Quantum Computing

“Quantum Circuit-1”

Dr. Cahit Karakuş, Mart - 2021

Kimler?

- Amazon
- D-Wave Systems
- Microsoft
- Google
- Intel
- IBM
- IonQ
- Quantum Computing Inc. (QCI)
- Rigetti Computing
- Xanadu Quantum Technologies

Quantum - Matematik

- Yeni bir dil olan matematiğin dilini öğrenmemiz gerekiyor ve bu da quantum mekaniğini gerçekten anlamamızı sağlayacak tek şey, onu matematiksel olarak öğrenmektir.
- Super basic linear algebra, Hesaplamayı temel lineer cebirle temsil etme (Vektörler ve Matrisler), Matris çarpımları, Özdeğerler, Özvektörler
- Qubits, Superpozition and Quantum logic gates
- Kuantum bilgisayar (ALU), klasik bir bilgisayardan daha iyi performans gösterir.
- Bir kuantum bilgisayarın klasik bir problemi yendiği en basit problem.
- Bonus konular: kuantum dolanıklığı ve ışınlanma

Representing classical bits as a vector

One bit with the value 0, also written as $|0\rangle$ (Dirac vector notation)

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

One bit with the value 1, also written as $|1\rangle$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Matrix Multiplication

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax + by + cz \\ dx + ey + fz \\ gx + hy + iz \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Tensor product of vectors

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \\ x_1 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \otimes \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 z_0 \\ x_0 y_0 z_1 \\ x_0 y_1 z_0 \\ x_0 y_1 z_1 \\ x_1 y_0 z_0 \\ x_1 y_0 z_1 \\ x_1 y_1 z_0 \\ x_1 y_1 z_1 \end{pmatrix}$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Represinting multiple cbits

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad |11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

$$|4\rangle = |100\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix}$$

- We call this tensored representation the **product state**
- We can **factor** the product state back into the **individual state** representation
- The product state of n bits is a vector of size 2^n

Örnek:

- $|8\rangle = |100\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

Örnek:

$$H_0 Z_0 H_0 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X_0$$

$$H_0 Z_0 H_0 |\psi\rangle = X_0 |\psi\rangle$$

$$HZH = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X$$

Reversible Computing

- Reversible means given the operation and output value, you can find the input value
  - For $Ax = b$, given b and A, you can uniquely find x
- Operations which permute are reversible; operations which erase & overwrite are not
  - Identity and Negation are reversible
  - Constant-0 and Constant-1 are not reversible
- Quantum computers use only reversible operations, so we will only care about those
  - In fact, all quantum operators *are their own inverses*

Operations on multiple cbits: CNOT

- Operates on pairs of bits, one of which is the "control" bit and the other the "target" bit
- If the control bit is 1, then the target bit is flipped
- If the control bit is 0, then the target bit is unchanged
- The control bit is always unchanged
- With most-significant bit as control and least-significant bit as target, action is as follows:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CNOT:

- Çıkışdaki ilk bit her zaman girişdeki ilk bit değerini alır.
- İlk 0 ise çıkışdaki ikinci bit girişdeki ikinci bit değerini alır.
- İlk bit 1 ise çıkışdaki ikinci bit girişdeki ikinci bitin tersini alır.

Operations on multiple cbits: CNOT

$$C|00\rangle = C\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = |00\rangle$$

$$C|01\rangle = C\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = |01\rangle$$

Operations on multiple cbits: CNOT

$$C|10\rangle = C\left(\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = |11\rangle$$

$$C|11\rangle = C\left(\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} = |10\rangle$$

Qubits and Superpozition

- Surprise! We've actually been using qbits all along!
- The cbit vectors we've been using are just special cases of qbit vectors
- A qbit is represented by $\binom{a}{b}$ where a and b are Complex numbers and $||a||^2 + ||b||^2 = 1$
  - The cbit vectors $\binom{1}{0}$ and $\binom{0}{1}$ fit within this definition
  - Don't worry! For this presentation, we'll only use familiar Real numbers.
- Example qbit values:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \quad \begin{pmatrix} -1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

Örnek: Qubits and Superpozition

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = 1$$

Qubits and Superpozition

- How can a qbit to have a value which is not 0 or 1? This is called superposition.
- Superposition means the qbit is both 0 and 1 and the same time
- When we **measure** the qbit, it **collapses** to an actual value of 0 or 1
  - We usually do this at the end of a quantum computation to get the result
- If a qbit has value $\binom{a}{b}$ then it collapses to 0 with probability $\|a\|^2$ and 1 with probability $\|b\|^2$
  - For example, qbit $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ has a $\left\|\frac{1}{\sqrt{2}}\right\|^2 = \frac{1}{2}$ chance of collapsing to 0 or 1 (coin flip)
  - The qbit $\binom{1}{0}$ has a 100% chance of collapsing to 0, and $\binom{0}{1}$ has a 100% chance of collapsing to 1

Qubits and Superpozition

- Multiple qbits are similarly represented by the tensor product $\binom{a}{b} \otimes \binom{c}{d} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$
  - Note that $\|ac\|^2 + \|ad\|^2 + \|bc\|^2 + \|bd\|^2 = 1$
- For example, the system $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$ (note that $\left\|\frac{1}{2}\right\|^2 = \frac{1}{4}$, and $\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$)
  - There's a ¼ chance each of collapsing to $|00\rangle, |01\rangle, |10\rangle$, or $|11\rangle$

Operations on qubits

- How do we operate on qbits? The same way we operate on cbits: with matrices!
- All the matrix operators we've seen also work on qbits (bit flip, CNOT, etc.)
- Matrix operators model the effect of some device which manipulates qbit spin/polarization without measuring and collapsing it

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix}$$

- There are several important matrix operators which only make sense in a quantum context

The Hadamard gate

- The Hadamard gate takes a 0- or 1-bit and puts it into exactly equal superposition

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

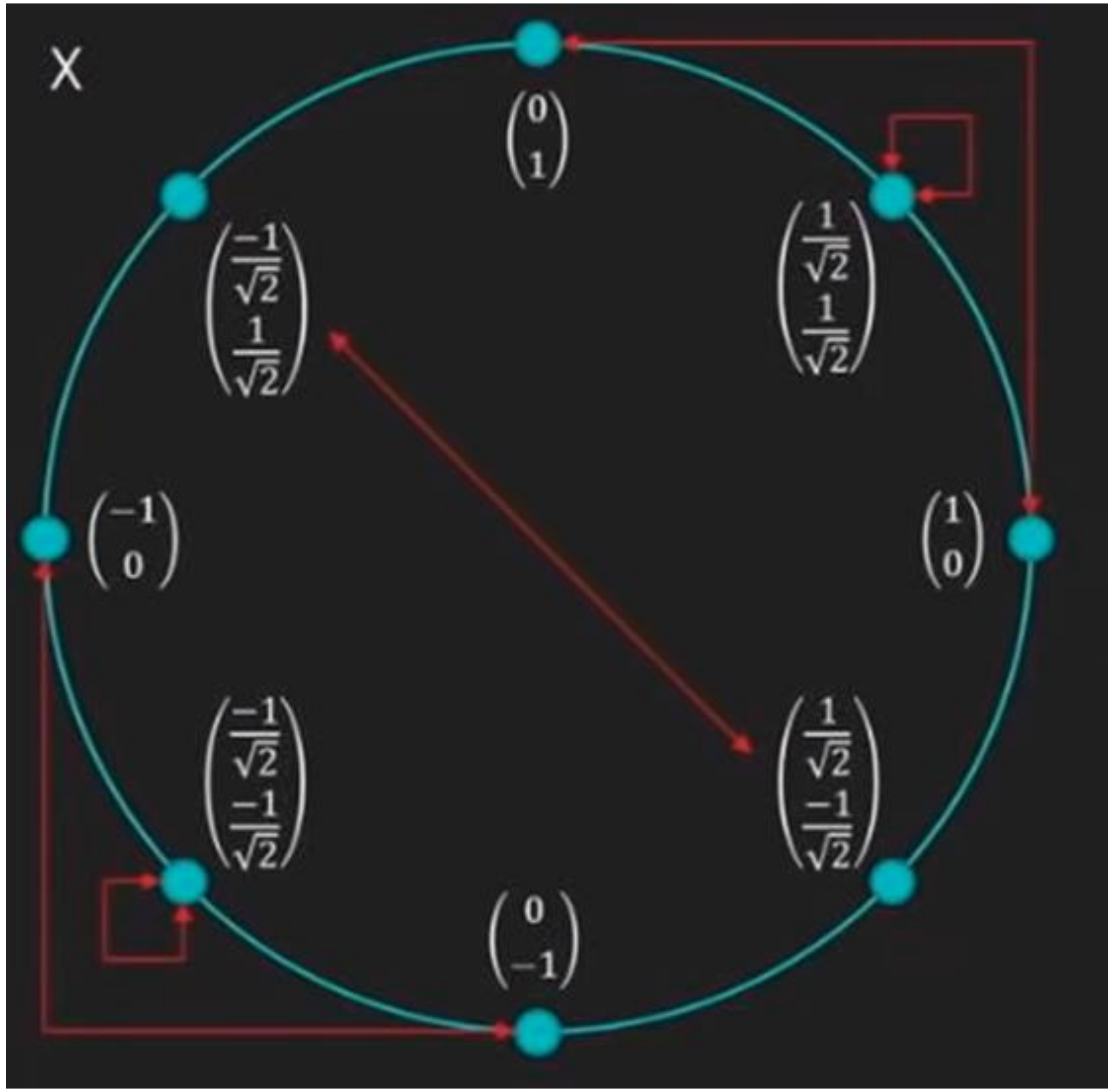
The Hadamard gate

- The Hadamard gate also takes a qbit in exactly-equal superposition, and transforms it into a 0- or 1-bit! (This should be unsurprising – remember operations are their own inverse!)

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- We can transition out of superposition without measurement!
- We can thus structure quantum computation deterministically instead of probabilistically

The unit circle state machine (X)



$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ qubitler vektörler ile temsil edilir.

