METU	**PHYS 455 (2021-1)** **Take home exam** Due: Feb. 2, 2022, Wednesday.

Correction:

- If there is a correction in the exams, I will show it in here and (also do the correction in the text.)

Notes:

- Please keep in mind that this is an exam. This means that you are not allowed to talk to each other. You are not also allowed to talk to another person outside the class. If you have any question to ask, you can ask me. You can also write an e-mail to me. You can share your *lecture notes* with your friends; there is no problem with this. In the past, there have been some students who violated this rule. For some reason they thought that I cannot understand. I do. And if I understand that you have violated this rule, I will not hesitate to lower your letter grade *at least* by one letter.
- The questions appear to be complicated. They are not. They are simple.
- The questions appear to be long. They are not. Try to keep your solution short.
- The primary purpose of this exam is for you to learn. For this reason, if you have any questions, or if you need some clarification, you should ask me.
- To err is human. I usually make mistakes. If you find any mistakes in this exam sheet, tell me so that I can correct them. The corrected versions will be posted on odtuclass. I will not send an e-mail notification if the correction is not critical. For this reason, it is a good idea to check odtuclass to see if there are any new corrections.
- Submit your exam by odtuclass. When you are taking pictures of your papers, use an app (like CamScanner in android) that cleans the pictures and builds a single PDF file.

50 **1.** (**Teleportation**) Alice and Bob are at two different cities. They can communicate with each other by telephone which can transmit only classical information. They also have particles A and B in the entangled state $|\Psi\rangle_{AB}$, which is described at the end of this problem. Alice also has a qubit C in the state

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \ ,$$

but it is not known what the coefficients are and therefore the state is unknown. In other words, C is a qubit which stores and unknown quantum information. Alice wants to teleport this state to Bob. After the successful completion of the teleportation protocol, Bob's particle should be in state $|\psi\rangle_B = a\,|0\rangle_B + b\,|1\rangle_B$.

Describe the protocol: Which projective measurement should Alice do on CA? Which information should be given to Bob over the telephone? Which unitaries should Bob apply to complete the protocol?

The state $|\Psi\rangle_{AB}$: To ensure that each student solves the problem independently of the others, each student will be given a different state $|\Phi\rangle$. We are going to decide which student works which state as follows: Let p be the last digit of your seven digit student ID. For example, if your student ID is 1234567 then $p = 7$. Find your last digit and use the appropriate state $|\Psi\rangle$ given in the following table:

Last digit, p	The state of AB
0	$\|\Psi\rangle_{AB} = \dfrac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
1	$\|\Psi\rangle_{AB} = \dfrac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
2	$\|\Psi\rangle_{AB} = \dfrac{\|01\rangle + \|10\rangle}{\sqrt{2}}$
3	$\|\Psi\rangle_{AB} = \dfrac{\|11\rangle - i\,\|00\rangle}{\sqrt{2}}$
4	$\|\Psi\rangle_{AB} = \dfrac{\|01\rangle - \|10\rangle}{\sqrt{2}}$
5	$\|\Psi\rangle_{AB} = \dfrac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
6	$\|\Psi\rangle_{AB} = \dfrac{\|11\rangle - i\,\|00\rangle}{\sqrt{2}}$
7	$\|\Psi\rangle_{AB} = \dfrac{\|01\rangle + i\,\|10\rangle}{\sqrt{2}}$
8	$\|\Psi\rangle_{AB} = \dfrac{\|00\rangle - i\,\|11\rangle}{\sqrt{2}}$
9	$\|\Psi\rangle_{AB} = \dfrac{\|00\rangle + i\,\|11\rangle}{\sqrt{2}}$

50 **2.** In Deutsch-Jozsa algorithm, it is possible to distinguish if a function is constant or balanced by doing a single function evaluation. Using the same algorithm it is also possible to say more about the unknown function. Consider bit-valued functions of 2-bits, i.e., $f : \{0,1\}\times\{0,1\} \longrightarrow \{0,1\}$, or $y = f(x_1, x_2)$ where each x_1, x_2 and y is a bit. There are 8 functions that are either constant or balanced, all of which are listed in the table below.

x_1x_2	f_1	$\overline{f}_1$	f_2	$\overline{f}_2$	f_3	$\overline{f}_3$	f_4	$\overline{f}_4$
00	0	1	0	1	0	1	0	1
01	0	1	0	1	1	0	1	0
10	0	1	1	0	0	1	1	0
11	0	1	1	0	1	0	0	1

