G53NSC and G54NSC Non-Standard Computation

Dr. Alexander S. Green

16th of February 2010

Introduction

- Last week we introduced the idea of Qubits
- Qubits can exist in a linear superposition of the classical base states $|0\rangle$ and $|1\rangle$.
- E.g. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- with $\alpha, \beta \in \mathbb{C}$
- and the normalisation constraint that $|\alpha|^2 + |\beta|^2 = 1$
- We can think of the state of a qubit as a point on the Bloch sphere
- Unitary operations on single qubits correspond to rotations on the Bloch sphere

Introduction

- We also looked at the EPR experiment and how locality doesn't hold in Quantum Mechanics
- We shall look at this today in terms of Quantum Computation
- How multiple qubits can become Entangled...
- meaning the state of a qubit can depend on the states of other qubits
- We'll then go on to look at implementing the EPR experiment in *QIO*

Part I

Measurement

Measurement

- To understand entanglement, it is important to understand measurement
- For a single qubit, we know that measurement collapses a qubit into one of its base states, $|0\rangle$ or $|1\rangle$
- We also know that the probability of measuring either base state is related to the amplitude of that state
- E.g. for an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:
  - The probability of measuring $|0\rangle$ is $|\alpha|^2$
  - The probability of measuring $|1\rangle$ is $|\beta|^2$
- Lets try some examples...

Measurement Examples

- The state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  - will measure to $|0\rangle$ with probability $\frac{1}{2}$
  - will measure to $|1\rangle$ with probability $\frac{1}{2}$
- The state $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
  - will measure to $|0\rangle$ with probability $\frac{1}{2}$
  - will measure to $|1\rangle$ with probability $\frac{1}{2}$
- The state $\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}i|1\rangle$
  - will measure to $|0\rangle$ with probability $\frac{1}{4}$
  - will measure to $|1\rangle$ with probability $\frac{3}{4}$
- But, what happens when we have more than one qubit?

Multiple qubit states

- How can we describe multiple qubit states?
- How did we represent multiple bit states when we looked at Dirac notation with classical reversible computation?
- Classically, multiple bit states correspond to bit strings in a single Ket structure
- E.g. two bits can be any of the states $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$
- and a tensor product is implicit in this notation
- E.g. we write $|10\rangle$ for the state $|1\rangle \otimes |0\rangle$
- How does this extend to qubits?

Multiple qubit states

- A two-qubit state can appear in a linear superposition of all four of the classical two-bit states
- E.g. An arbitrary two-qubit state $|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$
- with $\alpha, \beta, \gamma, \delta \in \mathbb{C}$
- and the normalisation constraint: $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$

Tensor product

- We can still *build up* states using the tensor product
- E.g. $|01\rangle = |0\rangle \otimes |1\rangle$
- or $|+-\rangle = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle)$
- and we can use the distributivity laws of tensor product and addition to simplify this:
  - $(v_1 + v_2) \otimes w = (v_1 \otimes w) + (v_2 \otimes w)$
  - $v \otimes (w_1 + w_2) = (v \otimes w_1) + (v \otimes w_2)$
- $|+-\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

Multiple qubit states

- This extends to n-qubit states (for any $n \in \mathbb{N}$)
- Classically an n-bit state can be in any of 2^n states
- An n-qubit state is described by a linear superposition of all the 2^n classical states
- With complex amplitudes and the normalisation condition as before
- What about measurement?

Measuring multiple qubits

- The amplitudes still correspond to the probability of measuring each classical base state
- E.g. for an arbitrary two-qubit state $|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$
  - The probability of measuring $|00\rangle$ is $|\alpha|^2$
  - The probability of measuring $|01\rangle$ is $|\beta|^2$
  - The probability of measuring $|10\rangle$ is $|\gamma|^2$
  - The probability of measuring $|11\rangle$ is $|\delta|^2$
- But the qubits are separate entities...
- We don't have to measure them both