- $\boldsymbol{X|0\rangle = ?}$
- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$

- $\boldsymbol{X|1\rangle = ?}$
- $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$

- $\boldsymbol{X}\begin{pmatrix}\mathbf{-1}\\\mathbf{0}\end{pmatrix}$=?
- $\mathrm{X}=\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
- $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}-1\\0\end{pmatrix}=\begin{pmatrix}0\\-1\end{pmatrix}=-|1\rangle$

- $\boldsymbol{X}\begin{pmatrix}\mathbf{0}\\\mathbf{-1}\end{pmatrix}$=?
- $\mathrm{X}=\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
- $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\-1\end{pmatrix}=\begin{pmatrix}-1\\0\end{pmatrix}=-|0\rangle$

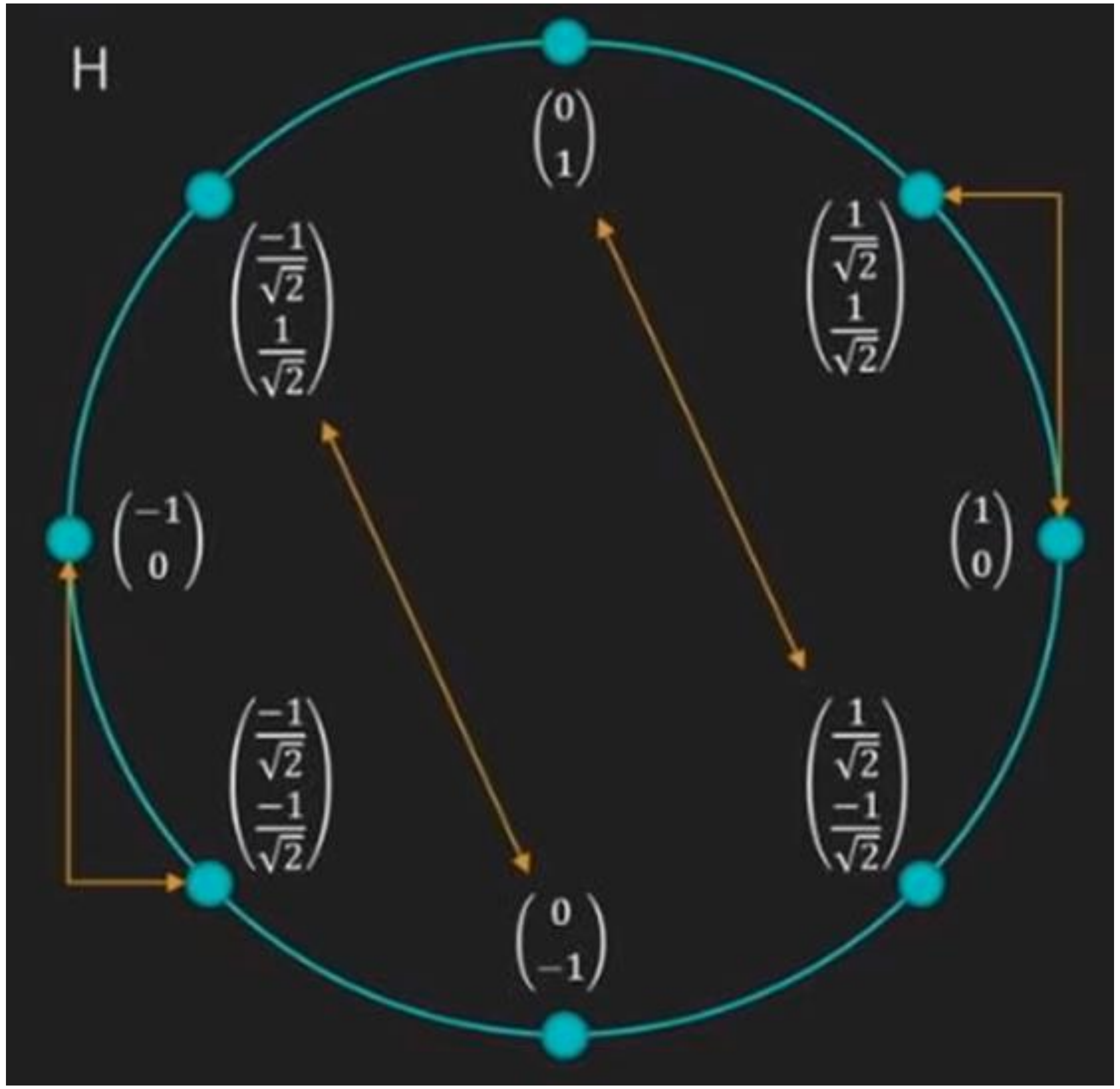
- $\boldsymbol{X}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}=?$
- $X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
- $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}$

- $\boldsymbol{X}\begin{pmatrix}-\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}=?$
- $X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
- $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}-\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}=\begin{pmatrix}-\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}$

- $\boldsymbol{X}\begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$=?
- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$

- $\boldsymbol{X}\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$=?
- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$

The unit circle state machine (H)



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

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ qubitler vektörler ile temsil edilir.

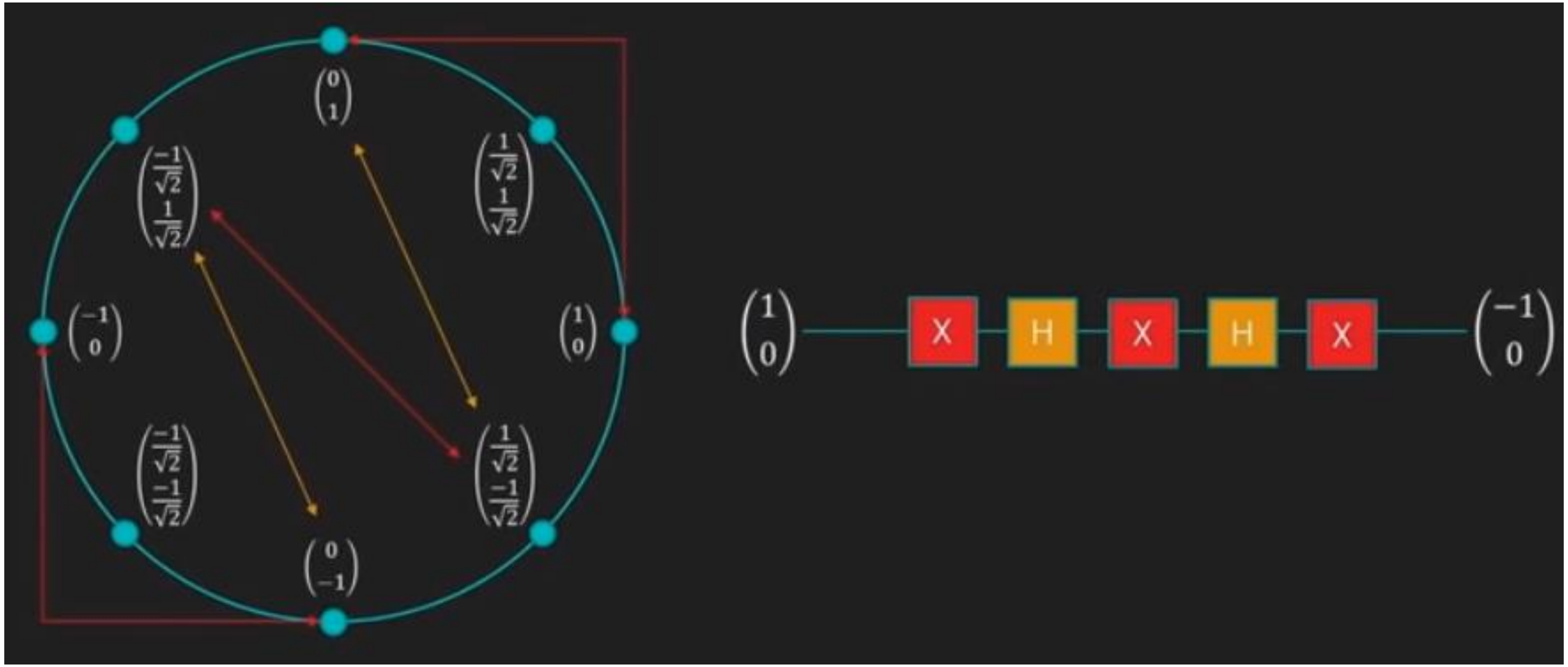
- $H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

- $H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

- $\boldsymbol{H}\begin{pmatrix}\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\\ \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\\ \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\frac{\mathbf{2}}{\sqrt{\mathbf{2}}}\\ \mathbf{0}\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle$

- $\boldsymbol{H}\begin{pmatrix}\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\\ -\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\\ -\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\mathbf{0}\\ \frac{\mathbf{2}}{\sqrt{\mathbf{2}}}\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$

The unit circle state machine



$$\begin{pmatrix}-1\\0\end{pmatrix}=-1\begin{pmatrix}1\\0\end{pmatrix}=-1|0\rangle=e^{i\pi}\ |0\rangle$$

$XHXHX|0\rangle$

- $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$=?
- $\frac{1}{2}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$=?
- $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}$=$\begin{pmatrix}0\\1\end{pmatrix}$
- $\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}$=$\begin{pmatrix}1\\-1\end{pmatrix}$
- $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\-1\end{pmatrix}$=$\begin{pmatrix}-1\\1\end{pmatrix}$
- $\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}-1\\1\end{pmatrix}$=-2$\begin{pmatrix}0\\1\end{pmatrix}$
- -2*$\frac{1}{2}\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}$=-$\begin{pmatrix}1\\0\end{pmatrix}$= $-|0\rangle$=$e^{i\pi}$ $|0\rangle$

Recap

- Cbits are just a special case of qbits, which are 2-vectors of Complex numbers
- Qbits can be in superposition, and are probabilistically collapsed to cbits by measurement
- Multi-qbit systems are tensor products of single-qbit systems, like with cbits
- Matrices represent operations on qbits, same as with cbits
- The Hadamard gate takes 0- and 1-bits to equal superposition, and back
- We can think of qbits and their operations as forming a state machine on the unit circle
  - Actually the unit sphere if we use complex numbers

The Deutsch oracle

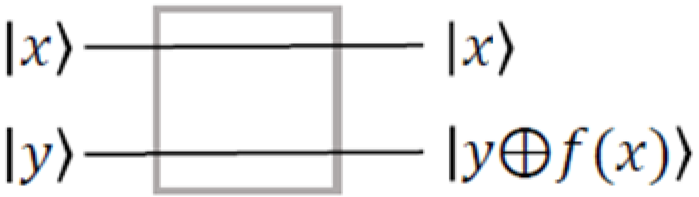
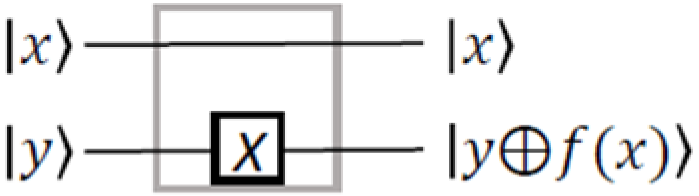
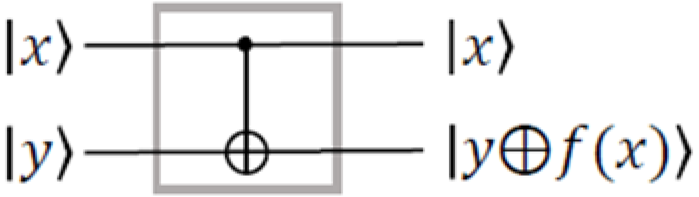
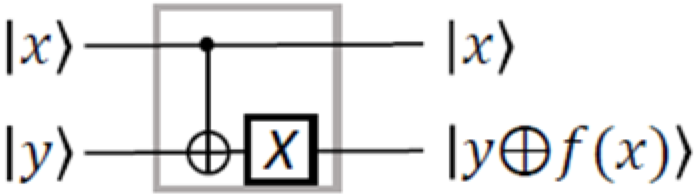
- Imagine someone gives you a black box containing a function on one bit
  - Recall! What are the four possible functions on one bit?
- You don't know which function is inside the box, but can try inputs and see outputs
- How many queries would it take to determine the function on a classical computer?
- How many on a quantum computer?

Deutsch kehaneti

- Kapınıza geldiğimi ve size bir paket verdiğimi hayal edin, paket sadece kara kutu, korkunç bir şekilde mevcut. Bir bit üzerinde bir işlevi olan bir kara kutudur. Bir bitte bir sonraki slaytta verilen dört fonksiyondan biri var, bunların ne olduğunu hatırlıyor musunuz? Sıfır ayarla, bir ayarla, kimlik, gösterge. Hangisinin kara kutunun içinde olduğunu size söylemem.
- Kara kutunun içinde hangi işlevin olduğunu anlamak için klasik bir bilgisayarda kaç sorgu gerekir? İki, tam olarak. Sıfır gönder bak ne çıkacak, bir gönder bak ne çıkacak. Böylece bu, hangi işlev olduğunu benzersiz bir şekilde tanımlayacaktır. 00, 01, 10,11
- Şimdi, bir quantum bilgisayarda bunun için kaç sorgu gerektirdiğini düşünün? İki yanıtı yanlış. Quantum bilgisayarlar tüm değerleri aynı anda hesaplamazlar. Günün sonunda, qübitinizi tek bir bilgi bitine daraltırsınız ve tek bir bilgi, dört işlevden birini benzersiz bir şekilde tanımlamak için yeterli olmaz mı? En azından iki bite ihtiyacın var. Bu aslında bir quantum bilgisayarda iki sorgu gerektirir.

