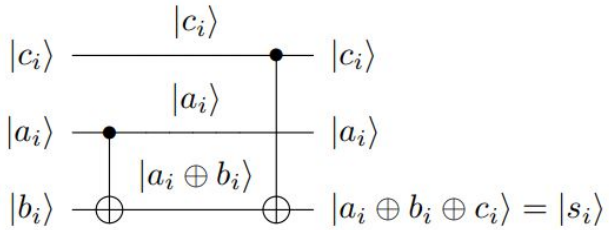
Presentation-3
21/06/2022

Chapters that will be presented are Chapters 6 and 7

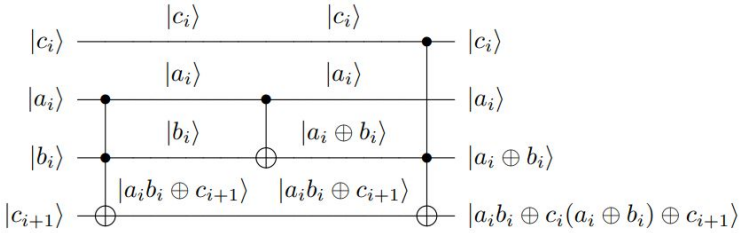
Quantum Adders

For quantum sum, we need two CNOT gates to get the following output.

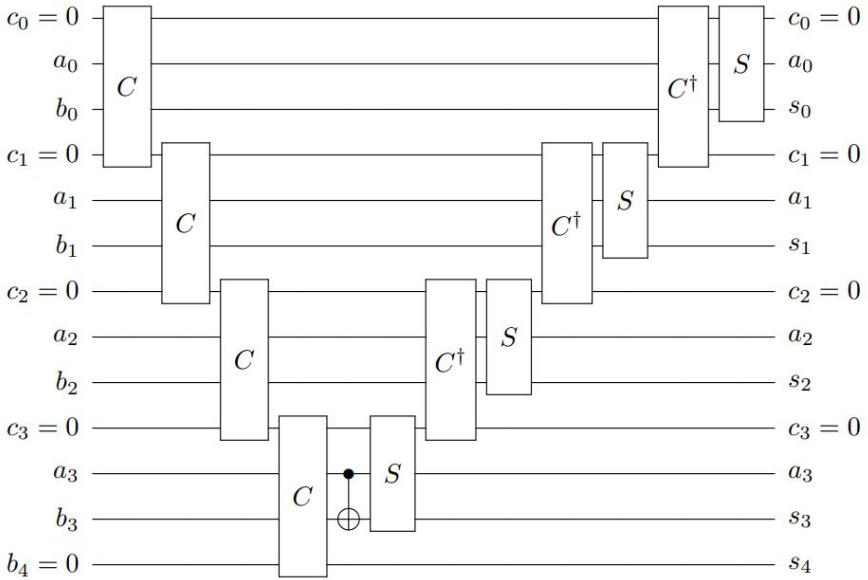


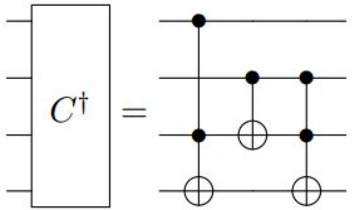
where |c> is the ancilla qubit, |a> and |b> are input qubits and |b> stores the sum value

For quantum carry, we need two toffoli gates and one CNOT gate. $|C_{i+1}\rangle$ is the carry bit



