Freie Universität Berlin
Tutorials on Quantum Information Theory
Winter term 2020/21

Problem Sheet 2
POVMs and encoding classical information

J. Eisert, J. Haferkamp, J. C. Magdalena De La Fuente

1. **Non-uniqueness of the decomposition of mixed states.**

   Consider two macroscopically different preparation schemes of a large number of polarised photons:

   Preparation A. For each photon we toss a fair coin. Depending on whether we get head or tail, we prepare the photon to have either vertical or horizontal *linear* polarisation.

   Preparation B. For each photon we toss a fair coin. Depending on whether we get head or tail, we prepare the photon to have either left-handed or right-handed *circular* polarisation.

   We are given a large number of photons which all were prepared by the same scheme.

   a) Argue that having only access to the photons we can not distinguish which of the preparation schemes was used.

   Solution: Both preparations give rise to the same quantum state, namely, the maximally mixed state. Hence, there is no measurement that distinguishes the two preparations.

   b) Argue that if it were possible to distinguish such types of preparations by measuring the photon, locality would be violated.

   Solution: Protocol: EPR setting with Bell state

   Bob chooses a measurement setting, X or Z and measures his half of the state.

   Then, the state reads

   $$\rho_A = \mathrm{Tr}[|\psi\rangle\langle\psi| P_1] + \mathrm{Tr}[|\psi\rangle\langle\psi| P_2], \tag{1}$$

   where $P_{1,2}$ are either $|+\rangle\langle+|, |-\rangle\langle-|$ or $|0\rangle\langle 0|, |1\rangle\langle 1|$.

   Depending on which measurement setting Bob chooses, the state on Alice's side reads $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ or $\frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$.

   If Alice had a way of distinguishing the two mixtures, they could have communicated a bit encoded as $\{X, Z\}$.

2. **Impossible machines – no cloning.**

   In this problem we will re-derive the impossibility results that you have seen in the lecture but now directly using the structure of quantum theory.

   Show that there does not exist a unitary map on two copies of a Hilbert space $\mathcal{H}$ which acts in the following way:

   $$\forall |\psi\rangle \in \mathcal{H} : U|\psi\rangle|0\rangle = \mathrm{e}^{\mathrm{i}\phi(\psi)}|\psi\rangle|\psi\rangle\ .$$

Solution: Assume this was the case for $|\psi\rangle$ and $|\phi\rangle$ with $|\psi\rangle \neq \mathrm{e}^{\mathrm{i}\alpha}|\phi\rangle$ for any α. Let us consider the scalar product between two such vectors

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

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.

3. **The most general quantum measurements.**

In a quantum mechanics course, measurements are typically introduced as projective measurements of the eigenvalues of observables. But from a theoretical perspective another measurement description is often helpful. For simplicity—and in the spirit of information theory—we assume that the possible measurement outcomes are from a discrete set $\mathcal{X}$. [1]

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 $\sum_{x\in\mathcal{X}} \mu(x) = \mathrm{Id}$. 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 $\mathrm{Tr}(\mu(x)\rho)$.

a) What is the difference between POVM measurements and the measurement description using observables?

Solution: 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 $\sum_i \Pi = \mathrm{Id}$. The converse however the constituent operators $\mathrm{range}(\mu) = \{E_i\}$ of a POVM μ are not required to be orthogonal projectors, i.e. in general we do not have $E_i E_j = \delta_{ij} E_j$ as for the so-called projector valued measurements (PVM) that can be directly expressed as observables. Nevertheless every POVM can be implemented with PVMs using an ancillar system. More on this, probably on a up-coming sheet.

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. $M : \rho \mapsto p_\rho$ with $p_\rho : \mathcal{X} \to [0, 1]$ such that $\sum_{x\in X} p_\rho(x) = 1$.

b) Show that there is a one-to-one mapping between general quantum measurements as defined above and POVMs on $\mathcal{X}$.

Solution: Let M be a general measurement. To make sense of the other principles of quantum mechanics, in particular the statistical interpration mixtures of quantum states, we require that M is a linear map.