Constant and balanced function on a single bit

If the input, x, is a single bit (as is the output), then we have four possible functions:

Function	x	$f(x)$	Type	Unitary
$f(x) = 0$	0 1	0 0	Constant	
$f(x) = 1$	0 1	1 1	Constant	
$f(x) = x$	0 1	0 1	Balanced	
$f(x) = x \oplus 1$	0 1	1 0	Balanced	

$\oplus$: Klasik bit aritmetiğini tanımlar

0+0=0

0+1=1

1+0=1

1+1=0 elde var 1, 1 ihmal edilir.

Black Box: xout=x, yout=y⊕f(x)

x	y	f(x)	Xout=x	f(x)⊕ y
0	0	0	0	0
0	1	0	0	1
1	0	0	1	0
1	1	0	1	1

x	y	f(x)=x	Xout=x	f(x)⊕ y
0	0	0	0	0
0	1	0	0	1
1	0	1	1	1
1	1	1	1	0

Toplama, XOR

x	y	f(x)	Xout=x	f(x)⊕ y
0	0	1	0	1
0	1	1	0	0
1	0	1	1	1
1	1	1	1	0

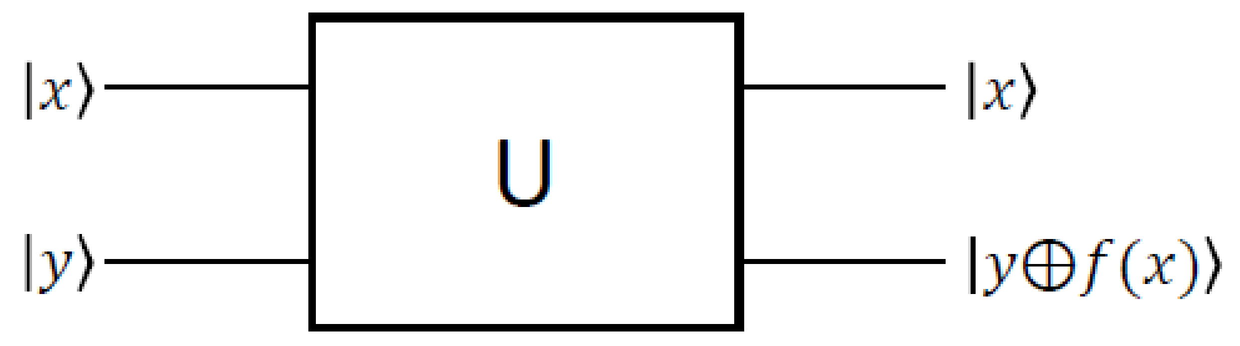
x	y	f(x)=x+1	Xout=x	f(x)⊕ y
0	0	1	0	1
0	1	1	0	0
1	0	0	1	0
1	1	0	1	1

Karşılaştırma, XNOR

Deutsch's algorithm set-up

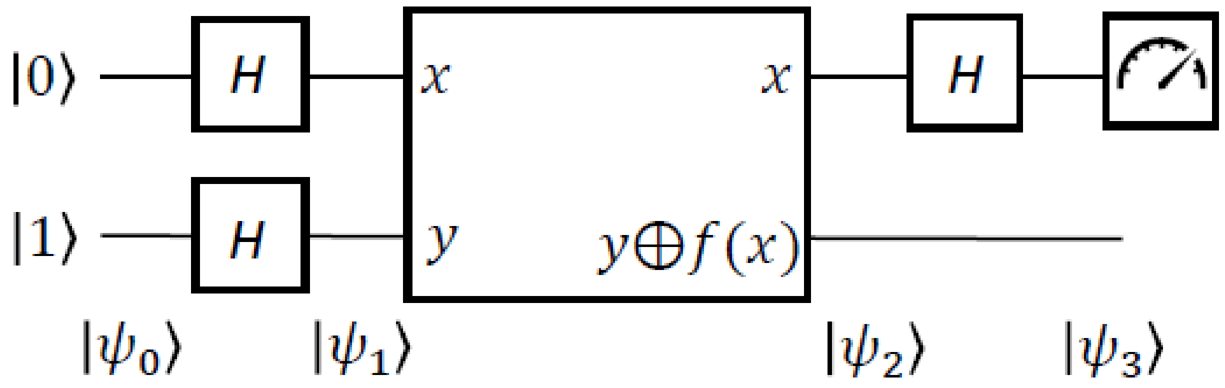
We want to find out whether a particular function, with one input bit and one output bit is constant or balanced. Classically, we need to evaluate the function *twice* (i.e., for input $= 0$ and input $= 1$), but remarkably, we only need to evaluate the function *once* quantumly, by using Deutsch's algorithm.

We have a two qubit unitary, which is one of the four on the previous slide (we don't know which):



Which we are going to incorporate into a quantum circuit.

Deutsch's algorithm (1)



Initially we prepare the state:

$$|\psi_0\rangle = |01\rangle$$

Which the initial Hadamard gates put in the superposition state:

$$\begin{aligned} |\psi_1\rangle &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) \end{aligned}$$

Deutsch's algorithm (2)

$$|\psi_1\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Next the unitary is implemented, which sets the second qubit to $y \oplus f(x)$, so we have four options for $|\psi_2\rangle$:

$$\begin{array}{ll} f(x) = 0 & |\psi_2\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \\ f(x) = 1 & |\psi_2\rangle = \frac{1}{2}(|01\rangle - |00\rangle + |11\rangle - |10\rangle) \\ f(x) = x & |\psi_2\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) \\ f(x) = x \oplus 1 & |\psi_2\rangle = \frac{1}{2}(|01\rangle - |00\rangle + |10\rangle - |11\rangle) \end{array}$$

which factorises as:

$$|\psi_2\rangle = \begin{cases} \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1) \end{cases}$$

That is the two balanced cases differ only by an unobservable global phase (and likewise for the two constant cases).

Deutch algoritmasında fonksiyonun 4 durumu mevcuttur.
4 durum için Box'ın üst tarafındaki çıkışı, x=x olur. Box'ın alt tarafındaki çıkışı = $y \oplus f(x)$ dir.

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$, elde var 1 dir.

Deutsch's algorithm (3)

$$|\psi_2\rangle = \begin{cases} \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0)=f(1) \\ \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0)\neq f(1) \end{cases}$$

The next step is to use the Hadamard gate to interfere the superposition on the first qubit, which yields:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0)=f(1) \\ \pm|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0)\neq f(1) \end{cases}$$

The final step is to measure the first qubit, and we can see that the outcome will always be 0 if the function is constant, and 1 if balanced.

We can see that superposition and interference, in some sense, play complementary roles: we prepare a state in superposition, perform some operations, and then use interference to discern some global property of the state.

The Deutsch oracle

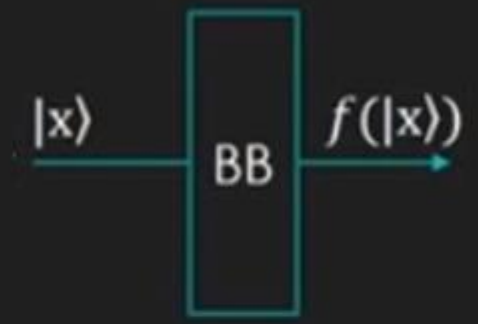
- What if you want to check whether the unknown function is constant, or variable?
  - Constant-0 & constant-1 are constant, identity & negation are variable
- How many queries would it take on a classical computer?
- How many on a quantum computer?

- We can do this in a single query on a quantum computer. We can tell whether its consants or variable. This like undeniably outperforms a classical computer

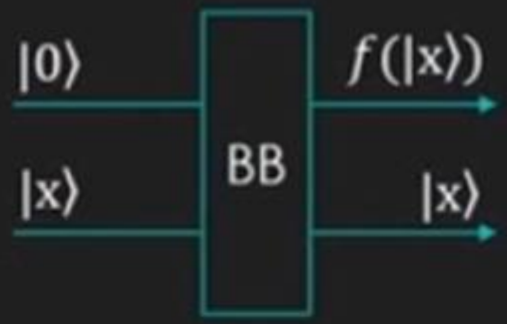
The Deutsch oracle

- How do we write nonreversible functions in a reversible way?
- Common hack: add an additional **output qbit** to which the function action is applied
- We thus have to rewire our black box:

Before:

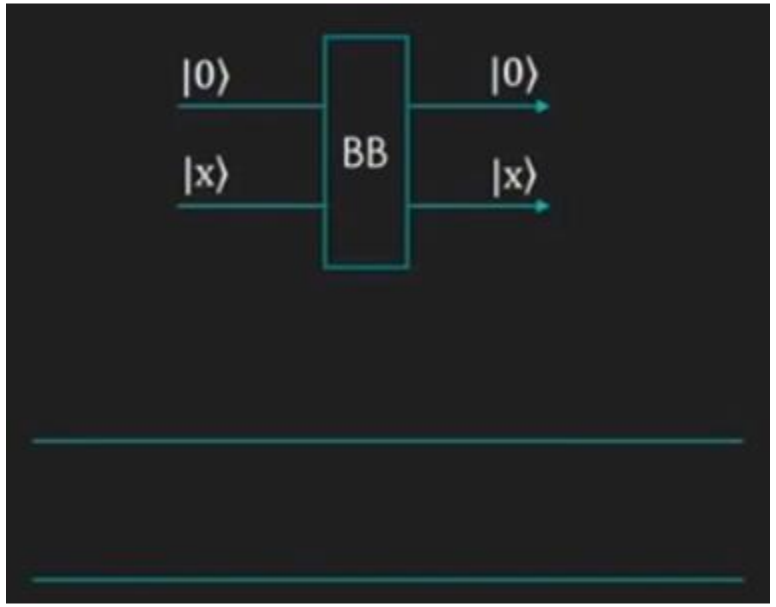


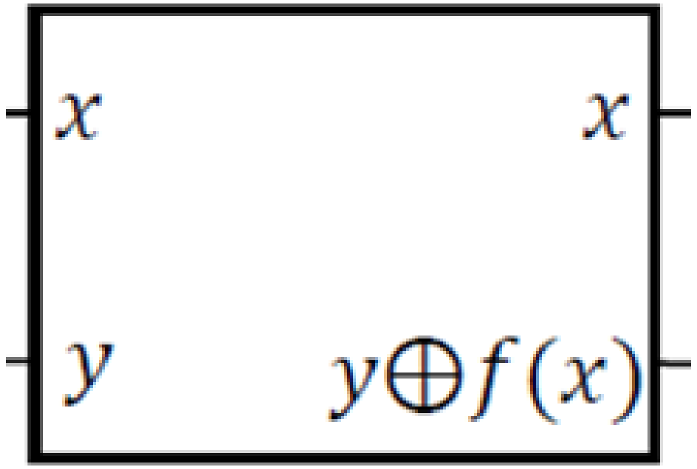
After:

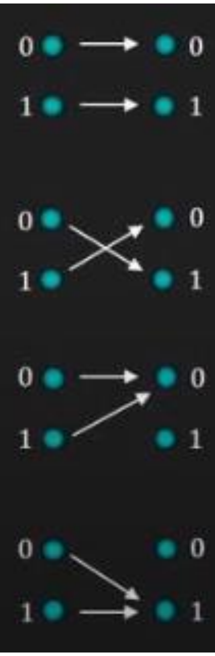


- The black box leaves the **input qbit** unchanged, writing function output to **output qbit**

