## Intro to Quantum Computing I

Prepared by Mark on February 19, 2024

## Part 1: Probabilistic Bits

## Definition 1:

As we already know, a classical bit may take the values 0 and 1 .
We can model this with a two-sided coin, one face of which is labeled 0 , and the other, 1.
Of course, if we toss such a "bit-coin," we'll get either 0 or 1.
We'll denote the probability of getting 0 as $p_{0}$, and the probability of getting 1 as $p_{1}$.
As with all probabilities, $p_{0}+p_{1}$ must be equal to 1 .

## Definition 2:

Say we toss a "bit-coin" and don't observe the result. We now have a probabilistic bit, with a probability $p_{0}$ of being 0 , and a probability $p_{1}$ of being 1 .
We'll represent this probabilistic bit's state as a vector: $\left[\begin{array}{l}p_{0} \\ p_{1}\end{array}\right]$
We do not assume this coin is fair, and thus $p_{0}$ might not equal $p_{1}$.
This may seem a bit redundant: since $p_{0}+p_{1}$, we can always calculate one probability given the other.
We'll still include both probabilities in the state vector, since this provides a clearer analogy to quantum bits.

## Definition 3:

The simplest probabilistic bit states are of course [0] and [1], defined as follows:

- $[0]=\left[\begin{array}{l}1 \\ 0\end{array}\right]$
- $[1]=\left[\begin{array}{l}0 \\ 1\end{array}\right]$

That is, [0] represents a bit that we known to be 0 , and [1] represents a bit we know to be 1.

## Definition 4:

[0] and [1] form a basis for all possible probabilistic bit states:
Every other probabilistic bit can be written as a linear combination of [0] and [1]:

$$
\left[\begin{array}{l}
p_{0} \\
p_{1}
\end{array}\right]=p_{0}\left[\begin{array}{l}
1 \\
0
\end{array}\right]+p_{1}\left[\begin{array}{l}
0 \\
1
\end{array}\right]=p_{0}[0]+p_{1}[1]
$$

## Problem 5:

Every possible state of a probabilistic bit is a two-dimensional vector.
Draw all possible states on the axis below.


## Part 2: Measuring Probabilistic Bits

## Definition 6:

As we noted before, a probabilistic bit represents a coin we've tossed but haven't looked at.
We do not know whether the bit is 0 or 1 , but we do know the probability of both of these outcomes.
If we measure (or observe) a probabilistic bit, we see either 0 or 1 -and thus our knowledge of its state is updated to either [0] or [1], since we now certainly know what face the coin landed on.

Since measurement changes what we know about a probabilistic bit, it changes the probabilistic bit's state. When we measure a bit, it's state collapses to either [0] or [1], and the original state of the bit vanishes. We cannot recover the state $\left[x_{0}, x_{1}\right]$ from a measured probabilistic bit.

## Definition 7: Multiple bits

Say we have two probabilistic bits, $x$ and $y$, with states $[x]=\left[x_{0}, x_{1}\right]$ and $[y]=\left[y_{0}, y_{1}\right]$

The compound state of $[x]$ and $[y]$ is exactly what it sounds like:
It is the probabilistic two-bit state $|x y\rangle$, where the probabilities of the first bit are determined by $[x]$, and the probabilities of the second are determined by $[y]$.

## Problem 8:

Say $[x]=[2 / 3,1 / 3]$ and $[y]=[3 / 4,1 / 4]$.

- If we measure $x$ and $y$ simultaneously, what is the probability of getting each of $00,01,10$, and 11 ?
- If we measure $y$ first and observe 1 , what is the probability of getting each of $00,01,10$, and 11 ?
Note: $[x]$ and $[y]$ are column vectors, but I've written them horizontally to save space.


## Problem 9:

Say $[x]=[2 / 3,1 / 3]$ and $[y]=[3 / 4,1 / 4]$.
What is the probability that $x$ and $y$ produce different outcomes?

