March 2, 2006

Physics 681-481; CS 483: Discussion of #3

I.

(a) For each of the four possibilities for the unknown function f, the corresponding forms for the state

$$|\psi\rangle = |0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle \tag{1}$$

are

$$|\psi\rangle_{00} = \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|0\rangle, \qquad f(0) = 0,\ f(1) = 0; \tag{2}$$

$$|\psi\rangle_{11} = \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|1\rangle, \qquad f(0) = 1,\ f(1) = 1; \tag{3}$$

$$|\psi\rangle_{01} = \tfrac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big), \quad f(0) = 0,\ f(1) = 1; \tag{4}$$

$$|\psi\rangle_{10} = \tfrac{1}{\sqrt{2}}\big(|0\rangle|1\rangle + |1\rangle|0\rangle\big), \quad f(0) = 1,\ f(1) = 0. \tag{5}$$

We know that $|\psi\rangle$ has one of these four forms, and wish to distinguish between two cases:

$$\textbf{Case 1: } |\psi\rangle = |\psi\rangle_{00} \text{ or } |\psi\rangle_{11}; \quad \textbf{Case 2: } |\psi\rangle = |\psi\rangle_{01} \text{ or } |\psi\rangle_{10}.$$

By applying Hadamard transformations we can change the four possible states to

$$\big(\mathbf{H}\otimes\mathbf{H}\big)|\psi\rangle_{00} = \tfrac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |0\rangle|1\rangle\big), \quad f(0) = 0,\ f(1) = 0, \tag{6}$$

$$\big(\mathbf{H}\otimes\mathbf{H}\big)|\psi\rangle_{11} = \tfrac{1}{\sqrt{2}}\big(|0\rangle|0\rangle - |0\rangle|1\rangle\big), \quad f(0) = 1,\ f(1) = 1, \tag{7}$$

$$\big(\mathbf{H}\otimes\mathbf{H}\big)|\psi\rangle_{01} = \tfrac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big), \quad f(0) = 0,\ f(1) = 1, \tag{8}$$

$$\big(\mathbf{H}\otimes\mathbf{H}\big)|\psi\rangle_{10} = \tfrac{1}{\sqrt{2}}\big(|0\rangle|0\rangle - |1\rangle|1\rangle\big), \quad f(0) = 1,\ f(1) = 0. \tag{9}$$

If we now make a measurement then if we have one of the Case-1 states, (6) or (7), we get 00 half the time and 01 half the time, while if we have one of the Case-2 states, (8) or (9), we get 00 half the time and 11 half the time. So regardless of what the state is, half the time we get 00 and learn nothing whatever, and half the time we get 01 (Case 1) or 11 (Case 2) and learn which case we are dealing with.

(b) We know that the state (1) is one of the four states (2)-(5). We are allowed to apply an arbitrary two-Qbit unitary transformation $\mathbf{U}$ to $|\psi\rangle$ before we make the measurement. If every possible measurement outcome must rule out one or the other of the two cases, then if $\mathbf{U}|\psi\rangle_{00}$, $\mathbf{U}|\psi\rangle_{11}$, $\mathbf{U}|\psi\rangle_{01}$, and $\mathbf{U}|\psi\rangle_{10}$ are all expanded in the computational basis, then those computational-basis states that appear in the Case-1 expansions cannot appear in the Case-2 expansions, for otherwise there would be a non-zero probability of a measurement outcome that did not enable us to discriminate between the two cases. Consequently $\mathbf{U}|\psi\rangle_{00}$ and $\mathbf{U}|\psi\rangle_{11}$ must each be orthogonal to each of $\mathbf{U}|\psi\rangle_{01}$ and $\mathbf{U}|\psi\rangle_{10}$. But this is

impossible, because unitary transformations preserve inner products, while (2)-(5) show that the inner product of any Case-1 state with any Case-2 state is $\frac{1}{2}$.

(c) We're asked to show that no matter what unitary transformation is applied to the state (1) prior to a measurement, the probability of being able to learn from the measurement whether or not $f(0) = f(1)$ cannot exceed $\frac{1}{2}$. I show this below in an even more general situation, in which we bring in n additional (*ancillary*) Qbits. These might be used to further process the input and output registers through some elaborate quantum subroutine, producing an arbitrary unitary transformation $\mathbf{W}$ that acts on all $n+2$ Qbits before a final measurement of all $n+2$ Qbits is made. This reduces to the simpler case if $\mathbf{W}$ acts as the identity except on the original two Qbits (hereafter called the pair).

