Quantum Computing

Seungcheol Oh

I. Introduction

Quantum computing takes advantage of a natural quantum phenomena. This phenomena can best be described by introducing an experiment designed by Otto Stern and Walther Gerlach. The main objective of the experiment was to figure out the spin of an electron in an atom. Particularly, they were interested to find the spin of an electron in a silver atom.

First of all, what is the spin of an electron? According to Niels Bohr's model, an atom consists of a positive nucleus orbited by negative electrons. Electrons occupy energy levels that constrain them to certain radii. These levels usually have electrons paired with opposite spins, meaning their magnetic moments cancel each other out. However, in a silver atom, the outermost energy level has a single unpaired electron, resulting in a net magnetic moment because there is no other electron to cancel its magnetic field in that energy level.

Stern and Gerlach were curious to find out the orientation of the magnetic field of the silver atom. Therefore, they set up an experiment where they aligned north magnet on top and south magnet on bottom in vertical direction with a space between them. Now, south magnet has stronger magnetic field then the north magnet. We also know that for magnets, opposites attract and likes repel. The experiment is set up such that Stern and Gerlach shoot a silver atom in between these magnets. If the orientation of the silver atom's magnet is north on top and south on bottom, the atom will shoot up towards north since south magnet on the bottom is stronger then the north magnet on the top. If the silver atom has south on top and north on bottom, attraction force from bottom south magnet will be stronger, therefore the silver atom will shoot down towards south.

In a classical view, if the silver atom's magnetic moment were aligned with the field, it would deflect in one direction, and if aligned against the field, it would deflect in the opposite direction. However, the results of the experiment showed that the silver atoms split into two distinct beams, one deflecting up and the other down. To everyone's surprise, the atoms did not deflect in a continuous range but rather in discrete steps, indicating the quantization of the spin. Each silver atom's electron had a 50% probability of being measured in the spin-up state and a 50% probability of being in the spin-down state, regardless of its initial state before measurement.

This outcome demonstrated the inherent quantum nature of particles, where the electron's spin does not have a definite value until it is measured. Instead, it exists in a superposition of spin-up and spin-down states, a fundamental concept in quantum mechanics and essential for quantum computing.

II. Qubit

Qubits are fundamental unit of quantum information. For a bit, a fundamental unit of classical information, it only needs to represent two mutually exclusive states (on or off). A practical implementation of a bit; therefore, is an electrical switch. In contrast, qubits are usually represented by two-dimensional column vectors called kets. Further, qubits are measured which outcomes two possible mutually exclusive states. To describe these states, we use an ordered orthonormal basis, typically denoted as $|0\rangle$ and $|1\rangle$.

Qubits are fundamentally different from classical bits because two mutually exclusive states co-exist probabilistically before measurement. This phenomenon is called superposition. Superposition is described as

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle , \tag{1}$$

where α_0 and α_1 are probability amplitudes and $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. Absolute value of these probability amplitudes $|\alpha_0|^2$ and $|\alpha_1|^2$ are probability of the qubit state jumping to $|0\rangle$ and $|1\rangle$, respectively, when measurement takes place. Consequently, the sum of absolute value of probability amplitudes sum up to 1 to satisfy the probability axiom.

A. Bloch Sphere

III. Entanglement

You have two particles, in which one particle's state is described as $\alpha_0 |a_0\rangle + \alpha_1 |a_1\rangle$, and another particle's state is described as $\beta_0 |b_0\rangle + \beta_1 |b_1\rangle$. In quantum computing, description of state of the two particles is expressed by tensor product. Therefore, we can describe the state of the two particles as

$$\big(\alpha_0 |a_0\rangle + \alpha_1 |a_1\rangle\big) \otimes \big(\beta_0 |b_0\rangle + \beta_1 |b_1\rangle\big) = \alpha_0 |a_0\rangle \otimes \beta_0 |b_0\rangle + \alpha_0 |a_0\rangle \otimes \beta_1 |b_1\rangle + \alpha_1 |a_1\rangle \otimes \beta_0 |b_0\rangle + \alpha_1 |a_1\rangle \otimes \beta_1 |b_1\rangle . \tag{2}$$

Let's consider another state that describes the state of the two particles described as

$$|a_0\rangle \otimes |b_0\rangle + |a_1\rangle \otimes |b_1\rangle . \tag{3}$$

Now, if we take a closer look at (2), right side of the equation can successfully factor out the individual states of particle one and particle two in the left side of the equation. However, can we do this with (3)? Clearly, we cannot; this means that this state cannot be described by individually describing the state of the first particle and the state of the second particle. Therefore, the two particles are entangled.

