COL866: Quantum Computation and Information

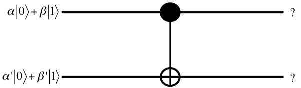
Ragesh Jaiswal, CSE, IIT Delhi

Introduction

- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical `NOT` gate. If there is a similar analogue for `NAND` gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? `NAND` gate is a universal gate.
  - Does a quantum analogue of `NAND` gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or `CNOT` gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

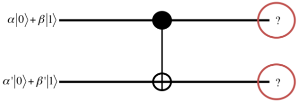
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or CNOT gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

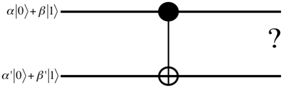
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical `NOT` gate. If there is a similar analogue for `NAND` gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? `NAND` gate is a universal gate.
  - Does a quantum analogue of `NAND` gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or `CNOT` gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

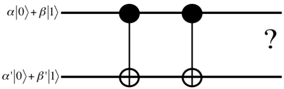
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or CNOT gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

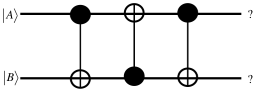
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or CNOT gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes the CNOT gate
    - This is called the controlled-NOT gate or CNOT gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

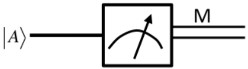
    - Claim: *Any multiple qubit logic gate may be composed from* CNOT *and single qubit gates.*

- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical `NOT` gate. If there is a similar analogue for `NAND` gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? `NAND` gate is a universal gate.
  - Does a quantum analogue of `NAND` gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes the `CNOT` gate

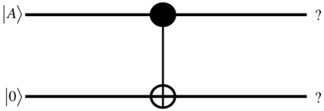
- Measurements:
  - We now have a high-level understanding of how a quantum circuit evolves. What can be obtain or measure from the circuit?
  - We said that we can measure a qubit in the computation basis $|0\rangle$ and $|1\rangle$ which are just one orthonormal basis. Can we measure in some other orthonormal basis?

- Measurements:
  - We now have a high-level understanding of how a quantum circuit evolves. What can be obtain or measure from the circuit?
  - We said that we can measure a qubit in the computation basis $|0\rangle$ and $|1\rangle$ which are just one orthonormal basis. Can we measure in some other orthonormal basis? Yes
    - We can measure in any orthonormal basis $|a\rangle, |b\rangle$. If the state of the qubit can be expressed as $\alpha |a\rangle + \beta |b\rangle$, then the measurement result is a with probability $|\alpha|^2$ and b with probability $|\beta|^2$.
    - One such popular basis is the $|+\rangle, |-\rangle$ basis that are expressed as $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.
    - Question: Express $\alpha |0\rangle + \beta |1\rangle$ in the $|+\rangle, |-\rangle$ basis.

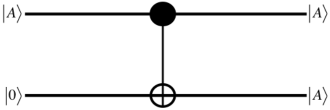
- Measurements:
  - We now have a high-level understanding of how a quantum circuit evolves. What can be obtain or measure from the circuit?
  - We said that we can measure a qubit in the computation basis $|0\rangle$ and $|1\rangle$ which are just one orthonormal basis. Can we measure in some other orthonormal basis? Yes
    - We can measure in any orthonormal basis $|a\rangle, |b\rangle$. If the state of the qubit can be expressed as $\alpha|a\rangle + \beta|b\rangle$, then the measurement result is a with probability $|\alpha|^2$ and b with probability $|\beta|^2$.
    - One such popular basis is the $|+\rangle, |-\rangle$ basis that are expressed as $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
    - In quantum circuit diagrams, measurement of a qubit is represented as below:



- Some exercises:
  - What is the output of the following circuit?

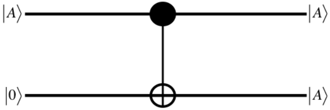


- Some exercises:
  - What is the output of the following circuit?

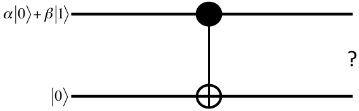


  - So, is the above circuit a qubit-copying circuit?

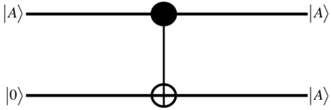
- Some exercises:
  - What is the output of the following circuit?



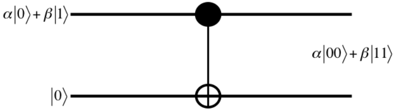
  - So, is the above circuit a qubit-copying circuit? No
    - Consider what happens in the following circuit?



