# Ph 219a/CS 219a

**Exercises**
**Due: Wednesday 6 November 2013**

## 2.1 The price of quantum state encryption

Alice and Bob are working on a top secret project. I can't tell you exactly what the project is, but I will reveal that Alice and Bob are connected by a perfect quantum channel, and that Alice uses the channel to send quantum states to Bob. Alice and Bob are worried that an eavesdropper (Eve) might intercept some of Alice's transmissions. By measuring the intercepted quantum state, Eve could learn something about what Alice is sending, and perhaps make an inference about the nature of the project.

To protect against eavesdropping, Alice and Bob decide to *encrypt* the quantum states that Alice sends. They share a *secret key*, a string of random bits about which the eavesdropper knows nothing. By consuming $2n$ bits of secret key, Alice can encrypt, and Bob can decrypt, an arbitrary $n$-qubit state $\rho$. For every possible state $\rho$, the encrypted state looks exactly the same to Eve, so she cannot find out anything about $\rho$.

Here is how the encryption procedure works: We may express the $2n$ bit string $x$ as $x = x_1 x_2 \cdots x_n$, where $x_i \in \{0, 1, 2, 3\}$, and denote a tensor product of $n$ Pauli operators as

$$\sigma(x) = \sigma_{x_1} \otimes \sigma_{x_2} \otimes \cdots \otimes \sigma_{x_{n-1}} \otimes \sigma_{x_n} \tag{1}$$

(where $\sigma_0 = I$). Note that $\sigma(x)^2 = I^{\otimes n}$, the identity operator acting on $n$ qubits. To encrypt, Alice consults her random string to determine $x$ (which is chosen uniformly at random), and applies $\sigma(x)$ to the state, obtaining $\sigma(x)\rho\sigma(x)$. To decrypt, Bob, consults the same string and applies $\sigma(x)$ to recover $\rho$.

*a*) Since Eve does not know the secret key, to her the encrypted state is indistinguishable from

$$\mathcal{E}(\rho) = \frac{1}{2^{2n}} \sum_x \sigma(x)\rho\sigma(x) \; . \tag{2}$$

Show that, for any $n$-qubit state $\rho$

$$\mathcal{E}(\rho) = \frac{1}{2^n} I^{\otimes n} \ . \tag{3}$$

Since $\mathcal{E}(\rho)$ is independent of $\rho$, no information about $\rho$ is accessible to Eve.

*b*) Alice wonders if it is possible to encrypt the state using a shorter key. Alice and Bob could use their shared randomness to sample an arbitrary probability distribution. That is, they could agree on a set of $N$ unitary matrices $\{U_a, a = 1, 2, 3, \ldots, N\}$, and Alice could encrypt by applying $U_a$ with probability $p_a$. Then Bob could decrypt by applying $U_a^{-1}$. To Eve, the encrypted state would then appear to be

$$\mathcal{E}'(\rho) = \sum_a p_a U_a \rho U_a^{-1} \ . \tag{4}$$

Show that, if $\mathcal{E}'(\rho) = I^{\otimes n}$, then $p_a \leq 2^{-2n}$ for each $a$.

**Hint**: Note that $\mathcal{E}$ has an operator sum representation with Kraus operators $\{\sigma(x)/2^n\}$ and that $\mathcal{E}'$ has an operator sum representation with Kraus operators $\{\sqrt{p_a}\, U_a\}$. Furthermore $\mathcal{E} = \mathcal{E}'$. Therefore, there exists an $M \times M$ unitary matrix $V_{ax}$ (where $M = \mathrm{Max}(N, 2^{2n})$ such that $\sqrt{p}_a U_a = \sum_x V_{ax}\sigma(x)/2^n$. Now express $p_a \mathrm{tr}\left(U_a U_a^\dagger\right)$ in terms of $V$.

**Remark**: The result shows that encryption requires $N \geq 2^{2n}$, and that at least $2n$ bits of key are required to specify $U_a$. Thus the encryption scheme in which $\sigma(x)$ is applied is the most efficient possible scheme. (For encryption to be effective, it is enough for $\mathcal{E}(\rho)$ to be independent of $\rho$; it is not necessary that $\mathcal{E}(\rho) = I^{\otimes n}/2^n$. But the same result applies under the weaker assumption that $\mathcal{E}(\rho)$ is independent of $\rho$.)