A. Example: Entangled Qubits

Let us look deeper into (3). This state means that $\alpha_0\beta_0 = \alpha_1\beta_1 = 1$ and $\alpha_0\beta_1 = \alpha_1\beta_0 = 0$. With this, we can rewrite (3) as

$$\alpha_0\beta_0 \left|a_0\right\rangle \left|b_0\right\rangle + \alpha_0\beta_1 \left|a_0\right\rangle \left|b_1\right\rangle + \alpha_1\beta_0 \left|a_1\right\rangle \left|b_0\right\rangle + \alpha_1\beta_1 \left|a_1\right\rangle \left|b_1\right\rangle, \tag{4}$$

where for no-tational convenience we rewrite $\left|a_x\right\rangle \left|b_y\right\rangle = \left|a_x\right\rangle \otimes \left|b_y\right\rangle$. We then factor out $\left|a_0\right\rangle$ and $\left|a_1\right\rangle$, and describe 4 as

$$\left|a_0\right\rangle (\alpha_0\beta_0 \left|b_0\right\rangle + \alpha_0\beta_1 \left|b_1\right\rangle) + \left|a_1\right\rangle (\alpha_1\beta_0 \left|b_0\right\rangle + \alpha_1\beta_1 \left|b_1\right\rangle) = \frac{1}{\sqrt{2}} \left|a_0\right\rangle (1 \left|b_0\right\rangle + 0 \left|b_1\right\rangle) + \frac{1}{\sqrt{2}} \left|a_1\right\rangle (0 \left|b_0\right\rangle + 1 \left|b_1\right\rangle). \tag{5}$$

Now, Alice who has the first qubit measures her qubit. Then with probability $\frac{1}{2}$ the state either jumps to $\left|a_0\right\rangle$ associated with $1\left|b_0\right\rangle + 0\left|b_1\right\rangle$ or $\left|a_1\right\rangle$ associated with $0\left|b_0\right\rangle + 1\left|b_1\right\rangle$. After jumping to either state, Bob's qubit, linked with states $\left|b_0\right\rangle$ and $\left|b_1\right\rangle$ immediately is determined to $\left|b_0\right\rangle$ or $\left|b_1\right\rangle$.

B. Example: Unentangled Qubits

Consider unentangled qubits in state described by 2. We can rewrite this as

$$\big(\alpha_0 \left|a_0\right\rangle + \alpha_1 \left|a_1\right\rangle\big) \otimes \big(\beta_0 \left|b_0\right\rangle + \beta_1 \left|b_1\right\rangle\big) = \left|a_0\right\rangle (\alpha_0\beta_0 \left|b_0\right\rangle + \alpha_0\beta_1 \left|b_1\right\rangle) + \left|a_1\right\rangle (\alpha_1\beta_0 \left|b_0\right\rangle + \alpha_1\beta_1 \left|b_1\right\rangle). \tag{6}$$

Let us assume that $\alpha_0\beta_0 = \frac{1}{2\sqrt{2}}$, $\alpha_0\beta_1 = \frac{\sqrt{3}}{2\sqrt{2}}$, $\alpha_1\beta_0 = \frac{1}{2\sqrt{2}}$ and $\alpha_1\beta_1 = \frac{\sqrt{3}}{2\sqrt{2}}$. Then, (6) can be expressed as

$$\left|a_0\right\rangle \big(\frac{1}{2\sqrt{2}} \left|b_0\right\rangle + \frac{\sqrt{3}}{2\sqrt{2}} \left|b_1\right\rangle\big) + \left|a_1\right\rangle \big(\frac{1}{2\sqrt{2}} \left|b_0\right\rangle + \frac{\sqrt{3}}{2\sqrt{2}} \left|b_1\right\rangle\big) = \frac{1}{\sqrt{2}} \left|a_0\right\rangle \big(\frac{1}{2} \left|b_0\right\rangle + \frac{\sqrt{3}}{2} \left|b_1\right\rangle\big) + \frac{1}{\sqrt{2}} \left|a_1\right\rangle \big(\frac{1}{2} \left|b_0\right\rangle + \frac{\sqrt{3}}{2} \left|b_1\right\rangle\big). \tag{7}$$

Same as example with entangled states, if Alice measures her qubit, it either jumps to $\left|a_0\right\rangle$ or $\left|a_1\right\rangle$ with half probability. However, this time, Bob's qubit state does not get affected, it still remains as $\frac{1}{2}\left|b_0\right\rangle + \frac{\sqrt{3}}{2}\left|b_1\right\rangle$ in both states.

