Quantum Cryptography (fall 2018)

Dominique Unruh

Exercise Sheet 2

Out: 2018-09-20

Due: 2018-09-27

Problem 1: Simple quantum systems

- (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) 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 $|ij\rangle$.

(d) 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.

Problem 2: Quantum Circuits

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

 $|1\rangle$

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) 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.



Figure 1: Bomb tester

Problem 3: Improved bomb tester (bonus problem)

Consider a beam splitter that is parametrised by an angle θ . This beam splitter performs the following operation B_{θ} :

$$B_{\theta} |\mathrm{up}\rangle = \cos \theta |\mathrm{up}\rangle + \sin \theta |\mathrm{down}\rangle$$
$$B_{\theta} |\mathrm{down}\rangle = -\sin \theta |\mathrm{up}\rangle + \cos \theta |\mathrm{down}\rangle$$

(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

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_{θ} (i.e., the photon enters the beam splitter in state $|up\rangle$).

Then the photon exits the beam splitter in a superposition $|\Psi_1\rangle$ between $|up\rangle$ and $|down\rangle$. Put the box with the bomb in the down-path. After passing (or not passing) the box, the photon is in a superposition $|\Phi_1\rangle$ between $|up\rangle$ and $|down\rangle$ (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 $|\Phi_1\rangle$). The photon leaves the beam splitter in a superposition $|\Psi_2\rangle$. Put the box in the down-path. The photon is in state $|\Phi_2\rangle$. Etc.

After *n* iterations, measure $|\Phi_n\rangle$.

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 $|\Gamma_{\alpha}\rangle := \cos \alpha |up\rangle + \sin \alpha |down\rangle$.

- (a) Assume that no bomb is in the box. Show that then $|\Psi_j\rangle = |\Phi_j\rangle = |\Gamma_{j\theta}\rangle$ for j = 1, ..., n. What is $|\Gamma_{n\theta}\rangle$? What is the probability of measuring $|\text{down}\rangle$ after the experiment (i.e., for measuring $|\Phi_n\rangle$ as $|\text{down}\rangle$)?
- (b) For the following questions, assume that there is a bomb in the box. What is the value of $|\Psi_1\rangle$? What is the probability that the bomb explodes when $|\Psi_1\rangle$ passes through the box? What is the state $|\Phi_1\rangle$ 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 $|\Psi_i\rangle$ 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 $|\Phi_n\rangle$ as $|\text{down}\rangle$?
- (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 $(\cos \frac{\pi}{2n})^{2n} \to 1$.