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 $|\psi_j^k\rangle$.

Solution

In bra-ket notation, the probability of getting result λ_k can be written in these two ways:

$$p(k) = \langle\phi|P_k|\phi\rangle$$
$$p(k) = \sum_{j:\mathrm{EV}\lambda_k} |\langle\phi|\psi_j^k\rangle|^2$$

The same formula in density matrix notation can be found in the lecture notes.

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

Solution

In bra-ket notation, the state immediately after measuring if we observed outcome λ_k is:

$$|\phi_k^{\text{post}}\rangle = \frac{P_k|\phi\rangle}{\|P_k|\phi\rangle\|_2} = \frac{P_k|\phi\rangle}{\sqrt{\langle\phi|P_kP_k|\phi\rangle}} = \frac{P_k|\phi\rangle}{\sqrt{\langle\phi|P_k|\phi\rangle}} = \frac{P_k|\phi\rangle}{\sqrt{p(k)}}.$$

The same formula in density matrix notation can be found in the lecture notes.

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] $(P_k)_k$.

[1] Sanity check, you should have $\sum_k P_k = \mathbb{I}$ the identity matrix.

Solution

One could do the calculation explicitly for the diagonalization of the matrix, but here we show a different approach. We use knowledge from the regular *single qubit* Pauli matrices, and also intuitive properties of the tensor product.

We know that all three Pauli operators have two eigenvalues $\{-1, 1\}$. We also know what the corresponding eigenvectors are: $|\pm\rangle$ for X, $|\pm i\rangle$ for Y, and $|0/1\rangle$ for Z. For $B \in \{X, Y, Z\}$, with eigenvectors $|\pm B\rangle$, we know the spectral decomposition of B is:

$$B = |{+B}\rangle\langle{+B}| - |{-B}\rangle\langle{-B}|.$$

Next, let's say matrix A has eigenvalues $(\lambda_i)_i$ (allowing for duplicates if an eigenvalue is degenerate) and eigenvectors $(|a_i\rangle)_i$, and matrix B has eigenvalues $(\sigma_j)_j$ (allowing for duplicates if an eigenvalue is degenerate) and eigenvectors $(|b_j\rangle)_j$. Then it follows that matrix $A \otimes B$ has eigenvalues $(\lambda_i \sigma_j)_{i,j}$ and eigenvectors $(|a_i b_j\rangle)_{i,j}$.

For this particular exercise, we combine the spectral decomposition of $X = |+\rangle\langle+| - |-\rangle\langle-|$ with this property of the tensor product to reach the spectral decomposition of A:

$$\begin{aligned} A = X^{\otimes 2} &= (|+\rangle\langle+| - |-\rangle\langle-|)^{\otimes 2} \\ &= |{++}\rangle\langle{++}| + |{--}\rangle\langle{--}| - |{+-}\rangle\langle{+-}| - |{-+}\rangle\langle{-+}|. \end{aligned}$$

The unique eigenvalues are $\lambda_{\pm 1} = \pm 1$, and the corresponding projectors are:

$$\begin{aligned} P_1 &= |{++}\rangle\langle{++}| + |{--}\rangle\langle{--}|, \\ P_{-1} &= |{+-}\rangle\langle{+-}| + |{-+}\rangle\langle{-+}|. \end{aligned}$$

To see this fulfills the sanity check we observe that, if we replaced $+ \mapsto 0$ and $- \mapsto 1$, then $P_1 + P_{-1}$ would be the identity matrix "in ketbra notation". That means it is also the identity matrix without the replacement, since the replacement was only a change of basis.

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}?

Solution

We start with a small useful observation for the $P_{\pm 1}$ from the previous exercise:

$$P_{\pm 1} = \frac{\mathbb{I} \pm (X \otimes X)}{2}.$$

With this, we just plug in the variables into the formulas from exercises (a) and (b). Start with the outcome probabilities $p(k) = \langle\phi|P_k|\phi\rangle$.