Individual Measurements

- What if we have an arbitrary two-qubit state and only want to measure the first qubit?
- $|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$
- Measuring a single qubit collapses the overall state into a superposition of all the states in which it is in the measured state
- The probability of measuring each base state is the sum of the probabilities of each state in which it is that base state
- E.g. for the arbitrary two-qubit state above
  - The probability of measuring the first qubit as $|0\rangle$ is $|\alpha|^2 + |\beta|^2$
  - and the overall state collapses to $\alpha'\,|00\rangle + \beta'\,|01\rangle$
  - The probability of measuring the first qubit as $|1\rangle$ is $|\gamma|^2 + |\delta|^2$
  - and the overall state collapses to $\gamma'\,|10\rangle + \delta'\,|11\rangle$

- Where α', β' and γ', δ' are re-normalised:

$$\alpha' = \frac{\alpha}{\sqrt{|\alpha|^2+|\beta|^2}} \ \beta' = \frac{\beta}{\sqrt{|\alpha|^2+|\beta|^2}}$$

$$\gamma' = \frac{\gamma}{\sqrt{|\gamma|^2+|\delta|^2}} \ \delta' = \frac{\delta}{\sqrt{|\gamma|^2+|\delta|^2}}$$

- We can generalise this for n-qubit systems
- and measuring any $m \leqslant n$ qubits

Measurement example

- The state $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$ is in an equal superposition
- What happens if we measure the first qubit?
  - We measure $|0\rangle$ with probability $\frac{1}{2}$
  - and the remaining state collapses to $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  - We measure $|1\rangle$ with probability $\frac{1}{2}$
  - and the remaining state also collapses to $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- We could have predicted this, as this state can be written in terms of each of its constituent qubits
- $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle = (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes (\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)$
- This is not always the case...

Part II

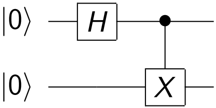
Entanglement

Entanglement

- The state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is an entangled state
- What does this mean?
- What happens if we measure the first qubit?
  - We get $|0\rangle$ with probability $\frac{1}{2}$
  - and the remaining state collapses to $|00\rangle$
  - We get $|1\rangle$ with probability $\frac{1}{2}$
  - and the remaining state collapses to $|11\rangle$
- Measuring the first qubit has the side effect of collapsing both qubits into a single base state
- Can we actually create a state like this?

Entanglement Circuit

- Look at the following circuit:



- What is the output of this circuit?
- The state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is known as a Bell state

QIO Entanglement

- Equivalently, look at the following *QIO* code:

$$
\begin{aligned}
&\mathit{bell} :: \mathit{QIO}\ (\mathit{Qbit}, \mathit{Qbit})\\
&\mathit{bell} = \mathbf{do}\ \mathit{q1} \leftarrow \mathit{mkQbit\ False}\\
&\qquad\qquad\ \mathit{q2} \leftarrow \mathit{mkQbit\ False}\\
&\qquad\qquad\ \mathit{applyU}\ (\mathit{hadamard\ q1})\\
&\qquad\qquad\ \mathit{applyU}\ (\mathit{controlledX\ q1\ q2})\\
&\qquad\qquad\ \mathit{return}\ (\mathit{q1}, \mathit{q2})
\end{aligned}
$$

- What state are the pair of qubits in?

QIO Entanglement

- What do we get if we measure the qubits?

$$
\begin{aligned}
&\mathit{measureBell} :: \mathit{QIO}\ (\mathit{Bool}, \mathit{Bool})\\
&\mathit{measureBell} = \textbf{do}\ (\mathit{q1}, \mathit{q2}) \leftarrow \mathit{bell}\\
&\qquad\qquad\qquad\qquad\ \ \mathit{b1} \leftarrow \mathit{measQbit}\ \mathit{q1}\\
&\qquad\qquad\qquad\qquad\ \ \mathit{b2} \leftarrow \mathit{measQbit}\ \mathit{q2}\\
&\qquad\qquad\qquad\qquad\ \ \mathit{return}\ (\mathit{b1}, \mathit{b2})
\end{aligned}
$$

- Simulating this *QIO* computation gives:

[((True,True),0.5),((False,False),0.5)]

- The two separate measurements always agree

Entanglement

- It is Entanglement that can be exploited in the EPR experiment
- We shall look at a variant of the EPR experiment in *QIO* shortly
- The two-qubit state that we created previously is called a Bell state...
- and is often described as a maximally entangled state
- Entanglement is an important part of quantum computation
- It plays a big role in many quantum algorithms, including:
  - Quantum teleportation
  - Superdense coding
  - Quantum cryptography
- We will be looking at these algorithms next week

