Ph219/CS219: Quantum Computation
Fall 2005

Solutions to Problem Set 1

Problem 1.1

We first express Bob's E_a^B in his Schmidt basis $\{|\beta_i\rangle\}$ as

$$E_a^B = \sum_{i,j} m_{i,j} |\beta_i\rangle\langle\beta_j| \ , \tag{1}$$

where the Schmidt decomposition of $|\Psi\rangle$ is

$$|\Psi\rangle = \sum_k \sqrt{p_k}\ |\alpha_k\rangle \otimes |\beta_k\rangle \ . \tag{2}$$

Therefore, the unnormalized state after Bob's projection is

$$\left(I \otimes E_a^B\right) |\Psi\rangle = \sum_{i,k} \sqrt{p_k}\ m_{i,k}\ |\alpha_k\rangle \otimes |\beta_i\rangle \ . \tag{3}$$

Two bipartite states are "locally" equivalent if they have the same Schmidt coefficients. So, Alice wants her projector E_a^A to project the initial state $|\Psi\rangle$ to a state with the same Schmidt coefficients as Bob's projector E_a^B. She can choose the projector E_a^A to have the same form as E_a^B, but now in her Schmidt basis $\{|\alpha_i\rangle\}$, i.e.

$$E_a^A = \sum_{i,j} m_{i,j} |\alpha_i\rangle\langle\alpha_j| \ . \tag{4}$$

The unnormalized state after Alice's projection is

$$\left(E_a^A \otimes I\right) |\Psi\rangle = \sum_{i,k} \sqrt{p_k}\ m_{i,k}\ |\alpha_i\rangle \otimes |\beta_k\rangle \ . \tag{5}$$

The states in Eqs. (3) and (5) have the same norm, so the outcome a occurs after Alice's or Bob's projection with the same probability. Furthermore, the two states differ by a "swap" $|\alpha_k\rangle \otimes |\beta_i\rangle \to |\alpha_i\rangle \otimes |\beta_k\rangle$.

This means that if $U_a^A \otimes U_a^B$ rotates the state after Bob's projection in Eq. (3) to Schmidt form, then $U_a^B \otimes U_a^A$ will rotate the state after Alice's projection in Eq. (5) to Schmidt form (with the same Schmidt coefficients). Therefore

$$\left(U_a^A \otimes U_a^B\right) \left(I \otimes E_a^B\right) |\Psi\rangle = \left(U_a^B \otimes U_a^A\right) \left(E_a^A \otimes I\right) |\Psi\rangle \ . \tag{6}$$

$$\Rightarrow \left(I \otimes E_a^B\right)|\Psi\rangle = \left(V_a^A \otimes V_a^B\right)\left(E_a^A \otimes I\right)|\Psi\rangle\ , \tag{7}$$

where $V_a^A = (U_a^A)^{-1}U_a^B$ and $V_a^B = (U_a^B)^{-1}U_a^A$. $\square$

Problem 1.2

The GHJW theorem says that two ensemble realizations $\{|\alpha_i\rangle, p_i\}$ and $\{|\phi_\mu\rangle, q_\mu\}$ of a density matrix ρ

$$\begin{aligned} \rho &= \sum_i p_i\ |\alpha_i\rangle\langle\alpha_i| \\ &= \sum_\mu q_\mu\ |\phi_\mu\rangle\langle\phi_\mu| \end{aligned} \tag{8}$$

are related by

$$\sqrt{q_\mu}|\phi_\mu\rangle = \sum_i \sqrt{p_i}\ V_{\mu,i}|\alpha_i\rangle\ , \tag{9}$$

for some unitary V.

Now, in the forward direction, suppose $q \prec p$. By Horn's lemma we can write

$$q_\mu = \sum_i |V_{\mu,i}|^2 p_i\ , \tag{10}$$

for some unitary V. Therefore, if $\rho = \sum_i p_i\ |\alpha_i\rangle\langle\alpha_i|$, we can define $|\phi_\mu\rangle$ by Eq. (9). We can then check

$$\begin{aligned} \sum_\mu q_\mu\ |\phi_\mu\rangle\langle\phi_\mu| &= \sum_{\mu,i,j} \sqrt{p_i p_j}\ V_{\mu,i}\ |\alpha_i\rangle\langle\alpha_j|\ V^*_{\mu,j} \\ &= \sum_i p_i\ |\alpha_i\rangle\langle\alpha_i|\ , \end{aligned} \tag{11}$$

since $\sum_\mu V_{\mu,i}V^*_{\mu,j} = \delta_{i,j}$ for V unitary.

