Intro to Quantum Computing II

Prepared by Mark on February 22, 2024

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 $|ab\rangle$ is the four-dimensional unit vector

$$\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \tag{1}$$

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 $|\psi\rangle = c_0|000\rangle + c_1|001\rangle + ... + c_7|111\rangle$.
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,

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

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

Problem 42:
Factor the following product state:

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

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 $f : \mathbb{R}^2 \to \mathbb{R}^2$ is a linear map, we can write it as follows:

$$f\left(|x\rangle\right) = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} m_1x_1 + m_2x_2 \\ m_3x_1 + m_4x_2 \end{bmatrix}$$

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:

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

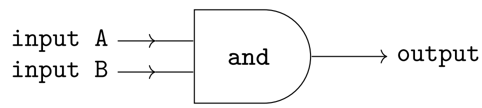
Write the `not` gate as a matrix that operates on single-bit vector states.
That is, find a matrix X so that $X\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$ and $X\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right] = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$

Problem 47:
The `and` gate is a map $\mathbb{B}^2 \to \mathbb{B}$ 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 $A\,|\texttt{ab}\rangle$ 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:

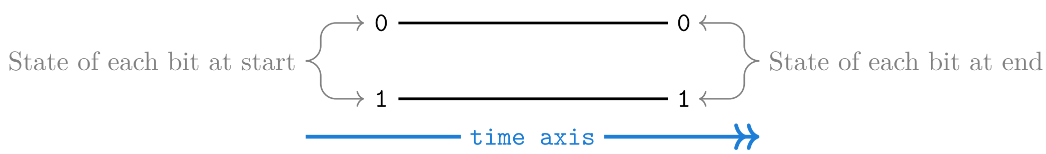


This model, however, won't work for quantum logic. If we want to understand quantum gates, we need to see them not as *functions*, but as *transformations*. This distinction is subtle, but significant:

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

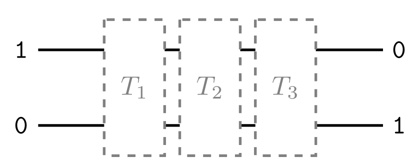
Our usual logic circuit notation models logic gates as functions—we thus can't use it.
We'll need a different diagram to draw quantum circuits.

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:



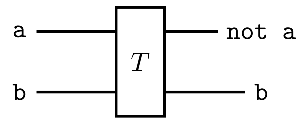
In the diagram above, we didn't change our bits—so the labels at the start match those at the end.

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

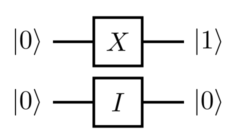


In other words, we want a matrix T satisfying the following equalities:

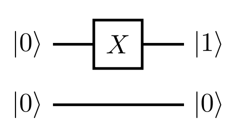
- $T\,|00\rangle = |10\rangle$
- $T\,|01\rangle = |11\rangle$
- $T\,|10\rangle = |00\rangle$
- $T\,|11\rangle = |01\rangle$

Problem 48:
Find the matrix that corresponds to the above transformation.
Hint: Remember that $|0\rangle = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $|1\rangle = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$
Also, we found earlier that $X = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$, and of course $I = \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$.

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:



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 $GG^{\mathrm{T}} = I$.
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 $|x| = |Gx|$.
  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:

$$G\big(a_0\,|0\rangle + a_1\,|1\rangle\big) = a_0 G\,|0\rangle + a_1 G\,|1\rangle$$

Problem 52:
Consider the *controlled not* (or *cnot*) gate, defined by the following table:

- $\mathrm{X_c}\,|00\rangle = |00\rangle$
- $\mathrm{X_c}\,|01\rangle = |01\rangle$
- $\mathrm{X_c}\,|10\rangle = |11\rangle$
- $\mathrm{X_c}\,|11\rangle = |10\rangle$

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:

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

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:
$\mathrm{X}_{\text{c, flipped}}\,|ab\rangle$ should invert $|a\rangle$ iff $|b\rangle$ is $|1\rangle$.

