| **Quantum Cryptography (spring 2023)** | Dominique Unruh |
|---|---|
| **Exercise Sheet 02** | |
| Out: 2023-02-20 | Due: 2023-02-27 |

**The intro below was accidentally omitted in homework 1, so here it is again.**

**Read me:** 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. For nicely typeset solutions, you can get up to three extra points for the effort.

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.

You may work in teams to solve the problems. If you do, everyone has to formulate their own solution! (No copy&paste.)

Each problem has a table with some data to be filled by you. The prefilled field "knowlets" refers to the knowlets that this problem is based on (see the lecture notes). If you think the problem depends on a knowlet not indicated there, please add it. In the field "time", please indicate how long it took for you to solve this problem. In the field "difficulty", please indicate the perceived difficulty level as a grade from A–E. (E.g., B means that B-level student would probably be able to solve this fully.) The data you enter here does not affect your grade, it is used for statistics for future semesters. (If the exercise sheet itself is not part of your submission, please just provide the data somewhere in your submission.)

# 1 Working with quantum states (ctd.)

(a)

| **Knowlets:** | QState, Rota, ComplMeas ProblemID: RotaPolPhoton |
|---|---|
| **Time:** | |
| **Difficulty:** | |

Assume that a photon is in the state $\Psi = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$. (Here the $\alpha$ component corresponds to the vertical part and the $\beta$ component to the horizontal part.) Let $R$ be a rotation of angle $\theta = \frac{\pi}{3}$. Let $F$ denote a polarisation filter that lets only vertically polarised light through. Assume that the photon $\Psi$ 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 $\alpha$? (I.e., what are the possible values of $\alpha$?)

## 2 Composed systems

(a)

| | | |
|---|---|---|
| **Knowlets:** | Tensor | ProblemID: TensorDistrib |
| **Time:** | | |
| **Difficulty:** | | |

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 $|ij\rangle$.

(b)

| | | |
|---|---|---|
| **Knowlets:** | Tensor | ProblemID: TensorBili |
| **Time:** | | |
| **Difficulty:** | | |

**[Bonus problem]** 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.

(c)

| | | |
|---|---|---|
| **Knowlets:** | ProjMeas | ProblemID: ProjMeasPr1 |
| **Time:** | | |
| **Difficulty:** | | |

**[Bonus problem]** 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.

(d)

| | | |
|---|---|---|
| **Knowlets:** | ProjMeas | ProblemID: 5PathsMeas |
| **Time:** | | |
| **Difficulty:** | | |

In the situation of Homework 1, Problem 1 (h),[1] 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] 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?"

(e)

| Knowlets: | ProjMeas ProblemID: 5PathsMultiMeas |
|---|---|
| **Time:** | |
| **Difficulty:** | |

In the situation of Homework 1, Problem 1 (i),[2] 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).

## 3 Quantum circuits

(a)

| Knowlets: | PauliX, Hada, UniTrafo ProblemID: CircXHXH |
|---|---|
| **Time:** | |
| **Difficulty:** | |

What is the state after this quantum circuit?

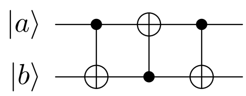
$$\begin{pmatrix}0\\1\end{pmatrix} \;-\!\boxed{X}\!-\!\boxed{H}\!-\!\boxed{X}\!-\!\boxed{H}\!-$$

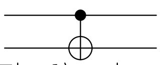
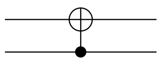
Note that $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ is the bit flip, and $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ is the Hadamard transform.

(b)

| Knowlets: | UniTrafo, ComposQState, CNOT ProblemID: TripleCNOT |
|---|---|
| **Time:** | |
| **Difficulty:** | |

What state comes out of the following circuit (for $a, b \in \{0, 1\}$)?



Here  denotes the controlled NOT, i.e., the operation defined by $\mathrm{CNOT}|a, b\rangle = |a, a \oplus b\rangle$. (And  analogously denotes the operation mapping $|a, b\rangle$ to $|a \oplus b, b\rangle$.)

