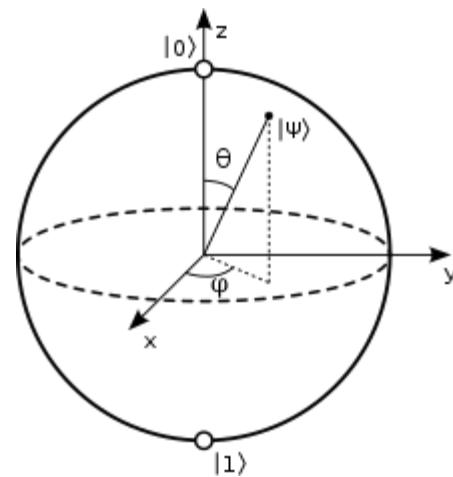


Intro to Quantum Computing

Quantum Algorithms I: Deutsch's Algorithm



Today's topic

Today's topic

- Description of the 1st (historically) Quantum *Algorithm*.

Today's topic

- Description of the 1st (historically) Quantum *Algorithm*.
- (with the exceptions of the Quantum Information Protocols we have seen so far...).

Today's topic

- Description of the 1st (historically) Quantum *Algorithm*.
- (with the exceptions of the Quantum Information Protocols we have seen so far...).
- Deutsch's Algorithm (1985)

Today's topic

- Description of the 1st (historically) Quantum *Algorithm*.
- (with the exceptions of the Quantum Information Protocols we have seen so far...).
- Deutsch's Algorithm (1985)



Today's Topic

- It is also the first computational task that *provably* can be solved faster on a quantum computer.

Today's Topic

- It is also the first computational task that ***provably*** can be solved faster on a quantum computer.
- Originally, it was a randomized quantum algorithm (it outputs the correct solution with probability $\frac{1}{2}$)

Today's Topic

- It is also the first computational task that ***provably*** can be solved faster on a quantum computer.
- Originally, it was a randomized quantum algorithm (it outputs the correct solution with probability $\frac{1}{2}$)
- There were some improvements by *Deutsch & Josza* (1992).

Today's Topic

- It is also the first computational task that ***provably*** can be solved faster on a quantum computer.
- Originally, it was a randomized quantum algorithm (it outputs the correct solution with probability $\frac{1}{2}$)
- There were some improvements by *Deutsch & Josza* (1992).
- Further improvements by *Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca* (1998).

Today's Topic

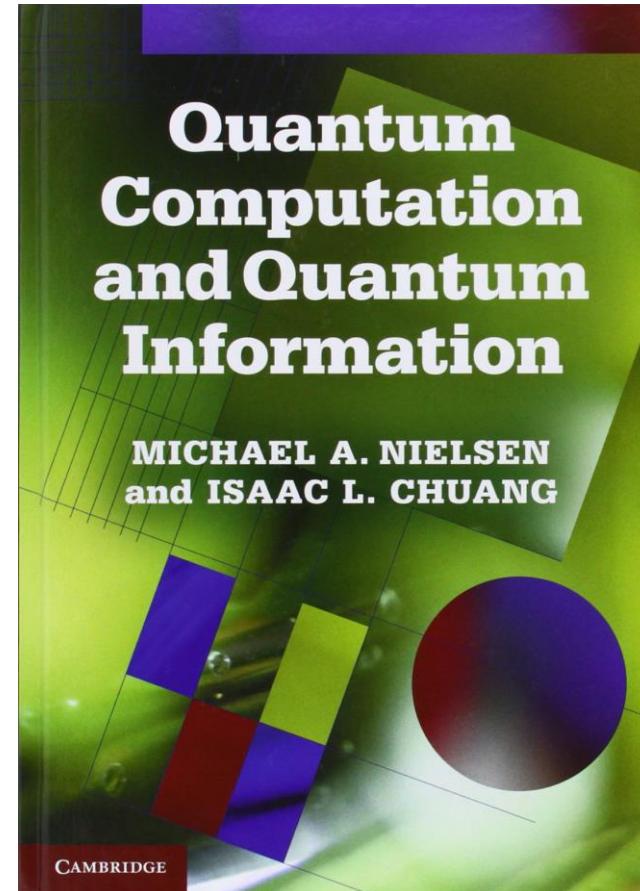
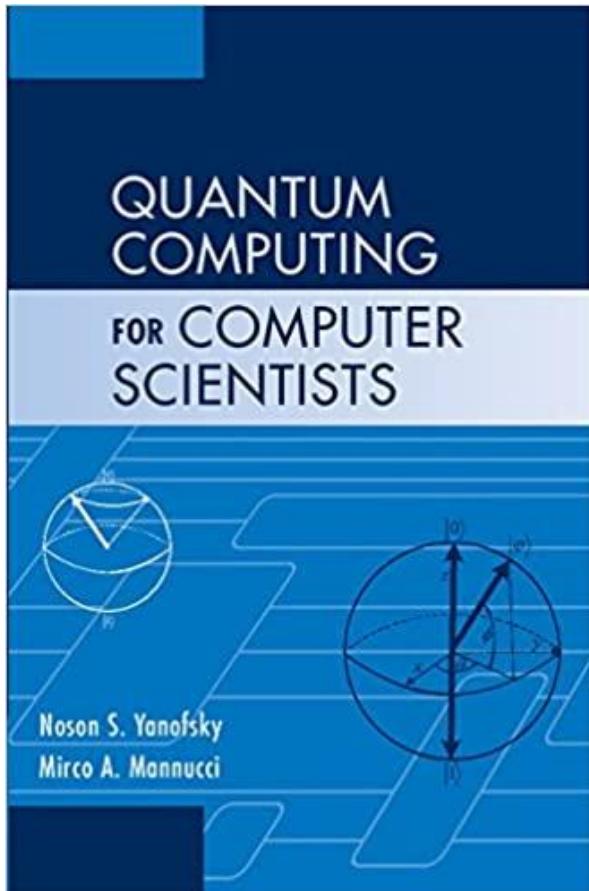
- It is also the first computational task that ***provably*** can be solved faster on a quantum computer.
- Originally, it was a randomized quantum algorithm (it outputs the correct solution with probability $\frac{1}{2}$)
- There were some improvements by *Deutsch & Josza* (1992).
- Further improvements by *Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca* (1998).
- We will present an approach bases on the latter version.

