Out: March 16, 2001.
To be submitted one week later, in class.

PROBLEM SET 1

1. Quantum vs. classical Correlations.

   (a) Alice, Bob and Charlie share an arbitrarily long common random string. Each of them is given one bit as an input: we denote the input bits by X_A, X_B, and X_C, respectively. The bits are chosen uniformly at random conditioned that $X_A \oplus X_B \oplus X_C = 0$. Without communicating with each other, Alice, Bob and Charlie wish to output bits a, b and c respectively such that $x_A \vee x_B \vee x_C = a \oplus b \oplus c$. Prove that the best protocol that Alice, Bob and Charlie follow has success probability 3/4.

   Solution: the string X_A, X_B, X_C can be one of four: 011 or 110 or 101 or 000. Each happens with probability 1/4. The players are shooting for $a \oplus b \oplus c = 1$ in the first three cases and 0 in the fourth case. An easy deterministic protocol for the players is to output $a = b = c = 1$ regardless of their inputs. $a \oplus b \oplus c$ is then always 1. The protocol will err only in the last case, i.e. it has probability 3/4 to succeed.

   We now prove that any deterministic protocol is wrong in at least 1/4 the cases. We denote by a_0 the bit which Alice outputs if $X_A = 0$ (we can do this because a_0 is deterministic) We denote by a_1 the bit which Alice outputs if $X_A = 1$, and similarly we denote by b_0, b_1 the bit which Bob output if $X_B = 0$, $X_B = 1$ respectively, and in the same way we define c_0, c_1.

   We now write the output in the four cases ($X_A, X_B, X_C = 011, 110, 101$ or 000) and near it we write the correct expected result of the protocol, $X_A \vee X_B \vee X_C$.

$$
\begin{array}{ll}
a_0 \oplus b_1 \oplus c_1 & 0 \vee 1 \vee 1 = 1 \\
a_1 \oplus b_1 \oplus c_0 & 1 \vee 1 \vee 0 = 1 \\
a_1 \oplus b_0 \oplus c_1 & 1 \vee 0 \vee 1 = 1 \\
a_0 \oplus b_0 \oplus c_0 & 0 \vee 0 \vee 0 = 0
\end{array}
$$

   We take exclusive or of all the outputs on the left hand side. Since each value appears exactly twice, this exclusive or is 0, regardless of the value of each of the variables. Now, if the four outputs are correct, then there is equality between the left hand side and the right hand side of the above expressions. But if we take the exclusive or of the right hand side we get 1! Hence, this is a contradiction; There must be at least one expression where there is inequality, which means that any deterministic protocol will have at most 3/4 probability to be correct.

   It remains to prove that this is true also for any probabilistic protocol. In a Classical probabilistic protocol there is a public random string of bits, and also the players can each toss private coins. Without loss of generality, we can assume that Alice and Bob the private coins are part of the public string; this can only make the players lives easier. Given a random string r, the protocol performs some deterministic process. Hence, a probabilistic protocol D can be viewed as a probability distribution $Pr(r)$ over deterministic protocols D_r and so

$$Pr_{r,X_A,X_B,X_C}(D \ \ Succeeds) = \sum_r Pr_r(Pr_{X_A,X_B,X_C}(D_r Succeeds))$$

But we know from before that $Pr_{X_A,X_B,X_C}(D_r Succeeds) \leq 3/4$ since D_r is deterministic.

(b) Alice, Bob and Charlie share a Greenberger-Horne-Zeilinger state (called a GHZ state) of 3 qubits:

$$\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle).$$

They are given as input bits X_A, X_B, X_C respectively, which satisfy the condition $X_A \oplus X_B \oplus X_C = 0$. They wish to output a, b, c s.t. $X_A \vee X_B \vee X_C = a \oplus b \oplus c$. In contrast to the classical case, there is a quantum protocol which achieves this with certainty. Find one and show that it works. Hint: The only quantum operations that are needed are measurements of one qubit, in either the standard basis, $|0\rangle, |1\rangle$, or the Hadamard basis: $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

Solution: The strategy of all players is the same. We will state it for Alice: If $X_A = 0$ Alice performs a measurements in the standard basis. Alice outputs $a = 0$ if the qubit measured collapses to $|0\rangle$, and outputs $a = 1$ if the qubit measured collapses to $|1\rangle$. If $X_A = 1$ Alice performs a measurements in the Hadamard basis

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

Alice outputs $a = 0$ if the qubit measured collapses to $|+\rangle$, and outputs $a = 1$ if the qubit measured collapses to $|-\rangle$. Bob and Charlie perform exactly the same protocol, with their bits and qubits.

