Programming a quantum computer – Day 2
Exercises

Peter Brown

June 20, 2022

1 Theory questions

1. **A general qubit gate** Note that a general qubit gate can be written as

$$U(\theta,\phi,\lambda) = \begin{pmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\phi}\sin(\theta/2) & e^{i(\phi+\lambda)}\cos(\theta/2) \end{pmatrix} \tag{1}$$

and so by specifying (θ,ϕ,λ) we can write any single qubit quantum gate.

(a) Write down the parameters (θ,ϕ,λ) that specify the Pauli gates X, Y and Z and the Hadamard gate.

(b) Show that U is really a quantum gate.

2. **Entanglement as quantum correlations**

(a) Show that if two qubits are not entangled then regardless of whatever measurement we perform the statistics will always be independent, i.e.,

$$\mathbb{P}(a,b) = \mathbb{P}(a)\mathbb{P}(b) \tag{2}$$

where $\mathbb{P}(a,b)$ is the joint probability of getting outcome a on qubit 1 and outcome b on qubit 2 and $\mathbb{P}(a)$, $\mathbb{P}(b)$ are the marginal probabilities for the measurements on qubit 1 and qubit 2 respectively. This shows that non-entangled quantum systems lead to independent measurement results.

(b) Suppose we have a two qubit system in the state

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{3}$$

and Alice holds the first qubit and Bob holds the second. Alice then measures her qubit in the $\{|0\rangle, |1\rangle\}$ basis.

i. What are the possible outcomes, probabilities and post-measurement states for Alice's measurement?

Outcome	Probability	Post-measurement state
0		
1		

ii. If Alice received the outcome 0 and she knows Bob will measure in the $\{|0\rangle, |1\rangle\}$ basis, can she predict the outcome of his measurement? What if he measures in the $\{|+\rangle, |-\rangle\}$ basis instead?

iii. Prove that if Alice and Bob measure the state $|\psi\rangle$ in the same orthonormal basis $\{|v_0\rangle, |v_1\rangle\}$ then they will always get perfectly anti-correlated outcomes i.e.,

$$\mathbb{P}(a,b) = \begin{cases} 1/2 & \text{if } a \neq b \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

(c) Consider the orthonormal basis of entangled two-qubit states known as the Bell-basis

$$\begin{aligned} |\Phi_{00}\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ |\Phi_{01}\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ |\Phi_{10}\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ |\Phi_{11}\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned} \tag{5}$$

i. Suppose that you share $|\Phi_{00}\rangle$ with Bob but you only have access to the first qubit. By applying gates *only* to your qubit, how can you change the global state to each of the different Bell states? I.e., find U_{xy} such that

$$|\Phi_{xy}\rangle = (U_{xy} \otimes I)\,|\Phi_{00}\rangle \tag{6}$$

for $x, y \in \{0,1\}$.

ii. Suppose you have the first qubit of the two-qubit state

$$(U \otimes I)\,|\Phi_{00}\rangle \tag{7}$$

where U is *any* qubit gate. Show that no matter what orthonormal basis you choose to measure your qubit in, $\{|v_0\rangle, |v_1\rangle\}$, you will *always* have

$$\mathbb{P}(0) = 1/2 = \mathbb{P}(1)\,. \tag{8}$$

This means that any *local* information about these two-qubit entangled states is always uniformly random. In a sense, all of the meaningful information about these two-qubit entangled states must come from both qubits.

(d) **Optimal winning probability for the CHSH game (Difficult)**

[PB: Do not attempt before looking at exercise 6 in the practical section]

Alice and Bob play the CHSH game. For convenience we label the inputs as $x, y \in \{0,1\}$ and the outputs as $a, b \in \{+1, -1\}$. The winning condition then becomes $(-1)^{xy} = ab$. Let $|\psi\rangle$ be the quantum state shared by Alice and Bob. Let Alice's projective measurement on input x be $\{A_{+1|x}, A_{-1|x}\}$ and let Bob's projective measurement on input y be $\{B_{+1|y}, B_{-1|y}\}$. Finally define the observables (expectation operators) $A_x = A_{+1|x} - A_{-1|x}$ and $B_y = B_{+1|y} - B_{-1|y}$.

i. Show that for any fixed (x, y) the expected value of the product ab is given by

$$\langle\psi|\, A_x \otimes B_y \,|\psi\rangle\,.$$

ii. Let $K = A_0 \otimes B_0 + A_0 \otimes B_1 + A_1 \otimes B_0 - A_1 \otimes B_1$. Show that the expected winning probability is

$$\frac{1}{2} + \frac{1}{8}\langle\psi|\, K \,|\psi\rangle\,.$$

iii. Show that

$$K^2 = 4I - [A_0, A_1] \otimes [B_0, B_1]$$

where $[X, Y] = XY - YX$.