Here, $\overline{f}_i$ expresses the NOT of f_i. Suppose that we have chip, a black-box, that computes one of these functions, but you don't know which. Remember that the effect of the function evaluation by the chip on 3 qubits can be described as

$$|x_1, x_2, r\rangle \longrightarrow U_f\,|x_1, x_2, r\rangle = |x_1, x_2, r \oplus f(x_1, x_2)\rangle \ ,$$

where $\oplus$ represents addition modulo 2. In Deutsch's problem, your job is to understand whether the unknown function computed by the chip is constant (either f_1 or $\overline{f}_1$) or balanced (one of the remaining 6). Deutsch-Jozsa algorithm solves this problem with a single evaluation of the function.

(a) The measurement of the Deutsch-Jozsa algorithm produces a 2-bit information, however, and using the additional information you can say more about the unknown function. Let's represent the measurement outcome as $x_1'x_2'$. For each possible outcome, $x_1'x_2'$, list *all* possible functions that the chip might be computing. (*Hint: First compute $P(x_1'x_2'|f)$, the probability of each outcome for each possible function. Then, for a given outcome $x_1'x_2'$, list all functions that could have produced it.*)

(b) All of the above will be valid if it is known for certain that the function that the chip computes is one of the above 8 functions. For this part of the question, suppose that the function computed by the chip might also be a ninth function, say g, as well as the above 8. The function g is obviously neither constant nor balanced. Suppose that you apply the Deutsch-Jozsa algorithm without any change. Compute the probability of each outcome, $P(x_1'x_2'|g)$, for the case the function computed is g. Finally, explain if you can distinguish between functions based on the measurement outcome.

The function g: To ensure that each student solves the problem independently of the others, each student will be given a different g function. We are going to decide which student works which function as follows: Let q be the second to last digit of your seven digit student ID. For example, if your student ID is 1234567 then $q = 6$. Find your second to last digit and use the appropriate function g given in the following table:

Second to last digit, q	The function to be used in part (b)
0	g_A
1	g_B
2	g_C
3	g_A
4	g_D
5	g_C
6	g_E
7	g_F
8	g_G
9	g_H

x_1x_2	g_A	g_B	g_C	g_D	g_E	g_F	g_G	g_H
00	1	0	0	0	0	1	1	1
01	0	1	0	0	1	0	1	1
10	0	0	1	0	1	1	0	1
11	0	0	0	1	1	1	1	0

50 **3. (BB84: A possible attack by Eve.)** Remember BB84 protocol for Quantum Key Distribution (QKD) between Alice and Bob. Alice randomly prepares qubits in one of the following 4 possible states

$$|\phi_{00}\rangle = |0\rangle \quad , \quad |\phi_{10}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad ,$$
$$|\phi_{01}\rangle = |1\rangle \quad , \quad |\phi_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad ,$$

and sends them to Bob. In $|\phi_{b,k}\rangle$ the subscript b indicates the basis and k denotes the value of the *private key* which Alice wants to communicate to Bob. Of course, they want to make sure that nobody else learns the value of k. After receiving the qubit, Bob measures the state either in $b = 0$ basis or $b = 1$ basis (chosen randomly) and determines his measured key value k'. Alice and Bob then announce the basis of preparation and the basis of measurement respectively. If they match, then they both know the value of the private key $k = k'$. To understand the presence of a possible eavesdropper (Eve), they announce some part of the private bits collected. If the disagreement between bits (bit value prepared by Alice and bit value measured by Bob) exceed a certain threshold, they understand the presence of Eve and stop communicating. Otherwise, if they agree, then they use the rest of the private bits for secret communication (by using one-time pad).

Let us use the following measure for the "disagreement". We will define this quantity for the two bases separately. For example, consider the situation where Alice prepares the qubit in b basis and Bob measures them in the same basis. The disagreement in b basis is then

$$\begin{aligned} D_b^{AB} =& \text{Prob(A prepares } |\phi_{b0}\rangle\text{, B measures 1)} \\ &+ \text{Prob(A prepares } |\phi_{b1}\rangle\text{, B measures 0)} \end{aligned}$$

which is essentially the probability that $k' \neq k$. We should have $D_0^{AB} = D_1^{AB} = 0$ if Eve is not listening. Note that, if Bob's measured key value k' is completely uncorrelated to Alice's k and it is uniformly distributed, then half of the outcomes will match accidentally even though there is no correlation. Therefore, the maximum value of disagreement is $D_b^{AB} = 1/2$. (Perhaps, $2D_b^{AB}$ is a more natural measure of disagreement because it is 1 when the disagreement is the largest.)

