Notes 8.370/18.435 Fall 2022

Lecture 1: Introduction and History Prof. Peter Shor

Quantum mechanics is a decidedly weird theory. I start with a few quotes about this. On the web, there are lots of quotes attributed to famous physicists saying how strange quantum theory is. Unfortunately, it seems like most of them are apocryphal. Here are some which seem to be verified:

> "Those who are not shocked when they first come across quantum theory cannot possibly have understood it." — Niels Bohr.

> "I admit, of course, that there is a considerable amount of validity in the statistical approach which you were the first to recognize clearly as necessary given the framework of the existing formalism. I cannot seriously believe in it because the theory cannot be reconciled with the idea that physics should represent a reality in time and space, free from spooky actions at a distance." — Albert Einstein

> "If you will simply admit that maybe [nature] does behave like this, you will find her a delightful, entrancing thing. Do not keep saying to yourself, if you can possible avoid it, 'But how can it be like that?' because you will get 'down the drain', into a blind alley from which nobody has escaped."— Richard Feynman

In the first lecture, I'm going to explain the mechanics of the course (see the syllabus for this) and I'm going to give a very abbreviated history of quantum mechanics. Quantum mechanics is a very non-intuitive theory, and in this lecture, I'm going to concentrate not on the usual parts of quantum mechanics, but the non-intuitive parts, so maybe this should be called a history of the discovery of the weirdness of quantum mechanics.

Quantum mechanics was formulated over the early part of the 20th century, but it really came together as a coherent theory in 1925 when several physicists, most notably Werner Heisenberg, Max Born, and Erwin Schrödinger, put together the matrix mechanics formulation of quantum mechanics and the wave-function formulation of quantum mechanics and showed that they were equivalent.

Einstein wasn't particularly happy with the theory they came up with. After a few earlier attempts trying to explain why he didn't like it, he wrote a paper in 1935 with Boris Podolsky and Nathan Rosen (generally called EPR after the initials of the authors) explaining why he thought the then-current formulation of quantum mechanics couldn't be complete. This paper sparked a lot of discussion, with Schrödinger agreeing with Einstein (and coming up with his famous cat to explain what was wrong with quantum mechanics), while Heisenberg, Born, and Wolfgang Pauli took Bohr's side, arguing that the then-current formulation of quantum mechanics was completely satisfactory, and did not need to be changed.

What was the gist of the argument? The Heisenberg uncertainty principle says that you cannot simultaneously measure the position and the momentum of a particle with a

high degree or precision for both measurements. One possible reason for this might be that a particle cannot have both an exact position and an exact momentum; in fact, this is indeed one reason for this. However, Einstein came up with a thought experiment which he thought showed that a particle must necessarily possess both, and from this he concluded that the then-current quantum mechanics was incomplete,

What was Einstein's argument? You can create a state of two quantum particles where, if you measure both of their positions, they will be opposite, and if you measure both of their momenta, they will also be opposite. Take these particles, make sure they're well separated, and measure them simultaneously. The EPR argument assumes that information cannot travel faster than light. And since information about which measurement you chose for the leftmost particle cannot get to the rightmost one faster than light, the rightmost particle must "know" what result it will give for both of these measurements, even though you can only carry out one of these measurements. Thus, quantum mechanics cannot describe the entire state of the rightmost particle, so it is incomplete.

In 1964, John Bell took the ideas of the EPR paper, and formalized them to prove that quantum mechanics violates either realism or locality. (Of course, this theorem depends on your exact definitions of "realism" and "locality".) We will go over his proof later in the course. This theorem involves showing that two particles (that are now called an EPR pair and said to be *entangled*) have probabilities of experimental outcomes that cannot be explained by standard probability theory; i.e., that quantum probability is fundamentally different from classical probability. We will explain Bell's theorem in detail later in the course.

In 1981, Alain Aspect performed the experiment proposed in Bell's paper and showed that the results agreed with the predictions of quantum mechanics, and thus that the quantum "paradoxes" were real. This experiment has been performed many times since. In 2022, three physicists, Alain Aspect, John Clauser, and Anton Zeilinger, were given the Nobel Prize for similar experiments.

