C S 358H: Intro to Quantum Information Science

Sayam Sethi

September 2024

Contents

1 Local Evolution of Entangled States

Question 1.1

Question. *Suppose Alice and Bob share the two qubit entangled state*

$$|EPR\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

and suppose that Alice applies a one qubit unitary transformation U to her qubit. Show that this has exactly the same effect as if Bob had applied the unitary transformation U^T (not the conjugate-transpose of U, just the transpose) to his qubit.

Proof. Let the unitary transform U be given by $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then, the state of the system after Alice applies U to her qubit is,

$$\begin{aligned} |\mathrm{EPR}'\rangle &= (U \otimes I)\,|\mathrm{EPR}\rangle \\ &= \begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \frac{a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle}{\sqrt{2}} \end{aligned} \tag{1}$$

Now, the state of the system after Bob applies U^T to his qubit is,

$$\begin{aligned} |\mathrm{EPR}''\rangle &= (I \otimes U^T)\,|\mathrm{EPR}\rangle \\ &= \begin{pmatrix} a & c & 0 & 0 \\ b & d & 0 & 0 \\ 0 & 0 & a & c \\ 0 & 0 & b & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &= \frac{a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle}{\sqrt{2}} \end{aligned} \tag{2}$$

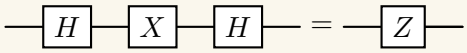
Therefore, $|\mathrm{EPR}'\rangle = |\mathrm{EPR}''\rangle$. Hence, proved. □

2 Multi-qubit quantum circuits

For the following circuits, calculate the output state before the measurement.

Question 2.1

Question. *Prove the following identity.*



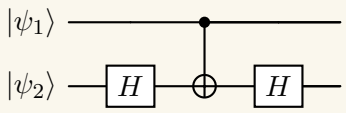
Show that this also implies

Proof. To prove the identitiy, it is enough the prove that it holds for both the basis states $|0\rangle$ and $|1\rangle$. Note that the eigenvectors of the X gate are the $|+\rangle$ and $|-\rangle$ states with the eigenvalues equal to $+1, -1$ respectively. Therefore, the result of applying the circuit on the left, HXH is equal to doing nothing on the $|0\rangle$ state, whereas it adds a global phase of -1 on the $|1\rangle$ state as input. This is exactly what the Z gate does. Therefore, the identity holds, since for any arbitrary quantum state, we will be applying the operations in superposition on both the basis states.
Similarly, it is easy to see that the second identity also holds. We just pre-multiply and post-multiply both sides with the H gate. This cancels out the H gate on the LHS (since it is it's own inverse), resulting in X, but the RHS transforms to HZH. □

Question 2.2

Question. *The 2-qubit CSIGN gate (also known as a controlled-Z gate) operates by applying a relative phase shift of -1 to the $|1\rangle$ component of the second qubit if the first qubit is equal to 1 and otherwise does nothing. As a matrix it is given explicitly by the diagonal matrix diag(1,1,1,-1). Using part a, show how to simulate a CSIGN gate using only CNOT and Hadamard gates by writing down the appropriate circuit; show your derivation or give a brief explanation of why the circuits are equivalent.*

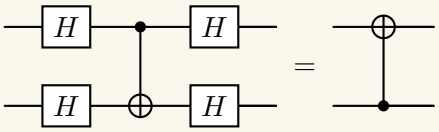
Solution. Note that the CNOT gate is equivalent to applying a conditional X gate on the second qubit, conditioned on the value of the first qubit. Therefore, we can execute the CSIGN gate as follows,



The reason this circuit works is because the CNOT gate has no effect when the control qubit is in the $|0\rangle$ state, and therefore the H gates cancel out. However, when the control qubit is in the $|1\rangle$ state, the operations on the second qubit act as if we are applying HXH, which is equal to Z, as shown in Question 2.1. □

