February 2, 2006

Physics 681-481; CS 483: Assignment #2

(please hand in after the lecture, Thursday, February 16th)

I. Non-spooky construction of a spooky 2-Qbit state

Section A4 of the appendix to chapter 1 describes the strange properties of a pair of Qbits in the entangled state $|\Phi\rangle$ given by:

$$|\Phi\rangle = \tfrac{1}{\sqrt{12}}\big(3|00\rangle + |01\rangle + |10\rangle - |11\rangle\big). \tag{1}$$

To do this problem you do not have to read Section A4, which explains what is strange about the behavior of two Qbits in the state $|\Phi\rangle$. The problem is only about how to prepare two Qbits in that state — a prologue to A4.) It is easy to show (and you should convince yourself of this to make sure you understand the notation, but it is an example of the kind of routine algebraic manipulation that doesn't have to be included in your essay) that

$$|\Phi\rangle = \big(\mathbf{H}\otimes\mathbf{H}\big)|\Psi\rangle, \tag{2}$$

where

$$|\Psi\rangle = \tfrac{1}{\sqrt{3}}\big(|00\rangle + |01\rangle + |10\rangle\big), \tag{3}$$

so if you can produce a pair of Qbits in the state $|\Psi\rangle$ then you can get them into the state Φ by sending each through a Hadamard gate.

This question is about how to get a pair of Qbits into the state $|\Psi\rangle$, if they are initially in the standard state $|00\rangle$ (which is easily prepared with the aid of measurement gates and NOT gates, as described in chapter 1.) How would you go about changing the state of the Qbits from the easily prepared and boring state $|00\rangle$ into the exotic state $|\Psi\rangle$, if the gates that are available to you are restricted by the following rules? You are allowed to apply arbitrary 1-Qbit gates associated with arbitrary 1-Qbit unitary transformations, but the only non-trivial 2-Qbit unitary transformation you are allowed to use is a cNOT (controlled-not) operation $\mathbf{C}$, which you can apply just once. (A trivial 2-Qbit transformation is one that is a product of 1-Qbit transformations.) I did this by breaking it up into two pieces (feel free to find a better way):

(a) Show how to do it with 1-Qbit unitary transformations if you also have a 2-Qbit controlled-Hadamard transformation, $\mathbf{C}_H$, defined just as $\mathbf{C}$ is defined except that the operation applied to the target Qbit when the state of the control Qbit is $|1\rangle$ is not $\mathbf{X}$, but the Hadamard transformation $\mathbf{H}$.

(b) Show how to construct $\mathbf{C}_H$ out of a single $\mathbf{C}$ and 1-Qbit unitary transformations. You might well be able to do this by just playing around, but the direct way is to make use of the relation between two-dimensional unitary transformations and rotations developed in Section A2 of the appendix to chapter 1, taking advantage of the fact that $\mathsf{X} = \mathbf{x}\cdot\sigma$ and $\mathsf{H} = \frac{1}{\sqrt{2}}(\mathsf{X}+\mathsf{Z}) = \frac{1}{\sqrt{2}}\big(\mathbf{x}+\mathbf{z}\big)\cdot\sigma$. (Related tricks for more general controlled-unitary operators are described in Section E of chapter 2; in general two cNOT's are needed, but the controlled Hadamard is simple enough to require only one.)

II. Measurement gates.

The most powerful version of the Born rule is in the form stated on page 25 of Chapter 1 of the lecture notes. In this form, the rule notes that the general state of $m+n$ Qbits can be written as

$$|\Psi\rangle_{m+n} = \sum_x \alpha_x |x\rangle_m |\Phi_x\rangle_n \tag{4}$$

where $\sum_x |\alpha_x|^2 = 1$ and the states $|\Phi_x\rangle_n$ are normalized, but not necessarily orthogonal. The rule asserts that if only the m Qbits associated with the states $|x\rangle_m$ in (4) are measured, then with probability $|\alpha_x|^2$ the result will be x, and after the measurement the state of all $m+n$ Qbits, will be the product state

$$|x\rangle_m |\Phi_x\rangle_n \tag{5}$$

in which the m measured Qbits are in the state $|x\rangle_m$ and the n unmeasured ones are in the state $|\Phi_x\rangle_n$. Show that this rule satisfies the reasonable requirement that measuring r Qbits and then immediately measuring s more, is exactly the same as measuring the $r+s$ Qbits all at once:

(a) Given n Qbits in the state $|\Psi\rangle_n$, suppose r of the Qbits are measured, immediately after which s additional Qbits are measured (with $r+s<n$). Find the possible states of the n Qbits after the two measurements and their associated probabilities, by first applying the rule to the r-Qbit measurement and then applying the rule a second time to the subsequent s-Qbit measurement.

(b) Show that what you found in (a) is the same as what you would have found, more simply, by just applying the rule a single time to a single measurement of all $r+s$ Qbits.

Working this through is a straightforward exercise, but explaining what you are doing is a less trivial exercise in organization and clear exposition. In the way I would organize things it is important to invoke the probabilistic rule (a form of "Bayes's rule")

$$p(xy) = p(y|x)p(x), \tag{6}$$

where $p(x,y)$ is the joint probability of getting x for the first measurement and y for the second, $p(y|x)$ is the conditional probability of getting y for the second, given x for the first, and $p(x)$ is the probability of getting x for the first.