Contents

1 Introduction 1/8

1.1 Introduction Stuff and General Things to Note

Stuff to know

This course will need to know more about qubits and determine their probabilities of ending on a quantum state. Some knowledge of linear algebra to help, *NOT* required.

Texts (where one by Elanor and Wolfgang is going to be most used):

- Quantum Computer Science, by David Mermin
- Quantum Computing: A Gentle Introduction, by Elanor Rieffel and Wolfgang Polak

1.2 Polarization of Photons

These are states

$$\hat{y} \Rightarrow |0\rangle$$
$$\hat{x} \Rightarrow |1\rangle$$

Dot product of

$$\vec{A} * \vec{B} = AB\cos\theta$$
$$\vec{A} * \hat{i} = A * 1 * \cos\theta = A\cos\theta$$

Generally speaking, $\vec{A} = (\hat{i} * \vec{A}) * \hat{i} + (\hat{j} + \vec{A}) * \hat{j}$

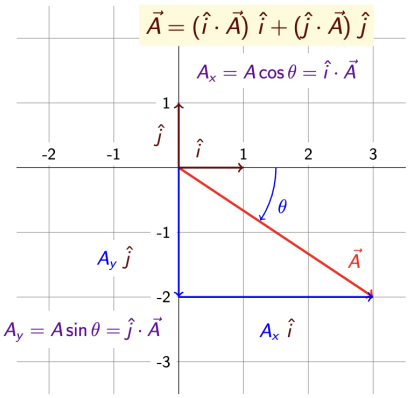


Figure 1: Some introductory material on real vectors in the plane

2 Polarization 1/10

$$\vec{\varepsilon}(t) = \vec{E}\cos(\omega t + \phi)$$

Where ω is the angular frequency and ϕ is the phase shift

$\vec{E}$ Is the most important variable
Where it is defined as:

$$\vec{E} = E_x * \hat{i} + E_y\hat{j} \doteq \begin{pmatrix} E_x \\ E_y \end{pmatrix}$$

Certain direction of the polarization is let through polarized lens Where parallel to polarized lens will go through while those that are perpendicular will not pass through...

For example, if in the y direction nothing will get through, if it is in x direction it will go through

Examples

Passes through $\hat{i}$ Polaroid:

$$\vec{E} = E_x\hat{i} = (\hat{i} * \vec{E}) * \hat{i} = \hat{i} * \hat{i} * \vec{E}$$

Passes through $\hat{j}$ Polaroid:

$$\vec{E} = E_y * \hat{j} = (\hat{j} * \vec{E}) * \hat{j}$$

$$\hat{P} = \cos\theta\hat{i} + \sin\theta\hat{j} \doteq \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$

Where $\hat{P}$ Is the orientation of the polaroid vector $(\hat{P} * \vec{E}) * \hat{P}$

Energy of a wave is $\propto$ (proportional) E^2 Fraction of energy that sets through $\hat{P}$.

$$F = (\hat{P} * \vec{E})^2$$

This is the fraction of energy that gets through the polaroid. It is squared as it the same square of the length of the vector

$\hat{p}$ Is the unit vector of E

Where $\hat{p} = \frac{\vec{E}}{|\vec{E}|}$ and

$$F = (\hat{P} * \vec{E})^2 = (\hat{P} * \hat{p})^2$$

Example Question

A linearly polarized wave with a polarization vector of magnitude E_0 making a 60-degree angle with the x-axis impinges on a polarizer that allows only x-polarized light through. What fraction of the energy is transmitted?

