Assignment 1

Please submit it electronically to ELMS. This assignment is 6% in your total points. For the simplicity of the grading, the total points for the assignment are 60. Note that we will reward the use of Latex for typesetting with bonus points (an 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.

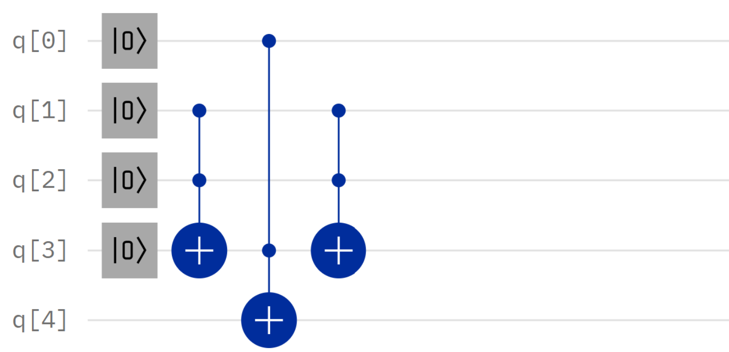

Figure 1: CCCNOT Gate Implementation

Disclaimer for figure 1: I didn't quite understand how to use the IBM workspace to make my diagram so I will explain it here to avoid confusion.

q[0],q[1],and q[2] are the 3 input control bits,q[3] is an extra control bit for workspace that always starts set to 0 (lets say the flag bit), and q[4] is the target bit.

the first toffoli gate sets the flag bit to 1 if q[1] and q[2] are 1, the second gate checks if q[0] and the flag bit (therefore q[1]q[2] are 0). If this is true it flips the target bit because all input bits are set to 1. the third gate flips the flag bit back if it was changed by the first gate

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.)

Answer:

For the CNOT gate suppose A is your control bit and B is your target bit. This gate can be represented by the operation (A+B)% 2 = Output. i.e if both are 1 or neither are 1 -¿ 0 and if only one of the bits is 1 then output is equal to 1

For the Toffoli gate suppose A and B are control bits and C is your target bit. this gate can be represented by the operation (AB+C)% 2 = Output. i.e if either control bit is 0 output will be equal to C (target bit doesnt change). if both are 1 the target bit will flip.

Based on these two operations we can see that the Toffoli gate can not be constructed fromany number of CNOT gate's because there is no operation to get from (A+B)%2 to (AB+C)%2

Problem 2. *Mach-Zehnder interferometer with a phase shift.*

$e^{i\varphi}$

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 $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to model the beamsplitters.)

1. *(3 points)* Compute the quantum state of the system just before reaching the detectors. Express your answer using Dirac notation.

Answer:

$$\frac{1}{2}(1+e^{i\varphi})\,|0\rangle + \frac{1}{2}(1-e^{i\varphi})\,|1\rangle$$

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

Answer:

$$p_0 = \frac{\cos\varphi + 1}{2}$$

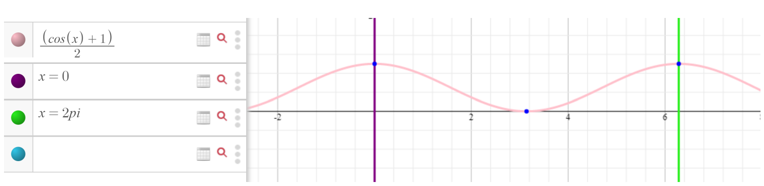

Figure 2: p_0 $\varphi \in [0, 2\pi]$

Problem 3.

1. *(3 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.

   Answer:

$$X = |0\rangle \langle 1| + |1\rangle \langle 0|$$
$$Y = i\,|1\rangle \langle 0| - i\,|0\rangle \langle 1|$$
$$Z = |0\rangle \langle 0| - |1\rangle \langle 1|$$

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

   Answer:

$$X, Y, Z : Eigvals : 1, -1$$
$$X : v1, v2 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$Y : v1, v2 = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$$
$$Z : v1, v2 = |0\rangle, |1\rangle$$

3. *(2 points)* Write the operator $X \otimes Z$ as a matrix and using Dirac notation (in both cases using the computational basis).

