Ph219a/CS219a

Solutions
Nov 8, 2013

Problem 2.1

(a) Consider how the protocol works for the special case $n = 1$, ie. when Alice encrypts a single qubit state ρ. The effect of Alice's encryption protocol can then be viewed as a quantum channel which applies one of the Pauli operators or the identity at random, each with probability 1/4. Notice that this channel (which we call $\mathcal{E}_1$) is simply the single qubit depolarizing channel[1] with $p = 3/4$. Recall that the effect of this channel is to map any state into the maximally mixed state -

$$\begin{aligned} \mathcal{E}_1(\rho) &= \frac{1}{4}\sum_{x=0}^{3}\sigma(x)\rho\sigma(x) \\ &= \frac{1}{4}(\rho + \sigma_1\rho\sigma_1 + \sigma_2\rho\sigma_2 + \sigma_3\rho\sigma_3) \\ &= \frac{1}{2}\mathcal{I} \end{aligned} \tag{1}$$

Now, in the case of a general n-qubit encryption, the channel $\mathcal{E}$ is nothing but the channel $\mathcal{E}_1$ acting separately on each qubit, ie. $\mathcal{E} = \mathcal{E}_1^{\otimes n}$. As we know, each qubit gets mapped to the maximally mixed state, in the process destroying all correlations between qubits. Therefore

$$\mathcal{E}(\rho) = (\frac{1}{2}\mathcal{I})^{\otimes n} = \frac{1}{2^n}\mathcal{I}^{\otimes n} \tag{2}$$

(b) If Alice and Bob are to achieve the same result with this new encryption scheme, then the channels $\mathcal{E}'$ and $\mathcal{E}$ must be the same. It follows from the Kraus representation theorem that two different Kraus representations ($\{\frac{1}{2^n}\sigma(x)\}$ and $\sqrt{p_a}U_a$) of this channel ($\mathcal{E}$) must be related by a unitary transformation. Lets call this transformation V, where

$$\sqrt{p_a}U_a = \sum_x V_{ax}\left(\frac{1}{2^n}\sigma(x)\right) \tag{3}$$

Since $\{x\}$ are $2n$-bit strings, there are 2^{2n} Kraus operators in the first representation and N in the second representation (since a takes values from 1 to N). The dimension of V is therefore

[1] See §3.4.1 in http://www.theory.caltech.edu/people/preskill/ph229/notes/chap3.ps

$\max(N, 2^{2n})$ where we add zeros to the shorter set of Kraus operators so that both sets have the same cardinality, $\max(N, 2^{2n})$.
Multiplying both sides of equation(36) by their adjoints and taking the trace, we have,

$$\begin{aligned} \mathrm{Tr}[p_a U_a^\dagger U_a] &= \mathrm{Tr}[\frac{1}{2^{2n}} \sum_{x,y} V_{ax} V_{ay}^* \sigma(x)\sigma(y)] \\ \Rightarrow 2^n p_a &= \frac{1}{2^{2n}} \sum_x 2^n |V_{ax}|^2 \end{aligned} \tag{4}$$

We have simplified the left hand side using the fact that $\{U_a\}$ are unitaries acting on a n-qubit space, so $\mathrm{Tr}[U_a^\dagger U_a] = \mathrm{Tr}[\mathcal{I}] = 2^n$. To see how the right hand side simplifies, recall that single qubit Pauli operators have the property $\sigma_i \sigma_j = 2\delta_{ij}$ ie. they are orthogonal and square to identity. Generalizing this to n-qubits, we have $\sigma(x)\sigma(y) = \mathcal{I}^{\otimes n} \delta_{xy}$ which gives the RHS of equation (37). Thus we have,

$$p_a = \frac{1}{2^{2n}} \sum_x |V_{ax}|^2 \leq \frac{1}{2^{2n}} \tag{5}$$

since we are summing over the elements ath row the unitary matrix of dimension $\max(N, 2^{2n})$, with x ranging from 0 to 2^{2n}.