There are many ways to entangle qubits which were initially unentangled. However, in theory of quantum computing, we abstract away from the practical method of entangling qubit. Instead, we describe it mathematically by applying CNOT gate. In the later section, we will discuss quantum gates which are just operations that can be described by orthogonal matrices.

IV. Quantum Gates

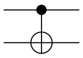
In classical computation, logic gates such as AND, NAND, OR, NOR, XOR, and NOT, are used to perform Boolean function, which is a function whose argument and result both assumes value from a two-element set. This is why logic gates are used in classical computation whose unit is in bits (0 or 1). Therefore, logic gates are just electrical circuits that manipulate bits in classical computation. In quantum computation, there also exists quantum gates which does similar operation to manipulate qubits. Since qubits are represented by vectors in a complex vector space, with the standard basis (computational basis) consisting of two orthogonal states, quantum gates, abstracted away from practical methods to make them, are represented by unitary matrices that operate on these basis states. These matrices change the state of qubits through linear transformations, allowing for superposition and entanglement, which are key features of quantum computation. For example, as briefly mentioned in Sec. III, CNOT gate is a quantum gate. In the following subsections, we describe the important gates that become foundation for quantum circuit and quantum algorithms.

A. Controlled NOT (CNOT) Gate

CNOT gate described by

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{8}$$

In diagram, CNOT gate is represented as



The main usage of CNOT gate as mentioned, is that it entangles the qubits. For example, consider two qubits each in state $\alpha\left|a\right\rangle$ and $\beta\left|b\right\rangle$. We can describe the states of two quibits with tensor product as

$$\alpha\left|a\right\rangle \otimes \beta\left|b\right\rangle, \tag{9}$$

where $a = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$ and $b = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$. We put this through CNOT gate which becomes

$$CNOT(\alpha\left|a\right\rangle \otimes \beta\left|b\right\rangle) = \alpha\beta \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a_0b_0 \\ a_0b_1 \\ a_1b_0 \\ a_1b_1 \end{bmatrix} = \alpha\beta \begin{bmatrix} a_0b_0 \\ a_0b_1 \\ a_1b_1 \\ a_1b_0 \end{bmatrix}. \tag{10}$$

Note that 10 cannot be factored out as individual qubit state tensor product with the other qubit state. Therefore, two qubits are entangled in the state 10. We can see that product of inner amplitudes is $a_0a_1b_1b_1$ and outer amplitudes is $a_0a_1b_0b_0$; therefore, two qubits are entangled.

B. Pauli Gates

There are four other gates, called Pauli Gates, which are important to note. They become foundation for superdense coding and quantum teleportation. First, there is the I gate which is described as

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{11}$$

This is a standard identity matrix which will leave the state of qubit unchanged. Next is Z gate which preserves the basis vectors, but changes the sign of probability amplitude. This gate is described as

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{12}$$

For example, consider a qubit in superposition state $a_0\left|0\right\rangle + a_1\left|1\right\rangle$. We put this through Z gate, which results in

$$Z(a_0\left|0\right\rangle + a_1\left|1\right\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_0 \\ -a_1 \end{bmatrix} = a_0\left|0\right\rangle - a_1\left|1\right\rangle. \tag{13}$$

Next, we have X gate which interchanges the basis vectors, it is described as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{14}$$

Consider putting a qubit in state $a_0\left|0\right\rangle + a_1\left|1\right\rangle$ through X gate.

$$X(a_0\left|0\right\rangle + a_1\left|1\right\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_0 \end{bmatrix} = a_1\left|0\right\rangle + a_0\left|1\right\rangle. \tag{15}$$

Lastly, there is Y gate which interchanges the basis as well as the relative phase. This gate is described by an orthogonal matrix

$$Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{16}$$

We put a qubit in state $a_0\left|0\right\rangle + a_1\left|1\right\rangle$ through this gate to produce,

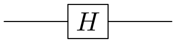
$$Y(a_0\left|0\right\rangle + a_1\left|1\right\rangle) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} -a_1 \\ a_0 \end{bmatrix} = -a_1\left|0\right\rangle + a_0\left|1\right\rangle. \tag{17}$$

C. Hadamard Gate

Hadamard gate puts standard basis vector into superposition, it is described as

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{18}$$

Hadamard gate is foundation of Bell circuit, which gets used for quantum teleportation and superdense coding. In diagram, it is represented as



If we input $\left|0\right\rangle$ through Hadamard gate, it becomes

$$H(\left|0\right\rangle) = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle). \tag{19}$$

Analogously, $\left|1\right\rangle$ through Hadamard gate produces

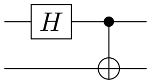
$$H(\left|1\right\rangle) = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle). \tag{20}$$

V. Quantum Circuits

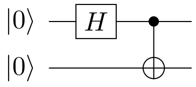
We have discussed various number of gates that can be used to manipulate qubits. If we place them carefully together, we can create circuits. These circuits become basis to perform superdense coding and quantum teleportation.