The Deutsch oracle: Constant-0

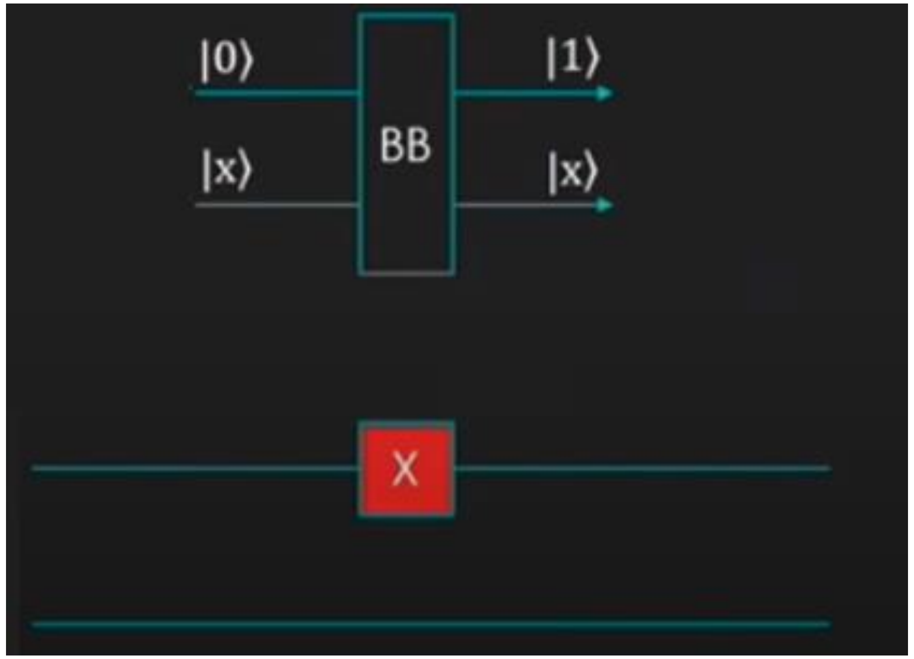


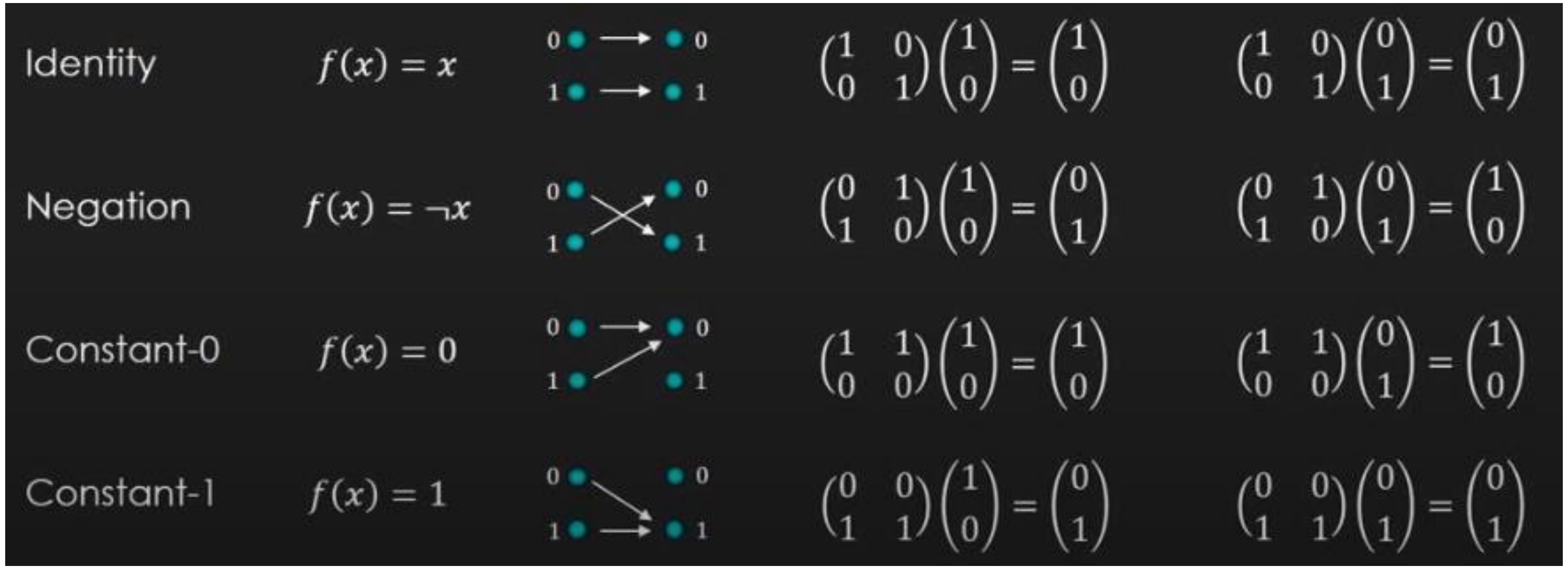




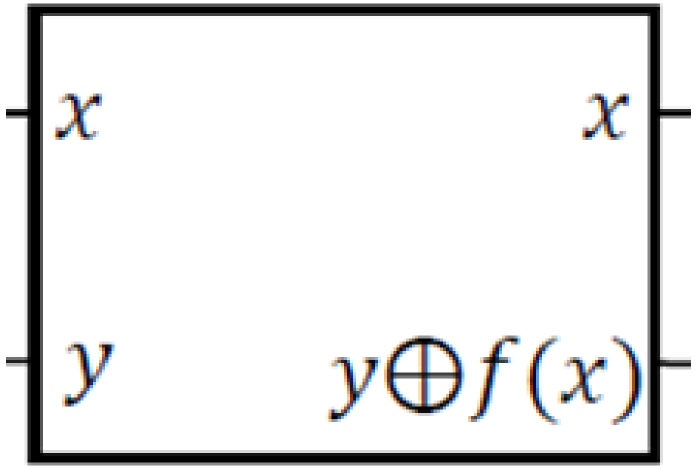
Identity	$f(x) = x$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$
Negation	$f(x) = \neg x$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$
Constant-0	$f(x) = 0$	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$
Constant-1	$f(x) = 1$	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}$

The Deutsch oracle: Constant-1

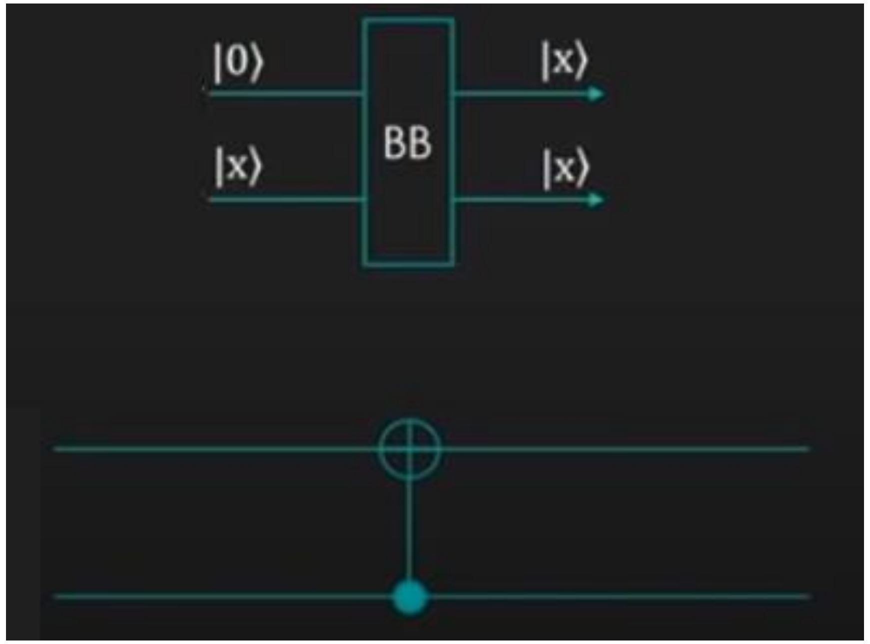


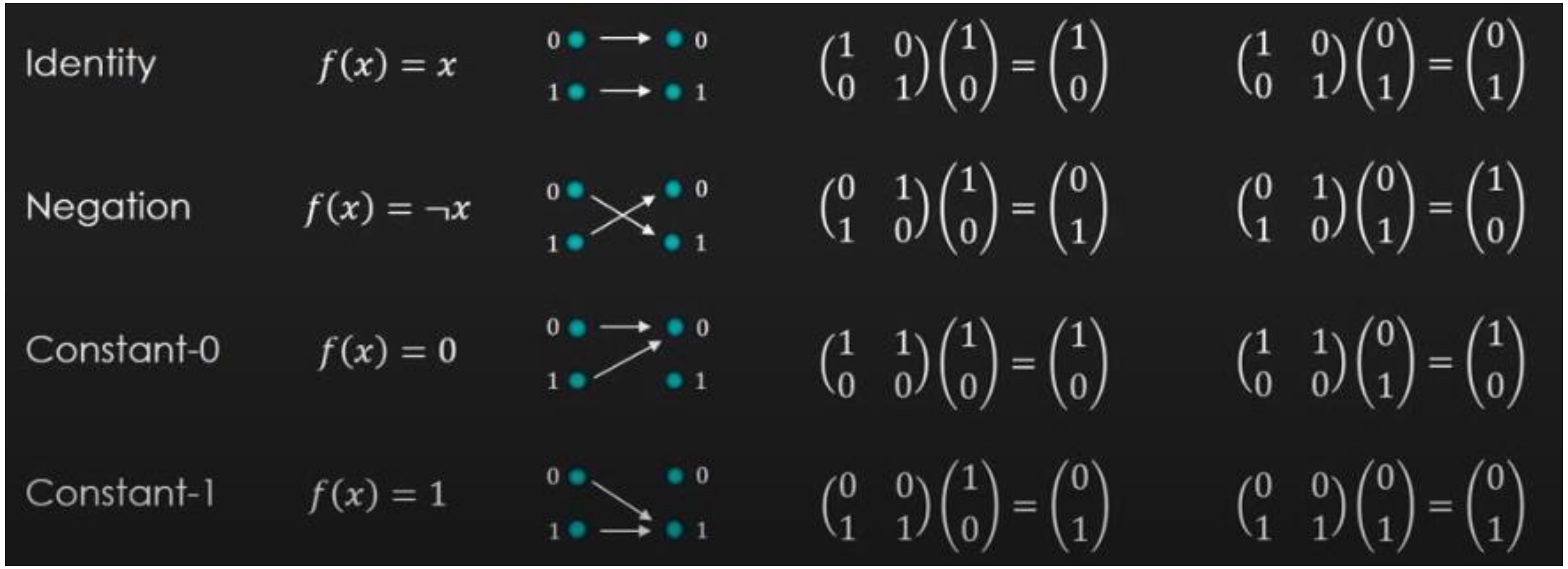


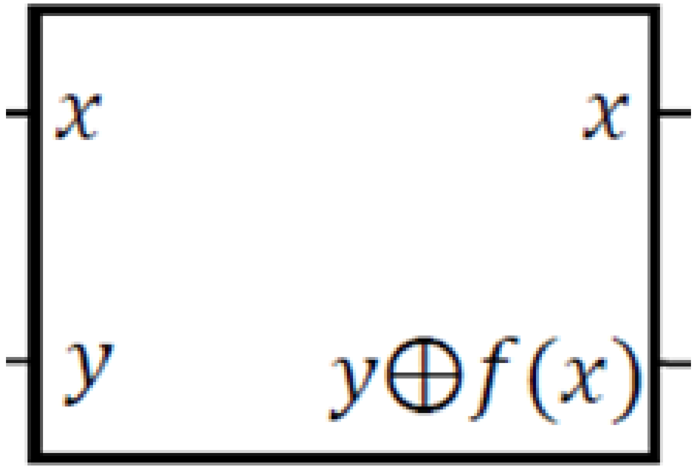
Identity	$f(x) = x$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$
Negation	$f(x) = \neg x$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$
Constant-0	$f(x) = 0$	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$
Constant-1	$f(x) = 1$	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$



