Computational Complexity December 6, 2018

Lecture 16 (Notes)

Lecturer: Ola Svensson *Scribes: Ola Svensson*

Disclaimer: These notes were written for the lecturer only and may contain inconsistent notation, typos, and they do not cite relevant works. They also contain extracts from the two main inspirations of this course:

1. The book *Computational Complexity: A Modern Approach* by Sanjeev Arora and Boaz Barak;
2. The course *http://theory.stanford.edu/ trevisan/cs254-14/index.html* by Luca Trevisan.

1 Introduction

Recall last lecture:

- Unpredictability implies secure pseudorandomness.
  - proof used interesting technique: *hybrid argument*.
- Start of the proof of one-way permutation implies pseudorandom generators.

Today:

- Finish the proof that one-way permutation implies pseudorandom generator (see notes for last lecture).
- Introduction to Quantum Computing
  - Two-slit experiment;
  - Qubits, superposition, unitary operations;
  - The EPR paradox.

2 Introduction to Quantum Computing

- Different model of computing.
- Challenges the strong Church-Turing thesis that all computations can be simulated by a Turing machine with polynomial slow down:
  - Currently, there exists problems (e.g. FACTORING) for which there is efficient quantum algorithms but no efficient classic algorithms.
  - So it is plausible that Quantum Computers could lead to exponential speed-up for important problems.
- Still outstanding open problem to build a quantum computer.

2.1 Quantum weirdness: the two-slit experiment

- Very little physics is required to understand the central results of quantum computing.
- However, let us look at a specific experiment to get some intuition behind the definitions.

In the *two-slit experiment* a photon source is placed between a wall with two slits and a detector array (see Figures 10.1 and 10.2 in the textbook). We measure the number of times each detector lights up during an hour. We have two cases

- *One slit is covered (and one is uncovered):* We expect that the detector that are directly behind the open slit will receive the largest number of hits; this is indeed the case.
- *Both slits are uncovered:* We would expect that the number of times each detector is hit is the sum of the number of times it is hit when the first slit is open and the number of times it is is hit when the second slit is open. In particular, uncovering both slits should only *increase* the number of times each location is hit.

  Surprisingly, this is *not* what happens. In particular, at several detectors the total hit rate is *lower* when both slits are open as compared to when a single slit is open. Photons do not behave as particles or "little balls!"

How can we explain that? According to quantum mechanics, a photon instantaneously explores all possible paths to the detectors through the all open slits. Some paths are taken with positive "amplitude" and some with negative "amplitude".

> "The only difference between a probabilistic classical world and the equations of the quantum world is that somehow or other it appears as if the probabilities would have to go negative." —Richard Feynman in "Simulating Physics with Computers," 1982.

Of course, one may be skeptical about this "path exploration". To check it we could put a detector behind both slits. If a photon is really going through both slits simultaneously, you hope to detect it at both slits. HOWEVER, when you try to make the photon reveal its quantum nature in this way, the interference pattern disappear and it behaves like "little balls!"

The "explanation" is that *observing* an object "collapses" its distribution of possibilities and so changes the result of the experiment.

2.2 Quantum superposition and qubits

Classical computing involves the manipulation of bits. The analogous unit of storage in quantum computing is *qubit.*

- We can think of a qubit as an elementary particle that can be in two different states, which we denote by zero and one (exactly like a bit so far).
- However, unlike a classical bit, this particle can be simultaneously in both basic states.
- Thus, the state of a qubit at any time is called a *superposition* of these basic states.

Formally, we denote the basic states by $|0\rangle$ and $|1\rangle$ (sorry for the notation but it is there because of a long tradition) and a qubit can be in any state of the form

$$\alpha_0|0\rangle + \alpha_1|1\rangle,$$

where α_0, α_1 are called *amplitudes* and are complex numbers satisfying $|\alpha_0|^2 + |\alpha_1|^2 = 1$. When the qubit is observed

- with probability $|\alpha_0|^2$, it is revealed to be in state $|0\rangle$;
- and with probability $|\alpha_1|^2$, it is revealed to be state $|1\rangle$.

Example 1 *Two different state vectors for a one-qubit quantum system are:*

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

Although these states have the same measurement probabilities, they are considered distinct states.

Because states are always unit vectors, we often drop the normalization factor and use $|0\rangle - |1\rangle$ to denote the state $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

Also, the above discussion can be generalized to systems of many qubits. For example, the state of a two-qubit system at any time is described by a superposition of the type

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where $\sum_{b_1,b_2} |\alpha_{b_1,b_2}|^2 = 1$. When this system is observed, its state is revealed to be $|b_1 b_2\rangle$ with probability $|\alpha_{b_1,b_2}|^2$.

To manipulate the state of a qubit, we have to use a *quantum operation*, which is a function that maps the current state to a new state. Today, we only use operations on single qubits. Quantum mechanics allows only *unitary* operations, which are linear operations that preserve the invariant $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Example 2 *In the case of single qubit operations with real coefficients, this means that the allowed operations involve either a* reflection *of the state vector about a fixed vector in* $\mathbb{R}^2$ *or a* rotation *of the state vector by some angle* $\sigma \in [0, 2\pi)$.

2.3 The EPR paradox

- The EPR paradox, named after its proposers, Einstein, Podosky, and Rosen'1935, is a thought experiment that shows that quantum mechanics allow systems in two far corners of the univers to instantaneously coordinate their actions, seemingly contradicting the axiom of Einstein's special theory of relativity that nothing can travel faster than light.
- In 1964, John Bell showed how to turn the EPR thought experiment into an actual experiment. Two systems far away from each other in the universe have a shared quantum state (actually, a two-qubit system). This shared state allows them to to coordinate their actions in a way that is provably impossible in a "classical" system.
- Since then Bell's experiment has been repeated many times in various settings always with the same conclusion: the predictions of quantum mechanics are correct.
- Today, it is not seen as a paradox, since the systems involved do not *transmit* information faster than the speed of light — they merely act upon information that was already shared, albeit in the form of a quantum superposition.