## Part 3: Tensor Products

## Definition 10: Tensor Products

The tensor product of two vectors is defined as follows:

$$
\left[\begin{array}{l}
x_{1} \\
x_{2}
\end{array}\right] \otimes\left[\begin{array}{l}
y_{1} \\
y_{2}
\end{array}\right]=\left[\begin{array}{l}
x_{1}\left[\begin{array}{l}
y_{1} \\
y_{2}
\end{array}\right] \\
x_{2}\left[\begin{array}{l}
y_{1} \\
y_{2}
\end{array}\right]
\end{array}\right]=\left[\begin{array}{l}
x_{1} y_{1} \\
x_{1} y_{2} \\
x_{2} y_{1} \\
x_{2} y_{2}
\end{array}\right]
$$

That is, we take our first vector, multiply the second vector by each of its components, and stack the result. You could think of this as a generalization of scalar mulitiplication, where scalar mulitiplication is a tensor product with a vector in $\mathbb{R}^{1}$ :

$$
a\left[\begin{array}{l}
x_{1} \\
x_{2}
\end{array}\right]=\left[a_{1}\right] \otimes\left[\begin{array}{l}
y_{1} \\
y_{2}
\end{array}\right]=\left[a_{1}\left[\begin{array}{l}
y_{1} \\
y_{2}
\end{array}\right]\right]=\left[\begin{array}{l}
a_{1} y_{1} \\
a_{1} y_{2}
\end{array}\right]
$$

## Problem 11:

Say $x \in \mathbb{R}^{n}$ and $y \in \mathbb{R}^{m}$.
What is the dimension of $x \otimes y$ ?

## Problem 12:

What is the pairwise tensor product $\left\{\left[\begin{array}{l}1 \\ 0 \\ 0\end{array}\right],\left[\begin{array}{l}0 \\ 1 \\ 0\end{array}\right],\left[\begin{array}{l}0 \\ 0 \\ 1\end{array}\right]\right\} \otimes\left\{\left[\begin{array}{l}1 \\ 0\end{array}\right],\left[\begin{array}{l}0 \\ 1\end{array}\right]\right\}$ ?
in other words, distribute the tensor product between every pair of vectors.

## Problem 13:

What is the span of the vectors we found in Problem 12 ?
In other words, what is the set of vectors that can be written as linear combinations of the vectors above?

## Problem 14:

Say $[x]=[2 / 3,1 / 3]$ and $[y]=[3 / 4,1 / 4]$.
What is $[x] \otimes[y]$ ? How does this relate to Problem 8?

## Problem 15:

The compound state of two vector-form bits is their tensor product.
Compute the following. Is the result what we'd expect?

- $[0] \otimes[0]$
- $[0] \otimes[1]$
- [1] $\otimes[0]$
- $[1] \otimes[1]$

Hint: Remember that $[0]=\left[\begin{array}{l}1 \\ 0\end{array}\right]$ and $[1]=\left[\begin{array}{l}0 \\ 1\end{array}\right]$.

## Problem 16:

Of course, writing $[0] \otimes[1]$ is a bit excessive. We'll shorten this notation to [01].
In fact, we could go further: if we wanted to write the set of bits $[1] \otimes[1] \otimes[0] \otimes[1]$, we could write [1101] - but a shorter alternative is [13], since 13 is 1101 in binary.
Write [5] as three-bit probabilistic state.

## Problem 17:

Write the three-bit states [0] through [7] as column vectors.
Hint: You do not need to compute every tensor product. Do a few and find the pattern.

## Part 4: Operations on Probabilistic Bits

Now that we can write probabilistic bits as vectors, we can represent operations on these bits with linear transformations - in other words, as matrices.

## Definition 18:

Consider the NOT gate, which operates as follows:

- $\operatorname{NOT}[0]=[1]$
- $\mathrm{NOT}[1]=[0]$

What should NOT do to a probabilistic bit $\left[x_{0}, x_{1}\right]$ ?
If we return to our coin analogy, we can think of the NOT operation as flipping a coin we have already tossed, without looking at its state. Thus,

$$
\operatorname{NOT}\left[\begin{array}{l}
x_{0} \\
x_{1}
\end{array}\right]=\left[\begin{array}{l}
x_{1} \\
x_{0}
\end{array}\right]
$$

