Quantum Computation and Cryptography
Day 4

Alexandru Gheorghiu

The University of Edinburgh

Part I
Quantum algorithms

A note on notation

A note on notation

As before $|\psi\rangle \otimes |\chi\rangle$ same as $|\psi\rangle\,|\chi\rangle$

A note on notation

As before $|\psi\rangle \otimes |\chi\rangle$ same as $|\psi\rangle\,|\chi\rangle$

We'll denote $\underbrace{|\psi\rangle \otimes |\psi\rangle \otimes \ldots \otimes |\psi\rangle}_{N \text{ times}}$ as $|\psi\rangle^{\otimes N}$

A note on notation

As before $|\psi\rangle \otimes |\chi\rangle$ same as $|\psi\rangle\,|\chi\rangle$

We'll denote $\underbrace{|\psi\rangle \otimes |\psi\rangle \otimes \ldots \otimes |\psi\rangle}_{N \text{ times}}$ as $|\psi\rangle^{\otimes N}$

Also $\underbrace{U \otimes U \otimes \ldots \otimes U}_{N \text{ times}}$ as $U^{\otimes N}$

A note on notation

A note on notation

We'll be using latin alphabet for computational basis states

$$|x\rangle, |y\rangle, |z\rangle$$

A note on notation

We'll be using latin alphabet for computational basis states $|x\rangle$, $|y\rangle$, $|z\rangle$

So for example if $x = 1001$, then $|x\rangle = |1001\rangle$

A note on notation

We'll be using latin alphabet for computational basis states
$|x\rangle$, $|y\rangle$, $|z\rangle$

So for example if $x = 1001$, then $|x\rangle = |1001\rangle$

Greek letters for any states (computational basis or not)
E.g. $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Binary operations

Binary operations

$\oplus$ is XOR

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

If $x = x_1 x_2 ... x_N$, $y = y_1 y_2 ... y_N$ then
$x \oplus y = (x_1 \oplus y_1)(x_2 \oplus y_2)...(x_N \oplus y_N)$

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

If $x = x_1 x_2 ... x_N$, $y = y_1 y_2 ... y_N$ then
$x \oplus y = (x_1 \oplus y_1)(x_2 \oplus y_2)...(x_N \oplus y_N)$

E.g. $x = 011101$, $y = 110111$ then
$x \oplus y =$

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

If $x = x_1 x_2 ... x_N$, $y = y_1 y_2 ... y_N$ then
$x \oplus y = (x_1 \oplus y_1)(x_2 \oplus y_2)...(x_N \oplus y_N)$

E.g. $x = 011101$, $y = 110111$ then
$x \oplus y = 101010$

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

If $x = x_1 x_2 ... x_N$, $y = y_1 y_2 ... y_N$ then
$x \oplus y = (x_1 \oplus y_1)(x_2 \oplus y_2)...(x_N \oplus y_N)$

E.g. $x = 011101$, $y = 110111$ then
$x \oplus y = 101010$

$\cdot$ is binary dot product

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

If $x = x_1 x_2 ... x_N$, $y = y_1 y_2 ... y_N$ then
$$x \oplus y = (x_1 \oplus y_1)(x_2 \oplus y_2)...(x_N \oplus y_N)$$

E.g. $x = 011101$, $y = 110111$ then
$$x \oplus y = 101010$$

$\cdot$ is binary dot product

$$x \cdot y = (x_1 \wedge y_1) \oplus (x_2 \wedge y_2) \oplus ... \oplus (x_N \wedge y_N)$$

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

If $x = x_1 x_2 ... x_N$, $y = y_1 y_2 ... y_N$ then
$$x \oplus y = (x_1 \oplus y_1)(x_2 \oplus y_2)...(x_N \oplus y_N)$$

E.g. $x = 011101$, $y = 110111$ then
$$x \oplus y = 101010$$

$\cdot$ is binary dot product

$$x \cdot y = (x_1 \wedge y_1) \oplus (x_2 \wedge y_2) \oplus ... \oplus (x_N \wedge y_N)$$

E.g. $x = 011101$, $y = 110111$ then
$$x \cdot y =$$

Binary operations

$\oplus$ is XOR

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1$$
$$1 \oplus 0 = 1,\ 1 \oplus 1 = 0$$

If $x = x_1 x_2 ... x_N$, $y = y_1 y_2 ... y_N$ then
$$x \oplus y = (x_1 \oplus y_1)(x_2 \oplus y_2)...(x_N \oplus y_N)$$

E.g. $x = 011101$, $y = 110111$ then
$$x \oplus y = 101010$$

$\cdot$ is binary dot product

$$x \cdot y = (x_1 \wedge y_1) \oplus (x_2 \wedge y_2) \oplus ... \oplus (x_N \wedge y_N)$$

E.g. $x = 011101$, $y = 110111$ then
$$x \cdot y = 1$$

Running times

Running times

In the **worst case**, algorithm A runs in time T on input of size N

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$
- $T = 2^N, 3^N, 10^{13N} \ldots$ $O(exp(N))$

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$
- $T = 2^N, 3^N, 10^{13N} \ldots$ $O(exp(N))$
- $O(f(N)) =$ on the order of $f(N)$

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$
- $T = 2^N, 3^N, 10^{13N} \ldots$ $O(exp(N))$
- $O(f(N)) =$ on the order of $f(N)$

In the **best case**, algorithm A runs in time T on input of size N

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$
- $T = 2^N, 3^N, 10^{13N} \ldots$ $O(exp(N))$
- $O(f(N)) =$ on the order of $f(N)$

In the **best case**, algorithm A runs in time T on input of size N

- Denoted as $\Omega(f(N))$

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$
- $T = 2^N, 3^N, 10^{13N} \ldots$ $O(exp(N))$
- $O(f(N)) =$ on the order of $f(N)$

In the **best case**, algorithm A runs in time T on input of size N

- Denoted as $\Omega(f(N))$
- E.g. $\Omega(1)$, $\Omega(N)$ etc

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$
- $T = 2^N, 3^N, 10^{13N} \ldots$ $O(exp(N))$
- $O(f(N)) =$ on the order of $f(N)$

In the **best case**, algorithm A runs in time T on input of size N

- Denoted as $\Omega(f(N))$
- E.g. $\Omega(1)$, $\Omega(N)$ etc
- Ω is lower bound, O is upper bound

Running times

In the **worst case**, algorithm A runs in time T on input of size N

- $T = 1, 12, 100, 1000, 19842894 \ldots$ $O(1)$
- $T = N, 2N, \frac{7N}{3}, \pi N, 1000N \ldots$ $O(N)$
- $T = \sqrt{N}, 2\sqrt{N}, \sqrt{2N} \ldots$ $O(\sqrt{N})$
- $T = N, 7N^2, 34N^{10} + N^5 + 2N^2 \ldots$ $O(poly(N))$
- $T = 2^N, 3^N, 10^{13N} \ldots$ $O(exp(N))$
- $O(f(N)) =$ on the order of $f(N)$

In the **best case**, algorithm A runs in time T on input of size N

- Denoted as $\Omega(f(N))$
- E.g. $\Omega(1)$, $\Omega(N)$ etc
- Ω is lower bound, O is upper bound

E.g.: A succeeds with probability $3/4$ and its running time is $O(N^2)$ and $\Omega(N)$

Input size

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

What is N (the input size) in this case?

