CSE 291 / Math 277A - Quantum Complexity Theory October 4, 2022

Lecture 4

Lecturer: Daniel Grier *Scribe: Aditya Giridharan*

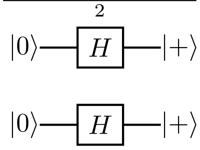
1 Warm Up

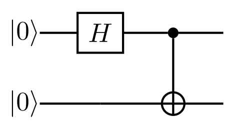
Question: What circuits constructed using CX, X, H (the Controlled NOT, NOT and Hadamard respectively) gates give the following?

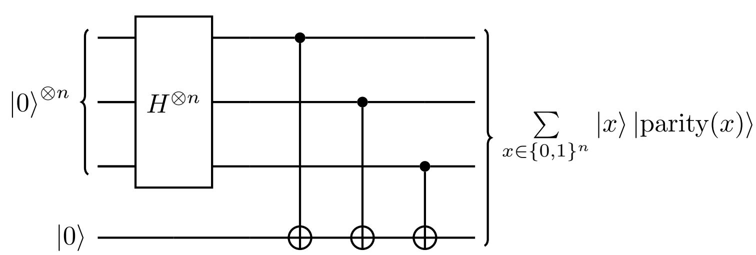
1. $\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$
2. $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
3. $\sum_{x\in\{0,1\}^n} |x\rangle\,|\text{parity}(x)\rangle$ where $\text{parity}(x) = \sum_i x_i \mod 2$
4. $\sum_{x\in\{0,1\}^n} (-1)^{\text{parity}(x)}\,|x\rangle$

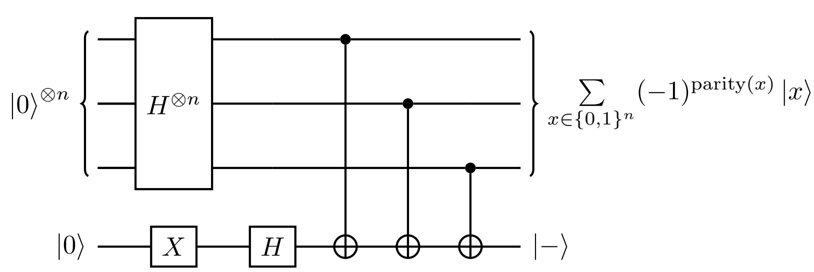
Solution

1. $\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$ can be factored as $|+\rangle\,|+\rangle$, giving us the following circuit —



2. 

3. 

4. 

For parts (3) and (4), we make use of an extra working qubit usually called an **ancillary** qubit.
An intuitive way to understand the solution for (4) is to look at the $|-\rangle$ state:

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Applying the X gate to this state gives us:

$$\begin{aligned} X\left|-\right\rangle &= \frac{-\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}} \\ &= -\left|-\right\rangle \\ &= (-1)^1\left|-\right\rangle \end{aligned}$$

And applying the X gate once more gives us:

$$\begin{aligned} X^2\left|-\right\rangle &= \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} \\ &= (-1)^2\left|-\right\rangle \end{aligned}$$

Clearly, applying the X gate n times to the $\left|-\right\rangle$ state results in a global phase of $(-1)^n$.
By this intuition, if we have the n-qubit state $x \in \{0,1\}^n$ and an ancillary qubit $y = \left|-\right\rangle$ and we apply a CX gate from each qubit in x to y, then each "occurrence" of 1 in x will introduce a phase factor of -1, leading to a final phase on $\left|x\right\rangle$ of $(-1)^{\mathrm{parity(x)}}$.

2 Nobel Prize in Physics (2022)

The 2022 Nobel Prize in Physics was awarded to Alain Aspect, John F. Clauser, and Anton Zeilinger, *"for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science"*.

2.1 Background

In 1935, Albert Einstein, Boris Podolsky, and Nathan Rosen laid out a thought experiment that seemed to show that quantum mechanics violated the Principle of Locality - the idea that an object is only directly influenced by its immediate surroundings. The gist of the thought experiment is as follows -

- Prepare an entangled state of 2 qubits, say $\left|\psi\right\rangle = \frac{\left|00\right\rangle + \left|11\right\rangle}{\sqrt{2}}$.
- Separate the qubits, giving qubit 1 to Alice and qubit 2 to Bob such that they are light-years apart
- If Alice now measures her qubit in the Z basis, then she sees $\left|0\right\rangle$ or $\left|1\right\rangle$ with probability $\frac{1}{2}$ each. However, once Alice has measured her qubit, the wavefunction of the system has collapsed. So, if Alice saw $\left|0\right\rangle$, then Bob's qubit is instantly known to be in the state $\left|0\right\rangle$, and if Alice saw $\left|1\right\rangle$, then Bob's qubit is also in the state $\left|1\right\rangle$
- In a way, the measurement of Alice's qubit has influenced the state of Bob's qubit despite their large separation.

