# Quantum computing for dummies

Carlos Cotrini

ETH Zürich

*ccarlos@inf.ethz.ch*

September 14, 2019

# What is quantum computing?

From Wikipedia: "Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation."

It can, in some cases, be much more faster than classical computing.

# A toy problem

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

# A toy problem

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

### The problem

Given a bit array $f$ of length $2^n$, known to be balanced or constant, decide if it is balanced.

# A toy problem

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

**The problem**

Given a bit array $f$ of length $2^n$, known to be balanced or constant, decide if it is balanced.

A classical computer takes time linear in the length of the bit array to solve this problem.

# A toy problem

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

## The problem

Given a bit array $f$ of length $2^n$, known to be balanced or constant, decide if it is balanced.

A classical computer takes time linear in the length of the bit array to solve this problem.
A quantum computer takes **logarithmic** time (by the Deutsch-Jozsa algorithm).

# A more practical example

A quantum computer can find an element in an array of length $N$ in $O(\sqrt{N})$-time (by Grover's algorithm).

# Overview

1. Background
   - Qubits and qubit arrays
   - Quantum gates
2. The Deutsch-Jozsa algorithm
3. Grover's algorithm
   - Background in linear algebra
   - Grover's algorithm

# Qubits

Assume I have a closed box with a cat inside.

# Qubits

Assume I have a closed box with a cat inside.

If it is a classical cat, then it is either dead or alive.

# Qubits

Assume I have a closed box with a cat inside.

If it is a classical cat, then it is either dead or alive.

If it is a quantum cat, then it is both dead and alive. A quantum phenomenon called *superposition*.

# Qubits

Assume I have a closed box with a cat inside.

If it is a classical cat, then it is either dead or alive.

If it is a quantum cat, then it is both dead and alive. A quantum phenomenon called *superposition*.

A bit is a value that is either 0 or 1.

# Qubits

Assume I have a closed box with a cat inside.

If it is a classical cat, then it is either dead or alive.

If it is a quantum cat, then it is both dead and alive. A quantum phenomenon called *superposition*.

A bit is a value that is either 0 or 1.

A quantum bit is a value that is both 0 and 1 (superposition).

# Qubits

What is a qubit?

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2 =$ probability that we get a 0, when we measure the qubit.

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2 =$ probability that we get a 0, when we measure the qubit.
- $|a_1|^2 =$ probability that we get a 1, when we measure the qubit.

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2$ = probability that we get a 0, when we measure the qubit.
- $|a_1|^2$ = probability that we get a 1, when we measure the qubit.

Examples:

| Qubits | $P(0)$ | $P(1)$ |
|---|---|---|
| $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2 =$ probability that we get a 0, when we measure the qubit.
- $|a_1|^2 =$ probability that we get a 1, when we measure the qubit.

Examples:

| Qubits | $P(0)$ | $P(1)$ |
|---|---|---|
| $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ | | |

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2 =$ probability that we get a 0, when we measure the qubit.
- $|a_1|^2 =$ probability that we get a 1, when we measure the qubit.

Examples:

| Qubits | $P(0)$ | $P(1)$ |
|---|---|---|
| $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2 =$ probability that we get a 0, when we measure the qubit.
- $|a_1|^2 =$ probability that we get a 1, when we measure the qubit.

Examples:

| Qubits | $P(0)$ | $P(1)$ |
|---|---|---|
| $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(0, 1)$ | | |

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2 =$ probability that we get a 0, when we measure the qubit.
- $|a_1|^2 =$ probability that we get a 1, when we measure the qubit.

Examples:

| Qubits | $P(0)$ | $P(1)$ |
|---|---|---|
| $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(0, 1)$ | 0 | 1 |

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2 =$ probability that we get a 0, when we measure the qubit.
- $|a_1|^2 =$ probability that we get a 1, when we measure the qubit.

Examples:

| Qubits | $P(0)$ | $P(1)$ |
|---|---|---|
| $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(0, 1)$ | 0 | 1 |
| $(-1, 0)$ | | |

# Qubits

What is a qubit?

$$(a_0, a_1) \in \mathbb{C}^2 \text{ with } |a_0|^2 + |a_1|^2 = 1.$$

- $|a_0|^2$ = probability that we get a 0, when we measure the qubit.
- $|a_1|^2$ = probability that we get a 1, when we measure the qubit.

Examples:

| Qubits | $P(0)$ | $P(1)$ |
|---|---|---|
| $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $(0, 1)$ | 0 | 1 |
| $(-1, 0)$ | 1 | 0 |

# Qubits

| Value | | State | | Probability |
|---|---|---|---|---|
| 0 | $\mapsto$ | $a_0$ | $\mapsto$ | $\lvert a_0 \rvert^2$ |
| 1 | $\mapsto$ | $a_1$ | $\mapsto$ | $\lvert a_1 \rvert^2$ |

A qubit represents a single storage unit where **both** a 0 and a 1 are stored at the same time (in superposition). It is not that a qubit is storing two values in "physically" different spaces. The 0 and the 1 are in the same "physical" space.

# Qubit arrays

# Qubit arrays

Fix $n \in \mathbb{N}$.

# Qubit arrays

Fix $n \in \mathbb{N}$.
A bit array is one sequence of $n$ bits.

# Qubit arrays

Fix $n \in \mathbb{N}$.
A bit array is one sequence of $n$ bits.
A qubit array is **all** sequences of $n$ bits (superposition).

# Qubit arrays

Fix $n \in \mathbb{N}$.
A bit array is one sequence of $n$ bits.
A qubit array is **all** sequences of $n$ bits (superposition).
When you observe the array, you see a bit array $x$ of $n$ bits with probability $|a_x|^2$.

# Qubit arrays

Fix $n \in \mathbb{N}$.
A bit array is one sequence of $n$ bits.
A qubit array is **all** sequences of $n$ bits (superposition).
When you observe the array, you see a bit array $x$ of $n$ bits with probability $|a_x|^2$.
So a qubit array is defined by one complex number $a_x$ for each possible bit array in $\{0, 1\}^n$.

# Qubit arrays

# Qubit arrays

What is a qubit array of length $n$?