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

What is N (the input size) in this case?

$$N = log_2(x)$$

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

What is N (the input size) in this case?

$$N = log_2(x)$$

Let's say we run the naive algorithm where we go up to $\sqrt{x}$ to search for divisors.

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

What is N (the input size) in this case?

$$N = log_2(x)$$

Let's say we run the naive algorithm where we go up to $\sqrt{x}$ to search for divisors.

What is the running time in the worst case?

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

What is N (the input size) in this case?

$$N = log_2(x)$$

Let's say we run the naive algorithm where we go up to $\sqrt{x}$ to search for divisors.

What is the running time in the worst case?

$$O(\sqrt{2^N})$$

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

What is N (the input size) in this case?

$$N = log_2(x)$$

Let's say we run the naive algorithm where we go up to $\sqrt{x}$ to search for divisors.

What is the running time in the worst case?

$$O(\sqrt{2^N}) \iff O(2^{N/2})$$

Input size

We have an algorithm which receives as input a number x and determines if it is prime.

What is N (the input size) in this case?

$$N = log_2(x)$$

Let's say we run the naive algorithm where we go up to $\sqrt{x}$ to search for divisors.

What is the running time in the worst case?

$$O(\sqrt{2^N}) \iff O(2^{N/2})$$

Exponential!

Universality

Universality

A quantum computation will be a unitary operation

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

All of them

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

All of them ...to a certain approximation

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

All of them ...to a certain approximation

If we only use unitaries from the set $\{H, T, CNOT\}$ we can approximate any unitary to any accuracy $\epsilon > 0$

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

All of them ...to a certain approximation

If we only use unitaries from the set $\{H, T, CNOT\}$ we can approximate any unitary to any accuracy $\epsilon > 0$

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

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

All of them ...to a certain approximation

If we only use unitaries from the set $\{H, T, CNOT\}$ we can approximate any unitary to any accuracy $\epsilon > 0$

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

We care about what you can do with a polynomial number of gates

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

All of them ...to a certain approximation

If we only use unitaries from the set $\{H, T, CNOT\}$ we can approximate any unitary to any accuracy $\epsilon > 0$

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

We care about what you can do with a polynomial number of gates

Class of problems solvable by a QC in poly time BQP

Universality

A quantum computation will be a unitary operation

What unitaries can we do?

All of them ...to a certain approximation

If we only use unitaries from the set $\{H, T, CNOT\}$ we can approximate any unitary to any accuracy $\epsilon > 0$

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

We care about what you can do with a polynomial number of gates

Class of problems solvable by a QC in poly time BQP

This includes all classical polynomial time computation

What is a quantum algorithm?

What is a quantum algorithm?

- Some combination of quantum gates

What is a quantum algorithm?

- Some combination of quantum gates
- Typically represented with quantum circuits

What is a quantum algorithm?

- Some combination of quantum gates
- Typically represented with quantum circuits
- Some more efficient than the corresponding classical algorithm

What is a quantum algorithm?

- Some combination of quantum gates
- Typically represented with quantum circuits
- Some more efficient than the corresponding classical algorithm
- Most of the time probabilistic

What is a quantum algorithm?

- Some combination of quantum gates
- Typically represented with quantum circuits
- Some more efficient than the corresponding classical algorithm
- Most of the time probabilistic
- Probability of success can easily be made absurdly high

What is a quantum algorithm?

- Some combination of quantum gates
- Typically represented with quantum circuits
- Some more efficient than the corresponding classical algorithm
- Most of the time probabilistic
- Probability of success can easily be made absurdly high
- Period finding, order finding, searching, factoring, discrete logarithm, optimization, "solving" linear systems etc

Absurdly high success probability

Absurdly high success probability

Two cases

Absurdly high success probability

Two cases

Assume in both that success probability is p

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

- Run algorithm k times or until solution is found

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

- Run algorithm k times or until solution is found
- Runs are independent

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

- Run algorithm k times or until solution is found
- Runs are independent
- Only need one successful run

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

- Run algorithm k times or until solution is found
- Runs are independent
- Only need one successful run
- Probability that all runs fail is $(1 - p)^k$

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

- Run algorithm k times or until solution is found
- Runs are independent
- Only need one successful run
- Probability that all runs fail is $(1-p)^k$
- If $p = 2/3$ and $k = 20 \rightarrow$ less than one in 3 billion!

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

- Run algorithm k times or until solution is found
- Runs are independent
- Only need one successful run
- Probability that all runs fail is $(1-p)^k$
- If $p = 2/3$ and $k = 20 \rightarrow$ less than one in 3 billion!

Why not $p > 0$? What's with the constant?

Absurdly high success probability

Two cases

Assume in both that success probability is p

Case 1

Can check whether we've found the solution (NP problems)

$p >$ positive constant

- Run algorithm k times or until solution is found
- Runs are independent
- Only need one successful run
- Probability that all runs fail is $(1-p)^k$
- If $p = 2/3$ and $k = 20 \rightarrow$ less than one in 3 billion!

Why not $p > 0$? What's with the constant?

We don't want p to be arbitrarily close to 0

Absurdly high success probability

Absurdly high success probability

Case 2

Can't check whether we've found the solution

$p > 1/2 +$ positive constant

Absurdly high success probability

Case 2

Can't check whether we've found the solution

$p > 1/2 +$ positive constant

- Run algorithm k times and take majority outcome

Absurdly high success probability

Case 2

Can't check whether we've found the solution

$p > 1/2 +$ positive constant

- Run algorithm k times and take majority outcome
- Runs are independent

Absurdly high success probability

Case 2

Can't check whether we've found the solution

$p > 1/2 +$ positive constant

- Run algorithm k times and take majority outcome
- Runs are independent
- Probability that more than half runs fail is $O((1-p)^{k/2})$

Absurdly high success probability

Case 2

Can't check whether we've found the solution

$p > 1/2 +$ positive constant

- Run algorithm k times and take majority outcome
- Runs are independent
- Probability that more than half runs fail is $O((1-p)^{k/2})$
- Choose a k that you're comfortable with

Absurdly high success probability

Case 2

Can't check whether we've found the solution

$p > 1/2 +$ positive constant

- Run algorithm k times and take majority outcome
- Runs are independent
- Probability that more than half runs fail is $O((1-p)^{k/2})$
- Choose a k that you're comfortable with

Why $p > 1/2 +$ constant? Why not $1/2$?

Absurdly high success probability

Case 2

Can't check whether we've found the solution

$p > 1/2 +$ positive constant

- Run algorithm k times and take majority outcome
- Runs are independent
- Probability that more than half runs fail is $O((1-p)^{k/2})$
- Choose a k that you're comfortable with

Why $p > 1/2 +$ constant? Why not $1/2$?

p could be arbitrarily (e.g. exponentially) close to $1/2$

First problem - Deutsch-Josza problem

First problem - Deutsch-Josza problem

Say we have $f : \{0,1\}^N \to \{0,1\}$ as a black box

First problem - Deutsch-Josza problem

Say we have $f : \{0,1\}^N \to \{0,1\}$ as a black box

We are **promised** that f is either *constant* or *balanced*

First problem - Deutsch-Josza problem

Say we have $f : \{0,1\}^N \to \{0,1\}$ as a black box

We are **promised** that f is either *constant* or *balanced*

Balanced means f outputs 0 on half of inputs
and 1 on the other half

First problem - Deutsch-Josza problem

Say we have $f : \{0,1\}^N \to \{0,1\}$ as a black box

We are **promised** that f is either *constant* or *balanced*

Balanced means f outputs 0 on half of inputs
and 1 on the other half

E.g. constant $\forall x, f(x) = 0$

First problem - Deutsch-Josza problem

Say we have $f : \{0,1\}^N \to \{0,1\}$ as a black box

We are **promised** that f is either *constant* or *balanced*

Balanced means f outputs 0 on half of inputs
and 1 on the other half

E.g. constant $\forall x, f(x) = 0$
balanced $\forall x, f(x) =$ parity of x

First problem - Deutsch-Josza problem

Say we have $f : \{0,1\}^N \to \{0,1\}$ as a black box

We are **promised** that f is either *constant* or *balanced*

Balanced means f outputs 0 on half of inputs
and 1 on the other half

E.g. constant $\forall x, f(x) = 0$
balanced $\forall x, f(x) =$ parity of x

How many calls to f do we need, worst case, to determine type?