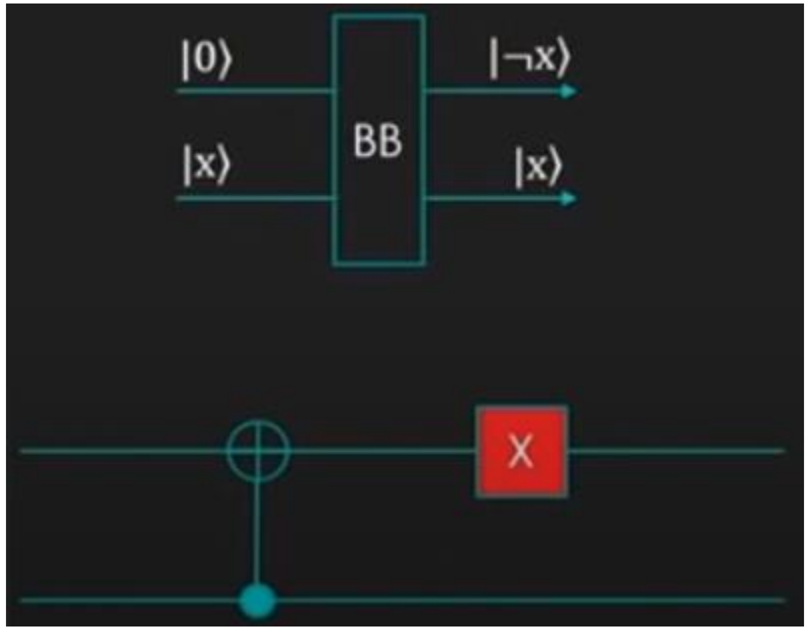
The Deutsch oracle: identity

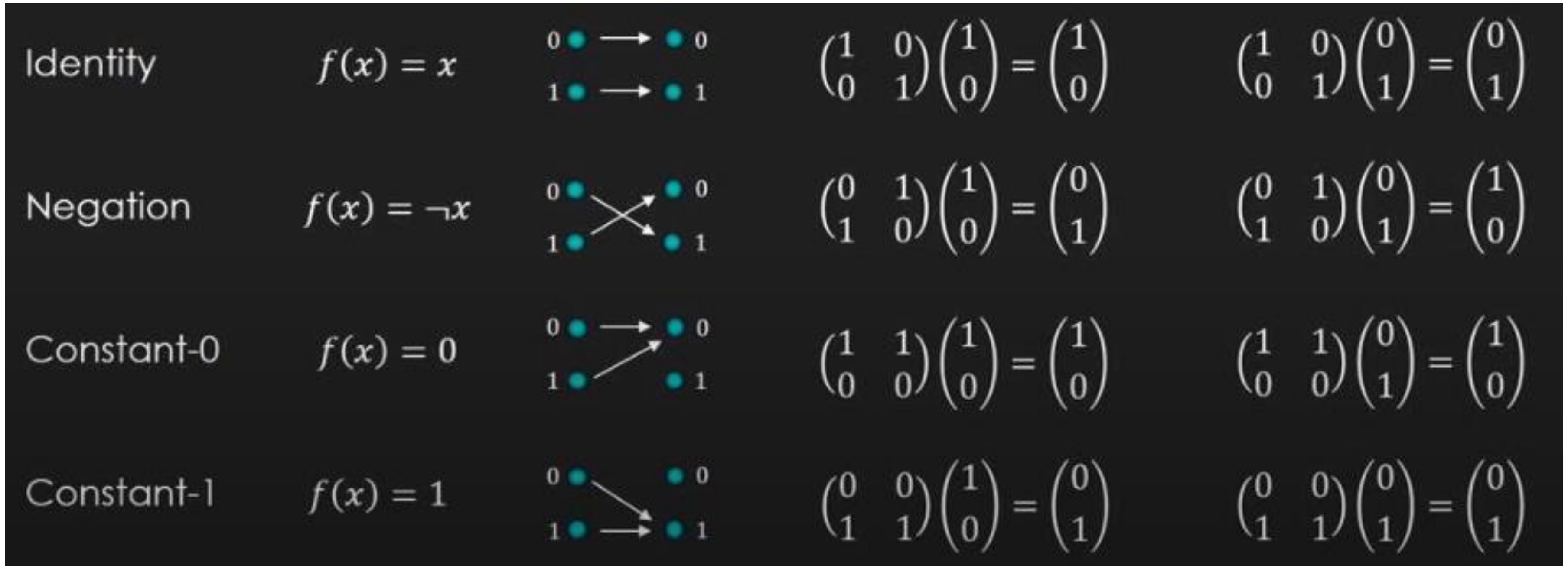




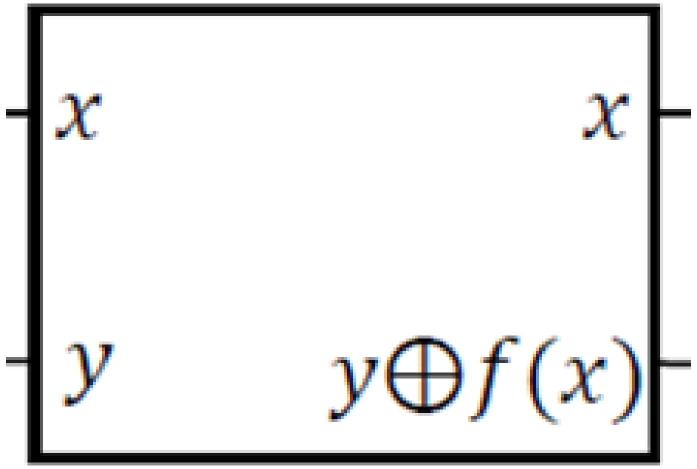


The Deutsch oracle: negation



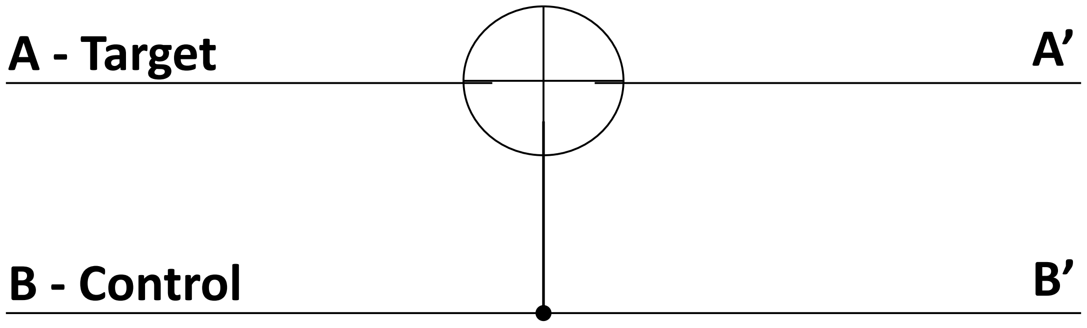


Identity	$f(x) = x$	0 → 0, 1 → 1	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$
Negation	$f(x) = \neg x$	0 → 1, 1 → 0	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$
Constant-0	$f(x) = 0$	0 → 0, 1 → 0	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$
Constant-1	$f(x) = 1$	0 → 1, 1 → 1	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0 & 0\\1 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$



Quantum Gates - Controlled NOT

- A gate which operates on two qubits is called a ***Controlled-NOT (CN) Gate.*** If the bit on the control line is 1, invert the bit on the target line. B= 0 ise B'=B, A'=A olarak çıkış üretiyor, B=1 ise B'=B, A'=not(A) olarak çıkış üretiyor.

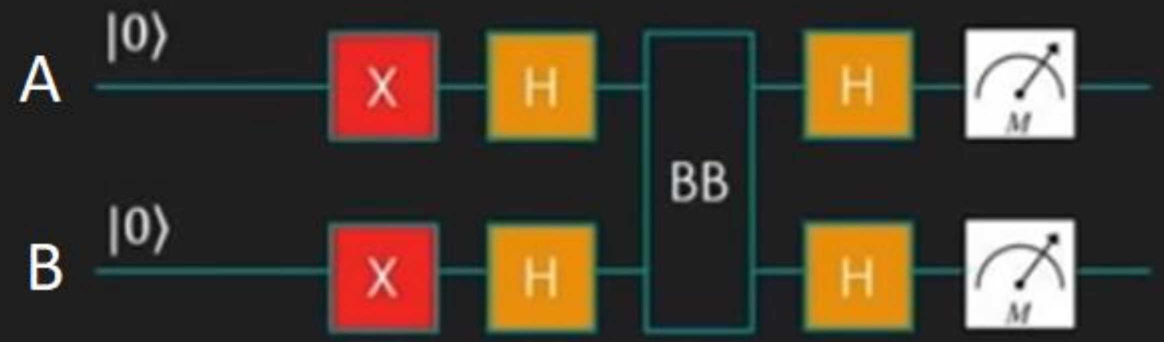


Input		Output	
A	B	A'	B'
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Not: CN lojik kapısı, XOR geçidine benzer bir davranışa sahiptir ve onu tersinir hale getirmek için bazı ekstra bilgiler vardır.

Örnek: The Deutsch oracle

- How do we solve it on a quantum computer in one query?

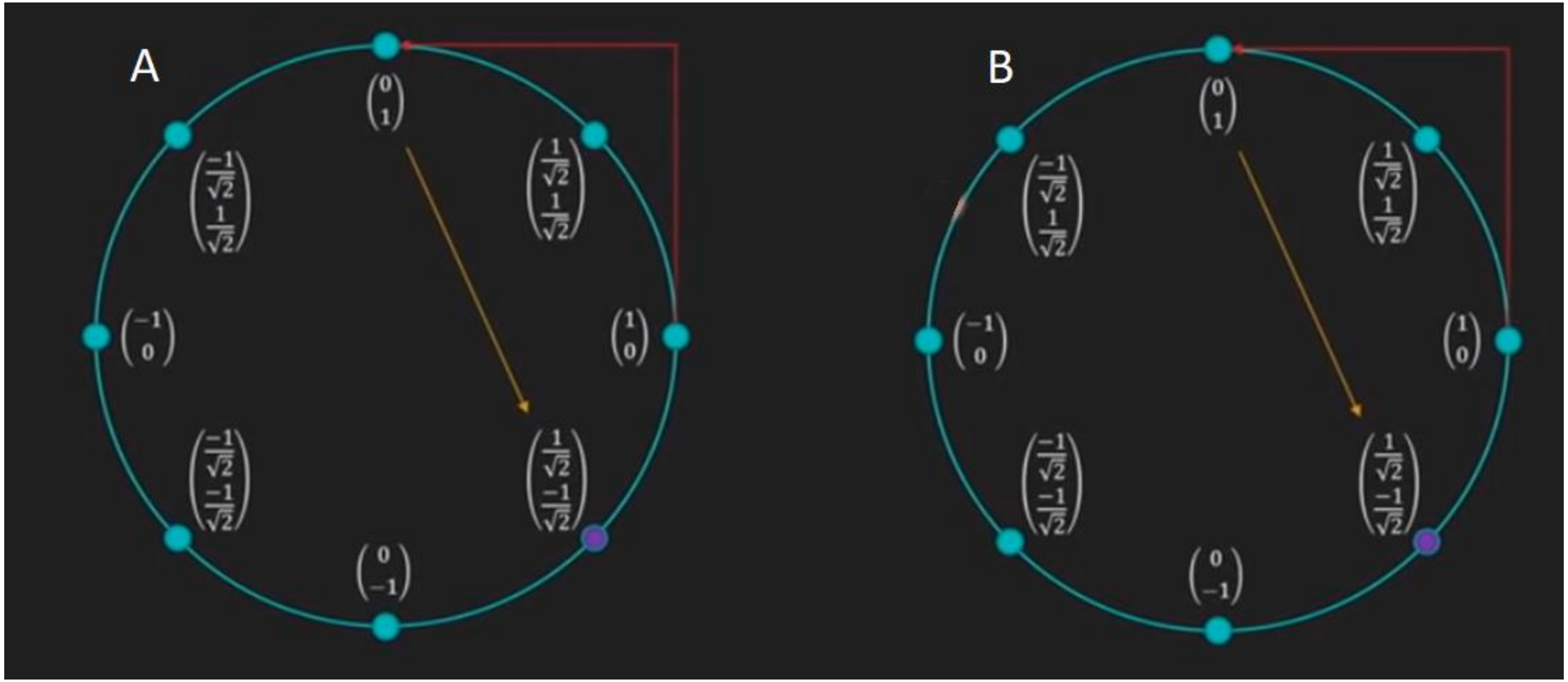


- If the black-box function is constant, system will be in state |11⟩ after measurement
- If the black-box function is variable, system will be in state |01⟩ after measurement