## Review: Matrix Multiplication

Matrix multiplication works as follows:

$$
A B=\left[\begin{array}{ll}
1 & 2 \\
3 & 4
\end{array}\right]\left[\begin{array}{ll}
a_{0} & b_{0} \\
a_{1} & b_{1}
\end{array}\right]=\left[\begin{array}{ll}
1 a_{0}+2 a_{1} & 1 b_{0}+2 b_{1} \\
3 a_{0}+4 a_{1} & 3 b_{0}+4 b_{1}
\end{array}\right]
$$

Note that this is very similar to multiplying each column of $B$ by $A$.
The product $A B$ is simply $A c$ for every column $c$ in $B$ :

$$
A c_{0}=\left[\begin{array}{ll}
1 & 2 \\
3 & 4
\end{array}\right]\left[\begin{array}{l}
a_{0} \\
a_{1}
\end{array}\right]=\left[\begin{array}{l}
1 a_{0}+2 a_{1} \\
3 a_{0}+4 a_{1}
\end{array}\right]
$$

This is exactly the first column of the matrix product.
Also, note that each element of $A c_{0}$ is the dot product of a row in $A$ and a column in $c_{0}$.

## Problem 19:

Compute the following product:

$$
\left[\begin{array}{cc}
1 & 0.5 \\
0 & 1
\end{array}\right]\left[\begin{array}{l}
3 \\
2
\end{array}\right]
$$

## Remark:

Also, recall that every matrix is linear map, and that every linear map may be written as a matrix. We often use the terms matrix, transformation, and linear map interchangably.

## Problem 20:

Find the matrix that represents the NOT operation on one probabilistic bit.

## Problem 21: Extension by linearity

Say we have an arbitrary operation $M$.
If we know how $M$ acts on [1] and [0], can we compute $M[x]$ for an arbitrary state $[x]$ ? Say $[x]=\left[x_{0}, x_{1}\right]$.

- What is the probability we observe 0 when we measure $x$ ?
- What is the probability that we observe $M[0]$ when we measure $M x$ ?


## Problem 22:

Write $M\left[x_{0}, x_{1}\right]$ in terms of $M[0], M[1], x_{0}$, and $x_{1}$.

## Remark:

Every matrix represents a linear map, so the following is always true:

$$
A \times(p x+q y)=p A x+q A y
$$

Problem 22 is just a special case of this fact.

## Part 5: One Qubit

Quantum bits (or qubits) are very similar to probabilistic bits, but have one major difference: probabilities are replaced with amplitudes.

Of course, a qubit can take the values 0 and 1 , which are denoted $|0\rangle$ and $|1\rangle$.
Like probabilistic bits, a quantum bit is written as a linear combination of $|0\rangle$ and $|1\rangle$ :

$$
|\psi\rangle=\psi_{0}|0\rangle+\psi_{1}|1\rangle
$$

Such linear combinations are called superpositions.
The $\rangle$ you see in the expressions above is called a "ket," and denotes a column vector. $|0\rangle$ is pronounced "ket zero," and $|1\rangle$ is pronounced "ket one." This is called bra-ket notation. Note: $\langle 0|$ is called a "bra," but we won't worry about that for now.
This is very similiar to the "box" [ ] notation we used for probabilistic bits.
As before, we will write $|0\rangle=\left[\begin{array}{l}1 \\ 0\end{array}\right]$ and $|1\rangle=\left[\begin{array}{l}0 \\ 1\end{array}\right]$.

Recall that probabilistic bits are subject to the restriction that $p_{0}+p_{1}=1$.
Quantum bits have a similar condition: $\psi_{0}^{2}+\psi_{1}^{2}=1$.
Note that this implies that $\psi_{0}$ and $\psi_{1}$ are both in $[-1,1]$.
Quantum amplitudes may be negative, but probabilistic bit probabilities cannot.
If we plot the set of valid quantum states on our plane, we get a unit circle centered at the origin:


Recall that the set of probabilistic bits forms a line instead:


## Problem 23:

In the above unit circle, the counterclockwise angle from $|0\rangle$ to $|\psi\rangle$ is 30 . Write $|\psi\rangle$ as a linear combination of $|0\rangle$ and $|1\rangle$.