Today's Topic

- It is also the first computational task that ***provably*** can be solved faster on a quantum computer.
- Originally, it was a randomized quantum algorithm (it outputs the correct solution with probability $\frac{1}{2}$)
- There were some improvements by *Deutsch & Josza* (1992).
- Further improvements by *Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca* (1998).
- We will present an approach bases on the latter version.
- Next lecture, we will generalize it to Deutsch-Josza Algorithm (a bit more difficult)

Today's Topic

- Sources



But what is a Quantum Algorithm?

- An algorithm that runs on a realistic model of Quantum Computation

But what is a Quantum Algorithm?

- An algorithm that runs on a realistic model of Quantum Computation
- Like the Circuit model!

But what is a Quantum Algorithm?

- An algorithm that runs on a realistic model of Quantum Computation
- Like the Circuit model!
- We have a quantum circuit which acts on (some) input Qbits and it terminates with a measurement on some of the Qbits.

But what is a Quantum Algorithm?

- An algorithm that runs on a realistic model of Quantum Computation
- Like the Circuit model!
- We have a quantum circuit which acts on (some) input Qbits and it terminates with a measurement on some of the Qbits.
- Big Question:

Are there computational tasks for which a quantum algorithm runs faster than any classical algorithm?

But what is a Quantum Algorithm?

- An algorithm that runs on a realistic model of Quantum Computation
- Like the Circuit model!
- We have a quantum circuit which acts on (some) input Qbits and it terminates with a measurement on some of the Qbits.
- Big Question:

Are there computational tasks for which a quantum algorithm runs faster than any classical algorithm?

- Yes! Deutsch algorithm is one of these (not many) tasks!

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$
- I.e., f takes as input a Boolean variable x and outputs either **0** or **1**.

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$
- I.e., f takes as input a Boolean variable x and outputs either **0** or **1**.
- How many such Boolean functions exist?

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$
- I.e., f takes as input a Boolean variable x and outputs either **0** or **1**.
- How many such Boolean functions exist?
- $f_0(0) = 0, f_0(1) = 0$

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$
- I.e., f takes as input a Boolean variable x and outputs either **0** or **1**.
- How many such Boolean functions exist?
- $f_0(0) = 0, f_0(1) = 0$
- $f_1(0) = 0, f_1(1) = 1$

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$
- I.e., f takes as input a Boolean variable x and outputs either **0** or **1**.
- How many such Boolean functions exist?
- $f_0(0) = 0, f_0(1) = 0$
- $f_1(0) = 0, f_1(1) = 1$
- $f_2(0) = 1, f_2(1) = 0$

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$
- I.e., f takes as input a Boolean variable x and outputs either **0** or **1**.
- How many such Boolean functions exist?
- $f_0(0) = 0, f_0(1) = 0$
- $f_1(0) = 0, f_1(1) = 1$
- $f_2(0) = 1, f_2(1) = 0$
- $f_3(0) = 1, f_3(1) = 1$

Evaluating Boolean Functions

- Let us say that we are given a Boolean function $f: \{0, 1\} \rightarrow \{0, 1\}$
- I.e., f takes as input a Boolean variable x and outputs either **0** or **1**.
- How many such Boolean functions exist?
- $f_0(0) = 0, f_0(1) = 0$
- $f_1(0) = 0, f_1(1) = 1$
- $f_2(0) = 1, f_2(1) = 0$
- $f_3(0) = 1, f_3(1) = 1$
- *Constant* vs *non-constant* functions

Evaluating Boolean Functions

Question:

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.
- Is it a **constant** or a **non-constant** function?

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.
- Is it a **constant** or a **non-constant** function?
- Well, that sounds **very** easy!

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.
- Is it a **constant** or a **non-constant** function?
- Well, that sounds **very** easy!
- Plug *both* values **0, 1** in f and see the result.

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.
- Is it a **constant** or a **non-constant** function?
- Well, that sounds **very** easy!
- Plug *both* values **0, 1** in f and see the result.
- We need to **ask f** twice in order to determine the answer.

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.
- Is it a **constant** or a **non-constant** function?
- Well, that sounds **very** easy!
- Plug *both* values **0, 1** in f and see the result.
- We need to *ask* f twice in order to determine the answer.
- It is impossible to do will less than two **queries**.

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.
- Is it a **constant** or a **non-constant** function?
- Well, that sounds **very** easy!
- Plug *both* values **0, 1** in f and see the result.
- We need to **ask f** twice in order to determine the answer.
- It is impossible to do will less than two **queries**.
- The **query complexity** is **2**.