What useful (and simple) function does the above circuit perform?

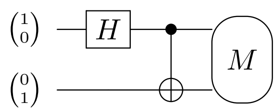
**Note:** Recall that $|a\rangle$ for some bit $a$ simply stands for one of the computational basis vectors. E.g., $|a\rangle = |0\rangle = \binom{1}{0}$ if $a = 0$. And similarly, $|a, b\rangle$ stands for one of the four basis vectors of a 2-qubit system. E.g., $|a, b\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$ if $a = 0$, $b = 1$.

[2] 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?"

(c)

| | |
|---|---|
| **Knowlets:** | ComposQState, ComposUni, Hada, CNOT, ComplMeas ProblemID: CircHCNOTM |
| **Time:** | |
| **Difficulty:** | |

What are the possible outcomes of the measurement $M$? With which probabilities do they occur?

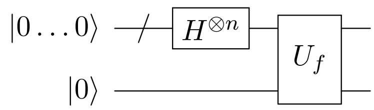


Here $-\!\!(M)$ is the complete measurement in the computational basis on the first and the second qubit.

(d)

| | |
|---|---|
| **Knowlets:** | ComposQState, ComposUni ProblemID: CircHadaAllUf |
| **Time:** | |
| **Difficulty:** | |

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



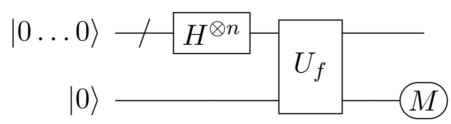
By $-\!\!/\!\!-$ we denote a wire consisting of $n$ qubits. The unitary operation $U_f$ is defined by $U_f|x,y\rangle := |x, y \oplus f(x)\rangle$ with $\oplus$ being the XOR. $H^{\otimes n}$ means $H \otimes H \otimes \cdots \otimes H$ ($n$ times).

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

(e)

| | |
|---|---|
| **Knowlets:** | ComposQState, ComposUni, ComposMeas ProblemID: CircHadaAllUfMeas |
| **Time:** | |
| **Difficulty:** | |

**[Bonus problem]** 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.

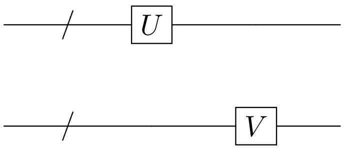
**Note:** Do/recall Problem 3 (d) first.

# 4 Independent operations

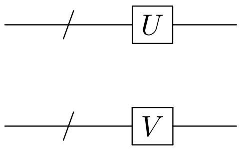
(a)

| | | |
|---|---|---|
| **Knowlets:** | ComposUni, Tensor | ProblemID: IndepU |
| **Time:** | | |
| **Difficulty:** | | |

Show that the following two circuits perform the same unitary operation.




and



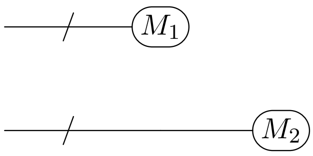

By this we mean that in the first case, first $U$ is applied to the first system while nothing is done to the second, and then $V$ is applied to the second system while nothing is done to the first. In the second case, both operations are applied simultaneously.

(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.)

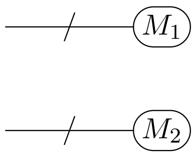
(b)

| | | |
|---|---|---|
| **Knowlets:** | Tensor, ComposMeas | ProblemID: IndepM |
| **Time:** | | |
| **Difficulty:** | | |

**[Bonus problem]** Assume that the measurement $M_1$ is given by projectors $P_1, \dots, P_n$ and that the measurement $M_2$ is given by projectors $Q_1, \dots, Q_m$. 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)

| | | |
|---|---|---|
| **Knowlets:** | | ProblemID: NoFTL |
| **Time:** | | |
| **Difficulty:** | | |

Explain (shortly) why Problem 4 (a) and Problem 4 (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.)