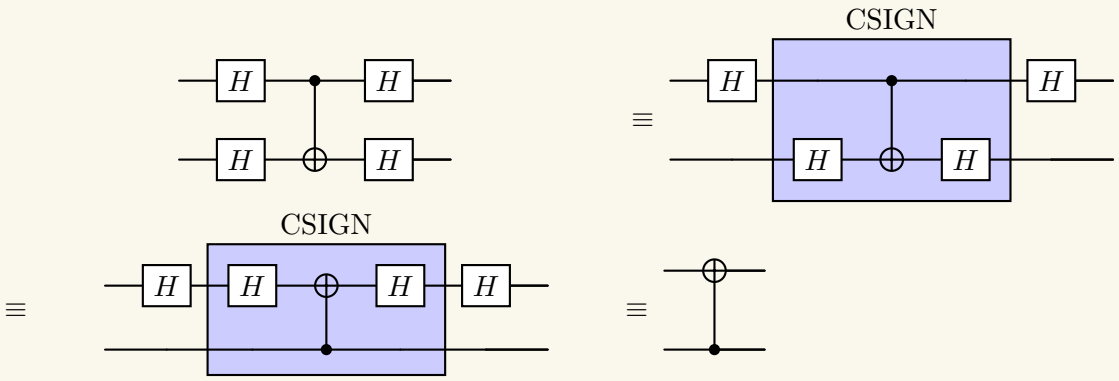
Question 2.3

Question. *Prove the following identity:*



In other words: show that a CNOT by which qubit A controls qubit B, when viewed in a different basis, is actually a CNOT by which qubit B controls qubit A! This illustrates how, with quantum information, unlike with classical information, there's no way for one system to affect another one without the possibility of being affected itself.
We do not want you to solve this problem by brute force. Max of 2 points for a solution using explicit matrix multiplication.
Hint: Using parts a and b, note that CSIGN is the same when applied in either direction.

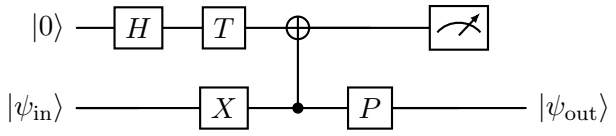
Proof. Note that the CSIGN gate has a non-trivial effect (out of all basis states) only when both the control and target qubits are in the state $|1\rangle$. This is symmetric in both the control and target qubits and the effect is just going from $|11\rangle \to -|11\rangle$, which is also symmetric in the control and target. Therefore, the CSIGN gate is equivalent even if we swap the control and target qubits.
Now we show the equality using the following circuit transformations:



Hence, proved. □

3 IBM Q Experience & Multi-qubit measurements

Consider the following circuit. Write $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.



Where

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, \quad X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}, \quad P = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}.$$

Note: You must show work for question (a) thru (d).

Question 3.1

Question. *What is the state of the first qubit before the CNOT?*

Solution. The state of the qubit after the H gate is $|+\rangle$ and after the T gate is $\frac{|0\rangle+e^{i\pi/4}|1\rangle}{\sqrt{2}}$, which is also the state before the CNOT. □

Question 3.2

Question. *What is the state of the two qubits before the measurement?*

Solution. The state of the second qubit before the CNOT is $\beta|0\rangle + \alpha|1\rangle$. Therefore, the combined state of the two qubits after the CNOT is,

$$\begin{aligned}|\Psi\rangle &= \frac{1}{\sqrt{2}}\left(\beta|00\rangle + e^{i\pi/4}\beta|10\rangle + e^{i\pi/4}\alpha|01\rangle + \alpha|11\rangle\right)\\ &= |0\rangle\frac{1}{\sqrt{2}}\left(\beta|0\rangle + e^{i\pi/4}\alpha|1\rangle\right) + |1\rangle\frac{1}{\sqrt{2}}\left(e^{i\pi/4}\beta|0\rangle + \alpha|1\rangle\right)\end{aligned} \tag{3}$$

The state of the two qubits after applying the P gate is,

$$|\Psi\rangle = |0\rangle\frac{1}{\sqrt{2}}\left(\beta|0\rangle + e^{3i\pi/4}\alpha|1\rangle\right) + |1\rangle\frac{e^{i\pi/4}}{\sqrt{2}}\left(\beta|0\rangle + e^{i\pi/4}\alpha|1\rangle\right) \tag{4}$$

□

Question 3.3

Question. *What are the probabilities of measuring $|0\rangle$ and of measuring $|1\rangle$ on the first qubit?*

