Quantum Cryptography (spring 2020)	Dominique Unruh
Exercise Sheet 3	
Out: 2020-03-15	Due: 2020-03-23

Problem 1: Simple quantum systems

(a) Consider the following state on n qubits: $\frac{1}{\sqrt{2}}|0\dots0\rangle + \frac{1}{\sqrt{2}}|1\dots1\rangle \in \mathbb{C}^{2^n}$.[1] Someone measures the last qubit (i.e., whether it is 0 or 1). What happens to the state?[2]

(b) Show that $(U \otimes V) \cdot (U' \otimes V') = (UU') \otimes (VV')$. Here U, U', V, V' are $n \times n$ matrices.

Hint: To show that two matrices A, B are equal, it is sufficient to show that $A|ij\rangle = B|ij\rangle$ for all basis vectors $|ij\rangle$.

(c) Show that $\otimes$ is bilinear, i.e., $(a+b)\otimes c = (a\otimes c)+(b\otimes c)$ and $c\otimes(a+b) = (c\otimes a)+(c\otimes b)$. This holds both if a, b, c are matrices and if they are vectors.

(d) Show that in a projective measurement with outcomes $i \in I$, it holds that $\sum_{i\in I} \Pr[\text{outcome } i \text{ occurs}] = 1$. (I.e., some outcome will always occur.)

Note: Recall that $\|x\|^2$ for any vector x is $x^\dagger x$. And that $P^\dagger P = P$ for orthogonal projectors P. And that $(xy)^\dagger = y^\dagger x^\dagger$. Then take the formula for the measurement probability and just simplify.

(e) In the situation of Homework 2, Problem 1 (a),[3] we measure whether there is a photon on path 3. Formulate this mathematically (i.e., as a projective measurement).

Note: You only need to formulate the measurement. You are not required to apply it (i.e., to compute probabilities and post-measurement states).

---

[1] We call this a *cat state* because of its similarity to Schrödinger's cat: A cat which is dead can be seen as consisting of n dead particles ($|\text{dead}, \dots, \text{dead}\rangle$), and a living cat can be seen as consisting of n living particles ($|\text{alive}, \dots, \text{alive}\rangle$). (This is of course a simplification!).

[2] This can be seen as an explanation what happens if we try to implement Schrödinger's cat: Even with a very high quality box, information about at least one atom of the cat will leak to the outside (i.e., it is measured whether the atom is "alive"). This has then an effect on the state of the whole cat.

[3] Reminder: "Consider a system in which a single photon may be sent through 5 different paths. The photon may be polarised in any direction. Give a Hilbert space for describing the state of this photon and give a natural basis for expressing this state. How do you write that the photon is 45°-polarised and on path 3?"

(f) In the situation of Homework 2, Problem 1 (b),[4] we measure whether there is a photon on path 3. Formulate this mathematically (i.e., as a projective measurement).

Note: You only need to formulate the measurement. You are not required to apply it (i.e., to compute probabilities and post-measurement states).

Problem 2: Quantum State Probability Distributions and Density Operators

(a) Consider the following quantum state probability distributions:

$$\begin{aligned}
E_1 &= \{|0\rangle @ \tfrac{1}{2},\ |+\rangle @ \tfrac{1}{2}\}, \\
E_2 &= \{|0\rangle @ \tfrac{1}{4},\ |1\rangle @ \tfrac{3}{4}\}, \\
E_3 &= \{|0\rangle @ \tfrac{1}{4},\ |1\rangle @ \tfrac{1}{4},\ |+\rangle @ \tfrac{1}{4}, |-\rangle @ \tfrac{1}{4}\}.
\end{aligned}$$

Compute the corresponding density operators ρ_1, ρ_2, ρ_3 as explicitly given matrices. (Note: $|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and $|-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.)

(b) Consider the following process: First, a random value $x \in \{0,1\}^n$ is chosen. Then an n-bit quantum register is prepared to have the value $|\Psi\rangle := |x\rangle$. Then a unitary transformation U is applied to Ψ. What is the density operator corresponding to the resulting quantum state probability distribution?

Hint: As the first step, consider the case that U is the identity.

(c) Let a measurement M consisting of projectors $P_1, \dots, P_n$ be given. Let a quantum state $|\Psi\rangle$ be given. Assume that $|\Psi\rangle$ is measured using M but the measurement outcome **is not recorded** (i.e., it is forgotten, erased). What is the quantum state probability distribution describing the state of the system after this experiment? What is the corresponding density operator?

Note: The formula in the lecture was for the case where the measurement outcome is **not** forgotten.

(d) **(Bonus problem)** Assume a quantum system is in the state described by a density operator ρ. We apply a measurement M consisting of projectors $P_1, \dots, P_n$ to the system and forget the outcome. What is the density operator describing the resulting state of the system?

[4] Reminder: "Consider a system in which each of 5 paths may contain a photon (or not), and each of these photons may be polarised in any direction. Give a Hilbert space for describing the state of these photons and give a natural basis for expressing this state. How do you write that there is a photon on path 3 that is 45°-polarised and no photons on the other paths?"

Problem 3: Physical indistinguishability – the opposite direction (bonus problem)

Let E_1 and E_2 be quantum state probability distributions with density matrices ρ_1 and ρ_2. Assume that $\rho_1 \neq \rho_2$. Prove that E_1 and E_2 are physically distinguishable by specifying a measurement $M = \{Q_{\text{yes}}, Q_{\text{no}}\}$ with the following property: When measuring E_1 and E_2 with M, we get the outcome yes with different probabilities P_1 and P_2 (where $P_i := \Pr[\text{Outcome is yes when measuring } \rho_i]$).

Hint: Consider the matrix $\sigma := \rho_1 - \rho_2$. Show that σ is diagonalisable and that it therefore has an eigenvector $|\Psi\rangle$ with eigenvalue $\lambda \neq 0$. Set $Q_{\text{yes}} := |\Psi\rangle\langle\Psi|$. You may use without proof the fact that a density operator is always Hermitean.