Introduction to Quantum Information Science
Homework 3

Due Wednesday, September 22 at 11:59 PM

1. Local Evolution of Entangled States [3 Points] Suppose Alice and Bob share the two qubit entangled state

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

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.

Solution: Alice applying U yields

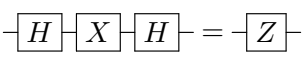
$$\left(U \otimes I\right)|\text{EPR}\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} u_{00} & & u_{00} & \\ & u_{01} & & u_{01} \\ u_{10} & & u_{10} & \\ & u_{11} & & u_{11} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}.$$

And Bob applying U^T gives

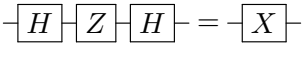
$$\left(I \otimes U^T\right)|\text{EPR}\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} u_{00} & u_{10} & & \\ u_{01} & u_{11} & & \\ & & u_{00} & u_{10} \\ & & u_{01} & u_{11} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}.$$

2. Multi-qubit quantum circuits

a) [4 Points] Prove the following identity.



Show that this also implies



Solution:

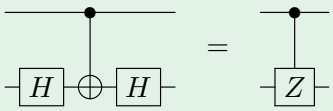
$$HXH = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

Noting that $H^2 = I$, we can right and left multiply both sides of the equation by H to get

$$H^2XH^2 = HZH \implies X = HZH.$$

b) [3 Points] 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: Observe $HXH = Z$. Applying the identity,

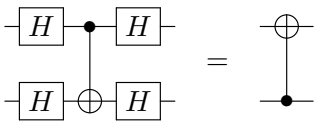


where recall the CNOT is the same as a controlled-X gate.

Substituting single-qubit identities into multi-qubit gates does not work in general. But, this works because all of the unitaries involved are block diagonal. In block form, we have:

$$\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & Z \end{bmatrix}$$

c) [3 Points] Prove the following identity:

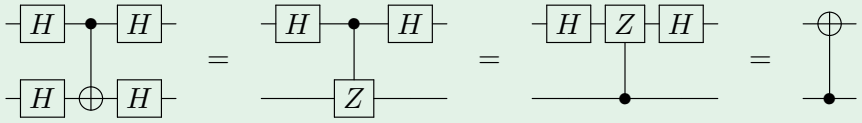


In other words: show that a CNOT by which qubit A controls qubit B, when viewed in a different basis, is actually a CNOT by which qubit B controls qubit A! This illustrates how, with quantum information, unlike with classical information, there's no way for one system to affect another one without the 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.

Solution:



Of course, one may choose to do the calculations.

The first way of doing so is by checking via matrix multiplication:

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

$$\frac{1}{4}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}$$

Here is one way to do it in Dirac notation. The CNOT gate can be written like this:

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

Now conjugate everything with the Hadamard gate:

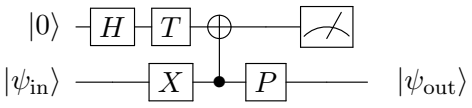
$$\begin{aligned}(H \otimes H)\text{CNOT}(H \otimes H) &= |+\rangle\langle +| \otimes I + |-\rangle\langle -| \otimes Z \\ &= \frac{I+X}{2} \otimes \big(|0\rangle\langle 0| + |1\rangle\langle 1|\big) + \frac{I-X}{2} \otimes \big(|0\rangle\langle 0| - |1\rangle\langle 1|\big) \\ &= I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|\end{aligned}$$

Yet another way is to look at what happens to the computational basis states. We can verify that:

$$\begin{aligned}|00\rangle &\xrightarrow{H\otimes H} |++\rangle \xrightarrow{CNOT} |++\rangle \xrightarrow{H\otimes H} |00\rangle \\ |01\rangle &\xrightarrow{H\otimes H} |+-\rangle \xrightarrow{CNOT} |--\rangle \xrightarrow{H\otimes H} |11\rangle \\ |10\rangle &\xrightarrow{H\otimes H} |-+\rangle \xrightarrow{CNOT} |-+\rangle \xrightarrow{H\otimes H} |10\rangle \\ |11\rangle &\xrightarrow{H\otimes H} |--\rangle \xrightarrow{CNOT} |+-\rangle \xrightarrow{H\otimes H} |01\rangle\end{aligned}$$

which is precisely the affect of applying CNOT from the second qubit to the first qubit.