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \ldots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$

$$\text{such that } \sum_x |a_x|^2 = 1.$$

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \ldots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \ldots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

Examples:

| Qubit array | $P(00)$ | $P(01)$ | $P(10)$ | $P(11)$ |
|---|---|---|---|---|

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \dots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

Examples:

| Qubit array | $P(00)$ | $P(01)$ | $P(10)$ | $P(11)$ |
|---|---|---|---|---|
| $(0, \frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ | | | | |

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \dots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

Examples:

| Qubit array | $P(00)$ | $P(01)$ | $P(10)$ | $P(11)$ |
|---|---|---|---|---|
| $(0, \frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ | 0 | $\frac{1}{2}$ | 0 | $\frac{1}{2}$ |

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \ldots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

Examples:

| Qubit array | $P(00)$ | $P(01)$ | $P(10)$ | $P(11)$ |
|---|---|---|---|---|
| $(0, \frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ | 0 | $\frac{1}{2}$ | 0 | $\frac{1}{2}$ |
| $(0, \frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2})$ | | | | |

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \ldots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

Examples:

| Qubit array | $P(00)$ | $P(01)$ | $P(10)$ | $P(11)$ |
|---|---|---|---|---|
| $(0, \frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ | 0 | $\frac{1}{2}$ | 0 | $\frac{1}{2}$ |
| $(0, \frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2})$ | 0 | $\frac{1}{2}$ | $\frac{1}{4}$ | $\frac{1}{4}$ |

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \dots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

Examples:

| Qubit array | $P(00)$ | $P(01)$ | $P(10)$ | $P(11)$ |
|---|---|---|---|---|
| $(0, \frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ | 0 | $\frac{1}{2}$ | 0 | $\frac{1}{2}$ |
| $(0, \frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2})$ | 0 | $\frac{1}{2}$ | $\frac{1}{4}$ | $\frac{1}{4}$ |
| $(1, 0, 0, 0)$ | | | | |

# Qubit arrays

What is a qubit array of length $n$?

$$(a_0, a_1, \ldots, a_{N-1}) \in \mathbb{C}^N, \text{ with } N = 2^n \text{ and}$$
$$\text{such that } \sum_x |a_x|^2 = 1.$$

$|a_x|^2$ is the probability, that after observing the qubit array, we get $x$.

Examples:

| Qubit array | $P(00)$ | $P(01)$ | $P(10)$ | $P(11)$ |
|---|---|---|---|---|
| $(0, \frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}})$ | 0 | $\frac{1}{2}$ | 0 | $\frac{1}{2}$ |
| $(0, \frac{1}{\sqrt{2}}, \frac{1}{2}, \frac{1}{2})$ | 0 | $\frac{1}{2}$ | $\frac{1}{4}$ | $\frac{1}{4}$ |
| $(1, 0, 0, 0)$ | 1 | 0 | 0 | 0 |

# Qubit arrays

More examples:

- $(1/2, 0, 0, 1/2, 0, 0, 0, 1/\sqrt{2})$ is a qubit array that, when observed, yields 000 with prob $1/4$, 011 with prob $1/4$, and 111 with probability $1/2$.

# Qubit arrays

More examples:

- $(1/2, 0, 0, 1/2, 0, 0, 0, 1/\sqrt{2})$ is a qubit array that, when observed, yields 000 with prob $1/4$, 011 with prob $1/4$, and 111 with probability $1/2$.
- $(1/\sqrt{8}, 1/\sqrt{8}, 1/\sqrt{8}, 1/\sqrt{8}, 1/\sqrt{8}, 1/\sqrt{8}, 1/\sqrt{8}, 1/\sqrt{8})$ is a qubit array that, when observed, yields any bit array of length 3 with equal probability.

# Qubit arrays

$$
\begin{array}{ccccccc}
000 & \mapsto & a_{000} & \mapsto & a_0 & \mapsto & |a_0|^2 \\
001 & \mapsto & a_{001} & \mapsto & a_1 & \mapsto & |a_1|^2 \\
010 & \mapsto & a_{010} & \mapsto & a_2 & \mapsto & |a_2|^2 \\
011 & \mapsto & a_{011} & \mapsto & a_3 & \mapsto & |a_3|^2 \\
100 & \mapsto & a_{100} & \mapsto & a_4 & \mapsto & |a_4|^2 \\
101 & \mapsto & a_{101} & \mapsto & a_5 & \mapsto & |a_5|^2 \\
110 & \mapsto & a_{110} & \mapsto & a_6 & \mapsto & |a_6|^2 \\
111 & \mapsto & a_{111} & \mapsto & a_7 & \mapsto & |a_7|^2
\end{array}
$$

A qubit array of length $n$ is a storage unit with $n$ bits of capacity. A qubit array is not a data structure containing all bit arrays in $2^n$ "physically" different locations. All $2^n$ bit arrays are in the "physical" storage unit with $n$ bits of capacity, coexisting in superposition.

# Qubit arrays are vectors in $\mathbb{C}^N$

For $x \in \{0,1\}^n$, let $|x\rangle$ be the qubit array with all entries equal zero except the $x$-th, which is 1.

# Qubit arrays are vectors in $\mathbb{C}^N$

For $x \in \{0,1\}^n$, let $|x\rangle$ be the qubit array with all entries equal zero except the $x$-th, which is 1.

Examples:

# Qubit arrays are vectors in $\mathbb{C}^N$

For $x \in \{0,1\}^n$, let $|x\rangle$ be the qubit array with all entries equal zero except the $x$-th, which is 1.

Examples:

- $|10\rangle = (0, 0, 1, 0)$.

# Qubit arrays are vectors in $\mathbb{C}^N$

For $x \in \{0,1\}^n$, let $|x\rangle$ be the qubit array with all entries equal zero except the $x$-th, which is 1.

Examples:

- $|10\rangle = (0,0,1,0)$.
- $|011\rangle = (0,0,0,1,0,0,0,0)$.

# Qubit arrays are vectors in $\mathbb{C}^N$

For $x \in \{0,1\}^n$, let $|x\rangle$ be the qubit array with all entries equal zero except the $x$-th, which is 1.

Examples:

- $|10\rangle = (0,0,1,0)$.
- $|011\rangle = (0,0,0,1,0,0,0,0)$.
- $|0000\rangle = (1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$.

