

Physics 681-481; CS 483: Assignment #3

(please hand in after the lecture, Thursday, March 2nd)

I. Other aspects of Deutsch's problem

Suppose one tried to solve Deutsch's problem, not by the clever trick used in Chapter 2, Section B, but by doing the standard thing: Start with input and output registers in the state $|0\rangle|0\rangle$, apply a Hadamard to the input register, and then apply \mathbf{U}_f , thereby associating with the two Qbits the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle. \quad (1)$$

Given two Qbits in this state, a direct measurement only reveals the value of f at either 0 or 1 (randomly), but gives no information about whether $f(0) = f(1)$. But is there anything more clever one can do to two Qbits in the state (1) to learn whether or not $f(0) = f(1)$, by applying a further unitary transformation before measuring? Deutsch noticed a way to do this successfully half the time:

(a) Show that if you apply a Hadamard \mathbf{H} to each Qbit prior to the measurement, then regardless of which of the four possible states (1) you have been given (corresponding to the four possible ways a function f can take one bit to one bit), there is a 50% chance that the measurement will enable you to conclude whether or not $f(0) = f(1)$. But the other 50% of the time you learn nothing whatever from the measurement outcome, neither about whether $f(0) = f(1)$ nor about the value of either $f(0)$ or $f(1)$.

(b) Suppose you can apply any unitary transformation \mathbf{U} you wish (including arbitrary 2-Qbit unitaries) to the pair of Qbits described by the state (1). Show that a subsequent measurement will still have (with non-zero probability) outcomes that do not enable you to learn whether or not $f(0) = f(1)$. (The only property of \mathbf{U} I needed to show this was that it preserves inner products.)

(c) [*Optional*.¹] Strengthen the result of (b) by proving that you cannot do better than the 50-50 chance of knowing whether or not $f(0) = f(1)$ (and knowing that you know it) found in (a) above for the special case $\mathbf{U} = \mathbf{H} \otimes \mathbf{H}$, no matter how you pick the general \mathbf{U} . (It took me a while to prove this conjecture, but maybe I overlooked a really simple argument.)

(continued on next page)

¹ Questions marked optional are more challenging. This being an SU-only course, the reward for doing optional questions is (a) the pleasure of the hunt and (b) accrued glory.

II. Constructing an arbitrary two-Qbit state

In Assignment #2, Part I — see also the Discussion of #2 — we explored how to construct a Hardy state from cNOT gates and one-Qbit unitaries acting on $|0\rangle|0\rangle$. More generally, one can construct *any* two-Qbit state

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \quad (2)$$

by acting on $|0\rangle|0\rangle$ with a circuit made up of cNOT gates and one-Qbit unitary gates.

(a) Show that this can be done with two cNOT gates, by exploiting the fact that a controlled- U gate for arbitrary one-Qbit \mathbf{U} can be built of two cNOT gates and one-Qbit unitaries (pictured in Figure 2.12 and discussed in Section E of Chapter 2).

(b) Show that this can also be done with only a single cNOT gate. I found I needed to use the fact (a special case of the “Schmidt decomposition theorem”) that any two-Qbit state $|\Psi\rangle$ can be expressed in the form:

$$|\Psi\rangle = (\mathbf{u} \otimes \mathbf{v})(\lambda|00\rangle + \mu|11\rangle) \quad (3)$$

for appropriately chosen 1-Qbit unitaries \mathbf{u} and \mathbf{v} and appropriately complex numbers λ and μ (which can always be picked to be real and non-negative, but that is not needed in what follows.)

(c) Explain why a representation of the form (3) holds for any 2-Qbit state $|\Psi\rangle$. Although Nielsen and Chuang (page 109) prove a very general form of the Schmidt decomposition theorem for arbitrary states of n Qbits, I have in mind a much simpler argument that works specifically for 2-Qbit states (*but see the Addendum on the next page for an even simpler argument*):

(i) Explain why (3) holds if and only if $(\mathbf{u} \otimes \mathbf{v})|01\rangle$ and $(\mathbf{u} \otimes \mathbf{v})|10\rangle$ are both orthogonal to $|\Psi\rangle$.

(ii) Explain why (i) implies that it is enough to show that one can find two orthogonal pairs — $|\phi_0\rangle, |\phi_1\rangle$ and $|\chi_0\rangle, |\chi_1\rangle$ — with the property that $|\phi_0\rangle \otimes |\chi_1\rangle$ and $|\phi_1\rangle \otimes |\chi_0\rangle$ are both orthogonal to $|\Psi\rangle$.

(iii) Explain why such pairs of states will exist if and only if they exist for (in general unnormalized) pairs of the special form

$$|\phi_0\rangle = |0\rangle + \gamma|1\rangle, \quad |\phi_1\rangle = |1\rangle - \gamma^*|0\rangle; \quad (4)$$

$$|\chi_0\rangle = |0\rangle - \beta^*|1\rangle, \quad |\chi_1\rangle = |1\rangle + \beta|0\rangle. \quad (5)$$

(iv) Putting the forms (4) and (5) into condition (ii), show that the two equations that result for the two complex numbers γ and β always have a solution, whatever the values of the amplitudes α_{ij} . (In fact it’s easy to give the explicit solutions, but I didn’t find them to be of much interest, so there’s no reason to write them down unless you discover something interesting about them.)

Addendum 28 February 2006:

An even simpler way to do II(c) just occurred to me:

(1) Explain why (3) holds if and only if

$$(\mathbf{u}^\dagger \otimes \mathbf{1})|\Psi\rangle = |0\rangle \otimes |\alpha\rangle + |1\rangle \otimes |\beta\rangle, \quad (6)$$

where $|\alpha\rangle$ and $|\beta\rangle$ are orthogonal (but in general not unit) vectors.

(2) Noting that the general 2-Qbit $|\Psi\rangle$ in (2) is of the form

$$|\Psi\rangle = |0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\phi\rangle \quad (7)$$

where $|\psi\rangle$ and $|\phi\rangle$ are in general neither orthogonal nor unit vectors, show that there is indeed a 1-Qbit unitary \mathbf{u} that brings about (6) with orthogonal $|\alpha\rangle$ and $|\beta\rangle$, with the action of \mathbf{u}^\dagger taken explicitly to be of the form

$$\mathbf{u}^\dagger|0\rangle = a|0\rangle + b|1\rangle; \quad \mathbf{u}^\dagger|1\rangle = -b^*|0\rangle + a^*|1\rangle. \quad (8)$$