Quantum Cryptography (fall 2018) Dominique Unruh

Exercise Sheet 3

Out: 2018-10-01 Due: 2018-10-08

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 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.

(c) 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).

(d) 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).

---

[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!).

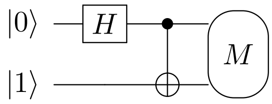
[2] This can be seen as an explanation what happens if we try to implement Schrödinger's cat: Even with a very high quality box, information about at least one atom of the cat will leak to the outside (i.e., it is measured whether the atom is "alive"). This has then an effect on the state of the whole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

[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?"

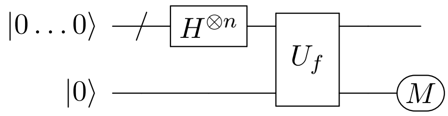
Problem 2: Quantum Circuits

(a) What are the possible outcomes of the measurement M? With which probabilities do they occur?



Here M is the complete measurement in the computational basis on the first and the second qubit.

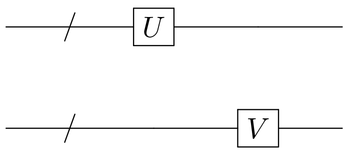
(b) Let $n := 8$ and $f(x) := 1$ iff x is a prime number (the bitstring $x \in \{0,1\}^n$ is interpreted as an integer in binary representation). What is the probability of measuring 1 in the measurement M?



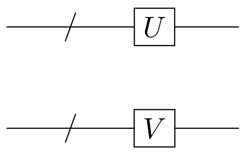
The unitary operation U_f is defined by $U_f|x, y\rangle := |x, y \oplus f(x)\rangle$ with $\oplus$ being the XOR.

Problem 2: Composite Systems

(a) Show that the following two circuits perform the same unitary operation.



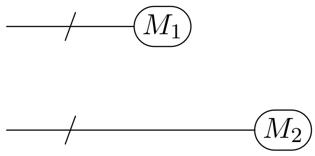
and



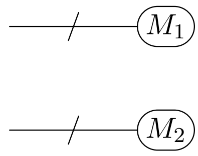
By this we mean that in the first case, first U is applied to the first system while nothing is done to the second, and then V is applied to the second system while nothing is done to the first. In the second case, both operations are applied simultaneously.

(Note that this implies that on independent subsystems, it does not matter whether we first operate on the first and then the second, or vice versa.)

(b) **(Bonus question)** Assume that the measurement M_1 is given by projectors $P_1, \ldots, P_n$ and that the measurement M_2 is given by projectors $Q_1, \ldots, Q_m$. Show that the following two circuits have the same effect. I.e., prove that for each i, j, the probability of getting the outcomes i, j is the same in both circuits, and the state after performing the measurements is the same.



and



(c) Explain (shortly) why (a) and (b) imply that one cannot use quantum mechanics to transfer information faster than light. (I.e., the only way to transfer information is to actually send something.)