

1 Readings

Benenti, Casati, Strini: Introduction

Kaye, Laflamme, Mosca: Chs. 1.6-1.7, 2.1-2.2

2 Course Philosophy/Outline

Over the last decade there has been great foundational progress at the interface of quantum physics and computer science. The remarkable power of computing devices based on quantum mechanics is the subject of the emerging area of quantum computation (which incidentally provides an alternative to the exponential Moore's law dash towards fundamental limits in classical computation). This course provides an introduction to this area, the basic ideas of quantum mechanics, the formal model of quantum computers, basic quantum algorithms and more concrete proposals for experimental realization of quantum computers.

Qubits are the building blocks of quantum computation, quantum information and cryptography. They also provide a particularly simple setting in which to introduce the basic concepts of quantum mechanics such as the superposition principle, tensor products, measurements, and the enigmatic Bell's inequalities and Heisenberg uncertainty principle. The first part of this course provides a simple introduction to quantum mechanics for non-physics majors, while providing physics majors an opportunity to deepen their understanding of this important topic.

This course will focus on the enormous computational power latent in quantum mechanics and how it can be used to design quantum computers and quantum algorithms that provide algorithmic speedup relative to classical algorithms. We will also discuss schemes for quantum error-correction and for implementing unconditionally secure cryptography based on the principles of quantum mechanics.

Finally, we will turn our attention to physical realization: we will discuss in detail the spin properties of elementary particles - the vehicle of choice for carrying a qubit. The course will conclude with a survey of schemes for implementing quantum computers in the laboratory.

There are four main properties of quantum systems that are useful in quantum computation, cryptography and Information:

- Interference
- Superposition
- Entanglement
- Measurement

In particular, the detailed study of entanglement is the most important point of departure from more traditional approaches to the subject. For example, quantum computation derives its power from the fact that the

description of the state of an n -particle quantum system grows exponentially in n . This enormous information capacity is not easy to access, since any measurement of the system only yields n pieces of classical information. Thus the main challenge in the field of quantum algorithms is to manipulate the exponential amount of information in the quantum state of the system, and then extract some crucial pieces via a final measurement.

Quantum cryptography relies on a fundamental property of quantum measurements: that they inevitably disturb the state of the measured system. Thus if Alice and Bob wish to communicate secretly, they can detect the presence of an eavesdropper Eve by using cleverly chosen quantum states and testing them to check whether they were disturbed during transmission.

3 Quantum duality: Young's double-slit experiment

Recall Young's double-slit experiment from high school physics, which was used to demonstrate the wave nature of light. The apparatus consists of a source of light, a screen with two very thin identical slits, and a screen to view the (interference) pattern created by transmitted light (see picture on next page). If only one slit is open then intensity of light on the viewing screen is maximum on the straight line path and falls off in either direction. However, if both slits are open, then the intensity oscillates according to the interference pattern predicted by wave theory.