Answer: $\hat{P}$ is on the bottom and $\hat{p}$ is on top of big P hat such that it creates an angle of 60 degrees, creates

$$\hat{p} * \hat{P} = |\hat{p}| * |\hat{P}| \cos 60 \deg$$

Which boils down to:

$$F = \cos^2 \theta = \frac{1}{4}$$

Light consisting of photons, a bunch of them combined into light to create a wave. Photons are fundamentally the same, yet if you put a polaroid in 45 deg, some will go through, some will not... Some fraction will go through some fraction will not go through. All you know is that there is a **Probability** of going through

$$\text{Photon polarization} = \hat{p} \text{ Polaroid orientation} = \hat{P}$$

The probability that each photon passes through w.p.

$$(\hat{p} * \hat{P})^2$$

3 Representing Qubits 1/13

Remark 1. Recall that the Probability is:

$$(\hat{P} * \hat{p})^2$$

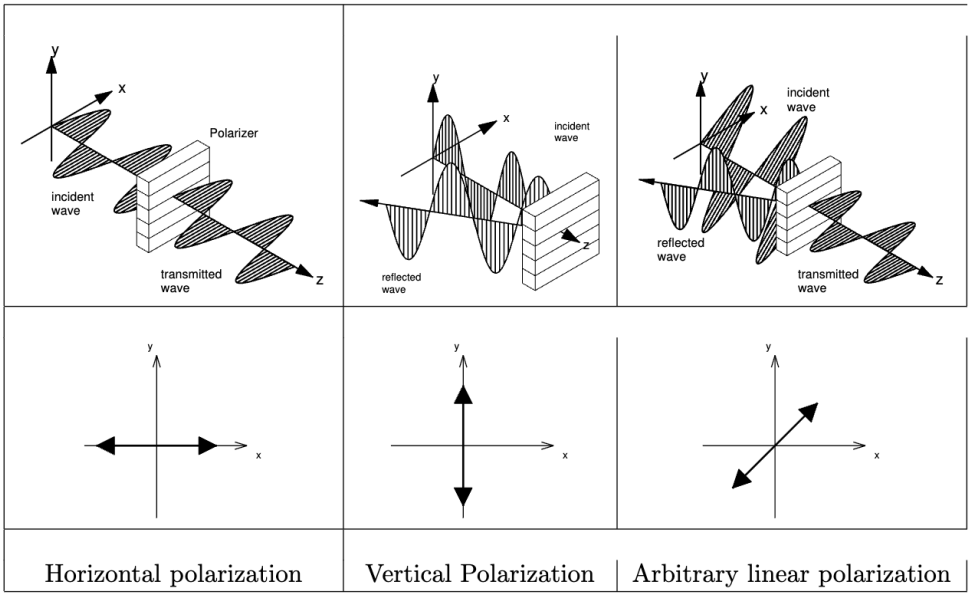


Figure 2: Polarization of electron based on wave direction

$$E_x(t) = E_x \cos(\omega t + \psi)$$

$$E_y(t) = E_y \sin(\omega t + \psi)$$

$E_x = E_y$,

Where Left circular polarization is $\alpha = +\frac{\pi}{2}$

And Right Circular Polarization is $\alpha = -\frac{\pi}{2}$

$$\hat{P}_L = \frac{1}{\sqrt{2}}(i * \hat{i} + 1\hat{j}) \doteq \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}$$

$$\hat{P}_R = \frac{1}{\sqrt{2}}(-i * \hat{i} + 1\hat{j}) \doteq \frac{1}{\sqrt{2}} \begin{pmatrix} -i \\ 1 \end{pmatrix}$$

Reflects and lets through vectors are perpendicular

Ket:$|v\rangle$ and we can use arrows to show the photon state of polarization

Where each state is vertical and horizontal respectively.

$$0, |0\rangle = |\uparrow\rangle$$
$$1, |1\rangle = |\rightarrow\rangle$$

3 Each of these are qubit states, 0 and 1

Moreover, We can combine them giving us:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$$

You have to do something to make it a 0 or 1, and we can check by letting all 1's through but not 0's

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle)$$

3.1 Complex Numbers

i is defined as:

$$i = \sqrt{-1}$$

Complex numbers are denoted with Z, where

$$Z = a + ib$$

and A and B are real numbers and it is on the complex plane.