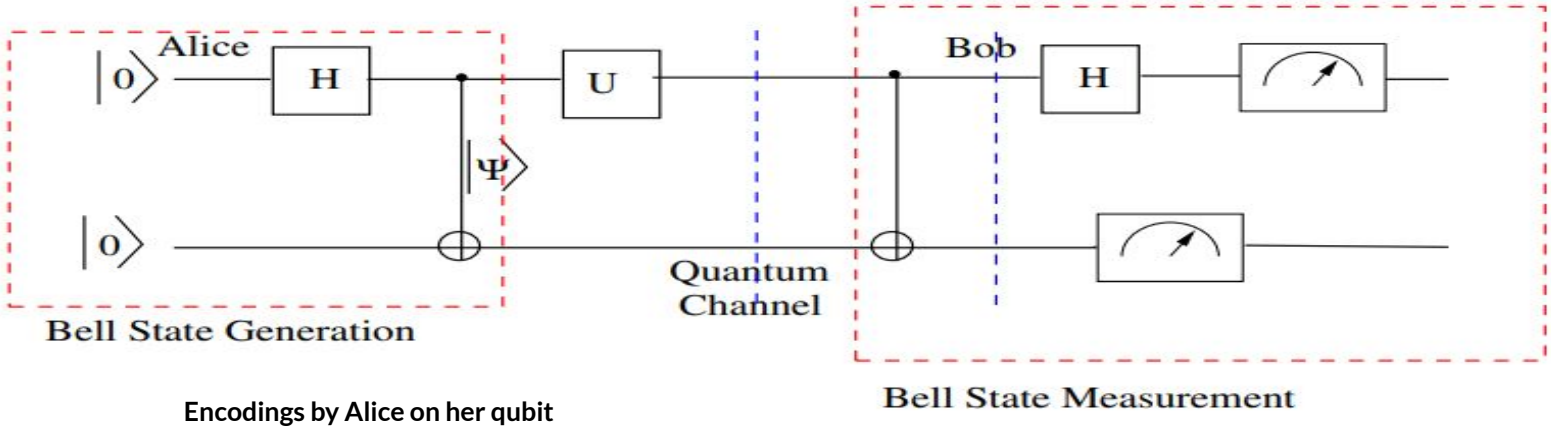
Quantum Ripple-Carry Adder





To find the sum of the values encoded in two quantum states, we first find carry bits for each bit in the input strings. The last carry bit will be stored as a sum(in s_4). To get b_3, we add CNOT gate between b_3 and a_3. This CNOT gate can be removed and directly apply the quantum sum gate to get s_3. Since we need c_3 to find s_2, inverse CNOT gate is operated followed by the sum gate to find s_2. This process continues until s_0 is found.

Superdense Coding



Encodings by Alice on her qubit

cbit to be sent	Action by Alice	Resulting state
00	No action by Alice	$\frac{1}{\sqrt{2}}(\mid 00\rangle + \mid 11\rangle)$
01	Alice applies $X \otimes I$	$\frac{1}{\sqrt{2}}(\mid 10\rangle + \mid 01\rangle)$
10	Alice applies $iY \otimes I$	$\frac{1}{\sqrt{2}}(- \mid 10\rangle + \mid 01\rangle)$
11	Alice applies $Z \otimes I$	$\frac{1}{\sqrt{2}}(\mid 00\rangle - \mid 11\rangle)$

Two classical bits of information is passed through a single qubit via a quantum channel.

Superdense Coding

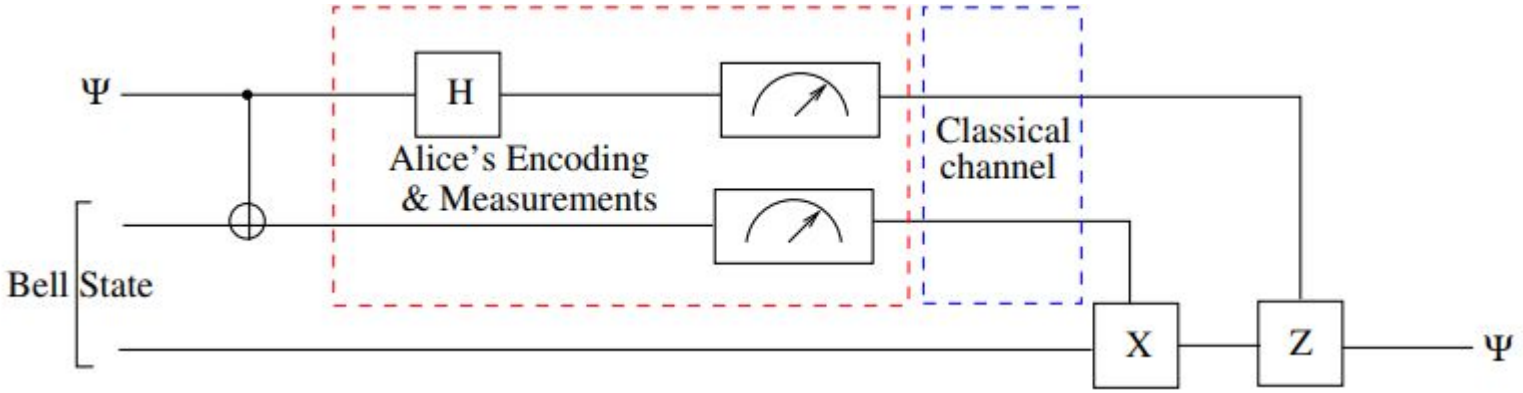
Decodings by Bob on her qubit - 1. CNOT gate, 2. Hadamard gate on first qubit, 3. Measures the qubits and does relevant operations to obtain the result.

cbit to be sent	state Bob has	Result of CNOT
00	$\frac{1}{\sqrt{2}}(\mid 00\rangle + \mid 11\rangle)$	$\frac{1}{\sqrt{2}}(\mid 00\rangle + \mid 10\rangle)$
01	$\frac{1}{\sqrt{2}}(\mid 10\rangle + \mid 01\rangle)$	$\frac{1}{\sqrt{2}}(\mid 11\rangle + \mid 01\rangle)$
10	$\frac{1}{\sqrt{2}}(- \mid 10\rangle + \mid 01\rangle)$	$\frac{1}{\sqrt{2}}(- \mid 11\rangle + \mid 01\rangle)$
11	$\frac{1}{\sqrt{2}}(\mid 00\rangle - \mid 11\rangle)$	$\frac{1}{\sqrt{2}}(\mid 00\rangle - \mid 10\rangle)$

cbit	State
00	$\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}} \otimes \mid 0\rangle$
01	$\frac{\mid 0\rangle + \mid 1\rangle}{\sqrt{2}} \otimes \mid 1\rangle$
10	$\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \otimes \mid 1\rangle$
11	$\frac{\mid 0\rangle - \mid 1\rangle}{\sqrt{2}} \otimes \mid 0\rangle$

cbit	Final State
00	$\mid 0\rangle \otimes \mid 0\rangle$
01	$\mid 0\rangle \otimes \mid 1\rangle$
10	$\mid 1\rangle \otimes \mid 1\rangle$
11	$\mid 1\rangle \otimes \mid 0\rangle$

Quantum Teleportation



1. CNOT between |k> and qubit 2
2. Hadamard gate on |k>
3. Measurements which are then sent to Bob via classical channel

Information of a quantum state |k⟩ has to be shared through the entangled stated between Alice and Bob using classical communication.

$$CNOT\left[(\alpha\mid 0\rangle+\beta\mid 1\rangle)\otimes\frac{1}{\sqrt{2}}(\mid 0\rangle\otimes\mid 0\rangle+\mid 1\rangle\otimes\mid 1\rangle)\right]=\frac{1}{\sqrt{2}}\left[\alpha(\mid 000\rangle+\mid 011\rangle)+\beta(\mid 110\rangle+\mid 101\rangle)\right]$$

$$\frac{1}{2}\left[\alpha(\mid 000\rangle+\mid 100\rangle+\mid 011\rangle+\mid 111\rangle)+\beta(\mid 010\rangle-\mid 110\rangle+\mid 001\rangle-\mid 101\rangle)\right]$$

$$\mid 00\rangle(\alpha\mid 0\rangle+\beta\mid 1\rangle)+\mid 01\rangle(\alpha\mid 1\rangle+\beta\mid 0\rangle)+\mid 10\rangle(\alpha\mid 0\rangle-\beta\mid 1\rangle)+\mid 11\rangle(\alpha\mid 1\rangle-\beta\mid 0\rangle)$$

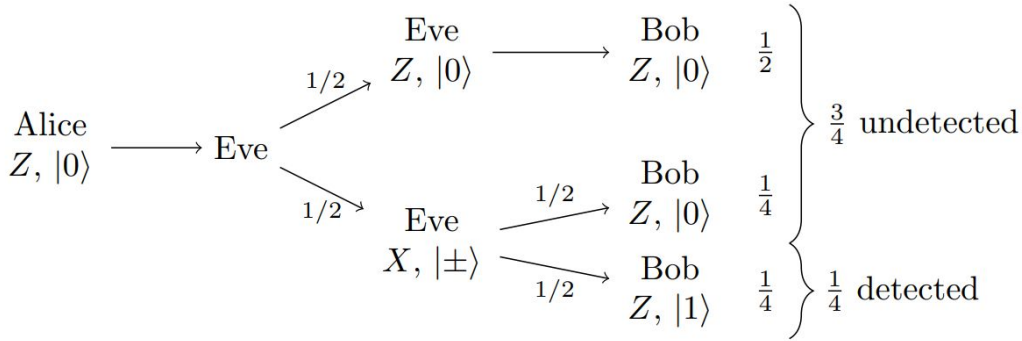
Quantum Teleportation

Bob does the following to obtain the state |k> in his laboratory-

1. No operation is done by Bob on his qubit if a $|0\rangle + b\ |1\rangle$ when the measurements give 00.
2. Bob applies X on his qubit if a $|1\rangle + b\ |0\rangle$ when the measurements give 01.
3. Bob applies Y on his qubit if a $|0\rangle - b\ |1\rangle$ when the measurements give 10.
4. Bob applies ZX on his qubit if a $|1\rangle - b\ |0\rangle$ when the measurements give 11.

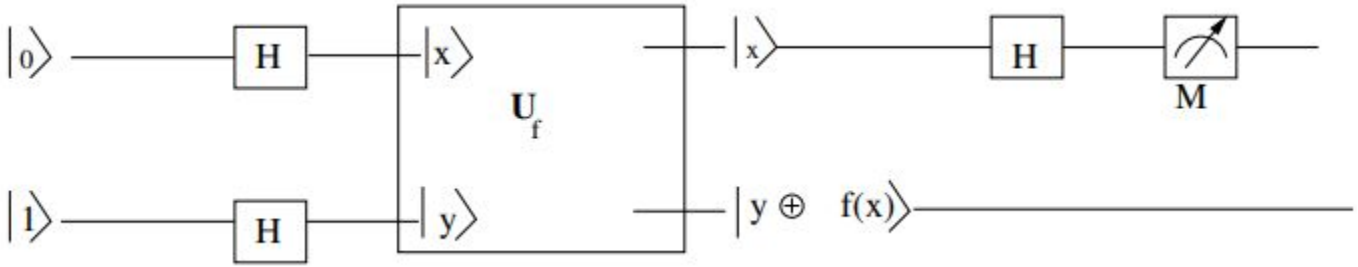
Quantum Key Distribution

1. Using BB-84 protocol, we can generate secret keys to be shared between two parties, Alice and Bob, with a third party, named Eve, trying to get information about the key.
2. Two bases are used to encode $|0\rangle$ and $|1\rangle$ using photons. These two bases are H/V (called the computational basis, denoted by H) and angle of 45◦ with horizontal/ angle of 135◦ with horizontal (called the diagonal basis, denoted by D). Alice uses these two bases randomly encode the key and takes note of it. Then, she sends the qubits through a quantum network.
3. Assuming Eve is secretly measuring the bits and then re-sends to Bob, then in this case, Bob decodes the bits correctly irrespective of the basis 75% and decodes incorrectly 1/4 times.
4. Supposing Alice and Bob generate k bits, and compare n (n<<k) bits randomly to detect the presence of Eve. Then, in this case, the presence of Eve is undetected is $(3/4)^n$ and the probability of Eve being detected is $1 - (3 /4)^n$ which is close to 0.99999...



Deutsch's Algorithm

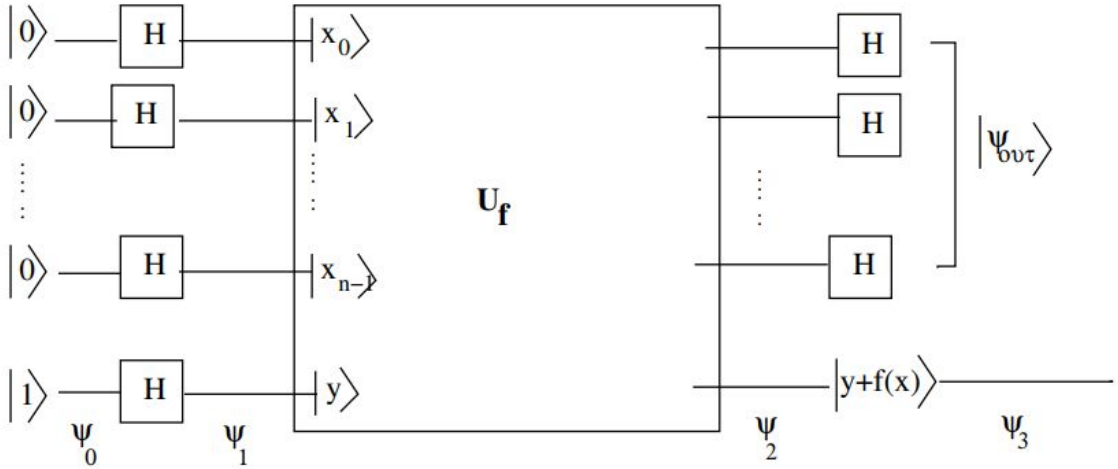
1. Single query to find if a univariate function is constant or balanced.
2. After applying the operations as shown in the diagram, we get If f(0) = f(1), then we will get $1/\sqrt{2}\,(|0\rangle + |1\rangle)(|f(0) - \neg f(0)\rangle)$, else we will get $1/\sqrt{2}\,(|0\rangle - |1\rangle)(|f(0) - \neg f(0)\rangle)$, followed by - apply the hadamard gate only to the input register and measuring input register.