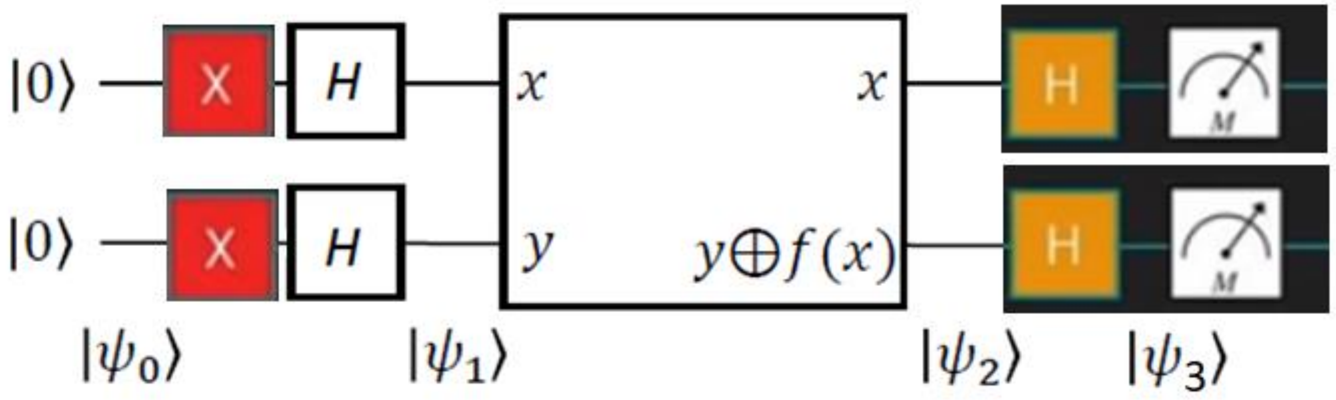
Black Box is a matrix.

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ve $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ qubitler vektörler ile temsil edilir.
- $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$
- Hadamard kapısı çıkışı,
- $HX|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ elde edilir.
- Black Box is a matrix.

The Deutsch oracle: preprocessing

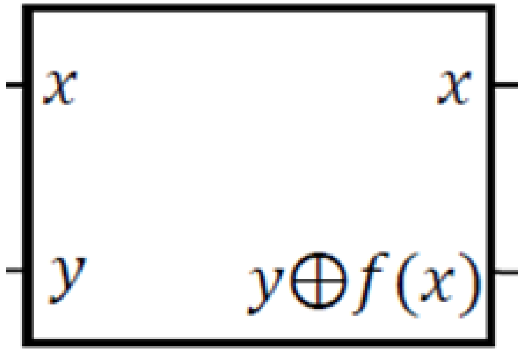


X-kapısı, ardından da Hadamard kapısı çıkışı yukardaki dairesel döngü ile hesaplanır.



- $\psi_0 = |00\rangle$
- $\psi_1 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $\psi_1 = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$
- $f(x)=0$, $\psi_2 = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

The Deutsch oracle: Constant-0

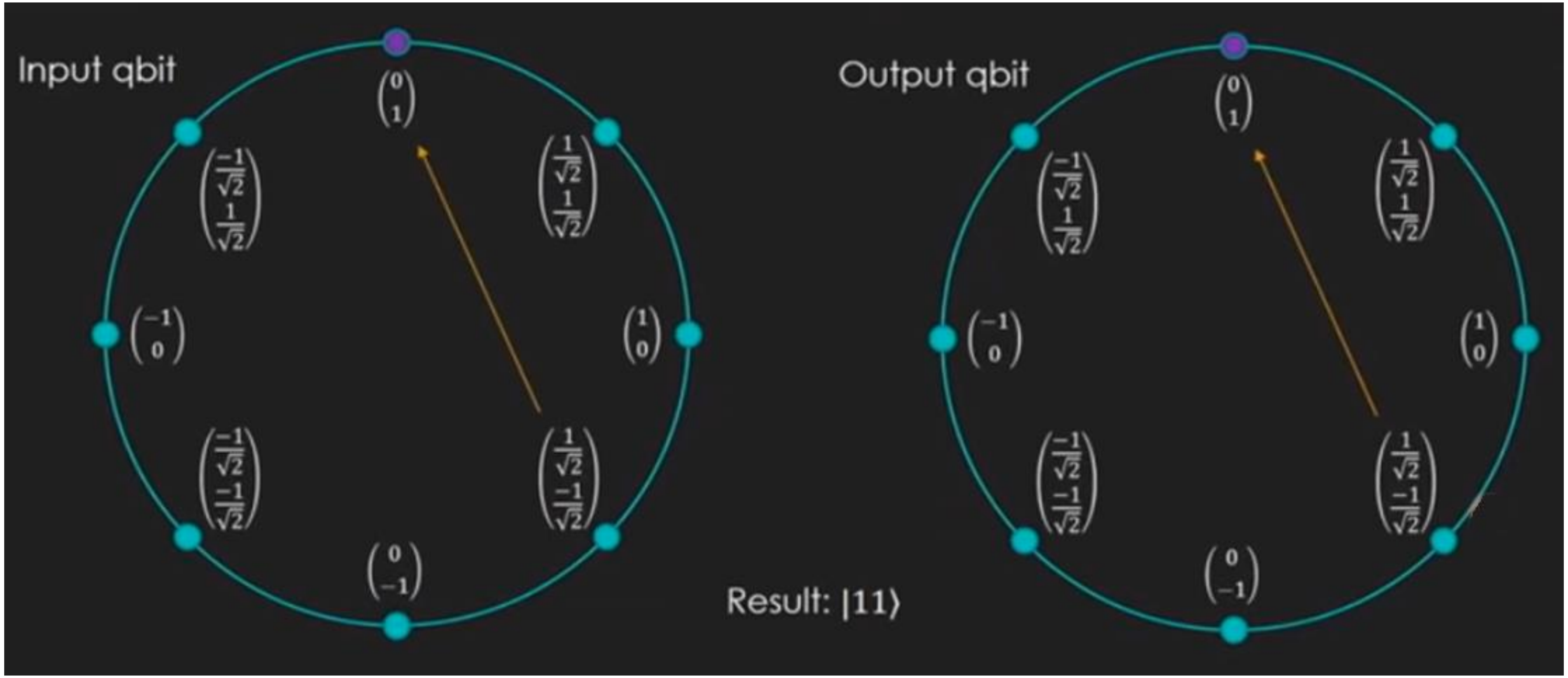


- Before BB $|\mathrm{x}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
- After BB $|\mathrm{x}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
- $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$

- Before BB $|y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
- f(x)=0, After BB $|y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
- $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle$