First problem - Deutsch-Josza problem

Say we have $f : \{0,1\}^N \to \{0,1\}$ as a black box

We are **promised** that f is either *constant* or *balanced*

Balanced means f outputs 0 on half of inputs
and 1 on the other half

E.g. constant $\forall x, f(x) = 0$
balanced $\forall x, f(x) =$ parity of x

How many calls to f do we need, worst case, to determine type?

$$2^{N-1} + 1$$

Quantum case

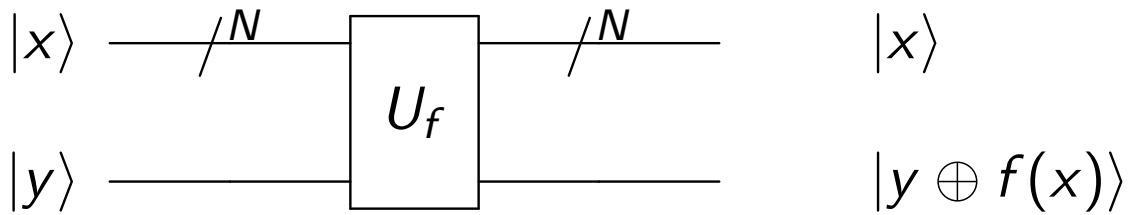
Quantum case

We must have a quantum implementation of f, a unitary U_f

Quantum case

We must have a quantum implementation of f, a unitary U_f

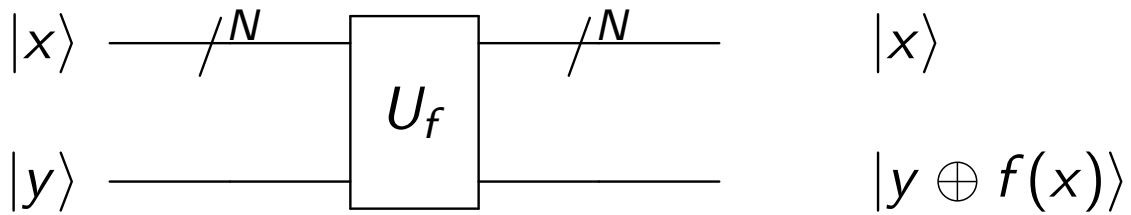
Would look like this:



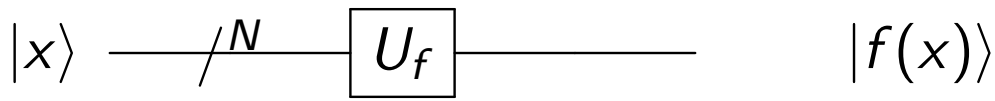
Quantum case

We must have a quantum implementation of f, a unitary U_f

Would look like this:



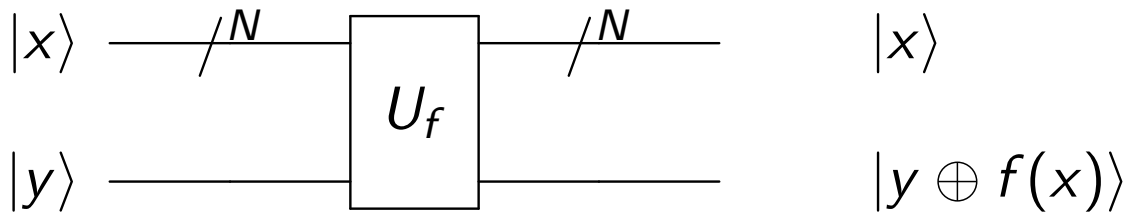
Why not...



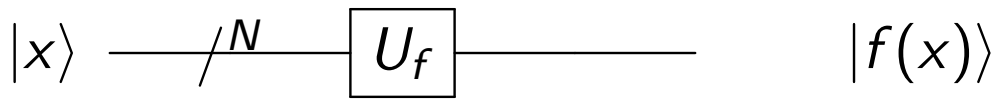
Quantum case

We must have a quantum implementation of f, a unitary U_f

Would look like this:



Why not...

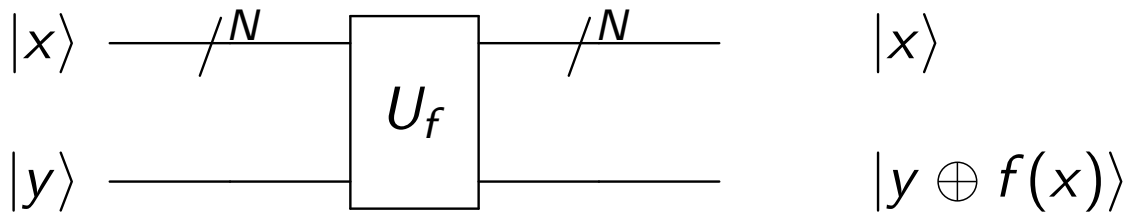


Not unitary!

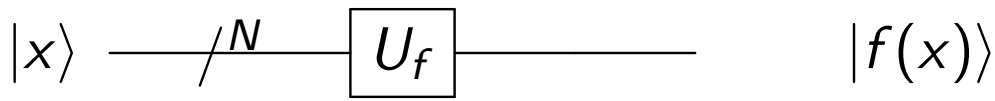
Quantum case

We must have a quantum implementation of f, a unitary U_f

Would look like this:



Why not...



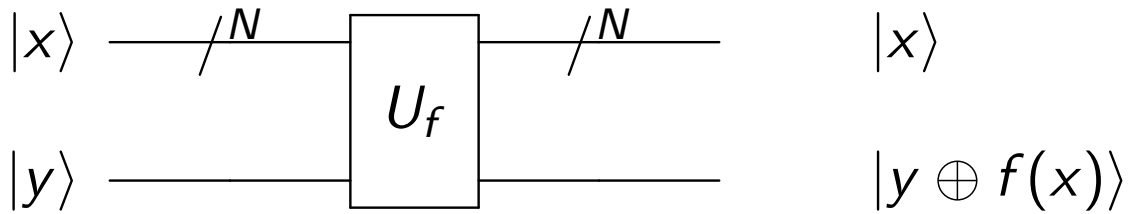
Not unitary!

Number of inputs must equal number of outputs!

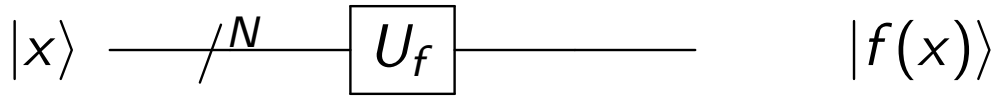
Quantum case

We must have a quantum implementation of f, a unitary U_f

Would look like this:



Why not...