$$\begin{aligned}
p(1) = \langle\phi|P_1|\phi\rangle &= \langle\phi|\frac{1}{2}(\mathbb{I} + X \otimes X)|\phi\rangle = \frac{1}{2}(1 + \langle\phi|(X \otimes X)|\phi\rangle) \\
&= \frac{1}{2}\left(1 + \frac{1}{\sqrt{30}}\begin{pmatrix}1 & -2i & 3i & -4\end{pmatrix}\begin{pmatrix}0 & 0 & 0 & 1\\0 & 0 & 1 & 0\\0 & 1 & 0 & 0\\1 & 0 & 0 & 0\end{pmatrix}\frac{1}{\sqrt{30}}\begin{pmatrix}1\\2i\\-3i\\-4\end{pmatrix}\right) \\
&= \frac{1}{2}\left(1 + \frac{1}{30}\begin{pmatrix}1 & -2i & 3i & -4\end{pmatrix}\begin{pmatrix}-4\\-3i\\2i\\1\end{pmatrix}\right) \\
&= \frac{1}{2}\left(1 + \frac{1}{30}(-4 - 6 - 6 - 4)\right) = \frac{1}{2}\left(1 - \frac{20}{30}\right) \\
&= \frac{1}{6}.
\end{aligned}$$

It follows that $p(-1) = 1 - p(1) = \frac{5}{6}$.
Now for the state after measurement outcome λ_k: $|\phi_k^{\text{post}}\rangle = \frac{P_k|\phi\rangle}{\sqrt{p(k)}}$.

$$\begin{aligned}
|\phi_1^{\text{post}}\rangle &= \frac{P_1|\phi\rangle}{\sqrt{p(1)}} = \frac{\frac{\mathbb{I}+X\otimes X}{2}|\phi\rangle}{\sqrt{\frac{1}{6}}} = \frac{\sqrt{6}}{2}\left(|\phi\rangle + (X \otimes X)|\phi\rangle\right) \\
&= \sqrt{\frac{3}{2}}\left(\frac{1}{\sqrt{30}}\begin{pmatrix}1\\2i\\-3i\\-4\end{pmatrix} + \frac{1}{\sqrt{30}}\begin{pmatrix}-4\\-3i\\2i\\1\end{pmatrix}\right) = \frac{1}{\sqrt{20}}\begin{pmatrix}-3\\-i\\-i\\-3\end{pmatrix}. \\
|\phi_{-1}^{\text{post}}\rangle &= \frac{P_{-1}|\phi\rangle}{\sqrt{p(-1)}} = \frac{\frac{\mathbb{I}-X\otimes X}{2}|\phi\rangle}{\sqrt{\frac{5}{6}}} = \frac{\sqrt{6}}{2\sqrt{5}}\left(|\phi\rangle - (X \otimes X)|\phi\rangle\right) \\
&= \sqrt{\frac{3}{10}}\left(\frac{1}{\sqrt{30}}\begin{pmatrix}1\\2i\\-3i\\-4\end{pmatrix} - \frac{1}{\sqrt{30}}\begin{pmatrix}-4\\-3i\\2i\\1\end{pmatrix}\right) = \frac{1}{10}\begin{pmatrix}5\\5i\\-5i\\-5\end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix}1\\i\\-i\\-1\end{pmatrix}.
\end{aligned}$$

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}?

[2] Recall that the purity of a state ρ is computed as $\text{Tr}[\rho^2]$

Solution

If we do not observe the measurement outcome, the measure prepares a classical mixture of both output states with their corresponding probabilities:

$$\rho^{\text{post}} = p(1)|\phi_1^{\text{post}}\rangle\langle\phi_1^{\text{post}}| + p(-1)|\phi_{-1}^{\text{post}}\rangle\langle\phi_{-1}^{\text{post}}|.$$

We could just plug in the results from the last exercise. Or we could use the formulas so that the solution of this exercise does not depend on the correctness of the other ones:

$$\begin{aligned}
\rho^{\text{post}} &= p(1)\frac{P_1|\phi\rangle}{\sqrt{p(1)}}\frac{\langle\phi|P_1}{\sqrt{p(1)}} + p(-1)\frac{P_{-1}|\phi\rangle}{\sqrt{p(-1)}}\frac{\langle\phi|P_{-1}}{\sqrt{p(-1)}} \\
&= P_1|\phi\rangle\langle\phi|P_1 + P_{-1}|\phi\rangle\langle\phi|P_{-1} \\
&= \frac{1}{2}(\mathbb{I} + (X\otimes X))|\phi\rangle\langle\phi|\frac{1}{2}(\mathbb{I} + (X\otimes X)) \\
&\quad + \frac{1}{2}(\mathbb{I} - (X\otimes X))|\phi\rangle\langle\phi|\frac{1}{2}(\mathbb{I} - (X\otimes X)) \\
&= \frac{1}{4}(|\phi\rangle + (X\otimes X)|\phi\rangle)(\langle\phi| + \langle\phi|(X\otimes X)) \\
&\quad + \frac{1}{4}(|\phi\rangle - (X\otimes X)|\phi\rangle)(\langle\phi| - \langle\phi|(X\otimes X)) \\
&= \frac{1}{2}\left(|\phi\rangle\langle\phi| + (X\otimes X)|\phi\rangle\langle\phi|(X\otimes X)\right) \\
&= \frac{1}{2}\left(\frac{1}{30}\begin{pmatrix}1\\2i\\-3i\\-4\end{pmatrix}\begin{pmatrix}1 & -2i & 3i & -4\end{pmatrix} + \frac{1}{30}\begin{pmatrix}-4\\-3i\\2i\\1\end{pmatrix}\begin{pmatrix}-4 & 3i & -2i & 1\end{pmatrix}\right) \\
&= \frac{1}{60}\left(\begin{pmatrix}1 & -2i & 3i & -4\\ 2i & 4 & -6 & -8i\\ -3i & -6 & 9 & 12i\\ -4 & 8i & -12i & 16\end{pmatrix} + \begin{pmatrix}16 & -12i & 8i & -4\\ 12i & 9 & -6 & -3i\\ -8i & -6 & 4 & 2i\\ -4 & 3i & -2i & 1\end{pmatrix}\right) \\
&= \frac{1}{60}\begin{pmatrix}17 & -14i & 11i & -8\\ 14i & 13 & -12 & -11i\\ -11i & -12 & 13 & 14i\\ -8 & 11i & -14i & 17\end{pmatrix}.
\end{aligned}$$

Good sanity check: ρ^{post} is Hermitian (real diagonal, symmetric for the real part, antisymmetric for the imaginary part), and $\text{Tr}[\rho^{\text{post}}] = 1$.
In order to compute the purity, we could either compute $(\rho^{\text{out}})^2$ or we could notice that $|\phi_1^{\text{post}}\rangle$ and $|\phi_{-1}^{\text{post}}\rangle$ are orthogonal and normalized. With this knowledge, we can say there exists an orthonormal basis with these two states as the first two elements. In this basis, we know ρ^{post} takes a diagonal form $\rho^{\text{post}} = \text{diag}(p(1), p(-1), 0, 0)$. We know the purity is basis-independent, so with this we can quickly reach the conclusion that

$$\text{Tr}[(\rho^{\text{post}})^2] = p(1)^2 + p(-1)^2 = \frac{1}{36} + \frac{25}{36} = \frac{13}{18}.$$

We see the purity is closer to 1 (maximum) than to 1/4 (minimum), so while ρ^{post} is not pure, it is still very far from the maximally mixed state.

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.

Solution

Yes, this is always possible. This can be seen as follows: Let $A = \sum_i \lambda_i \Pi_i$ be an observable with $\mathrm{spec}(A) = \{\lambda_i\}$ and Π_i the orthogonal projector to the i-th eigenspace. Then, the map $\mathrm{spec}(A) \to \mathrm{Pos}(\mathcal{H})$, $\lambda_i \mapsto \Pi_i$ defines a POVM, because $\sum_i \Pi = \mathbb{I}$.

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?)

Solution

Not every POVM can be phrased as a PVM. In particular, the projectors of a PVM fulfill pairwise orthonormality $\mathrm{Tr}[P_i P_j] = \delta_{ij}$ whereas the elements of a POVM do not, in general, $\mathrm{Tr}[E_i E_j] \neq \delta_{ij}$.
Counterexample: we only need to give a set of PSD matrices that add up to the identity but are not pairwise orthonormal.
Define E_1, E_2 as follows:

$$\begin{aligned} E_1 &= \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|, \\ E_2 &= \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|. \end{aligned}$$

The condition $E_1 + E_2 = \mathbb{I}$ is fulfilled. Then $\{E_1, E_2\}$ describes a POVM which cannot be rephrased as a PVM, because, on the one hand $\mathrm{Tr}[E_1 E_2] = 4/9 \neq 0$, and on the other hand $\mathrm{Tr}[E_1^2] = 5/9 \neq 1$.
Notice each of those conditions is sufficient individually.