Definition 56:
The *Hadamard Gate* is given by the following matrix:

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

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

Review: Matrix Multiplication

Matrix multiplication works as follows:

$$AB = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a_0 & b_0 \\ a_1 & b_1 \end{bmatrix} = \begin{bmatrix} 1a_0 + 2a_1 & 1b_0 + 2b_1 \\ 3a_0 + 4a_1 & 3b_0 + 4b_1 \end{bmatrix}$$

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

$$Ac_0 = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} 1a_0 + 2a_1 \\ 3a_0 + 4a_1 \end{bmatrix}$$

This is exactly the first column of the matrix product.
Also, note that each element of Ac_0 is the dot product of a row in A and a column in c_0.

Problem 57:
What is HH?
Using this result, find H^{-1}.

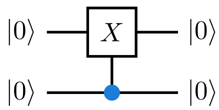
Problem 58:
What geometric transformation does H apply to the unit circle?
Hint: Rotation or reflection? How much, or about which axis?

Problem 59:
What are $H\left|0\right\rangle$ and $H\left|1\right\rangle$?
Are these states entangled?

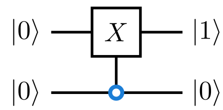
Part 10: HXH

Let's return to the quantum circuit diagrams we discussed a few pages ago.
Keep in mind that we're working with quantum gates and proper half-qubits—not classical bits, as we were before.

Definition 60: Controlled Inputs
A *control input* or *inverted control input* may be attached to any gate.
These are drawn as filled and empty circles in our circuit diagrams:



Non-inverted control input



Inverted control input

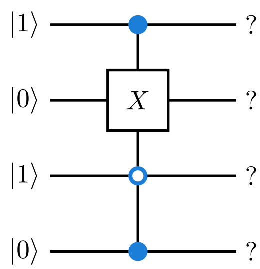
An X gate with a (non-inverted) control input behaves like an X gate if *all* its control inputs are $|1\rangle$, and like I otherwise. An X gate with an inverted control inputs does the opposite, behaving like I if its input is $|1\rangle$ and like X otherwise. The two circuits above illustrate this fact—take a look at their inputs and outputs.

Of course, we can give a gate multiple controls.
An X gate with multiplie controls behaves like an X gate if...

- all non-inverted controls are $|1\rangle$, and
- all inverted controls are $|0\rangle$

...and like I otherwise.

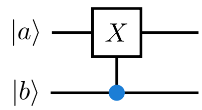
Problem 61:
What are the final states of the qubits in the diagram below?



Problem 62:

Consider the diagram below, with one controlled X gate:

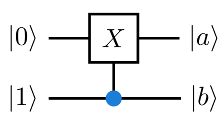
Note: The CNOT gate from Problem 52 is a controlled X gate.

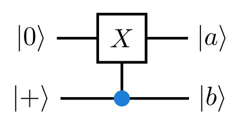


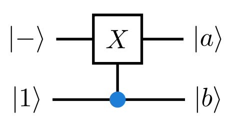
Find a matrix X_c that represents this gate, so that $\text{X}_\text{c} |ab\rangle$ works as expected.

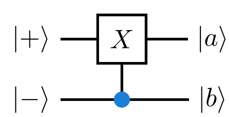
Problem 63:

Now, evaluate the following. Remember that $|+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)$ and $|-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big)$







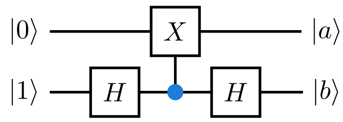


Hint: Note that some of these states are entangled. The circuit diagrams are a bit misleading: we can't write an entangled state as two distinct qubits!

So, don't try to find $|a\rangle$ and $|b\rangle$.

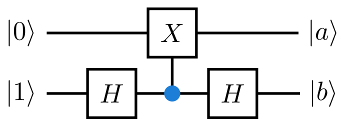
Instead find $|ab\rangle = \psi_0 |00\rangle + \psi_1 |01\rangle + \psi_2 |10\rangle + \psi_3 |11\rangle$, and factor it into $|a\rangle \otimes |b\rangle$ if you can.