Not unitary!

Number of inputs must equal number of outputs!

Must be **reversible**!

An example

An example

You've already seen an example of balanced U_f!

An example

You've already seen an example of balanced U_f!

Suppose $f : \{0, 1\} \to \{0, 1\}$, $f(x) = x$

An example

You've already seen an example of balanced U_f!

Suppose $f : \{0, 1\} \to \{0, 1\}$, $f(x) = x$

What is U_f?

An example

You've already seen an example of balanced U_f!

Suppose $f : \{0,1\} \to \{0,1\}$, $f(x) = x$

What is U_f?

CNOT

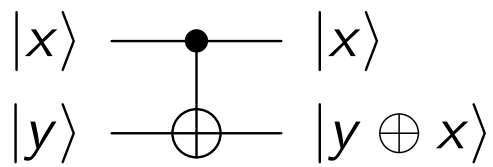
An example

You've already seen an example of balanced U_f!

Suppose $f : \{0,1\} \to \{0,1\}$, $f(x) = x$

What is U_f?

CNOT



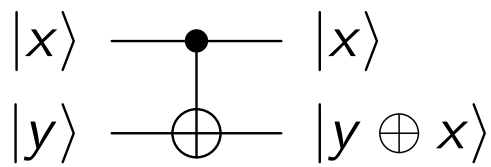
An example

You've already seen an example of balanced U_f!

Suppose $f : \{0, 1\} \to \{0, 1\}$, $f(x) = x$

What is U_f?

CNOT



What is $f(x) = 1 \oplus x$?

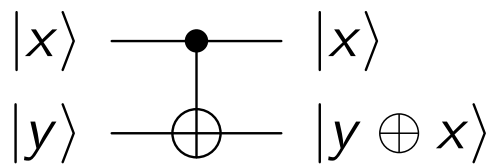
An example

You've already seen an example of balanced U_f!

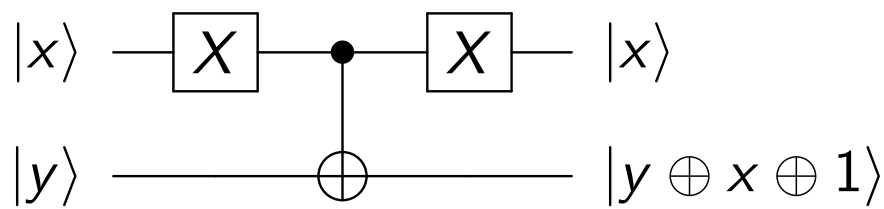
Suppose $f : \{0,1\} \to \{0,1\}$, $f(x) = x$

What is U_f?

CNOT



What is $f(x) = 1 \oplus x$?



Simplified version

Simplified version

For simplicity, stick to $N = 1$

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Superposition!

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly,

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly, $|0\rangle$,

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly, $|0\rangle$, $|1\rangle$,

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly, $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), ...$

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly, $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), ...$

So what if we plug-in $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$?

Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

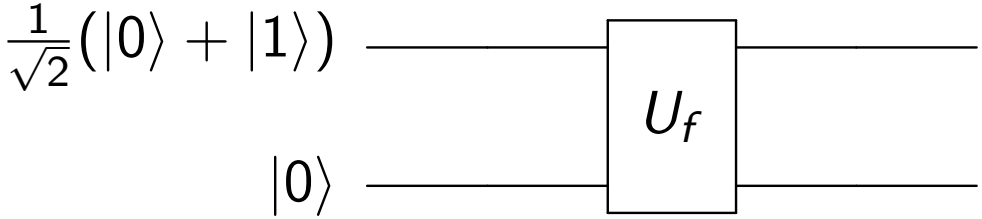
What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly, $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \ldots$

So what if we plug-in $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$?



Simplified version

For simplicity, stick to $N = 1$
(so classically we'd need 2 calls of f)

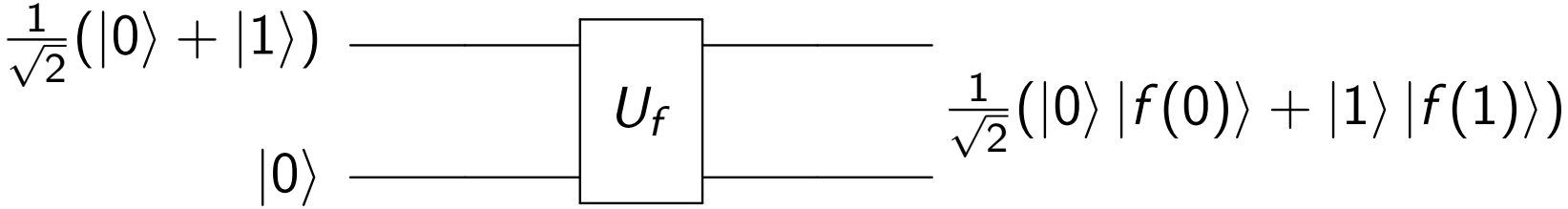
What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly, $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \ldots$

So what if we plug-in $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$?



Simplified version

For simplicity, take $N = 1$
(so classically we'd need 2 calls of f)

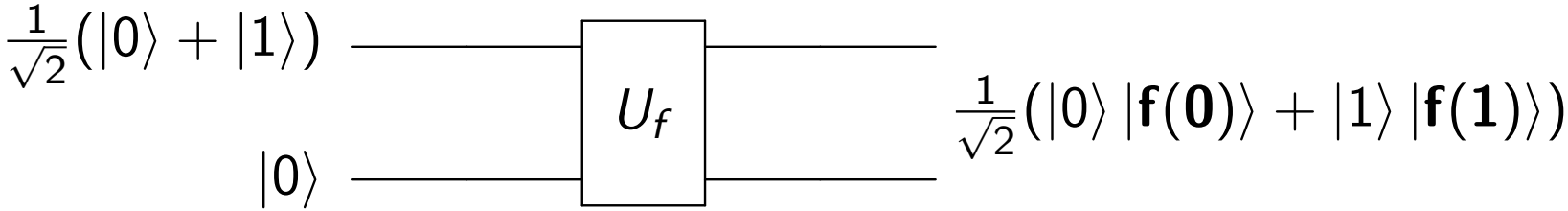
What can we do quantumly that we can't classically?

Superposition!

Classically, $x = 0, 1$

Quantumly, $|x\rangle = |0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \ldots$

So what if we plug-in $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|y\rangle = |0\rangle$



Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)$$

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle)$$

If f were constant...

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)$$

If f were constant... $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |f(0)\rangle$

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)$$

If f were constant... $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |f(0)\rangle$

A separable state!

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)$$

If f were constant... $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |f(0)\rangle$

A separable state!

Can't determine this in one measurement

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)$$

If f were constant... $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |f(0)\rangle$

A separable state!

Can't determine this in one measurement

What if the second input were also in superposition?

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)$$

If f were constant... $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |f(0)\rangle$

A separable state!

Can't determine this in one measurement

What if the second input were also in superposition?

Let's try: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle\,|f(0)\rangle + |1\rangle\,|f(1)\rangle)$$

If f were constant... $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |f(0)\rangle$

A separable state!

Can't determine this in one measurement

What if the second input were also in superposition?

Let's try: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

So input is: $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

Simplified version

$$\frac{1}{\sqrt{2}}(|0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle)$$

If f were constant... $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |f(0)\rangle$

A separable state!