Solution. Since the amplitudes for both $|0\rangle$ and $|1\rangle$ on the first qubit have equal magnitude ($= \frac{|\alpha|^2+|\beta|^2}{2} = \frac{1}{2}$), therefore the probability of measuring both states is equal. □

Question 3.4

Question. *When the first qubit is measured as* $|0\rangle$*, then what is the second qubit state* $|\psi_{out}\rangle$*? How about when it's measured as* $|1\rangle$*?*

Solution. The state of the second qubit if the first qubit is measured as $|0\rangle$ is $|\psi_{\text{out},0}\rangle = \beta|0\rangle + e^{3i\pi/4}\alpha|1\rangle$. Similarly, if the first qubit is measured as $|1\rangle$, then the state of the second qubit is $|\psi_{\text{out},1}\rangle = e^{i\pi/4}\left(\beta|0\rangle + e^{i\pi/4}\alpha|1\rangle\right) \equiv \beta|0\rangle + e^{i\pi/4}\alpha|1\rangle$. □

Question 3.5

Question. *Launch the IBM Quantum Composer. The website should give you a brief tutorial; it's optional whether you complete the tasks it suggests.*
Create the circuit above.
Once you have done this, change the backend to a real quantum computer with enough qubits, and run it.
Submit a screenshot of the results. *Your simulated results were likely not exactly what you predicted, due to statistical noise. The results from the real device will likely be even more different; this is an example of noise due to hardware errors on real quantum devices! (Caveat: Your results are likely better than they should be, because IBM performs some optimization to remove and simplify various gates before submitting your job to the device.)*

Solution. The screenshots for running on the statevector and IBM Sherbrooke are attached.

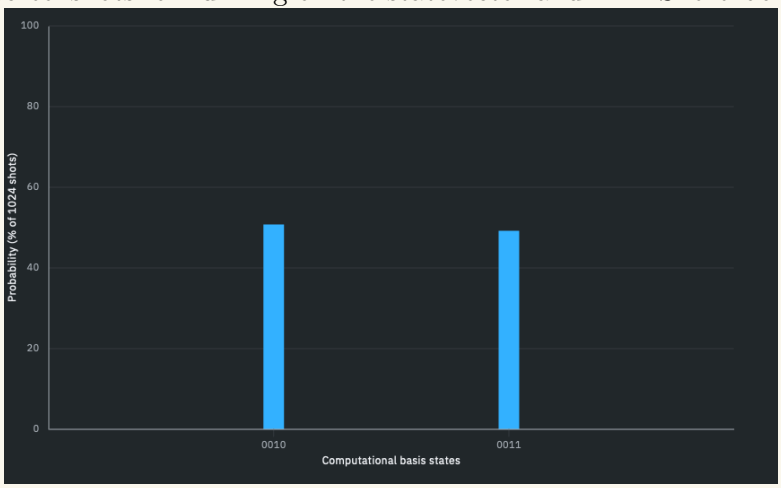


Figure 1: Screenshot of the results from the IBM Quantum Composer for statevector simulation.

Figure 2: Screenshot of the results from the IBM Quantum Composer on IBM Sherbrooke. □

Question 3.6

Question. *For discrete classical distributions, the Total Variational (TV) distance between two distributions p and q is $\frac{1}{2}\sum_{x\in X}|p(x)-q(x)|$ where X is the set of all possible outcomes. Calculate the empirical TV distances of the ideal distribution you calculated in parts (a) to (d) from the distribution produced by the qasm simulator and from the distribution produced by the quantum computer. Show your work.*

Solution. The probability distribution for the ideal circuit is $\{0, 0.5, 0, 0.5\}$ for the states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ respectively. The probability distribution for the statevector simulation is approximately $\{0, 0.507, 0, 0.493\}$. The probability distribution on running it on IBM Sherbrooke is approximately $\{0.011, 0.475, 0.040, 0.474\}$. Note that we consider the states as $|q_0q_1\rangle$, unlike the plots from IBM which consider the states as $|q_1q_0\rangle$. The TV distance between the ideal and statevector simulation is,

$$\begin{aligned}\mathsf{TV}(\text{ideal, statevector}) &= \frac{1}{2}\left(|0-0|+|0.5-0.507|+|0-0|+|0.5-0.493|\right)\\ &= \frac{1}{2}(0.007+0.007)\\ &= 0.007\end{aligned} \tag{5}$$