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).

a) [1 point] What is the state of the first qubit before the CNOT?

b) [1 point] What is the state of the two qubits before the measurement?

c) [1 point] What are the probabilities of measuring $|0\rangle$ and of measuring $|1\rangle$ on the first qubit?

d) [2 points] When the first qubit is measured as $|0\rangle$, then what is the second qubit state $|\psi_{\text{out}}\rangle$? How about when it's measured as $|1\rangle$?

Solution: (a) Let $|\psi_{\text{in}}\rangle = \alpha|0\rangle + \beta|1\rangle$. The state before the CNOT is:

$$\begin{aligned} TH|0\rangle \otimes X|\psi_{\text{in}}\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\pi/4}|1\rangle\big) \otimes \big(\alpha|1\rangle + \beta|0\rangle\big) \\ &= \frac{1}{\sqrt{2}}\big(\beta|00\rangle + \alpha|01\rangle + \beta e^{i\pi/4}|10\rangle + \alpha e^{i\pi/4}|11\rangle\big). \end{aligned}$$

The state of the first qubit is given above: $\frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\pi/4}|1\rangle\big)$.

(b) After the CNOT, just before measuring:

$$|\psi_{\text{meas}}\rangle = \frac{1}{\sqrt{2}}\big(\beta|00\rangle + \alpha e^{i\pi/4}|01\rangle + \beta e^{i\pi/4}|10\rangle + \alpha|11\rangle\big)$$

If you want you could also multiply in the P before measuring, it does not affect the measurement results:

$$(I \otimes S)|\psi_{\text{meas}}\rangle = \frac{1}{\sqrt{2}}\big(\beta|00\rangle + i\alpha e^{i\pi/4}|01\rangle + \beta e^{i\pi/4}|10\rangle + i\alpha|11\rangle\big)$$

(c) The probability of measuring $|0\rangle$ on the first qubit is the sum of the probability of $|00\rangle$ and the probability of $|01\rangle$:

$$P_0 = |\langle 00|\psi_{\text{meas}}\rangle|^2 + |\langle 01|\psi_{\text{meas}}\rangle|^2 = \frac{|\beta|^2}{2} + \frac{|\alpha|^2}{2} = \frac{1}{2}$$

So $P_1 = 1/2$ as well. The probabilities do not depend on $|\psi_{\text{in}}\rangle$.

(d) For each case, we keep the terms compatible with the measurement result. These terms don't immediately give a normalzied state (magnitude 1), so we normalize; here, it's equivalent to dropping the factor of $1/\sqrt{2}$. We have

$$\begin{aligned} |\psi^0_{\text{out}}\rangle &= \beta|0\rangle + i\alpha e^{i\pi/4}|1\rangle = \beta|0\rangle + \alpha e^{i3\pi/4}|1\rangle \\ |\psi^1_{\text{out}}\rangle &= \beta e^{i\pi/4}|0\rangle + i\alpha|1\rangle. \end{aligned}$$

Note, in case P was ignored earlier, the last state is equivalent to $\beta|0\rangle + \alpha e^{i\pi/4}|1\rangle$ up to a phase.

e) [Ungraded] Create an account with IBM Q Experience `https://quantum-computing.ibm.com/`. It's probably fastest to create an account using the Google, GitHub, or other OAuth sign in.

f) [3 Points] 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. The composer will automatically set $|\psi\rangle = |0\rangle$. Add a measurement to both qubits, not just the top one. It may be tricky to add the CNOT: note that you can add a NOT gate, then right-click and select "add control". Make sure that when you add the P gate, its parameter is set to $\pi/2$.

Note that when you add a measurement operator, the plots automatically generated below the circuit will give bad results. You can ignore them. (Those plots are useful for circuits which contain no measurements, because they represent the state at the end of the circuit, but measurements collapse the state.)

