# Assignment 1

——

Please submit it electronically to ELMS. This assignment is 10% in your total points. For the simplicity of the grading, the total points for the assignment is 100. Note that we will reward the use of Latex for typesetting by bonus points (extra 5% of your points).

Problem 1. *Quantum Circuits*

1. *(10 points)* The CCCNOT (triple-controlled NOT) gate is a four-bit reversible gate that flips its fourth bit if and only if the first three bits are all in the state 1. Show how to implement a CCCNOT gate using Toffoli gates. You may use additional workspace as needed. You may assume that bits in the workspace start with a particular value, either 0 or 1, provided you return them to that value.

2. *(Bonus: 10 points)* Show that a Toffoli gate cannot be implemented using any number of CNOT gates, with any amount of workspace. Hence the CNOT gate alone is not universal. (Hint: It may be helpful to think of the gates as performing arithmetic operations on integers mod 2.)

——

Problem 2. *Mach-Zehnder interferometer with a phase shift.*
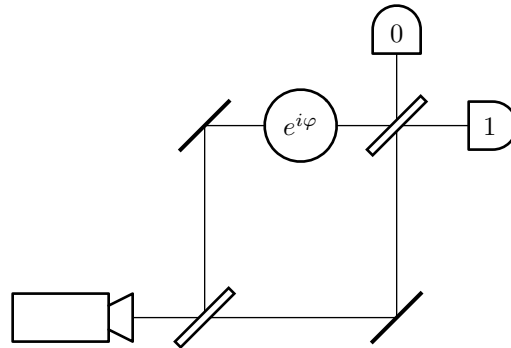
Analyze the experiment depicted above using the mathematical model described in class. (Note that the model from class differs slightly from the model described in the textbook; in particular, you should use the matrix $\frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix} \right)$ to model the beamsplitters.)

1. *(7 points)* Compute the quantum state of the system just before reaching the detectors. Express your answer using Dirac notation.

2. *(3 points)* Compute the probability that the "0" detector clicks as a function of φ, and plot your result for $\varphi \in [0, 2\pi]$.

——

Problem 3.

1. *(4 points)* Express each of the three Pauli operators,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

   using Dirac notation in the computational basis.

2. *(5 points)* Find the eigenvalues and the corresponding eigenvectors of each Pauli operator. Express the eigenvectors using Dirac notation.

3. *(3 points)* Write the operator $X \otimes Z$ as a matrix and using Dirac notation (in both cases using the computational basis).

4. *(3 points)* What are the eigenspaces of the operator $X \otimes Z$? Express them using Dirac notation.

5. *(5 points)* Using the Spectral Decomposition show that $HXH^\dagger = Z$, where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

———

Problem 4. *Unitary operations and measurements.* Consider the state

$$|\psi\rangle = \frac{2}{3}|00\rangle + \frac{1}{3}|01\rangle - \frac{2}{3}|11\rangle.$$

1. *(3 points)* Let $|\phi\rangle = (I \otimes H)|\psi\rangle$, where H denotes the Hadamard gate. Write $|\phi\rangle$ in the computational basis.

2. *(4 points)* Suppose the first qubit of $|\phi\rangle$ is measured in the computational basis. What is the probability of obtaining 0, and in the event that this outcome occurs, what is the resulting state of the second qubit?

3. *(4 points)* Suppose the second qubit of $|\phi\rangle$ is measured in the computational basis. What is the probability of obtaining 0, and in the event that this outcome occurs, what is the resulting state of the first qubit?

4. *(4 points)* Suppose $|\phi\rangle$ is measured in the computational basis. What are the probabilities of the four possible outcomes? Show that they are consistent with the marginal probabilities you computed in the previous two parts.

———

Problem 5. Let θ be a fixed, known angle. Suppose someone flips a fair coin and, depending on the outcome, either gives you the state

$$|0\rangle \quad \text{or} \quad \cos\theta|0\rangle + \sin\theta|1\rangle$$

(but does not tell you which).

1. *(5 points)* Consider measuring the given state in the orthonormal basis consisting of

$$|\phi\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle, \quad |\phi^\perp\rangle = \sin\phi|0\rangle - \cos\phi|1\rangle$$

   Find the probabilities of all the possible measurement outcomes for each possible value of the given state

2. *(7 points)* Calculate the probability of correctly distinguisihing the two possible states using the above measurement (In terms of ϕ)

3. *(8 points)* Calculate the optimal value of ϕ in order to best distinguish the states. What is the optimal success probability?

———

Problem 6. *Entanglement swapping.* Alice and Bob would like to share the entangled state $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Unfortunately, they do not initially share any entanglement, but fortunately, they have a mutual friend, Charlie. Alice shares a copy of $|\beta_{00}\rangle$ with Charlie, and Bob also shares a copy of $|\beta_{00}\rangle$ with Charlie.

1. *(5 points)* Write the initial state using Dirac notation in the computational basis, with the first qubit belonging to Alice, the second and third qubits belonging to Charlie, and the fourth qubit belonging to Bob.

2. *(5 points)* Suppose Charlie performs a Bell measurement on his two qubits (one of which is entangled with Alice and the other of which is entangled with Bob). For each possible measurement outcome, give the probability with which it occurs and the resulting post-measurement state for Alice and Bob.

3. *(5 points)* Describe a protocol whereby Charlie sends a classical message to Alice, and Alice processes her quantum state, such that Alice and Bob share the state $|\beta_{00}\rangle$ at the end of the protocol.

———

Problem 7. *Non-cloning theorem.* Please provide your answer and a brief explanation.

- *(5 points)* (Clone a random bit?) Given one sample of an unknown biased random coin (say, 0 with probability p and 1 with probability $1 - p$ and p unknown), is there a procedure to create two copies of such biased random coin? Namely, this procedure needs to generate two independent random coins with the same p.

- *(5 points)* (Clone one certain basis?) Is there a procedure to clone qubits restricted to $\{|+\rangle, |-\rangle\}$?

- *(Bonus: 5 points)* (Clone with many samples?) If you are given 1000 samples of an unknown biased random coin, is it possible to create 1,000,000 independent copies of the random coin? Here we allow the generated copies can be a little different from the original copy. Note that the precise number 1000 (or 1,000, 000) does not change the answer.

———