Quantum Computing: A Guide in English

Struan McDonough

February 24, 2017

1 An introduction

1.1 Why does this guide exist

I wrote this guide because while studying Quantum Computing, I found that the notes available to students are inaccessible and rely heavily upon a knowledge of Physics. This document aims to explain the Physics which grounds the course and attempts to make this area of study accessible to Computer Scientists.

1.2 Transition Systems

1.2.1 Definitions

A transition system can be used to describe an observable system. It's a mathematical way of describing the different states something can take, and how those states can be connected with actions. An action simply takes something, and changes it state from a state s_1, to a state s_2.

- A **state space** is a set S of states the observed system can take.

- An **initial state** is a fixed element $s_1 \in S$.

- A **current state** is a variable element $s \in S$.

- A **action** belongs to a set of possible actions Act.

- A **transition** is a triple (s, act, s') where act is an action which takes s to the state of s'.

- A **transition system** S on (S, Act) is a set of transitions built using a state space and a set of Actions Act.

Usually in Quantum Computing, we assume that there is only ever one action between any two states. Hence we can write a transition as (s, s') as opposed to (s, act, s').

1.2.2 Example

If we consider a 32 bit register, we can deconstruct this scenario in terms of a transition system.

- The state space is the set of values which can be held in the register

- The initial state of a register is what it looks like when it is turned on. In most cases, this is every value in the register taking the value of 0.

- The current state is the value held in the register at any given time.

- The actions are the set of all machine instructions which can be performed on the register.

- The transitions are the set of all possible computation steps (from one state to another using a given instruction).

1.2.3 Deterministic vs Non-Deterministic Behaviour

We say that an action is **deterministic** if when repeated, it yields the same result. For example, $1 + 1$ always equals 2.

We say that an action is **non-deterministic** if when repeated, it yields a different result. A fair coin toss is non-deterministic.

1.2.4 Different Types of Transition Systems

We can have both **deterministic transition systems** and **non-deterministic transition systems**. This is where all of the actions are deterministic or non-deterministic respectively.

A **Stochastic Transition System** is one in which every transition (s, s') has an associated probability $p(s, s')$. The sum of all transition probabilities leaving a state must equal 1.

A **Quantum Transition System** is one in which every transition (s, s') has an associated probability amplitude $\psi(s, s')$.

A **Probability Amplitude** is a different measurement used to label transitions. These can be turned into probabilities by taking the modulus, and then squaring it.

$$|(\psi(s, s'))|^2 = p(s, s').$$

The probabilities these generate must also equal 1.

$$\sum_{s'} |\psi(s, s')|^2 = 1$$

1.3 Probability Amplitudes

In Quantum Systems, we must use Probability Amplitudes to describe changes in a meaningful way. Particles have two main properties which are of interest to us, the information of position and momentum, and the information about the spin of the particle. The position and momentum can change in a continuous way, but the spin of a particle can only take distinct, discrete values. The Mathematics of a Quantum System cannot be expressed using probabilities alone, due to some quite advanced Physics involving Wave Functions and so forth. Normal probabilities can't handle quantum transitions in a meaningful way.

1.3.1 Sequential Composition
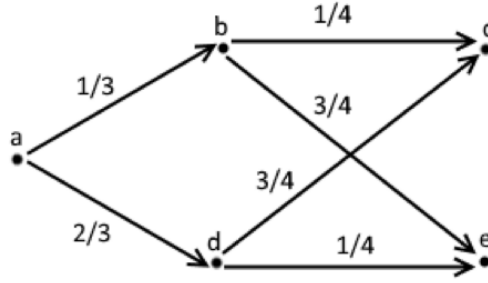
If we have states a, b, c, then to find the probability of going from a to c through b $p(a, b, c)$, we have to compose them. This works by finding all the intermediate steps. $p(a, b) \times p(b, c) = p(a, b, c)$. In the example above, $p(a, b, c) = 1/12$

The same works for probability amplitudes. $\psi(a, b, c) = \psi(a, b) \times \psi(b, c)$.