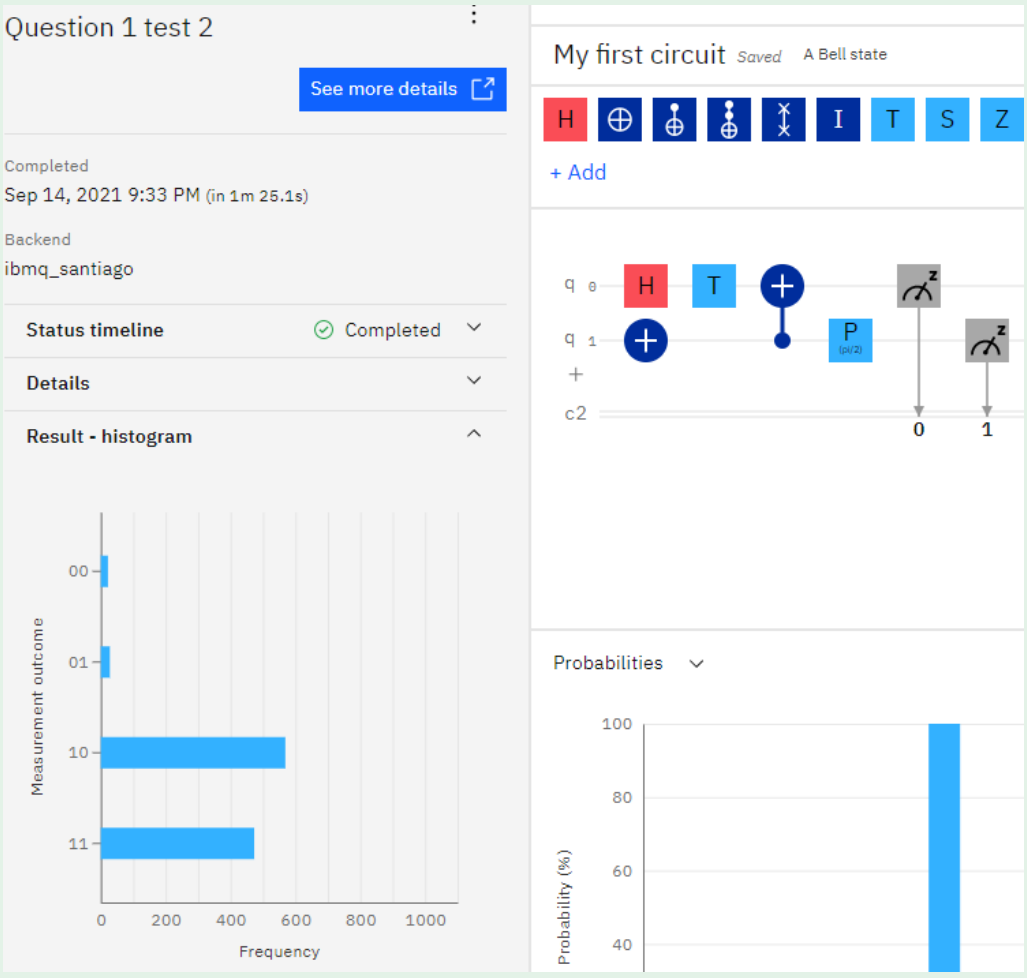
Click "Setup and run" and choose the *ibmq_qasm_simulator*. Keep the number of shots at the default 1024. View the results and verify that they match (ignoring some statistical noise) your predictions from the previous question for when $|\psi\rangle = |0\rangle$. (1 shot is 1 run of the circuit — remember these are probabilistic, so we need to run the circuits many times to learn what the output distribution is.) **Note:**

IBM flips the order of the qubits, so the top qubit is the least-significant/rightmost bit, and the bottom qubit is the most-significant/leftmost bit (apparently, IBM is staking a claim on quantum little-endian vs big-endian).

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:



g) [1 Point] 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 exact numbers will change based on your results.

For the simulator, the total shots was 1092, the state $|01\rangle$ was observed 556 times, and $|11\rangle$ was observed 536 times. That gives probabilities 0.5091 and 0.4908, respectively. The ideal distribution

is probability 0.5 for these two states. Therefore, the total variation distance is

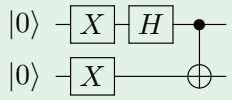
$$\frac{1}{2}\left(|0.5 - 0.5091| + |0.5 - 0.4908|\right) \approx 0.00915.$$

For the real quantum computer, the total shots was 1092, the state $|00\rangle$ was observed 22 times which is 0.02014, the state $|01\rangle$ was observed 569 times which is 0.52106, the state $|10\rangle$ was observed 28 times which is 0.02564, and the state $|11\rangle$ was observed 472 times which is 0.43223. The ideal distribution would have had probabilities 0, 0.5, 0, and 0.5, respectively. Therefore, the total variation distance is ≈ 0.067305.