# Qubit arrays are vectors in $\mathbb{C}^N$

For $x \in \{0,1\}^n$, let $|x\rangle$ be the qubit array with all entries equal zero except the $x$-th, which is 1.

Examples:

- $|10\rangle = (0,0,1,0)$.
- $|011\rangle = (0,0,0,1,0,0,0,0)$.
- $|0000\rangle = (1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$.

**Definition**

$\mathcal{B}_n := \{|x\rangle \mid x \in \{0,1\}^n\}$.

# Qubit arrays are vectors in $\mathbb{C}^N$

For $x \in \{0,1\}^n$, let $|x\rangle$ be the qubit array with all entries equal zero except the $x$-th, which is 1.

Examples:

- $|10\rangle = (0,0,1,0)$.
- $|011\rangle = (0,0,0,1,0,0,0,0)$.
- $|0000\rangle = (1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$.

**Definition**

$\mathcal{B}_n := \{|x\rangle \mid x \in \{0,1\}^n\}$.

Example: $\mathcal{B}_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

# $\mathcal{B}_n$ is a basis

Let $|\psi\rangle = (a_0, a_1, \ldots, a_{N-1})$, then

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle .$$

# $\mathcal{B}_n$ is a basis

Let $|\psi\rangle = (a_0, a_1, \ldots, a_{N-1})$, then

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle .$$

$\sum_{x \in \{0,1\}^n} a_x |x\rangle$ is $|\psi\rangle$'s *algebraic representation*.

# $\mathcal{B}_n$ is a basis

Let $|\psi\rangle = (a_0, a_1, \ldots, a_{N-1})$, then

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle .$$

$\sum_{x \in \{0,1\}^n} a_x |x\rangle$ is $|\psi\rangle$'s *algebraic representation*.

$(a_0, a_1, \ldots, a_N)$ is $|\psi\rangle$'s *vector representation*.

# $\mathcal{B}_n$ is a basis

Let $|\psi\rangle = (a_0, a_1, \ldots, a_{N-1})$, then

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle .$$

$\sum_{x \in \{0,1\}^n} a_x |x\rangle$ is $|\psi\rangle$'s *algebraic representation*.

$(a_0, a_1, \ldots, a_N)$ is $|\psi\rangle$'s *vector representation*.

Examples:

# $\mathcal{B}_n$ is a basis

Let $|\psi\rangle = (a_0, a_1, \ldots, a_{N-1})$, then

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x |x\rangle .$$

$\sum_{x\in\{0,1\}^n} a_x |x\rangle$ is $|\psi\rangle$'s *algebraic representation*.

$(a_0, a_1, \ldots, a_N)$ is $|\psi\rangle$'s *vector representation*.

Examples:

- $\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(1,0) - \frac{1}{\sqrt{2}}(0,1) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle .$

# $\mathcal{B}_n$ is a basis

Let $|\psi\rangle = (a_0, a_1, \ldots, a_{N-1})$, then

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x |x\rangle .$$

$\sum_{x\in\{0,1\}^n} a_x |x\rangle$ is $|\psi\rangle$'s *algebraic representation*.

$(a_0, a_1, \ldots, a_N)$ is $|\psi\rangle$'s *vector representation*.

Examples:

- $\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(1,0) - \frac{1}{\sqrt{2}}(0,1) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle .$
- $\left(0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right) = \frac{1}{\sqrt{2}}(0,1,0,0) - \frac{1}{\sqrt{2}}(0,0,1,0) = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle .$

# $\mathcal{B}_n$ is a basis

Let $|\psi\rangle = (a_0, a_1, \ldots, a_{N-1})$, then

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle .$$

$\sum_{x \in \{0,1\}^n} a_x |x\rangle$ is $|\psi\rangle$'s *algebraic representation*.

$(a_0, a_1, \ldots, a_N)$ is $|\psi\rangle$'s *vector representation*.

Examples:

- $\left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(1,0) - \frac{1}{\sqrt{2}}(0,1) = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle .$
- $\left(0, \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0\right) = \frac{1}{\sqrt{2}}(0,1,0,0) - \frac{1}{\sqrt{2}}(0,0,1,0) = \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle .$
- $(0,0,0,0,0,0,0,-1) = -(0,0,0,0,0,0,0,1) = -|111\rangle .$

# Measurements

A measurement operator receives as input a qubit array $\sum_x a_x |x\rangle$ and outputs $x$ with probability $|a_x|^2$.

# Measurements

A measurement operator receives as input a qubit array $\sum_x a_x |x\rangle$ and outputs $x$ with probability $|a_x|^2$.

Examples:

- Measuring $-\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ yields 1 with probability $\frac{3}{4}$.

# Measurements

A measurement operator receives as input a qubit array $\sum_x a_x |x\rangle$ and outputs $x$ with probability $|a_x|^2$.

Examples:

- Measuring $-\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ yields 1 with probability $\frac{3}{4}$.
- Measuring $|1\rangle$ yields 1 with probability 1.

# Measurements

A measurement operator receives as input a qubit array $\sum_x a_x |x\rangle$ and outputs $x$ with probability $|a_x|^2$.

Examples:

- Measuring $-\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ yields 1 with probability $\frac{3}{4}$.
- Measuring $|1\rangle$ yields 1 with probability 1.

## Observation

After measuring a qubit array, all its uncertainty is lost. Measuring again gives the same result.

# Quantum gates

A *quantum gate* is a unitary transformation $G : \mathbb{C}^N \to \mathbb{C}^N$.

# Quantum gates

A *quantum gate* is a unitary transformation $G : \mathbb{C}^N \to \mathbb{C}^N$.

For now, the most important thing to know about unitary transformations is that they are *linear*:

$$G\left(\sum_x a_x |x\rangle\right) = \sum_x a_x G |x\rangle .$$

# Quantum gates

A *quantum gate* is a unitary transformation $G : \mathbb{C}^N \to \mathbb{C}^N$.

For now, the most important thing to know about unitary transformations is that they are *linear*:

$$G\left(\sum_x a_x |x\rangle\right) = \sum_x a_x G |x\rangle .$$

Example:

$$G\left(\frac{1}{2}|00\rangle - \frac{1}{2}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{2}G|00\rangle - \frac{1}{2}G|10\rangle - \frac{1}{\sqrt{2}}G|11\rangle .$$

# Quantum gates

A *quantum gate* is a unitary transformation $G : \mathbb{C}^N \to \mathbb{C}^N$.