Why does physics work like this, and what is the underlying mechanism of the universe? Some physicists have been arguing for decades about what the real structure of the universe might be that would give rise to these rules. They have been regularly coming up with new proposals. These theories of the real structure of the universe are called "interpretations" of quantum mechanics, because they all give the same experimental predictions. However, there's no consensus about which of them are reasonable, or even workable. Furthermore, many of the theories they have come up with are relatively useless for doing actual physics calculations.

One of these interpretations, and possibly the most popular, is the "Copenhagen interpretation." Niels Bohr, one of the physicists who contributed to the invention of quantum mechanics, founded and was director of the Institute for Physics at the University of Copenhagen, where much of the theory of quantum mechanics was discovered. Bohr also wrote several papers on the philosophy of quantum mechanics, some of which are very difficult to understand. The Copenhagen interpretation of quantum mechanics is suposedly the interpretation that Niels Bohr developed there.

There is no consensus as to the exact details of the Copenhagen interpretation; however, it often involves something called "the collapse of the wave function." However, it appears that Bohr did not believe that this collapse was real — one view is that

nothing on the quantum scale is real, but that quantum mechanics is a mechanism for doing calculations so as to predict the outcomes of experiments. Some things Bohr said support the idea that this was his view, for instance, he said "Everything we call real is made of things that cannot be regarded as real." As we have gotten better and better at imaging quantum systems, this view has become increasingly untenable, but the alternative interpretations all have other problems.

When David Mermin (who had generally been dismissive of the Copenhagen interpretation) started teaching quantum computing to computer scientists, he found himself reinventing the Copenhagen interpretation, as this is possibly the interpretation that is easiest to explain. In this course, I will explain the rules of quantum mechanics using a variant of the Copenhagen interpretation, for exactly this reason. And maybe this was one of the reasons that physicists at the Institute of Physics settled on the Copenhagen interpretation during the 1920s and 1930s — they were teaching quantum mechanics to physicists who didn't know it, and the Copenhagen interpretation is the one they naturally came up with.

In 1968, a grad student, Stephen Wiesner, started wondering whether the weirdness of quantum mechanics could be used for something. One thing he came up with was something he called "quantum money". He wrote up the idea, submitted the paper, and it was rejected, at which point he gave up. It wasn't actually published until 1983, when Charlie Bennett sent it to a theoretical computer science newsletter.

Stephen Wiesner's quantum money scheme actually has several flaws in it, but Charlie Bennett and Gilles Brassard took Wiesner's basic idea and came up with a quantum key distribution protocol, now called BB84 (after the proposers and the year it was published) which was sound. This protocol lets two people who have never communicated in the past and who are connected by a (possibly noisy) quantum channel, that an eavesdropper can listen to, establish an absolutely secure secret key. Classically, you can do this only if you rely on the eavesdropper not being able to solve some problem that you believe is computationally hard. Several companies are selling quantum key distribution systems today. If we have time, we will cover this at the end of the course.

In the early 1980s, Feynman started thinking about the complexity of simulating quantum physics on a classical computer. It appeared to require exponential time in the worst case (it still appears to), so he wondered about using quantum computers to simulate quantum systems[1]. He published a paper about this in 1982, and another in 1985, and simulating quantum systems is still believed to be one of the most likely applications of quantum computers, if we ever manage to build them.

Feynman's paper started computer scientists and others thinking about quantum computing. David Deutsch asked the question: "if quantum computers are faster for simulating quantum mechanics, might they be faster for other problems?" David Deutsch and Richard Jozsa found the first algorithm that was significantly faster than a classical algorithm for the same problem (although this speed-up was rather unimpressive). This was followed by an algorithm of Dan Simon which gave much stronger evidence that quantum computers could speed up solving classical problems. Looking

[1] R.P. Poplavskii and Yu. Manin also observed this earlier in the Soviet Union, but they each wrote a few paragraphs about it rather than two full papers.

at Simon's algorithm, In 1994 I found an algorithm that could factor large integers into primes efficiently. Again, we will explain this algorithm later in the course.

Lov Grover, around a year later, found a quantum algorithm that sped up exhaustive search. We will be covering his algorithm as well.

Digital computers are built out of bits, which are systems that can take on two states. Quantum computers are built out of quantum bits (called "qubits" for short) rather than classical bits. On Friday, I will tell you what a qubit is, and we will start explaining how qubits behave.