2.3.1 The Parity Game

We start by describing a game that seems to involve no quantum mechanics at all. The game involves two players Alice and Bob isolated from each other and an experimenter. It proceeds as follows:

1. The experimenter chooses two random bits $x, y \in \{0, 1\}$.
2. He presents x to Alice and y to Bob.
3. Alice and Bob respond with bits a, b, respectively.
4. Alice and Bob win if and only if $a \oplus b = x \wedge y$, where $\oplus$ denotes the XOR operation.

Observe that there is an easy strategy for Alice and Bob so that they win with probability 3/4. Bot always responds with 0 bits. This makes them win in every case except when $x = y = 1$ which happens with probability 3/4. The following theorem is also easy to prove and left as an exercise (see also book).

Theorem 1 *No (deterministic or probabilistic) strategy used by Alice and Bob can cause them to win with probability more than* 3/4.

2.3.2 The parity game with sharing of quantum information

We show that if Alice and Bob can share a two-qubit system (which they created in a certain state, and split between them before they were taken light year apart), then they can circumvent Theorem 1 and win the parity game with probability better than 3/4 using the following strategy:

1. Before the game begins, Alice and Bob prepare a two-qubit system in the state $|00\rangle + |11\rangle$, which we call the *EPR state.*
2. Alice and Bob split the qubits: Alice takes the first qubit, and Bob takes the second qubit.

   (Quantum mechanism does not require the individual bits of a two-qubit quantum system to be physically close to one another. It is important that Alice and Bob have not measured these qubits yet.)
3. Alice receives the qubit x from the experimenter, and if $x = 1$, then she applies rotation by $\pi/8$ (22.5 degrees) operation to her qubit.
4. Bob receives the qubit y from the experimenter, and if $y = 1$, then he applies rotation by $-\pi/8$ (-22.5 degrees) to his qubit.
5. Both Alice and Bob measure their respective qubits and output the values obtained as their answers a and b.

Some remarks:

- We remark that the order in which Alice and Bob perform their rotations and measurements does not matter: It can be shown that all orders yield exactly the same distribution.
- While splitting a two-qubit system and applying unitary transformations to the different parts may sound far fetched, this experiment has been performed several times in practice, verifying the theorem below (which is the prediction of quantum mechanics).

Theorem 2 *With the above strategy, Alice and Bob win with probability at least* 0.8.

Proof Alice and Bob win the game if they output a different answer when $x = y = 1$ and the same otherwise.

The intuition behind the proof is that unless $x = y = 1$, the states of the two qubits will be close to one another (with an angle of at most $\pi/8$) and otherwise the states will be "far" (having an angle of $\pi/4$). Specifically, we will show that

1. If $x = y = 0$, then $a = b$ with probability 1.
2. If $x \neq y$, then $a = b$ with probability $\cos^2(\pi/8) \geq 0.85$.
3. If $x = y = 1$, then $a = b$, with probability $1/2$.

This implies the theorem as then the overall acceptance probability is at least $\frac{1}{4} \cdot 1 + \frac{1}{2} \cdot 0.85 + \frac{1}{4} \cdot \frac{1}{2} = 0.8$.

Let us now prove the three different cases.

- In case (1) both Alice and Bob perform no operation on their qubits and so when measured it will be either in the state $|00\rangle$ or $|11\rangle$, both resulting in Alice and Bob outputting the same answer and winning the game.
- To analyze case (2), it suffices to consider the case $x = 0, y = 1$ (the other case is symmetrical). In this case, Alice applies no transformation but Bob rotates his qubit in a $-\pi/8$ angle. So after the rotation of Bob, the two-qubit system has the state

  $$|0\rangle \cdot (\cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle) + |1\rangle \cdot (\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle$$

  implying that the probability that they measure the same value is $\cos^2(\pi/8)$.[1]
- In case (3) we again use direct computation. After both rotations are performed, the two-qubit system has the state

  $$\begin{aligned}&(\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle)(\cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle)\\ &\quad + (-\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle)(\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle)\end{aligned}$$

  which equals (by collecting the terms)

  $$\begin{aligned}&\left(\cos^2(\pi/8) - \sin^2(\pi/8)\right)|00\rangle - 2\sin(\pi/8)\cos(\pi/8)|01\rangle\\ &+ 2\sin(\pi/8)\cos(\pi/8)|10\rangle + \left(\cos^2(\pi/8) - \sin^2(\pi/8)\right)|11\rangle\end{aligned}$$

  Now since $(\cos^2(\pi/8) - \sin^2(\pi/8)) = \cos(\pi/4) = \sin(\pi/4) = 2\cos(\pi/8)\sin(\pi/8)$ we have that all the coefficients in this state have the same absolute value; hence, when measured, the two-qubit system will output two qubits of same value with probability 1/2.

■

Some remarks:

- Exist games with more dramatic differences between classical and quantum cases.
- The ideas behind the EPR's and Bell's experiments have recently been used to device quantum encryption schemes whose security depends only on the principles of quantum mechanics; rather than any unproven conjecture such as $\mathbf{P} \neq \mathbf{NP}$.

[1] We remark that here we have also used the notation $|x\rangle|y\rangle$ to denote the state $|xy\rangle$. An operation that is easily checked to respect the distributive law.