INTRO TO QUANTUM COMPUTING

GLENN SUN
OLGA RADKO MATH CIRCLE ADVANCED 3

xx xx, 2021

Today we will study quantum computation through a simple example known as the CHSH game. To help you pace yourself to reach the punchline of this worksheet, hints are provided at the back of this worksheet for the trickier problems. Definitely feel free to use these hints if you are stuck because many of these problems are quite difficult. On the other hand, a bunch of extra problems are located at the end if you find this worksheet too easy.

1 The CHSH game

The CHSH game, first introduced in 1969 by the physicists Clauser, Horne, Shimony, and Holt, is a simple game that shows how quantum mechanics can be used to obtain advantages that are just not possible in the classical world.

Definition 1 (CHSH game)**.** Alice and Bob play the following game:

1. A referee chooses $x, y \in \{0, 1\}$ uniformly at random.
2. The referee gives Alice x and Bob y.
3. Alice responds with $a \in \{0, 1\}$ and Bob responds with $b \in \{0, 1\}$.

Alice and Bob win if $a \oplus b = x \wedge y$, where $\oplus$ means exclusive or and $\wedge$ means and. That is, if $x = y = 1$, then Alice and Bob must give different outputs, and in all other cases Alice and Bob must give the same output.

Problem 1. Play the CHSH game a few times. Find a good strategy.

Note that any deterministic strategy for Alice and Bob can be regarded as a pair of functions $A, B : \{0, 1\} \to \{0, 1\}$, meaning that they each output 0 or 1 depending on whether they get 0 or 1 as input.

Problem 2. In the previous problem, you should have come up with a strategy that succeeds with probability 75%. Prove that this is optimal for deterministic strategies, meaning that every pair of strategies A and B succeeds with probability at most 75%.

Although Alice and Bob can only succeed with probability 75% in the classical world, you will see today that the power of quantum mechanics allows them to do better! This game has in fact been experimentally verified, and gives strong evidence for the correctness of quantum mechanics.

2 Quantum states

Hopefully, you are already familiar with the idea of vectors from physics or precalculus. If not, a vector (for us) is a just a list of numbers. Vectors of the same length can be added componentwise, and any vector can be scaled by any regular number. For example,

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) \quad \text{and} \quad c(a_1, a_2) = (ca_1, ca_2).$$

In quantum computing, there are two vectors that are very important, and we will give them a special notation. Define

$$|0\rangle = (1, 0) \quad \text{and} \quad |1\rangle = (0, 1).$$

These vectors, as well as their products with each other as we will soon define, are known as *pure states.* The $|\cdot\rangle$ notation is sometimes called *ket notation.*

Definition 2 (tensor product of vectors)**.** Let $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_m)$ be vectors. The tensor product of a and b is the vector $a \otimes b$ of length nm, defined as

$$a \otimes b = (a_1 b, \dots, a_n b).$$

When we take the product of vectors in ket notation, we usually drop the $\rangle \otimes |$ in the middle, i.e. $|0\rangle \otimes |0\rangle$ is denoted $|00\rangle$.

Problem 3. Compute $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Explain why it's equivalent to write a vector (a_1, a_2, a_3, a_4) as $a_1|00\rangle + a_2|01\rangle + a_3|10\rangle + a_4|11\rangle$. State the analogous result for longer vectors (of length 2^n).

Problem 4. Verify that kets naturally distribute, i.e.

$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle.$$

This property makes it easy remember how to compute tensor product, so from now on we always prefer to write (a_1, a_2) as $a_1|0\rangle + a_2|1\rangle$, and likewise for longer vectors.

Definition 3 (state and measurement)**.** A quantum system on n qubits has a vector $x = x_1|0\dots0\rangle + \cdots + x_{2^n}|1\dots1\rangle$ such that $|x_1|^2 + \cdots + |x_{2^n}|^2 = 1$, called the *state vector.* Associated with the state vector is a probability distribution over the pure states $|0\dots0\rangle, \dots, |1\dots1\rangle$, where the i^{th} pure state occurs with probability $|x_i|^2$. By *measuring* the system, we mean sampling a pure state from this probability distribution.