## Definition 24: Measurement I

Just like a probabilistic bit, we must observed $|0\rangle$ or $|1\rangle$ when we measure a qubit. If we were to measure $|\psi\rangle=\psi_{0}|0\rangle+\psi_{1}|1\rangle$, we'd observe either $|0\rangle$ or $|1\rangle$, with the following probabilities:

- $\mathcal{P}(|1\rangle)=\psi_{1}^{2}$
- $\mathcal{P}(|0\rangle)=\psi_{0}^{2}$

Note that $\mathcal{P}(|0\rangle)+\mathcal{P}(|1\rangle)=1$.
As before, $|\psi\rangle$ collapses when it is measured: its state becomes that which we observed in our measurement, leaving no trace of the previous superposition.

## Problem 25:

- What is the probability we observe $|0\rangle$ when we measure $|\psi\rangle$ ?
- What can we observe if we measure $|\psi\rangle$ a second time?
- What are these probabilities for $|\varphi\rangle$ ?


As you may have noticed, we don't need two coordinates to fully define a quibit's state. We can get by with one coordinate just as well.
Instead of referring to each state using its cartesian coordinates $\psi_{0}$ and $\psi_{1}$, we can address it using its polar angle $\theta$, measured from $|0\rangle$ counterclockwise:


## Problem 26:

Find $\psi_{0}$ and $\psi_{1}$ in terms of $\theta$ for an arbitrary qubit $\psi$.

## Problem 27:

Consider the following qubit states:

- Where are these on the unit circle?
-What are their polar angles?
- What are the probabilities of observing $|0\rangle$ and $|1\rangle$ when measuring $|+\rangle$ and $|-\rangle$ ?



## Part 6: Operations on One Qubit

We may apply transformations to qubits just as we apply transformations to probabilistic bits. Again, we'll represent transformations as $2 \times 2$ matrices, since we want to map one qubit state to another. In other words, we want to map elements of $\mathbb{R}^{2}$ to elements of $\mathbb{R}^{2}$.
We will call such maps quantum gates, since they are the quantum equivalent of classical logic gates.
There are two conditions a valid quantum gate $G$ must satisfy:

- For any valid state $|\psi\rangle, G|\psi\rangle$ is a valid state.

Namely, $G$ must preserve the length of any vector it is applied to.
Recall that the set of valid quantum states is the set of unit vectors in $\mathbb{R}^{2}$

- Any quantum gate must be invertible.

We'll skip this condition for now, and return to it later.
In short, a quantum gate is a linear map that maps the unit circle to itself.
There are only two kinds of linear maps that do this: reflections and rotations.

## Problem 28:

The $X$ gate is the quantum analog of the not gate, defined by the following table:

- $X|0\rangle=|1\rangle$
- $X|1\rangle=|0\rangle$

Find the matrix $X$.

## Problem 29:

What is $X|+\rangle$ and $X|-\rangle$ ?
Hint: Remember that all matrices are linear maps. What does this mean?

## Problem 30:

In terms of geometric transformations, what does $X$ do to the unit circle?

## Problem 31:

Let $Z$ be a quantum gate defined by the following table:

- $Z|0\rangle=|0\rangle$,
- $Z|1\rangle=-|1\rangle$.

What is the matrix $Z$ ? What are $Z|+\rangle$ and $Z|-\rangle$ ?
What is $Z$ as a geometric transformation?

## Problem 32:

Is the map $B$ defined by the table below a valid quantum gate?

- $B|0\rangle=|0\rangle$
- $B|1\rangle=|+\rangle$

Hint: Find a $|\psi\rangle$ so that $B|\psi\rangle$ is not a valid qubit state

## Problem 33: Rotation

As we noted earlier, any rotation about the center is a valid quantum gate.
Let's derive all transformations of this form.

- Let $U_{\phi}$ be the matrix that represents a counterclockwise rotation of $\phi$ degrees. What is $U|0\rangle$ and $U|1\rangle$ ?
- Find the matrix $U_{\phi}$ for an arbitrary $\phi$.


## Problem 34:

Say we have a qubit that is either $|+\rangle$ or $|-\rangle$. We do not know which of the two states it is in. Using one operation and one measurement, how can we find out, for certain, which qubit we received?

## Part 7: Two Qubits

## Definition 35:

Just as before, we'll represent multi-quibit states as linear combinations of multi-qubit basis states. For example, a two-qubit state $|a b\rangle$ is the four-dimensional unit vector

$$
\left[\begin{array}{l}
a  \tag{1}\\
b \\
c \\
d
\end{array}\right]=a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle
$$

As always, multi-qubit states are unit vectors.
Thus, $a^{2}+b^{2}+c^{2}+d^{2}=1$ in the two-bit case above.
Problem 36:
Say we have two qubits $|\psi\rangle$ and $|\varphi\rangle$.
Show that $|\psi\rangle \otimes|\varphi\rangle$ is always a unit vector (and is thus a valid quantum state).

## Definition 37: Measurement II

Measurement of a two-qubit state works just like measurement of a one-qubit state:
If we measure $a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle$,
we get one of the four basis states with the following probabilities:

- $\mathcal{P}(|00\rangle)=a^{2}$
- $\mathcal{P}(|01\rangle)=b^{2}$
- $\mathcal{P}(|10\rangle)=c^{2}$
- $\mathcal{P}(|11\rangle)=d^{2}$

Of course, the sum of all the above probabilities is 1 .

## Problem 38:

Consider the two-qubit state $|\psi\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{2}|01\rangle+\frac{\sqrt{3}}{4}|10\rangle+\frac{1}{4}|11\rangle$

- If we measure both bits of $|\psi\rangle$ simultaneously, what is the probability of getting each of $|00\rangle,|01\rangle,|10\rangle$, and $|11\rangle$ ?
- If we measure the ONLY the first qubit, what is the probability we get $|0\rangle$ ? How about $|1\rangle$ ? Hint: There are two basis states in which the first qubit is $|0\rangle$.
- Say we measured the second bit and read $|1\rangle$.

If we now measure the first bit, what is the probability of getting $|0\rangle$ ?

## Problem 39:

Again, consider the two-qubit state $|\psi\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{2}|01\rangle+\frac{\sqrt{3}}{4}|10\rangle+\frac{1}{4}|11\rangle$
If we measure the first qubit of $|\psi\rangle$ and get $|0\rangle$, what is the resulting state of $|\psi\rangle$ ? What would the state be if we'd measured $|1\rangle$ instead?

## Problem 40:

Consider the three-qubit state $|\psi\rangle=c_{0}|000\rangle+c_{1}|001\rangle+\ldots+c_{7}|111\rangle$.
Say we measure the first two qubits and get $|00\rangle$. What is the resulting state of $|\psi\rangle$ ?

## Definition 41: Entanglement

Some product states can be factored into a tensor product of individual qubit states. For example,

$$
\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)
$$

Such states are called product states. States that aren't product states are called entangled states.

## Problem 42:

Factor the following product state:

$$
\frac{1}{2 \sqrt{2}}(\sqrt{3}|00\rangle-\sqrt{3}|01\rangle+|10\rangle-|11\rangle)
$$

## Problem 43:

Show that the following is an entangled state.

$$
\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle
$$

## Part 8: Logic Gates

## Definition 44: Matrices

Throughout this handout, we've been using matrices. Again, recall that every linear map may be written as a matrix, and that every matrix represents a linear map. For example, if $f: \mathbb{R}^{2} \rightarrow \mathbb{R}^{2}$ is a linear map, we can write it as follows:

$$
f(|x\rangle)=\left[\begin{array}{ll}
m_{1} & m_{2} \\
m_{3} & m_{4}
\end{array}\right]\left[\begin{array}{l}
x_{1} \\
x_{2}
\end{array}\right]=\left[\begin{array}{l}
m_{1} x_{1}+m_{2} x_{2} \\
m_{3} x_{1}+m_{4} x_{2}
\end{array}\right]
$$

## Definition 45:

Before we discussing multi-qubit quantum gates, we need to review to classical logic.
Of course, a classical logic gate is a linear map from $\mathbb{B}^{m}$ to $\mathbb{B}^{n}$