For now, the most important thing to know about unitary transformations is that they are *linear*:

$$G\left(\sum_x a_x |x\rangle\right) = \sum_x a_x G|x\rangle .$$

Example:

$$G\left(\frac{1}{2}|00\rangle - \frac{1}{2}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{2}G|00\rangle - \frac{1}{2}G|10\rangle - \frac{1}{\sqrt{2}}G|11\rangle .$$

To compute $G|\psi\rangle$, you only need to know how $G$ works on $\mathcal{B}_n$.

# Popular quantum gates

- Hadamard gate.
- Emulation gate.
- Reflection gate.

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y \in \{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle ,$$

where $x^\top y := \sum_{i \leq n} x[i]y[i]$ is the classical inner product.

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y\in\{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle,$$

where $x^\top y := \sum_{i\leq n} x[i]y[i]$ is the classical inner product.

Example:

$$H|0\rangle =$$

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y \in \{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle,$$

where $x^\top y := \sum_{i \le n} x[i]y[i]$ is the classical inner product.

Example:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y \in \{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle,$$

where $x^\top y := \sum_{i \leq n} x[i]y[i]$ is the classical inner product.

Example:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

$$H|01\rangle =$$

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y \in \{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle ,$$

where $x^\top y := \sum_{i \leq n} x[i]y[i]$ is the classical inner product.

Example:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle .$$

$$H|01\rangle = \frac{1}{2}|00\rangle$$

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y \in \{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle ,$$

where $x^\top y := \sum_{i \leq n} x[i]y[i]$ is the classical inner product.

Example:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle .$$

$$H|01\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle$$

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y \in \{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle ,$$

where $x^\top y := \sum_{i \leq n} x[i]y[i]$ is the classical inner product.

Example:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle .$$

$$H|01\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle$$

# Quantum gate example: Hadamard gate

For $|x\rangle \in \mathcal{B}_n$,

$$H|x\rangle := \sum_{y \in \{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle,$$

where $x^\top y := \sum_{i \leq n} x[i]y[i]$ is the classical inner product.

Example:

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

$$H|01\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle.$$

# Quantum gate example: Hadamard gate

$$H\left|x\right\rangle := \sum_{y\in\{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}}\left|y\right\rangle,$$

In particular,

$$H\left|00\ldots0\right\rangle =$$

# Quantum gate example: Hadamard gate

$$H\left|x\right\rangle := \sum_{y\in\{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}}\left|y\right\rangle,$$

In particular,

$$H\left|00\dots0\right\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\left|y\right\rangle =: \left|?\right\rangle.$$

# Quantum gate example: Hadamard gate

In general, for any qubit array $|\psi\rangle = \sum_x a_x |x\rangle$,

$$H|\psi\rangle = H\left(\sum_x a_x |x\rangle\right)$$

# Quantum gate example: Hadamard gate

In general, for any qubit array $|\psi\rangle = \sum_x a_x |x\rangle$,

$$
\begin{aligned}
H|\psi\rangle &= H\left(\sum_x a_x |x\rangle\right) \\
&= \sum_x a_x H|x\rangle \\
&= \sum_{x,y} \frac{a_x (-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle \\
&= \sum_y \left(\sum_x \frac{a_x (-1)^{x^\top y}}{\sqrt{2^n}}\right) |y\rangle .
\end{aligned}
$$

Applying the Hadamard gate takes *constant* time! It is not that the gate computes $H|x\rangle$, for each $x$! Remember that all bit arrays $x$ are in **superposition**!

# Quantum gate example: Emulation gate

If $f : \{0,1\}^n \to \{0,1\}$ is a Boolean circuit, then

$$U_f |x\rangle := (-1)^{f(x)} |x\rangle .$$

# Quantum gate example: Emulation gate

If $f : \{0,1\}^n \to \{0,1\}$ is a Boolean circuit, then

$$U_f \left|x\right\rangle := (-1)^{f(x)} \left|x\right\rangle.$$

In general, for any qubit array $|\psi\rangle$,

$$U_f \left|\psi\right\rangle = U_f \left( \sum_x a_x \left|x\right\rangle \right) = \sum_x a_x (-1)^{f(x)} \left|x\right\rangle.$$

# Quantum gate example: Emulation gate

If $f : \{0,1\}^n \to \{0,1\}$ is a Boolean circuit, then

$$U_f |x\rangle := (-1)^{f(x)} |x\rangle .$$

In general, for any qubit array $|\psi\rangle$,

$$U_f |\psi\rangle = U_f \left( \sum_x a_x |x\rangle \right) = \sum_x a_x (-1)^{f(x)} |x\rangle .$$

If computing $f(x)$ takes $O(K)$-time, then computing $U_f |\psi\rangle$ also takes $O(K)$-time.

# Quantum gate example: Reflection gate

$$F|x\rangle \begin{cases} |00\ldots 0\rangle & \text{if } x = 00\ldots 0 \text{ and} \\ -|x\rangle & \text{otherwise.} \end{cases}$$

# Classical vs parallel vs quantum computation

$f : \{0,1\}^n \to \{0,1\}$. Suppose that computing $f(x)$ takes $O(K(n))$-time.

# Classical vs parallel vs quantum computation

$f : \{0,1\}^n \to \{0,1\}$. Suppose that computing $f(x)$ takes $O(K(n))$-time. How much you need to compute $f$'s table?