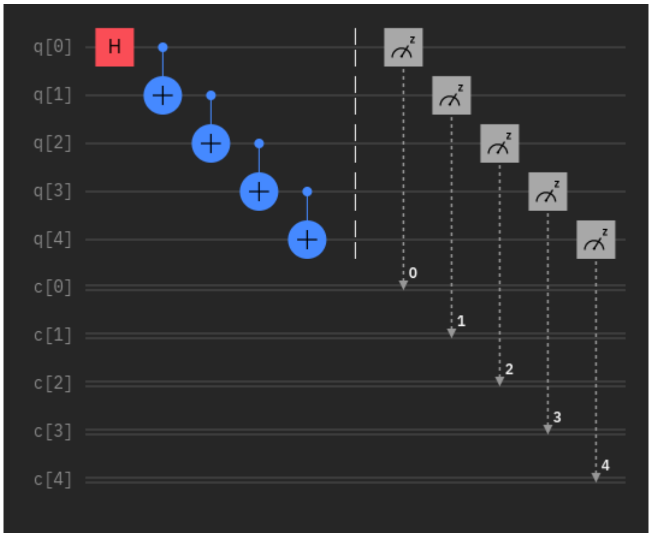
iv. Show that $\langle\psi| K |\psi\rangle \leq 2\sqrt{2}$. What does this say about the maximum winning probability for the CHSH game? (Hint: begin with the Cauchy-Schwarz inequality to bound $\langle\psi| K |\psi\rangle$ in terms of $\langle\psi| K^2 |\psi\rangle$).

2 Practical exercises

You should hopefully now be getting a bit familiar with running quantum circuits on the IBM platform (either via QISKIT or the composer). Let's dive into some exercises about quantum states and entanglement and its usage.

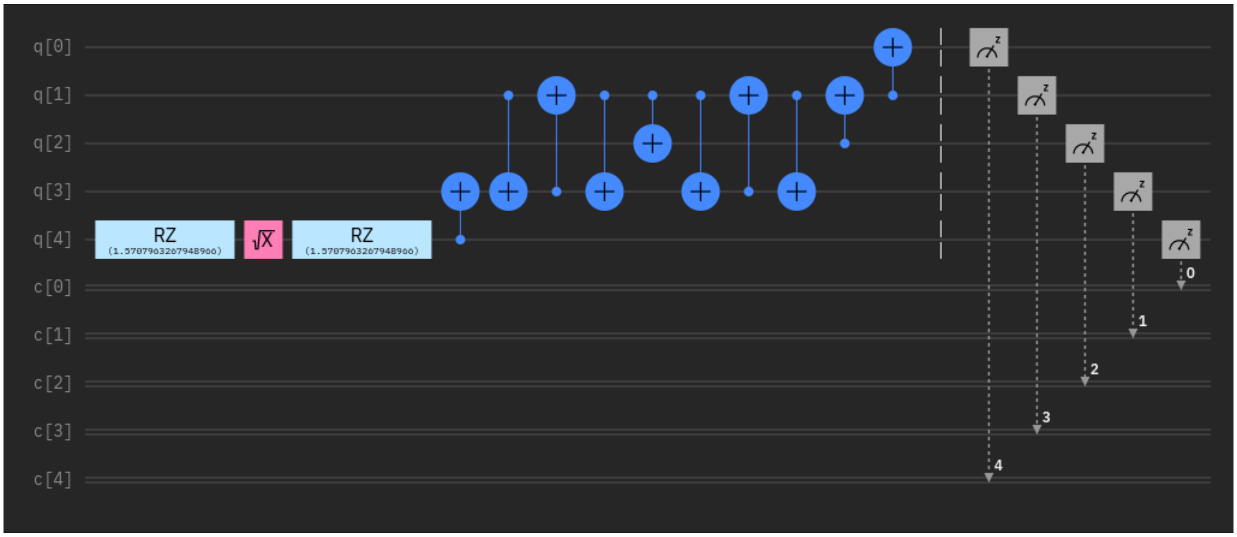
1. **Efficient entanglement generation**

You may or may not have noticed but the circuit you design may not be the circuit that the quantum computer actually implements. (**Question**: Can you think about why this might be?) For example, I designed the following circuit on the composer



which is meant to generate a 5 qubit entangled state $(|00000\rangle + |11111\rangle)/\sqrt{2}$ and then measure it in the computational basis. (**Question**: what outcomes do we expect to get from the measurement and with what probabilities?).