Mathematically, the number of qubits in a system is defined as just the base-2 logarithm of the length of the state vector. For now, treat the definition as purely mathematical, and we will shortly discuss its physical meaning.

Problem 5. Check your understanding of the previous definition. In particular:

1. Recall that we said vectors like $|0\rangle$ and $|10\rangle$ are known as pure states. Why is every pure state a quantum state?
2. How many qubits are in the quantum state $|00\rangle$? What about $|0000\rangle$?
3. Check that the tensor product of two states is a state. If the two original states have n and m qubits, how many qubits are in the product?
4. Find the unique positive value $c \in \mathbb{R}$ that makes $c(|00\rangle + |11\rangle)$ into a valid quantum state. What about $c(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$? What about $\frac{1}{2}|0\rangle + c|1\rangle$? When measuring these states, what are the resulting probability distributions?

Now let's discuss the physical interpretation of this definition. Our universe has real qubits, and a common example is an electron where the pure states $|0\rangle$ and $|1\rangle$ correspond to whether it is spin up and spin down. A 1-qubit state is a combination $x_1|0\rangle + x_2|1\rangle$ of these pure states, sometimes called a *superposition* in physics. But when we actually observe the electron, i.e. measure it, quantum mechanics tells us that we will see it either as spin up with probability $|x_1|^2$ or spin down with probability $|x_2|^2$. Then naturally, a 2-qubit system can then be obtained with 2 electrons, and the 4 combinations of possible spins correspond to the 4 pure states on 2 qubits.

Problem 6. Explain how the tensor product of quantum states should be physically interpreted.

Here is one interesting idea: recall that we can take the tensor product of quantum states to form new states. But can we do the opposite, i.e. factor quantum states into states on fewer qubits?

Definition 4 (entanglement)**.** A quantum system on $n \geq 2$ qubits is called entangled if its state cannot be written as the tensor product of states on fewer qubits.

Problem 7. Show that the state $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ is not entangled, but that $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled. Based on your answer to the previous problem, physically interpret entanglement.

The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is called an *EPR pair* after the physicists Einstein, Podolsky, and Rosen. The EPR pair will play a crucial role in our solution to the CHSH game.

A natural question is whether or not it physically possible to construct entangled states, since such states cannot come from just considering two electrons as one system. The answer is yes, but this involves some physics and is beyond the scope of this worksheet. We will take for granted that physically constructing an EPR pair is indeed possible. (If you're interested in exploring the construction a little further, see Extra Problem 4.)

Problem 8. Here is a taste of our CHSH game solution. Suppose Alice and Bob have an EPR pair, i.e. they each carry one qubit and the state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice measures just her own qubit and announces: "Oh! I now know what Bob will see when he measures his qubit." How does Alice know? Would this be possible with a non-entangled pair?

3 Quantum gates

The power of quantum systems happens when we modify quantum states. By the laws of quantum mechanics, it turns out that these modifications are limited to a very particular type of modification known as a quantum gate.

Definition 5 (quantum gate)**.** A quantum gate on n qubits is a function f that takes as input vectors with 2^n components and outputs vectors with 2^n components satisfying:

- For all vectors a, b and all regular numbers c, we have

  $$f(a+b) = f(a) + f(b) \quad \text{and} \quad f(ca) = cf(a).$$

  This requirement is called "f is linear."

- If x is a valid quantum state on n qubits, then $f(x)$ is a quantum state. In other words, if $|x_1|^2 + \cdots + |x_{2^n}|^2 = 1$, then $|f(x)_1|^2 + \cdots + |f(x)_{2^n}|^2 = 1$. This requirement is called "f is unitary."

Problem 9. Check your understanding of the previous definition. In particular:

1. Explain why the identity function $f(x) = x$ is a quantum gate.
2. Is the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 2x + 1$ linear? Can you describe all the linear functions $f : \mathbb{R} \to \mathbb{R}$ (no proofs needed)?
3. Give an example of a linear function that is not unitary.
4. Recall that the composition of two functions f and g is denoted $f \circ g$, and defined as $(f \circ g)(x) = f(g(x))$ (i.e. apply g then apply f). Check that if f and g are quantum gates, then $f \circ g$ is a quantum gate.

