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

Exercise Sheet 1

Out: September 12, 2013 — Due: September 19, 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: Qubits

(a) Let a quantum state $|\Psi\rangle \in \mathbb{C}^2$ and an (orthonormal) measurement basis $|\text{yes}\rangle, |\text{no}\rangle \in \mathbb{C}^2$ be given. Measure $|\Psi\rangle$ in that measurement basis. Let P_{yes} be the probability of outcome yes, and P_{no} the probability of outcome no. Show that $P_{\text{yes}} + P_{\text{no}} = 1$.

(b) Show that by applying a unitary transformation to a quantum state, no information is ever lost. More exactly, assume that a unitary transformation U is applied to a given quantum state $|\Psi\rangle$, resulting in a state $|\Phi\rangle$. Then show that there is another unitary transformation V (not depending on $|\Psi\rangle$ or $|\Phi\rangle$) such that applying V to $|\Phi\rangle$ gives $|\Psi\rangle$ again.

(c) Assume that a photon is in the state $|\Psi\rangle = \alpha|\updownarrow\rangle + \beta|\leftrightarrow\rangle$. Let R be a rotation of angle $\theta = \frac{\pi}{3}$. Let F denote a polarisation filter that lets only vertically polarised light through ($|\updownarrow\rangle$). Assume that the photon $|\Psi\rangle$ is first sent through R and then through F. It turns out that in this setting, the photon is absorbed by F with probability 1.

Given these informations, what do you know about α? (I.e., what are the possible values of α?)

(d) What is wrong with the following approach:

Alice has a qubit $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. She wants to initialise the qubit to $|0\rangle$. She knows that when measuring $|\Psi\rangle$ in the computational basis $|0\rangle, |1\rangle$, with probability $\frac{1}{2}$ she get the measurement outcome 0 and the qubit will be in state $|0\rangle$. Thus she repeatedly measures the qubit in the computational basis until she gets the outcome 0. Since the probability is $\frac{1}{2}$ each time, the expected number of measurements until she gets her $|0\rangle$-initialised qubit is 2.

(e) Which of the following are valid quantum states:

$$|1\rangle, \quad |0\rangle + |1\rangle, \quad \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle), \quad \tfrac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |1\rangle), \quad \sqrt{\tfrac{2}{3}}|0\rangle + \tfrac{i}{\sqrt{3}}|1\rangle.$$

(f) Which of the following are valid (unitary) transformations:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}}\begin{pmatrix} i & -1 \\ i & 1 \end{pmatrix}.$$

Problem 2: Bomb tester

In the lecture, we have described the bomb tester (see also Section 3 in the lecture notes). To test whether there is a bomb, we send a photon through the *upper* input path of the bomb tester (called $|0\rangle$ in the lecture, and $|\text{up}\rangle$ in the lecture notes). Assume instead that, with the same setup, we send the photon through the *lower* path. What happens? (Compute the probabilities for “bomb explodes”, “photon in upper path”, “photon in lower path” in the cases of “bomb” and “no bomb”.)