The ancillary Qbits start off in some state $|\chi\rangle_n$, which we can take to be $|0\rangle_n$.[1] After $\mathbf{W}$ acts the probability of a measurement giving x ($0 \le x \le 3$) for the pair and y ($0 \le y < 2^n$) for the ancillary Qbits, given that the initial state of the pair was $|\psi\rangle$, is

$$p_{\,|\psi\rangle}(x,y) = |\langle x,y|\mathbf{W}|\psi,0\rangle|^2, \tag{10}$$

where it is convenient to write a $2+n$ Qbit state of the form $|\psi\rangle_2 \otimes |\chi\rangle_n$ as $|\psi,\chi\rangle$.

Note next that since

$$p_{\,|\phi\rangle}(x,y) = 0 \quad \text{if and only if} \quad \langle x,y|\mathbf{W}|\phi,0\rangle = 0, \tag{11}$$

if $p_{\,|\phi\rangle}(x,y)$ vanishes for several different states $|\phi\rangle$, linearity requires it also to vanish for any state in the subspace they span. So any measurement outcome that enables us to discriminate between Case 1 and Case 2 must either have zero probability for both of the states (2) and (3), and hence on the subspace they span, or it must have zero probability for both of the states (4) and (5), and on the subspace they span. Since (2)-(5) reveal that the state

$$|\alpha\rangle = \tfrac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big) \tag{12}$$

belongs to *both* subspaces, if there are any measurement outcomes x, y with

$$p_{\,|\alpha\rangle}(x,y) \neq 0, \tag{13}$$

then such outcomes are uninformative. So if the state of the pair is $|\psi\rangle$, then the probability of a measurement outcome that does not allow us to discriminate between Case-1 and Case-2 is at least

$$p_{\min} = {\sum_{x,y}}' \, p_{\,|\psi\rangle}(x,y), \tag{14}$$

where the prime indicates that the sum is restricted to those measurement outcomes x, y that satisfy (13).

[1] Any other n-Qbit state is related to $|0\rangle_n$ by a unitary transformation in the ancillary subspace, which can be absorbed into $\mathbf{W}$

Now it is easy to verify that every one of the four possible forms (2)-(5) for $|\psi\rangle$ is of the form

$$|\psi\rangle = \tfrac{1}{\sqrt{2}}\big(|\alpha\rangle + |\beta\rangle\big) \tag{15}$$

where $|\alpha\rangle$ is as in (12) and $|\beta\rangle$ is orthogonal to $|\alpha\rangle$. Since $|\psi\rangle$ has the form (15), then we have from (10) and (14)

$$p_{\min} = \tfrac{1}{2}{\sum_{x,y}}' \big(p_{\,|\alpha\rangle}(x,y) + 2\mathrm{Re}\langle\beta,0|\mathbf{W}^\dagger|x,y\rangle\langle x,y|\mathbf{W}|\alpha,0\rangle + p_{\,|\beta\rangle}(x,y)\big). \tag{16}$$

Although the sum is restricted to those x, y satisfying (13), we can extend it in each of the first two terms in (16) to run over all x, y since this adds either zero probabilities (first term) or, because of (11), zero amplitudes (second term). The first term then gives

$$\sum_{\text{all } x,y} p_{\,|\alpha\rangle}(x,y) = 1, \tag{17}$$

while the second gives

$$2\mathrm{Re}\sum_{\text{all } x,y}\langle\beta,0|\mathbf{W}^\dagger|x,y\rangle\langle x,y|\mathbf{W}|\alpha,0\rangle = \langle\beta,0|\mathbf{W}^\dagger\mathbf{W}|\alpha,0\rangle = \langle\beta,0|\mathbf{1}|\alpha,0\rangle = 0, \tag{18}$$

since $|\alpha\rangle$ and $|\beta\rangle$ are orthogonal. Hence

$$p_{\min} = \tfrac{1}{2}\big(1 + {\sum_{x,y}}' p_{\,|\beta\rangle}(x,y)\big) \geq \tfrac{1}{2}. \tag{19}$$

II.

(a) If we define

$$\alpha_0 = \sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}, \quad \alpha_1 = \sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}, \tag{20}$$

then the state

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{21}$$

has the form

$$|\Psi\rangle = \alpha_0|0\rangle|\phi_0\rangle + \alpha_1|1\rangle|\phi_1\rangle \tag{22}$$

where $|\phi_0\rangle$ and $|\phi_1\rangle$ are normalized one-Qbit states and $\alpha_0^2 + \alpha_1^2 = 1$. Since $|\phi_0\rangle$ and $|\phi_1\rangle$ are unit vectors there is a unitary transformation $\mathbf{U}$, satisfying $\mathbf{U}|\phi_0\rangle = |\phi_1\rangle$. If $\mathbf{C}_U$ is the two-Qbit controlled-U gate then

$$|\Psi\rangle = \mathbf{C}_U\big(\alpha_0|0\rangle + \alpha_1|1\rangle\big)|\phi_0\rangle. \tag{23}$$