Evaluating Boolean Functions

Question:

- We are given some *unknown* function $f: \{0, 1\} \rightarrow \{0, 1\}$.
- Is it a **constant** or a **non-constant** function?
- Well, that sounds **very** easy!
- Plug *both* values **0, 1** in f and see the result.
- We need to *ask f* twice in order to determine the answer.
- It is impossible to do will less than two **queries**.
- The **query complexity** is **2**.
- *What if we had a quantum computer? Can we do better?*

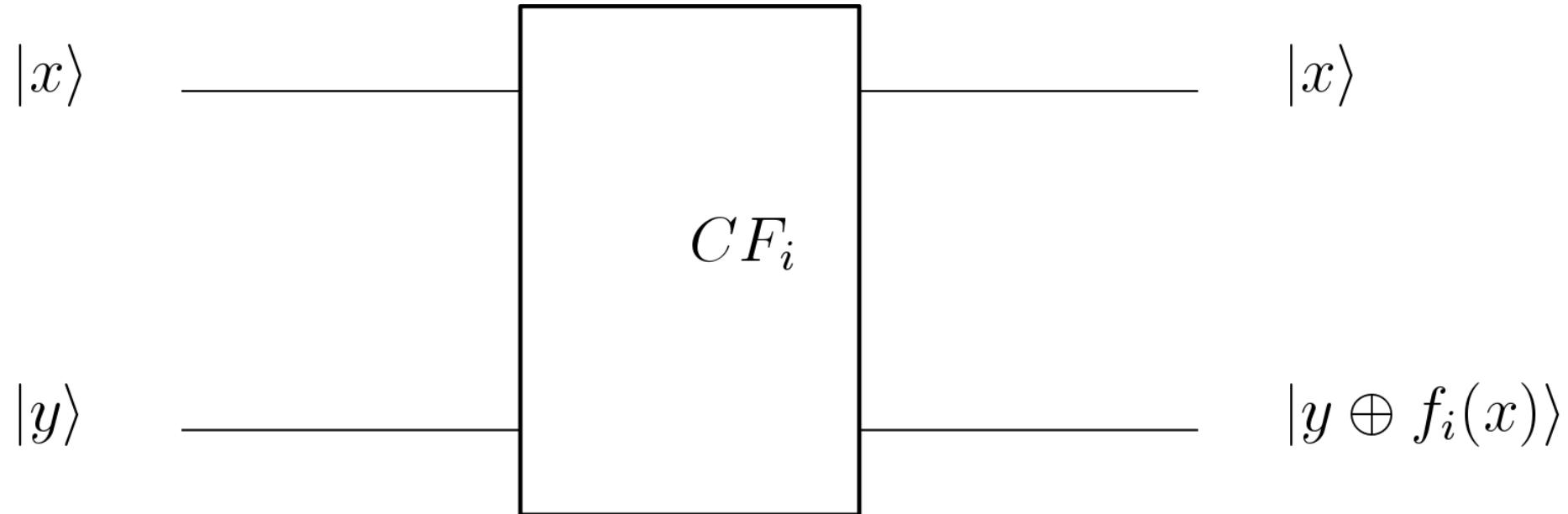
Evaluating Boolean Functions Quantumly

Evaluating Boolean Functions Quantumly

- Let's construct quantum circuits that corresponds to the four Boolean functions

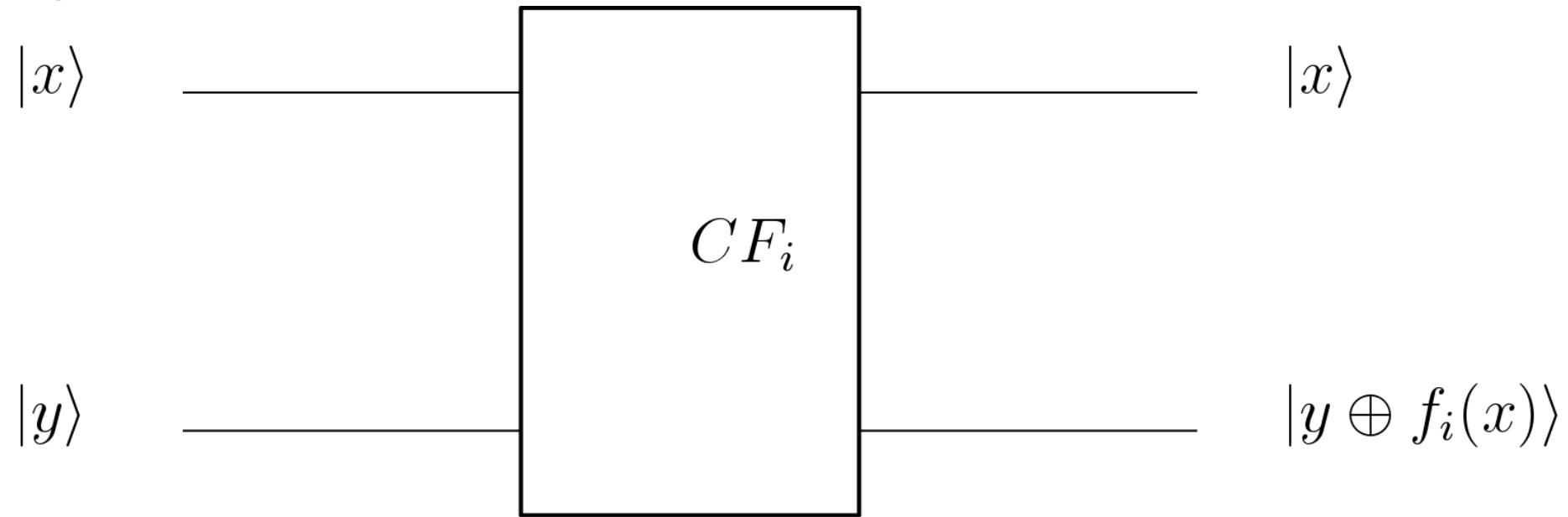
Evaluating Boolean Functions Quantumly

- Let's construct quantum circuits that corresponds to the four Boolean functions



