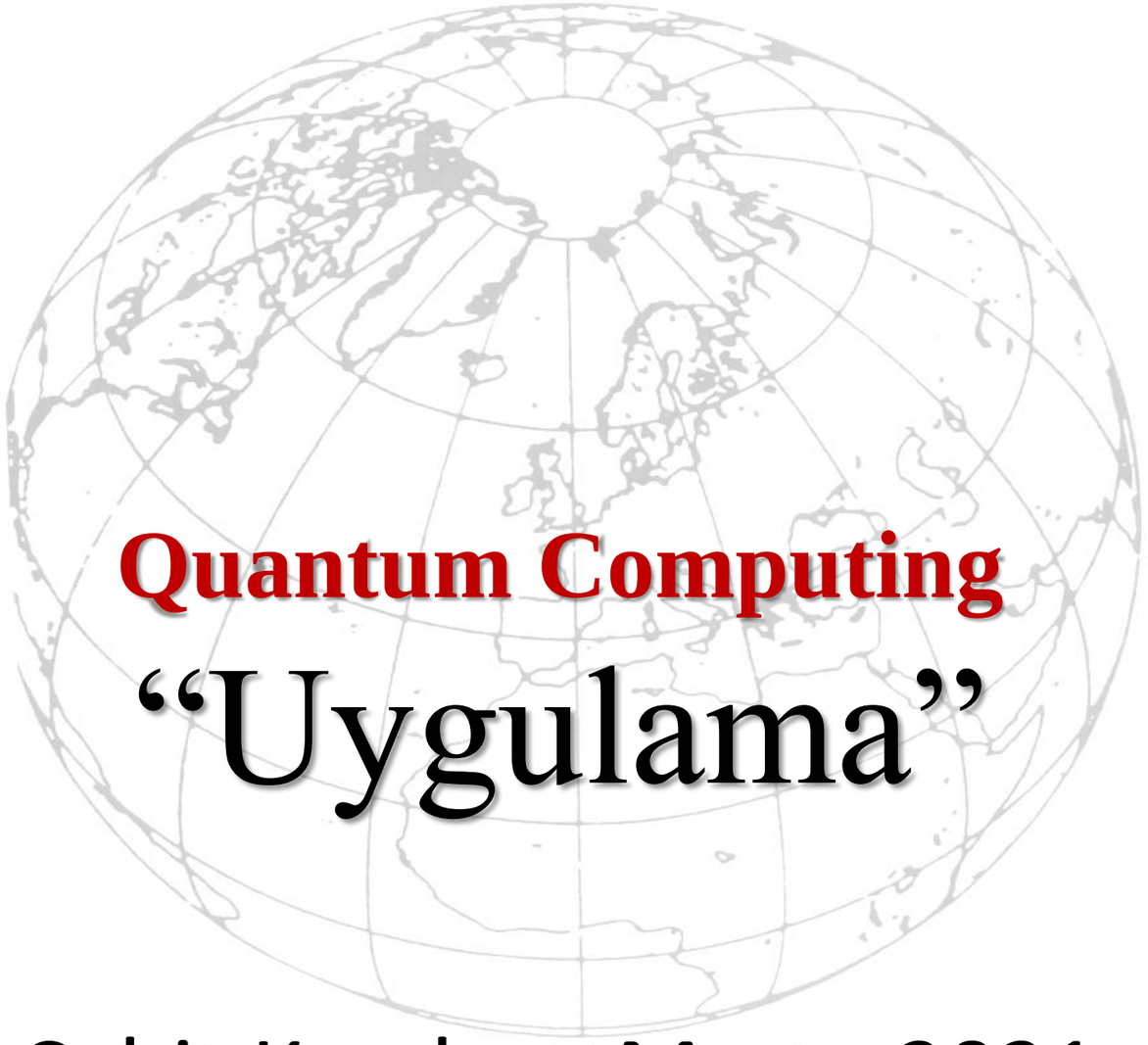


Quantum Computing

“Uygulama”

Dr. Cahit Karakuş, Mart - 2021

Örnek-1:

- $\psi = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$ ise $|0\rangle = \begin{pmatrix}1\\ 0\end{pmatrix}$ ve $|1\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}$ vektörleri ile temsil edilir.
- $ZR_{\varphi}\psi = \alpha|0\rangle - \beta|1\rangle$ olması için φ=?