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.

[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.

Solution

For a POVM $\mu : \mathcal{X} \to \mathrm{Pos}(\mathcal{H})$ we can define the general measurement M which maps $\rho \mapsto \mathrm{Tr}(\rho\mu(\cdot)) : \mathcal{X} \to [0,1]$. Here, $\mathrm{Tr}[\rho\mu(x)] \geq 0$ holds for all $x \in \mathcal{X}$ because both ρ and $\mu(x)$ are PSD. Next, observe that $\sum_{x\in\mathcal{X}} \mathrm{Tr}[\rho\mu(x)] = \mathrm{Tr}[\rho \sum_{x\in\mathcal{X}} \mu(x)] = \mathrm{Tr}[\rho\mathbb{1}] = \mathrm{Tr}[\rho] = 1$. So, $\{\mathrm{Tr}[\rho\mu(x)]\}_{x\in\mathcal{X}}$ indeed forms a probability measure on $\mathcal{X}$ as desired.

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.

Solution

The expected success probability of the POVM is

$$\sum_x p(x)\,\mathrm{Tr}[\Lambda_x\rho_x]. \tag{4}$$

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.

Solution

$\mathbb{I} - \rho = U(\mathbb{I} - \Lambda)U^\dagger$, where U diagonalises ρ. But since ρ is a quantum state with eigenvalues smaller than one, $\mathbb{I} - \Lambda$ has only nonnegative entries, hence the claim $\mathbb{I} \geq \rho$.

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

$$\mathrm{Tr}[AB] \geq 0. \tag{5}$$

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.

Solution

We establish the claim by expanding A and B into their respective eigenbases:

$$\begin{aligned}\mathrm{Tr}[AB] &= \mathrm{Tr}\left[\sum_{i=1}^{d} a_i |a_i\rangle\langle a_i| \sum_{j=1}^{d} b_j |b_j\rangle\langle b_j|\right] \\ &= \sum_{i=1}^{d}\sum_{j=1}^{d} a_i b_j |\langle a_i|b_j\rangle|^2.\end{aligned}$$

As A and B are positive semi-definite, all a_i and b_j are non-negative and the above is a sum that only involves non-negative terms which establishes the claim.
The product AB is easily seen to be positive semi-definite when A and B commute, because then they share a common eigenbasis in which the (non-negative) eigenvalues are just multiplied and stay non-negative. If A and B fail to commute, we have that $AB \neq BA$, and the operator AB is hence not Hermitian. It can thus have eigenvalues with an imaginary part for which the definition non-negative makes no sense in the first place, which means that positive semidefiniteness is not well-defined in the first place. This is ultimately a consequence of the fact that the complex numbers admit no total order.

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 $2^{-n}d$.

Solution

The fact that $\rho_x \leq \mathbb{I}$ for all x is equivalent to $\mathbb{I} - \rho_x \geq 0$. Using the result of the previous exercise then establishes that for all POVM effects Λ_x, which are also positive semi-definite, we have that

$$\mathrm{Tr}[\Lambda_x(\mathbb{I} - \rho)] \geq 0 \;\Leftrightarrow\; \mathrm{Tr}[\Lambda_x] \geq \mathrm{Tr}[\Lambda_x \rho].$$

Applying this to the expected success probability for the uniform distribution yields

$$\sum_x p(x)\,\mathrm{Tr}[\rho_x\Lambda_x] = 2^{-n}\sum_x \mathrm{Tr}[\rho_x\Lambda_x] \leq 2^{-n}\sum_x \mathrm{Tr}[\Lambda_x] = 2^{-n}\,\mathrm{Tr}[\mathbb{I}] = 2^{-n}d$$

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.

Solution

From the previous exercise we know the success probability is upper bounded by $2^{-n}d$. We write $1 \leq 2^{-n}d$ and solve for n: $n \leq \log_2 d$. So the number of classical bits that can be encoded and decoded perfectly is the same as the number of qubits in the system, which is precisely $\log_2 d$.

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 $|\psi\rangle \in \mathcal{H}$:

$$U|\psi\rangle|0\rangle = e^{i\phi(|\psi\rangle)}|\psi\rangle|\psi\rangle. \tag{6}$$

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.)