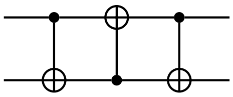
I sent the above circuit to be ran on the IBM QUITO machine. Before running the circuit, the IBM platform transformed my circuit into



as you can see this is quite a lot more complicated than the original circuit that I sent. In particular, the number of CNOT gates has grown significantly.

(a) Why did IBM transform my circuit into the second circuit before running the program?

(b) Interpret how the second circuit is performing the same task as the first. Hint: what is


(9)

doing?

(c) Can you find a circuit that does the same preparation and measurement as the first circuit but transpiles into fewer CNOT gates? (What's the optimal?)

(d) What is the best way to create the 5 qubit entangled state $(|00000\rangle+|11111\rangle)/\sqrt{2}$ and measure it on the QUITO machine? Here "best" refers to the circuit that produces the most accurate statistics. That is, we end up with a 5 bit distribution which should have $\mathbb{P}(00000) = \mathbb{P}(11111) = 1/2$. Let $\mathbb{Q}(x_0x_1x_2x_3x_4)$ be the 5 bit distribution coming from the statistics of the quantum computer. We can measure the error by the total variation

$$\Delta(\mathbb{P},\mathbb{Q}) = \sum_{x_1x_2x_3x_4x_5} |\mathbb{P}(x_1x_2x_3x_4x_5) - \mathbb{Q}(x_1x_2x_3x_4x_5)| \,. \tag{10}$$

Can you design a circuit that produces a smaller $\Delta(\mathbb{P},\mathbb{Q})$ than the second circuit? Does the circuit you found in part (c) do better? What about the other machines?

2. **Learning unknown quantum states**

If you receive a single unknown qubit

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\phi}\,|1\rangle \qquad \theta\in[0,\pi], \quad \phi\in[0,2\pi). \tag{11}$$

(i.e., you don't know the values of θ and ϕ) then it is impossible to tell what state you received. You can measure it but your measurement will almost certainly disturb the state and so you can only collect a single shot of statistics (not so useful).

Instead suppose you receive *many* copies of $|\psi\rangle$, this means you can collect lots of statistics by measuring each one individually (potentially in different bases).

(a) Given many copies of $|\psi\rangle$ can you develop a way to approximate the values of θ and ϕ?

(b) What’s the most efficient way you can find to do this, in terms of the number of different bases you need to measure in?

(c) Implement your protocol on the quantum computers of IBM. Have a friend write a state preparation circuit for you to prepare a state of the form (11). Try to work out (approximate) the θ and ϕ that they chose for you. (Remember to collect enough statistics by increasing the shots and you will probably need to use different circuits to perform different measurements[1]). Are you able to get good approximations?

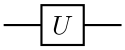
Hint: To create a custom quantum state you could the following function

```
    from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
    from math import cos, sin, pi
    from cmath import exp

    qr = QuantumRegister(1, name=”q”)          # Initialize 1 qubit
    out = ClassicalRegister(1, name='out')
    qc = QuantumCircuit(qr, out)

    def initialize_unknown_state(qc):
      # IF TESTING DON’T CHEAT AND LOOK HERE
      theta, phi = pi/4, pi/8
      state = [cos(theta/2), sin(theta/2) * exp(1j * phi)]
      qc.initialize(state, 0)

    initialize_unknown_state(qc)

```

Unfortunately, if you try to print the circuit after you’ve initialized the custom state then it will display the coefficients of the initialized state (I couldn’t find a way to change the label. . .). You can try to avoid this by designing the circuit first without the initialized state and only when you are running the protocol add the unknown state and don’t print.

