**Quantum Cryptography (spring 2020)** Dominique Unruh

# Exercise Sheet 2

Out: 2020-03-07 Due: 2020-03-22

## Problem 1: Simple quantum systems

(a) For each of the *valid* quantum states from Sheet 1 (a), answer the following: You perform a measurement in basis $\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}, \begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}$ (we call the corresponding outcomes "$+$" and "$-$"). What is the probability of answer $+$, what is the probability of answer $-$? What is the state after the measurement in each of those cases?

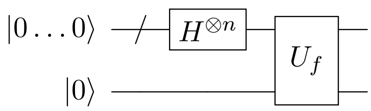
(b) Let a quantum state $\psi \in \mathbb{C}^2$ and an (orthonormal) measurement basis $\phi_{yes}, \phi_{no} \in \mathbb{C}^2$ be given. Measure $\psi$ in that measurement basis. Let $P_{\text{yes}}$ be the probability of outcome yes, and $P_{\text{no}}$ the probability of outcome no. Show that $P_{\text{yes}}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

(c) 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?

(d) 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

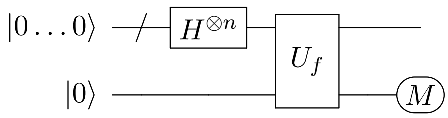
(a) Let $f$ be a function from $\{0,1\}^n$ to $\{0,1\}$. What is the state resulting from this circuit?




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. $H^{\otimes n}$ means $H \otimes H \otimes \dots \otimes H$ ($n$ times).

**Hint:** First figure out what $H^{\otimes n}|0\dots0\rangle$ is as a linear combination of basis vectors $|0\dots0\rangle, |0\dots01\rangle, |0\dots010\rangle, \dots$

(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 3: Improved bomb tester (bonus problem)

Consider a beam splitter that is parametrised by an angle $\theta$. This beam splitter performs the following operation $B_\theta$:

$$\begin{aligned} B_\theta \tbinom{1}{0} &= \cos\theta \tbinom{1}{0} + \sin\theta \tbinom{0}{1} \\ B_\theta \tbinom{0}{1} &= -\sin\theta \tbinom{1}{0} + \cos\theta \tbinom{0}{1} \end{aligned}$$

Here $\binom{1}{0}$ is a photon that is on the upper path, and $\binom{0}{1}$ a photon that is on the lower path.

(In other words, instead of reflecting half of the incoming light as did the beam splitter in the lecture, this beam splitter lets $(\sin\theta)^2$ of the light through and reflects $(\cos\theta)^2$.) Note that $B_{\frac{\pi}{4}}$ and $B_{-\frac{\pi}{4}}$ are the beam splitters described in the lecture.

Now consider the following setup: Let $n \in \mathbb{N}$. Fix $\theta := \frac{\pi}{2n}$. Take a photon and send it through the up-input of the beam splitter $B_\theta$ (i.e., the photon enters the beam splitter in state $\binom{1}{0}$).

Then the photon exits the beam splitter in a superposition $\Psi_1$ between $\binom{1}{0}$ and $\binom{0}{1}$. Put the box with the bomb in the down-path. After passing (or not passing) the box, the photon is in a superposition $\Phi_1$ between $\binom{1}{0}$ and $\binom{0}{1}$ (which depends on whether there was a bomb in the box or not).

Now take the photon and send it into the beam splitter again (without destroying the superposition $\Phi_1$). The photon leaves the beam splitter in a superposition $\Psi_2$. Put the box in the down-path. The photon is in state $\Phi_2$. Etc.

After $n$ iterations, measure $\Phi_n$.

This can be done with the experimental setup described in Figure 1 where the mirrors (a) and (b) need to be switched away at the right moment to let the light go into or come out of the experiment at the right iterations.

For notational convenience, define $\Gamma_\alpha := \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$.

(a) Assume that no bomb is in the box. Show that then $\Psi_j = \Phi_j = \Gamma_{j\theta}$ for $j = 1, \dots, n$. What is $\Gamma_{n\theta}$? What is the probability of measuring $\binom{0}{1}$ after the experiment (i.e., for measuring $\Phi_n$ as $\binom{0}{1}$)?

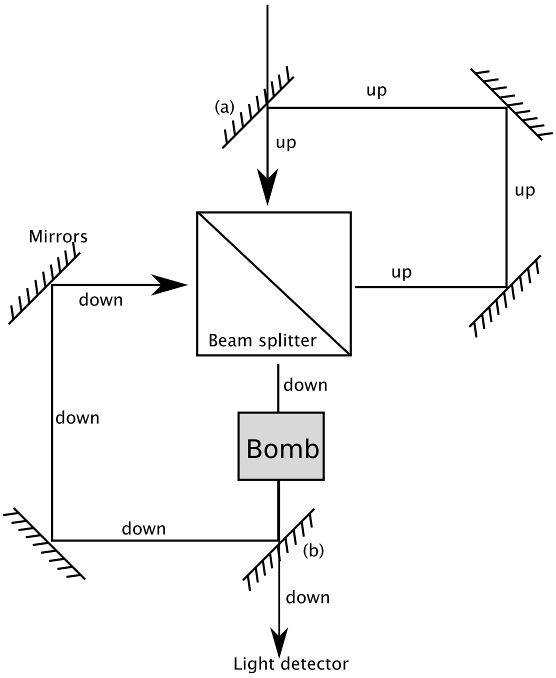



Figure 1: Bomb tester

(b) For the following questions, assume that there is a bomb in the box. What is the value of $\Psi_1$? What is the probability that the bomb explodes when $\Psi_1$ passes through the box? What is the state $\Phi_1$ of the photon after the box was in its path (under the condition that the bomb does not explode)?

(c) Show that the probability that the bomb does not explode in any of the $n$ iterations (i.e., that the state $\Psi_i$ will be measured as being in the up-path for each $i$) is $(\cos\theta)^{2n}$.

(d) Assuming that the bomb does not explode, what is the state coming out of the experiment? With what probability do we measure $\Phi_n$ as $\binom{0}{1}$?

(e) Fill out the following table (in terms of $n$):

| **Event** | **Probability if bomb** | **Probability if no bomb** |
|---|---|---|
| Bomb explodes | | 0 |
| Photon is in up-path | | |
| Photon is in down-path | | |

For interpreting these results, note that for $n \to \infty$, we have that $(\cos \frac{\pi}{2n})^{2n} \to 1$.