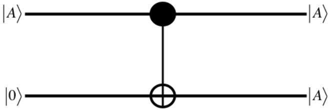
- Some exercises:
  - What is the output of the following circuit?



  - So, is the above circuit a qubit-copying circuit? No
    - Consider what happens in the following circuit?



- Some exercises:
  - What is the output of the following circuit?



  - So, is the above circuit a qubit-copying circuit? No
  - No-Cloning Theorem: It is impossible to copy an unknown quantum state input.

- Some exercises:
  - Let $\left[\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right]$ be any unitary matrix representing a single-qubit gate Q. Consider the matrix:

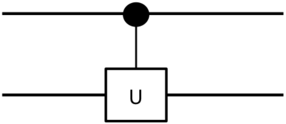
$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$$

    Is this matrix unitary?

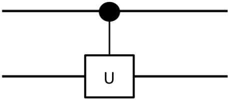
- Some exercises:
  - Let $\left[\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right]$ be any unitary matrix representing a single-qubit gate U. Consider the matrix:

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$$

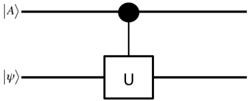
    Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:



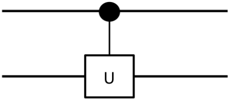
- Some exercises:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate U. Consider the matrix: $M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$. Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:



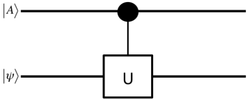
  - Question: Draw the quantum truth table for the circuit below:



- Some exercises:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate U. Consider the matrix: $M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$. Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:

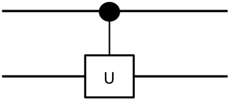


  - Question: Draw the quantum truth table for the circuit below:

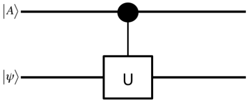


Input qubits	Output qubits
$\|0\rangle \|\psi\rangle$	$\|0\rangle \|\psi\rangle$
$\|1\rangle \|\psi\rangle$	$\|1\rangle U(\|\psi\rangle)$

- <u>Some exercises</u>:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate U. Consider the matrix: $M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$. Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:



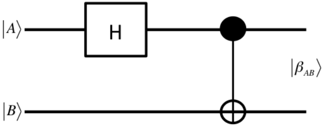
  - <u>Question</u>: Draw the quantum truth table for the circuit below:



Input qubits	Output qubits
$\|0\rangle\ \|\psi\rangle$	$\|0\rangle\ \|\psi\rangle$
$\|1\rangle\ \|\psi\rangle$	$\|1\rangle\ U(\|\psi\rangle)$

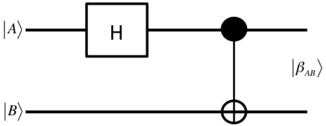
  - This is known as the controlled-U gate. The U gate is conditionally applied to the second qubit.

- Some exercises:
  - What is the output of the following circuit for different input states as shown:



In	Out
$\|00\rangle$	?
$\|01\rangle$	?
$\|10\rangle$	?
$\|11\rangle$	?

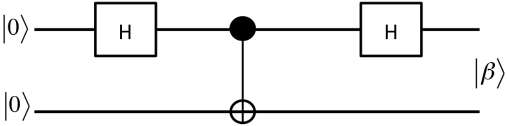
- Some exercises:
  - What is the output of the following circuit for different input states as shown:



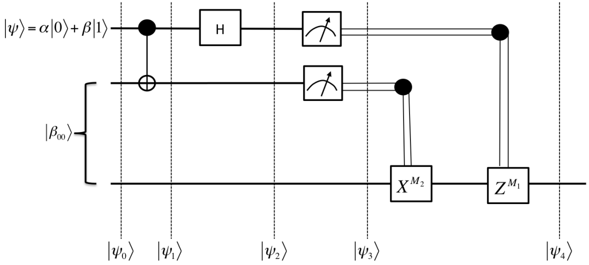
In	Out
$\|00\rangle$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}} \equiv \|\beta_{11}\rangle$

  - $|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle$ are called Bell states or EPR-pairs or EPR-states (after Bell, Einstein, Podolsky, and Rosen). These exhibit interesting properties as we will see in our first application to quantum-teleportation.

- Some exercises:
  - What is the output of the following circuit:

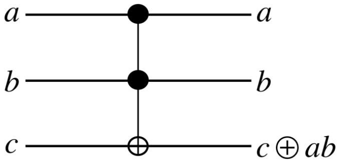


- Alice and Bob met sometime back and together they created Bell pair $|\beta_{00}\rangle$ and both kept one qubit each.
- They are now very far from each other perhaps in some opposite corners of the universe.
- Alice wants to deliver an unknown qubit $|\psi\rangle$ to Bob. Moreover, she can only communicate classical information to Bob.
- Fortunately, she knows quantum circuits and constructs the following circuit in a hope to communicate $|\psi\rangle$. The first two qubits in the circuit is in possession of Alice while Bob has the third qubit.