# Classical vs parallel vs quantum computation

$f : \{0,1\}^n \to \{0,1\}$. Suppose that computing $f(x)$ takes $O(K(n))$-time.
How much you need to compute $f$'s table?

| | Memory | Time | Energy |
|---|---|---|---|
| Classical | $O(2^n)$ | $O(2^n K(n))$ | $O(2^n K(n))$ |

$f : \{0,1\}^n \to \{0,1\}$. Suppose that computing $f(x)$ takes $O(K(n))$-time. How much you need to compute $f$'s table?

| | Memory | Time | Energy |
|---|---|---|---|
| Classical | $O(2^n)$ | $O(2^n K(n))$ | $O(2^n K(n))$ |
| Parallel ($2^n$ cores) | $O(2^n)$ | $O(K(n))$ | $O(2^n K(n))$ |

# Classical vs parallel vs quantum computation

$f : \{0,1\}^n \to \{0,1\}$. Suppose that computing $f(x)$ takes $O(K(n))$-time. How much you need to compute $f$'s table?

| | Memory | Time | Energy |
|---|---|---|---|
| Classical | $O(2^n)$ | $O(2^n K(n))$ | $O(2^n K(n))$ |
| Parallel ($2^n$ cores) | $O(2^n)$ | $O(K(n))$ | $O(2^n K(n))$ |
| Quantum | $O(n)$ | $O(K(n))$ | $O(K(n))$ |

# Classical vs parallel vs quantum computation

$f : \{0,1\}^n \to \{0,1\}$. Suppose that computing $f(x)$ takes $O(K(n))$-time. How much you need to compute $f$'s table?

| | Memory | Time | Energy |
|---|---|---|---|
| Classical | $O(2^n)$ | $O(2^n K(n))$ | $O(2^n K(n))$ |
| Parallel ($2^n$ cores) | $O(2^n)$ | $O(K(n))$ | $O(2^n K(n))$ |
| Quantum | $O(n)$ | $O(K(n))$ | $O(K(n))$ |

* Constants may vary substantially.

# Quantum computing for dummies

Carlos Cotrini

ETH Zürich

*ccarlos@inf.ethz.ch*

September 14, 2019

# The Deutsch-Jozsa algorithm

And now... a problem that can be solved in linear time by a classical computer, but in constant time by a quantum computer!

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

# The Deutsch-Jozsa algorithm

And now... a problem that can be solved in linear time by a classical computer, but in constant time by a quantum computer!

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

## The problem

Given a bit array $f$ of length $2^n$, known to be balanced or constant, decide if it is balanced.

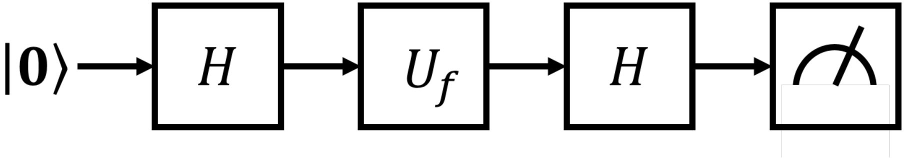
# The Deutsch-Jozsa algorithm

And now... a problem that can be solved in linear time by a classical computer, but in constant time by a quantum computer!

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

**The problem**

Given a bit array $f$ of length $2^n$, known to be balanced or constant, decide if it is balanced.



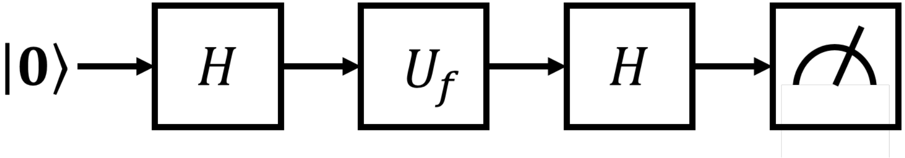
# The Deutsch-Jozsa algorithm

And now... a problem that can be solved in linear time by a classical computer, but in constant time by a quantum computer!

A bit array of length $2^n$ is *balanced* if exactly half of its entries are zero. A bit array is *constant* if all its entries are zero.

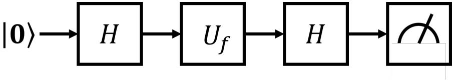
## The problem

Given a bit array $f$ of length $2^n$, known to be balanced or constant, decide if it is balanced.




Executing this circuit requires only **just one** call to $U_f$.

# Exercises




Observe that $|\mathbf{0}\rangle = |00...0\rangle$. Recall that

$$H|x\rangle := \sum_{y\in\{0,1\}^n} \frac{(-1)^{x^\top y}}{\sqrt{2^n}} |y\rangle . \qquad U_f|x\rangle := (-1)^{f(x)}|x\rangle .$$

We now show why this circuit decides if $f$ is balanced or constant.

- Show that

$$|\psi'\rangle = HU_fH|00\dots0\rangle = \sum_{z\in\{0,1\}^n}\left(\sum_{y\in\{0,1\}^n} \frac{(-1)^{z^\top y + f(y)}}{\sqrt{2^n}}\right)|z\rangle .$$

- After we measure $|\psi'\rangle$, what is the probability that we get $00\dots0$ if $f$ is balanced? What is the probability of getting $00\dots0$ if $f$ is constant?

# Agenda

1. Background in linear algebra.
    - Linear transformations.
    - Matrix representations.
    - Unitary transformations.
2. Grover's algorithm.

# Searching with a quantum computer

## The problem

Given a function $f : \{0,1\}^n \to \{0,1\}$, find an element $x \in \{0,1\}^n$ such that $f(x) = 1$. We call such an element *a solution of* $f$.

# Searching with a quantum computer

**The problem**

Given a function $f : \{0,1\}^n \to \{0,1\}$, find an element $x \in \{0,1\}^n$ such that $f(x) = 1$. We call such an element *a solution of* $f$.

A classical computer solves this in $O(2^n)$-time.

# Searching with a quantum computer

**The problem**

Given a function $f : \{0,1\}^n \to \{0,1\}$, find an element $x \in \{0,1\}^n$ such that $f(x) = 1$. We call such an element *a solution of* $f$.

A classical computer solves this in $O(2^n)$-time.
A quantum computer can solve this in $O(\sqrt{2^n})$-time!

# Searching with a quantum computer

## The problem

Given a function $f : \{0,1\}^n \to \{0,1\}$, find an element $x \in \{0,1\}^n$ such that $f(x) = 1$. We call such an element *a solution of* $f$.

A classical computer solves this in $O(2^n)$-time.
A quantum computer can solve this in $O(\sqrt{2^n})$-time!
We assume that there are $M \ll N = 2^n$ solutions of $f$.

