1 Course Philosophy/Outline

Over the last decade the there have been foundational progress at the interface of quantum physics and computer science. The emerging areas of quantum computation, quantum cryptography and quantum information theory all rely on the counter-intuitive information processing properties of quantum systems. There has been a growing feeling among researchers in these fields that the quantum computation and information perspective provides a new and more conceptual way of introducing students to quantum mechanics. The first part of this course will provide a brief introduction to some of the more conceptual aspects of quantum phusics from this new point of view. 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.

...

1.1 Young's double-slit experiment

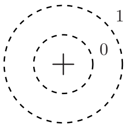
Let $\psi_1(x) \in \mathscr{C}$ be the amplitude if only slit 1 is open. Then the probability density of measuring a photon at x is $P_1(x) = |\psi_1(x)|^2$. Let $\psi_2(x)$ be the amplitude if only slit 2 is open. $P_2(x) = |\psi_2(x)|^2$.

$\psi_{12}(x) = \frac{1}{\sqrt{2}}\psi_1(x) + \frac{1}{\sqrt{2}}\psi_2(x)$ is the amplitude if both slits are open. $P_{12}(x) = |\psi_1(x) + \psi_2(x)|^2$. The two complex numbers $\psi_1(x)$ and $\psi_2(x)$ can cancel each other out – destructive interference.

But how can a single 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.

1.2 Qubits – Naive introduction

The basic entity of quantum information is a qubit (pronounced "cue-bit"), or a quantum bit. Consider the electron in a hydrogen atom. It can be in its ground state (i.e. an s orbital) or in an excited state. If this were a classical system, we could store a bit of information in the state of the electron: ground = 0, excited = 1.



In general, since the electron is a quantum system, it is in a linear superposition of the ground and excited state — it is in the ground state (0) with probability amplitude $\alpha \in \mathscr{C}$ and in the excited state (1) with probability amplitude $\beta \in \mathscr{C}$. It is as though the electron "does not make up its mind" as to which of the 2 classical states it is in. Such a 2-state quantum system is called a qubit, and its state can be written as a unit (column) vector $\binom{\alpha}{\beta} \in \mathscr{C}^2$. In Dirac notation, this may be written as:

$$\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle \quad \alpha,\beta \in \mathscr{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1$$

The Dirac notation has the advantage that the it labels the basis vectors explicitly. This is very convenient because the notation expresses both that the state of the qubit is a vector, and that it is data (0 or 1) to be processed. (The $\{\left|0\right\rangle, \left|1\right\rangle\}$ basis is called the standard or computational basis.)

This linear superposition $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ is part of the private world of the electron. For us to know the electron's state, we must make a measurement. Measuring $\left|\psi\right\rangle$ in the $\{\left|0\right\rangle, \left|1\right\rangle\}$ basis yields $\left|0\right\rangle$ with probability $|\alpha|^2$, and $\left|1\right\rangle$ with probability $|\beta|^2$.

One important aspect of the measurement process is that it alters the state of the qubit: the effect of the measurement is that the new state is exactly the outcome of the measurement. I.e., if the outcome of the measurement of$\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ yields $\left|0\right\rangle$, then following the measurement, the qubit is in state $\left|0\right\rangle$. This implies that you cannot collect any additional information about α, β by repeating the measurement.

More generally, we may choose any orthogonal basis $v, v^\perp$ and measure the qubit in it. To do this, we rewrite our state in that basis: $\left|\psi\right\rangle = \alpha'\left|v\right\rangle + \beta'\left|v^\perp\right\rangle$. The outcome is v with probability $|\alpha'|^2$, and $\left|v^\perp\right\rangle$ with probability $|\beta'|^2$. If the outcome of the measurement on $\left|\psi\right\rangle$ yields $\left|v\right\rangle$, then as before, the the qubit is then in state $\left|v\right\rangle$.

1.2.1 Measurement example I.

Q: We measure $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ in the $\left|v\right\rangle, \left|v^\perp\right\rangle$ basis, where $\left|v\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle$. What is the probability of measuring $\left|v\right\rangle$?