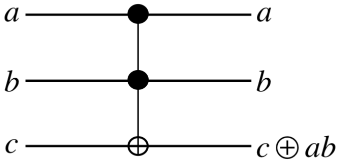


Introduction: Quantum Algorithms

- Can we simulate classical logic circuit using a quantum circuit?
- Claim: Any classical logic circuit can be implemented using just `NAND` and `COPY` gates.
- If we can build a quantum analogue of `NAND` and `COPY` gates, then we will be done.
- The following three-qubit gate, called the Toffoli gate, can be used to implement both `NAND` and `COPY`.



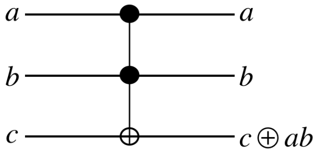
- Can we simulate classical logic circuit using a quantum circuit?
- Claim: Any classical logic circuit can be implemented using just `NAND` and `COPY` gates.
- If we can build a quantum analogue of `NAND` and `COPY` gates, then we will be done.
- The following three-qubit gate, called the Toffoli gate, can be used to implement both `NAND` and `COPY`.



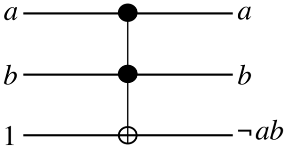
- Question: Can you build `NAND` using Toffoli gate?

Introduction
Quantum algorithms

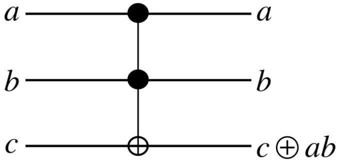
- Can we simulate classical logic circuit using a quantum circuit?
- Claim: Any classical logic circuit can be implemented using just NAND and COPY gates.
- If we can build a quantum analogue of NAND and COPY gates, then we will be done.
- The following three-qubit gate, called the Toffoli gate, can be used to implement both NAND and COPY.



- Question: Can you build NAND using Toffoli gate?

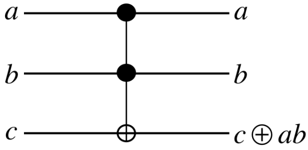


- Can we simulate classical logic circuit using a quantum circuit?
- Claim: Any classical logic circuit can be implemented using just `NAND` and `COPY` gates.
- If we can build a quantum analogue of `NAND` and `COPY` gates, then we will be done.
- The following three-qubit gate, called the Toffoli gate, can be used to implement both `NAND` and `COPY`.

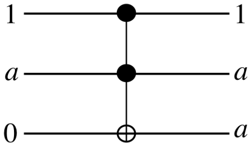


- Question: Can you build `COPY` using Toffoli gate?

- Can we simulate classical logic circuit using a quantum circuit?
- Claim: Any classical logic circuit can be implemented using just `NAND` and `COPY` gates.
- If we can build a quantum analogue of `NAND` and `COPY` gates, then we will be done.
- The following three-qubit gate, called the Toffoli gate, can be used to implement both `NAND` and `COPY`.

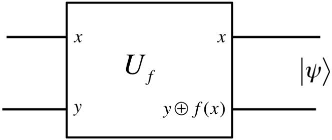


- Question: Can you build `COPY` using Toffoli gate?

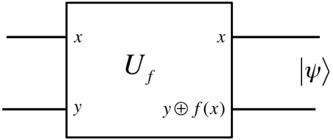


- Can we simulate classical logic circuit using a quantum circuit?
  Yes
- Can quantum circuits do more than just simulating classical ones?
  - We will introduce the idea of quantum parallelism. The main idea is simultaneous evaluation of a function over various inputs.
  - We will look at Deutsch's Algorithm which is a prototypical example used to demonstrate the idea of quantum parallelism.