## Problem 46:

The not gate is a map from $\mathbb{B}$ to $\mathbb{B}$ defined by the following table:

- $X|0\rangle=|1\rangle$
- $X|1\rangle=|0\rangle$

Write the not gate as a matrix that operates on single-bit vector states.
That is, find a matrix $X$ so that $X\left[\begin{array}{l}1 \\ 0\end{array}\right]=\left[\begin{array}{l}0 \\ 1\end{array}\right]$ and $X\left[\begin{array}{l}0 \\ 1\end{array}\right]=\left[\begin{array}{l}1 \\ 0\end{array}\right]$

## Problem 47:

The and gate is a map $\mathbb{B}^{2} \rightarrow \mathbb{B}$ defined by the following table:

| a | b | a and b |
| :---: | :---: | :---: |
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

Find a matrix $A$ so that $A|\mathrm{ab}\rangle$ works as expected.

## Remark:

The way a quantum circuit handles information is a bit different than the way a classical circuit does. We usually think of logic gates as functions: they consume one set of bits, and return another:


This model, however, won't work for quantum logic. If we want to understand quantum gates, we need to see them not as functions, but as transformations. This distinction is subtle, but significant:

- functions consume a set of inputs and produce a set of outputs
- transformations change a set of objects, without adding or removing any elements

Our usual logic circuit notation models logic gates as functions-we thus can't use it. We'll need a different diagram to draw quantum circuits.

First, we'll need a set of bits. For this example, we'll use two, drawn in a vertical array.
We'll also add a horizontal time axis, moving from left to right:


In the diagram above, we didn't change our bits - so the labels at the start match those at the end.

Thus, our circuit forms a grid, with bits ordered vertically and time horizontally.
If we want to change our state, we draw transformations as vertical boxes.
Every column represents a single transformation on the entire state:


Note that the transformations above span the whole state. This is important:
we cannot apply transformations to individual bits-we always transform the entire state.

## Setup:

Say we want to invert the first bit of a two-bit state. That is, we want a transformation $T$ so that


In other words, we want a matrix $T$ satisfying the following equalities:

- $T|00\rangle=|10\rangle$
- $T|01\rangle=|11\rangle$
- $T|10\rangle=|00\rangle$
- $T|11\rangle=|01\rangle$


## Problem 48:

Find the matrix that corresponds to the above transformation.
Hint: Remember that $|0\rangle=\left[\begin{array}{l}1 \\ 0\end{array}\right]$ and $|1\rangle=\left[\begin{array}{l}0 \\ 1\end{array}\right]$
Also, we found earlier that $X=\left[\begin{array}{ll}0 & 1 \\ 1 & 0\end{array}\right]$, and of course $I=\left[\begin{array}{ll}1 & 0 \\ 0 & 1\end{array}\right]$.

## Remark:

We could draw the above transformation as a combination $X$ and $I$ (identity) gate:


We can even omit the $I$ gate, since we now know that transformations affect the whole state:

$$
\begin{aligned}
& |0\rangle-\boxed{X}-|1\rangle \\
& |0\rangle-|0\rangle
\end{aligned}
$$

We're now done: this is how we draw quantum circuits. Don't forget that transformations always affect the whole state - even if our diagram doesn't explicitly state this.

## Part 9: Quantum Gates

In the previous section, we stated that a quantum gate is a linear map. Let's complete that definition.

## Definition 49:

A quantum gate is a orthonormal matrix, which means any gate $G$ satisfies $G G^{\mathrm{T}}=I$.
This implies the following:

- $G$ is square

If we think of $G$ as a map, this means that $G$ has as many inputs as it has outputs.
This is to be expected: we stated earlier that quantum gates do not destroy or create qubits.

- $G$ preserves lengths; i.e $|x|=|G x|$.

This ensures that $G|\psi\rangle$ is always a valid state.
(You will prove all these properties in any introductory linear algebra course.
This isn't a lesson on linear algebra, so you may take them as given today.)