Evaluating Boolean Functions Quantumly

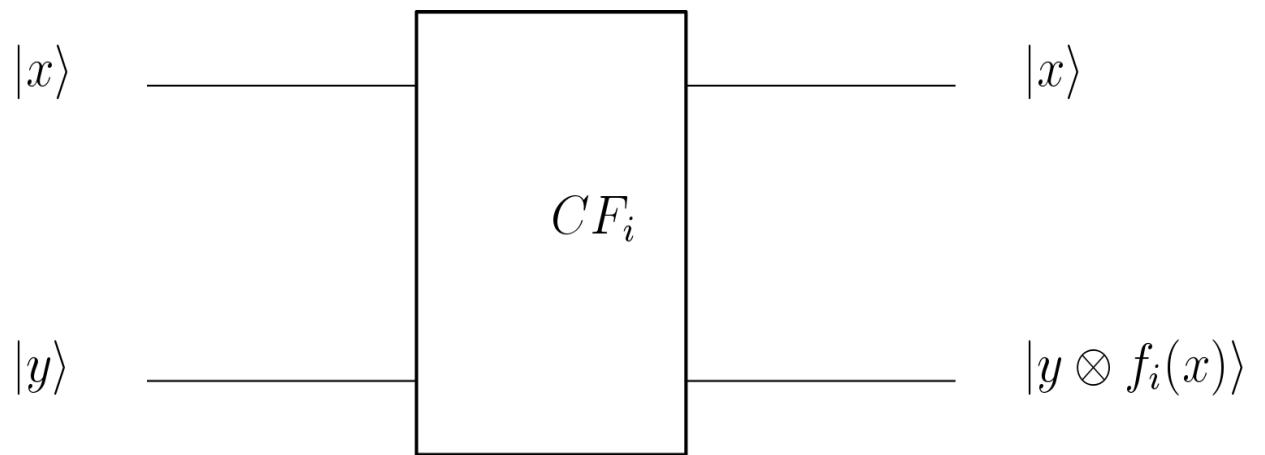
- Let's construct quantum circuits that corresponds to the four Boolean functions



- $|x\rangle$ is the input bit and $|y\rangle$ is a control bit: it controls the output $|y \oplus f_i(x)\rangle$.

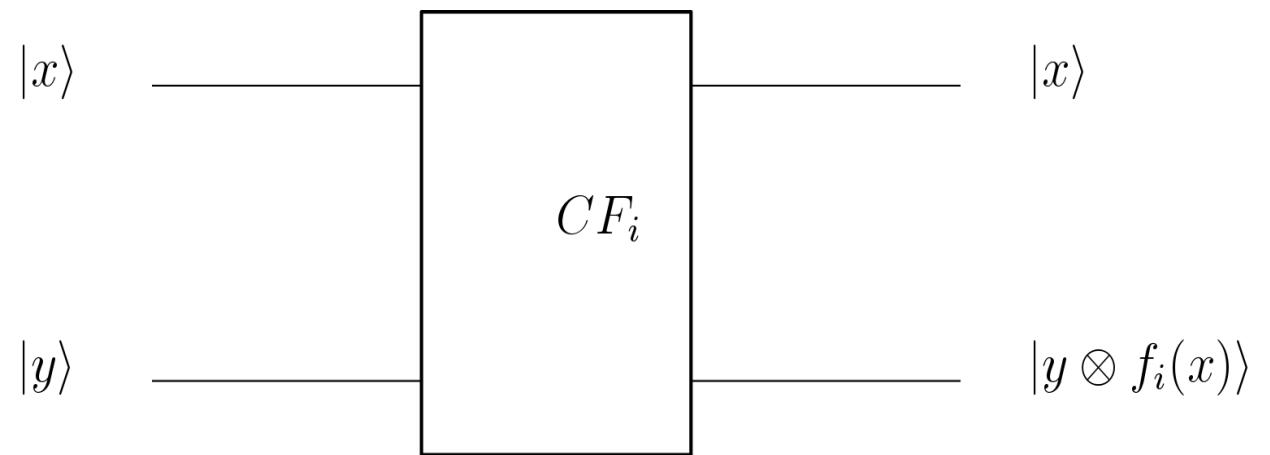
Evaluating Boolean Functions Quantumly

- What does the circuit say:



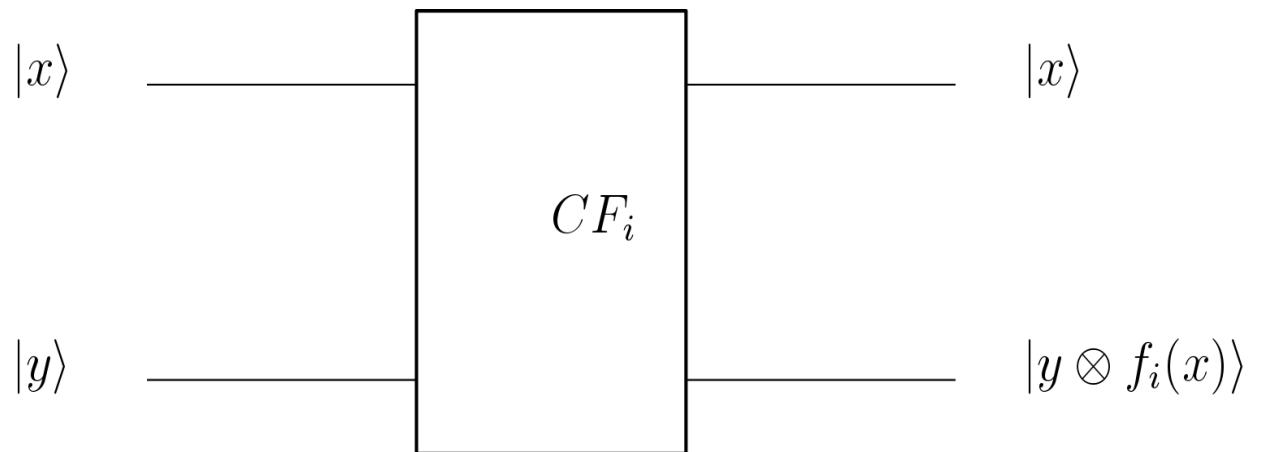
Evaluating Boolean Functions Quantumly

- What does the circuit say:
- $|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |f_i(0)\rangle$