We now prove that in all cases, $a \oplus b \oplus c = X_A \vee X_B \vee X_C$. First, if $X_A = X_B = X_C = 0$, all the players measure in the standard basis. This means that the GHZ state collapses to one of the basis states participating in it. Since the xor of the bits in each of these strings is 0, we get in this case that $0 = a \oplus b \oplus c = X_A \vee X_B \vee X_C$. We now analyze the case in which two of the players received input 1 and the last one is 0. Since the GHZ state is symmetric to permutations of the qubits, it suffices to analyze just one case, say $X_A = X_B = 1, X_C = 0$. We will write the GHZ state in the basis of measurements, i.e. we will leave Charlie's qubit in the standard basis but change the basis to the Hadamard basis for Alice's and Bob's qubits. This means that we write the GHZ state in terms of the basis $\{|++0\rangle, |++1\rangle, |+-0\rangle, |+-1\rangle, |-+0\rangle, |-+1\rangle, |--0\rangle, |--1\rangle\}$. The measurements will then collapse the state to one of these basis states. The result of the protocol will be correct if the total number of 1's and $-$'s in this basis state is odd. Thus, it suffices to show that there is zero probability to get a state in which the total number of 1's and $-$'s is even. In other words, it suffices to show that the coefficient in front of any of the four basis states $\{|++0\rangle, |+-1\rangle, |-+1\rangle, |--0\rangle\}$. is 0, or that the inner product between the GHZ state and any of these basis states is zero. We will demonstrate this for the first basis state $|++0\rangle$:

$$(|++0\rangle, 1/2(|000\rangle - |011\rangle - |101\rangle - |110\rangle)) = 1/2(\langle ++|00\rangle - \langle ++|11\rangle) = 1/2((\langle +|0\rangle)^2 - (\langle +|1\rangle)^2)$$

which is zero since $\langle +|0\rangle = \langle +|1\rangle$.

2. Tensor Product.

(a) Consider the gate CNOT on two qubits. CNOT applies a Not on one qubit, called the target qubit, conditioned that the other qubit, called the control qubit, is 1. We say we apply CNOT "from" the control qubit "to" the target qubit. We write CNOT(a,b) to indicate that we apply it from a to b. Write $CNOT(1,2)$ and

$CNOT(2,1)$ in matrix form, as matrices operating on the Hilbert space of two qubits.

Solution:

$$CNOT(1,2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, CNOT(2,1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

(b) Consider two vector spaces, A, B and their tensor product $A \otimes B$. Let the matrices M_A, M_B operate on A, B respectively. To define the matrix tensor product $M_A \otimes M_B$ we require that for all the vectors $|\alpha\rangle \in A, |\beta\rangle \in B$, $M_A \otimes M_B(|\alpha\rangle \otimes (|\beta\rangle)) = M_A|\alpha\rangle \otimes M_B(|\beta\rangle)$. (This requirement means that the mapping from A, B to $A \otimes B$ commutes with the application of the matrices M_A, M_B). Prove that this requirement implies that $(M_A \otimes M_B)_{ij,kl} = (M_A)_{i,k}(M_B)_{j,l}$ with i, k running over basis states of A, j, l running over B.

Solution:

Let us see how $M_A \otimes M_B$ looks like, written in the standard basis for tensor products: $|i\rangle \otimes |j\rangle$. We know that for any matrix A, we can write its matrix element A_{kl} as $(A|l\rangle)_k$, i.e. the matrix multiplied by the l's basis vector, and taking the k'th coordinate in the resulting vector. Applying this general rule, we get: $(M_A \otimes M_B)_{ij,i'j'} = (M_A \otimes M_B(|i'\rangle \otimes |j'\rangle))_{ij}$ We know by the requirement that this is equal to $(M_A|i'\rangle \otimes M_B(|j'\rangle)_{ij}$ So we have to show that the i, j coefficient of this vector is equal to $M_A)_{i,i'}(M_B)_{j,j'}$.

$M_A|i'\rangle$ is simply the i' column of M_A, i.e. $M_A|i'\rangle = \sum_i (M_A)_{i,i'}|i\rangle$ and $M_B|j'\rangle = \sum_j (M_B)_{j,j'}|j\rangle$ and by linearity of the tensor product of vectors, we have that the vector is $M_A|i'\rangle \otimes M_B(|j'\rangle = \sum_i (M_A)_{i,i'}|i\rangle \otimes \sum_j (M_B)_{j,j'}|j\rangle = \sum_i \sum_j (M_A)_{i,i'}(M_B)_{j,j'}|i\rangle \otimes |j\rangle$ and so the ij coefficient of this vector is simply $(M_A)_{i,i'}(M_B)_{j,j'}$.