This complex plane consists of a as the "x-axis" and ib as the "y-axis" There then exists a length with, r and angle with θ

Moreover,

$$Z = a + ib = re^{i\theta}$$

Because: (We must prove this in our homework)

$$e^{i\theta} = \cos\theta + i\sin\theta$$

Negative representation:

$$Z^* = \overline{Z} = a - ib = re^{-i\theta}$$

Furthermore,

$$|Z| = \sqrt{Z^* Z} = \sqrt{a^2 + b^2} = r^2$$

Which is the real, positive (when a or z are 0)

3.2 Vector Space and Vector Spaces w/ Complex Numbers

Definition

Vector Space is the set of vectors $\{|v\rangle\}$

$$|a\rangle + |b\rangle = |c\rangle = |b\rangle + |a\rangle$$

Which is another vector in vector space, think adding two vectors together to get c

These are also communicative and associative!

Can also give a magnitude to such vectors as well.

There is also a 0 vector, without the ket!

Every vector has an additive inverse for example, $|a\rangle$ and $-|a\rangle$ where adding these two will cancel out and give you the 0 vector

Examples

If $|a\rangle$ is a vector then c, which is an arbitrary complex number, $|a\rangle$ is a vector in space

If $|a\rangle$ and $|b\rangle$ are in vector space, then c$|a\rangle$ + d$|b\rangle$ is in space for all c and d

4 Orthogonal and Perpendicular 1/15

We will discuss linear independence first:

4.1 Linear independence

Definition

We have a set

$$\{|v\rangle\}, i = 1, 2, n$$

This is linearly independent iff, the Linear Combination:

$$|v\rangle = c_1|v_1\rangle + c_2|v_2\rangle \dots c_N|v_N\rangle$$

Example

If

$$c_1|v_1\rangle + c_2|v_2\rangle \cdots + c_N|v_N\rangle = 0$$

and at least one of the c's is not zero (and none of the $|v_i\rangle$, is the zero vector), then:
The set $\{|v_i\rangle\}$ cannot be linearly independent
If you were to move v_1 to the other side

$$|v_1\rangle = \frac{-1}{c_1}(c_2|v_2\rangle + \cdots + c_N|v_N\rangle)$$

meaning that they are not linearly independent (?)

Let's try another example

Example

$\hat{i}, \hat{j}$ a basis for on the board

If we have

$$\vec{v} = 2\hat{i} + \hat{j} = 2\hat{i} + 1\hat{j} \doteq \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

Where $\hat{i}$ is our "x" and $\hat{j}$ is our "y"

Example

A real 2-d vector has components $\begin{pmatrix}2\\1\end{pmatrix}$ in the usual basis, that is:

$$\vec{v} = 2\hat{i} + \hat{j} \dots$$

In a different basis $\vec{v_1} = \hat{i}, \vec{v_2} = \hat{i} + \hat{j}$, the components of $\vec{v}$ are:

$$\begin{pmatrix}1\\1\end{pmatrix}$$

This is because,

$$\vec{v} = 1\vec{v_1} + 1\vec{v_2} = 2\hat{i} + \hat{j}$$

Which is able to give us $\begin{pmatrix}1\\1\end{pmatrix}$ as this is the **components** of the given $\vec{v}$

4.2 Inner Products

Definition

Defining inner product where these two vectors:

$$\vec{v_1}, \vec{v_2}$$

Is given as $\langle v_1 | v_2 \rangle$

Moreover, if we are given the conditions that:

$$|A\rangle = C_1|v_1\rangle + C_2|v_2\rangle$$

Then $\langle B|A\rangle$ will equal:

$$C_1\langle B|v_1\rangle + C_2\langle B|v_2\rangle$$

Moreover, $\langle A|B_1\rangle = \langle B|A\rangle^* \Rightarrow \langle A|A\rangle$ is real
and

$$\langle A|A\rangle \geq 0$$

only if $|A\rangle = 0$

4.3 Orthogonal Basis

Orthogonal Basis is where $\{|e_i\rangle\}, i = 1, 2, \ldots, N$ And this is true if the inner product,

$$\langle e_i|e_j\rangle = 0 \; \forall \; i \neq j$$

and

$$\langle e_i|e_j\rangle = 1 \; \forall \; i$$

Example

$$|v\rangle = C_1|e_1\rangle + C_2|e_2\rangle + \cdots + C_N|e_N\rangle$$

Where $\langle e_i|v\rangle = C_i$

$$\vec{A} = A_x\hat{i} + A_y\hat{j}$$

Where $A_x = \hat{i} * A$ and $A_y = \hat{j} * A$

Furthermore,

$$|A\rangle = a_1|e_1\rangle + .. + a_n|e_N\rangle$$

$$|B\rangle = b_1|e_1\rangle + .. + b_n|e_N\rangle$$

$$\langle A|B\rangle = (a_1^*\langle e_1| + \cdots + a_N^*\langle e_N|)(b_1^*|e_1\rangle + \cdots + b_N^*|e_N\rangle)$$