No cloning theorem

- There is no unitary operation that can *clone* an arbitrary qubit state
- That is, given $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we cannot create the state $|\psi\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$
- However, we can use entanglement to *share* a quantum state
- E.g. given the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we can create the state $\alpha|00\rangle + \beta|11\rangle$
- This is what we did previously to create a Bell state from sharing the state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

Part III

EPR in the Quantum IO Monad

EPR in the Quantum IO Monad

- We shall use a Bell pair to simulate a variant of the EPR thought experiment using *QIO*
- Although it has not been mentioned, we have already introduced all the constructs for defining quantum computations in *QIO*
- We shall define the classical variant in Haskell, as well as the quantum variant in *QIO*
- We can repeatedly run the experiment and see what percentage of the runs yield a matching measurement
- Checking whether locality holds for quantum computations in *QIO*

Classical Detectors

- Each detector can be in any of three different settings:

  data *Setting* $= A \mid B \mid C$

- A classical particle must carry enough information for each setting of the detector

  type *Particle* $= (Bool, Bool, Bool)$

- A classical detector can take a setting and a particle, and return the corresponding value

  $cDetector :: Setting \rightarrow Particle \rightarrow IO\ Bool$
  $cDetector\ A\ (a, \_, \_) = return\ a$
  $cDetector\ B\ (\_, b, \_) = return\ b$
  $cDetector\ C\ (\_, \_, c) = return\ c$

Classical Source

- A classical source just returns two identical random particles

$$
\begin{aligned}
&\mathit{cSource} :: \mathit{IO}\ (\mathit{Particle}, \mathit{Particle}) \\
&\mathit{cSource} = \mathbf{do}\ a \leftarrow \mathit{randomIO} \\
&\qquad\qquad\quad\ b \leftarrow \mathit{randomIO} \\
&\qquad\qquad\quad\ c \leftarrow \mathit{randomIO} \\
&\qquad\qquad\quad\ \mathit{return}\ ((a, b, c), (a, b, c))
\end{aligned}
$$

- We can now look at the quantum setup...

Quantum Detectors

- In the quantum realm, we can use qubits as our particles
- The three settings on the detectors correspond to rotating the qubit by $0^o, 120^o$, or 240^o before measurement
- We can define a rotation of 120^o around the Y-axis using the following unitary:

$$
\begin{aligned}
&\mathit{u120} :: \mathit{Rotation} \\
&\mathit{u120}\ (a, b) = \textbf{if}\ (a \equiv b)\ \textbf{then}\ c\ \textbf{else}\ (\textbf{if}\ b\ \textbf{then}\ -s\ \textbf{else}\ s) \\
&\qquad\qquad\qquad \textbf{where}\ c = \mathit{cos}\ (\mathit{pi}\ /\ 3) \\
&\qquad\qquad\qquad\qquad\quad\ s = \mathit{sin}\ (\mathit{pi}\ /\ 3)
\end{aligned}
$$

- This can be calculated by an exponentiation of the pauli-Y operator. We shall be looking at what this means in the labs...

Quantum Detectors

- For each *Setting* we are able to define a *measurement rotation*:

$$
\begin{aligned}
&\mathit{measureAngle} :: \mathit{Setting} \rightarrow \mathit{Qbit} \rightarrow U \\
&\mathit{measureAngle}\ A\ q = \mathit{mempty} \\
&\mathit{measureAngle}\ B\ q = \mathit{rot}\ q\ \mathit{u120} \\
&\mathit{measureAngle}\ C\ q = (\mathit{rot}\ q\ \mathit{u120})\ `\mathit{mappend}`\ (\mathit{rot}\ q\ \mathit{u120})
\end{aligned}
$$

- The quantum detector can now be defined:

$$
\begin{aligned}
&\mathit{qDetector} :: \mathit{Setting} \rightarrow \mathit{Qbit} \rightarrow \mathit{QIO}\ \mathit{Bool} \\
&\mathit{qDetector}\ s\ q = \mathbf{do}\ \mathit{applyU}\ (\mathit{measureAngle}\ s\ q) \\
&\qquad\qquad\qquad\quad\ \ \mathit{measQbit}\ q
\end{aligned}
$$

Quantum Source

- The quantum source is able to make use of entanglement, which is what leads to the non-locality
- For this experiment, it is sufficient that the quantum source returns a bell pair as we have previously seen:

$$
\begin{aligned}
&qSource :: QIO\ (Qbit, Qbit)\\
&qSource = bell
\end{aligned}
$$

- We can now look at running our experiments...