If $\mathbf{V}$ is a one-Qbit unitary that takes $|0\rangle$ into the normalized one-Qbit state $\alpha_0|0\rangle + \alpha_1|1\rangle$, and $\mathbf{W}$ is a one-Qbit unitary that takes $|0\rangle$ into $|\phi_0\rangle$, then

$$|\Psi\rangle = \mathbf{C}_U\big(\mathbf{V}\otimes\mathbf{W}\big)|0\rangle|0\rangle. \tag{24}$$

Since $\mathbf{C}_U$ can be built out of two cNOT gates and one-Qbit unitaries (as described in Chapter 2), (24) constructs $|\Psi\rangle$ out of one-Qbit unitaries and two cNOT gates.

(b) Specialized to two Qbits, the Schmidt decomposition theorem says that if $|\Psi\rangle$ is a general normalized two-Qbit state,

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle, \tag{25}$$

then there are one Qbit unitary transformations $\mathbf{u}$ and $\mathbf{v}$ such that

$$|\Psi\rangle = \big(\mathbf{u}\otimes\mathbf{v}\big)\big(\lambda|00\rangle + \mu|11\rangle\big). \tag{26}$$

Given (26) the rest is straightforward. We have

$$\lambda|00\rangle + \mu|11\rangle = \mathbf{C}_X\big(\lambda|0\rangle + \mu|1\rangle\big)|0\rangle = \mathbf{C}_X\big(\mathbf{w}\otimes\mathbf{1}\big)|0\rangle|0\rangle, \tag{27}$$

where $\mathbf{w}$ is a one-Qbit unitary taking $|0\rangle$ into $\lambda|0\rangle + \mu|1\rangle$, which is indeed a unit vector since the normalization of $|\Psi\rangle$ in (26) requires that $|\lambda|^2 + |\mu|^2 = 1$. Therefore

$$|\Psi\rangle = \big(\mathbf{u}\otimes\mathbf{v}\big)\mathbf{C}_X\big(\mathbf{w}\otimes\mathbf{1}\big)|0\rangle|0\rangle. \tag{28}$$

(c) Simple derivation of the Schmidt representation (26) for any 2-Qbit state.

(1) The form

$$\big(\mathbf{u}^\dagger\otimes\mathbf{1}\big)|\Psi\rangle = |0\rangle\otimes|\alpha\rangle + |1\rangle\otimes|\beta\rangle, \quad \langle\alpha|\beta\rangle = 0, \tag{29}$$

follows from (26) by defining the unnormalized orthogonal vectors $|\alpha\rangle$ and $|\beta\rangle$ to be $\lambda\mathbf{v}|0\rangle$ and $\mu\mathbf{v}|1\rangle$. Conversely, (26) follows from (29) because any pair of orthonormal states defines a unitary transformation $\mathbf{v}$ that takes $|0\rangle$ and $|1\rangle$ into that pair. (Amplitudes λ and μ have to be extracted from the orthogonal vectors $|\alpha\rangle$ and $|\beta\rangle$ to convert them to unit vectors.)

(2) The general 2-Qbit $|\Psi\rangle$ (25) is of the form

$$|\Psi\rangle = |0\rangle\otimes|\psi\rangle + |1\rangle\otimes|\phi\rangle \tag{30}$$

where $|\psi\rangle$ and $|\phi\rangle$ are in general neither orthogonal nor unit vectors. Define $\mathbf{u}^\dagger$ by

$$\mathbf{u}^\dagger|0\rangle = a|0\rangle + b|1\rangle; \quad \mathbf{u}^\dagger|1\rangle = -b^*|0\rangle + a^*|1\rangle, \tag{31}$$

noting that this preserves orthogonality and preserves normalization if

$$|a|^2 + |b|^2 = 1.$$

It follows that

$$\big(\mathbf{u}^\dagger \otimes \mathbf{1}\big)|\Psi\rangle = \big(a|0\rangle + b|1\rangle\big) \otimes |\psi\rangle + \big(-b^*|0\rangle + a^*|1\rangle\big) \otimes |\phi\rangle =$$

$$|0\rangle \otimes \big(a|\psi\rangle - b^*|\phi\rangle\big) + |1\rangle \otimes \big(b|\psi\rangle + a^*|\phi\rangle\big). \tag{32}$$

So we only have to show that it is possible to pick complex numbers a and b that make the vectors

$$a|\psi\rangle - b^*|\phi\rangle \quad \text{and} \quad b|\psi\rangle + a^*|\phi\rangle \tag{33}$$

orthogonal. (We can then rescale a and b to satisfy (32) without altering orthogonality.) The inner product of the two vectors (33) is

$$a^2\langle\phi|\psi\rangle - b^{*2}\langle\psi|\phi\rangle + ab^*\big(\langle\psi|\psi\rangle - \langle\phi|\phi\rangle\big). \tag{34}$$

If $\langle\phi|\psi\rangle = 0$ then (30) is already of the desired form (29). Otherwise (34) is a quadratic equation for a/b^* which always has two complex solutions. There are two solutions because if $\mathbf{u}$ and $\mathbf{v}$ work in (26), so will $\mathbf{uX}$ and $\mathbf{vX}$ (with λ and μ interchanged.)

