3rd May, 2024

COURSE 4430— Quantum information theory

Mandatory assignment 1 of 1

Submission deadline

Thursday 23rd May 2024, 14:30 in Canvas (canvas.uio.no).

Instructions

Note that you have **one attempt** to pass the assignment. This means that there are no second attempts.

You can choose between scanning handwritten notes or typing the solution directly on a computer (for instance with LaTeX). The assignment must be submitted as a single PDF file. Scanned pages must be clearly legible. The submission must contain your name, course and assignment number.

It is expected that you give a clear presentation with all necessary explanations. Remember to include all relevant plots and figures. All aids, including collaboration, are allowed, but the submission must be written by you and reflect your understanding of the subject. If we doubt that you have understood the content you have handed in, we may request that you give an oral account.

In exercises where you are asked to write a computer program, you need to hand in the code along with the rest of the assignment. It is important that the submitted program contains a trial run, so that it is easy to see the result of the code.

Application for postponed delivery

If you need to apply for a postponement of the submission deadline due to illness or other reasons, you have to contact the Student Administration at the Department of Mathematics (e-mail: studieinfo@math.uio.no) no later than the same day as the deadline.

All mandatory assignments in this course must be approved in the same semester, before you are allowed to take the final examination.

Complete guidelines about delivery of mandatory assignments:

uio.no/english/studies/admin/compulsory-activities/mn-math-mandatory.html

GOOD LUCK!

Assigment: In the following, you find all 15 exercise sheets for the course. Select *one* problem from each exercise sheet and submit your solution. To pass the assignment your solutions for 10 of the problems have to be correct. If you are very sure, then you are allowed to only submit 10 problems from different exercise sheets in which case all of them have to be correct in order for you to pass the assigment. If anything about these rules is unclear, please contact me by email.

Sheet 1

Problem 1 (The relative entropy)**.** We define the *relative entropy* of probability distributions $p, q \in \mathcal{P}(\Sigma)$ as

$$D(p\|q) = \begin{cases} \sum_{x\in\Sigma} p(x) \log\left(\frac{p(x)}{q(x)}\right) & , \text{ if } \operatorname{supp}(p) \subseteq \operatorname{supp}(q) \\ +\infty & , \text{ otherwise.} \end{cases}$$

The relative entropy measures statistical difference and it is closely related to other entropic quantities. In this exercise, you will prove some important properties of the relative entropy and use them to determine properties of the Shannon entropy and the mutual information.

1. For positive numbers $a_1, \ldots, a_d \in \mathbb{R}^+$ and $b_1, \ldots, b_d \in \mathbb{R}^+$ show that

$$\sum_{i=1}^{d} a_i \log\left(\frac{a_i}{b_i}\right) \geq \left(\sum_{i=1}^{d} a_i\right) \log\left(\frac{\sum_{i=1}^{d} a_i}{\sum_{i=1}^{d} b_i}\right).$$

   Hint: Reformulate this inequality using the variables

$$\beta_i = \frac{b_i}{\sum_{j=1}^{d} b_j} \quad \text{and} \quad t_i = \frac{a_i}{b_i}.$$

2. Show Gibb's inequality

$$D(p\|q) \geq 0,$$

   for all $p, q \in \mathcal{P}(\Sigma)$ with equality if and only if $p = q$.

3. Given $p_1, p_2, q_1, q_2 \in \mathcal{P}(\Sigma)$ and $\lambda \in [0, 1]$ show that the relative entropy is jointly convex, i.e.,

$$D((1-\lambda)p_1 + \lambda p_2 \| (1-\lambda)q_1 + \lambda q_2) \leq (1-\lambda) D(p_1\|q_1) + \lambda D(p_2\|q_2).$$

4. Show that the Shannon entropy of a distribution $p \in \mathcal{P}(\Sigma)$ can be written as
$$H(p) = \log(|\Sigma|) - D\left(p \| u\right),$$
for the uniform distribution $u \in \mathcal{P}\left(\Sigma\right)$, i.e., the distribution with $u(x) = 1/|\Sigma|$. Conclude that $H(p) \leq \log(|\Sigma|)$ with equality if and only if $p = u$, and that the entropy function is concave.

Problem 2 (Conditional entropy and mutual information)**.** Let $p_{AB} \in \mathcal{P}(\Sigma_A \times \Sigma_B)$ denote a joint probability distribution and (X, Y) a pair of random variables distributed according to p_{AB}. We define the conditional entropy of X given Y as
$$H(X|Y) = \sum_{(x,y)\in\Sigma_A\times\Sigma_B} p_{AB}(x,y) \log\left(\frac{1}{p_{AB}(x|y)}\right).$$
The mutual information is given by
$$I(X:Y) = H(X) - H(X|Y),$$
where we write $H(X)$ for the marginal entropy, i.e., the entropy $H(p_A)$ of the marginal distribution of X.

1. Show that the mutual information is symmetric, i.e., that
$$I(X:Y) = I(Y:X).$$
2. Show that the mutual information can be written as
$$I(X:Y) = D\left(p_{AB} \| p_A \times p_B\right).$$
Conclude that $I(X:Y) \geq 0$ and that $I(X:Y) = 0$ holds if and only if X and Y are independent.
3. Show that conditioning cannot increase the entropy, i.e., that $H(X) \geq H(X|Y)$. When do we have equality here?

Problem 3 (Joint entropies)**.** Let $p_{AB} \in \mathcal{P}(\Sigma_A \times \Sigma_B)$ denote a joint probability distribution and (X, Y) a pair of random variables distributed according to p_{AB}. The joint entropy of (X, Y) is defined as
$$H(X,Y) = H(p_{AB}).$$
1. Prove the so-called chain rule of the entropy
$$H(X,Y) = H(X) + H(Y|X).$$

2. Prove that subadditivity of the entropy, i.e., the inequality

$$H(X,Y) \leq H(X) + H(Y),$$

and that we have equality if and only if X and Y are independent.

3. Consider the joint probability distribution $p_{AB} \in \mathcal{P}(\{1,2,3,4\} \times \{1,2,3,4\})$ given by

$$(p_{AB}(i,j))_{i,j} = \begin{pmatrix} 1/8 & 1/16 & 1/32 & 1/32 \\ 1/16 & 1/8 & 1/32 & 1/32 \\ 1/16 & 1/16 & 1/16 & 1/16 \\ 1/4 & 0 & 0 & 0 \end{pmatrix},$$

and a pair of random variables (X,Y) distributed according to p_{AB}. Compute the joint entropy $H(X,Y)$ the marginal entropies $H(X)$ and $H(Y)$, the conditional entropy $H(X|Y)$ and the mutual information $I(X:Y)$.

Problem 4 (Asymptotic discrimination of probability distributions)**.** Recall the experiment discussed in the lecture: Alice has a machine with two buttons labeled "0" and "1". After pressing a button the machine emits a letter containing a card with a single letter $x \in \Sigma$ from some finite alphabet Σ. If Alice presses the button "0", then the letter will be chosen according to a probability distribution $p_0 \in \mathcal{P}(\Sigma)$, and if she presses the button "1", then it will be chosen according to a probability distribution $p_1 \in \mathcal{P}(\Sigma)$. Bob now catches the letter, looks at the card inside, and tries to guess which button Alice has pressed. If we assume that Alice presses the button "0" with probability $\lambda \in [0,1]$ and the button "1" with probability $1-\lambda$, and that Bob knows the distributions p_0, p_1 and λ.

Now, we consider the same scenario involving the two characters Alice and Bob. This time Alice presses the same button multiple times in a row. How does this change the optimal probability for Bob guessing which button Alice has pressed? To answer this question, we proceed as follows:

1. Show that

$$\|\lambda p - (1-\lambda)q\|_1 \geq 1 - 2\sqrt{\lambda(1-\lambda)} \sum x \in \Sigma \sqrt{p(x)q(x)},$$

for any pair of distributions $p, q \in \mathcal{P}(\Sigma)$ and any $\lambda \in [0,1]$.

2. Now, show that $p \neq q$ if and only if

$$\|\lambda p^{\times n} - (1-\lambda)q^{\times n}\|_1 \to 1,$$

as $n \to \infty$.

3. What does this mean for the success probability in the asymptotic scenario where Bob tries to guess which button Alice pressed repeatedly?