Solution

We offer two solutions:

(a) *Solution without using linearity:* Assume this was the case for $|\psi\rangle$ and $|\phi\rangle$ with $|\psi\rangle \neq e^{i\alpha}|\phi\rangle$ for any α. Let us consider the scalar product between two such vectors

$$\begin{aligned}\langle\varphi|\psi\rangle &= \langle 0|\langle\varphi|U^\dagger U|\psi\rangle|0\rangle && (7)\\ &= e^{i(\phi(\psi)-\phi(\varphi))}\langle\varphi|\langle\varphi||\psi\rangle|\psi\rangle && (8)\\ &= \langle\varphi|\psi\rangle^2 e^{i(\phi(\psi)-\phi(\varphi))}. && (9)\end{aligned}$$

Taking absolute values on both sides shows that $\langle\varphi|\psi\rangle$ can only be 0 or 1, so it cannot be the case that U clones arbitrary states.

(b) *Solution using only linearity:* We prove this by reductio ad absurdum: we assume the thesis holds and then reach a contradiction. Take any state orthogonal to the $|0\rangle$ state $|\psi\rangle \in \mathcal{H} : \langle\psi|0\rangle = 0$. Consider the superposition $|\psi'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |\psi\rangle)$. Then, on the one hand, we have:

$$U|\psi'\rangle|0\rangle = e^{i\phi(|\psi'\rangle)}|\psi'\rangle|\psi'\rangle = \frac{e^{i\phi(|\psi'\rangle)}}{2}(|00\rangle + |0\psi\rangle + |\psi 0\rangle + |\psi\psi\rangle,$$

which we notice is a product state. On the other hand, we have:

$$\begin{aligned}U|\psi'\rangle|0\rangle &= U\left(\frac{1}{\sqrt{2}}(|0\rangle + |\psi\rangle)\right)|0\rangle\\ &= \frac{1}{\sqrt{2}}(U|0\rangle|0\rangle + U|\psi\rangle|0\rangle)\\ &= \frac{1}{\sqrt{2}}(e^{i\phi(|0\rangle)}|00\rangle + e^{i\phi(|\psi\rangle)}|\psi\psi\rangle),\end{aligned}$$

which we notice is an entangled state. But we do actually not need to talk about entanglement. Since we took $|\psi\rangle$ to be orthogonal to $|0\rangle$, it follows that the elements of the set $\{|00\rangle, |0\psi\rangle, |\psi 0\rangle, |\psi\psi\rangle\}$ are pairwise orthonormal. With this, it follows that

$$\frac{e^{i\phi(|\psi'\rangle)}}{2}(|00\rangle + |0\psi\rangle + |\psi 0\rangle + |\psi\psi\rangle) = \frac{1}{\sqrt{2}}(e^{i\phi(|0\rangle)}|00\rangle + e^{i\phi(|\psi\rangle)}|\psi\psi\rangle)$$

is a contradiction irrespective of the particular form of ϕ (LIGHTNING BOLT).

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?

Solution

Simply put, because we can easily find the unitary U that produces the copies! Given bitstrings $x \in \{0,1\}^n$ of length n, we can identify each bitstring with a computational basis state $x \leftrightarrow |x\rangle$. W.l.o.g. we consider $n = 1$. We see that the CNOT gate produces the desired effect:

$$\text{CNOT}|00\rangle = |00\rangle \tag{10}$$

$$\text{CNOT}|10\rangle = |11\rangle. \tag{11}$$

If we still don't know what the CNOT gate is, then there's a more winding answer. In order to show that the quantum copier cannot exist, we needed to consider a superposition of different states. If we map classical bits to a set of pairwise orthogonal states, then the set of states on which we want the quantum copier to work (this discrete set of pairwise orthogonal states) is much smaller (than the set of all possible states, including superposition states, which are not orthogonal with the computational basis states). In particular, linearity does not impose any limitations if we only need to copier to work on the set of pairwise orthogonal states. Said otherwise, given $x \neq x'$ we have $\langle x|x'\rangle = 0$, which means that the action of the hypothetical U on $|x\rangle$ is completely independent of the action on $|x'\rangle$. This means that, for any set of pairwise orthogonal states $\{|\psi_x\rangle\}_{x\in\{0,1\}^n}$, there will always exist at least one unitary U which maps the set $\{|x0\rangle\}_x$ to the set $\{|xx\rangle\}_x$, which can be seen as a simple change of basis.