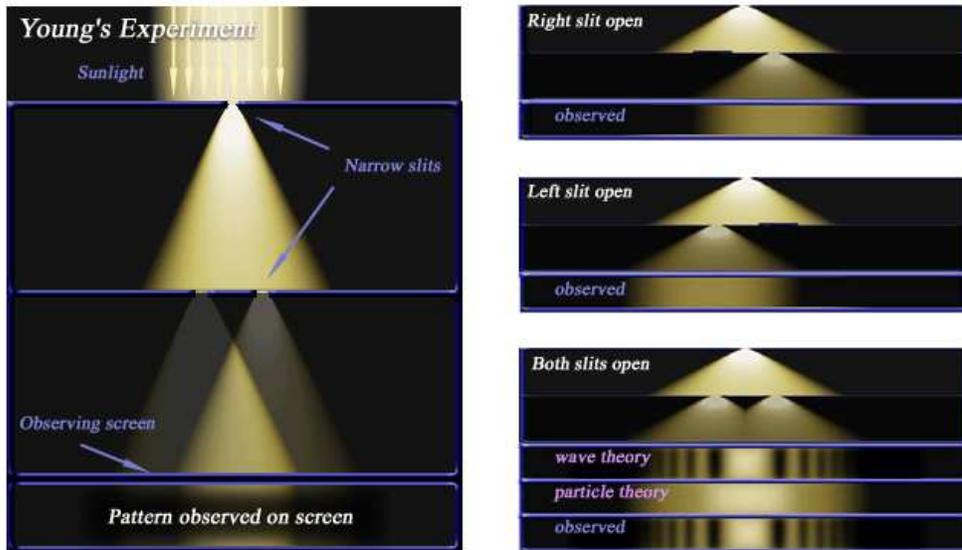
In the quantum version of this experiment, the light source is replaced by a source of single photons. Instead of the intensity of light falling on a point x on the viewing screen, we can only speak about the probability that a detector at point x detects the photon. If only a single slit is open, then plotting this probability of detection as a function of x gives the same curve as the intensity as a function of x in the classical Young experiment. What happens when both slits are open? Could the probability plot duplicate the interference pattern? Classical intuition strongly suggests that this is impossible. After all, for the photon to be detected at x , either it went through slit 1 and ended up at x or it went through slit 2 and ended up at x . The probability that it is detected at x is just the sum of the probabilities of these two events. However there are points x where the detection probability is large if only one slit is open although it is zero or small in the interference pattern. If the photon actually goes through slit 1, why should it matter whether slit 2 is open or shut. How could the probability that the photon goes through slit 1 and ends up at x be affected by whether or not slit 2 is open.

Nonetheless, the probability of detection when both slits are open does duplicate the interference pattern. How does quantum mechanics explain this? Quantum mechanics explains this as follows (although this might not be very satisfactory as an explanation, it does provide a good formal way of thinking about the phenomenon):

Quantum mechanics introduces the notion of the complex amplitude $\psi_1(x) \in \mathcal{C}$ with which the photon goes through slit 1 and hits point x on the viewing screen. The probability that the photon is actually detected at x is the square of the magnitude of this complex number: $P_1(x) = |\psi_1(x)|^2$. Similarly, let $\psi_2(x)$ be the amplitude if only slit 2 is open. $P_2(x) = |\psi_2(x)|^2$.

Now when both slits are open, the amplitude with which the photon hits point x on the screen is just the sum of the amplitudes over the two ways of getting there: $\psi_{12}(x) = \frac{1}{\sqrt{2}}\psi_1(x) + \frac{1}{\sqrt{2}}\psi_2(x)$. As before the probability that the photon is detected at x is the squared magnitude of this amplitude: $P_{12}(x) = |\psi_1(x) + \psi_2(x)|^2$. The two complex numbers $\psi_1(x)$ and $\psi_2(x)$ can cancel each other out to produce destructive interference, or reinforce each other to produce constructive interference or anything in between.

But in this quantum mechanical explanation, how does a particle that went through the first slit know that the other slit is open? In quantum mechanics, this question is not well-posed. Particles do not have trajectories,



but rather take all paths simultaneously. This is a key to the power of quantum computation.

4 Quantum States and Wavefunctions

The amplitude $\psi(x)$ is also known as the wavefunction. The argument 'x' shows us that the wavefunction is given in the position representation. This is the way in which we describe quantum states in configuration space. Mathematically, it can be viewed as kind of projection of the abstract 'quantum state' of a particle, which is a vector in a complex valued vector space known as Hilbert space, onto a set of basis functions that span configuration space. (Alternatively, as a map from the Hilbert space to the complex numbers.)

We shall deal with this more general concept of the quantum state, as distinct from any particular representation (position, momentum) extensively in the coming lectures. The quantum state provides the most complete possible description of the state of any physical system.

We shall use the Dirac ket notation for the quantum state vector, $|\psi\rangle$.