Can't determine this in one measurement

What if the second input were also in superposition?

Let's try: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

So input is: $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

Output is: $\frac{1}{2}(|0\rangle |f(0)\rangle - |0\rangle |1 \oplus f(0)\rangle + |1\rangle |f(0)\rangle - |1\rangle |1 \oplus f(1)\rangle)$

Simplified version

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

Simplified version

$$\frac{1}{2}(|0\rangle\,|f(0)\rangle - |0\rangle\,|1 \oplus f(0)\rangle + |1\rangle\,|f(1)\rangle - |1\rangle\,|1 \oplus f(1)\rangle)$$

How does it look if f is constant?

Simplified version

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

How does it look if f is constant?

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

Simplified version

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

How does it look if f is constant?

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

Simplified version

$$\frac{1}{2}(|0\rangle\,|f(0)\rangle - |0\rangle\,|1 \oplus f(0)\rangle + |1\rangle\,|f(1)\rangle - |1\rangle\,|1 \oplus f(1)\rangle)$$

How does it look if f is constant?

$$\frac{1}{2}(|0\rangle\,|f(0)\rangle - |0\rangle\,|1 \oplus f(0)\rangle + |1\rangle\,|f(0)\rangle - |1\rangle\,|1 \oplus f(0)\rangle)$$

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

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

Simplified version

$$\frac{1}{2}(|0\rangle\,|f(0)\rangle - |0\rangle\,|1 \oplus f(0)\rangle + |1\rangle\,|f(1)\rangle - |1\rangle\,|1 \oplus f(1)\rangle)$$

How does it look if f is constant?

$$\frac{1}{2}(|0\rangle\,|f(0)\rangle - |0\rangle\,|1 \oplus f(0)\rangle + |1\rangle\,|f(0)\rangle - |1\rangle\,|1 \oplus f(0)\rangle)$$

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

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

But if $f(0) = 0$, then $1 \oplus f(0) = 1$

Simplified version

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

How does it look if f is constant?

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

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

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

But if $f(0) = 0$, then $1 \oplus f(0) = 1$
And if $f(0) = 1$, then $1 \oplus f(0) = 0$

Simplified version

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

How does it look if f is constant?

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

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

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

But if $f(0) = 0$, then $1 \oplus f(0) = 1$
And if $f(0) = 1$, then $1 \oplus f(0) = 0$

So in the end, we have...
$$\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Simplified version

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

Simplified version

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

What if f is balanced?

Simplified version

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

What if f is balanced?

That means

$$f(0) = 1 \oplus f(1)$$
$$f(1) = 1 \oplus f(0)$$

Simplified version

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

What if f is balanced?

That means

$$f(0) = 1 \oplus f(1)$$
$$f(1) = 1 \oplus f(0)$$

$$\frac{1}{2}(|0\rangle |f(0)\rangle - |0\rangle |f(1)\rangle + |1\rangle |f(1)\rangle - |1\rangle |f(0)\rangle)$$

Simplified version

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

What if f is balanced?

That means

$$f(0) = 1 \oplus f(1)$$
$$f(1) = 1 \oplus f(0)$$

$$\frac{1}{2}(|0\rangle |f(0)\rangle - |0\rangle |f(1)\rangle + |1\rangle |f(1)\rangle - |1\rangle |f(0)\rangle)$$

$$\frac{1}{2}((|0\rangle - |1\rangle)|f(0)\rangle - (|0\rangle - |1\rangle)|f(1)\rangle)$$

$$\frac{1}{2}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

Simplified version

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

What if f is balanced?

That means

$$f(0) = 1 \oplus f(1)$$
$$f(1) = 1 \oplus f(0)$$

$$\frac{1}{2}(|0\rangle |f(0)\rangle - |0\rangle |f(1)\rangle + |1\rangle |f(1)\rangle - |1\rangle |f(0)\rangle)$$

$$\frac{1}{2}((|0\rangle - |1\rangle)|f(0)\rangle - (|0\rangle - |1\rangle)|f(1)\rangle)$$

$$\frac{1}{2}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

But if $f(0) = 0$, then $f(1) = 1$

Simplified version

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

What if f is balanced?

That means

$$f(0) = 1 \oplus f(1)$$
$$f(1) = 1 \oplus f(0)$$

$$\frac{1}{2}(|0\rangle |f(0)\rangle - |0\rangle |f(1)\rangle + |1\rangle |f(1)\rangle - |1\rangle |f(0)\rangle)$$

$$\frac{1}{2}((|0\rangle - |1\rangle)|f(0)\rangle - (|0\rangle - |1\rangle)|f(1)\rangle)$$

$$\frac{1}{2}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

But if $f(0) = 0$, then $f(1) = 1$
And if $f(0) = 1$, then $f(1) = 0$

Simplified version

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

What if f is balanced?

That means
$$f(0) = 1 \oplus f(1)$$
$$f(1) = 1 \oplus f(0)$$

$$\frac{1}{2}(|0\rangle |f(0)\rangle - |0\rangle |f(1)\rangle + |1\rangle |f(1)\rangle - |1\rangle |f(0)\rangle)$$

$$\frac{1}{2}((|0\rangle - |1\rangle)|f(0)\rangle - (|0\rangle - |1\rangle)|f(1)\rangle)$$

$$\frac{1}{2}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

But if $f(0) = 0$, then $f(1) = 1$
And if $f(0) = 1$, then $f(1) = 0$

So in the end, we have...
$$\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Simplified version

Simplified version

Constant: $\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Simplified version

Constant: $\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Balanced: $\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Simplified version

Constant: $\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Balanced: $\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

If we apply H to first qubit we get...

Simplified version

Constant: $\pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Balanced: $\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

If we apply H to first qubit we get...

Constant: $\pm|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Balanced: $\pm|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Simplified version

$$\text{Constant: } \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If we apply H to first qubit we get...

$$\text{Constant: } \pm|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

So just measure first qubit in $(|0\rangle, |1\rangle)$ basis and we're done!

Simplified version

$$\text{Constant: } \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If we apply H to first qubit we get...

$$\text{Constant: } \pm|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

So just measure first qubit in $(|0\rangle, |1\rangle)$ basis and we're done!

Only one call of U_f!

Simplified version

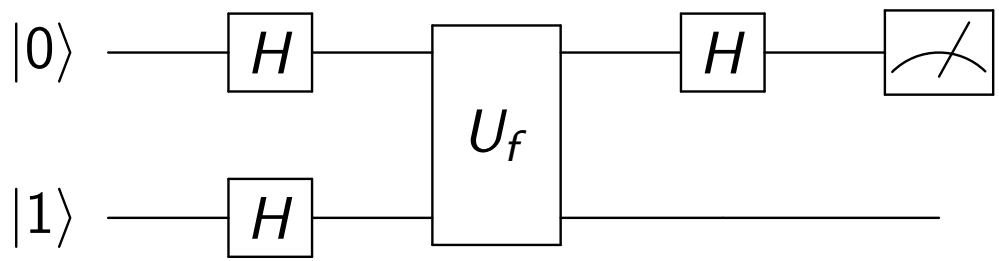
$$\text{Constant: } \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If we apply H to first qubit we get...

$$\text{Constant: } \pm|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

So just measure first qubit in $(|0\rangle, |1\rangle)$ basis and we're done!

Only one call of U_f!