A: First let's do the simpler case $a = b = \frac{1}{\sqrt{2}}$, so $\left|v\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \equiv \left|+\right\rangle$, $\left|v^\perp\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \equiv \left|-\right\rangle$. See Figure 1. We express $\left|\psi\right\rangle$ in the $\left|+\right\rangle, \left|-\right\rangle$ basis:

$$\begin{aligned}
\left|\psi\right\rangle &= \alpha\left|0\right\rangle + \beta\left|1\right\rangle \\
&= \alpha\tfrac{1}{\sqrt{2}}(\left|+\right\rangle + \left|-\right\rangle) + \beta\tfrac{1}{\sqrt{2}}(\left|+\right\rangle - \left|-\right\rangle) \\
&= \tfrac{1}{\sqrt{2}}\left((\alpha+\beta)\left|+\right\rangle + (\alpha-\beta)\left|-\right\rangle\right) \quad .
\end{aligned}$$

Therefore the probability of measuring $\left|+\right\rangle$ is $|\frac{1}{\sqrt{2}}(\alpha+\beta)|^2 = |\alpha+\beta|^2/2$. The probability of measuring $\left|-\right\rangle$ is $|\alpha+\beta|^2/2$. We will do the general case in §1.3.1.

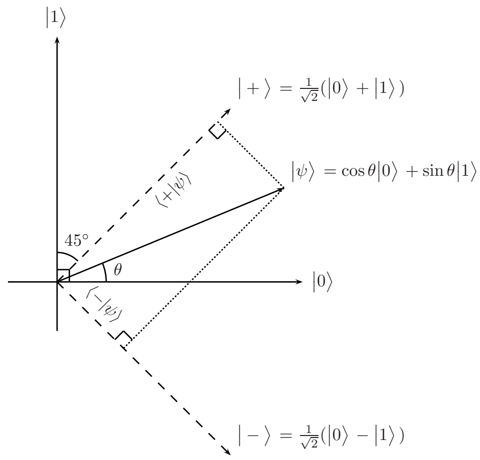


Figure 1:

1.3 Examples of Qubits

Photon Polarization:

There is a qubit associated with photon - its polarization. Recall that a photon moving along the z-axis has an associated electric field in the x-y plane. The frequency of the field is determined by the frequency of the photon. However, this still leaves the x-y components of the electric field unspecified. The 2-dimensional quantity specifying this field is the polarization of the photon. The polarization of a photon can be measured by using a polaroid or a calcite crystal. A polaroid sheet (suitably oriented) transmits x-polarized photons and absorbs y-polarized photons. Thus a photon that is in a superposition $|\phi\rangle = \alpha|x\rangle + \beta|y\rangle$ is transmitted with probability $|\alpha|^2$. If the photon now encounters another polariod sheet with the same orientation, then it is transmitted with probability 1. On the other hand, if the second polaroid sheet has its axes crossed at right angles to the first one, then if the photon is transmitted by the first polaroid, then it is definitely absorbed by the second sheet. An interesting experiment may be performed by interposing a third polariod sheet at a 45 degree angle between the first two. Now a photon that is transmitted by the first sheet makes it through the next two with probability $1/4$.

Proof: Indeed, the polarization of light after the first filter is $|0\rangle$. The probability this light passes the second filter is $|\langle 0|\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\rangle|^2 = \cos^2\frac{\pi}{4} = 1/2$. If light passes the second filter, its polarization is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Its probability of passing the third filter is then $|\langle\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle|^2 = 1/2$. $\square$

Spins:

Like photon polarization, the spin of a (spin-1/2) particle is exactly a two-state system. More next time!