Problem 2.2

Given, a density operator ρ and a unital map $\mathcal{E}$ with operator elements $\{M_\mu\}$ -

$$\mathcal{E}(\rho) = \sum_\mu M_\mu \rho M_\mu^\dagger \tag{6}$$

Let U be the unitary that diagonalizes ρ into Δ and V diagonalize $\mathcal{E}(\rho)$ into Δ' so that the above equation becomes

$$\begin{aligned} V\Delta' V^\dagger &= \sum_\mu M_\mu U \Delta U^\dagger M_\mu^\dagger \\ \Rightarrow \Delta' &= \sum_\mu N_\mu \Delta N_\mu^\dagger \end{aligned} \tag{7}$$

where $\{N_\mu = V^\dagger M_\mu U\}$ form a set of operator elements for a TPCP, unital map ie.

$$\begin{aligned} \sum_\mu N_\mu^\dagger N_\mu &= U^\dagger \left[\sum_\mu M_\mu^\dagger (V^\dagger V) M_\mu \right] U \\ &= \mathcal{I} \text{ (since } U, V \text{ are unitary, } \mathcal{E} \text{ is TP)} \\ \sum_\mu N_\mu N_\mu^\dagger &= V^\dagger \left[\sum_\mu M_\mu (UU^\dagger) M_\mu^\dagger \right] V \\ &= \mathcal{I} \text{ (since } \mathcal{E} \text{ is unital)} \end{aligned} \tag{8}$$

The eigenvalues of ρ are simply the elements of Δ, ie. $[\lambda(\rho)]_i = \Delta_i$ and $[\lambda(\mathcal{E}(\rho))]_i = \Delta'_i$. Then equation(40) implies

$$\begin{aligned}\Delta'_i &= \sum_\mu \sum_j [N_\mu]_{ij} \Delta_j [N_\mu^\dagger]_{ji} \\ &= \sum_j \left(\sum_\mu [N_\mu]_{ij} [N_\mu^\dagger]_{ji} \right) \Delta_j \\ &= \sum_j D_{ij} \Delta_j \end{aligned} \tag{9}$$

where $D_{ij} = \sum_\mu [N_\mu]_{ij} [N_\mu^\dagger]_{ji}$ is a double stochastic matrix -

$$\begin{aligned}\sum_i D_{ij} &= \sum_i \sum_\mu [N_\mu^\dagger]_{ji} [N_\mu]_{ij} = [\mathcal{I}]_j = 1 \ \text{ (since } \{N_\mu\} \text{ is a TPCP map)} \\ \sum_j D_{ij} &= \sum_j \sum_\mu [N_\mu]_{ij} [N_\mu^\dagger]_{ji} = [\mathcal{I}]_i = 1 \ \text{ (since } \{N_\mu\} \text{ is a unital map)} \end{aligned} \tag{10}$$

Thus we see that $\Delta' \prec \Delta$ which proves that $\mathcal{E}(\rho) \prec \rho$.

Problem 2.3

(a) After Bob's measurement, depending on his outcome, the joint state $|\psi(x)\rangle$ collapses to the state $P_B(|\psi(x)\rangle\langle\psi(x)|)P_B$ where P_B is the projector corresponding to Bob's outcome. Thus when his outcome is 0, the state after measurement is given by

$$\begin{aligned}|\psi(x)\rangle &\rightarrow (|0\rangle\langle 0|)_B (|\psi(x)\rangle\langle\psi(x)|)(|0\rangle\langle 0|)_B \\ &= (|0\rangle\langle 0|)_B \otimes \langle 0_B|\psi(x)\rangle\langle\psi(x)|0_B\rangle \\ &= (|0\rangle\langle 0|)_B \otimes \left(\sqrt{1-2x}\,|0\rangle + \sqrt{x}\,|1\rangle\right)_C \left(\sqrt{1-2x}\,\langle 0| + \sqrt{x}\,\langle 1|\right)_C \\ &= (|0\rangle\langle 0|)_B \otimes (|\phi\rangle\langle\phi|)_C \end{aligned} \tag{11}$$

