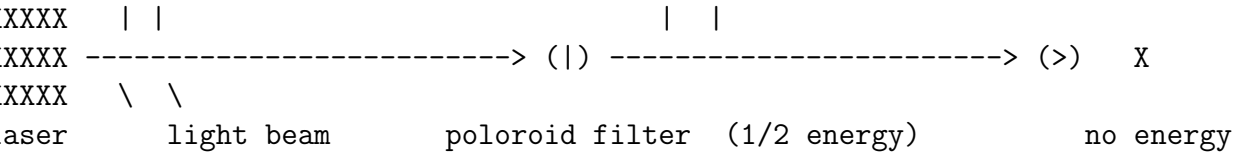
COS 533: Advanced Cryptography — Princeton University
Lecture 21 (12-4-17)
Lecturer: Mark Zhandry — Scribe: Jacob Edelman

Notes for Lecture 21

1 Experimental Examples

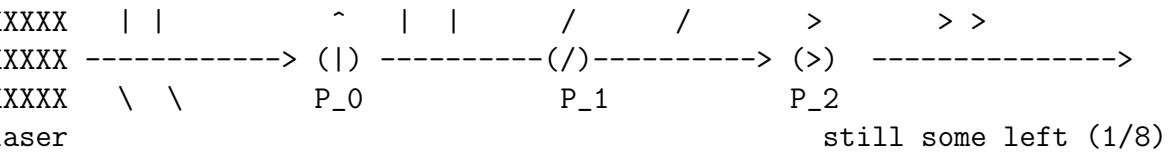
We will first discuss some experiments in order to start giving an idea of the physical properties quantum computing allows us to harness.

1.1 Experiment 1



Here we have a laser shooting out a light beam equally combining light with a 90 degree, |, and one hundred thirty-five degree,
, polarization. After the first polariod filter, the (|), which filters for light with the 90 degree polarization, only half the energy remains, all of it having a 90 degree polarization. The second filter, (>), filters for light with a 0 degree polarization, resulting in no energy remaining after this filter.

1.2 Experiment 2



Here we add in a polaroid filter (called P_1) in-between the filters from the previous experiment. Counter-intuitively, adding in this additional filter results in some energy, one-eighth of the original amount, being left after the final filter.

2 Explanations

We will now look at different ways to explain this phenomenon.

2.1 Classical Explanation

This can be described classically, with an electric field is a vector and the polaroid filters being projection.

This idea doesn't quite make sense with quantum mechanics, because light is made of photons, and you can't get half a photon.

2.2 Quantum Explanation

We will represent different polarizations with specific notations. We will use $|\uparrow\rangle$ to indicate a vertical polarization. We will use $|\rightarrow\rangle$ to indicate a horizontal polarization. $|\nearrow\rangle$ will be for a 45 degree polarization and $|\searrow\rangle$ for 135 degrees.

We will generalize this by representing them in the form $\alpha|\uparrow\rangle + \beta|\rightarrow\rangle$, with normalization. For instance, $|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$. In general, for an angle θ we have $|\psi\rangle = e^{i\gamma}\cos(\theta)|\uparrow\rangle + \sin(\theta)|\rightarrow\rangle$.

Now, for the diagrams above, a photon will be emitted with a random θ. When it hits P_0, with probability $\cos^2(\theta)$, the photon passes through and becomes $|\uparrow\rangle$. With $\sin^2(\theta)$ it will be absorbed. If there is not P_1, should a photon make it past P_0 it will be absorbed by P_2.

In general we will have that for a photon $|\theta\rangle = e^{i\gamma}\cos(\theta)|\uparrow\rangle + \sin(\theta)|\rightarrow\rangle$ and a filter P polarized with $|\theta'\rangle = \cos(\theta')|\uparrow\rangle + sin(\theta')|\rightarrow\rangle$ with probability $\cos^2(\theta - \theta')$ the photon passes through and becomes $|\theta'\rangle$ and with probability $\sin^2(\theta - \theta')$ it will be absorbed. This formula can be used to analyze the diagram with P_0, P_1, P_2 and it will return the correct probabilities.

2.2.1 Notation

$|\uparrow\rangle, |\rightarrow\rangle$, or the more general $|\psi\rangle$ represent column vectors. In general we will have things of the form $\begin{pmatrix} e^{i\gamma}cos\theta \\ sin\theta \end{pmatrix}$.

$\langle\psi|$ will represent the row vector, which has the general form $\begin{pmatrix} e^{-i\gamma}cos\theta & sin\theta \end{pmatrix}$. This is basically the conjugate transpose of a column vector.

We also have $\langle\psi|\ \psi'\rangle$ which is the inner project. Our normalizing condition is equivalent to $\langle\psi|\ \psi'\rangle = 1$.

We can now rewrite the general polarization rule from before. If polarization is $|\psi'\rangle$, photon is $|\psi\rangle$, the photon will pass with probability $|\langle\psi'|\,\psi\rangle|^2$, and becomes $|\psi'\rangle$. The remainder of the time it is absorbed.