Sheet 2

Problem 5 (Probabilistic method)**.** In this exercise, you should try to find a probabilistic proof for a statement in linear algebra. Consider vectors $v_1, \dots, v_n \in \mathbb{R}^n$ with Euclidean norms $\|v_i\|_2 = 1$. We want to show that there exist signs $\epsilon_1, \dots, \epsilon_n \in \{-1, +1\}$ such that

$$\|\epsilon_1 v_1 + \cdots + \epsilon_n v_n\|_2 \leq \sqrt{n}.$$

1. Choose random signs $\epsilon_1, \dots, \epsilon_n \in \{-1, +1\}$ uniformly and independently and consider the random variable

   $$N = \|\epsilon_1 v_1 + \cdots + \epsilon_n v_n\|_2^2.$$

   Compute the expectation value $\mathbb{E}[N]$ and conclude the desired statement.

2. Show that there also exist signs $\epsilon_1, \dots, \epsilon_n \in \{-1, +1\}$ such that

   $$\|\epsilon_1 v_1 + \cdots + \epsilon_n v_n\|_2 \geq \sqrt{n}.$$

Problem 6 (Data processing inequality for the mutual information)**.** Let $p_{AB} \in \mathcal{P}(\Sigma_A \times \Sigma_B)$ denote a joint distribution and $N : \Sigma_B \to \mathcal{P}(\Sigma_C)$ a classical channel. Show that

$$I(A:B)_{p_{AB}} \geq I(A:C)_{q_{AC}},$$

where $q_{AC} \in \mathcal{P}(\Sigma_A \times \Sigma_C)$ is the distribution given by

$$q_{AC}(x,z) = \sum_{y \in \Sigma_B} N(z|y) p_{AB}(x,y).$$

Problem 7 (The $(7,4)$-Hamming code)**.** The $(7,4)$-Hamming code encodes four bits of information into seven bits as follows. To bits $b_1, b_2, b_3, b_4 \in \{0,1\}$ we assign the codeword

$$E(b_1, b_2, b_3, b_4) = (b_1, b_2, b_3, b_4, s_1, s_2, s_3),$$

with bits s_1, s_2, s_3 such that each of the four circles in the diagram depicted in Figure 1 contains an even number of 1s. Check your understanding by verifying that

$$E(1001) = (1001110).$$

In the following, we will study the performance of this code under the binary symmetric channel BSC_p for $p \in [0, 1/2]$.

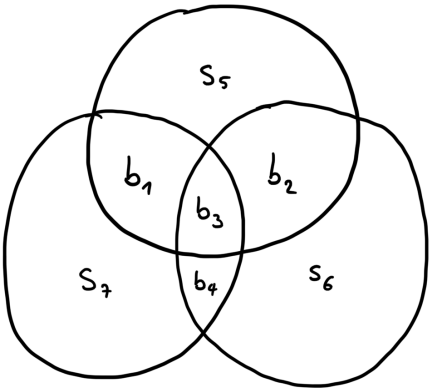


Figure 1: Defining codewords of the $(7, 4)$-Hamming code.

1. Find a simple rule to describe the maximum-likelihood decoder D for the $(7, 4)$-Hamming code and show that it corrects any single bit-flip.

2. Compute the probability of a decoding error

$$p_e = \max_{b_1,\ldots,b_4} P(\mathrm{BSC}_p^{\times 7}(E(b_1, b_2, b_3, b_4)) \notin D^{-1}(b_1, b_2, b_3, b_4)).$$

3. Compare the performance of the $(7, 4)$-Hamming code to the 3-repetition code. Which code is better?

Problem 8 (The channel mutual information)**.** To quantify how noisy a classical channel is we introduce the *channel mutual information*. Let $N : \Sigma_A \to \mathcal{P}(\Sigma_B)$ denote a classical channel and consider the quantity

$$I(N) = \max_{p_A \in \mathcal{P}(\Sigma_A)} I(A : B)_{p_{AB}^N},$$

where for a given $p_A \in \mathcal{P}(\Sigma_A)$ the distribution $p_{AB}^N \in \mathcal{P}(\Sigma_A \times \Sigma_B)$ is given by

$$p_{AB}^N(x, y) = p_A(x)N(y|x).$$

The distribution p_{AB}^N can be understood as the joint distribution of inputs and outputs when input symbols chosen from a distribution $p_A \in \mathcal{P}(\Sigma_A)$ are send through the channel N.

1. Compute the channel mutual information $I(\mathrm{BSC}_p)$ for the binary symmetric channel $\mathrm{BSC}_p : \{0, 1\} \to \mathcal{P}(\{0, 1\})$ introduced in the lecture.

2. Compute the channel mutual information $I(\mathrm{Erase}_p)$ for the binary erasure channel $\mathrm{Erase}_p : \{0,1\} \to \mathcal{P}(\{0,1\})$ introduced in the lecture.

3. Show that we have $I(N) = 0$ for a classical channel $N : \Sigma_A \to \mathcal{P}(\Sigma_B)$ if and only if the channel N is constant, i.e., there exists a probability distribution $q \in \mathcal{P}(\Sigma_B)$ such that $N(x) = q$ for every $x \in \Sigma_A$.

Sheet 3

Problem 9. Go through the material on classical information theory we have covered so far and think of a *good* question. Submit your question via email.

Sheet 4

Problem 10 (Sums of projections)**.** For a complex Euclidean space $\mathcal{H}$ consider projections $\{P_n\}_{n=1}^N \subset B(\mathcal{H})$ such that

$$\sum_{n=1}^{N} P_n = \mathbb{1}_{\mathcal{H}}. \tag{1}$$

Show that $P_i P_j = 0$ all $i \neq j$. What is the maximal number $N \in \mathbb{N}$ such that there exists a set of projections $\{P_n\}_{n=1}^N \subset B(\mathcal{H})$ satisfying (1).

Problem 11 (Positivity of certain matrices)**.** Let $\mathcal{H}$ denote a complex Euclidean space.

1. For $x \in \mathbb{C}$ consider the operator $A \in B(\mathbb{C}^2)$ given by

$$A = \begin{pmatrix} 1 & \overline{x} \\ x & 1 \end{pmatrix}.$$

   Show that A is positive semidefinite if and only if $|x| \leq 1$.

2. For $X \in B(\mathcal{H})$ consider the operator $B \in B(\mathcal{H} \oplus \mathcal{H})$ given by the matrix

$$B = \begin{pmatrix} \mathbb{1}_{\mathcal{H}} & X^\dagger \\ X & \mathbb{1}_{\mathcal{H}} \end{pmatrix}.$$

   Show that B is positive semidefinite if and only if the operator norm $\|X\| \leq 1$.

3. Show that an operator $C \in B(\mathcal{H})$ is positive if and only if the operator

$$\begin{pmatrix} C & C \\ C & C \end{pmatrix} \in B(\mathcal{H} \oplus \mathcal{H})$$

   is positive semidefinite.

Problem 12 (The qubit)**.** Let us consider the complex Euclidean space $\mathcal{H} = \mathbb{C}^2$, and recall that the quantum states on $\mathcal{H}$ are the positive semidefinite matrices in $B(\mathcal{H})$ with trace equal to 1. We refer to this set as $D(\mathbb{C}^2)$. How can we understand this set geometrically?

1. Consider the so-called Pauli matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

   Show that $\{\mathbb{1}_2, \sigma_1, \sigma_2, \sigma_3\}$ is an orthogonal basis of the Hilbert-Schmidt inner product space, i.e., the vector space $B(\mathcal{H})$ with the inner product $\langle A, B\rangle = \mathrm{Tr}\left[A^\dagger B\right]$. Show that their real span is $B(\mathcal{H})_{sa}$.

2. Show that we have

$$\left(\sum_{i=1}^{3} x_i \sigma_i\right)^\dagger \left(\sum_{i=1}^{3} x_i \sigma_i\right) = \|x\|_2^2 \mathbb{1}_2,$$

   for any $x \in \mathbb{R}^3$. Conclude that the matrix

$$\rho_x = \frac{1}{2}\mathbb{1}_2 + \frac{1}{2}\sum_{i=1}^{3} x_i \sigma_i,$$

   is a quantum state, i.e., positive and of unit trace, for any vector $x \in \mathbb{R}^3$ satisfying $\|x\|_2 \leq 1$.