For the converse, suppose ρ has the two ensemble representations in Eq. (8). Computing the norm on both sides of Eq. (9) we get

$$\begin{aligned} q_\mu &= \sum_{i,j} \sqrt{p_i p_j}\ V_{\mu,i}\ V^*_{\mu,j}\ \langle\alpha_j|\alpha_i\rangle \\ &= \sum_i |V_{\mu,i}|^2\ p_i\ . \end{aligned} \tag{12}$$

Since D such that $D_{\mu,i} = |V_{\mu,i}|^2$ for V unitary is doubly stochastic, it follows that $q \prec p$. $\square$

Problem 1.3 If the deterministic transformation $|\Psi\rangle \to |\Phi\rangle$ is possible, then there is a POVM with elements $\{M_\mu\}$ Alice can perform and a superoperator $\mathcal{E}_\mu$

conditioned on the outcome μ of Alice's measurement that Bob can apply so that

$$\forall \mu \ : \ (I \otimes \mathcal{E}_\mu) \left(M_\mu |\Psi\rangle\langle\Psi| M_\mu^\dagger \right) \propto |\Phi\rangle\langle\Phi| \ , \tag{13}$$

where $\sum_\mu M_\mu^\dagger M_\mu = I$. This follows from Problem 1.1 and the fact that Alice's post-measurement unitary can be included in the M_μ's.

Bob's superoperator $\mathcal{E}_\mu$ cannot change Alice's reduced density matrix ρ^A, so that

$$\forall \mu \ : M_\mu \ \rho_\Psi^A \ M_\mu^\dagger = c_\mu \ \rho_\Phi^A \ , \tag{14}$$

where $\rho_\Psi^A = \mathrm{Tr}_B \left(|\Psi\rangle\langle\Psi| \right)$, $\rho_\Phi^A = \mathrm{Tr}_B \left(|\Phi\rangle\langle\Phi| \right)$ and c_μ is the proportionality constant such that $\sum_\mu c_\mu = 1$ (since c_μ is the probability of outcome μ).

We first polar-decompose $M_\mu \sqrt{\rho_\Psi^A}$ to get

$$M_\mu \sqrt{\rho_\Psi^A} = \sqrt{M_\mu \ \rho_\Psi^A \ M_\mu^\dagger} \ U_\mu = \sqrt{c_\mu \ \rho_\Phi^A} \ U_\mu \ , \tag{15}$$

where U_μ is unitary and we have used Eq. (14). This decomposition is useful if we consider the sequence of identities

$$\rho_\Psi^A = \sqrt{\rho_\Psi^A}\sqrt{\rho_\Psi^A} = \sqrt{\rho_\Psi^A} \ I \ \sqrt{\rho_\Psi^A} = \sum_\mu \sqrt{\rho_\Psi^A} \ M_\mu^\dagger M_\mu \ \sqrt{\rho_\Psi^A} \ . \tag{16}$$

Therefore, using Eq. (15) we can write

$$\begin{aligned} \rho_\Psi^A &= \sum_\mu \sqrt{\rho_\Psi^A} \ M_\mu^\dagger M_\mu \ \sqrt{\rho_\Psi^A} \\ &= \sum_\mu U_\mu^\dagger \sqrt{c_\mu \ \rho_\Phi^A} \sqrt{c_\mu \ \rho_\Phi^A} \ U_\mu \\ &= \sum_\mu c_\mu \ U_\mu^\dagger \ \rho_\Phi^A \ U_\mu \ . \end{aligned} \tag{17}$$

This means that ρ_Ψ^A is obtained from ρ_Φ^A by applying a unitary U_μ conditioned on the outcome μ.

