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.

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

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:

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

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 $\mathrm{Pos}(\mathcal{H}) \coloneqq \{A \in L(\mathcal{H}) \mid A \geq 0\}$ 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?

[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.

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 $\mathcal{X}$.

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

4. **Encoding classical bits.** On the last excercise sheet 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.

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.)

c) What does this imply?