### 2.2 Unital maps and majorization

Recall that the action of a trace-preserving completely positive (TPCP) map $\mathcal{E}$ can be expressed as

$$\mathcal{E}(\rho) = \sum_\mu M_\mu \rho M_\mu^\dagger \ , \tag{5}$$

where

$$\sum_\mu M_\mu^\dagger M_\mu = I \ . \tag{6}$$

A TPCP map is said to be *unital* if $\mathcal{E}(I) = I$, or equivalently if

$$\sum M_\mu M_\mu^\dagger = I \ . \tag{7}$$

If $A$ is a nonnegative Hermitian operator with unit trace ($\mathrm{tr}\ A = 1$), let $\lambda(A)$ denote the vector of eigenvalues of $A$, which can be regarded as a probability vector. If $A$ and $B$ are nonnegative Hermitian operators with unit trace, we say that $A \prec B$ ("$A$ is majorized by $B$") if $\lambda(A) \prec \lambda(B)$. (Recall that for two probability vectors $p$ and $q$, we say that $p \prec q$ if there is a doubly stochastic matrix $D$ such that $p = Dq$.)

Show that if $\rho$ is a density operator and $\mathcal{E}$ is a unital map, then

$$\mathcal{E}(\rho) \prec \rho \ . \tag{8}$$

**Hint**: Express $\rho = U\Delta U^\dagger$ where $\Delta$ is diagonal and $U$ is unitary, and express $\rho' \equiv \mathcal{E}(\rho) = V\Delta' V^\dagger$, where $\Delta'$ is diagonal and $V$ is unitary. Then try to show that the diagonal entries of $\Delta'$ can be expressed as a doubly stochastic matrix acting on the diagonal entries of $\Delta$.

**Remark**: A unital map is the natural quantum generalization of a doubly stochastic map (a doubly stochastic map can be regarded as the special case of a unital map that preserves the basis in which $\rho$ is diagonal). The result of the exercise shows that a unital map takes an input density operator to an output density operator that is no less random than the input.

### 2.3 Hardy's theorem

Bob (in Boston) and Claire (in Chicago) share many identically prepared copies of the two-qubit pure state

$$|\psi(x)\rangle = \sqrt{(1-2x)}\ |00\rangle + \sqrt{x}\ |01\rangle + \sqrt{x}\ |10\rangle \ , \tag{9}$$

where $x$ is a real number between 0 and 1/2. They conduct many trials in which each measures his/her qubit in the basis $\{|0\rangle, |1\rangle\}$, and they learn that if Bob's outcome is 1 then Claire's is always 0, and if Claire's outcome is 1 then Bob's is always 0.

Bob and Claire conduct further experiments in which Bob measures in the basis $\{|0\rangle, |1\rangle\}$ and Claire measures in the orthonormal basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$. They discover that if Bob's outcome is 0, then Claire's outcome is always $\varphi$ and never $\varphi^\perp$. Similarly, if Claire measures in the basis $\{|0\rangle, |1\rangle\}$ and Bob measures in the basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, then if Claire's outcome is 0, Bob's outcome is always $\varphi$ and never $\varphi^\perp$.

*a*) Express the basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$ in terms of the basis $\{|0\rangle, |1\rangle\}$.

Bob and Claire now wonder what will happen if they both measure in the basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$. Their friend Albert, a firm believer in local realism, predicts that it is impossible for both to obtain the outcome $\varphi^\perp$ (a prediction known as *Hardy's theorem*). Albert argues as follows:

> When both Bob and Claire measure in the basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, it is reasonable to consider what might have happened if one or the other had measured in the basis $\{|0\rangle, |1\rangle\}$ instead.
>
> So suppose that Bob and Claire both measure in the basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, and that they both obtain the outcome $\varphi^\perp$. Now if Bob had measured in the basis $\{|0\rangle, |1\rangle\}$ instead, we can be certain that his outcome would have been 1, since experiment has shown that if Bob had obtained 0 then Claire could not have obtained $\varphi^\perp$. Similarly, if Claire had measured in the basis $\{|0\rangle, |1\rangle\}$, then she certainly would have obtained the outcome 1. We conclude that if Bob and Claire both measured in the basis $\{|0\rangle, |1\rangle\}$, both would have obtained the outcome 1. But this is a contradiction, for experiment has shown that it is not possible for both Bob and Claire to obtain the outcome 1 if they both measure in the basis $\{|0\rangle, |1\rangle\}$.
>
> We are therefore forced to conclude that if Bob and Claire both measure in the basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, it is impossible for both to obtain the outcome $\varphi^\perp$.

Though impressed by Albert's reasoning, Bob and Claire decide to investigate what predictions can be inferred from quantum mechanics.

*b*) If Bob and Claire both measure in the basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$, what is the quantum-mechanical prediction for the probability $P(x)$ that both obtain the outcome $\varphi^\perp$?