But you can always write the inner product as

$$a_1^*b_1 + a_2^*b_2 + \cdots + a_n^*b_n$$

The "bra," $\langle e_1|$ for example, of the "ket", is not something to worry about but rather to expand out

5 Probability 1/17

Recap

Remember that when:

$$|a\rangle = a_1 |e_1\rangle + a_2 |e_2\rangle$$

Then:

$$\langle A|B\rangle = a_1^* \langle e_1|B\rangle + a_2^* \langle e_2|B\rangle$$

Where * is the complex conjugate
Any number multiplied by its complex conjugate is a **positive** number

Moreover, we can see with the given matrices:

$$|A\rangle \doteq \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix}$$

$$|B\rangle \doteq \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix}$$

We see that the inner product of the two is:

$$\langle A|B\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \dots & b_N \end{pmatrix} = a_1^* b_1 + a_n^* b_n$$

Now lets get back to probability:

Recap

Go back with $\hat{p}$ and $\hat{P}$, We know that the probability of the photons getting through is, linear polarization

$$(\hat{p} * \hat{P})^2$$

Definition

Lets all of them through

$$|U\rangle$$

Where $|U\rangle$ is some sort of photon state that always "goes through"

If $|v\rangle$ is like $\hat{p}$ then $|U\rangle$ is similar to $\hat{P}$
And

$$|U_\perp\rangle$$

Is the state where it doesn't "go through"
Where

$$\langle U|U_\perp\rangle = 0$$

Shows us that it must be perpendicular ALWAYS

$$|v\rangle = \alpha\,|U\rangle + \beta\,|U_\perp\rangle$$

Thus, the probability of being $|U\rangle$ after the measurement Is

$$|\,\langle U|v\rangle\,|^2 = |\alpha|^2$$

And probability of being on $|U_\perp\rangle$ is

$$|\,\langle U_\perp|v\rangle\,|^2 = |\beta|^2$$

Therefore,

$$|\alpha|^2 + |\beta|^2 = 1 \iff |v\rangle$$

Where $|v\rangle$ must be a unit vector

So once you "collapse" the state vector, $|v\rangle$, then it is either $|U\rangle$ or $|U_\perp\rangle$, one part of it is simply gone

Definition

Say we have a quantum computer with 3 qubits, where

$$|w_0\rangle \longrightarrow a\,|000\rangle + b\,|001\rangle + c\,|010\rangle \cdots + \cdots + h\,|111\rangle$$

Therefore, since each coefficient, i.e. a, b, c, etc., have the same probability or different probabilities, you have to arrange gates to make it so that those wrong coefficients are very small or 0

Example

Suppose a photon has polarization state

$$|\psi\rangle = \sqrt{\frac{1}{3}}\,|\rightarrow\rangle + \sqrt{\frac{2}{3}}\,|\uparrow\rangle$$

The probability that the photon will be reflected and observed on the "incoming" side of a horizontally oriented polaroid is:

$$\frac{2}{3}$$

As the inner product of:

$$\langle rightarrow|X\rangle = \sqrt{\frac{1}{3}}$$

Therefore, the P(go through) $= \frac{1}{3}$ and P(reflected) $= \frac{2}{3}$

Example

Suppose

$$|\psi\rangle = \sqrt{\frac{1}{3}}\,|\rightarrow\rangle + \sqrt{\frac{2}{3}}\,|\uparrow\rangle$$

The probability that the photon will be reflected and observed on the "incoming" side of a polaroid oriented at +45 deg with respect to the horizontal is: Answer:

$$|\psi\rangle \doteq \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \sqrt{\frac{2}{3}} \end{pmatrix}$$