A. Bell's Circuit

The basic configuration of Bell's circuit is drawn as such



where it applies Hadamard gate followed by CNOT gate. Consider applying $|0\rangle$ to both top and bottom qubit which would look like a figure below.



After the first qubit passes through Hadamard gate, the qubit will be expressed as $\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$. This with bottom qubit forms $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle$. Then it goes through CNOT gate and it finally becomes $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$. Now, we can do the same operation to all possible combinations of qubits $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$. Then, we get what is called a Bell basis described as

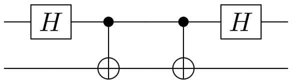
$$B(|00\rangle)=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle \tag{21}$$

$$B(|01\rangle)=\frac{1}{\sqrt{2}}|10\rangle+\frac{1}{\sqrt{2}}|01\rangle \tag{22}$$

$$B(|10\rangle)=\frac{1}{\sqrt{2}}|00\rangle-\frac{1}{\sqrt{2}}|11\rangle \tag{23}$$

$$B(|11\rangle)=\frac{1}{\sqrt{2}}|10\rangle-\frac{1}{\sqrt{2}}|01\rangle. \tag{24}$$

Very neat operation that we can do on the Bell's basis is that once we apply the reverse circuit, we extract out the original qubit state. The complete circuit even with the reverse operation in diagram is illustrated as



where this becomes basis for superdense coding.

B. Superdense Coding

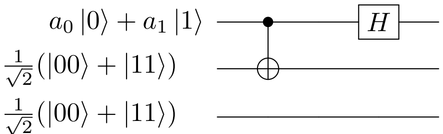
Superdense coding has a simple objective. Alice wants to transmit 2 bits of information to Bob. This means that she sends one of 00, 01, 10, or 11 to Bob. If we assume that there is no error between Alice and Bob's transmission channel and they are using classical bits, this is a simple task. Alice would send two bits to Bob and he can receive them without error; the task is done. However, the challenge is that they are performing this task with two qubits; one at Alice's side and the another at Bob's side. How would they communicate two bits of information if Alice is to only send one qubit to Bob? Further, even if Alice successfully sends her qubit in superposition state $a_0|0\rangle+a_1|1\rangle$ to Bob, Bob randomly measures one of her basis with probability. Moreover, Bob would have to receive the second bit by measuring his own qubit with randomness.

Superdense coding solves the problem of randomness with entanglement. Alice and Bob each having one bit that is entangled with another. The entangled qubits are in the state $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$. Notice that this is one of the Bell's basis. Therefore, if Bob receives the Alice's qubit without any error, then he puts her qubit and his own qubit through a reverse Bell's circuit. Then he will measure 00. Same logic applies to any other bit information, if Alice wants to send 01, she would apply X gate to her qubits to swap the her basis. If she wants to send 10, she applies Z gate; finally, if she wants to send 11, she applies Y gate to her qubit. Whatever the bit Alice wants to send, Bob only has to put her transmitted qubit and his qubit through the reverse circuit and measure the top qubit and the bottom bit to receive the bits that Alice intended to send.

C. Quantum Teleportation

The objective of quantum teleportation is that Alice wants to teleport a specific qubit state that she has to Bob. Consider a qubit state, $a_0|0\rangle+a_1|1\rangle$, which Alice has and she wants to teleport this state to Bob. This is challenging because even Alice does not know the exact state of her qubit. Furthermore, lets say Alice is curious about the state of her qubit and she decides to measure it. Then, the qubit jumps to a state, which changes the state of her qubit that she originally wanted to teleport to Bob. Even though this is a challenging task, by utilizing entanglement and classical bit communication, this task is achievable.

For the quantum teleportation to take place, Alice and Bob must follow the following procedure described by the diagram below.