Simplified version

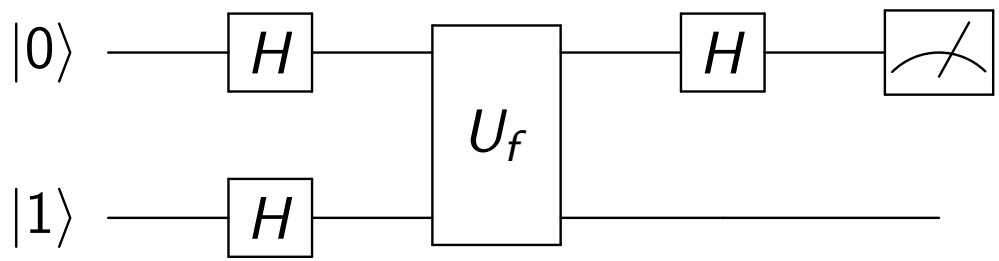
$$\text{Constant: } \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If we apply H to first qubit we get...

$$\text{Constant: } \pm|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\text{Balanced: } \pm|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

So just measure first qubit in $(|0\rangle, |1\rangle)$ basis and we're done!

Only one call of U_f!



Deutsch's algorithm

Before moving on... questions and discussions

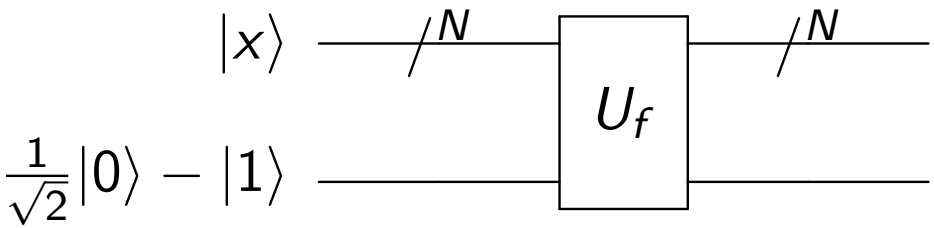
General version

General version

Back to the general case

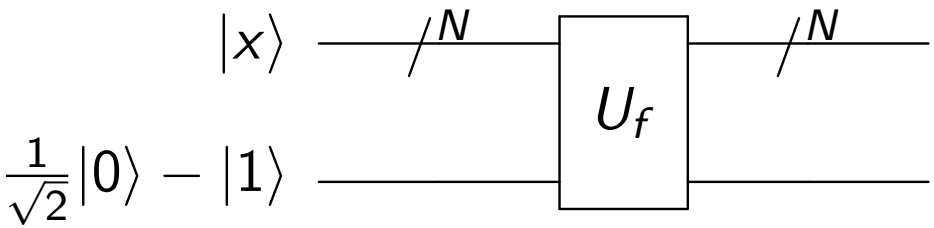
General version

Back to the general case



General version

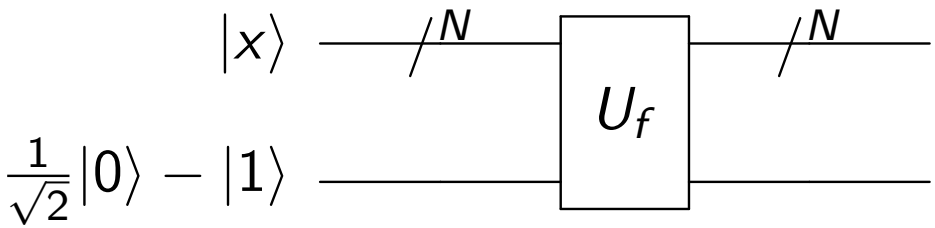
Back to the general case



What is the output when $|x\rangle$ is an arbitrary basis state?

General version

Back to the general case

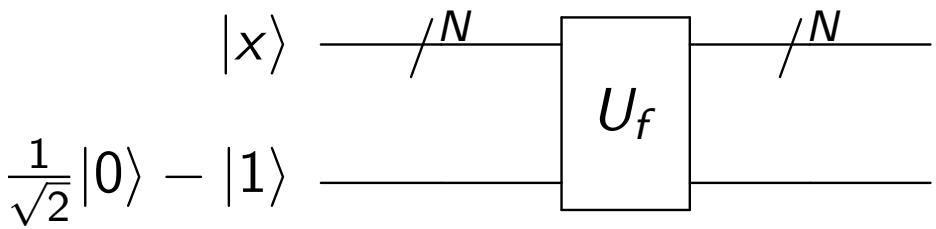


$$\frac{1}{\sqrt{2}}(|x\rangle\,|f(x)\rangle - |x\rangle\,|1 \oplus f(x)\rangle)$$

What is the output when $|x\rangle$ is an arbitrary basis state?

General version

Back to the general case

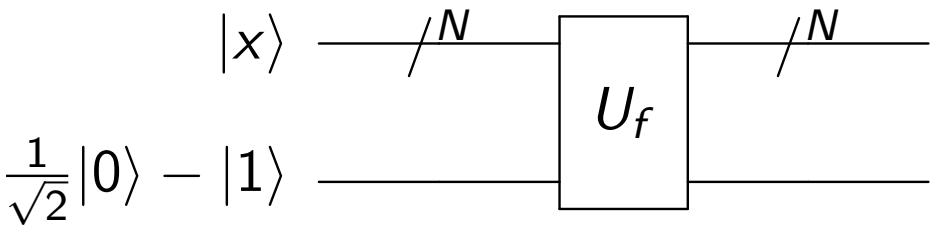


$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

What is the output when $|x\rangle$ is an arbitrary basis state?

General version

Back to the general case



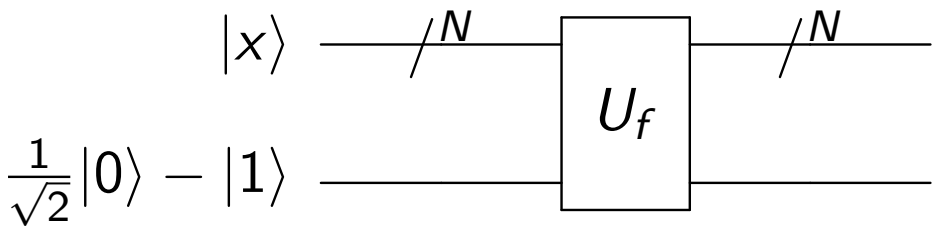
$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

What is the output when $|x\rangle$ is an arbitrary basis state?

But if $f(x) = 0$ then $1 \oplus f(x) = 1$
And if $f(x) = 1$ then $1 \oplus f(x) = 0$

General version

Back to the general case



$$|x\rangle \otimes \tfrac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

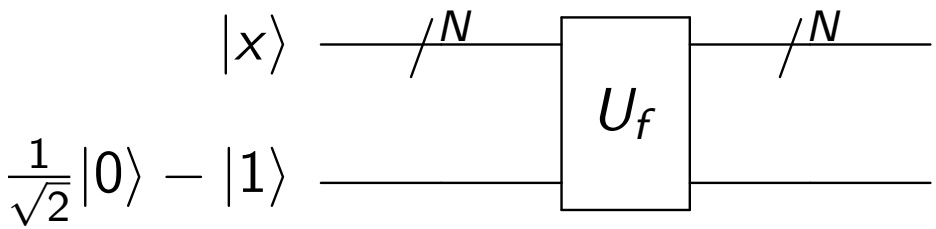
What is the output when $|x\rangle$ is an arbitrary basis state?