Obviously, we want gates to be unitary. Intuitively, the linear requirement just means that instead of changing a complicated state all at once, we can break it up and change some simpler parts, then put it back together. Although it might not be clear yet why this is necessary, you will soon see why it is super helpful. The study of linear functions is an extremely fundamental area of math called *linear algebra*, which will be touched on in Extra Problem 3. Futhermore, in 1991 it was shown that nonlinear quantum mechanics implies P = NP (which, if you recall, is strongly believed to be false).

Problem 10. The function R_θ, known as the rotation function by angle θ, is defined by

$$R_\theta(a_1|0\rangle + a_2|1\rangle) = (a_1\cos(\theta) - a_2\sin(\theta))|0\rangle + (a_1\sin(\theta) + a_2\cos(\theta))|1\rangle.$$

1. Show that R_θ is a quantum gate on 1 qubit.
2. Explain geometrically why R_θ rotates a vector $(a_1, a_2) = a_1|0\rangle + a_2|1\rangle$ counterclockwise around the origin by θ.

Recall that qubits are physical objects that we can manipulate independently, regardless of whether they are entangled or not. Hence, at least physically, it is possible to take a n qubit system and apply a quantum gate to only some of the qubits, or apply different gates to different qubits at the same time. Mathematically, just like grouping independent qubits into one system is tensor product of vectors, putting together these independent transformations can be understood as the tensor product of gates.

Definition 6 (tensor product of gates)**.** Let f be a quantum gate on n qubits and g be a quantum gate on m qubits. Then the tensor product of f and g, denoted $f \otimes g$, is the unique quantum gate on $n+m$ qubits such that

$$(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$$

for all quantum states a and b appropriately sized.

That is, $f \otimes g$ is the unique gate whose action on states a and b put together is the same as the independently applying f to a and g to b. The fact that such a quantum gate mathematically exists and is unique is the content of Extra Problem 3, so for now we will just assume this.

Problem 11. Let f and g be quantum gates on 1 qubit. Expand

$$(f \otimes g)\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$$

as much as possible. Interpret what you are doing physically.

4 Solution to the CHSH game

We are finally ready to give our solution to the CHSH game! Are you excited? Consider the following:

1. Alice and Bob form the entangled EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and separate, taking one qubit with them each.
2. If Alice receives $x = 1$, then she applies $R_{\pi/8}$ to her qubit, otherwise she does nothing. Then she waits a minute, measures her own qubit, and outputs the resulting pure state (that is, $a = 0$ if $|0\rangle$ and $a = 1$ if $|1\rangle$).

3. If Bob receives $y = 1$, then he applies $R_{-\pi/8}$ to his qubit, otherwise he does nothing. Then he waits a minute, measures his own qubit, and outputs the resulting pure state (that is, $b = 0$ if $|0\rangle$ and $b = 1$ if $|1\rangle$).

Intuitively, Alice and Bob's qubits start identical by Problem 8. Then if $x = y = 1$, Alice and Bob rotate their qubits to be quite far from each other, and otherwise they remain quite close, which is exactly what is necessary.

Problem 12. Prove that Alice and Bob achieve about 80% success probability with the above strategy. In particular, prove that:

1. If $x = y = 0$, then they win with probability 100%.
2. If $x = 1$ and $y = 0$ or vice versa, then they win with probability $\cos^2(\pi/8) \approx 85\%$.
3. If $x = y = 1$, then they win with probability 50%.
4. Conclude that Alice and Bob win with probability about 80% overall.

Congratulations! You've reached the end of this worksheet. If you're interested, take a look at the extra problems on the next page.

5 Takeaways

There are a couple of really cool that we hope you take away from this worksheet.

1. **Quantum computing is not overly complicated.** If you've heard about quantum mechanics through popular science, you might have gained some qualitative ideas about the subject, but the equations and mathematics were probably omitted for being "too hard." But it's really quite doable — you did it!

2. **Physical systems can be modelled with rigorous mathematics.** Although we studied something strongly rooted in the physical reality, notice that all of our definitions were abstract and all of our results followed from rigorous proof. It's a happy coincidence that physical objects like electrons can be used to make real qubits, and the process of doing so is physics or engineering, but the study of what you can do with qubits is purely mathematics.

