1 Why Quantum Computation?

There are several reasons why we might wish to study quantum computation. Here are a few:

- Moore's Law

  Moore's Law states that the density of transistors on a chip roughly doubles every eighteen months. Current estimates say that in about a decade this should be down to single electron transistors. This is the end of the road for further miniaturization of classical computers based on electronics. Long before that chip designers will have to contend with quantum phenomena. Quantum computation provides a method of bypassing the end of Moore's Law, and also provides a way of utilizing the inevitable appearance of quantum phenomena.

- Factoring, Discrete log, Pell's equations, etc..

  There are certain problems that quantum computation allows us to solve more efficiently that any classical computational method. A few examples are listed above. We may wish to exploit this feature of quantum computation.

- Cryptography

  Quantum computation allows us to do cryptography in a way that doesn't require assumptions about factoring primes, etc.. It also allows us to break classical cryptography schemas. Obviously, if we are interested in cryptography, we'll also have to be interested in quantum computation.

  Above are the three standard reasons for studying quantum computation. There are other reasons as well that are perhaps just as compelling.

- Quantum Mechanics is a model of computation

  We can study quantum mechanics as a model of computation.

- Quantum Entanglement

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.

...

2 Young's double-slit experiment

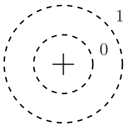
Let $\psi_1(x) \in \mathscr{C}$ be the amplitude if only slit 1 is open. Then the probability density of measuring a photon at x is $P_1(x) = |\psi_1(x)|^2$. Let $\psi_2(x)$ be the amplitude if only slit 2 is open. $P_2(x) = |\psi_2(x)|^2$.

$\psi_{12}(x) = \frac{1}{\sqrt{2}}\psi_1(x) + \frac{1}{\sqrt{2}}\psi_2(x)$ 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.

3 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.)

In general a column vector —called a "ket"— is denoted by $\left|\ \right\rangle$ and a row vector —called a "bra"— is denoted by $\left\langle\ \right|$.

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 $\left|v\right\rangle$.

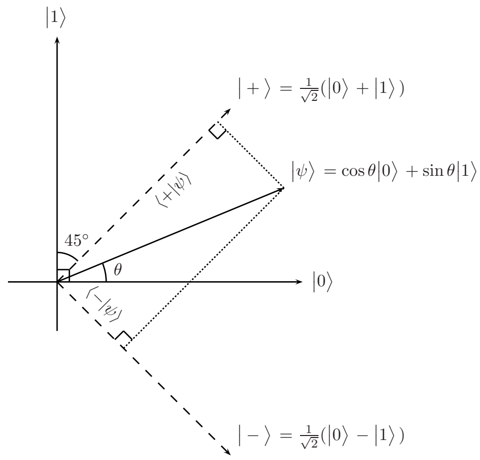


Figure 1:

3.0.1 Measurement example I.

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

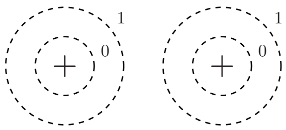
A: First let's do the simpler case $a = b = \frac{1}{\sqrt{2}}$, so $|v\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle$, $|v^{\perp}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle$. See Figure 1. We express $|\psi\rangle$ in the $|+\rangle, |-\rangle$ basis:

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

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

4 Two qubits:

Now let us examine the case of two qubits. Consider the two electrons in two hydrogen atoms:



Since each electron can be in either of the ground or excited state, classically the two electrons are in one of four states – 00, 01, 10, or 11 – and represent 2 bits of classical information. Quantum mechanically, they are in a superposition of those four states:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \quad ,$$

where $\sum_{ij}|\alpha_{ij}|^2 = 1$. Again, this is just Dirac notation for the unit vector in $\mathscr{C}^4$:

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

where $\alpha_{ij} \in \mathscr{C}$, $\sum |\alpha_{ij}|^2 = 1$.