(c) Find the matrix form of $R_\theta(2) \otimes CNOT(3,1)$, i.e. $R_\theta(2)$ operating on the second qubit and $CNOT$ operating from the third qubit to the first. (The names of qubits mean the following: We write the matrix in the basis states $|m, n, q\rangle$ with $m, n, q \in \{0, 1\}$. The first coordinate m corresponds to the first qubit; Since we consider $CNOT(3,1)$ m should run over the basis states of the target qubit. The second coordinate n corresponds to the second qubit, and since we want R_θ to be applied on the second qubit, n should run over the coordinates on which R_θ operates. The last coordinate q corresponds to the third qubit, so it should run over the basis states of the control qubit.)

Solution:

Let us denote $c = cos(\theta), s = sin(\theta)$. Let $U = R_\theta(2) \otimes CNOT(3,1)$. We give several ways to compute U.

First, by the previous exercise, $U_{abc,a'b'c'} = (R_\theta)_{b,b'}CNOT_{ca,c'a'}$. Where the CNOT is the first matrix in item a. (the conventional CNOT, where the first qubit is the controlled qubit.) As an example, $U_{001,111} = R_{0,1}CNOT_{10,11} = -s$.

Another way of calculating how the matrix looks like is to find out what happens to each basis state. For example:

$$|001> \longmapsto |\alpha> = |1> (c|0> + s|1>)|1> .$$

This gives the second column of the matrix.

We can calculate how each column looks like so we get:

$$\begin{pmatrix} c & 0 & -s & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c & 0 & -s \\ s & 0 & c & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & s & 0 & c \\ 0 & 0 & 0 & 0 & c & 0 & -s & 0 \\ 0 & c & 0 & -s & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & s & 0 & c & 0 \\ 0 & s & 0 & c & 0 & 0 & 0 & 0 \end{pmatrix}$$

One last way to compute this matrix is to calculate $R \otimes CNOT$, as if the R operates on the first qubit and the CNOT operates on the second and third qubits. When the tensor products appear in the correct order, the matrices look like blocks, and calculating the tensor product is very simple: One just multiplies each element from the first matrix by the entire second matrix. This will give:

$$\begin{pmatrix} c & 0 & 0 & 0 & -s & 0 & 0 & 0 \\ 0 & c & 0 & 0 & 0 & -s & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & 0 & -s \\ 0 & 0 & c & 0 & 0 & 0 & -s & 0 \\ s & 0 & 0 & 0 & c & 0 & 0 & 0 \\ 0 & s & 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & s & 0 & 0 & 0 & c \\ 0 & 0 & s & 0 & 0 & 0 & c & 0 \end{pmatrix}$$

The problem is that this matrix applies R on the first qubit and CNOT from the second qubit to the third, and we want to rename the qubits. $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. This gives the following order of the basis state:

$$000, 001, 010, 011, 100, 101, 110, 111 \; - - > 000, 100, 001, 101, 010, 110, 011, 111$$

Since we want to reorder the raws and the columns, we have to multiply the matrix from both sides by a permutation matrix, which calculates the correct permutation on the basis states, on the raws and columns.

Raw and Col 000 in the correct matrix remain as they are. Raw and Col 001 in the new matrix are Raw and Col 010 in the old matrix. Raw and Col 010 in the new matrix are Raw and Col 100 in the old matrix. Raw and Col 011 in the new matrix are Raw and Col 110 in the old matrix. Raw and Col 100 in the new matrix are Raw and Col 001 in the old matrix. Raw and Col 101 in the new matrix are Raw and Col 011 in the old matrix. Raw and Col 110 in the new matrix are Raw and Col 101 in the old matrix. Raw and Col 111 in the new matrix are Raw and Col 111 in the old matrix.

We will not do it here; The main reason I explain this is not because this method is simpler (it is not) but because it explains the notion of tensor products, and the notion of applying matrices on different bits. Make sure you understand what needs to be done; You don't have to do it.

(d) Prove that $(W \otimes U)(W' \otimes U') = (WW') \otimes (UU')$.

Solution:

$(W \otimes U)(W' \otimes U')_{ij,kl} = \sum_{m,n}(W \otimes U)_{ij,mn}(W' \otimes U')_{mn,kl} =$
$\sum_{m,n} W_{i,m}U_{j,n}W'_{m,k}U'_{n,l} = \sum_{m,n} W_{i,m}W'_{m,k}U_{j,n}U'_{n,l} = \sum_m W_{i,m}W'_{m,k}\sum_n U_{j,n}U'_{n,l} =$
$(WW')_{i,k}(UU')_{j,l} = (WW') \otimes (UU')_{ij,kl}$

(e) Suppose W and U are two gates, each operating on one qubit. The extension of a one qubit gate to the Hilbert space of two qubits is achieved by tensor product with identity on the second qubit: $\tilde{U}(1) = U(1) \otimes I(2)$. Prove that the process which first applies W on the first qubit and then U on the second qubit, is equivalent to the reverse order process, which first applies U on second qubit and then W on first qubit.