But if $f(x) = 0$ then $1 \oplus f(x) = 1$
And if $f(x) = 1$ then $1 \oplus f(x) = 0$

So our state is:
$(-1)^{f(x)}\,|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

General version

Back to the general case



$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

What is the output when $|x\rangle$ is an arbitrary basis state?

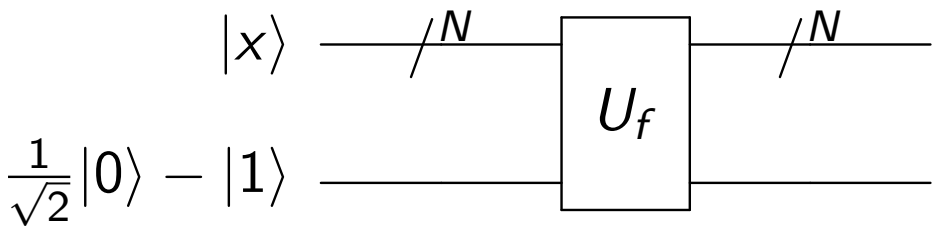
But if $f(x) = 0$ then $1 \oplus f(x) = 1$
And if $f(x) = 1$ then $1 \oplus f(x) = 0$

So our state is:
$$(-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

What if we had: $\sum_{x \in \{0,1\}^N} \frac{1}{\sqrt{2^N}}|x\rangle$

General version

Back to the general case



$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

What is the output when $|x\rangle$ is an arbitrary basis state?

But if $f(x) = 0$ then $1 \oplus f(x) = 1$
And if $f(x) = 1$ then $1 \oplus f(x) = 0$

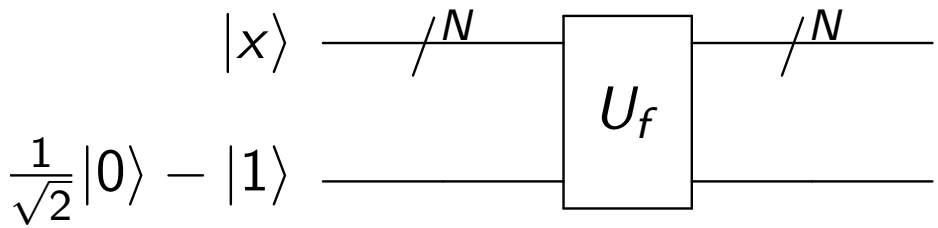
So our state is:
$$(-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

What if we had: $\sum_{x \in \{0,1\}^N} \frac{1}{\sqrt{2^N}}|x\rangle$

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

General version

Back to the general case



$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

What is the output when $|x\rangle$ is an arbitrary basis state?

But if $f(x) = 0$ then $1 \oplus f(x) = 1$
And if $f(x) = 1$ then $1 \oplus f(x) = 0$

So our state is:

$$(-1)^{f(x)}\,|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

What if we had: $\sum_{x\in\{0,1\}^N} \frac{1}{\sqrt{2^N}}\,|x\rangle$

$$\frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} (-1)^{f(x)}\,|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Where $|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Where $|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$

If $|\psi\rangle$ and $\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle$ are orthogonal, we are done!

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Where $|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$

If $|\psi\rangle$ and $\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle$ are orthogonal, we are done!

But $\langle x \,|\, \psi \rangle =$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Where $|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$

If $|\psi\rangle$ and $\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle$ are orthogonal, we are done!

But $\langle x \,|\, \psi \rangle = (-1)^{f(x)} \frac{1}{\sqrt{2^N}}$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Where $|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$

If $|\psi\rangle$ and $\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle$ are orthogonal, we are done!

But $\langle x \,|\, \psi\rangle = (-1)^{f(x)} \frac{1}{\sqrt{2^N}}$

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} \langle x \,|\, \psi\rangle =$$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Where $|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$

If $|\psi\rangle$ and $\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle$ are orthogonal, we are done!

But $\langle x \,|\, \psi\rangle = (-1)^{f(x)} \frac{1}{\sqrt{2^N}}$

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} \langle x \,|\, \psi\rangle = \frac{1}{2^N} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} =$$

General version

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is constant, then...

$$\pm\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

If f is balanced, then...

$$|\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

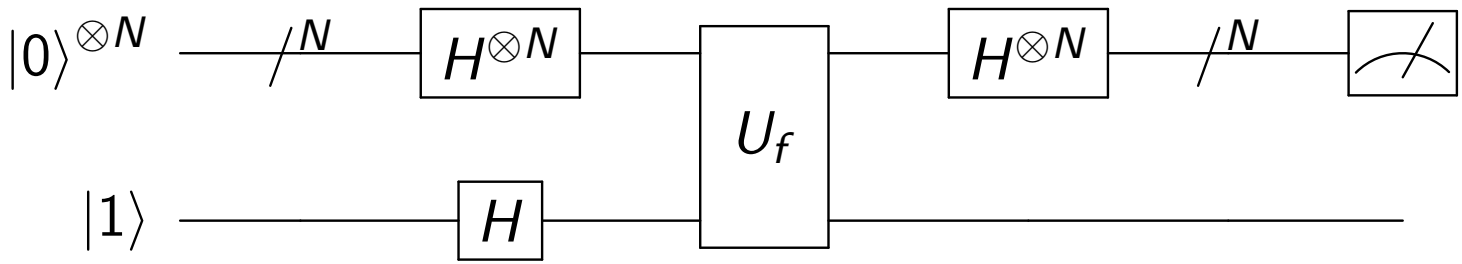
Where $|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle$

If $|\psi\rangle$ and $\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} |x\rangle$ are orthogonal, we are done!

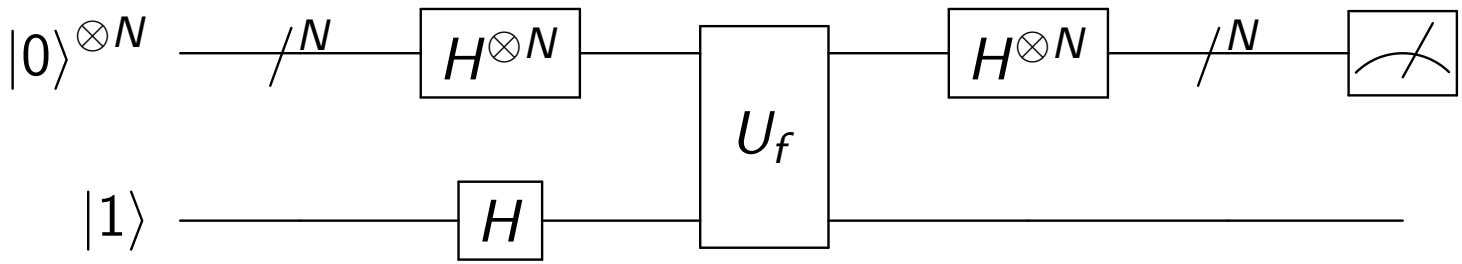
But $\langle x \,|\, \psi\rangle = (-1)^{f(x)} \frac{1}{\sqrt{2^N}}$

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} \langle x \,|\, \psi\rangle = \frac{1}{2^N} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} = 0$$