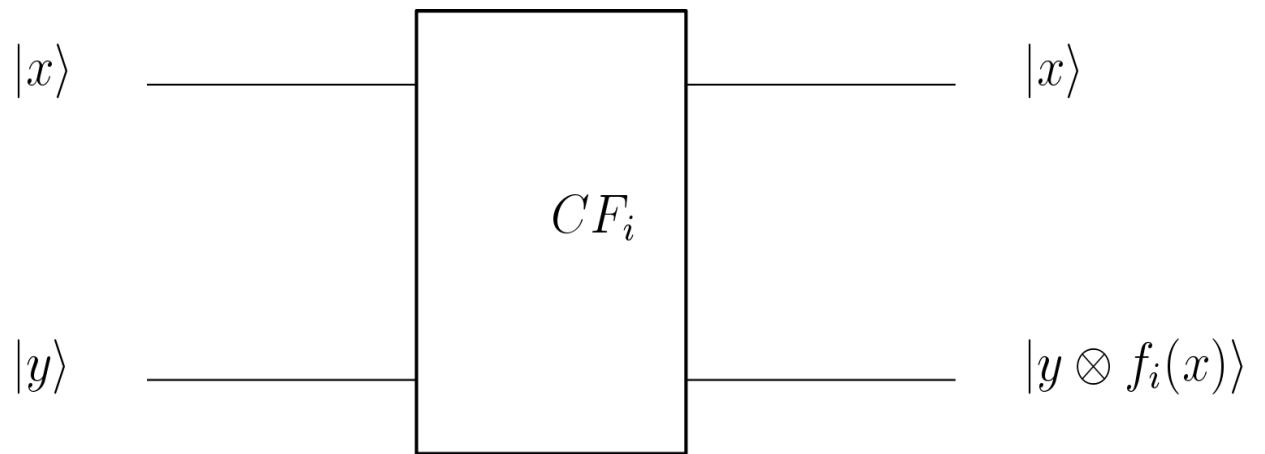
Evaluating Boolean Functions Quantumly

- What does the circuit say:
- $|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |f_i(0)\rangle$
- $|0\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |f_i(0) \oplus 1\rangle$



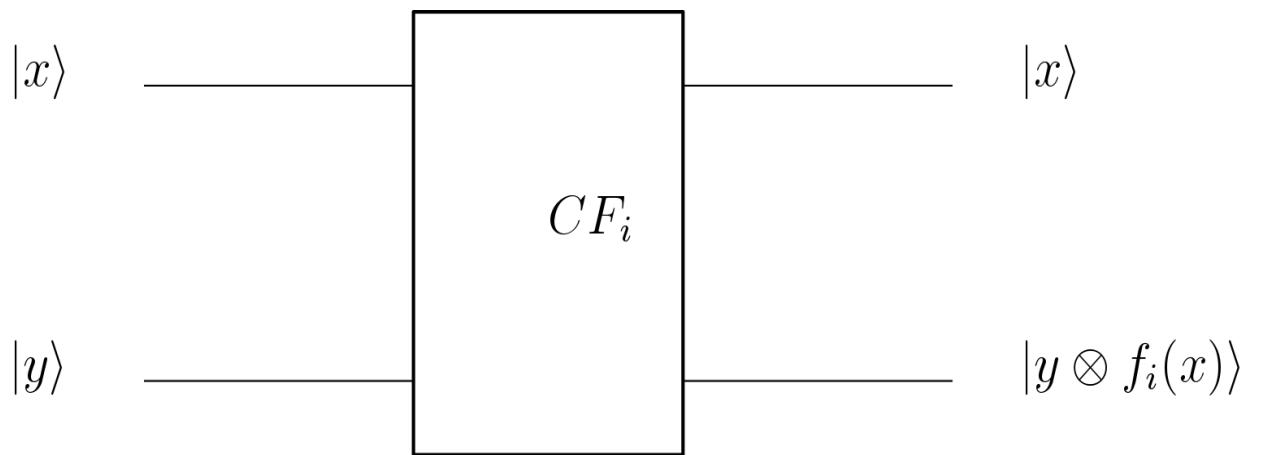
Evaluating Boolean Functions Quantumly

- What does the circuit say:
- $|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |f_i(0)\rangle$
- $|0\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |f_i(0) \oplus 1\rangle$
- $|1\rangle \otimes |0\rangle \rightarrow |1\rangle \otimes |f_i(1)\rangle$



Evaluating Boolean Functions Quantumly

- What does the circuit say:
- $|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |f_i(0)\rangle$
- $|0\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |f_i(0) \oplus 1\rangle$
- $|1\rangle \otimes |0\rangle \rightarrow |1\rangle \otimes |f_i(1)\rangle$
- $|1\rangle \otimes |1\rangle \rightarrow |1\rangle \otimes |f_i(1) \oplus 1\rangle$



Evaluating Boolean Functions Quantumly

- What does the circuit say:
- $|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |f_i(0)\rangle$
- $|0\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |f_i(0) \oplus 1\rangle$
- $|1\rangle \otimes |0\rangle \rightarrow |1\rangle \otimes |f_i(1)\rangle$
- $|1\rangle \otimes |1\rangle \rightarrow |1\rangle \otimes |f_i(1) \oplus 1\rangle$
- **So what?**

Evaluating Boolean Functions Quantumly

- What does the circuit say:
- $|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |f_i(0)\rangle$
- $|0\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |f_i(0) \oplus 1\rangle$
- $|1\rangle \otimes |0\rangle \rightarrow |1\rangle \otimes |f_i(1)\rangle$
- $|1\rangle \otimes |1\rangle \rightarrow |1\rangle \otimes |f_i(1) \oplus 1\rangle$
- **So what?**
- For every i , exactly one of $|f_i(0)\rangle$ and $|f_i(0) \oplus 1\rangle$ is equal to 0. The other is equal to 1.