The information gained by Eve can also be measured by a quantity defined in the same manner. We can define D_b^{AE} for the fraction of bit disagreement between Alice and Eve in the b basis. Information gain by Eve is opposite to these quantities. For example, if D_b^{AE} is small, then Eve obtains large information, etc. The general result is: If Eve obtains information in a basis, then she will cause disturbance in the other basis, i.e., if D_0^{AE} is small, then D_1^{AB} is large. In this problem, we will demonstrate this feature of BB84 protocol by considering one possible attack by Eve.

Suppose that Eve attacks like this: After Alice prepared the qubit in one of those 4 possible states and sends it through the quantum communication channel, Eve captures the qubit and measures its state in the orthonormal basis $\{|\alpha_0\rangle, |\alpha_1\rangle\}$. Eve gets her bit value by this. Eve then sends the qubit in the same collapsed state (either $|\alpha_0\rangle$ or $|\alpha_1\rangle$, depending on the bit value

she obtained) to Bob. The rest of the protocol is the same. Suppose the α-basis is the following

$$\begin{aligned} |\alpha_0\rangle &= \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \quad , \\ |\alpha_1\rangle &= -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle \quad . \end{aligned}$$

Here θ is an arbitrary angle in the range $0 \le \theta \le \pi/2$. For the special case $\theta = 0$, α-basis is identical with the $b = 0$ basis. At the opposite extreme, for $\theta = \pi/2$ the α-basis is the same as $b = 1$ basis.

(a) Let $\phi = \pi/2 - \theta$ be the complementary angle. (If you view these kets as real vectors, $|\alpha_0\rangle$ makes angles $\theta/2$ with $|\phi_{00}\rangle$ and $\phi/2$ with $|\phi_{10}\rangle$). Check that the following equalities are satisfied and express them as trigonometric functions of these angles (these expressions might be useful in the remaining of the problem).

$$|\langle\phi_{b0}|\alpha_0\rangle|^2 = |\langle\phi_{b1}|\alpha_1\rangle|^2 = ?$$
$$|\langle\phi_{b0}|\alpha_1\rangle|^2 = |\langle\phi_{b1}|\alpha_0\rangle|^2 = ?$$

(b) Suppose that Alice prepared the qubit in $b = 0$ basis and Bob took the measurement in the same basis, i.e., qubit's initial state is either $|\phi_{00}\rangle$ (probability 1/2) or $|\phi_{01}\rangle$ (probability 1/2). When Eve intercepts the qubit and takes her measurement she can obtain 0 or 1. After that, when Bob receives the qubit in one of α-states, he does his measurement and can obtain 0 or 1. There are 8 possible results if you consider all measurements. Make a table of all of these possible results and compute the probability of occurrence of each.

A	E	B	Prob
0	0	0	?
0	0	1	?
0	1	0	?
⋮	⋮	⋮	⋮

(c) Mark the sets of results where there is disagreement between A and E. Also mark the sets where there is disagreement between A and B. Then compute D_0^{AE} and D_0^{AB}.

(d) The quantities D_1^{AE} and D_1^{AB} can be computed also with the same manner. However, the expressions will be similar to those in (c), except that θ is replaced by ϕ. Write down D_1^{AE} and D_1^{AB}.

(e) Show that

$$2D_0^{AB} + 2D_1^{AB} = 1 \quad .$$

In other words, Alice and Bob will detect significant disagreement either in $b = 0$ basis or in $b = 1$ basis or both. Therefore, they will understand that somebody is listening.

(f) Show that

$$\sqrt{2D_0^{AB}} + 2D_1^{AE} = 1 \quad .$$

In other words, if Eve obtains large information in $b = 1$ basis (D_1^{AE} is small) then Alice and Bob will detect significant disagreement in $b = 0$ basis (D_0^{AB} will be large).

(g) Compute all of these quantities (i) for $\theta = 0$ and (ii) for $\theta = \pi/2$.

Note: The following identities will be most probably/definitely useful

$$\begin{aligned}
\sin\theta &= 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} \quad , \\
\cos\theta &= \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} \\
&= 2\cos^2\frac{\theta}{2} - 1 \\
&= 1 - 2\sin^2\frac{\theta}{2} \ .
\end{aligned}$$