3. Show that every quantum state $\rho \in D(\mathbb{C}^2)$ can be written as $\rho = \rho_x$ for some $x \in \mathbb{R}^3$. Therefore, we can identify $D(\mathbb{C}^2)$ with the unit ball in the 2-norm. What are the pure states in this picture? What quantum state is at the center of the ball?

Problem 13 (SICs)**.** Find four normalized vectors $|v_1\rangle, |v_2\rangle, |v_3\rangle, |v_4\rangle \in \mathbb{C}^2$ such that the absolute values $|\langle v_i|v_j\rangle|$ are the same for all $i \neq j$. You can start by verifying that in this case

$$|\langle v_i|v_j\rangle|^2 = \frac{2\delta_{ij} + 1}{3},$$

for any $i, j \in \{1, \ldots, 4\}$.

Sheet 5

Problem 14. Let $\mathcal{H}$ denote a complex Euclidean space of dimension $d = \dim(\mathcal{H})$. Consider the complex vector space $B(\mathcal{H})$ and the real vector space $B(\mathcal{H})_{sa}$, i.e., we consider the selfadjoint operators on $\mathcal{H}$ as an $\mathbb{R}$-vector space.

1. Show that $\dim(B(\mathcal{H})) = \dim(\mathcal{H})^2$ and find an orthonormal basis of the space $B(\mathcal{H})$ with respect to the Hilbert-Schmidt inner product.

2. Show that $\dim(B(\mathcal{H})_{sa}) = \dim(\mathcal{H})^2$ and find an orthonormal basis of the space $B(\mathcal{H})_{sa}$ with respect to the Hilbert-Schmidt inner product (turning $B(\mathcal{H})_{sa}$ into a real Euclidean space).

Problem 15 (Two decomposition theorems)**.**
Let $\mathcal{H}$ denote a complex Euclidean space.

1. Show that any selfadjoint operator $H \in B(\mathcal{H})_{sa}$ can be written as a difference $H = P - Q$ for some positive semidefinite operators $P, Q \in B(\mathcal{H})^+$ satisfying $PQ = 0$.

2. Show that any operator $X \in B(\mathcal{H})$ can be written as $X = H_1 + iH_2$ for some selfadjoint operators $H_1, H_2 \in B(\mathcal{H})_{sa}$.

3. Show that every operator $X \in B(\mathcal{H})$ can be written as a linear combination of positive semidefinite operators. In other words: The $\mathbb{C}$-span of $B(\mathcal{H})^+$ is $B(\mathcal{H})$.

Problem 16 (The Weyl-Heisenberg system)**.**
The goal of this exercise is to construct the so-called *Weyl-Heisenberg system*, an orthogonal basis consisting of unitary operators for the Hilbert-Schmidt inner product space $B(\mathbb{C}^d)$. This system generalizes the Pauli matrices to higher dimensions.

1. Consider the cyclic shift operator $S : \mathbb{C}^d \to \mathbb{C}^d$ given by

$$S|i\rangle = |i+1\rangle,$$

on the computational basis $\{|0\rangle, \ldots, |d-1\rangle\}$, and where addition is mod d. Show that the powers S^k for $k \in \{0, \ldots, d-1\}$ are orthogonal with respect to the Hilbert-Schmidt inner product $\langle X, Y \rangle_{HS} = \mathrm{Tr}\left[X^\dagger Y\right]$.

2. For the dth root of unity $\omega_d = \exp(\frac{2\pi i}{d})$ consider the diagonal matrix

$$D = \begin{pmatrix} 1 & & & & \\ & \omega_d & & & \\ & & \omega_d^2 & & \\ & & & \ddots & \\ & & & & \omega_d^{d-1} \end{pmatrix} \in B(\mathbb{C}^d).$$

Show that the powers D^l for $l \in \{0, \ldots, d-1\}$ are orthogonal with respect to the Hilbert-Schmidt inner product.

3. Finally, define unitary operators $U_{kl} = S^k D^l$ and show that they form an orthogonal basis for the Hilbert-Schmidt inner product space $B(\mathbb{C}^d)$. What operators do you get for $d = 2$?

Problem 17. Alice and Bob are playing a quantum guessing game similar to the guessing games we have considered before. Alice has a quantum device with two buttons labeled "0" and "1". After pressing the button "0" the device emits a particle in quantum state $\rho_0 \in D(\mathcal{H})$, and after pressing the button "1" the device emits a particle in quantum state $\rho_1 \in D(\mathcal{H})$. Bob catches the emitted particle and measures it using some POVM. Then, he tries to guess whether Alice pressed button 0 or button 1. Let us assume that Alice presses button "0" with probability 1/2 and button "1" with probability 1/2, then, what is the optimal success probability of Bob's guess?

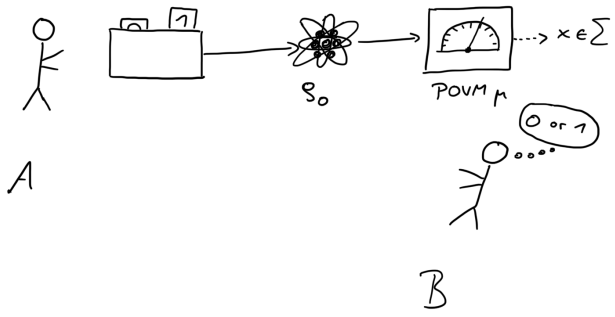


Figure 2: Alice and Bob at work.

1. Let $\mu : \Sigma \to B(\mathcal{H})^+$ denote a POVM that Bob could use to measure the system. Show that after Bob has performed the measurement μ the optimal success probability of Bob guessing the button Alice has pushed is given by

$$p_{opt}(\mu) = \frac{1}{2} + \frac{1}{4} \sum_{x \in \Sigma} |\operatorname{Tr}[\mu(x)(\rho_0 - \rho_1)]|.$$

2. Let p_{opt} denote the optimal probability of Bob guessing correctly, i.e., the solution to the optimization problem

$$p_{opt} = \sup\{p_{opt}(\mu) \ : \ \mu : \Sigma \to B(\mathcal{H})^+ \text{ POVM}\}.$$

Argue that the supremum is attained for a measurement with alphabet $\Sigma = \{1, \ldots, d^2\}$ with $d = \dim(\mathcal{H})$.

3. Define the 1-norm of an operator $X \in B(\mathcal{H})$ as

$$\|X\|_1 = \mathrm{Tr}\left[|X|\right],$$

where $|X|$ denotes the positive square root of $X^\dagger X$. Show that the 1-norm $\|X\|_1$ coincides with the sum of singular values of X. Finally, find a measurement $\mu : \{1, \ldots, d\} \to B(\mathcal{H})^+$ such that

$$p_{opt}(\mu) = \frac{1}{2} + \frac{1}{4}\|\rho_0 - \rho_1\|_1.$$

Is this the optimal value p_{opt}?

Sheet 6

Problem 18 (Identifying operators)**.** Show that for complex Euclidean spaces $\mathcal{H}_A, \mathcal{H}_B$ we have

$$B(\mathcal{H}_A) \otimes B(\mathcal{H}_B) \simeq B(\mathcal{H}_A \otimes \mathcal{H}_B).$$

Is it true that as vector spaces over $\mathbb{R}$ we have

$$B(\mathcal{H}_A)_{sa} \otimes B(\mathcal{H}_B)_{sa} \simeq B(\mathcal{H}_A \otimes \mathcal{H}_B)_{sa}, \tag{2}$$

for complex Euclidean spaces $\mathcal{H}_A, \mathcal{H}_B$? Is (2) true if $\mathcal{H}_A$ and $\mathcal{H}_B$ are real Euclidean spaces?

Problem 19 (Vectorization)**.** Consider complex Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ and let $d_A = \dim(\mathcal{H}_A)$ and $d_B = \dim(\mathcal{H}_B)$. Let us define the vectorization map $\mathrm{vec} : B(\mathcal{H}_A, \mathcal{H}_B) \to \mathcal{H}_A \otimes \mathcal{H}_B$ by

$$\mathrm{vec}(|v\rangle\langle w|) = |v\rangle \otimes \overline{|w\rangle},$$

and extended linearily.