2.3 Realizations

There are different ways to realize this idea of a $|\psi\rangle$ state that we have been describing, just like their are different ways to physically realize a bit, We call what is being realized by a photon here a qubit. We associate $|\uparrow\rangle$ with 0 and $|\rightarrow\rangle$ with 1.

3 Measurements

Our polarization filters allow us to detect polarization to some extent, We can implement a mechanism using this for measurement. Let $|b_0\rangle, |b_1\rangle$ be an orthogonal basis for a 2d complex space. For example $\begin{pmatrix}0\\1\end{pmatrix}$ and $\begin{pmatrix}1\\0\end{pmatrix}$.

Given a state $|\psi\rangle$ we can measure in our basis B, and with probability $|\langle b_0|\,\psi\rangle|^2$, we measure 0 and $|\psi\rangle$ becomes $|b_0\rangle$. With probability $|\langle b_1|\,\psi\rangle|^2$, we measure 1 and $|\psi\rangle$ becomes $|b_1\rangle$.

4 Operations

In addition to measurements, we can look at the operations we can do on qubits. It turns out that rotations and adding phases, and combinations of these, are the only operations we can do.

We can generalize these operations as linear norm preserving transformations, or equivalently, applying a unitary matrix.

Suppose that an operation takes $|\psi\rangle$ and goes to $U|\psi\rangle$ for some matrix U. The condition that it's norm preserving means that $\langle\psi|\,\psi\rangle = 1$ before we even do anything, so when we take the conjugate transpose we get $\langle\psi|\,U^t$ and multiply by $U|\psi\rangle$ we get that $\langle\psi|\,U^tU|\psi\rangle = 1$ in order to preserve the norm we want. Since this must hold for any ψ we get that U^tU must be the identity matrix. It turns out the only operations that have these forms are rotations, add phases, and combinations of these.

5 Comparison

We can compare the types of operations we can do with qubits and those we can do with normal probabilistic bits.

5.1 Quantum

1. The state is a vector over the complex numbers.
2. Transforms are unitary matrices where the columns are orthonormal.
3. Uses the L_2 norm.

5.2 Classical

1. A probabilistic process outputs a bit $\begin{pmatrix} a \\ b \end{pmatrix}$ where a is the probability of a 0, and b is the probability of a 1.
2. For some transform where 0 goes to 0 with prob p, and 1 with prob $1-p$, and 1 goes to 0 with prob q and 1 with prob $1-q$, we have, $\begin{pmatrix} a \\ b \end{pmatrix}$ goes to $\begin{pmatrix} p & q \\ 1-p & 1-q \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$. This sort of matrix is called a stochastic matrix. The key features are that the columns sum to 1 and all the entries are non-negative.
3. Uses the L_1 norm.

6 Quantum Key Distribution (QKD)

Using quantum computing, we can do two party key agreement, such that a passive adversary cannot discover the key.

Using Diffie-Hellman, or any pk encryption scheme works. classical solutions to this require computation assumptions. With quantum we can achieve unconditional security against unbounded adversaries.

6.1 Procedure

6.1.1 Alice

Choose random b_i, c_i bits for i from 1 to λ. she is going to make $\psi_i = |\uparrow\rangle$ if $b_i = 0$ and $b_i = 0$. $|\rightarrow\rangle$ if $b_i = 0$ and $b_i = 0$. $|\nearrow\rangle$ if $b_i = 1$ and $b_i = 1$. And $|\searrow\rangle$ if $b_i = 1$ and $b_i = 1$. she sends the ψ_i qubits to bob.

6.1.2 Bob

receives the ψ_i for each i qubits from Alice. he is going to choose random b'_i , he is going he will measure $|\psi_i\rangle$ in basis corresponding to b'_i to get c'_i note, if $b_i = b'_i$, we have $c'_i = c_i$

He will then tell Alice all the b'_i values

6.1.3 Alice

Alice will tell bob her b_i values

6.1.4 Alice and Bob

For all the $b_i = b'_i$ points, they will have $c_i = c'_i$ on these points. These c values will be there shared bits.

6.2 Eve Attacking

Suppose Eve tries to measure $|\psi_i\rangle$, she can measure herself, doing what bob does, to learn half the c bits. If Eve's basis is wrong for any $|\psi_i\rangle$, then the result will be that the $|\psi_i\rangle$ will be modified by the measurement. This will result in that c_i value being different for Alice and Bob

6.3 Procedure Continued

6.3.1 Bob

Choose a random subset S of indices where $b_i = b'_i$, also send the c'_i values at each of those indices to Alice.

6.3.2 Alice

Alice will send her own c_i values at each of those indices.

6.3.3 Alice and Bob

if any of those c_i and c'_i values are different, they abort because it means they were being observed, otherwise the remaining c_i values where $b_i = b'_i$ will be the key.

6.4 Issues

1. We are making the assumption that we already have a classical authenticated channel.

2. Eve can run a denial of service attack as the eavesdropper by just always measuring what we say.

6.5 Addendum

Considering an Eve that takes $|\psi_i\rangle$ and clones it, keeping one copy and sending the other onto Bob. This would let her replicate what Bob did and she will be able to get the keys. This is not possible because of the quantum no-cloning theorem.