The TV distance between the ideal and IBM Sherbrooke is,

$$\begin{aligned}\mathsf{TV}(\text{ideal, statevector}) &= \frac{1}{2}\left(|0-0.011|+|0.5-0.475|+|0-0.04|+|0.5-0.474|\right)\\ &= \frac{1}{2}(0.011+0.025+0.04+0.026)\\ &= 0.051\end{aligned} \tag{6}$$

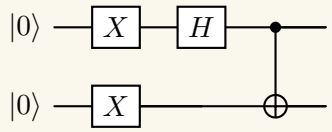
□

4 Constructing Quantum Circuits

Question 4.1

Question. *Without using any measurements, create a quantum circuit that maps* $|00\rangle$ *to* $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

Solution. Consider the following quantum circuit,



This circuit maps $|00\rangle$ to $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. □

Question 4.2

Question. *Create the circuit (with measurements added to both qubits) within the IBM Q Experience. Run it on a quantum computer. Again, include a screenshot of the results. Hopefully, this gives you a nice introduction to IBM Q. There are other software suites available online, but this may be the most convenient. In the future, if you're struggling with analyzing a quantum circuit, you might use this as a tool.*

Solution. The quantum circuit was created in the IBM Quantum Composer and run on the IBM Q Experience. The results are shown in Figure 3 and Figure 4.

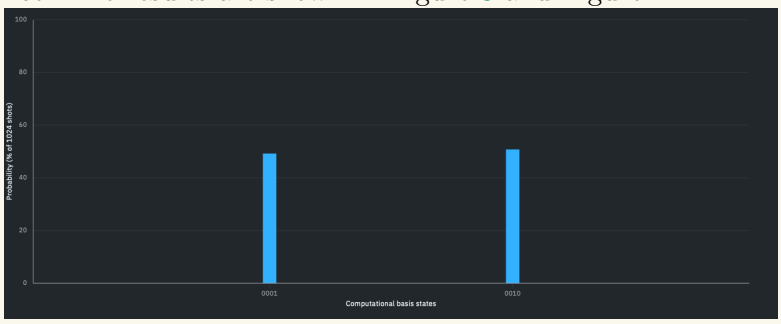


Figure 3: Screenshot of the results from the IBM Quantum Composer for statevector simulation.

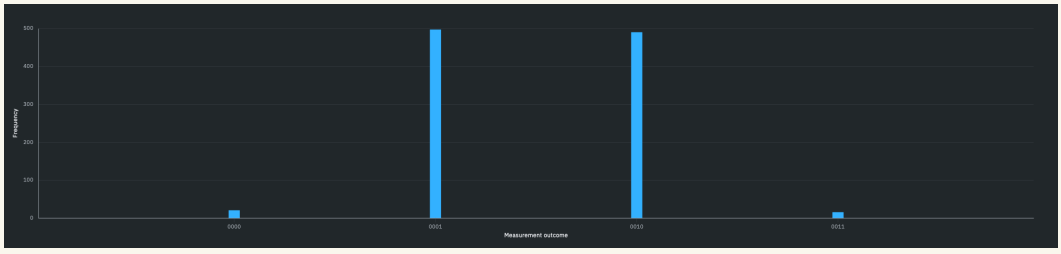


Figure 4: Screenshot of the results from the IBM Quantum Composer on IBM Sherbrooke.