4. Constructing Quantum Circuits

a) [3 Points] Without using any measurements, create a quantum circuit that maps $|00\rangle$ to $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

Solution:

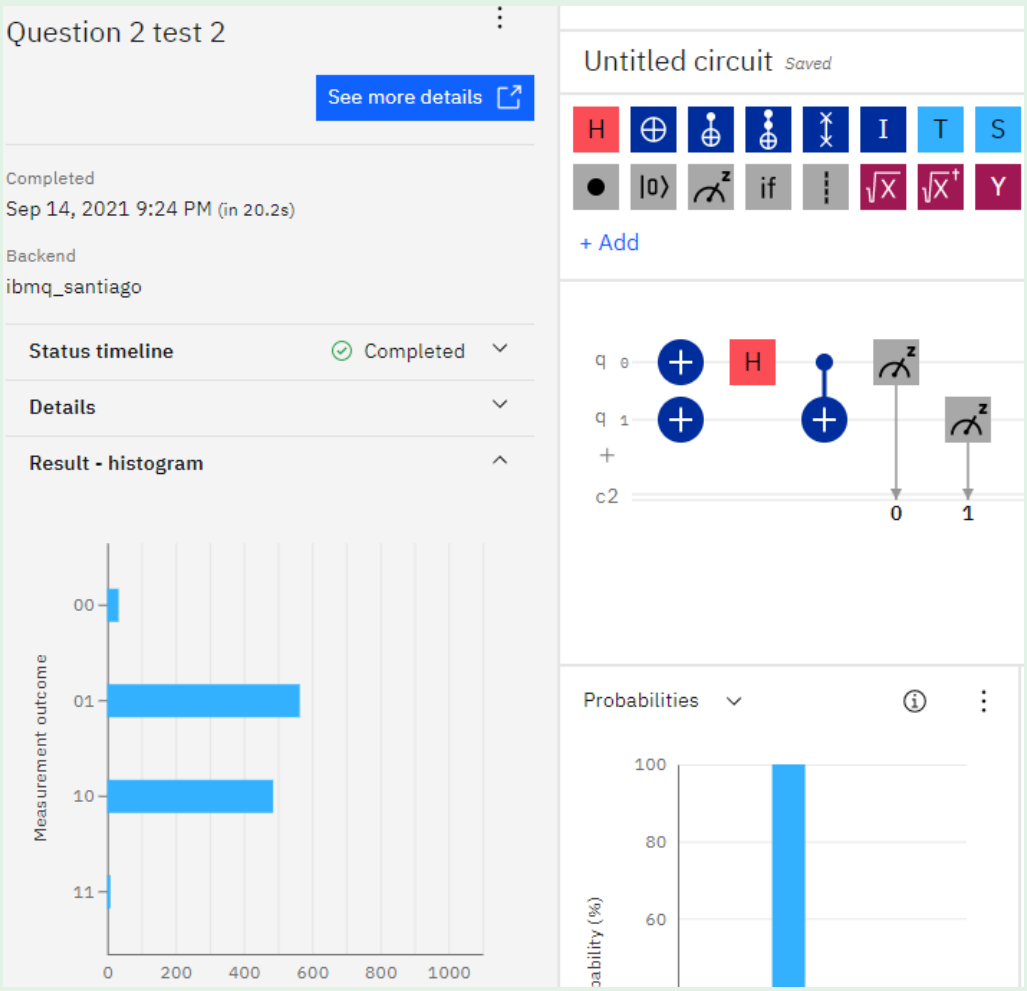


$$|00\rangle \to |11\rangle \to \frac{|01\rangle - |11\rangle}{\sqrt{2}} \to \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

b) [3 Points] 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:



c) [1 Point] 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 total shots was 1092, the state $|00\rangle$ was observed 33 times which is 0.03021, the state $|01\rangle$ was observed 486 times which is 0.44505, the state $|10\rangle$ was observed 564 times which is 0.5164, and the state $|11\rangle$ was observed 9 times which is 0.00824. The ideal distribution would have had probabilities 0, 0.5, 0.5, and 0, respectively. Therefore, the total variation distance is ≈ 0.0549.