Normalizing Claire's half of the state, we get the state observed by Claire when Bob's outcome is 0 as -

$$|\phi\rangle = \sqrt{\frac{1-2x}{1-x}}\,|0\rangle + \sqrt{\frac{x}{1-x}}\,|1\rangle \tag{12}$$

We can construct a state orthogonal to $|\phi\rangle$ using the same coefficients -

$$|\phi^\perp\rangle = \sqrt{\frac{x}{1-x}}\,|0\rangle - \sqrt{\frac{1-2x}{1-x}}\,|1\rangle \tag{13}$$

[Note: Given a state $a|0\rangle + b|1\rangle$, one can always construct an orthogonal state $b*|0\rangle - a*|1\rangle$.]
(b)Probability of both Bob and Claire obtaining the outcome $|\phi^\perp\rangle$ is

$$\begin{aligned}P(x) &= |\left(\langle\phi_B^\perp|\langle\phi_C^\perp|\right)|\psi(x)\rangle_{BC}|^2 \\ &= \left|\left(\frac{x}{1-x}\langle 00| + \frac{1-2x}{1-x}\langle 11| - \frac{\sqrt{x(1-2x)}}{1-x}\langle 01| - \frac{\sqrt{x(1-2x)}}{1-x}\langle 10|\right)\left(\sqrt{1-2x}\,|00\rangle + \sqrt{x}\,|01\rangle + \sqrt{x}\,|10\rangle\right)\right|^2 \\ &= \frac{x^2(1-2x)}{(1-x)^2} \end{aligned}$$

(c) To compute the maximum value of $P(x)$:

$$\begin{aligned} P'(x)|_{x=x^*} &= \frac{2x}{(1-x)^3}\left(x^2-3x+1\right)|_{x=x^*}=0 \\ \Rightarrow x^* &= \frac{1}{2}\left(3\pm\sqrt{5}\right) \text{ or } \; x^*=0 \end{aligned} \tag{14}$$

The only non-trivial critical point that lies in the interval ($0 \leq x \leq \frac{1}{2}$) is $x^* = \frac{3-\sqrt{5}}{2}$. Plugging this value in the expression for $P(x)$ we find the maximal value of probability as $P(x^*) = \frac{5\sqrt{5}-11}{2}$.

(d) Albert's reasoning went wrong because it was counterfactual - when Bob and Claire choose to measure in the $\{|\phi\rangle\,|\phi^\perp\rangle\}$ basis, he makes a prediction about what might have happened if they had measured in the $\{|0\rangle, |1\rangle\}$ basis instead. This is possible only if the joint probability distributions corresponding to their measurements can be drawn from an underlying hidden variable model. Since the two sets of bases are non-commuting, there is no such local hidden variable theory and hence Albert's counterfactual reasoning goes wrong.

Notice that the fact that they shared state is entangled does not by itself imply incompatibility with local hidden variable theories - as long as they consider commuting commuting observables, Albert can construct a hidden variable theory to explain the correlations of the outcomes. For example, when $x = 0$ and $x = \frac{1}{2}$, the $\{|\phi\rangle\,, |\phi^\perp\rangle\}$ basis is identical with the $\{|0\rangle\,, |1\rangle\}$ basis and $P(x) = 0$ as predicted by Albert. But while $|\psi(0)\rangle$ is a product state, $|\psi(\frac{1}{2})\rangle$ is an entangled state!

Problem 2.4

(a) For variables $x, x', y, y' \in \{0, 1\}$ we need to show $xy + xy' + x'y - x'y' \leq x + y$. We can do this in one of two alternate ways (without enumerating all 16 possibilities!):

(i) Note that for the variables defined as above, $xy \leq x$, $xy \leq y$ etc. Now let $y' = 1$. Then

$$\begin{aligned} xy + xy' + x'y - x'y' &= xy + x + x'y - x' \\ &\leq y + x + x' - x' = x + y \end{aligned} \tag{15}$$

Similarly, if $y' = 0$, we have,

$$xy + xy' + x'y - x'y' = xy + x'y \leq x + y \tag{16}$$

thus proving the inequality.