Measurement:

If the two electrons (qubits) are in state $|\psi\rangle$ and we measure them, then the probability that the first qubit is in state i, and the second qubit is in state j is $P(i,j) = |\alpha_{ij}|^2$. Following the measurement, the state of the two qubits is $|\psi'\rangle = |ij\rangle$. What happens if we measure just the first qubit? What is the probability that the first qubit is 0? In that case, the outcome is the same as if we had measured both qubits: $\Pr\{\text{1st bit } = 0\} = |\alpha_{00}|^2 + |\alpha_{01}|^2$. The new state of the two qubit system now consists of those terms in the superposition that are consistent with the outcome of the measurement – but normalized to be a unit vector:

$$|\phi\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

.

A more formal way of describing this partial measurement is that the state vector is projected onto the subspace spanned by $|00\rangle$ and $|01\rangle$ with probability equal to the square of the norm of the projection, or onto the orthogonal subspace spanned by $|10\rangle$ and $|11\rangle$ with the remaining probability. In each case, the new state is given by the (normalized) projection onto the respective subspace.

5 Entanglement

Consider the state of a two qubit system given by $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Notice that this state cannot be represented as $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$ for any complex numbers α_0, α_1, β_0 or β_1. We cannot analyze the state of each individual qubit in this sytem, because the states of the two qubits are entangled. If we take a measurement on the first qubit, then the state of the other qubit is determined by the outcome of the measurement. With probability $\frac{1}{2}$ we see $|0\rangle$ as the outcome of the measurement, and in this case, we know that the state of the system must be $|00\rangle$.

Entangled states provide one method of showing that the outcomes of quantum mechanics cannot be explained by any thory of "'hidden variables"'.

5.1 EPR Paradox:

In 1935, Einstein, Podolsky and Rosen (EPR) wrote a paper "Can quantum mechanics be complete?" [Phys. Rev. 47, 777, Available online via PROLA: `http://prola.aps.org/abstract/PR/v47/i10/p777_1`]

For example, consider coin-flipping. We can model coin-flipping as a random process giving heads 50% of the time, and tails 50% of the time. This model is perfectly predictive, but incomplete. With a more accurate experimental setup, we could determine precisely the range of initial parameters for which the coin ends up heads, and the range for which it ends up tails.

For Bell state, when you measure first qubit, the second qubit is determined. However, if two qubits are far apart, then the second qubit must have had a determined state in some time interval before measurement, since the speed of light is finite. Moreover this holds in any basis. This appears analogous to the coin flipping example. EPR therefore suggested that there is a more complete theory where “God does not throw dice.”

What would such a theory look like? Here is the most extravagant framework... When the entangled state is created, the two particles each make up a (very long!) list of all possible experiments that they might be subjected to, and decide how they will behave under each such experiment. When the two particles separate and can no longer communicate, they consult their respective lists to coordinate their actions.

But in 1964, almost three decades later, Bell showed that properties of EPR states were not merely fodder for a philosophical discussion, but had verifiable consequences: local hidden variables are not the answer.

5.2 Bell's Inequality

Bell's inequality states: There does not exist any local hidden variable theory consistent with these outcomes of quantum physics.

Consider the following communication protocol in the classical world: Alice (A) and Bob (B) are two parties who share a common string S. They receive independent, random bits X_A, X_B, and try to output bits a, b respectively, such that $X_A \wedge X_B = a \oplus b$. (The notation $x \wedge y$ takes the AND of two binary variables x and y, i.e., is one if $x = y = 1$ and zero otherwise. $x \oplus y \equiv x + y \bmod 2$, the XOR.)

In the quantum mechanical analogue of this protocol, A and B share the EPR pair $\left|\Psi^-\right\rangle$. As before, they receive bits X_A, X_B, and try to output bits a, b respectively, such that $X_A \wedge X_B = a \oplus b$.

If the odd behavior of $\left|\Psi^-\right\rangle$ can be explained using some hidden variable theory, then the two protocols give above should be equivalent.

However, Alice and Bob's best protocol for the classical game, as you will prove in the homework, is to output $a = 0$ and $b = 0$, respectively. Then $a \oplus b = 0$, so as long as the inputs $(X_A, X_B) \neq (1,1)$, they are successful: $a \oplus b = 0 = X_A \wedge X_B$. If $X_A = X_B = 1$, then they fail. Therefore they are successful with probability exactly 3/4.