Evaluating Boolean Functions Quantumly

- What does the circuit say:
- $|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |f_i(0)\rangle$
- $|0\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |f_i(0) \oplus 1\rangle$
- $|1\rangle \otimes |0\rangle \rightarrow |1\rangle \otimes |f_i(1)\rangle$
- $|1\rangle \otimes |1\rangle \rightarrow |1\rangle \otimes |f_i(1) \oplus 1\rangle$
- **So what?**
- For every i , exactly one of $|f_i(0)\rangle$ and $|f_i(0) \oplus 1\rangle$ is equal to 0. The other is equal to 1.
- Similarly exactly one of $|f_i(1)\rangle$ and $|f_i(1) \oplus 1\rangle$ is equal to 0. The other is equal to 1.

Evaluating Boolean Functions Quantumly

- This means that the four possible outputs give us (permutations of) the four basis elements.

Evaluating Boolean Functions Quantumly

- This means that the four possible outputs give us (permutations of) the four basis elements.
- \Rightarrow The matrix representing the circuit computation is orthonormal.

Evaluating Boolean Functions Quantumly

- This means that the four possible outputs give us (permutations of) the four basis elements.
- \Rightarrow The matrix representing the circuit computation is orthonormal.
- \Rightarrow It is unitary, and so it exists (in principle)!

Evaluating Boolean Functions Quantumly

- This means that the four possible outputs give us (permutations of) the four basis elements.
- \Rightarrow The matrix representing the circuit computation is orthonormal.
- \Rightarrow It is unitary, and so it exists (in principle)!

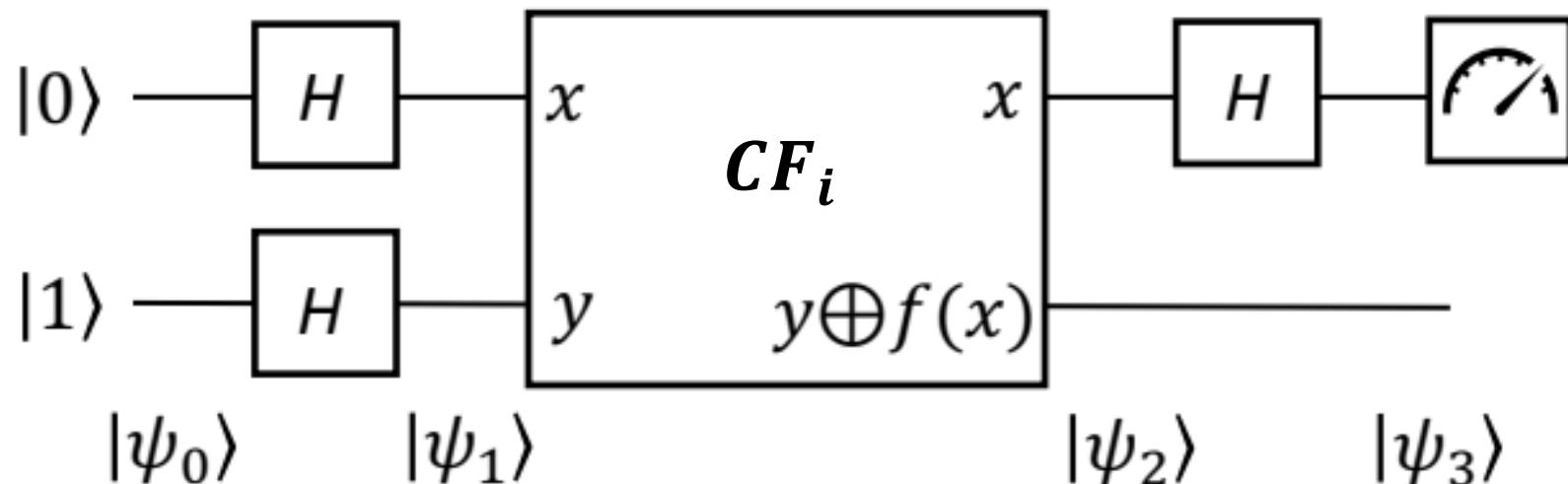
Given one of these four possible circuits, at random, how many times do we need to use the gate in order to determine if the underlying f_i is constant or not?

Evaluating Boolean Functions Quantumly

- We will incorporate the given quantum circuit implementing one of the f_i into the new following circuit

Evaluating Boolean Functions Quantumly

- We will incorporate the given quantum circuit implementing one of the f_i into the new following circuit



Evaluating Boolean Functions Quantumly

- The initial state is always the state $|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle$.

Evaluating Boolean Functions Quantumly

- The initial state is always the state $|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle$.
- We pass both Qbits through a Hadamard gate which puts the state on the following superposition

Evaluating Boolean Functions Quantumly

- The initial state is always the state $|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle$.
- We pass both Qbits through a Hadamard gate which puts the state on the following superposition

$$|\psi_1\rangle = H|\psi_0\rangle = H|0\rangle \otimes H|1\rangle$$

Evaluating Boolean Functions Quantumly

- The initial state is always the state $|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle$.
- We pass both Qbits through a Hadamard gate which puts the state on the following superposition

$$\begin{aligned} |\psi_1\rangle &= H|\psi_0\rangle = H|0\rangle \otimes H|1\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

Evaluating Boolean Functions Quantumly

- The initial state is always the state $|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle$.
- We pass both Qbits through a Hadamard gate which puts the state on the following superposition

$$\begin{aligned} |\psi_1\rangle &= H|\psi_0\rangle = H|0\rangle \otimes H|1\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = A \end{aligned}$$

Evaluating Boolean Functions Quantumly

- The initial state is always the state $|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle$.
- We pass both Qbits through a Hadamard gate which puts the state on the following superposition

$$\begin{aligned} |\psi_1\rangle &= H|\psi_0\rangle = H|0\rangle \otimes H|1\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = A \end{aligned}$$

- Then, the two Qbits pass through the CF_i circuit.