(ii) Alternately, recall the CHSH inequality: $\alpha\beta+\alpha'\beta+\alpha\beta'-\alpha'\beta' \leq 2$ for $\alpha, \alpha', \beta, \beta' \in \{-1, 1\}$. Now define $\alpha = (2x - 1)$, $\alpha' = 2x' - 1$, $\beta = 2y - 1$ and $\beta' = 2y' - 1$. Notice that $\alpha, \beta, \alpha', \beta'$ defined take values ± 1 so they satisfy the CHSH inequality. This gives us

$$\begin{aligned} (2x-1)(2y-1) + (2x'-1)(2y-1) + (2x-1)(2y'-1) - (2x'-1)(2y'-1) &\leq 2 \\ \Rightarrow 4xy + 4xy' + 4x'y - 4x'y' - 4x - 4y + 2 &\leq 2 \\ \Rightarrow 4(xy + xy' + x'y - x'y') - 4(x + y) &\leq 0 \\ \Rightarrow xy + xy' + x'y - x'y' &\leq x + y \end{aligned}$$

(b) Let first write down the probabilities $P_{++}(ab)$ etc. in terms of x, y, x' and y' -
Recall that the variable $x \in \{0,1\}$ indicates whether or not Alice's detector clicks when she measures a, $y \in \{0,1\}$ denotes whether or not Bob's detector clicks when he measures b and similarly x' for measurement a' and y' for measurement b'. $P_{++}(ab)$ which denotes the joint probability of both detectors clicking when Alice measures a and Bob measures b, is simply the probability that $x \wedge y = xy = 1$ ie. $P_{++}(ab) = p(x = y = 1)$. Similarly, $P_{++}(ab') = p(x = y' = 1)$ etc. $P_{+.}(a)$ is the probability that $x = 1$, independent of the values of y or y' ie. $P_{+.}(a) = p(x = 1)$ and $P_{+.}(b) = p(y = 1)$.
Now taking the average on both sides of the inequality of part(a), we have,

$$\langle xy + xy' + x'y - x'y' \rangle \leq \langle x + y \rangle \tag{17}$$

Since $< xy >= (0)p(x = y = 0) + (0)p(x = 0, y = 1) + (0)p(x = 1, y = 0) + (1)p(x = y = 1) = p(x = y = 1)$, this implies,

$$p(x = y = 1) + p(x = y' = 1) + p(x' = y = 1) - p(x' = y' = 1) \leq p(x = 1) + p(y = 1) \tag{18}$$

Now using our expressions for $P_{++}(ab)$ in term of x, y, x', y' this immediately gives the desired relation:

$$P_{++}(ab) + P_{++}(ab') + P_{++}(a'b) - P_{++}(a'b') \leq P_{+.}(a) + P_{+.}(b) \tag{19}$$

(c) Since Alice and Bob's detectors are such that they click only when the variables $\{a, a', b, b'\}$ take the value $+1$, with efficiency η_A and η_B respectively, the probabilities in (9) can be written as -

$$\begin{aligned} P_{++}(ab) &= \eta_A \eta_B p(a = 1 = b) \;\; P_{++}(ab') = \eta_A \eta_B p(a = b' = 1) \\ P_{++}(a'b) &= \eta_A \eta_B p(a' = b = 1) \;\; P_{++}(a'b') = \eta_A \eta_B p(a' = b' = 1) \end{aligned} \tag{20}$$

where $p(a = b = 1)$ is the joint probability that measurements a and b result in outcome 1, etc. We compute these probabilities using the given settings, which achieve maximal violation of the CHSH inequality ie. $a = \hat{x} = \sigma_1$, $a' = \hat{z} = \sigma_3$, $b = \frac{1}{\sqrt{2}}(\hat{x} + \hat{z})$, $b' = \frac{1}{\sqrt{2}}(\hat{x} - \hat{z})$ and Alice and Bob share the maximally entangled state $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (written in the eigenbasis for $\hat{z}$).