## Definition 50:

Let $\mathbb{U} \subset \mathbb{R}^{2}$ be the set of points in the unit circle.
We can restate the above definition as follows:
A quantum gate is an invertible map from $\mathbb{U}^{n}$ to $\mathbb{U}^{n}$.

## Definition 51:

Let $G$ be a quantum gate.
Since quantum gates are, by definition, linear maps, the following holds:

$$
G\left(a_{0}|0\rangle+a_{1}|1\rangle\right)=a_{0} G|0\rangle+a_{1} G|1\rangle
$$

## Problem 52:

Consider the controlled not (or cnot) gate, defined by the following table:

- $\mathrm{X}_{\mathrm{c}}|00\rangle=|00\rangle$
- $\mathrm{X}_{\mathrm{c}}|01\rangle=|01\rangle$
- $\mathrm{X}_{\mathrm{c}}|10\rangle=|11\rangle$
- $\mathrm{X}_{\mathrm{c}}|11\rangle=|10\rangle$

In other words, the cnot gate inverts its second bit if its first bit is $|1\rangle$.
Find the matrix that applies the cnot gate.

## Problem 53:

Evaluate the following:

$$
\mathrm{X}_{\mathrm{C}}\left(\frac{1}{2}|00\rangle+\frac{1}{2}|01\rangle-\frac{1}{2}|10\rangle-\frac{1}{2}|11\rangle\right)
$$

## Problem 54:

If we measure the result of Problem 53, what are the probabilities of getting each state?

## Problem 55:

Finally, modify the original cnot gate so that the roles of its bits are reversed: $\mathrm{X}_{\mathrm{c} \text {, flipped }}|a b\rangle$ should invert $|a\rangle$ iff $|b\rangle$ is $|1\rangle$.

## Definition 56:

The Hadamard Gate is given by the following matrix:

$$
H=\frac{1}{\sqrt{2}}\left[\begin{array}{cc}
1 & 1 \\
1 & -1
\end{array}\right]
$$

Note that we divide by $\sqrt{2}$, since $H$ must be orthonormal.

## Review: Matrix Multiplication

Matrix multiplication works as follows:

$$
A B=\left[\begin{array}{ll}
1 & 2 \\
3 & 4
\end{array}\right]\left[\begin{array}{ll}
a_{0} & b_{0} \\
a_{1} & b_{1}
\end{array}\right]=\left[\begin{array}{ll}
1 a_{0}+2 a_{1} & 1 b_{0}+2 b_{1} \\
3 a_{0}+4 a_{1} & 3 b_{0}+4 b_{1}
\end{array}\right]
$$

Note that this is very similar to multiplying each column of $B$ by $A$.
The product $A B$ is simply $A c$ for every column $c$ in $B$ :

$$
A c_{0}=\left[\begin{array}{ll}
1 & 2 \\
3 & 4
\end{array}\right]\left[\begin{array}{l}
a_{0} \\
a_{1}
\end{array}\right]=\left[\begin{array}{l}
1 a_{0}+2 a_{1} \\
3 a_{0}+4 a_{1}
\end{array}\right]
$$

This is exactly the first column of the matrix product.
Also, note that each element of $A c_{0}$ is the dot product of a row in $A$ and a column in $c_{0}$.

## Problem 57:

What is $H H$ ?
Using this result, find $H^{-1}$.

## Problem 58:

What geometric transformation does $H$ apply to the unit circle?
Hint: Rotation or reflection? How much, or about which axis?

## Problem 59:

What are $H|0\rangle$ and $H|1\rangle$ ?
Are these states entangled?

## Part 10: Bonus Problems (Putnam)

## Problem 60:

Suppose $A$ is a real, square matrix that satisfies $A^{3}=A+I$. Show that $\operatorname{det}(A)$ is positive.

## Problem 61:

Suppose $A, B$ are $2 \times 2$ complex matrices satisfying $A B=B A$, and assume $A$ is not of the form $a I$ for some complex $a$.
Show that $B=x A+y I$ for complex $x$ and $y$.

## Problem 62:

Is there an infinite sequence of real numbers $a_{1}, a_{2}, \ldots$ so that $a_{1}^{m}+a_{2}^{m}+\ldots=m$ for every positive integer $m$ ?