Deutsch-Josza algorithm

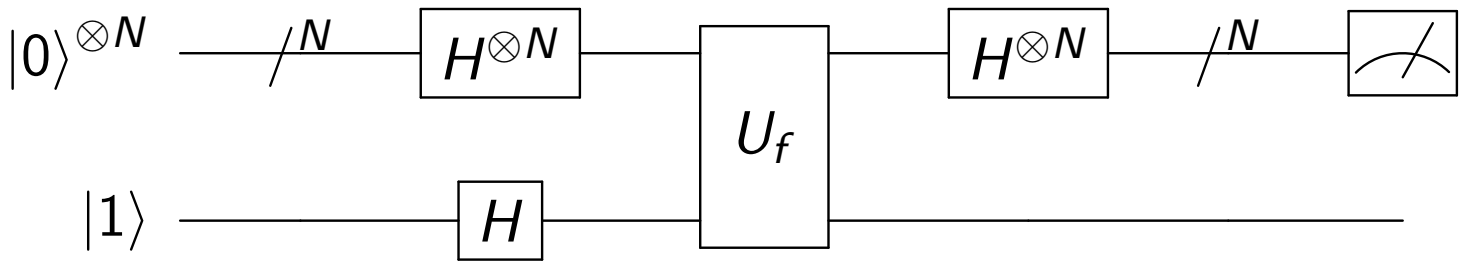


Deutsch-Josza algorithm



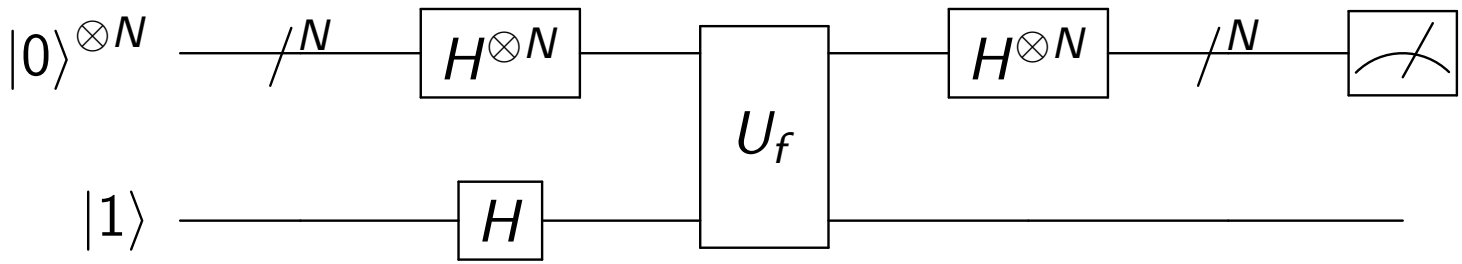
- If we measure $|0\rangle^{\otimes N}$ then **constant**

Deutsch-Josza algorithm



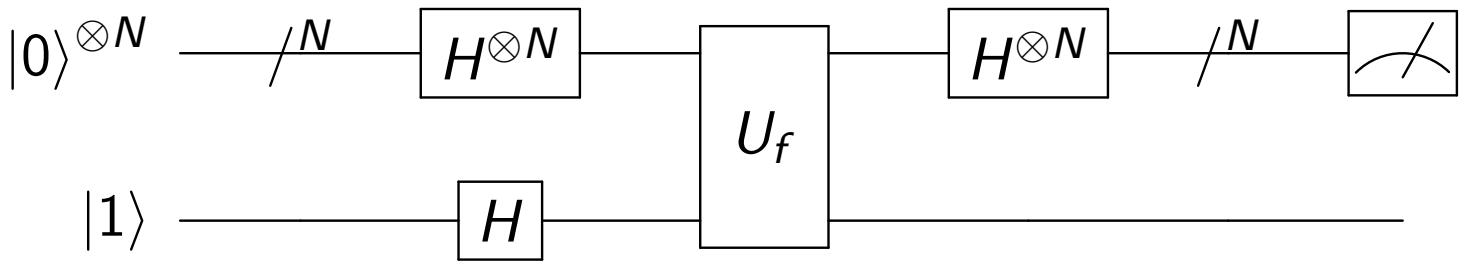
- If we measure $|0\rangle^{\otimes N}$ then **constant**
- Otherwise **balanced**

Deutsch-Josza algorithm



- If we measure $|0\rangle^{\otimes N}$ then **constant**
- Otherwise **balanced**
- Only <u>one evaluation</u> of U_f vs $2^{N-1}+1$

Deutsch-Josza algorithm



- If we measure $|0\rangle^{\otimes N}$ then **constant**
- Otherwise **balanced**
- Only <u>one evaluation</u> of U_f vs $2^{N-1}+1$
- Exponential speed-up!

Problems

Problems

Deutsch-Josza can be solved probabilistically with constant number of queries

Problems

Deutsch-Josza can be solved probabilistically with constant number of queries

It doesn't seem very useful

Problems

Deutsch-Josza can be solved probabilistically with constant number of queries

It doesn't seem very useful

Doesn't relate to cryptography

Problems

Deutsch-Josza can be solved probabilistically with constant number of queries

It doesn't seem very useful

Doesn't relate to cryptography

But it's a stepping stone :)

Problems

Deutsch-Josza can be solved probabilistically with constant number of queries

It doesn't seem very useful

Doesn't relate to cryptography

But it's a stepping stone :)

After the break we'll look at a more interesting problem

Problems

Deutsch-Josza can be solved probabilistically with constant number of queries

It doesn't seem very useful

Doesn't relate to cryptography

But it's a stepping stone :)

After the break we'll look at a more interesting problem

One last thing before that...

A very useful relation

A very useful relation

What is $H^{\otimes N} |x\rangle$?

A very useful relation

What is $H^{\otimes N} |x\rangle$?

$$H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

A very useful relation

What is $H^{\otimes N} |x\rangle$?

$$H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H^{\otimes N} |0\rangle^{\otimes N} = \frac{1}{2^{N/2}} \sum_{y \in \{0,1\}^N} |y\rangle$$

A very useful relation

What is $H^{\otimes N} |x\rangle$?

$$H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H^{\otimes N} |0\rangle^{\otimes N} = \frac{1}{2^{N/2}} \sum_{y \in \{0,1\}^N} |y\rangle$$

After some calculation...

A very useful relation

What is $H^{\otimes N} |x\rangle$?

$$H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H^{\otimes N} |0\rangle^{\otimes N} = \frac{1}{2^{N/2}} \sum_{y \in \{0,1\}^N} |y\rangle$$

After some calculation...

$$H^{\otimes N} |x\rangle = \frac{1}{2^{N/2}} \sum_{y \in \{0,1\}^N} (-1)^{x \cdot y} |y\rangle$$

A very useful relation

What is $H^{\otimes N} |x\rangle$?

$$H |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H^{\otimes N} |0\rangle^{\otimes N} = \frac{1}{2^{N/2}} \sum_{y \in \{0,1\}^N} |y\rangle$$

After some calculation...

$$H^{\otimes N} |x\rangle = \frac{1}{2^{N/2}} \sum_{y \in \{0,1\}^N} (-1)^{x \cdot y} |y\rangle$$

You should remember this, it comes up a lot :)

Useful resources and references

- **A graphical quantum simulator** - http://www.quantumplayground.net/
- **Python SymPy for Quantum Computation** - http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1038&context=physsp
- **Quantum Mechanics modules in SymPy** - http://docs.sympy.org/latest/modules/physics/quantum/index.html
- **Quantum Programming Languages** - http://www.quantiki.org/wiki/Quantum_Programming_Language
- **List of quantum algorithms** - http://math.nist.gov/quantum/zoo/
- **Lecture on quantum algorithms** - https://www.cs.berkeley.edu/~vazirani/algorithms/chap10.pdf
- **Quantum registers and algorithms** - http://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf