Exercise Sheet 2: Measurements and Co.

This sheet aims to deepen our understanding of the formalism of quantum information theory.

Measurements

Projective measurement. A projective measurement is described by a Hermitian observable A. We denote the unique eigenvalues of A as $\{\lambda_k\}_k$, and the eigenvectors as $\{|\psi_j\rangle\}_j$, which form an orthonormal basis. We index the eigenvectors with j because there could be multiple different eigenvectors for the same eigenvalue. To resolve this, we add a superscript to identify which individual eigenvalue corresponds to each eigenvector $\{|\psi_j^k\rangle\}_j$.

In the spectral decomposition of the observable,

$$A = \sum_k \lambda_k P_k, \tag{1}$$

the eigenvalues λ_k correspond to the possible outcomes from measuring A, and P_k are the projectors onto the subspaces corresponding to each eigenvalue:

$$P_k = \sum_{j:\mathrm{EV}\lambda_k} |\psi_j^k\rangle\langle\psi_j^k|, \tag{2}$$

where the sum is over all eigenvectors $|\psi_j^k\rangle$ associated to the eigenvalue λ_k.

11 P. Exercise 1.

2 P. (a) Upon measuring the observable A on the state $|\phi\rangle$, the probability of getting the result λ_k, $p(k)$, is the expected value of P_k on $|\phi\rangle$. Give two formulas for $p(k)$, one in terms of P_k and the other in terms of $|\psi_j^k\rangle$.

1 P. (b) If we observe the outcome λ_k, the state $|\phi\rangle$ gets projected onto the eigenspace of λ_k, becoming $|\phi_k^{\mathrm{post}}\rangle$. Give a formula for $|\phi_k^{\mathrm{post}}\rangle$ (do not forget the normalization).

2 P. (c) Consider the observable $A = X \otimes X$, where X is the Pauli-X operator. Give the spectral decomposition of A, identifying the eigenvalues $(\lambda_k)_k$ and the projectors to their corresponding eigenspaces[1] $(P_k)_k$.

3 P. (d) Consider A as defined in the previous exercise, and the following state $|\phi\rangle$:

$$|\phi\rangle = \frac{1}{\sqrt{30}} \begin{pmatrix} 1 \\ 2i \\ -3i \\ -4 \end{pmatrix}. \tag{3}$$

What are the probabilities of each possible outcome when measuring A on $|\phi\rangle$? What is the post-measurement state after observing λ_1? and after observing λ_{-1}?

3 P. (e) Given all of these, what is the (mixed) state ρ^{post} resulting from measuring A on $|\phi\rangle$ if we do not observe the measurement outcome? What is the purity[2] of ρ^{post}?

[1] Sanity check, you should have $\sum_k P_k = \mathbb{I}$ the identity matrix.
[2] Recall that the purity of a state ρ is computed as $\mathrm{Tr}[\rho^2]$

POVMs. From a theoretical perspective, a measurement description more general than the projective measurement is often helpful. For simplicity – and in the spirit of information theory – we assume that the possible measurement outcomes are from a discrete set[3] $\mathcal{X}$.

A measurement with outcomes $\mathcal{X}$ on a quantum system with Hilbert space $\mathcal{H}$ can be described by a *positive operator valued measure* (POVM) on $\mathcal{X}$. We denote by $\mathrm{Pos}(\mathcal{H}) := \{A \in L(\mathcal{H}) \mid A \geq 0\}$ the set of Hermitian positive semi-definite operators on $\mathcal{H}$. A POVM on a discrete space $\mathcal{X}$ is a map $\mu : \mathcal{X} \to \mathrm{Pos}(\mathcal{H})$ such that $\sum_{x\in\mathcal{X}} \mu(x) = \mathbb{I}$. If the system is in the quantum state $\rho \in \mathcal{D}(\mathcal{H})$, the probability of observing the outcome $x \in \mathcal{X}$ is given by $\mathrm{Tr}(\mu(x)\rho)$.

4 P. **Exercise 2.**

2 P. (a) Can every projective measurement (also called projector valued measurement, PVM) be phrased as a POVM? Either prove that this is always the case or show a counterexample.

2 P. (b) Can every POVM be phrased as a PVM on the same Hilbert space? Argue the answer, and give an illustrative example. (*Hint:* what is $\mathrm{Tr}[E_i E_j]$ for two elements E_i and E_j of a POVM?)

It is often stated that this is the most general form of a quantum measurement. We want to understand this statement in more detail. So what could be regarded as the most general quantum measurement? One can start as follows: A (general) quantum measurement M with outcomes in $\mathcal{X}$ is a map that associates to each quantum state $\rho \in \mathcal{D}(\mathcal{H})$ a probability measure p_ρ on $\mathcal{X}$, i.e. $M\colon \rho \mapsto p_\rho$ with $p_\rho\colon \mathcal{X} \to [0,1]$ such that $\sum_{x\in\mathcal{X}} p_\rho(x) = 1$.

2 P. **Exercise 3.** Show that any POVM on $\mathcal{X}$ defines a general quantum measurement as defined above.

Quantum information theory

Encoding classical bits. We know that describing quantum systems requires exponential amounts of classical bits. Then, *could we use a quantum state to store an exponential amount of bits?* Or *how many classical bits can be encoded and (perfectly) decoded in a d-dimensional quantum system in this way?* In this exercise, we see that the fact that we need to measure to access information stored in a quantum state limits the amount of classical information we can extract from the state of a quantum system.

Let $\mathcal{H}$ be a d-dimensional Hilbert space. Our aim is to encode n classical bits into the space of quantum states as density matrices $\mathcal{D}(\mathcal{H})$. There are 2^n possible different arrangements of n classical bits: $|\{0,1\}^n| = 2^n$. To this end, we choose a set of 2^n states $\{\rho_x\}_{x\in\{0,1\}^n} \subset \mathcal{D}(\mathcal{H})$, each state corresponding to a bit string. Now we would like to come up with a measurement protocol such that, when measuring each ρ_x, we observe the corresponding bit string $x \in \{0,1\}^n$ as the outcome of the measurement.

7 P. **Exercise 4.** Consider an ensemble $\{p(x), \rho_x\}$ of density operators and a POVM with elements $\{\Lambda_x\}$ that should identify the states ρ_x with high probability. That is, we would like $\mathrm{Tr}[\Lambda_x \rho_x]$ to be as large as possible. Consider a source that outputs the bit string $x \in \{0,1\}^n$ with probability $p(x)$.

1 P. (a) We say that the POVM is successful if outcome x is returned upon measuring on ρ_x. Define the expected success probability of the POVM with respect to the distribution p.

1 P. (b) There exists an (incomplete) order relation $\leq$ for PSD matrices. For A, B Hermitian PSD matrices, we say $A \leq B$ if $B - A$ is PSD, $B - A \geq 0$. Show that $\rho \leq \mathbb{I}$ for any density matrix ρ.

[3] More generally, one can replace $\mathcal{X}$ by the σ-algebra of a measurable Borel space. This is the natural structure from probability theory to describe a set of all possible events in an experiment. If you are curious and have some time left, it is an instructive and not so hard exercise to look up the definitions of a Borel space and a probability space and translate this exercise and its solution into this language.

2 P. (c) Show that for two positive semi-definite matrices $A \geq 0$ and $B \geq 0$ we have that

$$\mathrm{Tr}[AB] \geq 0. \tag{4}$$

Do *not* use the property that for any $A \geq 0$ there exists a unique $\sqrt{A} \geq 0$ such that $A = \sqrt{A}\sqrt{A}$. Argue why under the same assumptions, AB is only positive semidefinite when A and B commute.

2 P. (d) Use the results of the two preceding exercises to show that for $p(x) = 2^{-n}$ (the uniform distribution over bitstrings) the expected success probability is upper bounded by $2^{-n}d$.

1 P. (e) What is then the largest number of bits n such that, when selecting bitstrings uniformly at random, the POVM could still succeed with probability 1.

No-cloning theorem. We now want to revisit one of the most well-known results in quantum information theory.

3 P. Exercise 5.

2 P. (a) Show that there does not exist a unitary map U acting on two copies of a Hilbert space $\mathcal{H}$ which fulfills the following condition for any state in the Hilbert space $|\psi\rangle \in \mathcal{H}$:

$$U|\psi\rangle|0\rangle = e^{i\phi(|\psi\rangle)}|\psi\rangle|\psi\rangle. \tag{5}$$

Here ϕ is allowed to be any arbitrary phase function $\phi\colon \mathcal{H} \to \mathbb{R}$.

(*Style points*: this can be proved using only the fact that unitary operators are linear. Style points are not worth actual points.)

1 P. (b) Classical data can be freely copied. Why does that not contradict the no-cloning theorem even though we can identify strings of classical bits with the associated basis states of the quantum system?

Math

In this exercise we take a short break from following the main content covered in the lecture and return back to proving some simple but useful identities for operators on complex Hilbert spaces. In particular, we explore the two important facts that operators are completely specified by their diagonal elements in all bases as well as the power of the square root representation for positive (PSD) operators.

5 P. Bonus Exercise 1. Interestingly, in a complex inner product space an operator is fully specified when its diagonal elements in all bases are known.

1 P. (a) Start by verifying the identity

$$\langle\phi|A|\psi\rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \langle\psi + i^k\phi|A|\psi + i^k\phi\rangle, \tag{6}$$

where we define

$$|\psi + i^k\phi\rangle = |\psi\rangle + i^k|\phi\rangle. \tag{7}$$

(Careful, for the corresponding bra we need to flip the sign of the imaginary root.) This is known as the *polarization identity* in a complex inner product space.

1 P. (b) Use the previous identity to show that if $\langle\psi|A|\psi\rangle = \langle\psi|B|\psi\rangle$ holds for all $|\psi\rangle$, then $A = B$.

1 P. (c) Use this to show that the class of operators $A \in L(\mathcal{H})$ which preserve the inner product is exactly the set of unitaries. I.e. if $\forall \psi, \phi : \langle A\psi | A\phi \rangle = \langle \psi | \phi \rangle$ then A is unitary and vice versa.

1 P. (d) A useful property of positive operators is the following: If A is a positive operator then there exists a unique positive operator $A^{1/2}$ which satisfies $A^{1/2}A^{1/2} = A$. Moreover, this operator satisfies $[A, H] = 0 \implies [A^{1/2}, H] = 0$. Use this to show that the product of two positive operators is positive if and only if they commute. (hint: Also show that $A \geq B \wedge B \geq A \implies A = B$).

1 P. (e) Show that for two positive semi-definite matrices $A \geq 0$ and $B \geq 0$ we have that

$$\mathrm{Tr}[AB] \geq 0. \tag{8}$$

Use the property that for any $A \geq 0$ there exists a unique $\sqrt{A} \geq 0$ such that $A = \sqrt{A}\sqrt{A}$. *(Hint: You can start proving $ABA \geq 0$ for any two $A \geq 0, B \geq 0$.)*

Total Points: 27 (+5)