   Answer:

$$|00\rangle \langle 10| + |10\rangle \langle 00| - |11\rangle \langle 01| - |01\rangle \langle 11|$$

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

   Answer:

$$\lambda_1 = 1 : (|00\rangle + |10\rangle, |11\rangle - |01\rangle)$$

$$\lambda_2 = -1 : (|10\rangle - |00\rangle, |01\rangle + |11\rangle)$$

5. *(3 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

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

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

   Answer:

$$\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{3\sqrt{2}}\,|01\rangle - \frac{2}{3\sqrt{2}}\,|10\rangle + \frac{2}{3\sqrt{2}}\,|11\rangle$$

2. *(3 points)* Suppose the first qubit of $|\phi$ 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?

Answer:

1st Qubit:

$p_0 = (\frac{1}{\sqrt{2}})^2 + (\frac{1}{3\sqrt{2}})^2 = \frac{5}{9}$

2nd Qubit ($Q_1 = 0$):

$p_0 = 9/10$
$p_1 = 1/10$

State: $\sqrt{\frac{9}{10}}\,|0\rangle + \sqrt{\frac{1}{10}}\,|1\rangle$

3. *(3 points)* Suppose the second qubit of $|\phi$ 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?

Answer:

2nd Qubit:

$p_0 = (\frac{1}{\sqrt{2}})^2 + (\frac{2}{3\sqrt{2}})^2 = \frac{13}{8}$
1st Qubit ($Q_2 = 0$):

$p_0 = 9/13$
$p_1 = 4/13$

State: $\sqrt{\frac{9}{13}}\,|0\rangle + \sqrt{\frac{4}{13}}\,|1\rangle$

4. *(3 points)* Suppose $|\phi$ 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.

Answer:

$p(|00\rangle) = (\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$
$p(|01\rangle) = (\frac{1}{3\sqrt{2}})^2 = \frac{1}{18}$
$p(|10\rangle) = (\frac{-2}{3\sqrt{2}})^2 = \frac{2}{9}$
$p(|11\rangle) = (\frac{2}{3\sqrt{2}})^2 = \frac{2}{9}$

Probability of Q_1 and Q_2 equalling 0
$p(Q_1 == 0) = \frac{10}{18}$
$p(Q_2 == 0) = \frac{13}{18}$

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

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

(but does not tell you which).

1. *(4 points)* Consider measuring the given state in the orthonormal basis consisting of

$$|\phi = \cos\phi|0 + \sin\phi|1 , \qquad |\phi^{\perp} = \sin\phi|0 - \cos\phi|1$$

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

   Answer:

   $p_1(|0\rangle -> |\phi\rangle) = (\cos\phi)^2$
   $p_2(|0\rangle -> |\phi^{\perp}\rangle) = (\sin\phi)^2$
   $p_3(\cos\theta\,|0\rangle + \sin\theta\,|1\rangle -> |\phi\rangle) = (\cos\phi\cos\theta + \sin\phi\sin\theta)^2$
   $p_4(\cos\theta\,|0\rangle + \sin\theta\,|1\rangle -> |\phi^{\perp}\rangle) = (\cos\theta\sin\phi - \cos\phi\sin\theta)^2$

2. *(5 points)* Calculate the probability of correctly distinguishing the two possible states using the above measurement (In terms of ϕ)
   Answer:

   Probability of correctly distinguishing $== \frac{1}{2}(p_1 + p_4) == \frac{1}{2}((\cos\phi)^2 + (\cos\theta\sin\phi - \cos\phi\sin\theta)^2)$

3. *(Bonus: 5 points)* Calculate the optimal value of ϕ in order to best distinguish the states. What is the optimal success probability? **Optimal value: when ϕ is equal to θ**

Problem 6. *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.

  Answer Yes there is. In this scenario we are dealing with classic bits, therefore we can use the "CNOT" gate or Controlled not gate to clone the bits (outcomes of the coin flip 0 or 1 can be thought of as a bit)

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

  Answer No. This would violate the no-cloning theorem. In order to measure and clone the state we would be destroying it in the process, therefore we cannot clone it

- *(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.

  Answer With 1000 samples we can create an approximation of the random biased coin by setting a ratio based on the outcomes. With this, we can create our 1,000,000 approximate copies. It is okay that this is only an estimation because we allow for the copies to be slightly different from the original biased coin

---