*c*) Find the "maximal violation" of Hardy's theorem: show that the maximal value of $P(x)$ is $P[(3-\sqrt{5})/2] = (5\sqrt{5}-11)/2 \approx .0902$.

*d*) Bob and Claire conduct an experiment that confirms the prediction of quantum mechanics. What was wrong with Albert's reasoning?

### 2.4 Closing the detection loophole

Recall that the *CHSH inequality*

$$|\langle ab\rangle + \langle a'b\rangle + \langle ab'\rangle - \langle a'b'\rangle| \leq 2 \tag{10}$$

holds if the random variables $a, b, a', b'$ take values $\pm 1$ and are governed by a joint probability distribution. The maximal violation of this inequality by the quantum-mechanical predictions occurs when the left-hand-side is $2\sqrt{2}$, which is achieved if Alice and Bob share the maximally entangled state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $a, a'$ are measurements of Alice's qubit along axes $\hat{x}$ and $\hat{z}$, and $b, b'$ are measurements of Bob's qubit along axes $(\hat{x}+\hat{z})/\sqrt{2}$ and $(\hat{x}-\hat{z})/\sqrt{2}$.

Alice and Bob have done a beautiful experiment measuring the polarizations of entangled photon pairs, and have confirmed the CHSH inequality violation predicted by quantum mechanics. Albert is skeptical. He points out that the detectors used by Alice and Bob in their experiment are not very efficient. Usually, when Alice detects a photon, Bob does not, and when Bob detects a photon, Alice does not. Therefore, they discard the data for most of the photon pairs, and retain the results only in the case when two photons are detected in coincidence. In their analysis of the data, Alice and Bob assume that their results are based on a fair sample of the probability distribution governing the measured variables. But Albert argues that their conclusions could be evaded if *whether* a photon is detected is correlated with the *outcome* of the polarization measurement.

Alice and Bob wonder how much they will need to improve their detector efficiency to do an experiment that will impress Albert.

Alice can choose to orient her detector along any axis. Ideally, when she aligns the detector with the axis $\hat{a}$, the detector "clicks" with probability one if the qubit points up along the axis $\hat{a}$, and it clicks with probability zero if the qubit points down along $\hat{a}$. But the detector is imperfect — though the detector never clicks when the qubit points down, it clicks with probability $\eta_A < 1$ when the qubit points up; we

say that $\eta_A$ is the detector's *efficiency*. Thus, when the detector clicks, Alice is sure the qubit is up, but when it fails to click, she can't be sure whether the qubit is up or down. Bob has a similar detector with efficiency $\eta_B$.

Consider a local hidden variable model intended to describe Alice's and Bob's observations. Alice can make either one of two measurements, labeled $a$ and $a'$, and Bob can make either one of two measurements, labeled $b$ and $b'$. When the hidden variables are in a definite *local configuration*, it is determined whether Alice's detector will click if Alice measures $a$ and whether it will click if Alice measures $a'$; similarly, it is determined whether Bob's detector will click if Bob measures $b$ and whether it will click if Bob measures $b'$. Define a variable $x \in \{0, 1\}$ indicating whether Alice's detector will click if she measures $a$: $x = 1$ if it will click and $x = 0$ if not. Similarly, $x' \in \{0, 1\}$ indicates whether Alice's detector will click if she measures $a'$, $y \in \{0, 1\}$ indicates whether Bob's detector will click if he measures $b$ and $y' \in \{0, 1\}$ indicates whether Bob's detector will click if he measures $b'$.

Alice and Bob are free to decide how to align their detectors in each measurement; therefore, after many trials, they will be able to estimate with high statistical confidence the probabilities $P_{++}(ab)$, $P_{++}(a'b)$, $P_{++}(ab')$, and $P_{++}(a'b')$. Here *e.g* $P_{++}(ab)$ denotes the probability that both detectors click if Alice measures $a$ and Bob measures $b$ (including the effects of detector inefficiency).

*a*) If $x, x', y, y' \in \{0, 1\}$, show that

$$xy + xy' + x'y - x'y' \leq x + y \ . \tag{11}$$

*b*) Show that, in a local hidden variable model (*i.e.*, for any probability distribution on local configurations),

$$P_{++}(ab) + P_{++}(a'b) + P_{++}(ab') - P_{++}(a'b') \leq P_{+\cdot}(a) + P_{\cdot+}(b) \ ; \tag{12}$$

here $P_{+\cdot}(a)$ denotes the probability that Alice's detector clicks if oriented along $a$, and $P_{\cdot+}(b)$ denotes the probability that Bob's detector clicks if oriented along $b$.

