PHI 322 Quantum computation basics

Adam Elga

March 26, 2003

1 Measurement of a composite system

Idea is the same as for a single system: in the simplest case, each measurement is associated with an orthonormal basis, one basis element per experimental outcome. To get the probability of outcome associated with b_i, project the system's state onto b_i and square the length of the resulting vector.

For example, suppose that we are given a vector

$$v = az^+ \otimes z^+ + bz^+ \otimes z^- + cz^- \otimes z^+ + dz^- \otimes z^-$$

in the tensor product space for representing the spin states of two electrons. We might send each electron through a (distinct) z-spin measurer. Then our experimental outcomes are: "both go up", "first electron up, 2nd down", "first down, 2nd up", and "both go down". These are associated with the following basis elements

$$\left\{z^+ \otimes z^+, z^+ \otimes z^-, z^- \otimes z^+, z^- \otimes z^-\right\}$$

So for example, to get the probability of getting the outcome "first down, 2nd up", we project v onto $z^- \otimes z^+$. The result is $cz^- \otimes z^+$. Then we square the length of that vector to get our answer: c^2.

2 Quantum circuit model

This discussion follows the Rieffel article, which you may wish to consult as well.

Classical circuits perform operations on the basic states (bits) "0" and "1". Analogously, quantum circuits perform operations on basic states (**qubits**) $|0\rangle$ and $|1\rangle$. You can think of a qubit as the spin state of an electron, where $z^+ = |0\rangle$ and $z^- = |1\rangle$. (When people implement quantum computers, they use different physical systems than electrons—but the state spaces of the systems that they use have the same structure as the spin states we've already studied.)

A classical circuit is a system that performs a transformation on a fixed number of bits. We feed our input at the left side of the circuit. The input is propagated through the circuit according to some transformation. Then we measure the final state at the end of the day.

Analogously, think of a **quantum circuit** as a system that performs a unitary transformation on a fixed finite number of qubits (think: electron spin-states). We feed in our input at the left side of the circuit. The state of the input changes according to some unitary transformation. And then we measure the final state at the end of the day. If we've designed things right, we get the answer to an interesting question thereby.

The simplest classical logic gates have just a one bit input and a one bit output. There are only two: the identity gate, and the not gate.

There are many one bit **quantum logic gates**. Each is associated with a unitary transformation on the space of states for a single qubit. (Recall that unitary transformations are linear transformations that preserve inner products.) Every quantum logic gate has the same number of inputs as outputs.

Notice that given any basis, one can completely specify a linear transformation by saying what effect it has on each basis element. For example, consider the linear transformation I such that

$$I(|0\rangle) = |0\rangle\,,$$

$$I(|1\rangle) = |1\rangle\,.$$

Since $\{|0\rangle\,, |1\rangle\}$ is a basis (think of it as $\{z^+, z^-\}$), the above constraints determine what I does to any vector. (Why?)

Other important one-bit transformation are X and H:

$$X(|0\rangle) = |1\rangle\,,$$

$$X(|1\rangle) = |0\rangle\,.$$

$$H(|0\rangle) = 1/\sqrt{2}\,(|0\rangle + |1\rangle)\,,$$

$$H(|1\rangle) = 1/\sqrt{2}\,(|0\rangle - |1\rangle)\,.$$

Note that $H(|0\rangle \otimes \cdots \otimes |0\rangle)$ (H applied to the tensor product of n $|0\rangle$'s) equals an equally weighted sum of every tensor product of $|0\rangle$'s and $|1\rangle$'s of length n. (Why?)