3. **Learning unknown quantum gates**

In a similar spirit to the last task, imagine you have access to a qubit gate U



(12)

can you design a scheme to learn what the quantum gate is? Like in the previous question try to have a friend prepare a quantum gate for you and use it in your detection circuit to try to learn what gate they prepared.

To add your mystery gate to your circuit you can build a function like in the following code snippet that uses the general form of qubit gates (see (1)). So you will only need to guess the values (θ, ϕ, λ).

```
    from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
    from math import cos, sin, pi
    from cmath import exp

    qr = QuantumRegister(1, name=”q”)          # Initialize 1 qubit
    out = ClassicalRegister(1, name='out')
    qc = QuantumCircuit(qr, out)

    def add_mystery_gate(qc):
      # IF TESTING DON’T CHEAT AND LOOK HERE
      theta, phi, lam = 0, 0, 0
      qc.u(theta, phi, lam, 0)

    add_mystery_gate(qc)
```

[1] Although not necessarily, can you find a way to do random choices of different measurements in a single quantum circuit?

Like with the previous question, if you draw the circuit after you add the mystery gate then you'll see the parameters. To avoid this you can design your testing circuit with a known gate and only add the mystery gate once you are trying to run your protocol.

4. **Learning unknown measurements**

   What about the same problem as the previous two but the measurement basis is now fixed? Can you determine what the basis is by sending different states to be measured?

5. **Superdense coding**

   There's a result in quantum information theory that states that a single qubit can carry only one bit of information.[2] However, as this exercise will show, using entanglement Alice can send Bob two bits of information whilst sending only a single qubit.

   Suppose Alice and Bob share the two-qubit state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, Alice has qubit 1 and Bob has qubit 2.

   (a) Now Alice generates a 2 bit message $(a, b) \in \{0, 1\}^2$ that she wants to send to Bob. If $a = 1$ she applys X to her qubit and if $b = 1$ she then also applies Z. What are the 4 two qubit states that she could prepare?

   (b) Suppose that Alice then sends her qubit to Bob, i.e., he has access to both qubits. Design a circuit using Hadamard, CNOT and measurement that allows Bob to determine with probability 1 which state he received.

   (c) Now suppose that during the transmission of the qubit from Alice to Bob, an adversary Eve intercepts the qubit. Is it possible for Eve to gain any information about the message Alice was trying to send?

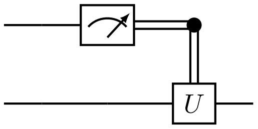
   (d) Try implementing the superdense coding scheme on the IBM machines and check that you can really use pre-shared entanglement to send additional (secret) information.

   (e) (Exploratory) Can you think of any ways to extend this protocol so Alice can send more information?

6. **Teleportation (More difficult)**

   The jupyter notebook Teleportation details how to simulate the teleportation protocol in qiskit.

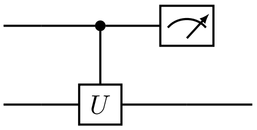
   (a) Unfortunately, the IBM machines cannot do everything that we'd expect a full quantum computer to perform. At the moment this means that conditioning a gate on a classical outcome is not possible. I.e., the circuit



(13)

   cannot be perform on the IBM machines because it relies on applying the unitary U conditioned on the outcome of a measurement of another qubit.

   Nevertheless, we can apply a quantum trick known as the *principle of deferred measurement* which states that we can always do the controlled gate before measuring



(14)

[2] This is called Holevo's theorem.

