ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Series 5

HS 11
Prof. M. Christandl

Exercise 5.1 Purification

A decomposition of a state $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ is a (non-unique) convex combination of pure states $\rho_A^x = |a_x\rangle\langle a_x|$ such that $\rho_A = \sum_x \lambda_x \rho_A^x$.

a) Show that $|\Psi\rangle = \sum_x \sqrt{\lambda_x}\,|a_x\rangle_A \otimes |b_x\rangle_B$ is a purification of ρ_A for *any* orthonormal basis $\{\,|b_x\rangle_B\,\}_x$ of $\mathcal{H}_{\mathrm{B}}$.

b) Show that any two purifications are related by a *local* isometry on the purifying system.

c) Mixed states can be decomposed in many different ways.

[**Example.** We can write

$$\begin{aligned}\frac{\mathbb{1}_2}{2} &= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}, \quad \text{or} \\ &= \frac{|+\rangle\langle +| + |-\rangle\langle -|}{2}, \quad \text{or (more interesting)} \\ &= \sum_{i=1}^{4} \frac{1}{4} |\theta_i, \phi_i\rangle\langle \theta_i, \phi_i|,\end{aligned}$$

where $\{|\theta_i, \phi_i\rangle\}$ are pure states, which lie on the surface of the sphere, and therefore can be parametrized by just two parameters, $(\theta, \phi) \in [0, \pi] \times [0, 2\pi)$. An example that works is when the vectors sit on the vertices of a regular tetrahedron,

$$(\theta_1, \phi_1) = (\psi, \frac{\pi}{4}), \quad (\theta_2, \phi_2) = (\pi - \psi, -\frac{\pi}{4}), \quad (\theta_3, \phi_3) = (\pi - \psi, \frac{3\pi}{4}), \quad (\theta_4, \phi_4) = (\psi, -\frac{3\pi}{4}),$$

with $\psi := \arccos(\frac{1}{\sqrt{3}})$.]

We will show that, from a purification of a mixed state ρ_A, we can generate any decomposition $\{\rho_A^x\}_x$ such that $\rho_A = \sum_x \lambda_x \rho_A^x$ by performing measurements on the purifying system. This is sometimes called *steering*.

More precisely, for ρ_A as defined above, and any purification $|\Phi\rangle$ of ρ_A on $\mathcal{H}_A \otimes \mathcal{H}_B$, find an measurement on $\mathcal{H}_B$, described by operators $\{\,M_B^x\,\}_x$, such that

$$\lambda_x = \mathrm{Tr}\left[|\Phi\rangle\langle\Phi|(\mathbb{1}_A \otimes M_B^x)\right] \quad \text{and} \quad \rho_A^x = \frac{\mathrm{Tr}_B\left[|\Phi\rangle\langle\Phi|(\mathbb{1}_A \otimes M_B^x)\right]}{\lambda_x}. \tag{1}$$

In this picture λ_x is the probability of measuring x and ρ_A^x is the state after the measurement.

Exercise 5.2 Distinguishing two quantum states

Suppose you know the density operators of two quantum states $\rho, \sigma \in \mathcal{H}_A$. Then you are given one of the states at random—it may either be ρ, with probability p, or σ, with probability $1 - p$. The challenge is to perform a single measurement on your state and then guess which state that is.

a) What is your best strategy? In which basis do you think you should perform the measurement? Can you express that measurement using a projector P?

b) What is the probability of guessing correctly, $\Pr_{\checkmark}^{p}(\rho, \sigma)$? Compare that with the case where the states are evenly distributed, $\Pr_{\checkmark}^{0.5}(\rho, \sigma) = \frac{1}{2}[1 + \delta(\rho, \sigma)]$, where $\delta(\rho, \sigma)$ is the trace distance between the two quantum states.

Exercise 5.3 Data hiding

Suppose you are M, and have two agents, Alice and Bond, at your service. You want them to deliver a secret message to your ally Sauron in New Zealand. You will split the message between Alice and Bond, and send them in different ways, to only meet again when they arrive at their safe destiny. You need a way of distributing the message between Alice and Bond such that, even if both of them are caught or sold to your enemies, no-one can extract the secret unless they are together. Your friend Q comes up with a quantum idea.