Same Settings

- The first experiment is with the detectors both set to the same *Setting*

$$
\begin{aligned}
&\mathit{testC} :: \mathit{Setting} \rightarrow \mathit{IO}\ \mathit{Bool}\\
&\mathit{testC}\ s = \mathbf{do}\ (\mathit{c1}, \mathit{c2}) \leftarrow \mathit{cSource}\\
&\qquad\qquad\qquad \mathit{b1} \leftarrow \mathit{cDetector}\ s\ \mathit{c1}\\
&\qquad\qquad\qquad \mathit{b2} \leftarrow \mathit{cDetector}\ s\ \mathit{c2}\\
&\qquad\qquad\qquad \mathit{return}\ (\mathit{b1} \equiv \mathit{b2})\\
&\mathit{testQ} :: \mathit{Setting} \rightarrow \mathit{QIO}\ \mathit{Bool}\\
&\mathit{testQ}\ s = \mathbf{do}\ (\mathit{q1}, \mathit{q2}) \leftarrow \mathit{qSource}\\
&\qquad\qquad\qquad \mathit{b1} \leftarrow \mathit{qDetector}\ s\ \mathit{q1}\\
&\qquad\qquad\qquad \mathit{b2} \leftarrow \mathit{qDetector}\ s\ \mathit{q2}\\
&\qquad\qquad\qquad \mathit{return}\ (\mathit{b1} \equiv \mathit{b2})
\end{aligned}
$$

Different Settings

- The tests both always return *True* as we would expect
- Now we can define the experiment for possibly different settings on each detector

$$
\begin{array}{l}
cExperiment :: (Setting, Setting) \rightarrow IO\ Bool \\
cExperiment\ (s1, s2) = \mathbf{do}\ \begin{array}[t]{l} (c1, c2) \leftarrow cSource \\ b1 \leftarrow cDetector\ s1\ c1 \\ b2 \leftarrow cDetector\ s2\ c2 \\ return\ (b1 \equiv b2) \end{array} \\
qExperiment :: (Setting, Setting) \rightarrow QIO\ Bool \\
qExperiment\ (s1, s2) = \mathbf{do}\ \begin{array}[t]{l} (q1, q2) \leftarrow qSource \\ b1 \leftarrow qDetector\ s1\ q1 \\ b2 \leftarrow qDetector\ s2\ q2 \\ return\ (b1 \equiv b2) \end{array}
\end{array}
$$

Random Settings

- We can now pass random settings to both experiments, combining them so we can correlate the results

$$
\begin{aligned}
& \mathit{experiment} :: \mathit{IO}\ (\mathit{Bool}, \mathit{Bool}) \\
& \mathit{experiment} = \mathbf{do}\ \mathit{s1} \leftarrow \mathit{randomSetting} \\
& \qquad\qquad\qquad\quad\ \mathit{s2} \leftarrow \mathit{randomSetting} \\
& \qquad\qquad\qquad\quad\ c \leftarrow \mathit{cExperiment}\ (\mathit{s1}, \mathit{s2}) \\
& \qquad\qquad\qquad\quad\ q \leftarrow \mathit{run}\ (\mathit{qExperiment}\ (\mathit{s1}, \mathit{s2})) \\
& \qquad\qquad\qquad\quad\ \mathit{return}\ (c, q)
\end{aligned}
$$

Random Settings

- What is the reuslt of running the experiment?
- If we just run it, we will get any of the following results:

$$(\mathit{False}, \mathit{False}),\ (\mathit{False}, \mathit{True}),\ (\mathit{True}, \mathit{False}),\ (\mathit{True}, \mathit{True})$$

- But what are the probabilities of either value being *True*?
- We shall be looking at this in the labs!

Thank you

- Remember: Labs are on Thursday
- I hope to see you there
- Project topics and pairings are now finalised
- Check the course webpage, and let me know of any problems...
- Thank you