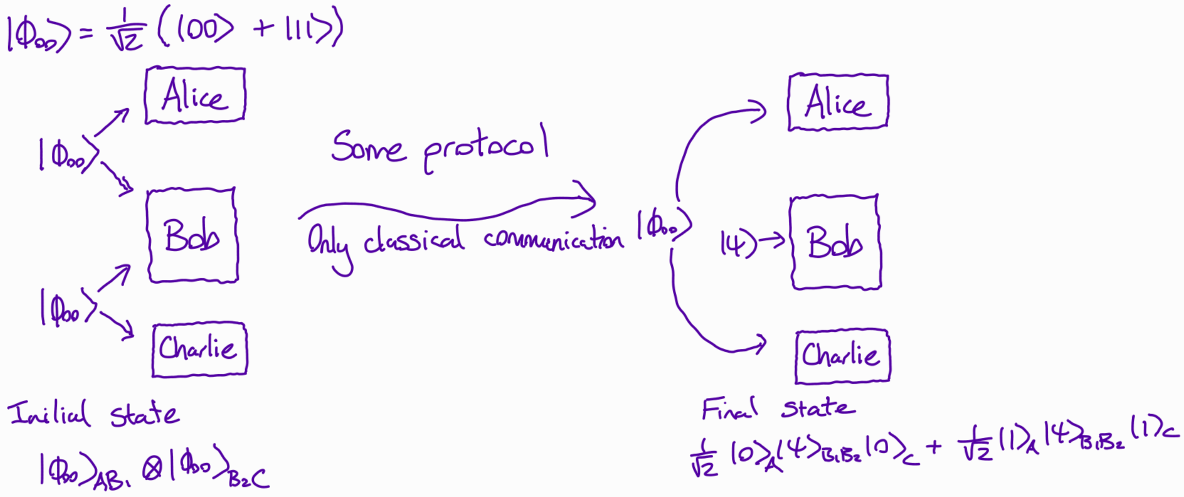

$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
Alice
$|\Phi_{00}\rangle$
Bob
$|\Phi_{00}\rangle$
Charlie
Some protocol
Only classical communication
$|\Phi_{00}\rangle$
Alice
$|\psi\rangle$
Bob
Charlie
Initial state
$|\Phi_{00}\rangle_{AB_1} \otimes |\Phi_{00}\rangle_{B_2C}$
Final state
$\frac{1}{\sqrt{2}}|0\rangle_A|\psi\rangle_{B_1B_2}|0\rangle_C + \frac{1}{\sqrt{2}}|1\rangle_A|\psi\rangle_{B_1B_2}|1\rangle_C$

Figure 1: The entanglement teleportation scenario. There are 3 parties, Alice, Bob and Charlie. Alice has one qubit A, Bob has 2 qubits B_1B_2 and Charlie has 1 qubit C. Initially, Alice and Bob have shared the entangled state $|\Phi_{00}\rangle_{AB_1}$ and Bob and Charlie have shared the entangled state $|\Phi_{00}\rangle_{B_2C}$. So Bob has two qubits, one entangled with Alice's qubit and the other entangled with Charlie's qubit. Alice, Bob and Charlie are far apart and cannot send their states to each other, but they can communicate classically, e.g., send measurement outcomes. (These are the same restrictions as in the standard teleportation protocol.) In entanglement teleportation, we want to design and execute a protocol that allows Alice and Charlie end up with entangled qubits despite having potentially never interacted before.

i. Show that for any two-qubit input state $|\psi\rangle$, the two circuits (13) and (14) act in the same way, i.e., the state at the end is the same for both circuits.

ii. Using the above principle, modify the teleportation protocol implementation in order to run it on one of the IBM quantum machines. Run the resulting circuit and check that teleportation really works in practice!

iii. Do you think that using the principle of deferred measurement leads to a realistic implementation of the teleportation protocol? What are your thoughts?

(b) (More difficult) We've already seen how if Alice shares entanglement with Bob, she can teleport an unknown quantum state to him by using the entanglement resource they share. Now consider the following scenario depicted in Fig. 1 which we call the entanglement teleportation scenario. There are 3 parties, Alice, Bob and Charlie. Alice has one qubit A, Bob has 2 qubits B_1B_2 and Charlie has 1 qubit C. Initially, Alice and Bob have shared the entangled state $|\Phi_{00}\rangle_{AB_1}$ and Bob and Charlie have shared the entangled state $|\Phi_{00}\rangle_{B_2C}$. So Bob has two qubits, one entangled with Alice's qubit and the other entangled with Charlie's qubit. Alice, Bob and Charlie are far apart and cannot send their states to each other, but they can communicate classically, e.g., measurement outcomes. (These are the same restrictions as in the standard teleportation protocol.) In entanglement teleportation, we want to execute a protocol so that Alice and Charlie end up with entangled qubits despite having potentially never interacted before.

Can you design such a protocol to achieve this task? Implement and simulate it to see if it works? Can you run it on the IBM machines?

Hint: Think along the lines of the teleportation protocol!

7. **Quantum nonlocality**

The famous thought-experiment of Einstein, Podolsky and Rosen concerned itself with the statistical correlations coming from the entangled state (3). In particular, they were concerned that if Alice and Bob each have one of the qubits in the state

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{15}$$

then if they both perform the measurement $\{|v_0\rangle, |v_1\rangle\}$ they will get perfectly anticorrelated outcomes $\mathbb{P}(0,1) = \mathbb{P}(1,0) = 1/2$. This means that as soon as Alice has the result of her measurement she immediately knows what outcome Bob's measurement will read, even if they are spacelike separated.