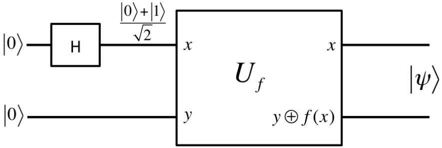
- Consider any boolean function over one-bit inputs $f : \{0,1\} \rightarrow \{0,1\}$.
- Claim: It is possible to construct the following quantum gate U_f (using basic gates):



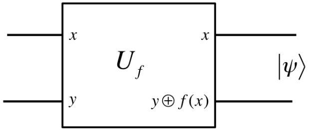
- Consider any boolean function over one-bit inputs $f : \{0,1\} \rightarrow \{0,1\}$.
- Claim: It is possible to construct the following quantum gate U_f (using basic gates):



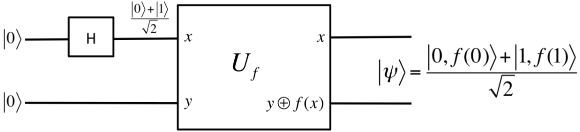
- By feeding inputs $|00\rangle$ and $|10\rangle$, we can compute $f(0)$ and $f(1)$.
- What happens when we feed the input $|+\rangle |0\rangle$ in this circuit? What is the output state $|\psi\rangle$?



- Consider any boolean function over one-bit inputs $f : \{0,1\} \rightarrow \{0,1\}$.
- Claim: It is possible to construct the following quantum gate U_f (using basic gates):



- By feeding inputs $|00\rangle$ and $|10\rangle$, we can compute $f(0)$ and $f(1)$.
- What happens when we feed the input $|\beta_{00}\rangle\, |0\rangle$ in this circuit? What is the output state $|\psi\rangle$?

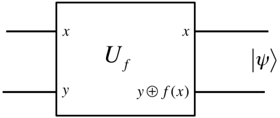


- This output state contains simultaneous evaluations of both $f(0)$ and $f(1)$!

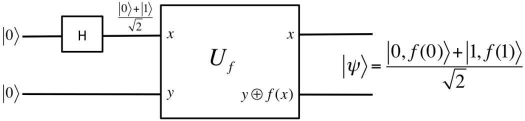
Introduction

Quantum algorithms $\rightarrow$ Deutsch's algorithm

- Consider any boolean function over one-bit inputs $f : \{0,1\} \rightarrow \{0,1\}$.
- Claim: It is possible to construct the following quantum gate U_f (using basic gates):

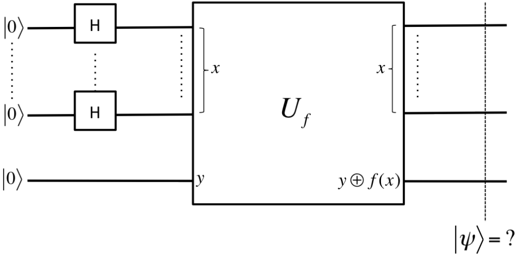


- By feeding inputs $|00\rangle$ and $|10\rangle$, we can compute $f(0)$ and $f(1)$.
- What happens when we feed the input $|\beta_{00}\rangle\,|0\rangle$ in this circuit? What is the output state $|\psi\rangle$?

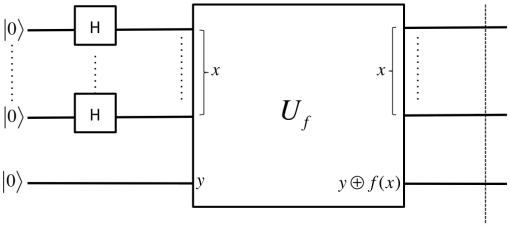


- This output state contains simultaneous evaluations of both $f(0)$ and $f(1)$!
- Question: Can we generalize this idea for boolean functions over multiple bit inputs?

- Question: Can we generalize this idea for boolean functions over multiple bit inputs?
- Consider any boolean function over n-bit inputs $f : \{0,1\}^n \rightarrow \{0,1\}$.
- What is the output of the following circuit?

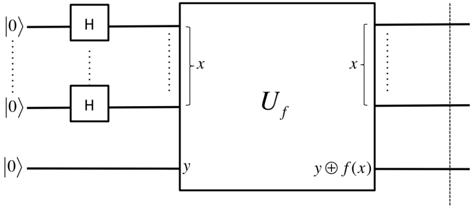


- Question: Can we generalize this idea for boolean functions over multiple bit inputs?
- Consider any boolean function over n-bit inputs $f : \{0,1\}^n \rightarrow \{0,1\}$.
- What is the output of the following circuit?



$$|\psi\rangle = \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle$$

- Question: Can we generalize this idea for boolean functions over multiple bit inputs?
- Consider any boolean function over n-bit inputs $f : \{0,1\}^n \rightarrow \{0,1\}$.
- What is the output of the following circuit?



$$|\psi\rangle = \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle$$

- Even though final state encodes evaluation of the function on all inputs, what we can measure is only one of them. So, it is important that we do not get carried away by the potential quantum parallelism exhibited in the above circuit.

End