1. Show that $\mathrm{vec} : B(\mathcal{H}_A, \mathcal{H}_B) \to \mathcal{H}_A \otimes \mathcal{H}_B$ is an isometric isomorphism between the complex Euclidean spaces $B(\mathcal{H}_A, \mathcal{H}_B)$, i.e., the linear operators $X_{A\to B} : \mathcal{H}_A \to \mathcal{H}_B$ with the Hilbert-Schmidt inner product, and $\mathcal{H}_A \otimes \mathcal{H}_B$.

2. Consider a vector $|v_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and define an operator $X_{A\to B} : \mathcal{H}_A \to \mathcal{H}_B$ such that $|v_{AB}\rangle = \mathrm{vec}(X_{A\to B})$. Using the singular value decomposition of $X_{A\to B}$ show that there exist orthonormal bases $\{|a_i\rangle\}_i$ of $\mathcal{H}_A$ and $\{|b_i\rangle\}_i$ of $\mathcal{H}_B$, and positive numbers $\lambda_i \geq 0$ such that

$$|v_{AB}\rangle = \sum_{i=1}^{\min(d_A,d_B)} \lambda_i |a_i\rangle \otimes |b_i\rangle.$$

Problem 20 (The partial transpose)**.** Recall the maximally entangled state

$$\omega_{\mathcal{H}} = \frac{1}{\dim(\mathcal{H})} |\Omega_{\mathcal{H}}\rangle\langle\Omega_{\mathcal{H}}|,$$

where

$$|\Omega_{\mathcal{H}}\rangle = \sum_{i=1}^{\dim(\mathcal{H})} |i\rangle \otimes |i\rangle.$$

1. Consider the transpose map $\vartheta : B(\mathcal{H}) \to B(\mathcal{H})$ given by $\vartheta(X) = X^T$ in the computational basis. Let $P \in B(\mathcal{H})^+$ be positive semidefinite and show that $\vartheta(P) = P^T$ is positive semidefinite as well.

2. Define the map $(\mathrm{id}_{\mathcal{H}} \otimes \vartheta) : B(\mathcal{H}) \otimes B(\mathcal{H}) \to B(\mathcal{H}) \otimes B(\mathcal{H})$ by setting $(\mathrm{id}_{\mathcal{H}} \otimes \vartheta)(X \otimes Y) = X \otimes Y^T$ and extended linearily. Compute $(\mathrm{id}_{\mathcal{H}} \otimes \vartheta)(\omega_{\mathcal{H}})$ and show that this operator is not positive semidefinite. Hint: Try it first in $\mathbb{C}^2$ and write down matrices.

3. Show that $(\mathrm{id}_{\mathcal{H}} \otimes \vartheta)(\rho_{AB})$ is positive semidefinite whenever ρ_{AB} is separable. Conclude that $\omega_{\mathcal{H}}$ is entangled.

Problem 21 (The realignment criterion)**.** For complex Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ we define the realignment map $R : B(\mathcal{H}_A \otimes \mathcal{H}_B) \to B(\mathcal{H}_B \otimes \mathcal{H}_B, \mathcal{H}_A \otimes \mathcal{H}_A)$ by

$$R\left(|i_A\rangle\langle j_A| \otimes |k_B\rangle\langle l_B|\right) = |i_A\rangle\langle k_B| \otimes |j_A\rangle\langle l_B|,$$

and extended linearily.

1. Show that

$$R(X \otimes Y) = |\,\mathrm{vec}(X^T)\rangle\langle \mathrm{vec}(Y^T)|,$$

for any $X \in B(\mathcal{H}_A)$ and $Y \in B(\mathcal{H}_B)$. Here, $\mathrm{vec}(\cdot)$ denotes the vectorization operation from exercise 2.

2. Assume that $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a separable quantum state. Show that

$$\|R(\rho_{AB})\|_1 \leq 1.$$

Here, $\|\cdot\|_1$ denotes the 1-norm, i.e., the norm given by

$$\|A\|_1 = \mathrm{Tr}\left[\sqrt{A^\dagger A}\right],$$

for any $A \in B(\mathcal{H})$, which also equals the sum of singular values of A.

3. Show that the maximally entangled state $\omega_{\mathcal{H}}$ satisfies

$$\|R(\omega_{\mathcal{H}})\|_1 > 1,$$

showing that $\omega_{\mathcal{H}}$ is entangled.

Sheet 7

Problem 22. For a complex Euclidean space $\mathcal{H}$ consider the maximally entangled vector

$$|\Omega_{\mathcal{H}}\rangle = \sum_{i=1}^{\dim(\mathcal{H})} |i\rangle \otimes |i\rangle,$$

and the maximally entangled state

$$\omega_{\mathcal{H}} = \frac{1}{\dim(\mathcal{H})} |\Omega_{\mathcal{H}}\rangle\langle\Omega_{\mathcal{H}}|.$$

1. Show that we have

$$(\mathbb{1}_{\mathcal{H}} \otimes X)|\Omega_{\mathcal{H}}\rangle = (X^T \otimes \mathbb{1}_{\mathcal{H}'})|\Omega_{\mathcal{H}'}\rangle$$

holds for any complex Euclidean space $\mathcal{H}'$ and any operator $X \in B(\mathcal{H}, \mathcal{H}')$, where the transpose is in the computational basis.

2. Consider the so-called partial trace $(\mathrm{id}_{\mathcal{H}} \otimes \mathrm{Tr}) : B(\mathcal{H} \otimes \mathcal{H}) \to B(\mathcal{H})$ defined as $(\mathrm{id}_{\mathcal{H}} \otimes \mathrm{Tr})(X \otimes Y) = \mathrm{Tr}[Y]\, X$ for $X, Y \in B(\mathcal{H})$ and extended linearily. For an operator $Z \in B(\mathcal{H})$ we define the vector

$$|v_Z\rangle = (\mathbb{1}_{\mathcal{H}} \otimes Z)|\Omega_{\mathcal{H}}\rangle.$$

Show that

$$(\mathrm{id}_{\mathcal{H}} \otimes \mathrm{Tr})\left[|v_Z\rangle\langle v_Z|\right] = Z^T \overline{Z}.$$

3. Show that for any quantum state $\rho \in D(\mathcal{H})$ there exists an operator $Z \in B(\mathcal{H})$ satisfying $\langle Z, Z \rangle_{HS} = 1$ such that

$$(\mathrm{id}_{\mathcal{H}} \otimes \mathrm{Tr})\left[|v_Z\rangle\langle v_Z|\right] = \rho.$$

Problem 23 (Product measurements)**.** Consider a composite quantum system with a state space $\mathcal{H}_A \otimes \mathcal{H}_B$ for complex Euclidean spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. Let $\alpha : \Sigma_A \to B(\mathcal{H}_A)^+$ and $\beta : \Sigma_B \to B(\mathcal{H}_B)^+$ denote POVMs and recall that the POVM $\gamma : \Sigma_A \times \Sigma_B \to B(\mathcal{H}_A \otimes \mathcal{H}_B)^+$ corresponding to the simultaneous measurement of α on the A-subsystem and β on the B-subsystem is given by

$$\gamma(a, b) = \alpha(a) \otimes \beta(b), \tag{3}$$

for any $a \in \Sigma_A$ and any $b \in \Sigma_B$

1. In the case where $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}$ we consider the maximally entangled state $\rho_{AB} = \omega_{\mathcal{H}}$ from the previous exercise. Show that

$$\mathrm{Tr}\left[\gamma(a, b)\omega_{\mathcal{H}}\right] = \frac{1}{\dim(\mathcal{H})}\langle\overline{\alpha(a)}, \beta(b)\rangle_{HS},$$

   for any $a, b \in \Sigma$, and where the conjugation is in the computational basis.

2. Show that the POVM $\gamma : \Sigma_A \times \Sigma_B \to B(\mathcal{H}_A \otimes \mathcal{H}_B)^+$ from above is the only POVM for which the formula

$$\mathrm{Tr}\left[\gamma(a, b)\rho_{AB}\right] = \mathrm{Tr}\left[\alpha(a)\sigma_A\right]\mathrm{Tr}\left[\beta(b)\tau_B\right].$$

   holds for any product state $\rho_{AB} = \sigma_A \otimes \tau_B$. Argue why this formula makes sense physically if product states represent the quantum states of joint quantum systems whose components have never interacted.

Problem 24. Assume that Alice and Bob perform a correlation experiment involving quantum systems with state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ in a quantum state $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$. Alice is using POVMs $\alpha_1, \ldots, \alpha_n : \Sigma \to B(\mathcal{H}_A)^+$ and Bob is using POVMs $\beta_1, \ldots, \beta_n : \Sigma \to B(\mathcal{H}_B)^+$ giving rise to the correlation $(P(a, b|A_i, B_j))_{a,b,i,j}$ given by

$$P(a, b|i, j) = \mathrm{Tr}\left[(\alpha_i(a) \otimes \beta_j(b))\rho_{AB}\right].$$

1. Show that this correlation is classical if ρ_{AB} is separable.

2. Conclude that the maximally entangled state $\omega_{\mathbb{C}^2} \in D(\mathbb{C}^2 \otimes \mathbb{C}^2)$ is entangled.

Problem 25. Let $n \in \mathbb{N}$ and Σ denote a finite alphabet. Assume that Alice and Bob perform some correlation experiment giving rise to a correlation $(P(a,b|A_i,B_j))_{a,b,i,j}$ with $a,b \in \Sigma$ and $i,j \in \{1,\ldots,n\}$. We call the correlation *non-signalling* if

$$\sum_{b\in\Sigma} P(a,b|A_i,B_j) = \sum_{b\in\Sigma} P(a,b|A_i,B_{j'})$$

for all $a \in \Sigma$ and any $i,j,j' \in \{1,\ldots,n\}$, and if

$$\sum_{a\in\Sigma} P(a,b|A_i,B_j) = \sum_{a\in\Sigma} P(a,b|A_{i'},B_j)$$

for all $b \in \Sigma$ and any $i,i',j \in \{1,\ldots,n\}$. The interpretation of these equations is that the probability distribution observed by Alice should not depend on Bob's choice of measurement, and the probability distribution observed by Bob should not depend on the choice of Alice's measurement.

1. Show that quantum correlations are non-signalling.

2. Show that the following correlation is not a quantum correlation.

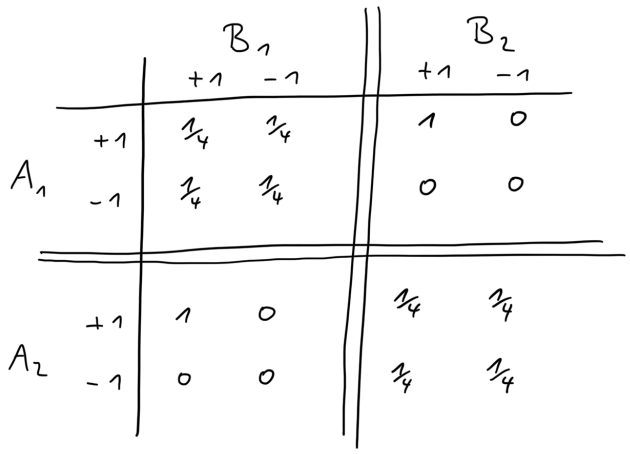


Figure 3: A correlation.

3. (**Bonus question:**) Show that the following correlation is non-signalling and not a quantum correlation.

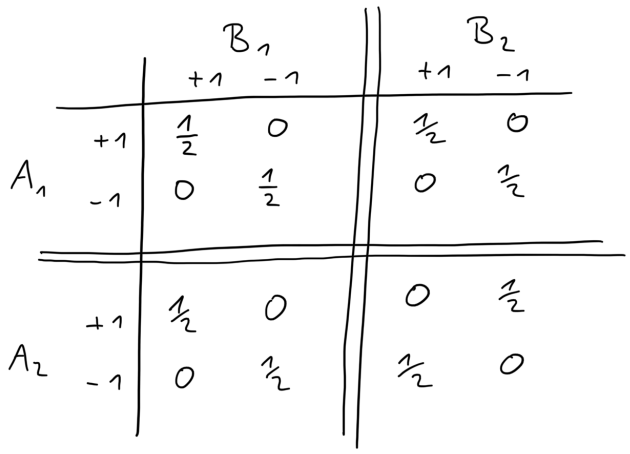


Figure 4: Yet another correlation.

Compare this correlation with the quantum correlation violating the CHSH inequality.

Sheet 8

Problem 26. Go through the material on quantum theory we have covered so far and think of a *good* question. Submit your question.

Sheet 9

Problem 27 (Monogamy of entanglement)**.** Show that all purifications of a pure state $\rho_A = |\psi\rangle\langle\psi| \in D(\mathcal{H}_A)$ are of the form

$$\rho_{AE} = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|.$$

Now consider a composite quantum system 'AB' with tensor product state space $\mathcal{H}_A \otimes \mathcal{H}_B$ and assume that it is in a pure entangled quantum state $|\psi_{AB}\rangle\langle\psi_{AB}| \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$. Argue that there is no third quantum system that is entangled with the composite system 'AB'.

Problem 28 (Examples of quantum channels)**.** Consider an isometry $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$. Show that the map $T : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ given by

$$T(X) = \mathrm{Tr}_E \left[V X V^\dagger \right],$$

is a quantum channel, i.e., it is completely positive and trace-preserving.

Problem 29 (Purifications and reduced density matrices)**.** Consider a pure quantum state $|\psi_{AB}\rangle\langle\psi_{AB}| \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ and denote by ρ_A and ρ_B its two marginals, i.e.,

$$\rho_A = \mathrm{Tr}_B\left[|\psi_{AB}\rangle\langle\psi_{AB}|\right] \quad \text{, and} \quad \rho_B = \mathrm{Tr}_A\left[|\psi_{AB}\rangle\langle\psi_{AB}|\right].$$

Show the following statements:

1. The spectra of ρ_A and ρ_B are the same. What is the relationship between the eigenvalues of these operators and the Schmidt coefficients of $|\psi_{AB}\rangle$?

2. There exists an operator $X \in B(\mathcal{H}_A, \mathcal{H}_B)$ such that

$$\rho_A = X^T\overline{X} \text{ and } \rho_B = XX^\dagger.$$

Problem 30. Consider a quantum state $\rho_A \in D(\mathcal{H}_A)$ with a purification $|\psi_{EA}\rangle\langle\psi_{EA}| \in D(\mathcal{H}_E \otimes \mathcal{H}_A)$ for some complex Euclidean space $\mathcal{H}_E$. Show that there is a complex Euclidean space $\mathcal{H}_{E'}$ with $\dim(\mathcal{H}_{E'}) = \mathrm{rk}\,(\rho_A)$ and a purification $|\phi_{E'A}\rangle\langle\phi_{E'A}| \in D(\mathcal{H}_{E'} \otimes \mathcal{H}_A)$ of ρ_A such that

$$|\psi_{EA}\rangle = (V \otimes \mathbb{1}_{\mathcal{H}_A})|\phi_{E'A}\rangle,$$

for some isometry $V : \mathcal{H}_{E'} \to \mathcal{H}_E$.

Sheet 10

Problem 31.

1. Let $V : \mathcal{H}_A \to \mathcal{H}_A \otimes \mathcal{H}_E$ denote an isometry and $|\psi_E\rangle \in \mathcal{H}_E$ a normalized vector. Show that there exists a unitary $U : \mathcal{H}_A \otimes \mathcal{H}_E \to \mathcal{H}_A \otimes \mathcal{H}_E$ such that
$$U(\mathbb{1}_{\mathcal{H}_A} \otimes |\psi_E\rangle) = V.$$

2. Show that for any quantum channel $T : B(\mathcal{H}) \to B(\mathcal{H})$ there exists a complex Euclidean space $\mathcal{H}_E$ such that for any normalized vector $|\psi_E\rangle \in \mathcal{H}_E$ there exists a unitary $U : \mathcal{H} \otimes \mathcal{H}_E \to \mathcal{H} \otimes \mathcal{H}_E$ such that

$$T(X) = \mathrm{Tr}_E\left[U(X \otimes |\psi_E\rangle\langle\psi_E|)U^\dagger\right].$$

for any $X \in B(\mathcal{H}_A)$. What is the minimal dimension of $\mathcal{H}_E$ needed to represent every quantum channel $T : B(\mathcal{H}) \to B(\mathcal{H})$ for a fixed complex Euclidean space $\mathcal{H}$.

Problem 32 (The amplitude damping channel)**.** For $\gamma \in [0,1]$ we define the *amplitude-damping channel* $N_\gamma : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ by

$$N_\gamma \left[\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \right] = \begin{pmatrix} x_{11} + \gamma x_{22} & \sqrt{1-\gamma} x_{12} \\ \sqrt{1-\gamma} x_{21} & (1-\gamma) x_{22} \end{pmatrix}.$$

1. Compute the Choi matrix of N_γ. Show that N_γ is indeed a quantum channel.

2. Compute a Choi-Kraus representation of N_γ.

3. Compute a Stinespring dilation of N_γ.

Problem 33 (Depolarizing channels)**.** For $p \in \mathbb{R}$ we define the map $D_p : B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ by

$$D_p(X) = (1-p) \operatorname{Tr}[X] \frac{\mathbb{1}_d}{d} + pX,$$

for any $X \in B(\mathbb{C}^d)$.

1. Compute the Choi operator of D_p. For which parameters $p \in \mathbb{R}$ is D_p a quantum channel?

2. Compute the Choi-Kraus representation of D_p for the values of p where it is a quantum channel.

3. Compute the Stinespring dilation of D_p for the values of p where it is a quantum channel.

4. Compute a complementary channel D_p^c for dimension $d = 2$ of D_p for the values of p where it is a quantum channel.

Problem 34 (Quantum teleportation)**.** Consider again the two researchers Alice and Bob who each have a laboratory. Alice's laboratory contains two quantum systems labelled 'A' and '$\tilde{A}$' and Bob's laboratory contains a quantum system labelled 'B'. Each of these quantum systems is a qubit. Initially, 'A' and 'B' are in a maximally entangled state. Assume furthermore, that the system '$\tilde{A}$' is initially in some quantum state $\rho_{\tilde{A}} \in D(\mathcal{H}_{\tilde{A}})$ unknown to Alice and Bob. Quantum teleportation is a protocol that lets Alice send this unknown state to Bob by performing a measurement and sending the measurement outcome to Bob. Proceed as follows:

1. Recall the Bell basis $\{|\psi_{ij}\rangle\}_{ij} \subset \mathbb{C}^2 \otimes \mathbb{C}^2$ given by

$$|\psi_{ij}\rangle = \frac{1}{\sqrt{2}} \operatorname{vec}(\sigma_{ij}),$$

where

$$\sigma_{00} = \mathbb{1}_2, \quad \sigma_{01} = \sigma_x, \quad \sigma_{10} = \sigma_y, \quad \sigma_{11} = \sigma_z,$$

are the identity matrix and the Pauli matrices. Compute the probability of obtaining the outcome $(k, l) \in \{0, 1\}^2$ when measuring the subsystems '$\tilde{A}A$' of the quantum state

$$\sigma_{ini} = \rho_{\tilde{A}} \otimes \omega_{AB},$$

using the von-Neumann measurement $\{|\psi_{ij}\rangle\langle\psi_{ij}|\}_{i,j}$ defined via the Bell basis.

2. What is the post-measurement state σ_{post}^{ij} after obtaining outcome (i, j) in the measurement of (1)?

3. If Alice communicates the measurement outcome (i, j) of the Bell measurement to Bob, what quantum channel can he apply so that his system is in the final state $\rho_{\tilde{A}}$?

4. How can we extend this protocol to quantum systems with dimension $d > 2$?

Problem 35.

1. Consider complex Euclidean spaces $\mathcal{H}$ and $\mathcal{H}'$ such that $\dim(\mathcal{H}) \leq \dim(\mathcal{H}')$. Let $\{|v_i\rangle\}_{i=1}^k \subset \mathcal{H}$ and $\{|w_i\rangle\}_{i=1}^k \subset \mathcal{H}'$ denote orthonormal sets of vectors. Show that there exists an isometry $V : \mathcal{H} \to \mathcal{H}'$ such that $V|v_i\rangle = |w_i\rangle$ for all $i \in \{1, \ldots, k\}$.

2. Let $\mathcal{H}_A, \mathcal{H}_E$ and $\mathcal{H}_{E'}$ denote complex Euclidean spaces. Consider a purification $|\psi_{AE}\rangle\langle\psi_{AE}| \in D(\mathcal{H}_A \otimes \mathcal{H}_E)$ of a quantum state $\rho_A \in D(\mathcal{H}_A)$ and a quantum state $\sigma_{AE'} \in D(\mathcal{H}_A \otimes \mathcal{H}_{E'})$ such that $\operatorname{Tr}_{E'}[\sigma_{AE'}] = \rho_A$. Show that there exists a quantum channel $S : B(\mathcal{H}_E) \to B(\mathcal{H}_{E'})$ such that

$$(\mathrm{id}_A \otimes S)(|\psi_{AE}\rangle\langle\psi_{AE}|) = \sigma_{AE'}.$$

Hint: Start by reducing the problem to the case, where $\sigma_{AE'}$ is a pure state as well.

Sheet 11

Problem 36 (The fully depolarizing channel)**.** Consider the fully depolarizing channel $\Delta : B(\mathbb{C}^d) \to B(\mathbb{C}^d)$ given by

$$\Delta(X) = \mathrm{Tr}\,[X]\,\frac{\mathbb{1}_{\mathbb{C}^d}}{d}.$$

1. Show that there exist unitary operators $\{U_1, \ldots, U_{d^2}\} \subset \mathcal{U}\left(\mathbb{C}^d\right)$ such that

$$\Delta = \frac{1}{d^2}\sum_{i=1}^{d^2} \mathrm{Ad}_{U_i}\,.$$

   (Hint: Use the Choi-Jamiolkowski isomorphism to figure out which sets of unitary operators work here. Then, use a previous exercise.)

2. Consider a quantum channel $T : B(\mathbb{C}^{d_A}) \to B(\mathbb{C}^{d_B})$. Use the open-system representation of T to show that there exists a dimension $d_E \in \mathbb{N}$ and a pure quantum state $|\psi_{EB}\rangle\langle\psi_{EB}| \in D\left(\mathbb{C}^{d_E} \otimes \mathbb{C}^{d_B}\right)$ such that

$$\frac{\mathbb{1}_{\mathbb{C}^{d_A}}}{d_A} \otimes \frac{\mathbb{1}_{\mathbb{C}^{d_E}}}{d_E} \otimes T(X) = \frac{1}{d_E^2 d_A^2}\sum_{i=1}^{d_E^2}\sum_{j=1}^{d_A^2} \mathrm{Ad}_{\left(U_i^A \otimes V_j^E \otimes \mathbb{1}_{d_B}\right)} \circ \mathrm{Ad}_W\left(X \otimes |\psi_{EB}\rangle\langle\psi_{EB}|\right),$$

   for some unitaries $\{U_1^A, \ldots, U_{d_A^2}^A\} \subset \mathcal{U}\left(\mathbb{C}^{d_A}\right)$ and $\{V_1^E, \ldots, V_{d_E^2}^E\} \subset \mathcal{U}\left(\mathbb{C}^{d_E}\right)$, and some unitary $W \in \mathcal{U}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_E} \otimes \mathbb{C}^{d_B}\right)$.

Problem 37 (Diagonalizing positive unital and trace-preserving qubit maps)**.** We want to diagonalize positive linear maps $P : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ satisfying $P(\mathbb{1}_{\mathbb{C}^2}) = \mathbb{1}_{\mathbb{C}^2}$ and $\mathrm{Tr}\,[P(X)] = \mathrm{Tr}\,[X]$ for any $X \in B(\mathbb{C}^2)$. For this we recall (from a previous exercise) that there is a 1-to-1 correspondence between the quantum states $D(\mathbb{C}^2)$ and the Euclidean unit ball $B_1(0) \subset \mathbb{R}^3$ (the Bloch ball) given by

$$\rho = \frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} + w \cdot \sigma\right) \in D(\mathbb{C}^2) \quad \longleftrightarrow \quad w \in B_1(0),$$

where we use the shorthand

$$w \cdot \sigma = \sum_{i=1}^{3} w_i \sigma_i,$$

with the Pauli matrices

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We will sometimes write $\sigma_0 = \mathbb{1}_{\mathbb{C}^2}$ and we recall that the real span of $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$ is $B(\mathbb{C}^2)_{sa}$ and the complex span is $B(\mathbb{C}^2)$. Proceed as follows:

1. Consider a positive map $P : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ satisfying $P(\mathbb{1}_{\mathbb{C}^2}) = \mathbb{1}_{\mathbb{C}^2}$ and $\operatorname{Tr}[P(X)] = \operatorname{Tr}[X]$ for any $X \in B(\mathbb{C}^2)$. Show that $M_{ij} = \frac{1}{2}\operatorname{Tr}[\sigma_j P(\sigma_i)] \in \mathbb{R}$ for every $i, j \in \{1, 2, 3\}$ and that

$$P\left(\frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} + w \cdot \sigma\right)\right) = \frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} + (Mw) \cdot \sigma\right),$$

   for any $w \in \mathbb{R}^3$, where we introduced $M \in B(\mathbb{R}^3)$ with entries M_{ij}.

2. Consider the unitary

$$U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

   Find an $R \in \mathrm{SO}(3)$ such that

$$\mathrm{Ad}_U\left(\frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} + w \cdot \sigma\right)\right) = \frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} + (Rw) \cdot \sigma\right).$$

3. Now, consider a general $R \in \mathrm{SO}(3)$, i.e., corresponding to a 3-dimensional rotation of the ball $B_1(0)$. Show that there exists a $U \in \mathcal{U}(\mathbb{C}^2)$ such that

$$\mathrm{Ad}_U\left(\frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} + w \cdot \sigma\right)\right) = \frac{1}{2}\left(\mathbb{1}_{\mathbb{C}^2} + (Rw) \cdot \sigma\right).$$

   Hint: Start with rotations around the coordinate axes. Then, use that a general $R \in \mathrm{SO}(3)$ can be written as the product three rotations around the coordinate axes with certain rotation angles (sometimes called *Euler angles*).

4. Consider a positive map $P : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ satisfying $P(\mathbb{1}_{\mathbb{C}^2}) = \mathbb{1}_{\mathbb{C}^2}$ and $\operatorname{Tr}[P(X)] = \operatorname{Tr}[X]$ for any $X \in B(\mathbb{C}^2)$. Use a modified singular value decomposition to show that there are unitary matrices $U_1, U_2 \in \mathcal{U}(\mathbb{C}^2)$ satisfying

$$\left(\mathrm{Ad}_{U_1} \circ P \circ \mathrm{Ad}_{U_2}\right)(\sigma_i) = \lambda_i \sigma_i,$$

   for any $i \in \{0, 1, 2, 3\}$ and some real numbers $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$ and $\lambda_0 = 1$.

Problem 38 (Visualizing positive maps)**.** For $\lambda = (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$, consider the trace-preserving map $P_\lambda : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ such that $P_\lambda(\mathbb{1}_{\mathbb{C}^2}) = \mathbb{1}_{\mathbb{C}^2}$ and

$$P_\lambda(\sigma_i) = \lambda_i \sigma_i$$

for $i \in \{1, 2, 3\}$.

1. For which $\lambda \in \mathbb{R}^3$ is P_λ positive? Visualize this set.

2. For which $\lambda \in \mathbb{R}^3$ is P_λ completely positive? Visualize this set.

   Hint: Compute the Choi-Jamiolkowski operator of P_λ. Use that $\sigma_i \otimes \sigma_i$ and $\sigma_j \otimes \sigma_j$ commute and are simultaneously diagonalized by the Bell basis.

3. For which $\lambda \in \mathbb{R}^3$ is $P_\lambda = \vartheta \circ T$ for the transpose $\vartheta : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ and a completely positive map $T : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$? Visualize this set.

4. Using your visualizations and Exercise 37, show that any positive map $P : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ satisfying $P(\mathbb{1}_{\mathbb{C}^2}) = \mathbb{1}_{\mathbb{C}^2}$ and $\operatorname{Tr}[P(X)] = \operatorname{Tr}[X]$ for any $X \in B(\mathbb{C}^2)$ can be written as

   $$P = T_1 + \vartheta \circ T_2,$$

   for completely positive maps $T_1, T_2 : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ and the transpose map $\vartheta : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$.

Problem 39 (Entanglement manipulation)**.** Let $\mathcal{H}_{A_1}, \mathcal{H}_{A_2}, \mathcal{H}_{B_1}, \mathcal{H}_{B_2}$ denote complex Euclidean spaces. A quantum channel

$$T : B(\mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1}) \to B(\mathcal{H}_{A_2} \otimes H_{\mathcal{B}_2})$$

is called a *separable*[1] *quantum channel* if it can be written as

$$T = \sum_{n=1}^{N} S_A^{(n)} \otimes R_B^{(n)},$$

for completely positive maps $S_A^{(n)} : B(\mathcal{H}_{A_1}) \to B(\mathcal{H}_{A_2})$ and $R_B^{(n)} : B(\mathcal{H}_{B_1}) \to B(\mathcal{H}_{B_2})$. Let us denote the set of separable channels by

$$\operatorname{SepC}((\mathcal{H}_{A_1}, \mathcal{H}_{B_1}) \to (\mathcal{H}_{A_2}, \mathcal{H}_{B_2})).$$

[1] Do not confuse this with separable quantum states!

1. Show that $T(\rho_{AB}) \in \mathrm{Sep}(\mathcal{H}_{A_2}, \mathcal{H}_{B_2})$ for any $\rho_{AB} \in \mathrm{Sep}(\mathcal{H}_{A_1}, \mathcal{H}_{B_1})$ and any $\mathrm{SepC}((\mathcal{H}_{A_1}, \mathcal{H}_{B_1}) \to (\mathcal{H}_{A_2}, \mathcal{H}_{B_2}))$. The separable states are preserved under separable operations!

2. Using the teleportation protocol, construct a separable quantum channel

$$T \in \mathrm{SepC}\left((\mathbb{C}^2 \otimes \mathbb{C}^2, \mathbb{C}^2) \to (\mathbb{C}^2 \otimes \mathbb{C}^2, \mathbb{C}^2)\right),$$

such that

$$T(\rho \otimes \omega_{AB}) = \frac{1}{4}(\mathbb{1}_{\mathbb{C}^2} \otimes \mathbb{1}_{\mathbb{C}^2}) \otimes \rho \in D(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2),$$

for any quantum state $\rho \in D(\mathbb{C}^2)$ and where $\omega_{AB} \in D(\mathbb{C}^2 \otimes \mathbb{C}^2)$ denotes the (normalized) maximally entangled state. How does this result generalize to dimensions $d > 2$.

3. Show that any quantum state $\rho \in D(\mathbb{C}^d \otimes \mathbb{C}^d)$ can be written as

$$\rho = T(\omega_d),$$

for some separable quantum channel $T \in \mathrm{SepC}\left((\mathbb{C}^d, \mathbb{C}^d) \to (\mathbb{C}^d, \mathbb{C}^d)\right)$, and where $\omega_d \in D(\mathbb{C}^d \otimes \mathbb{C}^d)$ denotes the normalized maximally entangled state. This is why ω_d is called *maximally* entangled.

Sheet 12

Problem 40 (Properties of the von Neumann entropy)**.** For a quantum state $\rho \in D(\mathcal{H})$ we define the *von Neumann entropy* as

$$H(\rho) = -\operatorname{Tr}[\rho \log(\rho)],$$

where the logarithm is in base 2.

1. Show that $0 \leq H(\rho) \leq \log(\dim(\mathcal{H}))$. For which quantum states do we have $H(\rho) = 0$ and for which quantum states do we have $H(\rho) = \log(\dim(\mathcal{H}))$?

2. Assume that $\rho = \operatorname{Tr}_B[|\psi_{AB}\rangle\langle\psi_{AB}|]$ and $\sigma = \operatorname{Tr}_A[|\psi_{AB}\rangle\langle\psi_{AB}|]$ for some pure state $|\psi_{AB}\rangle \in H_A \otimes H_B$. Show that $H(\rho) = H(\sigma)$.

3. Consider a probability distribution $p \in \mathcal{P}(\{1, \ldots, N\})$ and quantum states $\rho_1, \ldots, \rho_N \in D(\mathcal{H})$ satisfying $\rho_i \rho_j = 0$ for whenever $i \neq j$. Show that

$$H\left(\sum_{i=1}^N p_i \rho_i\right) = H(p) + \sum_{i=1}^N p_i H(\rho_i).$$

Problem 41 (Some classical information theory)**.** For finite alphabets Σ_A and Σ_B let $N : \Sigma_A \to \mathcal{P}(\Sigma_B)$ denote a classical channel. Show that

$$C(N) \leq \min(\log(|\Sigma_A|), \log(|\Sigma_B|)).$$

Problem 42 (The fidelity)**.** Let $\mathcal{H}$ denote a complex Euclidean space. For quantum states $\rho, \sigma \in D(\mathcal{H})$, we define the *fidelity* by

$$F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1,$$

where $\sqrt{\cdot}$ denotes the unique positive square root and $\|\cdot\|_1$ is the trace norm (i.e., the matrix 1-norm). The fidelity measures the distance between the two quantum states, and in the following we will prove some of its properties.

1. Show that
$$F(\rho, \sigma) = \operatorname{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right],$$
for all quantum states $\rho, \sigma \in D(\mathcal{H})$.
2. Show that $F(\rho, \sigma) = F(\sigma, \rho)$ for all quantum states $\rho, \sigma \in D(\mathcal{H})$.
3. Show $F(\rho, \sigma) \geq 0$ with equality if and only if $\rho\sigma = 0$.
4. Show that $F(\rho, \sigma) \leq 1$ with equality if and only if $\rho = \sigma$.
5. Show that $F(V\rho V^\dagger, V\sigma V^\dagger) = F(\rho, \sigma)$ for any isometry $V : \mathcal{H} \to \mathcal{H}'$ into a complex Euclidean space $\mathcal{H}'$.
6. Show that $F(|\psi\rangle\langle\psi|, \sigma) = \sqrt{\langle\psi|\sigma|\psi\rangle}$ for any pure quantum state $|\psi\rangle\langle\psi| \in B(\mathcal{H})$ and any $\sigma \in D(\mathcal{H})$.

Problem 43 (Entropies and measurements)**.** Consider a quantum state $\rho \in D(\mathcal{H})$ and a projection-valued measure $\mu : \Sigma \to B(\mathcal{H})^+$, i.e., a POVM such that the operators $\mu(x)$ are projections. Recall that measuring ρ using μ gives an outcome $x \in \Sigma$ with probability

$$p(x) = \operatorname{Tr}\left[\mu(x)\rho\right],$$

and after obtaining this outcome, the system will be in the quantum state

$$\rho_x = \frac{\mu(x)\rho\mu(x)}{\operatorname{Tr}\left[\mu(x)\rho\right]}.$$

If we do *not* learn the outcome $x \in \Sigma$ of the measurement, then the quantum system is in the quantum state

$$\rho_{meas} = \sum_{x\in\Sigma} p(x)\rho_x = \sum_{x\in\Sigma} \mu(x)\rho\mu(x).$$

1. Show that
$$H(\rho_{meas}) \geq H(\rho),$$
i.e., a projective measurement increases the entropy if we do not learn the measurement outcome. (*Hint:* You may use the data-processing inequality for the relative entropy, but there is also a way of solving the exercise without it.)

2. Find a 2-outcome instrument $\{T_1, T_2\}$ with completely positive maps $T_1, T_2 : B(\mathbb{C}^2) \to B(\mathbb{C}^2)$ and a quantum state $\rho \in D(\mathbb{C}^2)$ such that
$$H\left(T_1(\rho) + T_2(\rho)\right) < H(\rho).$$

Sheet 13

Problem 44. Go through the material we have covered so far and think of a *good* question. Submit your question.

Sheet 14

Problem 45. Let $\sigma \in D(\mathcal{H})$ denote a quantum state and consider the quantum channel $T_p : B(\mathcal{H}) \to B(\mathcal{H})$ with a parameter $p \in [0, 1]$ given by
$$T_p(X) = (1 - p)X + p \operatorname{Tr}[X]\, \sigma.$$
Show that we have
$$H\left(T_p^{\otimes n}(\rho)\right) \geq (1 - p)H(\rho) + pnH(\sigma),$$
for any $n \in \mathbb{N}$ and any $\rho \in D(\mathcal{H}^{\otimes n})$.

Hint: The case $\sigma = \mathbb{1}_{\mathcal{H}}/\dim(\mathcal{H})$ was done in the lectures.

Problem 46. Use the open-system representation of quantum channels to show that
$$\|T(X)\|_1 \leq \|X\|_1, \tag{4}$$
for every quantum channel $T : B(\mathcal{H}_A) \to B(\mathcal{H}_B)$ and every $X \in B(\mathcal{H}_A)$. In particular, this shows that for quantum states $\rho, \sigma \in D(\mathcal{H}_A)$ we have
$$\|T(\rho) - T(\sigma)\|_1 \leq \|\rho - \sigma\|_1.$$
Is (4) still true if we replace $\|\cdot\|_1$ by the Hilbert-Schmidt norm $\|\cdot\|_2$ or the operator norm $\|\cdot\|_\infty$?

Problem 47. Consider a quantum state $\rho_{AB} \in D(\mathcal{H}_A \otimes \mathcal{H}_B)$ and recall the quantum conditional entropy

$$H(A|B)_{\rho_{AB}} = H(\rho_{AB}) - H(\rho_B).$$

We aim to show that $H(A|B)_{\rho_{AB}} \geq 0$ whenever ρ_{AB} is separable.

1. Show that
$$H(A|B)_{\rho_{AB}} \geq 0,$$
whenever
$$\rho_{AB} = \sum_{i=1}^{k} p_i \sigma_i^A \otimes |i\rangle\langle i|.$$

2. Show that
$$H(A|B)_{\rho_{AB}} = H(\rho_A) - D(\rho_{AB} \| \rho_A \otimes \rho_B).$$

3. Show that for any quantum channel $T : B(\mathcal{H}_B) \to B(\mathcal{H}_{B'})$ we have
$$H(A|B')_{(\mathrm{id}_A \otimes T)(\rho_{AB})} \geq H(A|B)_{\rho_{AB}}.$$

4. Given a separable quantum state
$$\rho_{AB'} = \sum_{i=1}^{k} p_i \sigma_i^A \otimes \tau_i^{B'},$$
find a quantum channel $T : B(\mathcal{H}_B) \to B(\mathcal{H}_{B'})$ for $\mathcal{H}_B = \mathbb{C}^k$ such that
$$\rho_{AB'} = (\mathrm{id}_A \otimes T) \left(\sum_{i=1}^{k} p_i \sigma_i^A \otimes |i\rangle\langle i| \right).$$
Conclude that
$$H(A|B')_{\rho_{AB'}} \geq 0.$$

Problem 48 (Typical projectors)**.** Consider a quantum state $\rho \in D(\mathcal{H})$ with spectral decomposition $\rho = \sum_{x=1}^{d} p(x) |v_x\rangle\langle v_x|$ where $p \in \mathcal{P}(\{1, \ldots, d\})$ is a probability distribution and $|v_x\rangle \in \mathcal{H}$. Recall the ϵ-typical sequences $\mathcal{T}_{n,\epsilon}(p)$ from the first part of the course, and define a projector

$$\Pi_{n,\epsilon} = \sum_{(x_1,\ldots,x_n) \in \mathcal{T}_{n,\epsilon}(p)} |v_{x_1}\rangle\langle v_{x_1}| \otimes \cdots \otimes |v_{x_n}\rangle\langle v_{x_n}| \in B\left(\mathcal{H}^{\otimes n}\right).$$

Show the following statements:

1. For any $\epsilon > 0$ we have

$$\mathrm{Tr}\left[\Pi_{n,\epsilon}\rho^{\otimes n}\right] \to 1,$$

as $n \to \infty$.

2. We have

$$\mathrm{Tr}\left[\Pi_{n,\epsilon}\right] < 2^{nH(\rho)+\epsilon}.$$

3. For every $n \in \mathbb{N}$ let $\tilde{\Pi}_n \in B\left(\mathcal{H}^{\otimes n}\right)$ denote a projector such that $\mathrm{rank}\left(\tilde{\Pi}_n\right) \leq 2^{nR}$ for some $R < H(\rho)$. Show that

$$\mathrm{Tr}\left[\tilde{\Pi}_n\rho^{\otimes n}\right] \to 0,$$

as $n \to \infty$.

Sheet 15

Problem 49. Go through the material we have covered so far and think of a *good* question. Submit your question.