EPR thought that because this can occur when Alice and Bob are spacelike separated, the outcome of Alice's measurement cannot be influencing Bob's system (because no signal should travel faster than light). They therefore concluded that somehow it must be that the outcome of the measurement is determined beforehand in the past. Effectively, they wanted the statistics of the experiment to be described by a *local hidden variable model*

$$\mathbb{P}(A = a, B = b) = \sum_{\lambda} \mathbb{P}(\lambda)\mathbb{P}(A = a|\lambda)\mathbb{P}(B = b|\lambda) \tag{16}$$

i.e., there's some hidden randomness λ (shared information in the past) that is responsible for the correlations observed.

It's simple to come up with a hidden variable model for the $\{|v_0\rangle, |v_1\rangle\}$ measurement. Let $\mathbb{P}(\lambda) = 1/2$ for $\lambda \in \{0,1\}$, then let

$$\mathbb{P}(A = a|\lambda) = \begin{cases} 1 & \text{if } (a, \lambda) = (0,0) \\ 1 & \text{if } (a, \lambda) = (1,1) \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

$$\mathbb{P}(B = b|\lambda) = \begin{cases} 1 & \text{if } (b, \lambda) = (1,0) \\ 1 & \text{if } (b, \lambda) = (0,1) \\ 0 & \text{otherwise} \end{cases} \tag{18}$$

this gives a local hidden variable model for the statistics observed by Alice and Bob. (Flip a coin, if heads give Alice 0 and Bob 1, if tails give Alice 1 and Bob 0.)

EPR thought that quantum theory was an incomplete theory and that there should be some hidden variable model that better describes reality. We'll now show that local hidden variable models actually *cannot* explain all statistics coming from quantum theory and hence quantum theory cannot be explained by local hidden variables!

The CHSH game

Suppose Alice and Bob are separated so that they cannot communicate. Alice and Bob will each receive an input $x, y \in \{0,1\}$ and they are tasked with producing an output $a, b \in \{0,1\}$. They *win* the game if

$$a \oplus b = xy\,. \tag{19}$$

Suppose $\mathbb{P}(a, b|x, y)$ is the conditional distribution with which they produce their outputs given their inputs, then the probability they win the game (if the inputs are chosen uniformly) is given by

$$p_{\text{win}} = \sum_{a \oplus b = xy} \frac{1}{4} p(a, b|x, y)\,. \tag{20}$$

(a) The best winning probability for local hidden variable models is given by $p_{\text{win}} = 3/4$. Suppose Alice and Bob share the state $|\Phi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$, on input x Alice measures $\{|v_0^x\rangle, |v_1^x\rangle\}$ and on input y Bob measures $\{|w_0^y\rangle, |w_1^y\rangle\}$, i.e.,

$$\mathbb{P}(a, b|x, y) = \langle \Phi_{00}| \left(|v_a^x\rangle\langle v_a^x| \otimes |w_b^y\rangle\langle w_b^y|\right) |\Phi_{00}\rangle\ . \tag{21}$$

Can you choose a set of measurements so that Alice and Bob win with probability $p_{\text{win}} > 3/4$?

(b) Can you find measurements that achieve the optimal quantum winning probability of $\cos(\pi/8)^2 \approx 0.853$?

(c) Design a program to play the CHSH game on one of the IBM quantum computers. What's the best winning probability you can achieve on the IBM machines? Can you rule out a local hidden variable model by winning more than 3/4 of the time? Is it possible to incorporate the random question choices into the circuit?

Congratulations, if you managed to win the game with more than 3/4 probability then you've pretty much generated some provably secure randomness! Nonlocal correlations (under the assumptions of no communication between Alice and Bob) are only possible with entangled quantum systems and so by achieving such a score you "proved" that the system was using entanglement. Moreover, such correlations can be shown to be random, so you also "proved" randomness solely from the statistics! Something that is completely impossible without quantum theory.

8. **Further exploration**

   There are many more situations in which entanglement can be used to gain some advantage so feel free to explore other areas if you wish. There are various extensions of the things seen here and also new things.