Let

$$\begin{aligned} \rho_\Psi^A &= \sum_i p_i^\Psi |i\rangle\langle i| \ , \\ \rho_\Phi^A &= \sum_a p_a^\Phi |a\rangle\langle a| \ . \end{aligned} \tag{18}$$

Then, using Eq. (17), we have

$$
\begin{aligned}
\rho^A_\Psi &= \sum_i p^\Psi_i |i\rangle\langle i| \\
&= \sum_{\mu,a} c_\mu \, p^\Phi_a \, U^\dagger_\mu \, |a\rangle\langle a| \, U_\mu \\
&= \sum_{\mu,a,i,k} c_\mu \, p^\Phi_a \, (U^\dagger_\mu)_{a,i} \, |i\rangle\langle k| \, (U^\dagger_\mu)^*_{a,k} \\
&= \sum_{\mu,a,i,k} c_\mu \, p^\Phi_a \, (U^\dagger_\mu)_{a,i} \, (U^\dagger_\mu)^*_{a,k} \, |i\rangle\langle k| \\
\Rightarrow \; p^\Psi_i &= \sum_{\mu,a} c_\mu \, p^\Phi_a \, (U^\dagger_\mu)_{a,i} \, (U^\dagger_\mu)^*_{a,i} \\
&= \sum_a \left(\sum_\mu c_\mu |(U^\dagger_\mu)_{a,i}|^2 \right) \, p^\Phi_a \\
&= \sum_a D_{i,a} \, p^\Phi_a \; ,
\end{aligned}
\tag{19}
$$

where $D_{i,a} = \sum_\mu c_\mu |(U^\dagger_\mu)_{a,i}|^2$ is doubly stochastic because U is unitary and $\sum_\mu c_\mu = 1$ (note that $\sum_i |(U^\dagger_\mu)_{a,i}|^2 = \sum_a |(U^\dagger_\mu)_{a,i}|^2 = 1$). Hence, $p^\Psi \prec p^\Phi$. $\square$

Problem 1.4 Let's first repeat our model for the protocol Alice and Bob use—all details of the protocol will be known to both parties. The protocol has three stages: (a) Alice prepares two distinguishable density matrices ρ_0 and ρ_1 in system AB depending on her choice of $a = 0$ or $a = 1$ respectively, (b) Alice sends system B to Bob through a quantum channel and keeps system A to herself, (c) Alice decides to reveal her committed bit and sends her system A to Bob. He now has both parts of the system AB, so holds either ρ_0 or ρ_1 and he can perform an operation that distinguishes them to learn a.

After stage (b) and before stage (c), Alice and Bob can wait an undefinitely long time before proceeding to the next stage. If the protocol is concealing then there is no quantum operation Bob can do in the system B he holds which will reveal Alice's choice for a. The protocol will be binding if there is no quantum operation Alice can do after stage (b) and before stage (c) on her system A that can change—if she wants—ρ_0 to ρ_1 or vice versa without Bob being able to discover that she cheated.

First, the two density matrices ρ_0 and ρ_1 have a purification on system A and its "environment" E_A and system B and its "environment" E_B

$$\rho_0 \to |\Psi_0\rangle \;\; ; \;\; \rho_1 \to |\Phi_1\rangle \; . \tag{20}$$

Without loss of generality we can assume Alice (who may try to cheat by changing her bit) and Bob (who may try to cheat and learn Alice's bit before stage (c)) have full control over their environments. Thus we can consider the state on system AB after stage (b) and before stage (c) to be one of $|\Psi_0\rangle$ or $|\Psi_1\rangle$. Clearly any scenario in which the actual state is mixed gives less power to Alice and Bob to achieve their goals and can be simulated with pure states alone e.g. by attaching ancillas that simulate random bit generators that help them realize the ensemble corresponding to their density matrices.

Now, assume the protocol is concealing. After stage (b) and before stage (c), Bob may try to cheat and learn what bit Alice has committed but he will fail to gain any information about a. This implies that

$$\rho_0^{B,E_B} = \rho_1^{B,E_B} \ , \tag{21}$$

where $\rho_i^{B,E_B} = \mathrm{Tr}_{A,E_A}\left(|\Psi_i\rangle\langle\Psi_i|\right), i \in \{0,1\}$. In other words, the fact that Bob cannot distinguish $a = 0$ from $a = 1$ by performing a measurement on B and its environment E_B means that the reduced density matrices for the two cases look exactly the same to him.

But then, the GJHW theorem says that any two pure states on ABE_AE_B related by Eq. (21) on the reduced system BE_B differ by a unitary on one system alone, i.e.

$$|\Psi_1\rangle = (U_{A,E_A} \otimes I_{B,E_B})\,|\Psi_0\rangle \ . \tag{22}$$

The unitary $U_{A,E_A} \otimes I_{B,E_B}$ has support on system A and its environment E_A that Alice holds after stage (b). Therefore, Alice can cheat by applying U_{A,E_A} if she decides to change her committed bit a before sending her system to Bob in stage (c), and Bob will not be able to tell the difference. Hence, the protocol is not binding. $\square$