We will show that the quantum mechanical system can do better. Specifically, if Alice and Bob share an EPR pair, we will describe a protocol for which the probability $\Pr\{X_A \wedge X_B = a \oplus b\}$ is greater than 3/4.

We can setup the following protocol:

- if $X_A = 0$, then Alice measures in the standard basis, and outputs the result.
- if $X_A = 1$, then Alice rotates by $\pi/8$, then measures, and outputs the result.
- if $X_B = 0$, then Bob measures in the standard basis, and outputs the complement of the result.
- if $X_B = 1$, then Bob rotates by $-\pi/8$, then measures, and outputs the complement of the result.

Now we calculate $\Pr\{a \oplus b \neq X_A \wedge X_B\}$. (Recall that if measurement in the standard basis yields $\left|0\right\rangle$ with probability 1, then if a state is rotated by θ, measurement yields $\left|0\right\rangle$ with probability $\cos^2(\theta)$.) There are four cases:

$$\Pr\{a \oplus b \neq X_A \wedge X_B\} \quad = \quad \sum_{X_A, X_B} \tfrac{1}{4} \Pr\{a \oplus b \neq X_A \wedge X_B | X_A, X_B\}$$

Now we claim

$$\begin{aligned}
\Pr\{a \oplus b \neq X_A \wedge X_B \,|\, X_A = 0, X_B = 0\} &= 0 \\
\Pr\{a \oplus b \neq X_A \wedge X_B \,|\, X_A = 0, X_B = 1\} &= \sin^2(\pi/8) \\
\Pr\{a \oplus b \neq X_A \wedge X_B \,|\, X_A = 1, X_B = 0\} &= \sin^2(\pi/8) \\
\Pr\{a \oplus b \neq X_A \wedge X_B \,|\, X_A = 1, X_B = 1\} &= \sin^2(\pi/4) = 1/2 \ .
\end{aligned}$$

Indeed, for the first case, $X_A = X_B = 0$ (so $X_A \wedge X_B = 0$), Alice and Bob each measure in the computational basis, without any rotation. If Alice measures $a = 0$, then Bob's measurement is the opposite, and Bob outputs the complement, $b = 0$. Therefore $a \oplus b = 0 = X_A \wedge X_B$, a success. Similarly if Alice measures $a = 1$, they are always successful.

In the second case, $X_A = 0$, $X_B = 1$ ($X_A \wedge X_B = 0$). If Alice measures $a = 0$, then the new state of the system is $|01\rangle$; Bob's qubit is in the state $|1\rangle$. In the rotated basis, Bob measures a 1 (and outputs its complement, 0) with probability $\cos^2(\pi/8)$. The probability of *failure* is therefore $1 - \cos^2(\pi/8) = \sin^2(\pi/8)$. Similarly if Alice measures $a = 1$. The third case, $X_A = 1$, $X_B = 0$ is symmetrical.

In the final case, $X_A = X_B = 1$ (so $X_A \wedge X_B = 1$), Alice and Bob are measuring in bases rotated 45 degrees from each other, so their measurements are independent. The probability of failure is $1/2$.

Averaging over the four cases, we find

$$\begin{aligned}
\Pr\{a \oplus b \neq X_A \wedge X_B\} &= 1/4\left(2\sin^2(\pi/8) + 1/2\right) \\
&= 1/4\,(1 - \cos(2 * \pi/8) + 1/2) \\
&= 1/4\left(3/2 - \sqrt{2}/2\right) \\
&\approx 1/8\,(3 - 1.4) \\
&= 1.6/8 = .2 \ .
\end{aligned}$$

The probability of success with this protocal is therefore around .8, better than any protocol could achieve in the classical, hidden variable model.

Exercise: Consider the GHZ (Greenberger-Horne-Zeilinger) state, of 3 qubits:

$$\frac{1}{2}\left(|000\rangle - |011\rangle - |101\rangle - |110\rangle\right)$$

Suppose three parties, A, B and C with experiments X_A, X_B, X_C respectively, with the constraint $X_A \oplus X_B \oplus X_C = 0$. Output a, b, c s.t. $X_A \vee X_B \vee X_C = a \oplus b \oplus c$. Show that this can be done with certainty. Hint: you'll need the Hadamard matrix,

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

which takes

$$|0\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$|1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$