5. Another Quantum Money Attack [5 Points] 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.

Solution: Let's consider the case in which the qubit $|\psi_i\rangle$ on the bill is set to be $|0\rangle$. Then for the counterfeiter to succeed, she must either measure $|0\rangle$ on the first qubit and the bank must measure $|00\rangle$ on the second and third qubit. Or the counterfeiter must measure $|1\rangle$ while the bank still measures $|00\rangle$. In other words, if we treat this as a single measurement, we must either observe $|000\rangle$ or $|100\rangle$. Letting U be the unitary applied by the counterfeiter this gives us

$$\begin{aligned}\Pr[\text{success}] &= |\langle 000|\, U\, |000\rangle|^2 + |\langle 100|\, U\, |000\rangle|^2 \\ &= \left|\frac{\sqrt{3}}{2}\langle 000|000\rangle + \frac{\langle 000|110\rangle + \langle 000|101\rangle + \langle 000|011\rangle}{\sqrt{12}}\right|^2 \\ &\quad + \left|\frac{\sqrt{3}}{2}\langle 100|000\rangle + \frac{\langle 100|110\rangle + \langle 100|101\rangle + \langle 100|011\rangle}{\sqrt{12}}\right|^2 \\ &= \frac{3}{4}.\end{aligned}$$

By the exact same reasoning the other three cases are:

If given $|1\rangle$:

$$\begin{aligned}\Pr[\text{success}] &= |\langle 011|\, U\, |001\rangle|^2 + |\langle 111|\, U\, |001\rangle|^2 \\ &= \left|\frac{\sqrt{3}}{2}\langle 011|111\rangle + \frac{\langle 011|001\rangle + \langle 011|010\rangle + \langle 011|100\rangle}{\sqrt{12}}\right|^2 \\ &\quad + \left|\frac{\sqrt{3}}{2}\langle 111|111\rangle + \frac{\langle 111|001\rangle + \langle 111|010\rangle + \langle 111|100\rangle}{\sqrt{12}}\right|^2 \\ &= \frac{3}{4}.\end{aligned}$$

If given $|+\rangle$:

$$\begin{aligned}\Pr[\text{success}] &= |\langle 0{+}{+}|\, U\, |00{+}\rangle|^2 + |\langle 1{+}{+}|\, U\, |00{+}\rangle|^2 \\ &= \left|\frac{\langle 000|\, U\, |00{+}\rangle + \langle 001|\, U\, |00{+}\rangle + \langle 010|\, U\, |00{+}\rangle + \langle 011|\, U\, |00{+}\rangle}{2}\right|^2 \\ &\quad + \left|\frac{\langle 100|\, U\, |00{+}\rangle + \langle 101|\, U\, |00{+}\rangle + \langle 110|\, U\, |00{+}\rangle + \langle 111|\, U\, |00{+}\rangle}{2}\right|^2\end{aligned}$$

(Noting that $U|00+\rangle$ is the superposition of all eight terms in the definition of U and in each case only keeping the one yielding a non-zero inner product)

$$= \left|\frac{\frac{\sqrt{3}}{2} + \frac{1}{\sqrt{12}} + \frac{1}{\sqrt{12}} + \frac{1}{\sqrt{12}}}{2\sqrt{2}}\right|^2 + \left|\frac{\frac{1}{\sqrt{12}} + \frac{1}{\sqrt{12}} + \frac{1}{\sqrt{12}} + \frac{\sqrt{3}}{2}}{2\sqrt{2}}\right|^2$$
$$= \frac{3}{4}.$$

If given $|-\rangle$:

$$\begin{aligned}\Pr[\text{success}] &= |\langle 0--|\, U\, |00-\rangle|^2 + |\langle 1--|\, U\, |00-\rangle|^2 \\ &= \left|\frac{\langle 000|\, U\, |00-\rangle - \langle 001|\, U\, |00-\rangle - \langle 010|\, U\, |00+\rangle + \langle 011|\, U\, |00-\rangle}{2}\right|^2 \\ &\quad + \left|\frac{\langle 100|\, U\, |00-\rangle - \langle 101|\, U\, |00-\rangle - \langle 110|\, U\, |00-\rangle + \langle 111|\, U\, |00-\rangle}{2}\right|^2\end{aligned}$$

(As in the previous case, but carefully minding the signs)

$$= \left|\frac{\frac{\sqrt{3}}{2} + \frac{1}{\sqrt{12}} + \frac{1}{\sqrt{12}} + \frac{1}{\sqrt{12}}}{2\sqrt{2}}\right|^2 + \left|\frac{-\frac{1}{\sqrt{12}} - \frac{1}{\sqrt{12}} - \frac{1}{\sqrt{12}} - \frac{\sqrt{3}}{2}}{2\sqrt{2}}\right|^2$$
$$= \frac{3}{4}.$$

So no matter what we're given, the counterfeiting succeeds with probability $\frac{3}{4}$.