Data hiding refers to states that are easily distinguishable if we can perform whatever operations we want, like global measurements on Alice and Bond's systems, but nearly indistinguishable if we are restricted to some type of operations, like local operations and classical communication (LOCC). Formally, we say that a family of states $\left\{\rho^i\right\}_i$ is ε-secure under a set of operations $\mathbb{E}$ if

$$\delta(\mathcal{E}(\rho^i),\mathcal{E}(\rho^j)) < \varepsilon, \quad \forall i,j, \quad \forall \mathcal{E} \in \mathbb{E}.$$

In this exercise, we will see one scheme that is secure under local measurements followed by classical communication (comparison of the outcomes).

Consider a $2d$-qubit Hilbert space, $\mathcal{H}_A \otimes \mathcal{H}_B$, and the computational basis of both spaces. Consider the projectors onto the symmetric and antisymmetric subspaces of $\mathcal{H}_A \otimes \mathcal{H}_B$,

$$\Pi^S = \frac{1}{2}\sum_{i<j}\Big(|i\rangle_A|j\rangle_B + |j\rangle_A|i\rangle_B\Big)\Big(\langle i|_A\langle j|_B + \langle j|_A\langle i|_B\Big) + \sum_i |i\rangle_A|i\rangle_B\langle i|_A\langle i|_B,$$

$$\Pi^A = \frac{1}{2}\sum_{i<j}\Big(|i\rangle_A|j\rangle_B - |j\rangle_A|i\rangle_B\Big)\Big(\langle i|_A\langle j|_B - \langle j|_A\langle i|_B\Big).$$

You will encode only one bit of information, b, giving Alice and Bond each their $d-$qubit part of ρ^b_{AB}, with

$$\rho^{b=0} = \frac{2}{d(d+1)}\Pi^S, \qquad \rho^{b=1} = \frac{2}{d(d-1)}\Pi^A.$$

a) Show that $\rho^{b=0}$ and $\rho^{b=1}$ are valid density operators and explain how you would proceed to recover b if you had access to Alice and Bond's systems (together).

b) Consider the flip operator in basis $\{|i\rangle_A|j\rangle_B\}_{ij}$,

$$F = \Pi^S - \Pi^A = \sum_{i,j}|i\rangle_A|j\rangle_B\langle j|_A\langle i|_B.$$

Show that, for all operators $M_A \in \mathrm{End}(\mathcal{H}_A), N_B \in \mathrm{End}(\mathcal{H}_B)$,

$$\mathrm{Tr}[F(M_A \otimes N_B)] = \mathrm{Tr}(M_A N_B).$$

In particular, for all pure states $|x\rangle_A, |y\rangle_B$, $\mathrm{Tr}[F|xy\rangle\langle xy|] = |\langle x|y\rangle|^2$.

c) Suppose that Alice and Bond perform local projective measurements in arbitrary bases $\{|x\rangle_A\}$ and $\{|y\rangle_B\}$ respectively. We call the joint probability distribution of the outcomes P_{XY} when they measure state $\rho^{b=0}$ and Q_{XY} when they measure $\rho^{b=1}$. We want them to be unable to determine which state they measured, i.e., to distinguish the two distributions, so we want to show that $\delta(P_{XY},Q_{XY})$ is small. Remember that

$$P_{XY}(x,y) = \mathrm{Tr}(|xy\rangle\langle xy|\rho^{b=0}), \qquad Q_{XY}(x,y) = \mathrm{Tr}(|xy\rangle\langle xy|\rho^{b=1}).$$

Use the results from *b*) to show that $\delta(P_{XY},Q_{XY}) \leq \frac{2}{d+1}$.

Hint: start from the trace distance as

$$\delta(P_{XY},Q_{XY}) = \sum_{x,y\in\mathcal{S}} P_{XY}(x,y) - Q_{XY}(x,y),$$

with $\mathcal{S} = \{(x,y) : P_{XY}(x,y) > Q_{XY}(x,y)\}$.