Solution: From the previous exercise,

$$(U \otimes I)(I \otimes W) = U \otimes W$$

and also

$$(I \otimes W)(U \otimes I) = U \otimes W$$

so they are equal.

(f) Let $|\alpha\rangle, |\alpha^\perp\rangle$ be an orthonormal basis for one qubit, and $|\beta\rangle, |\beta^\perp\rangle$ be another such basis. Prove that given any state of two qubits, the order of applying a measurement in the α basis on the first qubit, and a measurement in the β basis on the second qubit, does not matter, i.e. the joint distribution on the classical and quantum outcomes is the same.

Solution: As a basis for the joint Hilbert space we use: $|\alpha\rangle \otimes |\beta\rangle, |\alpha\rangle \otimes |\beta^\perp\rangle, |\alpha^\perp\rangle \otimes |\beta\rangle, |\alpha^\perp\rangle \otimes |\beta^\perp\rangle$. We write the state in this basis. Suppose we first measure the first qubit and then the second. Let the result of the first measurement (α or $\alpha^\perp$) be denoted a, and the result of the first measurement (β or $\beta^\perp$) be denoted b. The probability to get the result a in the first measurement is:

$$Pr(a) = |C_{a,\beta}|^2 + |C_{a,\beta^\perp}|^2$$

Given that the result is a, the state collapses to

$$1/\sqrt{Pr(a)}(C_{a,\beta}|a\rangle \otimes |\beta\rangle + C_{a,\beta^\perp}|a\rangle \otimes |\beta^\perp\rangle),$$

where the factor $1/\sqrt{Pr(a)}$ is for normalization. The probability that this state will output b is now

$$Pr(b|a) = 1/Pr(a)|C_{a,b}|^2$$

So when we first measure a and then b:

$$Pr(a,b) = Pr(a)Pr(b|a) = |C_{a,b}|^2.$$

By the same argument we can show that

$$Pr(a,b) = |C_{a,b}|^2$$

also when we measure first b and then a, and so the two probabilities are equal.

3. Closeness of states implies closeness of classical outcomes.

Consider two states of n qubits, $|\phi_1\rangle, |\phi_2\rangle$ which are close, $\| |\phi_1\rangle - |\phi_2\rangle \| = \epsilon$. Consider a measurement (in any orthonormal basis) of the two states. Let D_1, D_2 be the two distributions on the classical outcomes of the measurement applied on $|\phi_1\rangle, |\phi_2\rangle$, respectively.

Prove that the total variation distance between D_1, D_2 is at most ϵ. Prove that this is true also in the case of performing a partial measurement, i.e. measuring only a subset of the qubits.

Solution: Let $|\phi_1\rangle = \sum_i c_i|i>, |\phi_2\rangle = \sum_i d_i|i>$. Then, if all qubits are measured,

$$|D_1 - D_2| = 1/2\sum_i ||c_i|^2 - |d_i|^2| = 1/2\sum_i (||c_i| - |d_i||)(||c_i| + |d_i||)$$

Using Cauchy Schwartz, we get

$$\leq 1/2\sqrt{\sum_i (|c_i| - |d_i|)^2}\sqrt{\sum_i (|c_i| + |d_i|)^2}$$

Now, $|c_i| - |d_i| \leq |c_i - d_i|$ by triangle inequality, and $|c_i| + |d_i|$ are the coefficients of a vector which is a sum of two vectors, each of norm 1, and hence its Euclidean norm is at most 2. Hence:

$$\leq 1/2\sqrt{\sum_i (|c_i| - |d_i|)^2}\sqrt{\sum_i (|c_i| + |d_i|)^2} \leq \sqrt{\sum_i (|c_i - d_i|)^2}$$

which is exactly the Euclidean norm of $\phi_1 - \phi_2$.

4. Teleportation.

   Give a protocol for teleporting a two qubit system. Does your solution generalize to n qubits?

Solution: We will teleport each of the qubits using the teleportation protocol given in class. We have to show that this works. The point is that teleportation preserves entanglement with the rest of the world- it does not ruin the correlations between the teleported qubit and any other qubit; It simply passes these correlations together with the teleportation.

To show that this works, we note that a general two qubit state can be written as

$$\alpha|0\rangle + \beta|1\rangle$$

where α and β are vectors describing the first qubit. Now, we perform the teleportation procedure, on the second qubit, to a third qubit in Bob's hand. Following the same proof in class, we note that we never used the fact that α and β are scalars. Hence, if they are vectors, it all goes through. This means that after the first teleportation, the state of the first and third qubit is the same as was the state of the first and second qubit. Now we have one "correct" qubit in Bob's hands; We again perform teleportation on the first qubit, and use the same argument, expressing Bob's third qubit's states by α and β.

This of course generalizes to any number of qubits.