3. **Quantum mechanics allows us to do things that we classically cannot.** This last takeaway is quite obvious now, but it's worth mentioning that quantum mechanics is not just some theory for describing the universe — it can be used actually do things. If you end up taking a course about quantum computing in college, you might see some really cool results like how to break encryption with quantum computing, but these results requires some more background knowledge like linear algebra to understand.

If you are interested to learn more about this topic, a good modern resource is the Qiskit textbook. Qiskit is a Python library for simulating quantum algorithms, though the online textbook is a general introduction to quantum computing, not just their library. Here it is: https://qiskit.org/textbook/preface.html

6 Extra Problems

1. A randomized strategy is a strategy where Alice and Bob may flip coins and make random decisions based on the inputs they get. Randomization is something that is possible in the classical world that we did not consider in Problem 2. For example, when Alice receives $x = 0$, she could output 0 with probability 60% and 1 with probability 40%, and output with different probabilities when she receives $x = 1$. Prove that randomization does not help Alice and Bob, i.e. any randomized strategy also succeeds with probability at most 75%.

2. Although certain features of quantum entanglement are unique to quantum mechanics, there is some sense in which you can "entangle" classical particles as well. Describe a real-world classical system that has the same measurement effect as an EPR pair. That is, there are two coins, and they are always randomly discovered to be both heads or both tails with equal probability.

3. In this extra problem, we prove the existence and uniqueness of tensor product of gates. Unfortunately, it's more or less unavoidable to take a short detour into linear algebra. However, you also get to see how cool linear functions are!

   (a) Show that a linear function f on n qubits can be evaluated on any state just by knowing its action on the 2^n relevant pure states.

   (b) A matrix is a grid of numbers. Matrices can be multiplied by vectors to produce vectors as follows:

   $$\begin{bmatrix} f_{1,1} & f_{1,2} & \cdots & f_{1,2^n} \\ f_{2,1} & f_{2,2} & \cdots & f_{2,2^n} \\ \vdots & \vdots & \ddots & \vdots \\ f_{2^n,1} & f_{2^n,2} & \cdots & f_{2^n,2^n} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^n} \end{bmatrix} = \begin{bmatrix} f_{1,1}x_1 + f_{1,2}x_2 + \cdots + f_{2,2^n}x_{2^n} \\ f_{2,1}x_1 + f_{2,2}x_2 + \cdots + f_{1,2^n}x_{2^n} \\ \vdots \\ f_{2^n,1}x_1 + f_{2^n,2}x_2 + \cdots + f_{2^n,2^n}x_{2^n} \end{bmatrix}$$

   Show that for all linear functions f on n qubits, there exists a unique matrix $[f]$ such that $f(x) = [f]x$ for all x.

   (Hint: Determine what each column of the matrix $[f]$ must be in order to satisfy $f(x) = [f]x$ for pure states x. This proves uniqueness. Then show that the matrix you found actually works for all x, not just pure states. This proves existence.)

   (c) Show that for all quantum gates f and g, there exists a unique gate $f \otimes g$ such that $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$ for all a and b.

   (Hint: Translate $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$ into an equation about matrices and vectors. Determine what each column of the matrix $[f \otimes g]$ must be in order to satisfy that equation for pure state inputs, which can always factor into smaller pure states a and b. This proves uniqueness. Then show that the matrix you found actually works for all a and b, not just pure states. This proves existence. By the previous part, this gives a unique linear function that satisfies the desired equation. Finally, show that this is unitary.)

4. In this extra problem, we will investigate how to construct an EPR pair, assuming that quantum gates are constructible.

   (a) Show that the Hadamard gate, defined by

   $$H(x_1|0\rangle + x_2|1\rangle) = \frac{1}{\sqrt{2}}((x_1 + x_2)|0\rangle + (x_1 - x_2)|1\rangle)$$

   is a valid 1-qubit gate.