Disturbed by this prospect, some physicists at the time believed that there must be *hidden variables* - inaccessible properties that were possessed by the particles which affected their measurement outcomes. Quantum mechanics was thought to be an incomplete theory.

In 1964, John Bell formulated the *Bell Inequalities*, which stated that if the hidden-variable theory were to be true, then there would be an upper bound on the amount of correlation that could be observed between the measurement outcomes of the two particles. Experiments however, have shown repeatedly that entangled particles are more correlated than the upper bound given by Bell's Inequalities, thereby supporting quantum mechanics over the hidden-variable theory.

2.2 CHSH Game

In 1969, Clauser, Horne, Shimony, and Holt derived the *CHSH inequality*, which provided an experimental means to support Bell's theorem. Similar to the Bell Inequalites, it imposes a constraint on the expected values of Bell test experiments. The CHSH game is a physically-realizable experiment based on the inequality that can be carried out to show that playing the game using a quantum strategy results in a higher chance of winning than playing the game using a classical strategy corresponding to local hidden-variable theories.

2.2.1 Setup

The CHSH game is set up as follows. Alice and Bob are 2 parties separated by a distance large enough to prohibit communication between them. An independent referee randomly chooses 2 challenge bits x and y - giving x to Alice and y to Bob respectively. Alice and Bob are then asked to send back bits a and b respectively. The game is won iff $a \oplus b = x \wedge y$. Alice and Bob are allowed to decide on a strategy in advance and they can even both have access to a shared random string.

2.2.2 Classical Strategy

The classical strategy that maximizes the winning probability is one in which Alice and Bob always send back $a = b = 0$ irrespective of x and y, giving them a 75% chance of winning (assuming that the referee chooses the bit x, y uniformly at random). Intuitively, since they share no information apart from the pre-decided strategy, and because $x \wedge y = 0$ with probability 0.75, they can do no better than always returning $a = b = 0$.

Formally, first assume Alice and Bob are using deterministic strategies—that is, Alice's and Bob's outputs are Boolean functions of their inputs: $f_A, f_B \colon \{0,1\} \to \{0,1\}$. If Alice and Bob are always passing the test, it means that all of the following equations must hold:

$$\begin{aligned}
0 = 0 \wedge 0 &= f_A(0) \oplus f_B(0) \\
0 = 0 \wedge 1 &= f_A(0) \oplus f_B(1) \\
0 = 1 \wedge 0 &= f_A(1) \oplus f_B(0) \\
1 = 1 \wedge 1 &= f_A(1) \oplus f_B(1)
\end{aligned}$$

Taking the sum of both sides, we get that $1 = 0$, so there is a contradiction. One of the equations must not have been satisfied, and if each questioned is asked with 25% probability, then Alice and Bob must fail with at least 25% probability.

If Alice and Bob have shared randomness, then their strategies look like a convex combination of deterministic strategies. However, since each deterministic strategy succeeds with probability at most 75%, then the entire randomized strategy succeeds with at most 75%.

2.2.3 Quantum Strategy

Assume that Alice and Bob share a Bell state $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. That is, they each have one qubit in the pair, which they share before they are asked any questions. For each question, they apply a specific unitary (specified below) and return the result of a computational basis measurement on their qubit to the referee:

- A's strategy:
  - If $x = 0$, Alice just measures.
  - If $x = 1$, Alice applies Hadamard, and then measures.
- B's strategy:
  - If $y = 0$, Bob applies the gate $R_Y(-\pi/8) := \begin{pmatrix} \cos\pi/8 & \sin\pi/8 \\ -\sin\pi/8 & \cos\pi/8 \end{pmatrix}$, and then measures.
  - If $y = 1$, Bob applies the gate $R_Y(\pi/8) := \begin{pmatrix} \cos\pi/8 & -\sin\pi/8 \\ \sin\pi/8 & \cos\pi/8 \end{pmatrix}$, and then measures.

Let's look at some specific inputs to see their winning probability:

- If $x = 0$ and $y = 0$: Therefore, $a \oplus b = 0 \wedge 0 = 0$. If Alice measures 0, then Bob's measurement is correct with probability $|\langle 0| R_Y(-\pi/8) |0\rangle|^2 = \cos(\pi/8)^2$. Similarly, if Alice measures 1, then Bob's measurement is correct with probability $|\langle 1| R_Y(-\pi/8) |1\rangle|^2 = \cos(\pi/8)^2$.