*c*) Now compare with the predictions of quantum mechanics, where Alice's detector has efficiency $\eta_A$ and Bob's detector has efficiency $\eta_B$. Choosing the $a, a', b, b'$ that maximally violate the CHSH

inequality, show that the quantum-mechanical predictions violate eq. (12) only if

$$\frac{\eta_A \eta_B}{\eta_A + \eta_B} > \frac{1}{1+\sqrt{2}} \ . \tag{13}$$

Thus, if $\eta_A = \eta_B$, Alice and Bob require detectors with efficiency above 82.84% to overcome Albert's objection.

### 2.5 Coherent classical communication

We saw that the tasks realized by superdense coding (SD) and by teleportation (TP) can be succinctly expressed as *resource inequalities*:

$$\begin{aligned} [q \to q] + [qq] &\geq 2[c \to c] \qquad \text{(SD)} \ , \\ 2[c \to c] + [qq] &\geq [q \to q] \qquad \text{(TP)} \ . \end{aligned} \tag{14}$$

Here $[c \to c]$ denotes one classical bit (cbit) sent from Alice to Bob, $[q \to q]$ denotes one qubit sent from Alice to Bob, and $[qq]$ denotes one *ebit* — a maximally entangled pair of qubits shared by Alice and Bob. The meaning of the inequality is that, using only local operations, the input resources on the left can be converted into the output resources on the right.

These inequalities are strict, in the sense that the resource conversions are irreversible — there is no protocol corresponding to SD or TP "running backwards." It turns out that there is a natural way to formulate versions of SD and TP that are reversible in the sense that the resource inequality can be replaced by an equality, but to do so we must replace classical communication with a stronger resource: *coherent classical communication*.

The three types of communication that we wish to consider can be realized as isometries (inner-product preserving linear maps). Sending a qubit from Alice to Bob can be expressed as

$$[q \to q] : |x\rangle_A \to |x\rangle_B \ , \tag{15}$$

where $x \in \{0, 1\}$. Sending a cbit from Alice to Bob can be expressed as

$$[c \to c] : |x\rangle_A \to |x\rangle_B \otimes |x\rangle_E \ ; \tag{16}$$

here $E$ denotes an environment that cannot be accessed by either Alice or Bob. The communication is classical because a quantum signal that

Alice attempts to send to Bob decoheres in the basis $\{|0\rangle, |1\rangle\}$. Sending a *cobit* (a unit of coherent classical communication) from Alice to Bob can be expressed as

$$[q \to qq] : |x\rangle_A \to |x\rangle_A \otimes |x\rangle_B \ ; \tag{17}$$

this is somewhat like classical communication, except that Alice maintains control of the "environment."

*a*) Show that

$$[q \to q] \geq [q \to qq] \geq [c \to c] \ , \quad \text{and} \quad [q \to qq] \geq [qq] \ . \tag{18}$$

(That is, explain how to use what is on the left side of each inequality, together with local operations, to achieve what is on the right side.)

*b*) Show that

$$[q \to q] + [qq] \geq 2[q \to qq] \ . \tag{19}$$

**Hint**: Use a coherent version of superdense coding, where Bob performs a local unitary transformation $U_B$ rather than a Bell measurement. That is, Alice has two qubits in the state $|xy\rangle_A$ and she shares a Bell pair with Bob. To achieve $|xy\rangle_A \to |xy\rangle_A \otimes |xy\rangle_B$, first Alice applies a local unitary transformation $U_A$ to her two qubits and her half of the entangled pair, then she sends her half of the Bell pair to Bob, and finally Bob applies a unitary transformation $U_B$. The problem is to find $U_A$ and $U_B$.

*c*) Show that

$$2[q \to qq] + [qq] \geq [q \to q] + 2[qq] \ . \tag{20}$$

**Hint**: Use a coherent version of teleportation, where Alice performs a local unitary transformation $V_A$ rather than a Bell measurement. That is, Alice applies $V_A$, then she sends two cobits to Bob, and finally Bob applies a local unitary transformation $V_B$. The problem is to find $V_A$ and $V_B$. Be sure to verify that Alice and Bob wind up with 2 ebits at the end of the protocol.

**Remark**: We see that coherent teleportation actually creates more entanglement than it consumes. We can express the results of (*b*) and (*c*) by saying

$$2[q \to qq] = [q \to q] + [qq] \ , \tag{21}$$

but where the the equality indicates that the resource conversion could be *catalytic* — a resource might need to be borrowed to activate the process, but this borrowed resource can be returned when the protocol is completed.