# Linear transformations

A *linear transformation* is a function $T : \mathbb{C}^N \rightarrow \mathbb{C}^N$ such that

$$T\left(a_1 \left|\psi_1\right\rangle + a_2 \left|\psi_2\right\rangle\right) = a_1 T \left|\psi_1\right\rangle + a_2 T \left|\psi_2\right\rangle .$$

# Linear transformations

A *linear transformation* is a function $T : \mathbb{C}^N \to \mathbb{C}^N$ such that

$$T\left(a_1 \left|\psi_1\right\rangle + a_2 \left|\psi_2\right\rangle\right) = a_1 T \left|\psi_1\right\rangle + a_2 T \left|\psi_2\right\rangle .$$

Every linear transformation $T$ is identified with a unique matrix $[\![T]\!] \in \mathbb{C}^{N \times N}$ such that $T \left|\psi\right\rangle = [\![T]\!] \left|\psi\right\rangle$. We identify $T$ with $[\![T]\!]$.

# How to compute the matrix representation of a linear transformation $T$?

1. List all basic qubit arrays: $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$.

# How to compute the matrix representation of a linear transformation $T$?

1. List all basic qubit arrays: $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$.
2. Apply $T$ to each of them: $T|00\ldots0\rangle, T|00\ldots1\rangle, \ldots, T|11\ldots1\rangle$.

# How to compute the matrix representation of a linear transformation $T$?

1. List all basic qubit arrays: $|00\dots0\rangle, |00\dots1\rangle, \dots, |11\dots1\rangle$.
2. Apply $T$ to each of them: $T|00\dots0\rangle, T|00\dots1\rangle, \dots, T|11\dots1\rangle$.
3. Write these qubit arrays as column vectors.

# How to compute the matrix representation of a linear transformation $T$?

1. List all basic qubit arrays: $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$.
2. Apply $T$ to each of them: $T|00\ldots0\rangle, T|00\ldots1\rangle, \ldots, T|11\ldots1\rangle$.
3. Write these qubit arrays as column vectors.
4. $[\![T]\!]$ is the matrix whose columns are the vectors above.

# Examples

Let $T$ be such that $T|0\rangle = -|1\rangle$ and $T|1\rangle = |0\rangle$. If we apply the steps above we get:

1. List all basic qubit arrays: $|0\rangle$, $|1\rangle$.

# Examples

Let $T$ be such that $T|0\rangle = -|1\rangle$ and $T|1\rangle = |0\rangle$. If we apply the steps above we get:

1. List all basic qubit arrays: $|0\rangle$, $|1\rangle$.
2. If we apply $T$ to these arrays we get: $-|1\rangle$, $|0\rangle$.

# Examples

Let $T$ be such that $T|0\rangle = -|1\rangle$ and $T|1\rangle = |0\rangle$. If we apply the steps above we get:

1. List all basic qubit arrays: $|0\rangle$, $|1\rangle$.
2. If we apply $T$ to these arrays we get: $-|1\rangle$, $|0\rangle$.
3. Writing them as column vectors yields: $\begin{pmatrix} 0 \\ -1 \end{pmatrix}$ $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
4. Hence,

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

# Multiplication of a matrix and a vector

Recall that $T\left|0\right\rangle = -\left|1\right\rangle$ and $T\left|1\right\rangle = \left|0\right\rangle$.

# Multiplication of a matrix and a vector

Recall that $T|0\rangle = -|1\rangle$ and $T|1\rangle = |0\rangle$.
Let $|\psi\rangle = a_0|0\rangle + a_1|1\rangle = (a_0, a_1)$. Let's verify that

$$T|\psi\rangle = [\![T]\!]|\psi\rangle .$$

# Multiplication of a matrix and a vector

Recall that $T\left|0\right\rangle = -\left|1\right\rangle$ and $T\left|1\right\rangle = \left|0\right\rangle$.
Let $\left|\psi\right\rangle = a_0\left|0\right\rangle + a_1\left|1\right\rangle = (a_0, a_1)$. Let's verify that

$$T\left|\psi\right\rangle = [\![T]\!]\left|\psi\right\rangle.$$

- $T\left|\psi\right\rangle = a_0 T\left|0\right\rangle + a_1 T\left|1\right\rangle = -a_0\left|1\right\rangle + a_1\left|0\right\rangle = (a_1, -a_0)$.

# Multiplication of a matrix and a vector

Recall that $T|0\rangle = -|1\rangle$ and $T|1\rangle = |0\rangle$.
Let $|\psi\rangle = a_0|0\rangle + a_1|1\rangle = (a_0, a_1)$. Let's verify that

$$T|\psi\rangle = [\![T]\!]|\psi\rangle .$$

- $T|\psi\rangle = a_0 T|0\rangle + a_1 T|1\rangle = -a_0|1\rangle + a_1|0\rangle = (a_1, -a_0)$.
- $[\![T]\!]|\psi\rangle$ can be visualized as follows:

$$\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

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

# Multiplication of a matrix and a vector

Recall that $T\,|0\rangle = -\,|1\rangle$ and $T\,|1\rangle = |0\rangle$.
Let $|\psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle = (a_0, a_1)$. Let's verify that

$$T\,|\psi\rangle = [\![T]\!]\,|\psi\rangle\,.$$

- $T\,|\psi\rangle = a_0\,T\,|0\rangle + a_1\,T\,|1\rangle = -a_0\,|1\rangle + a_1\,|0\rangle = (a_1, -a_0)$.
- $[\![T]\!]\,|\psi\rangle$ can be visualized as follows:

$$\begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{pmatrix} a_1 \\ -a_0 \end{pmatrix}$$

# Multiplication of a matrix and a vector

Recall that $T|0\rangle = -|1\rangle$ and $T|1\rangle = |0\rangle$.
Let $|\psi\rangle = a_0|0\rangle + a_1|1\rangle = (a_0, a_1)$. Let's verify that

$$T|\psi\rangle = [\![T]\!]\,|\psi\rangle\,.$$

- $T|\psi\rangle = a_0 T|0\rangle + a_1 T|1\rangle = -a_0|1\rangle + a_1|0\rangle = (a_1, -a_0)$.
- $[\![T]\!]\,|\psi\rangle$ can be visualized as follows:

$$\begin{array}{cc} & \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \begin{pmatrix} a_1 \\ -a_0 \end{pmatrix} \end{array}$$

Hence, $[\![T]\!]\,|\psi\rangle = (a_1, -a_0)$.