1.3.1 Measurement example II.

The notation $\langle v|$ ("bra v") denotes a row vector, the conjugate-transpose of $|v\rangle$, or $|v\rangle^\dagger$. For example, $\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}$ and $\langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$. More generally,

$$\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^\dagger = \begin{pmatrix} \bar{\alpha} & \bar{\beta} \end{pmatrix} = \bar{\alpha}\langle 0| + \bar{\beta}\langle 1| \quad .$$

The Dirac notation can be handy. For example, let

$$|v_1\rangle = a_1|0\rangle + b_1|1\rangle, \quad |v_2\rangle = a_2|0\rangle + b_2|1\rangle \ .$$

Then $\langle v_1|v_2\rangle$ (shorthand for $\langle v_1|\,|v_2\rangle$) is a matrix product of the 1×2 matrix $\langle v_1|$ and the 2×1 matrix $|v_2\rangle$, or just a scalar:

$$\langle v_1|v_2\rangle = \begin{pmatrix}\bar{a}_1 & \bar{b}_1\end{pmatrix}\begin{pmatrix}a_2\\ b_2\end{pmatrix} = \bar{a}_1 a_2 + \bar{b}_1 b_2 \ .$$

$\langle v_1|v_2\rangle = \overline{\langle v_2|v_1\rangle}$ is an inner product. Note that $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \overline{\langle 1|0\rangle} = 0$. Thus the above equation could have been expanded,

$$\begin{aligned}\langle v_1|v_2\rangle &= (\bar{a}_1\langle 0| + \bar{b}_1\langle 1|)(a_2|0\rangle + b_2|1\rangle)\\ &= \bar{a}_1 a_2\langle 0|0\rangle + \bar{a}_1 b_2\langle 0|1\rangle + \bar{b}_1 a_2\langle 1|0\rangle + \bar{b}_1 b_2\langle 1|1\rangle\\ &= \bar{a}_1 a_2\cdot 1 + \bar{a}_1 b_2\cdot 0 + \bar{b}_1 a_2\cdot 0 + \bar{b}_1 b_2\cdot 1\\ &= \bar{a}_1 a_2 + \bar{b}_1 b_2 \ .\end{aligned}$$

In this notation, $\alpha = \langle 0|\psi\rangle$, $\beta = \langle 1|\psi\rangle$. The normalization condition $|\alpha|^2 + |\beta|^2 = 1$ is

$$\begin{aligned}1 = |\alpha|^2 + |\beta|^2 &= \bar{\alpha}\alpha + \bar{\beta}\beta\\ &= \langle\psi|0\rangle\langle 0|\psi\rangle + \langle\psi|1\rangle\langle 1|\psi\rangle\\ &= \langle\psi|\,(|0\rangle\langle 0| + |1\rangle\langle 1|)\,|\psi\rangle\\ &= \langle\psi|\psi\rangle \ .\end{aligned}$$

The last equality above follows since $|0\rangle\langle 0| = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $|1\rangle\langle 1| = \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, so $|0\rangle\langle 0| + |1\rangle\langle 1|$ is the 2×2 identity matrix. (This trick is important enough to have its own name, the "resolution of the identity.")

In the next lecture, we will introduce tensor product spaces, where the advantages of this notation increase.

With the new notation, it is simple to solve the general case of the question asked in §1.2.1. Recall $|v\rangle = a|0\rangle + b|1\rangle$ and choose $|v^\perp\rangle = \bar{b}|0\rangle - \bar{a}|1\rangle$. Indeed, $\langle v|v^\perp\rangle = ab - ba = 0$.

$$\begin{aligned}|\psi\rangle &= \Big(|v\rangle\langle v| + |v^\perp\rangle\langle v^\perp|\Big)|\psi\rangle\\ &= \alpha(|v\rangle\langle v|0\rangle + |v^\perp\rangle\langle v^\perp|0\rangle) + \beta(|v\rangle\langle v|1\rangle + |v^\perp\rangle\langle v^\perp|1\rangle)\\ &= (\alpha\langle v|0\rangle + \beta\langle v|1\rangle)|v\rangle + (\alpha\langle v^\perp|0\rangle + \beta\langle v^\perp|1\rangle)|v^\perp\rangle\\ &= (\alpha\bar{a} + \beta\bar{b})|v\rangle + (\alpha b + \beta a)|v^\perp\rangle \ .\end{aligned}$$

The probability of measuring $|v\rangle$ in a measurement in the $v, v^\perp$ basis is therefore

$$|\langle v|\psi\rangle|^2 = |\alpha\bar{a} + \beta\bar{b}|^2 \ .$$