□

Question 4.3

Question. *Calculate the empirical TV distance of the theoretical output distribution of the circuit from the distribution produced by the quantum computer. Show your work.*

Solution. The theoretical output distribution will be $\{0, 0.5, 0.5, 0\}$. The output ditribution from the statevector is $\{0, 0.508, 0.492, 0\}$ and from IBM Sherbrooke is $\{0.020, 0.479, 0.485, 0.016\}$. Therefore, the TV distance between the theoretical distribution and statevector distribution is 0.008 and between the theoretical distribution and IBM Sherbrooke distribution is 0.036. □

5 Another Quantum Money Attack

Question 5.1

Question. *Suppose you're a quantum money counterfeiter, trying to forge a banknote in Wiesner's scheme. You're given a qubit that's* $|0\rangle$ *,*$|1\rangle$*,* $|+\rangle$ *or* $|-\rangle$*, each with equal probability 1/4. You can apply any quantum circuit you like to the qubit to produce a two-qubit state (two fake banknotes). Then, both of your output qubits will separately be given back to the bank for verification. In other words, if the bank's records indicate this banknote's original qubit was* $|0\rangle$ *or* $|1\rangle$*, then the bank will measure in the* $\{|0\rangle, |1\rangle\}$ *basis. You are a successful counterfeiter if and only if both of your qubits match the state of the original qubit and the bank accepts them (presumably you visit the bank multiple times, maybe in different outfits). Likewise if the original qubit was* $|+\rangle$ *or* $|-\rangle$*, the bank will measure and check in the* $\{|+\rangle, |-\rangle\}$ *basis. Your goal is to maximize the probability that the bank accepts. In class, we saw a procedure that breaks this scheme with probability* $\frac{5}{8}$*.*
Now, consider the following counterfeiting procedure. Consider two qubits set to $|0\rangle$ *and the qubit from a banknote to be counterfeited (we consider this the 'third' qubit below). Then, apply a 3-qubit unitary transformation whose effect is the following mapping:*

$$|000\rangle \mapsto \frac{\sqrt{3}}{2}|000\rangle + \frac{|110\rangle + |101\rangle + |011\rangle}{\sqrt{12}}$$
$$|001\rangle \mapsto \frac{\sqrt{3}}{2}|111\rangle + \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{12}}$$

Finally, measure the first qubit in the $\{|0\rangle, |1\rangle\}$*-basis. The second two qubits are your counterfeit banknotes.*
Show that the probability of success is strictly greater than $\frac{5}{8}$*.*
Hint: break it up into cases depending on whether the outcome of the measurement is $|0\rangle$ *or* $|1\rangle$*.*
Note: This procedure actually turns out to be the optimal one.

Proof. Let us find the probability to fool the bank in the cases when qubit is $|0\rangle$ and $|+\rangle$. The other two cases follow from it.
When qubit is $|0\rangle$,
After applying the unitary and discarding the first qubit, we get $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$ with probability $\frac{1}{6}$ and $\frac{3|00\rangle+|11\rangle}{\sqrt{10}}$ with probability $\frac{5}{6}$.
From here the chance of the strategy succeeding $= \frac{1}{6} \times 0 + \frac{5}{6} \times \frac{9}{10} = \frac{3}{4}$.
Similarly the probability for $|1\rangle$ is also $\frac{3}{4}$.

Now when qubit is $|+\rangle$,
After applying the unitary and discarding the first qubit, we get $\frac{3|00\rangle+|01\rangle+|10\rangle+|11\rangle}{\sqrt{12}}$ with probability $\frac{1}{2}$ and $\frac{|00\rangle+|01\rangle+|10\rangle+3|11\rangle}{\sqrt{12}}$ with probability $\frac{1}{2}$.
Working with first factor, we apply Hadamard on the two qubits, and then find the probability of getting $|00\rangle$(which corresponds to $|++\rangle$ in the original case).

Applying Hadamard, we get $\frac{3|00\rangle+|01\rangle+|10\rangle+|11\rangle}{\sqrt{12}}$ (note that this is the same as the state before the Hadamard, i.e., this implies that the state is an eigenvector for the $H \otimes H$ gate) and probability of getting $|00\rangle$ is $\frac{3}{4}$ in this case.
Similarly for the other factor, applying Hadamard, we get $\frac{3|00\rangle-|01\rangle-|10\rangle+|11\rangle}{\sqrt{12}}$ and probability of getting $|00\rangle$ is $\frac{3}{4}$ in this case as well.
Therefore the overall probabilty for this case comes out to be $\frac{3}{4}$.
Similarly for the case when qubit is $|-\rangle$, we get the probability as $\frac{3}{4}$.
Therefore the probability in all the four cases comes out to be $\frac{3}{4}$ which ultimately is the overall probability. □