- If $x = 1$ and $y = 1$: Therefore, $a \oplus b = 1 \wedge 1 = 1$. To start, notice that the Bell state $|\psi\rangle$ can be written as $\frac{|++\rangle + |--\rangle}{\sqrt{2}}$. Therefore, when Alice applies Hadamard the state becomes $\frac{|0+\rangle + |1-\rangle}{\sqrt{2}}$. Suppose she measures a 0, then Bob's state is $R_Y(\pi/8) |+\rangle$ after Bob applies his unitary. The probability that he outputs a 1 (i.e., the correct answer) is therefore $|\langle 1| R_Y(\pi/8) |+\rangle|^2 = |\langle +| R_Y(-\pi/8) |1\rangle|^2$ since $R_Y(\pi/8)$ and $R_Y(-\pi/8)$ are conjugate transposes of each other. We have

  $$|\langle +| R_Y(-\pi/8) |1\rangle|^2 = \left| \frac{\langle 0| + \langle 1|}{\sqrt{2}} (\sin(\pi/8) |0\rangle + \cos(\pi/8) |1\rangle) \right|^2 = \left(\frac{\sin(\pi/8) + \cos(\pi/8)}{\sqrt{2}} \right)^2 = \cos(\pi/8)^2.$$

  To prove the last equality, one can factor out the $\cos(\pi/8)$ term and use that $\tan(\pi/8) = \sqrt{2} - 1$.

  Similarly, if Alice measures 1, then by the same logic as above, Bob measures the the correct answer with probability $\langle 0| R_Y(\pi/8) |-\rangle|^2 = \left(\frac{\sin(\pi/8) + \cos(\pi/8)}{\sqrt{2}} \right)^2 = \cos(\pi/8)^2$

Without going through every case, it can be shown that the winning probability for any input is $\cos^2(\frac{\pi}{8}) \approx 0.85$, which is greater than 0.75. Therefore, by winning the game with greater that 75% probability, Alice and Bob can demonstrate that they are performing operations that are fundamentally non-classical.

2.3 The Nobel Prize

John Clauser was awarded the Nobel Prize for formulating a practical experiment that disproved hidden variable theories by violating the Bell Inequality. Alain Aspect was crucial in closing important loopholes that remained after Clauser's initial experiment. Anton Zeilinger and his research group demonstrated the phenomenon of quantum teleportation using entangled states.

3 Properties of Measurement

1. **Global phase doesn't matter**: Measuring the state $\sum_{i \in \{0,1\}^n} \alpha_i |i\rangle$ gives us the same probability distribution over the states $|i\rangle$ as measuring the state $\sum_{i \in \{0,1\}^n} e^{i\theta} \alpha_i |i\rangle$, because $|e^{i\theta}\alpha_i|^2 = |e^{i\theta}|^2 |\alpha_i|^2 = |\alpha_i|^2$.

2. **Principle of Deferred Measurement**: Measurements can be delayed until the end of a quantum computation without affecting the probability distribution of the outcomes.
   One example of this is when a measurement is performed between two unitary gate applications. Consider the circuits in Figures 1 and 2. In Figure 1, the measurement of qubit B is performed before the application of unitary V, and in Figure 2, the measurement is first replaced by a CNOT gate from B, the measured bit, to A, the ancilla bit, and deferred until after V is applied. Assume that U maps $|0\rangle$ to $\alpha |0\rangle + \beta |1\rangle$.
   If we compute the state of the system at point P_1 in Figure 1, we get the density matrix $|\alpha|^2 |0\rangle \langle 0| + |\beta|^2 |1\rangle \langle 1|$.
   If we do the same at point P_2 in Figure 2, we get $|\alpha|^2 |00\rangle \langle 00| + |\beta|^2 |11\rangle \langle 11|$, from which if we trace out the ancillary qubit, we get exactly $|\alpha|^2 |0\rangle \langle 0| + |\beta|^2 |1\rangle \langle 1|$. Since the density matrices at points P_1 and P_2 are exactly the same, the 2 circuits are equivalent.

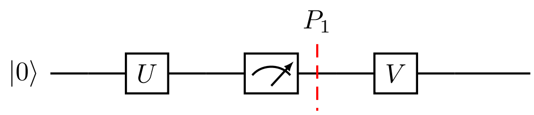


Figure 1: Circuit with intermediate measurement

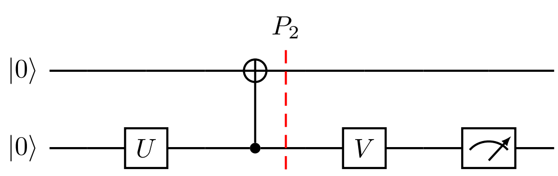


Figure 2: Circuit with deferred measurement