Deutsch-Jozsa Algorithm

1. Single query to find if a multivariate function is constant or balanced.
2. After applying the operations as shown in the circuit diagram, we get - $\frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{k=\{0,1\}^n}(-1)^{k\cdot j+f(j)}\,|k\rangle\,|-\rangle$

3. In case, the function is balanced, then the amplitude for the case $|k\rangle = |0\rangle^{\otimes n}$ will be zero, then it means that when we measure the input registers we will get any state other than $|00...0\rangle$. If the function is constant, then the amplitude for the state $|00..0\rangle$ will be one.



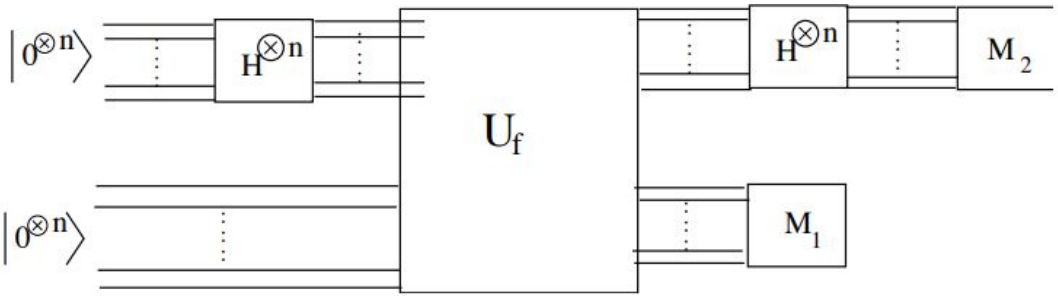
Bernstein-Vazirani Problem

1. We need to determine the value of a for a function f = a · x. The algorithm is same as that of Deutsch-Jozsa Algorithm.
2. The final state before measurement is the following - $\frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{k=\{0,1\}^n}^{2^n-1}(-1)^{(k+a)\cdot j}\,|k\rangle\,|-\rangle$

3. Only for the case when a = k, the probability amplitude of the state will be one, which means for all other states, the probability amplitude will be zero.

Simon's Problem

1. We need to find the value of a non-zero unknown string s. Let a function f be $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ such that $f(x) = f(y)$ if $x = y \oplus s$. We follow the steps as indicated in the circuit diagram.
2. On measuring the second register, we will get a certain value of f(x), then the first register is reduced to the linear combination of $|x\rangle$ and $|x \oplus s\rangle$, i.e, $1/\sqrt{2}\,(|x\rangle + |x \oplus s\rangle)$ and this happens if f is two-to-one. The measurement of the second register causes the two registers to be entangled with each other. We then pass the first register qubits to the hadamard gate. Then we obtain the state as - $$\frac{1}{2^{\frac{n+1}{2}}} \sum_{y=\{0,1\}^n} [(-1)^{x\cdot y} + (-1)^{(x\oplus s)\cdot y}]\,|y\rangle$$
3. If $(-1)^{x\cdot y} = (-1)^{(x\oplus s)\cdot y}$, we get $s \cdot y = 0$, i.e the inner product of s and y must be zero, they must be orthogonal to each other, and on measurement of the first register, we will get a value of y which satisfies this condition. In this case, the state will become - $$\frac{1}{2^{\frac{n-1}{2}}} \sum_{y=\{0,1\}^n} [(-1)^{x\cdot y}]\,|y\rangle$$



Simon's Problem

1. If $(-1)^{x\cdot y}$ is not equal to $(-1)^{(x\oplus s)\cdot y}$, then the coefficient of $|y\rangle$ will be zero and hence its probability amplitude. To find the unknown non-zero string s, we have to run this algorithm n times to obtain linearly independent vectors such that they are orthonormal to s and also we may consider that y is not equal to zero.
2. Upon solving each of those linearly independent vectors by taking inner product with s will give us its value.
3. Here, *b* is *s* and *z* is *y*. From which, s can be found such as by using Gaussian elimination.

$$\begin{cases} b \cdot z_1 = 0 \\ b \cdot z_2 = 0 \\ \quad \vdots \\ b \cdot z_n = 0 \end{cases}$$