# Multiplication of a matrix and a vector

Recall that $F : \mathbb{C}^4 \to \mathbb{C}^4$ is the quantum gate such that

$$F\left|x\right\rangle \begin{cases} \left|00\right\rangle & \text{if } \left|x\right\rangle = \left|00\right\rangle \\ -\left|x\right\rangle & \text{otherwise.} \end{cases}$$

# Multiplication of a matrix and a vector

Recall that $F : \mathbb{C}^4 \to \mathbb{C}^4$ is the quantum gate such that

$$F\left|x\right\rangle \begin{cases} \left|00\right\rangle & \text{if } \left|x\right\rangle = \left|00\right\rangle \\ -\left|x\right\rangle & \text{otherwise.} \end{cases}$$

$F$'s matrix representation is

# Multiplication of a matrix and a vector

Recall that $F : \mathbb{C}^4 \to \mathbb{C}^4$ is the quantum gate such that

$$F \left|x\right\rangle \begin{cases} \left|00\right\rangle & \text{if } \left|x\right\rangle = \left|00\right\rangle \\ -\left|x\right\rangle & \text{otherwise.} \end{cases}$$

$F$'s matrix representation is

1. $\left|00\right\rangle$, $\left|01\right\rangle$, $\left|10\right\rangle$, $\left|11\right\rangle$.

# Multiplication of a matrix and a vector

Recall that $F : \mathbb{C}^4 \to \mathbb{C}^4$ is the quantum gate such that

$$F |x\rangle \begin{cases} |00\rangle & \text{if } |x\rangle = |00\rangle \\ -|x\rangle & \text{otherwise.} \end{cases}$$

$F$'s matrix representation is

1. $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
2. $|00\rangle$, $-|01\rangle$, $-|10\rangle$, $-|11\rangle$.

# Multiplication of a matrix and a vector

Recall that $F : \mathbb{C}^4 \to \mathbb{C}^4$ is the quantum gate such that

$$F|x\rangle \begin{cases} |00\rangle & \text{if } |x\rangle = |00\rangle \\ -|x\rangle & \text{otherwise.} \end{cases}$$

$F$'s matrix representation is

1. $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
2. $|00\rangle$, $-|01\rangle$, $-|10\rangle$, $-|11\rangle$.
3. $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$

# Multiplication of a matrix and a vector

Recall that $F : \mathbb{C}^4 \to \mathbb{C}^4$ is the quantum gate such that

$$F\,|x\rangle \begin{cases} |00\rangle & \text{if } |x\rangle = |00\rangle \\ -\,|x\rangle & \text{otherwise.} \end{cases}$$

$F$'s matrix representation is

1. $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
2. $|00\rangle$, $-\,|01\rangle$, $-\,|10\rangle$, $-\,|11\rangle$.
3. $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$
4. $F$'s matrix representation is then

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

# Multiplication of a matrix and a vector

In consequence, $F\left|\psi\right\rangle$ for any qubit array $(a_{00}, a_{01}, a_{10}, a_{11})$ is

# Multiplication of a matrix and a vector

In consequence, $F\,|\psi\rangle$ for any qubit array $(a_{00}, a_{01}, a_{10}, a_{11})$ is

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

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

# Multiplication of a matrix and a vector

In consequence, $F|\psi\rangle$ for any qubit array $(a_{00}, a_{01}, a_{10}, a_{11})$ is

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} a_{00} \\ -a_{01} \\ -a_{10} \\ -a_{11} \end{pmatrix}$$

# Multiplication of a matrix and a vector

In consequence, $F|\psi\rangle$ for any qubit array $(a_{00}, a_{01}, a_{10}, a_{11})$ is

$$\begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \begin{pmatrix} a_{00} \\ -a_{01} \\ -a_{10} \\ -a_{11} \end{pmatrix}$$

That is, $F|\psi\rangle = (a_{00}, -a_{01}, -a_{10}, -a_{11})$.

# Composing linear transformations

If $T_1$ and $T_2$ are linear transformations, then

$$T_1\left(T_2 \left|x\right\rangle\right) = [\![T_1]\!][\![T_2]\!] \left|x\right\rangle .$$

# Example

Let $H$ be the Hadamard gate for $\mathbb{C}^2$. Recall that $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and that $H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

# Example

Let $H$ be the Hadamard gate for $\mathbb{C}^2$. Recall that $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and that $H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.
Hence,

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

# What happens if we apply the Hadamard gate twice?

$HH$ is equal to

# What happens if we apply the Hadamard gate twice?

*HH* is equal to

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

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

# What happens if we apply the Hadamard gate twice?

$HH$ is equal to

$$\begin{array}{cc} & \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \\ \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array}$$

# What happens if we apply the Hadamard gate twice?

*HH* is equal to

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

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

This means that $HH = I$. That is, $HH \left|\psi\right\rangle = \left|\psi\right\rangle$.

# Unitary transformations

A quantum gate $G$ is a unitary transformation. A linear transformation $G : \mathbb{C}^N \to \mathbb{C}^N$ is *unitary* if $G^\dagger G = I$.

# Unitary transformations

A quantum gate $G$ is a unitary transformation. A linear transformation $G : \mathbb{C}^N \to \mathbb{C}^N$ is *unitary* if $G^\dagger G = I$.

If you are not familiar with complex algebra, then you can think of $G^\dagger$ as $G^\top$, $G$'s transpose.

# Unitary transformations

A quantum gate $G$ is a unitary transformation. A linear transformation $G : \mathbb{C}^N \to \mathbb{C}^N$ is *unitary* if $G^\dagger G = I$.

If you are not familiar with complex algebra, then you can think of $G^\dagger$ as $G^\top$, $G$'s transpose.

Recall that the transpose of a matrix $G \in \mathbb{C}^{M\times N}$ is the matrix $G^\top \in \mathbb{C}^{N\times M}$ obtained by "mirroring" $G$ through its diagonal. More precisely, for $i \leq M, j \leq N$, we have that $\left(G^\top\right)_{ij} = G_{ji}$.

# Unitary transformations

A quantum gate $G$ is a unitary transformation. A linear transformation $G : \mathbb{C}^N \to \mathbb{C}^N$ is *unitary* if $G^\dagger G = I$.

If you are not familiar with complex algebra, then you can think of $G^\dagger$ as $G^\top$, $G$'s transpose.