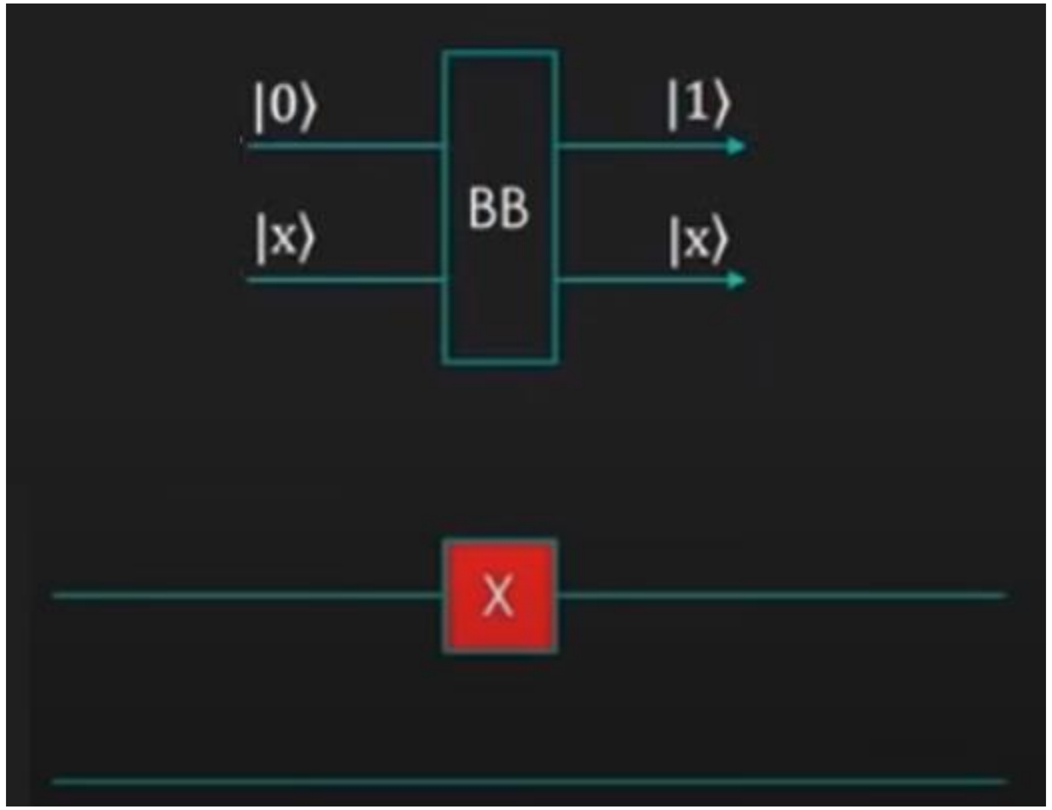
- Ölçülen Output= $|11\rangle$

The Deutsch oracle: Constant-0

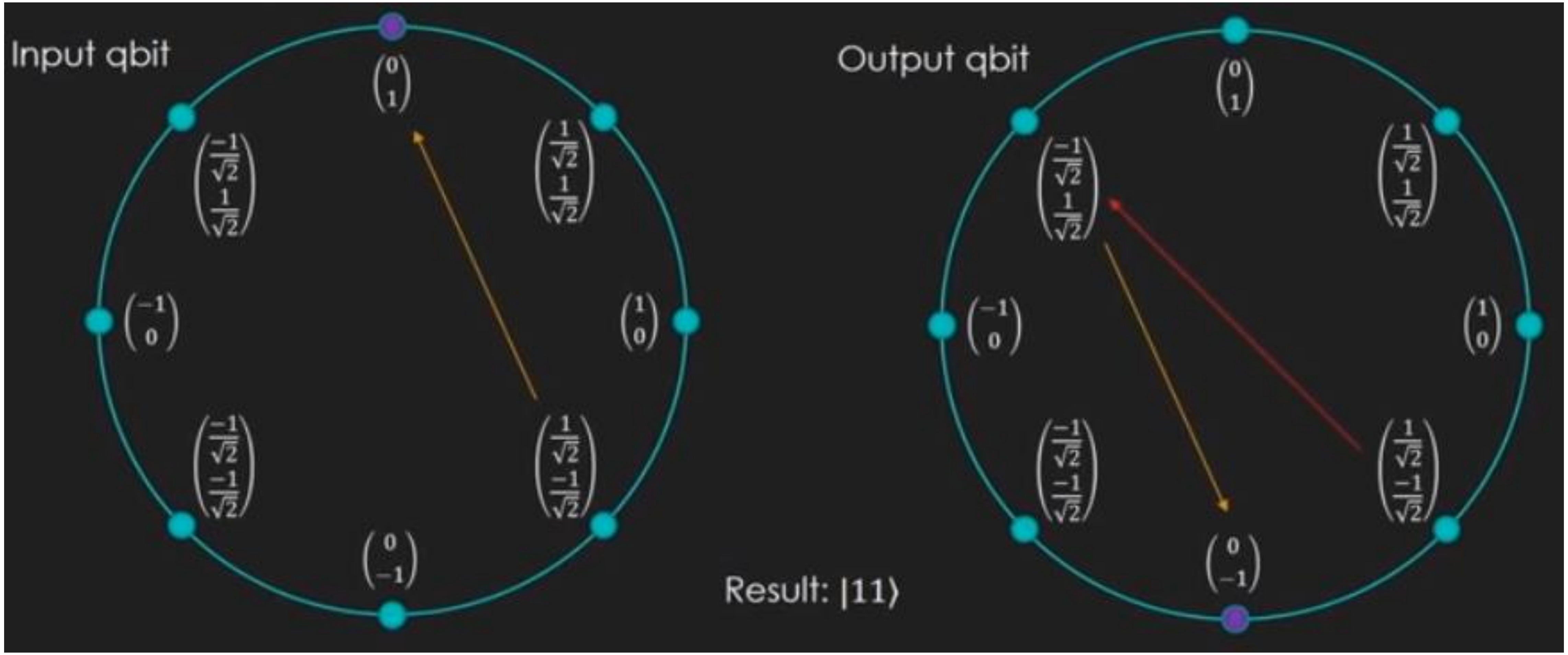


BB - çıkışı

The Deutsch oracle: Constant-1

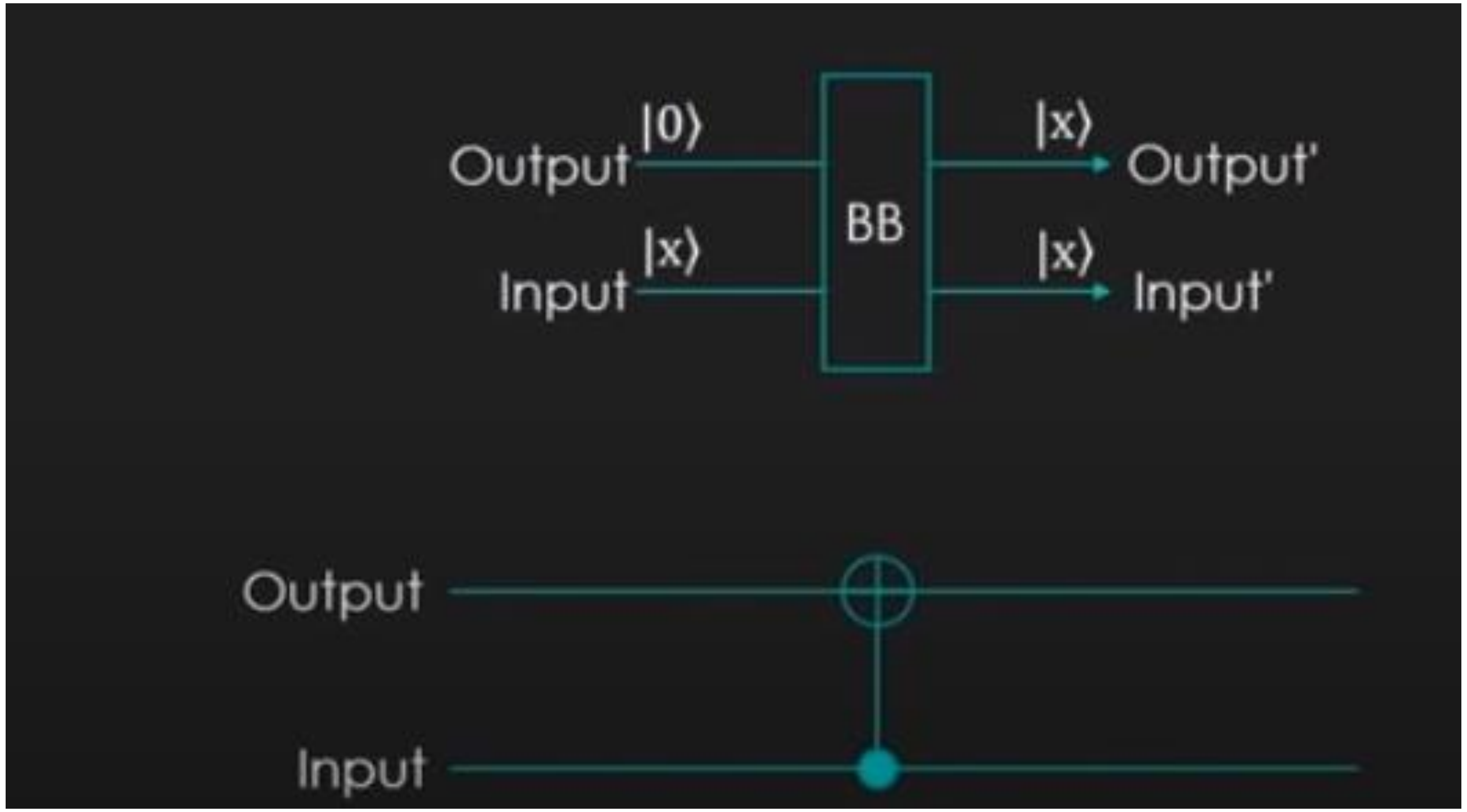


The Deutsch oracle: Constant-1

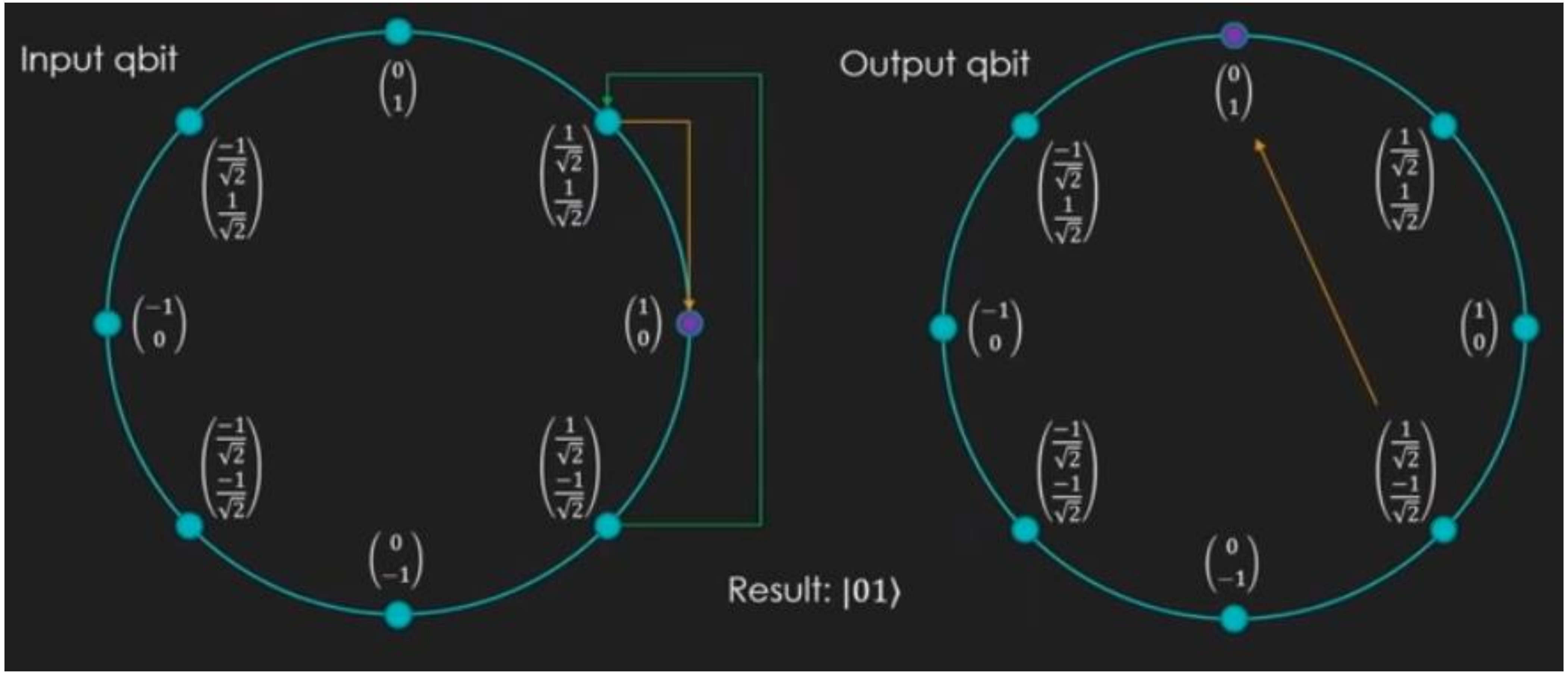


So is 100% probability of collapsing to one.