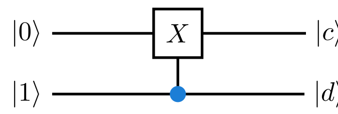
Remark:
Now, consider the following circuit:



We already know that H is its own inverse: $HH = I$.
Applying H to a qubit twice does not change its state.
Recall that $H = \frac{1}{\sqrt{2}} \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$

So, we might expect that the two circuits below are equivalent:
After all, we H the second bit, use it to control an X gate, and then H it back to its previous state.

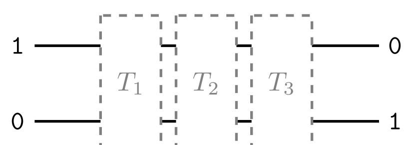




This, however, isn't the case:
If we compute the state $|ab\rangle$ in the left circuit, we get $[0.5,\ 0.5, -0.5,\ 0.5]$ (which is entangled),
but the state $|cd\rangle$ on the right is $|11\rangle = [0, 0, 0, 1]$.
This is easy to verify with a few matrix multiplications.

How does this make sense?
Remember that a two-bit quantum state is *not* equivalent to a pair of one-qubit quantum states. We must treat a multi-qubit state as a single unit.
Recall that a two-bit state $|ab\rangle$ comes with four probabilities: $\mathcal{P}(\texttt{00})$, $\mathcal{P}(\texttt{01})$, $\mathcal{P}(\texttt{10})$, and $\mathcal{P}(\texttt{11})$. If we change the probabilities of only $|a\rangle$, *all four of these change!*

Because of this fact, "controlled gates" may not work as you expect. They may seem to "read" their controlling qubit without affecting its state, but remember—a controlled gate still affects the *entire* state. As we noted before, it is not possible to apply a transformation to one bit of a quantum state.



Part 11: Superdense Coding

Consider the following entangled two-qubit states, called the *bell states*:

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$
- $|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$
- $|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

Problem 64:
The probabilistic bits we get when measuring any of the above may be called *anticorrelated bits*.
If we measure the first bit of any of these states and observe 1, what is the resulting compound state?
What if we observe 0 instead?
Do you see why we can call these bits anticorrelated?

Problem 65:
Show that the bell states are orthogonal
Hint: Dot product

Problem 66:
Say we have a pair of qubits in one of the four bell states.
How can we find out which of the four states we have, with certainty?
Hint: $H|+\rangle = |0\rangle$, and $H|-\rangle = |1\rangle$

Definition 67:
The Z gate is defined as follows:

$$Z \begin{bmatrix} \psi_0 \\ \psi_1 \end{bmatrix} = \begin{bmatrix} \psi_0 \\ -\psi_1 \end{bmatrix}$$

Problem 68:
Suppose that Alice and Bob are each in possession of one qubit.
These two qubits are entangled, and have the compound state $|\Phi^+\rangle$.
How can Alice send a two-bit classical state (i.e, one of the four values `00`, `01`, `10`, `11`) to Bob by only sending one qubit?

Remark:
Superdense coding consumes a pre-shared entangled pair to transmit two bits of information. This entanglement may *not* be re-used—it is destroyed when Bob measures the final qubit states.

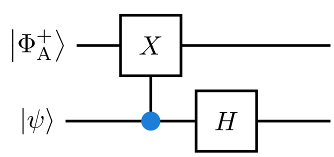
Part 12: Quantum Teleportation

Superdense coding lets us convert quantum bandwidth into classical bandwidth.
Quantum teleporation does the opposite, using two classical bits and an entangled pair to transmit a quantum state.

Setup:
Again, suppose Alice and Bob each have half of a $|\Phi^+\rangle$ state.
We'll call the state Alice wants to teleport $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$.

Problem 69:
What is the three-qubit state $|\psi\rangle |\Phi^+\rangle$ in terms of ψ_0 and ψ_1?

Problem 70:
To teleport $|\psi\rangle$, Alice applies the following circuit to her two qubits, where $\left|\Phi^+_{\mathrm{A}}\right\rangle$ is her half of $|\Phi^+\rangle$.
She then measures both qubits and sends the result to Bob.



What should Bob do so that $\left|\Phi^+_B\right\rangle$ takes the state $|\psi\rangle$ had initially?

Problem 71:
With an informal proof, show that it is not possible to use superdense coding to send more than two classical bits through an entangled two-qubit quantum state.