   (b) Show that the CNOT (controlled-not) gate, defined by

   $$C(x_1|00\rangle + x_2|01\rangle + x_3|10\rangle + x_4|11\rangle) = x_1|00\rangle + x_2|01\rangle + x_4|10\rangle + x_3|11\rangle$$

   is a valid 2-qubit gate. Explain why it is called the controlled not gate.

   (c) Use the Hadamard gate and the CNOT gate to create a gate that sends $|00\rangle$ to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Since $|00\rangle$ can be physically constructed by just looking at a bunch of electrons until we find two that are spin up, this gives a method to construct $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, supposing that gates are actually constructible.

5. Suppose Alice and Bob split an EPR pair and move to far away places without applying any gates. Recall that when Alice measures her qubit, she immediately knows that Bob's qubit collapsed to the same pure state. Doesn't this violate the fact that communication cannot happen faster than the speed of light? This question puzzled scientists for decades and even led Einstein to reject quantum mechanics entirely. However, it's not a paradox. Show that no matter what quantum gate Alice applies to her qubit, Bob's qubit collapses to $|0\rangle$ or $|1\rangle$ with probability 50% each. How does this resolve the paradox?

6. Let I denote the identity gate, i.e. $I(x) = x$. Show that for any gates f and g, we have

   $$f \otimes g = (f \otimes I) \circ (I \otimes g) = (I \otimes g) \circ (f \otimes I).$$

   Interpret this physically. We glossed over this fact when we presented Alice and Bob's solution to the CHSH game, but say why this fact is relevant.

7. Improve the strategy for the CHSH game to one that gives a 85% probability of success.

   (Hint: Try slightly different rotations.)

8. Prove that in the CHSH game, if Alice and Bob rotate their qubits depending on input they receive, then 85% is the optimal probability of success. (It turns out that this is the optimal success probability for all quantum algorithms, not just rotations, but that is much harder to prove.)

7 Hints

1. Aim for a strategy with a 75% chance of winning. Try a simple one.
2. There are only finitely many functions A and B, so you could just list all of them and bash the proof. There is an easier way though. Notice that for every input pair (x, y), either the strategy works or it doesn't. Hence, succeeding with probability more than 75% means that you succeed with probability 100%. From the assumption that Alice and Bob always succeed, you can write equations like $A(0) \oplus B(0) = 0$, meaning that Alice and Bob's strategies succeed when $x = y = 0$. From equations like this one, find a contradiction.
3. No hints.
4. Expand both sides.
5. No hints for parts 1 and 2. For part 3, you just need to check that the squared components of $a \otimes b$ sum to 1. Write the equation for this sum and factor it. For part 4, write that equation again and solve for c.
6. Start with physically interpreting tensor product of pure states. For example, recall that $|00\rangle = |0\rangle \otimes |0\rangle$. We know what $|0\rangle$ and $|00\rangle$ mean physically, so how does $\otimes$ connect them together? Now extend this interpretation to general systems and explain why the math of tensor products is compatible with this interpretation.
7. The only way to factor a 2 qubit state is into two 1 qubit states. So your factorizations have to look like $(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$. For the first one, find these coefficients. For the second one, assume for contradiction they exist, multiply out, and compare terms.
8. What are the possible pure states that the system can collapse to upon measurement?
9. No hints.
10. For part 1, you want to show that it is linear and unitary. To show linear, just expand out $R_\theta((a_1|0\rangle + a_2|1\rangle) + (b_1|0\rangle + b_2|1\rangle))$ and $R_\theta(c(a_1|0\rangle + a_2|1\rangle))$ (sorry, it's a little messy). For unitary, use the facts that $|a_1|^2 + |a_2|^2 = 1$ and $\sin^2(\theta) + \cos^2(\theta) = 1$. For part 2, focus on how R_θ acts on $|0\rangle = (1, 0)$ and $|1\rangle = (0, 1)$. Can you see how R_θ has to act on all other vectors now?
11. First apply linearity of $f \otimes g$.
12. For part 1, apply Problem 8. For parts 2 and 3, apply Problem 3 and simply the resulting expression until you can compute the probabilities of the 2-bit system collapsing into each pure state. For part 3, you will need the trig identity

$$\cos^2(\theta) - \sin^2(\theta) = 2\sin(\theta)\cos(\theta).$$