with the probabilities relating to the amplitudes of the qubit
- We'll see next week that measurements can have side effects, which gives rise to the monadic structure of *QIO*

Running *QIO* computations

- Quantum computations cannot be simulated efficiently on a classical computer
- However, two simulation functions are provided that can be used for all the programs we are likely to define
- They reside in the *QIO.Qio* library file
- $run :: QIO\ a \rightarrow IO\ a$
- *run* uses the random number generator to simulate probabilistic results
- $sim :: QIO\ a \rightarrow Prob\ a$
- *sim* returns a probability distribution of all possible results

Thank you

- Remember... labs are on Thursdays, 15:00 to 17:00 in A32
- Also, Friday is the deadline for choosing your pairs and topics for the Research paper and presentation
- If I haven't heard from you before then, I will assign them for you!
- Thank you