Since its reflected, we are interested in the -45 sin state thus

$$|\searrow\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Then:

$$|\langle\searrow|\psi\rangle|^2 = [\begin{pmatrix} \frac{1}{\sqrt{3}} \\ \frac{2}{\sqrt{3}} \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}]^2 = (\frac{1}{\sqrt{6}} - \sqrt{\frac{2}{6}})^2 = \frac{1}{6} + \frac{1}{3} - \frac{2\sqrt{2}}{6} = \frac{3-2\sqrt{2}}{6}$$

6 Modern Cryptography 1/22

Recap

Recall that

$$|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + i\,|\rightarrow\rangle)$$

And that

$$P(\nearrow) = |\,\langle\nearrow\,|\,\circlearrowleft\rangle\,|^2$$

Where their values are:

$$|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}$$

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}$$

Giving us:

$$\langle\nearrow\,|\,\circlearrowleft\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix} = \frac{1}{2}(1+i)$$

Therefore,

$$P(\nearrow) = \frac{1}{4}(1+i)(1-i) = \frac{1}{2}$$

If I have a normalized state,

$$|\psi\rangle$$

Then it will be the same as

$$e^{i\theta}\,|\psi\rangle$$

Which is also a normalized same quantum state

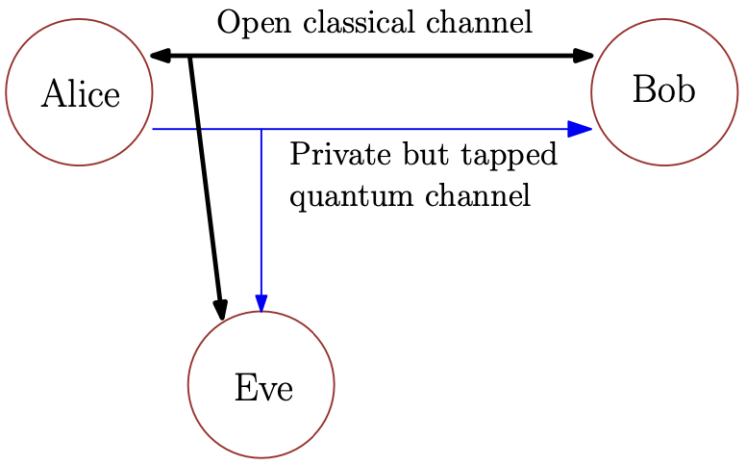
Example

$$a\,|\uparrow\rangle + b\,|\rightarrow\rangle$$

Is not the same as physically

$$a\,|\uparrow\rangle + be^{ie}\,|\rightarrow\rangle$$

Quantum communications or Quantum Key Protocol: Lets say, we want two people to communicate with each other, Alice and Bob. If they want to send a message to each other here is the diagram for that:



Moreover, we have two basis or encodings for these bits: Hadamard or Computation Basis to create a binary string

$$\begin{aligned} |0\rangle &\longrightarrow |\uparrow\rangle \\ |1\rangle &\longrightarrow |\rightarrow\rangle\,, \end{aligned} \tag{2.5.1}$$

and the "Hadamard basis:"

$$\begin{aligned} |0\rangle &\longrightarrow |\nearrow\rangle \\ |1\rangle &\longrightarrow |\nwarrow\rangle\,. \end{aligned} \tag{2.5.2}$$

It will only measure in the same basis, meaning that if they had the incorrect basis, then they would have to throw it away if it is incorrect basis

Getting it wrong If, for example, Eve is unaware of what basis Alice and Bob are communicating in, then they would disagree with the final result as Eve has interrupted the communications and changed the string

Example

Suppose Eve is intercepting Alice's qubits, measuring them in whichever of the two bases she guesses, and forwarding the measured qubit on to Bob. For what fraction of the qubits will Alice and Bob get different values, even though they measure in the same basis.

The answer of this is: $\frac{1}{4}$ as there is a $\frac{1}{2}$ chance of getting the right bases and then there is another $\frac{1}{2}$ prob of getting the photons are right after if it is the wrong basis