Matrices in Quantum Computing

A 2-qubit Entangler Circuit

Huan Q. Bui

Colby College CLAS 2019

PHYSICS & MATHEMATICS
Statistics

Class of 2021

April 29, 2019

1 Introduction

Quantum computing and quantum information science are rapidly growing fields in recent years. Progress is made everyday in not only in the physics labs but also in the mathematical foundation, most of which is linear algebra. The matrix theory behind quantum computing is voluminous, and thus it would be insane for me to talk about all kinds of matrices in quantum computing. So today, I would like to draw your attention to one of the simplest and basic yet interesting circuits in all of quantum computing: the 2-qubit entanglement circuit, and some of the matrix theory behind it.

$$a : |0\rangle \quad \oplus \quad \text{[measure]}$$
$$b : |0\rangle \quad \boxed{H} \quad \bullet \quad \text{[measure]}$$
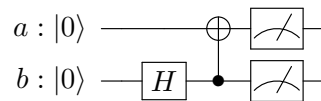
2 Presentation layout

Here's my plan for this presentation. I will

1. first provide some background on quantum computing. I will introduce some of the basic objects in quantum computing such as qubits, quantum circuits, quantum gates, and entanglement.

2. And as I introduce these objects, the mathematical concepts of the Kronecker product and tensor product will come up, as they are the building blocks of the theory of quantum computation. I will talk about what these matrix theories are, how they work, and, time permitting, "why" they are required.

3. Then, we will walkthrough the 2-qubit entanglement circuit that I have just shown. We will see how the tensor product appears and how we can use it "see" what the circuit actually does.

4. Finally, I will show how you can actually implement this circuit (or any other circuit) on your browser and have an actual quantum computer at IBM execute the commands.

3 Qubits

So let us start with qubits. Qubits are kind of like classical bits, but not really. Classical bits can take values of only 0 and 1, "on" or "off", "up" or "down," while quantum bits can take any "superposition" of those two states, since qubits are quantum mechanical objects.

Most of the time, qubits are individual atoms that can be excited to the excited state or de-excited into the ground state. Mathematically, we can think

Classical Bit **Qubit**
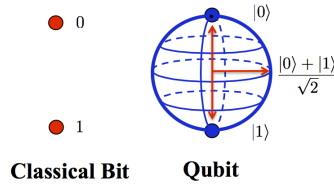
of these states as forming a basis for the space of all possible states of the atom, and the state of a qubit can be represented by the following linear combination:

$$a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

where $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ represents the ground state, and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ represents the excited state. The coefficients a, b are complex numbers such that the sum of the modulus squares is one:

$$|a|^2 + |b|^2 = 1,$$

the reason being, in quantum mechanics, it is require that the magnitude of the state vector is 1. In fact, in physics, it is often interpreted that $|a|^2$ is the probability of the qubit being in the ground state, and $|b|$ is the probability of the qubit being in the excited state.

Now, before we move on, for the sake of convenience, let us introduce a new notation for the basis states of a qubit. Let $|0\rangle$ represent the vector $\begin{bmatrix} 1 & 0 \end{bmatrix}^\top$ and $|1\rangle$ represent the vector $\begin{bmatrix} 0 & 1 \end{bmatrix}^\top$. The reason for doing this is that now we can just call the ground state the "zero" state and excited state the "one" state, giving us a nice way to relate the basis values of a classical bit. So, the state of single qubit can be written as

$$a |0\rangle + b |1\rangle.$$

4 Quantum gates

Another fundamental object in quantum computing is quantum gates. If we think of states of qubits as vectors, then quantum gates are modeled by linear transformations - matrices - on the state vectors of qubits. For example, one of the most common and important single-qubit quantum gates, is called the Hadamaar gate, which is in matrix form is

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

This gate is actually the first component on the quantum circuit we have seen:
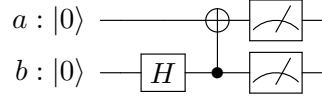
The Hadamaar gate is denoted with an H. We can see what H does to, say $|0\rangle$:

$$H\left|0\right\rangle = H\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix},$$

which we can equivalently write as

$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{2}\left|1\right\rangle.$$

So what the Hadamaar gate does is putting a pure state into a perfect superposition, with exactly 50% chance of finding the qubit either state $|0\rangle$ or $|1\rangle$.

5 Multiple qubits

Like classical circuits, quantum circuits require multiple qubits to operate. And so a natural question to ask now is how do we represent the quantum state of 2-qubits with the same vector. Let us say that the qubit 1 has state

$$a\left|0\right\rangle + b\left|1\right\rangle = \begin{bmatrix}a\\b\end{bmatrix}$$

and qubit 2 has state

$$c\left|0\right\rangle + d\left|1\right\rangle = \begin{bmatrix}c\\d\end{bmatrix}.$$

It is clear that we can neither add, nor "multiply" these "pairs" in any traditional way in order to get a vector of unit length. It turns out that if we do the following seemingly "magical" multiplication procedure,

$$\begin{bmatrix}a\\b\end{bmatrix} \boxtimes \begin{bmatrix}c\\d\end{bmatrix} = \begin{bmatrix}a\begin{bmatrix}c\\d\end{bmatrix}\\b\begin{bmatrix}c\\d\end{bmatrix}\end{bmatrix} = \begin{bmatrix}ac\\ad\\bc\\bd\end{bmatrix}.$$

We can check quite easily that this new vector has unit length. Applying this procedure to the basis states $|0\rangle$, $|1\rangle$, we actually get a basis for the vector space that contains all possible quantum states of two qubits:

$$\left|0\right\rangle \boxtimes \left|0\right\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \left|0\right\rangle \boxtimes \left|1\right\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \left|1\right\rangle \boxtimes \left|0\right\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \left|1\right\rangle \boxtimes \left|1\right\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix},$$

and so it is convenient for us to write

$$|00\rangle = |0\rangle \boxtimes |0\rangle$$
$$|01\rangle = |0\rangle \boxtimes |1\rangle$$
$$|10\rangle = |1\rangle \boxtimes |0\rangle$$
$$|11\rangle = |1\rangle \boxtimes |1\rangle$$

where the first slot indicates the (pure) state of the first qubit, and the second slot indicates the (pure) state of the second qubit. And so it is not so hard to see that

$$\begin{bmatrix} a \\ b \end{bmatrix} \boxtimes \begin{bmatrix} c \\ d \end{bmatrix} = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle\,.$$

6 Caveat 1

With this, we can see that given two qubits with defined states, this "product" always gives us a new two-qubit joint state, and we call this joint state **elementary**. Now, we might wonder whether any joint state can be expressed as this special product of two single-qubit states. It turns out that the answer is no.

This is a subtle fact. So, let us consider an analogue to this, with polynomials. Let us consider two vectors spaces of polynomials of x and of y. It is clear that $p(x)q(y)$ is contained in the vector space of polynomials of both x and y. However, this polynomial with both x and y,

$$xy + 1,$$

cannot be written as a product of a polynomial in x and one in y.

Back to qubits. Consider the following example. This joint state

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

cannot be written as this special product of two single-qubit states. These qubits are now in a state we call **entanglement**.

7 Kronecker product

similar thing for matrices?

4