The Deutsch oracle: Identity



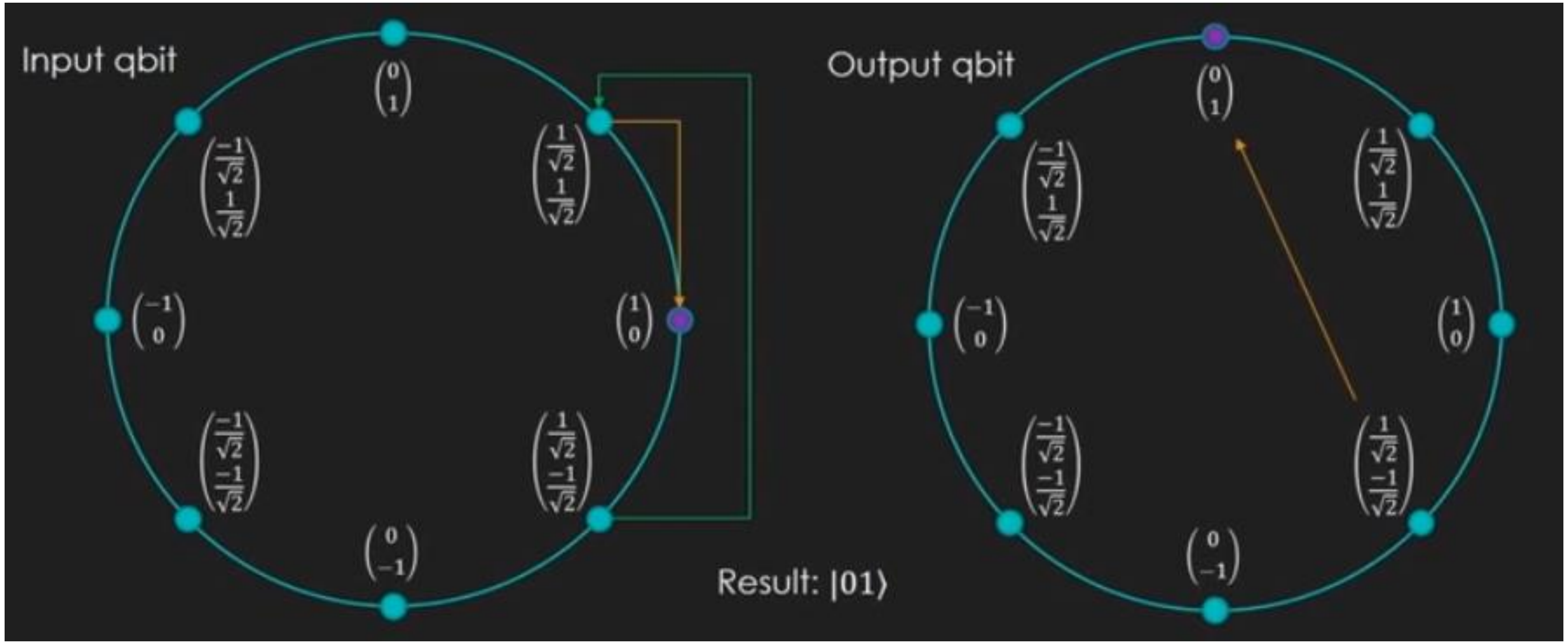
The Deutsch oracle: Identity



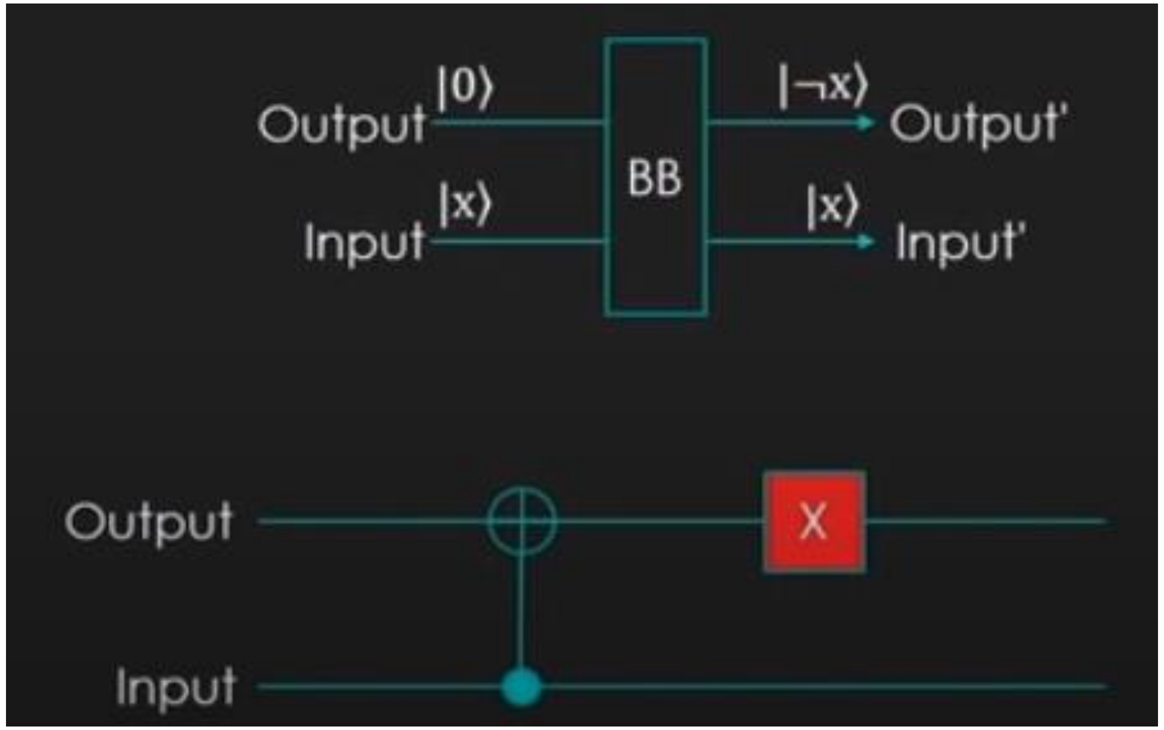
The Deutsch oracle: Identity

$$C\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}\right)=C\begin{pmatrix}\frac{1}{2}\\ \frac{-1}{2}\\ \frac{-1}{2}\\ \frac{1}{2}\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}$$

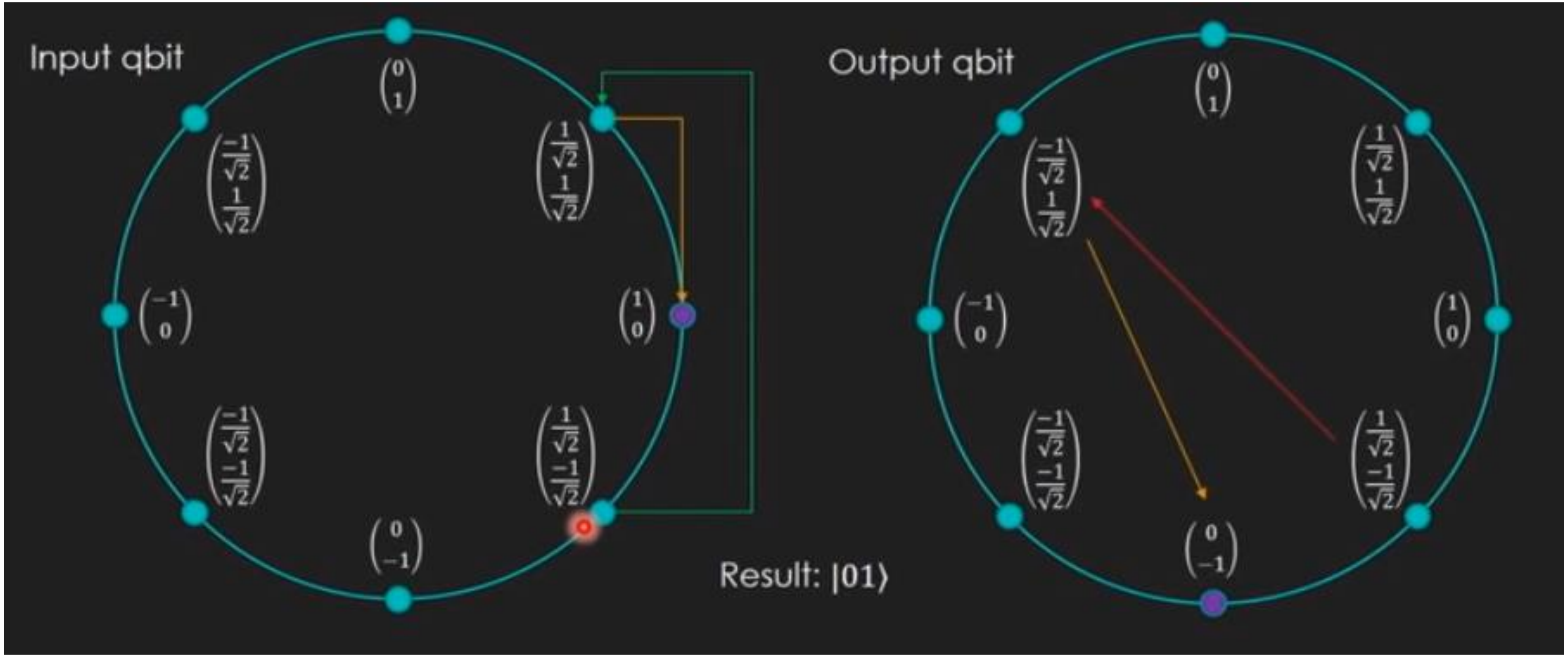
The Deutsch oracle: Identity



The Deutsch oracle: Negation



The Deutsch oracle: Negation



The Deutsch Oracle

- We did it! We determined whether the function was constant or variable in a single query!
- Intuition: the difference *within* the categories (negation) was neutralized, while the difference *between* the categories (CNOT) was magnified
- This problem seems pretty contrived (and it was, when it was published)
- A generalized version with an n-bit black box also exists (Deutsch-Josza problem)
  - Determine whether the function returns the same value for all 2^n inputs (i.e. is constant)
- A variant of the generalized version was an inspiration for Shor's algorithm!

Quantum entanglement
Quantum teleportation

Entanglement

- If the product state of two qbits cannot be factored, they are said to be **entangled**

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix}$$

$$\begin{aligned} ac &= \frac{1}{\sqrt{2}} \\ ad &= 0 \\ bc &= 0 \\ bd &= \frac{1}{\sqrt{2}} \end{aligned}$$

- The system of equations has no solution, so we cannot factor the quantum state!
- This has a 50% chance of collapsing to $|00\rangle$ and 50% chance of collapsing to $|11\rangle$

Entanglement

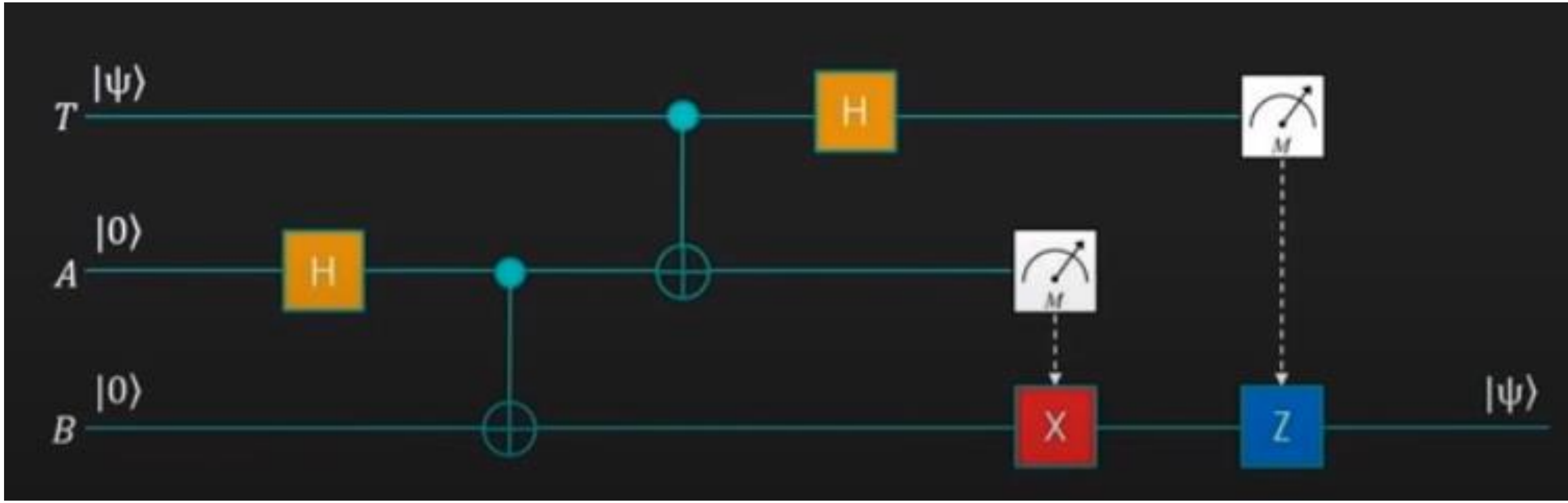
How can we reach an entangled state? Easy!

$$CH_1\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=C\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\ \frac{1}{\sqrt{2}}\\0\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\ \frac{1}{\sqrt{2}}\end{pmatrix}$$

Entanglement

- What's going on here? The qbits seem to be coordinating in some way
  - Measuring one qbit also collapses the other in a correlated state
- This coordination happens even across vast stretches of space
- The coordination even happens faster than the speed of light! It is instantaneous.
  - A 2013 experiment measured particles within 0.01% of the travel time of light between them
- Surely the qbits "decided" at the time of entanglement what they would do?
  - No! This is called "hidden variable" theory and was disproved by John Bell in 1964
- This does indeed break locality through faster-than-light coordination
  - However – and this is the critical part – *no information can be communicated*

Teleportation



$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$