Quantum Cryptography (fall 2013)	Prof. Dr. Dominique Unruh

Exercise Sheet 2

Out: September 19, 2013 — Due: September 25, 2013

You will need 50% of all homeworks to qualify for the exam. (That is, if you get at least 50%, your final grade will be the exam grade. And if you do not get 50%, you do not pass the course.)

You may hand in your solutions in person or by email. If you submit by email, either scan a handwritten solution or typeset your solution readably. I do not consider ASCII formulas readable.

When submitting, indicate your name and your matriculation number. On your first submission, please also indicate a password, this password will be needed for accessing the solutions and your points online.

Problem 1: Multiple qubits

(a) 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?

(b) 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?

(c) 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]

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

(e) 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.

(f) 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.)

(g) In the situation of (a), 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!).

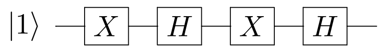
[2] This can be seen as an explanation what happens if we try to implement Schrödinger's cat: Even with a very high quality box, information about at least one atom of the cat will leak to the outside (i.e., it is measured whether the atom is "alive"). This has then an effect on the state of the whole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

(h) In the situation of (b), 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).

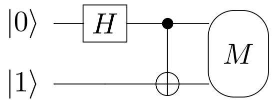
Problem 2: Quantum Circuits

(a) What is the state after this quantum circuit?



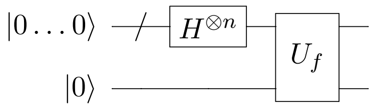
Note that $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the bit flip, and $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard transform.

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



Here $-\!\!(M)$ is the complete measurement on the first and the second qubit.

(c) Let f be a function from $\{0,1\}^n$ to $\{0,1\}$. What is the state resulting from this circuit?



By $-\!\!/\!\!-$ we denote a wire consisting of n qubits. The unitary operation U_f is defined by $U_f|x, y\rangle := |x, y \oplus f(x)\rangle$ with $\oplus$ being the XOR.

(d) 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?