*****

(c) Uglier derivation of the Schmidt representation (26) for any 2-Qbit state (as specified before the addendum was added to the Assignment.)

(i) Since unitary transformations preserve inner products, (26) holds if and only if $\big(\mathbf{u}^\dagger \otimes \mathbf{v}^\dagger\big)|\Psi\rangle$ is orthogonal to $|01\rangle$ and $|10\rangle$; but this, in turn, holds if and only if $|\Psi\rangle$ is orthogonal to $\big(\mathbf{u} \otimes \mathbf{v}\big)|01\rangle$ and $\big(\mathbf{u} \otimes \mathbf{v}\big)|10\rangle$.

(ii) *Any* orthonormal pair of state vectors is related to the pair $|0\rangle, |1\rangle$ by a unitary transformation (since the linear transformation taking one pair into the other preserves all inner products). Hence the condition in (i) is equivalent to the condition that there should be two orthonormal pairs — $|\phi_0\rangle, |\phi_1\rangle$ $(= \mathbf{u}|0\rangle, \mathbf{u}|1\rangle)$ and $|\chi_0\rangle, |\chi_1\rangle$ $(= \mathbf{v}|0\rangle, \mathbf{v}|1\rangle)$ — 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) Since the orthogonality of two state vectors is unaffected if either of them is multiplied by any scalar, all that matters is that the two members of each pair be orthogonal — they need not be unit vectors. Consequently one can rescale the expansion of $|\phi_0\rangle$ and $|\phi_1\rangle$ in the computational basis so that the coefficient of $|0\rangle$ in the expansion of $|\phi_0\rangle$ is 1, as is the coefficient of $|1\rangle$ in the expansion of $|\phi_1\rangle$. This reduces their form to

$$|\phi_0\rangle = |0\rangle + \gamma|1\rangle, \quad |\phi_1\rangle = |1\rangle - \gamma^*|0\rangle, \tag{35}$$

where the coefficient γ of $|1\rangle$ in the expansion of $|\phi_0\rangle$ is arbitrary, but the coefficient of $|0\rangle$ in the expansion of $|\phi\rangle_1$ is then required to be γ^* by the condition that $|\phi_0\rangle$ be orthogonal to $|\phi_1\rangle$. In the same way it is enough to consider $|\chi_0\rangle$ and $|\chi_1\rangle$ of the form

$$|\chi_0\rangle = |0\rangle - \beta^*|1\rangle, \quad |\chi_1\rangle = |1\rangle + \beta|0\rangle. \tag{36}$$

(The case in which the amplitude one divides by to get at the forms (35) or (36) is zero is included in the rest of the argument by taking the limit in which γ or β becomes infinite.)

(iv) The condition that $|\phi_0\rangle \otimes |\chi_1\rangle$ be orthogonal to $|\Phi\rangle$ gives

$$\alpha_{00}\beta^* + \alpha_{01} + \alpha_{10}\beta^*\gamma^* + \alpha_{11}\gamma^* = 0, \tag{37}$$

while the condition that $|\phi_1\rangle \otimes |\chi_0\rangle$ be orthogonal to $|\Phi\rangle$ gives

$$-\alpha_{00}\gamma + \alpha_{01}\beta\gamma + \alpha_{10} - \alpha_{11}\beta = 0. \tag{38}$$

Eq. (38) together with the complex conjugate of (37),

$$\alpha_{00}^*\beta + \alpha_{01}^* + \alpha_{10}^*\beta\gamma + \alpha_{11}^*\gamma = 0, \tag{39}$$

gives two equations for the two unknowns α and β. Eq. (38) gives γ in terms of β:

$$\gamma = \frac{\alpha_{10} - \alpha_{11}\beta}{\alpha_{00} - \alpha_{01}\beta}. \tag{40}$$

Using (40) to eliminate γ from (39) gives a quadratic equation for β. Since quadratic equations always have at least one complex solution, that solution, together with (40) gives us β and γ, therefore the required pairs $|\phi_0\rangle, |\phi_1\rangle$ and $|\chi_0\rangle, |\chi_1\rangle$, and therefore the unitary transformations $\mathbf{u}$ and $\mathbf{v}$.