$a_0|0\rangle + a_1|1\rangle$
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
H

First of all, Alice and Bob must share each of the entangled qubits in the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Alice also has a qubit in the state, $a_0|0\rangle + a_1|1\rangle$, that she wants to teleport to Bob. We have three qubits which can be described as

$$\Big(a_0|0\rangle + a_1|1\rangle\Big) \otimes \Big(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\Big) = \frac{a_0}{\sqrt{2}}|000\rangle + \frac{a_0}{\sqrt{2}}|011\rangle + \frac{a_1}{\sqrt{2}}|100\rangle + \frac{a_1}{\sqrt{2}}|111\rangle . \tag{25}$$

Now, the top two qubits gets passed through a CNOT gate which then changes the state of the qubit as

$$\frac{a_0}{\sqrt{2}}|000\rangle + \frac{a_0}{\sqrt{2}}|011\rangle + \frac{a_1}{\sqrt{2}}|110\rangle + \frac{a_1}{\sqrt{2}}|101\rangle = \frac{a_0}{\sqrt{2}}|0\rangle \otimes |00\rangle + \frac{a_0}{\sqrt{2}}|0\rangle \otimes |11\rangle + \frac{a_1}{\sqrt{2}}|1\rangle \otimes |10\rangle + \frac{a_1}{\sqrt{2}}|1\rangle \otimes |01\rangle . \tag{26}$$

Then, we apply Hadamard gate to the first qubit which changes the state as

$$\frac{a_0}{2}|00\rangle \otimes |0\rangle + \frac{a_0}{2}|10\rangle \otimes |0\rangle + \frac{a_0}{2}|01\rangle \otimes |1\rangle + \frac{a_0}{2}|11\rangle \otimes |1\rangle + \tag{27}$$

$$\frac{a_1}{2}|01\rangle \otimes |0\rangle - \frac{a_1}{2}|11\rangle \otimes |0\rangle + \frac{a_1}{2}|00\rangle \otimes |1\rangle - \frac{a_1}{2}|10\rangle \otimes |1\rangle = \tag{28}$$

$$\frac{1}{2}|00\rangle \otimes (a_0|0\rangle + a_1|1\rangle) + \frac{1}{2}|01\rangle \otimes (a_0|1\rangle + a_1|0\rangle) + \frac{1}{2}|10\rangle \otimes (a_0|0\rangle - a_1|1\rangle) + \frac{1}{2}|11\rangle \otimes (a_0|1\rangle - a_1|0\rangle). \tag{29}$$

Alice will get one of four states $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ with probability of $\frac{1}{4}$ if she measures her qubit. After she observes her measurement, she transmits the result to Bob in a classical manner. Based on what she communicated to Bob, he sends his qubit through specific Pauli gates to obtain the state $a_0|0\rangle + a_1|1\rangle$. For example, if Alice communicates 01, Bob would send his qubit through X gate. Now, Bob has fixed his qubit state to what Alice's original qubit state. Therefore, the qubit state of Alice successfully teleported to Bob.

VI. Quantum Algorithms

It is widely believed that quantum algorithms can perform faster than classical algorithms. This is because, instead of processing calculations one bit at a time, quantum algorithms can process qubits in multiple states simultaneously due to superposition. This ”quantum parallelism” is often cited as the reason why quantum algorithms are thought to be faster than classical algorithms. However, while this is partly true, the explanation cannot stop there. Even if a superposition of states is processed, obtaining a meaningful result requires measurement. Upon measurement, a qubit collapses into one of its possible states, which seems to introduce randomness. Wouldn't this make things more complex to deal with? The real advantage comes from the ability to carefully manipulate the superposition and entanglement of qubits such that, when measurement occurs, the result provides useful information. In this section, we will describe how exactly the quantum algorithms are used such that it outperforms classical algorithms.

A. P and NP problems

To fairly compare the time complexity between classical algorithm and quantum algorithm, we must define how speed of algorithms are measured. Best introduction to explain this is to introduce following problems.

- Find two whole numbers bigger than 1 whose product is equal to 35.
- Find two whole numbers bigger than 1 whose product is equal to 187.
- Find two whole numbers bigger than 1 whose product is euqal to 2,407
- Find two whole numbers bigger than 1 whose product is equal to 88,631.

Finding factors of a number seems like an easy task until the scale of the problem becomes larger. Compare the first and last problem statements. It is much easier to find two whole numbers that are factors of 35 than 88,631. Now, consider a different set of problems.

- Multiply 7 and 5 and check that it equals 35.
- Multiply 11 and 17 and check that it equals 187.
- Multiply 29 and 83 and check that it equals 2407.
- Multiply 337 and 263 and check that it equals 88,631.

B. Deutsch's Algorithm

C. Deutsch-Jozsa Algorithm

D. Simon's Algorithm

E. Shor's Algorithm