Lecture 4: Some Properties of Qubits

Dr Iain Styles: I.B.Styles@cs.bham.ac.uk

Introduction

Last lecture, we:
• Showed how qubit states can be changed by unitary transformations
• Showed how to construct composite states of several qubits

In this lecture we will:
• Discuss how much information is stored in a qubit
• Show how to make measurements on composite states
• Introduce the key concept of entanglement
• Prove the no-cloning theorem

A Brief Recap

• Qubits are two-state systems with state vector $|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$
• Measuring a qubit yields 0 with $p(0) = |a_0|^2$ and yields 1 with $p(1) = |a_1|^2$
• After the measurement the qubit is in the state corresponding to the result of the measurement ($|0\rangle$ or $|1\rangle$)
• Evolution of qubits is governed by unitary operators (e.g. quantum NOT gate: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$)
• The state vector of a composite state is given by the tensor product of the component states

Information in Qubits

• Measure a classical bit $\mapsto 0$ or 1
• Measure it again $\mapsto$ the same result
• A classical bit contains only one “piece” of information
• Qubits are rather different!
• There are infinitely many possible qubit states: $a_0$ and $a_1$ are only constrained by $|a_0|^2 + |a_1|^2 = 1$
• So can we store an “infinite” amount of information in a single qubit?
• Yes (in a certain sense)—provided we don’t measure it!
• Measuring a qubit only gives 0 or 1, like a classical bit
• To access the full information content of a qubit, need to determine $a_0$ and $a_1$
• Remember that on measurement, $p(0) = |a_0|^2$ and $p(1) = |a_1|^2$
Information in Qubits

- So we can deduce $a_0$ and $a_1$ by making lots of measurements and just counting $n(0)$ and $n(1)$, right?

- No: remember that after the measurement, the state of the system collapses onto the result of the measurement.

- We could prepare a large number of qubits in the same state and measure them all: this would work, but is impractical.

- Or we could keep re-preparing and re-measuring a single qubit—also rather impractical!

- So although we can store an infinite amount of information, we can’t access it.

- Although we can’t measure the coefficients, we can manipulate them (this is what our unitary evolution operators do).

- This is what gives quantum computers great power.

Measuring Composite States

- Last lecture, we showed how to construct multi-qubit systems from individual qubits.

- The general state of a two-qubit system is written

$$|\psi\rangle = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle$$

- Composite states obey the same rules as single-qubit states:
  - Normalisation: $\sum_{ij} |a_{ij}|^2 = 1$
  - Measurement: $p(00) = |a_{00}|^2$, $|\psi\rangle \rightarrow |00\rangle$

- But we don’t have to measure both qubits at once!

- Let’s say we measure only the first qubit, and get result 1.

- The only way we could get this is from the terms in $|10\rangle$ and $|11\rangle$.

- So $p(1) = |a_{10}|^2 + |a_{11}|^2$

The Bell States

- A special and interesting two-qubit state is the Bell state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- This state has the special property that when you measure one of the qubits, the second qubit must give the same result.

- Leads to quantum teleportation (later in the course).

- An additional property is that you can’t make this state from two independent qubits: you must combine them first, then program the state.

- Take two independent qubits:

$$|\psi_a\rangle = a_0 |0\rangle + a_1 |1\rangle; \quad |\psi_b\rangle = b_0 |0\rangle + b_1 |1\rangle$$
Entanglement

• Form a composite state from these two qubits:

$$|\psi\rangle = |\psi_a\rangle \otimes |\psi_b\rangle = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle$$

• To make this a Bell state, need $a_0 b_1 = a_1 b_0 = 0$
• But if (say) $a_0 = 0$, then also lose term in $|00\rangle$
• So we can’t form a Bell state from two independent qubits
• The two qubits are said to be entangled: measurements on them are perfectly correlated, and they can’t be “untangled” into two individual qubits
• Entangled states of up to five qubits have been seen very recently (Z Zhao et al. 2004 Nature 430 54)
• Bell states are also known as EPR pairs
• Entanglement is used in several applications including quantum teleportation and superdense coding

The No-Cloning Theorem

• An operation that we take for granted in classical computation is the ability to copy stuff
• How do we do this in a quantum computer? We treat it as an evolution of the system!
• Imagine there is some transformation $U$ which acts on a pair of quantum systems (e.g. two qubits), and copies the state of the first system onto the second. We would write this as:

$$U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle$$

• Note that the system is a composite state
• Assume that we can choose $U$ to work on two known states:

$$U(|\alpha\rangle |0\rangle) = |\alpha\rangle |\alpha\rangle; \quad U(|\beta\rangle |0\rangle) = |\beta\rangle |\beta\rangle$$

• The problem is that $U$ must be unitary, and hence linear
• This means that states in any form of superposition can’t be copied
• We could choose $U$ so that we could copy $|\gamma\rangle$
• But then it would fail for other states
• In general, to be able to copy a quantum state, we must know what it is!
• We’ve shown that normally, we don’t know what the state is as we can’t measure the coefficients!
• So we can’t copy a general quantum state
• This important result is known as the no-cloning theorem
Conclusions

In this lecture we have:

• Discussed how much information is stored in a qubit, and what we can do with it
• Analysed measurements of multi-qubit states
• Introduced the concept of entanglement and Bell states
• Proved that you can’t, in general, copy quantum states

Next lecture we will:

• Introduce the fundamental ideas of quantum logic