1.3.2 Composition of Different Sequences

This is when we want to get from one state to another, but can use multiple sequences.

$p(a, b, c) = p(a, b) \times p(b, c)$

$p(a, d, c) = p(a, d) \times p(d, c)$

$p(a, c) = p(a, b, c) + p(a, d, c) = (p(a, b) \times p(b, c)) + (p(a, d) \times p(d, c))$

Stochastic and Quantum Transition systems work in exactly the same way during composition of sequences.

3

However, when converting the Quantum System back into a Transition System, some odd things can happen!

$$p_Q(a, c) = (p_Q(a, b) \times p_Q(b, c)) + (p_Q(a, d) \times p_Q(d, c))$$

However, $p_Q(a, b) = |\psi(a, b)|^2$. (By the way, I'm going to stop writing the $\times$ explicitly...)

$$p_Q(a, c) = |\psi(a, b)\psi(b, c) + \psi(a, d)\psi(d, c)|^2$$

$$p_Q(a, c) = |\psi(a, b)\psi(b, c)|^2 + |\psi(a, d)\psi(d, c)|^2 + \psi(a, b)\psi(b, c)\psi^*(a, d)\psi^*(d, c) + \psi^*(a, b)\psi^*(b, c)\psi(a, d)\psi(d, c)$$

Now the above looks quite scary, but it's the simple $(ab + cd)^2$ expansion. Also, $\psi * (a, b)$ is the complex conjugate of $\psi(a, b)$.

2 Linear Algebra

2.1 Dirac Notation

Dirac Notation (Aka Bra-ket) notation is used for describing quantum states. $|x\rangle$ is called a bra, and $\langle y|$ is called a ket. Hence $\langle x|y\rangle$ is a bra-ket.

A bra $\langle x|$ denotes a row vector $\begin{bmatrix} x_1 & ... & x_n \end{bmatrix}$.

A ket $|y\rangle$ denotes a column vector $\begin{bmatrix} y_1 \\ ... \\ y_n \end{bmatrix}$.

To save space in documents, we sometimes write a column vector as $\begin{bmatrix} x_1 & ... & x_n \end{bmatrix}^T$, where T stands for transpose. Just imagine rotating it clockwise by 90 degrees.

2.1.1 Vector multiplication

There's two main types of vector multiplication: inner product and outer product.

The inner product is when you multiply a **bra** by a **ket** $\langle x|y\rangle$. This returns a scalar (a number), and is calculated by multiplying together each pair of entries at each index, then add up the result.

$$\langle x|y\rangle = \begin{bmatrix} x_1 & ... & x_n \end{bmatrix} \times \begin{bmatrix} y_1 \\ ... \\ y_n \end{bmatrix} = x_1 y_1 + x_2 y_2 + ... + x_n y_n$$

The outer product is when you multiply a **ket** by a **bra** $|x\rangle\langle y|$. This returns a matrix, and is defined as follows:

$$|x\rangle\langle y| = \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} \times \begin{bmatrix} y_1 & \dots & y_n \end{bmatrix} = \begin{bmatrix} x_1 y_1 & \dots & x_1 y_n \\ \dots & & \dots \\ x_n y_1 & \dots & x_n y_n \end{bmatrix}$$

2.2 Complex Inner Product Space

This is a type of set (H) which is defined by the following properties:

- Any two vectors in the set are **commutative under addition**:
$|x\rangle, |y\rangle \in H \implies |x\rangle + |y\rangle = |x+y\rangle = |y\rangle + |x\rangle \in H.$

- Any three vectors in the set are **associative under addition**:
$|x\rangle, |y\rangle, |z\rangle \in H \implies (|x\rangle + |y\rangle) + |z\rangle = |x\rangle(|y\rangle + |z\rangle)$

- The set **contains a zero element**, which does nothing when applied to a vector:
$\underline{0} \in H$ and $\underline{0} + |x\rangle = |x\rangle \in H$