- $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & e^{i\varphi}\end{bmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{pmatrix}\alpha\\ \beta e^{i\varphi}\end{pmatrix} = \begin{pmatrix}\alpha\\ -\beta e^{i\varphi}\end{pmatrix} = \alpha|0\rangle - \beta e^{i\varphi}|1\rangle$
- φ=0

Örnek-2:

- $\psi = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$ ise $|0\rangle = \begin{pmatrix}1\\ 0\end{pmatrix}$ ve $|1\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}$ vektörleri ile temsil edilir.
- $XR_\varphi\psi = \beta|0\rangle + \alpha|1\rangle$ olması için φ=?
- $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & e^{i\varphi}\end{bmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}\alpha\\ \beta e^{i\varphi}\end{pmatrix} = \begin{pmatrix}\beta e^{i\varphi}\\ \alpha\end{pmatrix} = \beta e^{i\varphi}|0\rangle + \alpha|1\rangle$
- φ=0

Örnek-3:

- $XS|1\rangle$=?
- $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}0\\ i\end{pmatrix}=\begin{pmatrix}i\\ 0\end{pmatrix}=i\begin{pmatrix}1\\ 0\end{pmatrix}=i|0\rangle$
-
- $XS|0\rangle$=?
- $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}0\\ 1\end{pmatrix}=|1\rangle$

Örnek-4:

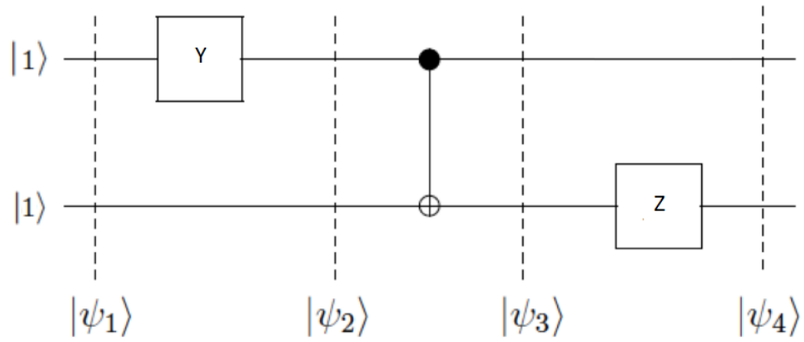
- $\begin{pmatrix} -i \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}$=?

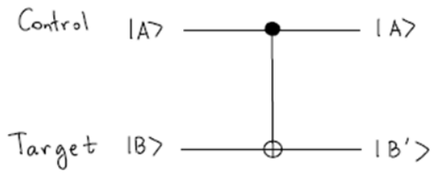
$$\begin{pmatrix} 0 \\ -i \\ 0 \\ 0 \end{pmatrix} = -i \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = -i|01\rangle$$

- $\begin{pmatrix} 0 \\ i \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}$=?

$$\begin{pmatrix} 0 \\ 0 \\ i \\ 0 \end{pmatrix} = i \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = i|10\rangle$$

Örnek-5:





|AB⟩	|AB'⟩
|00⟩	|00⟩
|01⟩	|01⟩
|10⟩	|11⟩
|11⟩	|10⟩

A kontrol grişi olduğu gibi geçer.
B çıkışı, A=0 ise B olduğu gibi geçer, A=1 ise B'nin tersi geçer,

Üst hatta,

$$|\psi_1\rangle = |1\rangle$$

$$|\psi_2\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -i \\ 0 \end{pmatrix} = -i|0\rangle$$

$$|\psi_3\rangle = -i|0\rangle$$

$$|\psi_4\rangle = -i|0\rangle$$

Alt hatta,

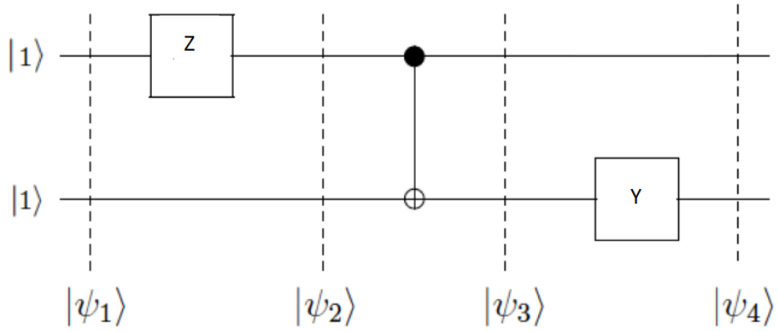
$$|\psi_1\rangle = |1\rangle$$

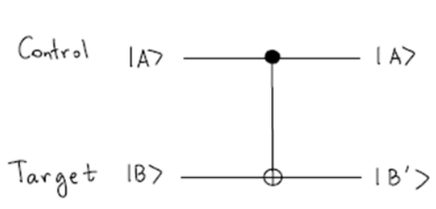
$$|\psi_2\rangle = |1\rangle$$

$$|\psi_3\rangle = |1\rangle$$

$$|\psi_4\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|1\rangle$$

Örnek-6:





|AB⟩	|AB'⟩
|00⟩	|00⟩
|01⟩	|01⟩
|10⟩	|11⟩
|11⟩	|10⟩

A kontrol grişi olduğu gibi geçer.
B çıkışı, A=0 ise B olduğu gibi geçer, A=1 ise B'nin tersi geçer,

Üst hatta,

$$|\psi_1\rangle = |1\rangle$$

$$|\psi_2\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|1\rangle$$

$$|\psi_3\rangle = -|1\rangle$$

$$|\psi_4\rangle = -|1\rangle$$

Alt hatta,

$$|\psi_1\rangle = |1\rangle$$

$$|\psi_2\rangle = |1\rangle$$

$|\psi_3\rangle = |0\rangle$; üst hat 1 olduğundan alt hattın tersi geçer.

$$|\psi_4\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ i \end{pmatrix} = i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = i|1\rangle$$

Örnek-6:

$$|\psi_2\rangle = \begin{pmatrix} -i \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -i \\ 0 \\ 0 \end{pmatrix} = -i \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = -i|01\rangle$$

$$|\psi_2\rangle = \begin{pmatrix} -i \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ i \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle$$

Örnek-7:

Entangled states

As we shall see, quantum computing draws its advantage from the fact that not all quantum states are separable. Consider the *two qubit unitary*

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

applied to the state

$|+\rangle \otimes |0\rangle = (1/\sqrt{2}) \begin{bmatrix} 1 & 1 \end{bmatrix}^T \otimes \begin{bmatrix} 1 & 0 \end{bmatrix}^T = \begin{bmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \end{bmatrix}^T$:

$$\text{CNOT}(|+\rangle \otimes |0\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix}$$

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

This is an an *entangled state* which cannot be separated as tensor product. We call CNOT an *entangling* operation (or "gate" in the quantum circuit model), and even though it operates on two qubits, Postulate 2 still applies – so it is still necessarily unitary.

Örnek-8:

More on entangled states and the Bell states

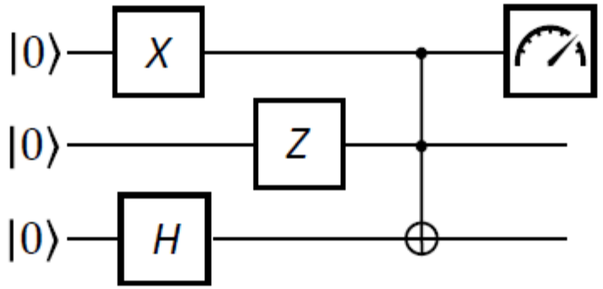
In quantum computing, we take non-separability as the definition of an entangled state, and so there are infinitely many entangled states. Four important two-qubit entangled states are the Bell states:

$$|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle) = (1/\sqrt{2}) \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$$
$$|\Phi^-\rangle = (1/\sqrt{2})(|00\rangle - |11\rangle) = (1/\sqrt{2}) \begin{bmatrix} 1 & 0 & 0 & -1 \end{bmatrix}$$
$$|\Psi^+\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle) = (1/\sqrt{2}) \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}$$
$$|\Psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle) = (1/\sqrt{2}) \begin{bmatrix} 0 & 1 & -1 & 0 \end{bmatrix}$$

Which form an orthonormal basis for $\mathbb{C}^4$ (**exercise: verify this**).

Örnek-9:

Quantum circuits



A quantum circuit is a tensor network of n qubits, with three stages:

- Initialisation of all qubits in the $|0\rangle$ state (denoted $|0\rangle^{\otimes n}$).
  - Sometimes it will be convenient to let the initial state be something other than $|0\rangle^{\otimes n}$ – but we should be able to efficiently prepare this initial state from $|0\rangle^{\otimes n}$ (that is, using a number of one- and two-qubit operations that is at most polynomial in the number of qubits).
- Some quantum gates, which represent unitary transformations.
- A final layer of measurements in the computational basis, on some or all of the qubits.
  - In fact, by the *principle of implicit measurement*, we can consider **all** qubits to be measured in the final layer.

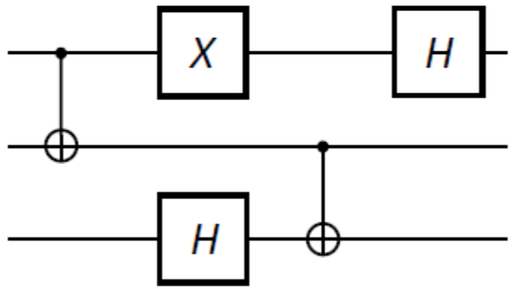
Örnek-10:

The matrix of a quantum circuit

As the quantum circuit (with the initialisation and measurement stages omitted) just represents a unitary evolution, we can express the whole thing as a matrix. We must follows the following two rules:

- Composition across wires is achieved by the tensor product.
- Composition along (sets of) wires is achieved by the normal matrix product, but right to left.

For example:



Is equal to:

$$(H \otimes I_4) \times (I_2 \otimes \text{CNOT}) \times (X \otimes I_2 \otimes H) \times (\text{CNOT} \otimes I_2)$$

where I_2 is the 2×2 identity, and $I_4 = I_2 \otimes I_2$ is the 4×4 identity.

Örnek-11:

A universal gate-set

Perhaps surprisingly, only three gates are needed to form a universal gate-set, two we have met: CNOT and H, and the third is:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

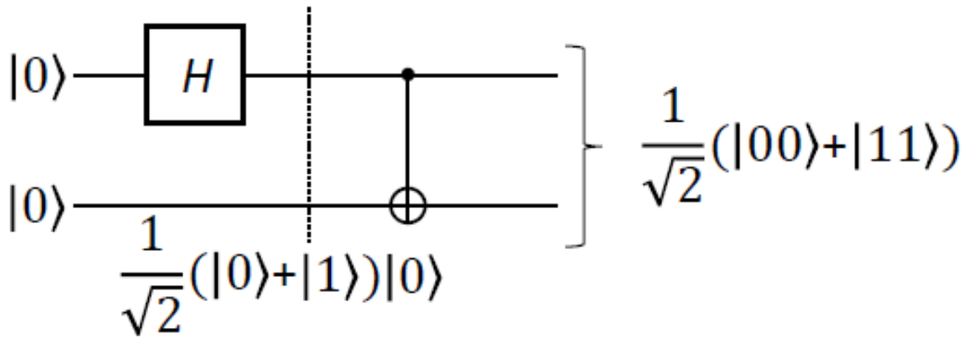
The introduction of this T gate is, however, crucial, and the famous Gottesman-Knill theorem holds that any circuit consisting of just the gates we have met thus far $X, Y, Z, H, S,$ CNOT can be efficiently simulated on a classical computer.

We can see that the single-qubit gates we have met so far can be expressed in terms of H and T as follows:

- $S = T^2$
- $Z = S^2$
- $X = HZH$
- $Y = iXZ = SXSZ$

Örnek-12:

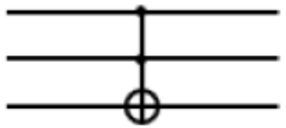
Quantum circuit example 1: entangling two qubits



Örnek-13:

The Toffoli gate

The Toffoli gate *does* provide a quantum generalisation of the classical AND gate, with three inputs and outputs.

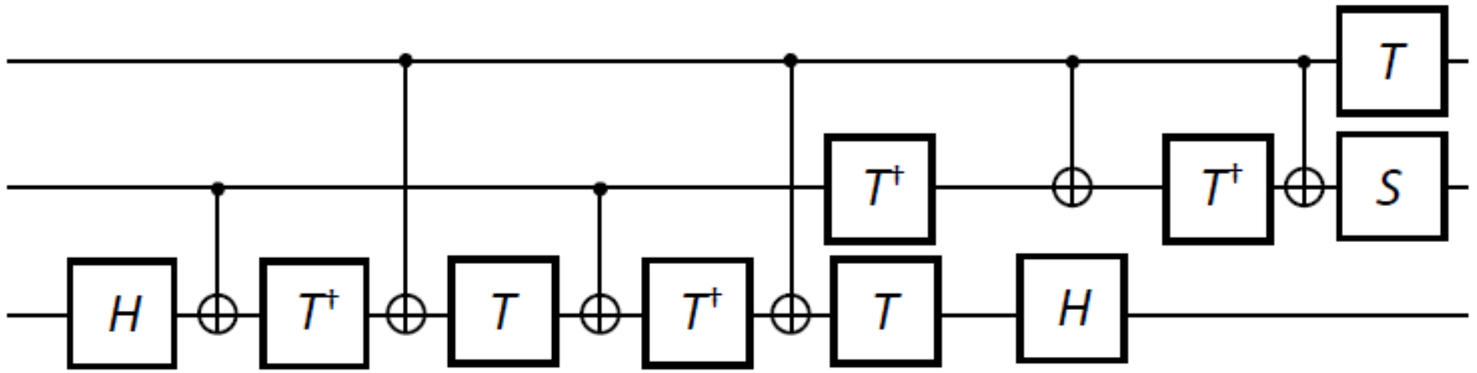


$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

When the first two inputs are classical bits ($|0\rangle$ or $|1\rangle$), and the third is $|0\rangle$ the third output is the AND of the first two inputs.

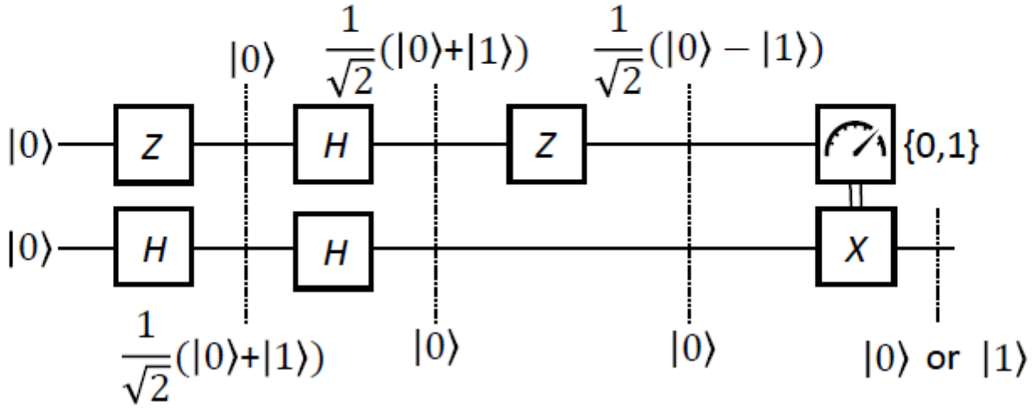
Örnek-14:

Quantum circuit example 2: decomposing the Toffoli gate into two-qubit unitaries



Örnek-15:

Quantum circuit example 3: self-inverse nature of H and classical control



- By convention, classical information (that is, a *bit* rather than a *qubit*) is represented by a double-line. So we should read this classical control as: if the measurement outcome is zero, then do nothing; if the measurement outcome is one, then perform the Pauli-X operation as shown.
- The inclusion of classical control may appear to contradict our definition of a quantum circuit as having measurement only in a final layer (which contains nothing other than measurement). However, the *principle of deferred measurement* means that any quantum circuit *can* be expressed in this form. But in practise it is often convenient to allow measurements to occur mid-circuit.