$$\begin{aligned} p(a = b = 1) &= \left\langle \phi^+ \right| \left(\frac{[I_A + \sigma_1^A]}{2} \otimes \frac{[I + \frac{1}{\sqrt{2}}(\sigma_1^B + \sigma_3^B)]}{2} \right) \left| \phi^+ \right\rangle = \frac{1}{4\sqrt{2}(\sqrt{2} - 1)} \\ p(a = b' = 1) &= \left\langle \phi^+ \right| \left(\frac{[I_A + \sigma_1^A]}{2} \otimes \frac{[I + \frac{1}{\sqrt{2}}(\sigma_1^B - \sigma_3^B)]}{2} \right) \left| \phi^+ \right\rangle = \frac{1}{4\sqrt{2}(\sqrt{2} - 1)} \\ p(a = b' = 1) &= \left\langle \phi^+ \right| \left(\frac{[I_A + \sigma_3^A]}{2} \otimes \frac{[I + \frac{1}{\sqrt{2}}(\sigma_1^B + \sigma_3^B)]}{2} \right) \left| \phi^+ \right\rangle = \frac{1}{4\sqrt{2}(\sqrt{2} - 1)} \\ p(a = b' = 1) &= \left\langle \phi^+ \right| \left(\frac{[I_A + \sigma_3^A]}{2} \otimes \frac{[I + \frac{1}{\sqrt{2}}(\sigma_1^B - \sigma_3^B)]}{2} \right) \left| \phi^+ \right\rangle = \frac{1}{4\sqrt{2}(\sqrt{2} + 1)} \end{aligned} \tag{21}$$

Thus, (9) is violated only if

$$\frac{\eta_A \eta_B}{\eta_A + \eta_B} > \frac{1}{1 + \sqrt{2}} \tag{22}$$

Problem 2.5

(a) To show $[q \to q] \geq [q \to qq] \geq [c \to c]$ -
Given her input qubit $|x\rangle_A$, Alice prepares the state $|xx\rangle_{AA'}$ - this can be done using a CNOT gate[2] with Alice's input qubit as the control bit and $|0\rangle$ as the target so that $|x0\rangle_A \to |xx\rangle_A$. Alice then sends the second qubit to Bob ($|x\rangle_{A'} \to |x\rangle_B$), thus achieving $|x\rangle_A \to |x\rangle_A \otimes |x\rangle_B$. This shows that Alice can use her ability to send a qubit to Bob ($[q \to q]$), combined with a local operation (a CNOT in this case) to send a cobit ($[q \to qq]$) to him.
Finally, Alice throws away her part of the state ($|x\rangle_A \to |x\rangle_E$) to simulate sending a cbit ($[c \to c]$) to Bob.
To show $[q \to qq] \geq [qq]$ - To share an entangled state (creating an ebit), Alice prepares a superposition state and sends a cobit to Bob so that $(|0\rangle + |1\rangle)_A \to (|00\rangle + |11\rangle)_{AB}$
(b) Alice and Bob share the Bell pair $|\phi^+\rangle$. Starting with her 2-qubit state $|xy\rangle_A$, Alice applies a unitary to her half of the Bell state, conditioned on her 2-qubit state as follows: $(\sigma_3^x \sigma_1^y \otimes \mathcal{I}) |\phi^+\rangle$ ie. she does a controlled **Z** gate with her first qubit as the control bit and a controlled **X** gate with her second qubit as the control and her half of the Bell state as the target in both cases. Alice then sends her half of the state to Bob. Alice's local operation applied one of the 3 Pauli operators or the identity operator on her half of the state. Thus Bob will have now one of the four Bell states (upto a normalization constant) depending on Alice's input state.
To transform his 2-qubit state into Alice's input state, Bob applies a CNOT gate followed by the Hadamard gate: $(\mathbf{H} \otimes \mathcal{I})\text{CNOT}(\sigma_3^x \sigma_1^y \otimes \mathcal{I}) |\phi^+\rangle$. This combination transforms the entangled Bell basis back into the standard basis:

$$\begin{aligned}
(\mathbf{H} \otimes \mathcal{I})\text{CNOT} \left|\phi^+\right\rangle &= \frac{1}{\sqrt{2}}(\mathbf{H} \otimes \mathcal{I})(|0\rangle + |1\rangle) |0\rangle = |0\rangle |0\rangle \\
(\mathbf{H} \otimes \mathcal{I})\text{CNOT} \left|\psi^+\right\rangle &= \frac{1}{\sqrt{2}}(\mathbf{H} \otimes \mathcal{I})(|0\rangle + |1\rangle) |1\rangle = |0\rangle |1\rangle \\
(\mathbf{H} \otimes \mathcal{I})\text{CNOT} \left|\psi^-\right\rangle &= \frac{1}{\sqrt{2}}(\mathbf{H} \otimes \mathcal{I})(|0\rangle - |1\rangle) |0\rangle = |1\rangle |0\rangle \\
(\mathbf{H} \otimes \mathcal{I})\text{CNOT} \left|\phi^-\right\rangle &= \frac{1}{\sqrt{2}}(\mathbf{H} \otimes \mathcal{I})(|0\rangle - |1\rangle) |1\rangle = |1\rangle |1\rangle
\end{aligned} \tag{23}$$

Thus if Alice and Bob share an ebit and have the ability to send and receive a qubit, they can send a 2cobits between them, ie. $[q \to q] + [qq] \geq [q \to qq]$ with the local operations $U_A = \sigma_3^x \sigma_1^y$ and $U_B = (\mathbf{H} \otimes \mathcal{I})\text{CNOT}$.
(c) Say, Alice wants to coherently teleport the state $|\psi\rangle_A$, given that Alice and Bob share the Bell state $|\phi^+\rangle$. Recall that the state $|\psi\rangle_A |\phi^+\rangle_{AB}$ can be rewritten as

$$|\psi\rangle_A \left|\phi^+\right\rangle_{AB} = \frac{1}{2} \left|\phi^+\right\rangle_A |\psi\rangle_B + \frac{1}{2} \left|\psi^+\right\rangle_A \sigma_1 |\psi\rangle_B + \frac{1}{2} \left|\psi^-\right\rangle_A (-i\sigma_2) |\psi\rangle_B + \frac{1}{2} \left|\phi^-\right\rangle_A \sigma_3 |\psi\rangle_B \tag{24}$$

Alice applies the unitary $V_A = \mathbf{H} \otimes \mathcal{I})\text{CNOT}(= U_B)$ which as we know transforms the Bell basis into the standard basis. Once she sends 2 cobits to Bob, their joint state becomes

$$\frac{1}{2} \sum_{x,y \in \{0,1\}} |xy\rangle_A |xy\rangle_B \sigma_3^x \sigma_1^y |\psi\rangle_B \tag{25}$$

[2]See section §4.1.1 to recall the action of the CNOT and Hadamard gates

Now Bob applies σ_3 conditioned on x and σ_1 conditioned on y, ie. $V_B = U_A$. This gives the final state

$$\begin{aligned} \frac{1}{2} \sum_{x,y \in \{0,1\}} |xy\rangle_A |xy\rangle_B |\psi\rangle_B &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}) |\psi\rangle_B \\ &= \left|\phi^+\right\rangle^{\otimes 2} |\psi\rangle_B \end{aligned} \tag{26}$$

showing that they wind up with two ebits in the end, and Alice succeeds in teleporting her state.