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

$$\langle\phi|A|\psi\rangle = \frac{1}{4}\sum_{k=0}^{3} i^k \langle\psi + i^k\phi|A|\psi + i^k\phi\rangle, \tag{12}$$

where we define

$$|\psi + i^k\phi\rangle = |\psi\rangle + i^k|\phi\rangle. \tag{13}$$

(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.

Solution

$$\begin{aligned}\frac{1}{4}\sum_{k=0}^{3} i^k\langle\psi+i^k\phi|A|\psi+i^k\phi\rangle &= \frac{1}{4}[\langle\psi|A|\psi\rangle(1+i-1-i)\\ &\quad+\langle\psi|A|\phi\rangle(1-1+1-1)\\ &\quad+\langle\phi|A|\psi\rangle(1+1+1+1)\\ &\quad+\langle\phi|A|\phi\rangle(1+i-1-i)]\\ &=\langle\phi|A|\psi\rangle.\end{aligned}$$

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 $A = B$.

Solution

We use the above identity on $\langle j|A|l\rangle$, for $|j\rangle$ and $|l\rangle$ computational basis vectors.

$$\langle\psi|A|\psi\rangle = \langle\psi|B|\psi\rangle \quad \forall\psi \tag{14}$$

$$\Downarrow \tag{15}$$

$$\langle l+i^kj|A|l+i^kj\rangle = \langle l+i^kj|B|l+i^kj\rangle \quad \forall k,j,l \tag{16}$$

$$\Downarrow \tag{17}$$

$$\frac{1}{4}\sum_{k=0}^{3}\langle l+i^kj|A|l+i^kj\rangle = \frac{1}{4}\sum_{k=0}^{3}\langle l+i^kj|B|l+i^kj\rangle \quad \forall j,l \tag{18}$$

$$\Downarrow \tag{19}$$

$$\langle j|A|l\rangle = \langle j|B|l\rangle \quad \forall j,l \tag{20}$$

$$\Downarrow \tag{21}$$

$$A = B. \tag{22}$$

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.

Solution

$\forall\psi,\phi : \langle A\psi|A\phi\rangle = \langle\psi|A^\dagger A|\phi\rangle = \langle\psi|\phi\rangle \implies A^\dagger A = \mathbb{I}$. Since left-inverses of operators are right-inverses as well we also have $AA^\dagger = \mathbb{I}$ making A unitary. Let now A be unitary. Then $\forall\psi,\phi : \langle A\psi|A\phi\rangle = \langle\psi|A^\dagger A|\phi\rangle = \langle\psi|\mathbb{I}|\phi\rangle = \langle\psi|\phi\rangle$

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 $A \geq B \wedge B \geq A \implies A = B$).

Solution

Let $AB = BA$ then $\langle\psi|AB|\psi\rangle = \langle\psi|A^{1/2}A^{1/2}B|\psi\rangle = \langle\psi|A^{1/2}BA^{1/2}|\psi\rangle \geq 0$.
Now Suppose $AB \geq 0$ then $\forall\psi : \langle\psi|AB|\psi\rangle \in \mathbb{R}$. Thus $\langle\psi|BA|\psi\rangle = \langle\psi|A^\dagger B^\dagger|\psi\rangle^* = \langle\psi|AB|\psi\rangle$. This implies by the previous exercise $\langle\psi|AB - BA|\psi\rangle = 0\forall\psi$ and thus $AB - BA = 0$.

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

$$\mathrm{Tr}[AB] \geq 0. \tag{23}$$

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 $A \geq 0, B \geq 0$.)*

Solution

Start proving the hint. We use that, for any Hermitian matrix C, $C^\dagger C \geq 0$. Then, using $B = \sqrt{B}\sqrt{B}$, it follows

$$ABA = A\sqrt{B}\sqrt{B}A \tag{24}$$

$$= \left(\sqrt{B}A\right)^\dagger \sqrt{B}A \geq 0. \tag{25}$$

It follows $\mathrm{Tr}[ABA] \geq 0$ for any $A \geq 0, B \geq 0$.
Finally:

$$\mathrm{Tr}\, AB = \mathrm{Tr}\, \sqrt{A}\sqrt{A}B = \mathrm{Tr}\, \sqrt{A}B\sqrt{A} \geq 0. \tag{26}$$

Total Points: 27 (+5)