Then, for fixed $x \in \mathcal{X}$ the map $\rho \mapsto p_\rho(x)$ is by definition an arbitrary element of the dual space of $\mathcal{D}(\mathcal{H})$. Being equipped with an inner product $(\cdot, \cdot)$, we can use the

[1] 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.

the canonical isomorphism $L(\mathcal{D}(\mathcal{H})) \simeq L^*(\mathcal{D}(\mathcal{H}))$ to express every element in the dual space as an element in $L(\mathcal{D}(\mathcal{H}))$. Explicitly, we can define $\mu(x) \in L(\mathcal{D}(\mathcal{H}))$ such that $\rho \mapsto p_\rho(x) = (\mu(x), \rho)$. The restriction to $p_\rho(x) \geq 0$ for all ρ and x amounts to restricting $\mu(x)$ to an positive semi-definite operator. (Recall that $\mathrm{Tr}(A\rho) \geq 0$ for all $\rho \in \mathcal{D}(\mathcal{H})$ if and only if $A \succcurlyeq 0$. To see this express the trace in the eigenbasis of ρ or A.)

Now, for fixed ρ if $x \mapsto p_\rho(x)$ should define a probability measure, we have the restriction that $\sum_{x\in X} p_\rho(x) = \sum_{x\in X}(\mu(x), \rho) = 1$ for all ρ. This is the case if and only if $\sum_{x\in X} \mu(x) = \mathrm{Id}$ (Uniqueness can be seen e.g. by parameter counting).

Can you come up with a more general notion of quantum measurements?

Solution: I can not.

4. **Encoding classical bits.** In the last exercise we introduced the description of quantum measurements with the help of POVMs. We want to use this formulation to study the following question:

Let $\mathcal{H}$ be a d-dimensional Hilbert space. Our aim is to encode n classical bits into the space of quantum states $\mathcal{D}(\mathcal{H})$. To this end, we choose a set of 2^n states $\{\rho_i\}_{i\in\{0,1\}^n} \subset \mathcal{D}(\mathcal{H})$, each state corresponding to a bit string. To decode the bit string we have to make a measurement described by a POVM $\{F_i\}_{i\in\{0,1\}^n}$, where the bit string is the outcome.

How many classical bits can be encoded and decoded in a d-dimensional quantum system in this way?

Consider a source that outputs the bit string $x \in \{0,1\}^n$ with probability $p(x)$.

a) Define the success probability of the decoding procedure.

Solution: $\mathrm{Tr}[\rho_i F_i]$ should be maximal (1) for each i. The total success probability is then the expectation of that with respect to p, i.e., $\sum_x p(x)\,\mathrm{Tr}[\rho_x F_x]$

b) Show that for $p(x) = 2^{-n}$ the success probability is bounded by $2^{-n}d$.
(*Hint:* Argue that $\mathbb{1} \geq \rho_i$ for all i and show that for $A \geq 0$ and $B \geq C$ it holds that $\mathrm{Tr}(AB) \geq \mathrm{Tr}(AC)$ as a starting point.)

Solution: Clearly $\mathbb{1} - \rho = U(\mathbb{1} - \Lambda)U^\dagger$, where U diagonalises ρ. But since ρ is a quantum state with eigenvalues smaller than one, $\mathbb{1} - \Lambda$ has only nonnegative entries, hence the claim $\mathbb{1} \geq \rho_i$ for all i. If $A \geq 0$ and $B - C \geq 0$, then $\mathrm{Tr}\,AB - \mathrm{Tr}\,AC = \mathrm{Tr}(A(B-C)) \geq 0$. Thus, $\mathrm{Tr}(AB) \geq \mathrm{Tr}(AC)$.

Hence, we have

$$\sum_x p(x)\,\mathrm{Tr}[\rho_x F_x] = 2^{-n}\sum_i \mathrm{Tr}[\rho_i F_i] \leq 2^{-n}\sum_i \mathrm{Tr}[F_i] = 2^{-n}\,\mathrm{Tr}\,\mathbb{1} = 2^{-n}d \quad (2)$$

and the claim follows.

c) What does this imply?

Solution: One cannot encode more than $\log_2 d$ bits in a d-dimensional quantum system.