Evaluating Boolean Functions Quantumly

- The initial state is always the state $|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle$.
- We pass both Qbits through a Hadamard gate which puts the state on the following superposition

$$\begin{aligned} |\psi_1\rangle &= H|\psi_0\rangle = H|0\rangle \otimes H|1\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = A \end{aligned}$$

- Then, the two Qbits pass through the CF_i circuit.
- This circuit leaves the 1st Qbit alone and the 2nd Qbit becomes $|y \oplus f_i(x)\rangle$.

Evaluating Boolean Functions Quantumly

- So expression A becomes

Evaluating Boolean Functions Quantumly

- So expression A becomes

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

Evaluating Boolean Functions Quantumly

- So expression A becomes

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

Evaluating Boolean Functions Quantumly

- So expression A becomes

$$A = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\ \frac{1}{2}(|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0) \oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1) \oplus 1\rangle)$$

Evaluating Boolean Functions Quantumly

- So expression A becomes

$$A = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\ \frac{1}{2}(|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0) \oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1) \oplus 1\rangle)$$

- Which can be re-written as

Evaluating Boolean Functions Quantumly

- So expression A becomes

$$A = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\ \frac{1}{2}(|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0) \oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1) \oplus 1\rangle)$$

- Which can be re-written as

$$\frac{1}{2}(|0\rangle \otimes (|f_i(0)\rangle - |f_i(0) \oplus 1\rangle) + |1\rangle \otimes (|f_i(1)\rangle - |f_i(1) \oplus 1\rangle))$$

Evaluating Boolean Functions Quantumly

- So expression A becomes

$$A = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\ \frac{1}{2}(|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0) \oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1) \oplus 1\rangle)$$

- Which can be re-written as

$$\frac{1}{2}(|0\rangle \otimes (|f_i(0)\rangle - |f_i(0) \oplus 1\rangle) + |1\rangle \otimes (|f_i(1)\rangle - |f_i(1) \oplus 1\rangle))$$

- Observe that $|f_i(0)\rangle - |f_i(0) \oplus 1\rangle$ is either $|0\rangle - |1\rangle$ or $|1\rangle - |0\rangle$ depending on whether $f_i(0)$ is $|0\rangle$ or $|1\rangle$.

Evaluating Boolean Functions Quantumly

- So expression A becomes

$$A = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \\ \frac{1}{2}(|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0) \oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1) \oplus 1\rangle)$$

- Which can be re-written as

$$\frac{1}{2}(|0\rangle \otimes (|f_i(0)\rangle - |f_i(0) \oplus 1\rangle) + |1\rangle \otimes (|f_i(1)\rangle - |f_i(1) \oplus 1\rangle))$$

- Observe that $|f_i(0)\rangle - |f_i(0) \oplus 1\rangle$ is either $|0\rangle - |1\rangle$ or $|1\rangle - |0\rangle$ depending on whether $f_i(0)$ is $|0\rangle$ or $|1\rangle$.

- Similarly $|f_i(1)\rangle - |f_i(1) \oplus 1\rangle = (-1)^{f_i(1)}(|0\rangle - |1\rangle)$

Evaluating Boolean Functions Quantumly

- So, the state of the Qbits passing through CF_i is

Evaluating Boolean Functions Quantumly

- So, the state of the Qbits passing through CF_i is

$$\frac{1}{2} (|0\rangle \otimes ((-1)^{f_i(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes ((-1)^{f_i(1)}(|0\rangle - |1\rangle)))$$

Evaluating Boolean Functions Quantumly

- So, the state of the Qbits passing through CF_i is

$$\begin{aligned}& \frac{1}{2}(|0\rangle \otimes ((-1)^{f_i(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes ((-1)^{f_i(1)}(|0\rangle - |1\rangle))) \\&= \frac{1}{2}\left(((-1)^{f_i(0)}|0\rangle \otimes (|0\rangle - |1\rangle)) + ((-1)^{f_i(1)}|1\rangle \otimes (|0\rangle - |1\rangle))\right)\end{aligned}$$

Evaluating Boolean Functions Quantumly

- So, the state of the Qbits passing through CF_i is

$$\begin{aligned}& \frac{1}{2}(|0\rangle \otimes ((-1)^{f_i(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes ((-1)^{f_i(1)}(|0\rangle - |1\rangle))) \\&= \frac{1}{2}\left(((-1)^{f_i(0)}|0\rangle \otimes (|0\rangle - |1\rangle)) + ((-1)^{f_i(1)}|1\rangle \otimes (|0\rangle - |1\rangle))\right) \\&= \frac{1}{2}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right) \otimes (|0\rangle - |1\rangle)\end{aligned}$$

Evaluating Boolean Functions Quantumly

- So, the state of the Qbits passing through CF_i is

$$\begin{aligned}& \frac{1}{2}(|0\rangle \otimes ((-1)^{f_i(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes ((-1)^{f_i(1)}(|0\rangle - |1\rangle))) \\&= \frac{1}{2}\left(((-1)^{f_i(0)}|0\rangle \otimes (|0\rangle - |1\rangle)) + ((-1)^{f_i(1)}|1\rangle \otimes (|0\rangle - |1\rangle))\right) \\&= \frac{1}{2}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right) \otimes (|0\rangle - |1\rangle) \\&= \frac{1}{\sqrt{2}}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\end{aligned}$$

