Intorduction to Quantum Computing: Homework #1

Due on April 28, 2020

Jakub Filipek

Question 1

Part (a)

We will prove that by contradiction.
Suppose such operation exists. Let P be a probability. Then there exists a quantum state Q such that, P corresponds to probabilities of that state.
In fact for each P there exist multiple quantum states Q, but for each Q there exists a unique probability state P.
Since Q cannot be copied due to the *No Clonning Theorem* on quantum distributions, that implies that P cannot be copied too (if it could then going

$$Q, 0 \rightarrow P, 0, \rightarrow P, P \rightarrow Q, Q$$

would break quantum version of *No Clonning Theorem*).
Hence probability distributions cannot be cloned.

Part (b)

The main similarity is the fact that they go hand in hand, and if one is true, then the other is true too. However, their main difference is in the fact the probability states have to preserve L_1 norm, while quantum states have to preserve L_2 norm.

Question 2

Part (a)

First let us denote states as integers. Hence $|10010\rangle = |18\rangle$ or just 18 in table below.
Let us consider the left side of the circuit. I omitted states 4-7 and 12-31. This is because we know that third and fifth qubit are in $|0\rangle$ on entrance.
Then let us consider right side of the equation. Since the first two Toffoli gates we can combine these steps. Secondly, we can push the measurement of the third qubit back, and make doubly controlled Z gate be controlled on 2 qubits (instead of qubit and a bit). This way we measure third qubit right after that controlled Z gate
Since last column in both table for left and right side of the equation are the same.

Operation:	Toffoli	Toffoli	Toffoli
0	0	0	0
1	1	1	1
2	2	2	2
3	7	7	3
8	8	8	8
9	9	9	9
10	10	10	10
11	15	31	27

Table 1: Table for left side of the equation. The first and third Toffoli gates are controlled on first and second qubit, with third as a target, while the middle is controlled on third and fourth, with fifth qubit as a target.

Operation:	2 x Toffoli	H	CCZ	Measurement + Classical Flip
0	0	0 + 4	0 + 4	0
1	1	1 + 5	1 + 5	1
2	2	2 + 6	2 + 6	2
3	7	3 - 7	3 + 7	3
8	8	8 + 12	8 + 12	8
9	9	9 + 13	9 + 13	9
10	10	10 + 14	10 + 14	10
11	31	27 - 31	27 + 31	27

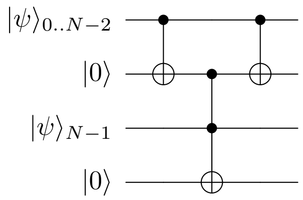
Table 2: Table for right side of the equation. The CCZ is Controlled-Controlled-Z Gate, with first and third qubits being contols, and second being a target. The Measurement and Classical Flip of the third qubit are combined into one step, since they occur on classical computation.

Part (b)

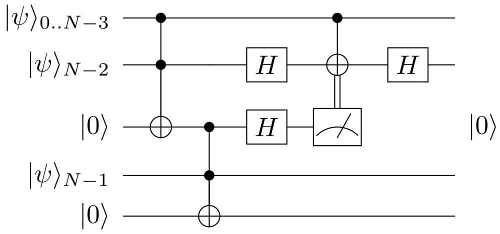
The assumption is the fact that the resulting 5 qubit state can be written as a product state of third qubit with remaining 4 qubits.
Hence measuring it does not affect other states (apart from possibly flipping the global phase, which is then flipped back).

Part (c)

The Naive (Left side) generalization of the N-bit is as follows



We can see that it already uses $C^{N-1}(X)$ and C^2X gates.
For the right side, first, lets note that $C^n(Z) = HC^n(X)H$, where Hadamard Gates are performed on the target qubit.
Then the circuit below generalizes the Craig Gidney circuit to N qubits:



Let us note that the half-classically, half-quantum controlled gate in a middle is really a $C^{N-2}(X)$ gate, but is only applied iff the measurement is 1. Then, while not noted in the circuit the ancilla qubit is flipped (conditioned classically) to $|0\rangle$. This can happen at any time after $C^{N-2}(X)$.
In that case we can think of the above circuit in the same exact way as a circuit from part a, if we think of $|\psi\rangle_{0..N-3}$ as just $|\psi\rangle_3$, which is $|1\rangle$ iff $|\psi\rangle_{0..N-3} = |11...11\rangle$, and $|0\rangle$ otherwise.

Hence we can use Table 2, to prove that this one works (since, as mentioned in class $HXH = Z$).

Part (d)

Firstly let's note that the ancilla qubit is a target of $C^{N-1}(X)$. Hence, apart from base case any new step up the stack of N's adds just a 1 new qubit per operation. This except for a base case ($N = 3$), where we need 2 qubits (ancilla and target).

Then number for implementation of $C^{N-2}(X)$ we can just reuse these ancilla qubits, because all of them will be in $|0\rangle$, when the main $C^2(X)$ is applied. Hence, no additional qubits are required for this step.

$$\begin{aligned}
Q(N) &= \\
&= \begin{cases} 2 & \text{if } N = 3 \\ 1 + Q(N-1) & \text{otherwise} \end{cases} \\
&= 1 + \sum_{3}^{N} 1 \\
&\in O(N)
\end{aligned}$$

Let $T(N)$ be a function that outputs number of Toffoli's given number of control qubits. Then $T(3) = 2$, otherwise:

$$\begin{aligned}
T(N) &= \\
&= 1 + T(N-1) + T(N-2) \\
&\leq 1 + 2T(N-1) \\
&= 1 + \sum_{i=3}^{N-1} 2^i \\
&\leq 1 + \sum_{i=0}^{N-1} 2^i \\
&= 1 + 2^N - 1 \\
&\in O(2^N)
\end{aligned}$$

Lastly let $C(N)$ be a function that outputs a number of CNOT gates, given the number of control qubits. In the base case $T(3) = 1$, otherwise:

$$C(N) = T(N-1) + T(N-2)$$

This is just a Fibonacci formula. Fibonacci numbers are bounded by $O(2^N)$. Hence, $C(N) \in O(2^N)$.

Question 3

Part (a)

Let $|\psi\rangle$ denote Alice's state. If $|\psi\rangle$ is a product state, then we can trivially see, that we can teleport each qubit separately, and they will not affect each other.
If $|\psi\rangle$ is an entangled state, then the same protocol (applied to each qubit) would also work. Let us assume that $|\psi_i\rangle$ and $|\psi_j\rangle$ are entangled. Then $|0_{Ai}\rangle$ and $|0_{Aj}\rangle$ would also get entangled during a process of teleportation protocol. Hence, their measurement results would not be independent from each other, and then there would be exact correlation between X and Z gates applied to the $|0_{Bi}\rangle$ and $|0_{Bj}\rangle$. Because of that Bob would also receive a quantum state entangled in the exactly same way as the Alice's.

Part (b)

Let us first consider the probability that a single qubit reached Bob:

$$P(Q) = (1-P)^d$$

Lastly, let R denote an number of successful runs, given r tries. Then, since it is a binomial distribution of Bernoulli runs with $p = P(Q)$:

$$E[R] = r(1-P)^{dN}$$

Let $1-\delta$ denote the high probability, of transferring at least one state. Then:

$$\begin{aligned} 1-\delta &\leq P(R \geq 1) \leq \frac{E[R]}{1} \\ 1-\delta &\leq r(1-P)^{dN} \\ \frac{1-\delta}{(1-P)^{dN}} &\leq r \end{aligned}$$

Hence we see that $r \in \Theta(\frac{1}{(1-P)^{dN}})$

Part (c)

Now instead we will use stations. Hence probability of single qubit reaching next station is:

$$P(Q) = (1-P) = E[Q]$$

Problem 3 continued on next page...

Then, for a whole state to reach a next station is:

$$P(S) = (1-P)^N = E[S]$$

Lastly, let R denote an number of successful transfers (between 2 stations), given r tries.

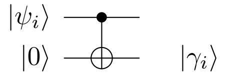
$$E[R] = r(1-P)^N$$

We will need to transfer a state successfully d times. Hence:

$$\begin{aligned} 1-\delta &\leq P(R \geq d) \leq \frac{E[R]}{d} \\ 1-\delta &\leq r\frac{(1-P)^N}{d} \\ d\frac{1-\delta}{(1-P)^N} &\leq r \end{aligned}$$

Hence we see that $r \in \Theta(\frac{d}{(1-P)^{dN}})$, which is exponentially better in d then in case of part b.

Let us assume, that Alice cannot generate copies of the state. With assumption that when state gets lost there is no information from it, we can do the following. Let Alice prepare r different states, and call this set Γ. For each $|\gamma\rangle \in \Gamma$, each qubit in gamma will be applied this transformation:



Hence $|\gamma\rangle$ will be strongly entangled with $|\psi\rangle$.

Then we just send all states in Γ. They can be lost, and measured (after being lost), but since we will receive none of that information, we can assume as if it did not happen. This is, $|\psi\rangle$ will become a mixed state, but to us there will be no difference, and we can view it a pure state.

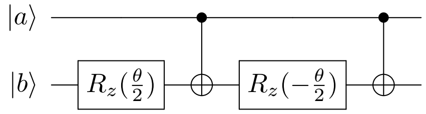
This way we can just repeat the procedure described in part c, and get $1-\delta$ success rate.

Question 4

Part (a)

$$\begin{aligned} XR_Z(\theta)X &= \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & e^{-i\frac{\theta}{2}} \\ e^{i\frac{\theta}{2}} & 0 \end{pmatrix} \\ &= \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix} \\ &= \begin{pmatrix} e^{-i\frac{-\theta}{2}} & 0 \\ 0 & e^{i\frac{-\theta}{2}} \end{pmatrix} \\ &= R_Z(-\theta) \end{aligned}$$

Part (b)



- if $|a\rangle = |0\rangle$, then the behaves as follows: $|a\rangle|b\rangle \rightarrow |a\rangle R_z(-\frac{\theta}{2})R_z(\frac{\theta}{2})|b\rangle$, since we rotate, and then *unrotate* $|b\rangle$, then this is just $|a\rangle|b\rangle \rightarrow |a\rangle|b\rangle$. Which is how controlled gate would behave.

- if $|a\rangle = |1\rangle$, then the behaves as follows: $|a\rangle|b\rangle \rightarrow |a\rangle XR_z(-\frac{\theta}{2})XR_z(\frac{\theta}{2})|b\rangle$.
  From part a, we can shorten this circuit to: $|a\rangle|b\rangle \rightarrow |a\rangle R_z(\frac{\theta}{2})R_z(\frac{\theta}{2})|b\rangle = |a\rangle R_z(\theta)|b\rangle$.

Hence this circuit behaves like Controlled $R_Z(\theta)$.