Evaluating Boolean Functions Quantumly

- So, the state of the Qbits passing through CF_i is

$$\begin{aligned}& \frac{1}{2}(|0\rangle \otimes ((-1)^{f_i(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes ((-1)^{f_i(1)}(|0\rangle - |1\rangle))) \\&= \frac{1}{2}\left(((-1)^{f_i(0)}|0\rangle \otimes (|0\rangle - |1\rangle)) + ((-1)^{f_i(1)}|1\rangle \otimes (|0\rangle - |1\rangle))\right) \\&= \frac{1}{2}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right) \otimes (|0\rangle - |1\rangle) \\&= \frac{1}{\sqrt{2}}\left((-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\end{aligned}$$

i.e...the two Qbits are not entangled

Evaluating Boolean Functions Quantumly

- Let's examine the state of the 1st Qbit for each possible case for f_i .

Evaluating Boolean Functions Quantumly

- Let's examine the state of the 1st Qbit for each possible case for f_i .
 1. For f_0 we have $f_0(0) = f_0(1) = 0$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Evaluating Boolean Functions Quantumly

- Let's examine the state of the 1st Qbit for each possible case for f_i .
 1. For f_0 we have $f_0(0) = f_0(1) = 0$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 2. For f_1 we have $f_1(0) = 0, f_1(1) = 1$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Evaluating Boolean Functions Quantumly

- Let's examine the state of the 1st Qbit for each possible case for f_i .
 1. For f_0 we have $f_0(0) = f_0(1) = 0$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 2. For f_1 we have $f_1(0) = 0, f_1(1) = 1$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 3. For f_2 we have $f_2(0) = 1, f_2(1) = 0$ and so $|x\rangle = \frac{-1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Evaluating Boolean Functions Quantumly

- Let's examine the state of the 1st Qbit for each possible case for f_i .
 1. For f_0 we have $f_0(0) = f_0(1) = 0$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 2. For f_1 we have $f_1(0) = 0, f_1(1) = 1$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 3. For f_2 we have $f_2(0) = 1, f_2(1) = 0$ and so $|x\rangle = \frac{-1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 4. For f_3 we have $f_3(0) = 1, f_3(1) = 1$ and so $|x\rangle = \frac{-1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Evaluating Boolean Functions Quantumly

- Let's examine the state of the **1st Qbit** for each possible case for f_i .
 1. For f_0 we have $f_0(0) = f_0(1) = 0$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 2. For f_1 we have $f_1(0) = 0, f_1(1) = 1$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 3. For f_2 we have $f_2(0) = 1, f_2(1) = 0$ and so $|x\rangle = \frac{-1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 4. For f_3 we have $f_3(0) = 1, f_3(1) = 1$ and so $|x\rangle = \frac{-1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Next, we send this Qbit $|x\rangle$ through another Hadamard gate and the outcome is $|0\rangle$ if $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Evaluating Boolean Functions Quantumly

- Let's examine the state of the **1st Qbit** for each possible case for f_i .
 1. For f_0 we have $f_0(0) = f_0(1) = 0$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
 2. For f_1 we have $f_1(0) = 0, f_1(1) = 1$ and so $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 3. For f_2 we have $f_2(0) = 1, f_2(1) = 0$ and so $|x\rangle = \frac{-1}{\sqrt{2}}(|0\rangle - |1\rangle)$
 4. For f_3 we have $f_3(0) = 1, f_3(1) = 1$ and so $|x\rangle = \frac{-1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Next, we send this Qbit $|x\rangle$ through another Hadamard gate and the outcome is $|0\rangle$ if $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, or $|1\rangle$ if $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Evaluating Boolean Functions Quantumly

- Now we know:

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$
 2. If $i = 1$ the Qbit is $|1\rangle$

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$
 2. If $i = 1$ the Qbit is $|1\rangle$
 3. If $i = 2$ the Qbit is $-|1\rangle$

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$
 2. If $i = 1$ the Qbit is $|1\rangle$
 3. If $i = 2$ the Qbit is $-|1\rangle$
 4. If $i = 3$ the Qbit is $-|0\rangle$

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$
 2. If $i = 1$ the Qbit is $|1\rangle$
 3. If $i = 2$ the Qbit is $-|1\rangle$
 4. If $i = 3$ the Qbit is $-|0\rangle$
- Now we measure (in the standard basis)

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$
 2. If $i = 1$ the Qbit is $|1\rangle$
 3. If $i = 2$ the Qbit is $-|1\rangle$
 4. If $i = 3$ the Qbit is $-|0\rangle$
- Now we measure (in the standard basis)
- We get 0 if $i = 0$ or 3 i.e., when the function is **constant**

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$
 2. If $i = 1$ the Qbit is $|1\rangle$
 3. If $i = 2$ the Qbit is $-|1\rangle$
 4. If $i = 3$ the Qbit is $-|0\rangle$
- Now we measure (in the standard basis)
- We get 0 if $i = 0$ or 3 i.e., when the function is **constant**
- We get 1 if $i = 1$ or 2 i.e., when the function is **non-constant!**

Evaluating Boolean Functions Quantumly

- Now we know:
 1. If $i = 0$ the Qbit is $|0\rangle$
 2. If $i = 1$ the Qbit is $|1\rangle$
 3. If $i = 2$ the Qbit is $-|1\rangle$
 4. If $i = 3$ the Qbit is $-|0\rangle$
- Now we measure (in the standard basis)
- We get 0 if $i = 0$ or 3 i.e., when the function is **constant**
- We get 1 if $i = 1$ or 2 i.e., when the function is **non-constant!**
- *And we got the answer by asking the circuit only once!*