Recall that the transpose of a matrix $G \in \mathbb{C}^{M \times N}$ is the matrix $G^\top \in \mathbb{C}^{N \times M}$ obtained by "mirroring" $G$ through its diagonal. More precisely, for $i \leq M, j \leq N$, we have that $\left(G^\top\right)_{ij} = G_{ji}$.

For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^\top = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}.$$

# Grover's algorithm

## The problem

Given a function $f : \{0,1\}^n \to \{0,1\}$, find an element $x \in \{0,1\}^n$ such that $f(x) = 1$. We call such an element *a solution of* $f$.

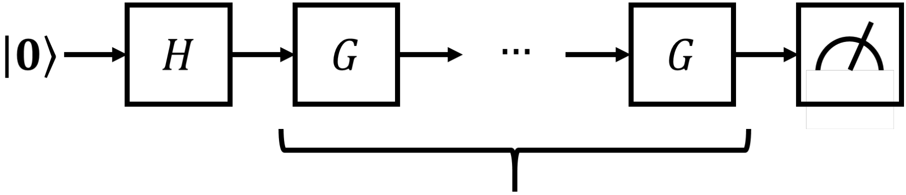
# Grover's algorithm

## The problem

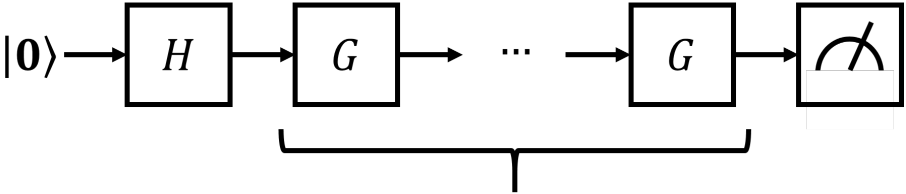
Given a function $f : \{0,1\}^n \to \{0,1\}$, find an element $x \in \{0,1\}^n$ such that $f(x) = 1$. We call such an element *a solution of* $f$.

We assume that there are $M \ll N = 2^n$ solutions of $f$.

# Quantum circuit

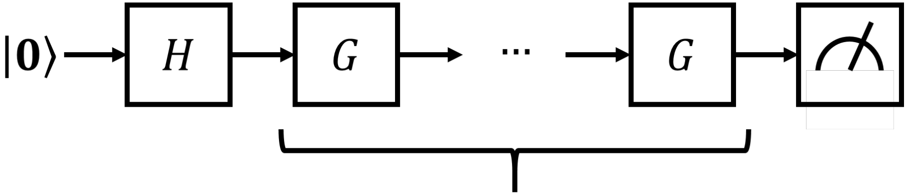



$$\approx \left\lfloor \pi \left(4 \arcsin \sqrt{N/M}\right)^{-1} \right\rfloor \approx O(\sqrt{N})$$




$$\approx \left\lfloor \pi\left(4 \arcsin \sqrt{N/M}\right)^{-1} \right\rfloor \approx O(\sqrt{N})$$

Let $|\sigma\rangle := \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$ and $|\sigma^{\perp}\rangle := \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$.

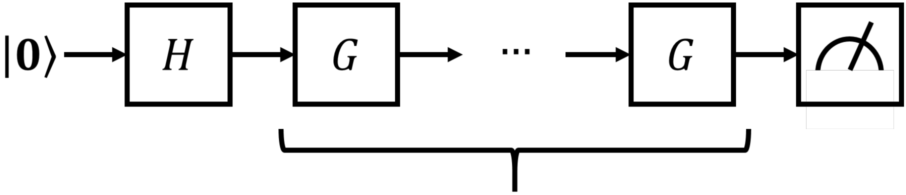



$$\approx \left\lfloor \pi\left(4 \arcsin \sqrt{N/M}\right)^{-1} \right\rfloor \approx O(\sqrt{N})$$

Let $|\sigma\rangle := \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$ and $|\sigma^{\perp}\rangle := \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$.

$|\sigma\rangle$ and $|\sigma^{\perp}\rangle$ are normal and orthogonal.

# Quantum circuit



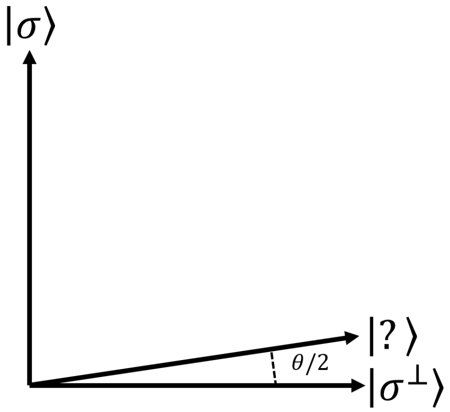

$$\approx \left\lfloor \pi \left( 4 \arcsin \sqrt{N/M} \right)^{-1} \right\rfloor \approx O(\sqrt{N})$$

Let $|\sigma\rangle := \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$ and $|\sigma^{\perp}\rangle := \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$.

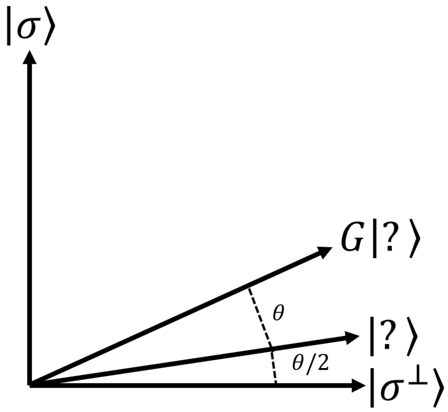
$|\sigma\rangle$ and $|\sigma^{\perp}\rangle$ are normal and orthogonal.

$|?\rangle$ lies in the span of these two vectors.

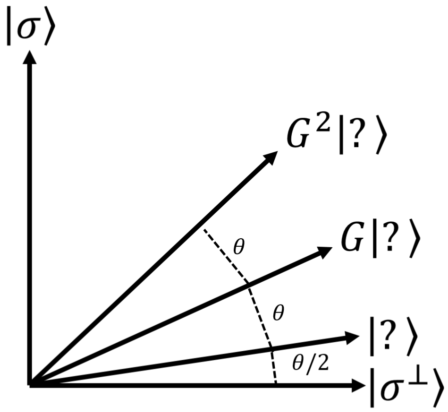
# Grover's rotation illustrated



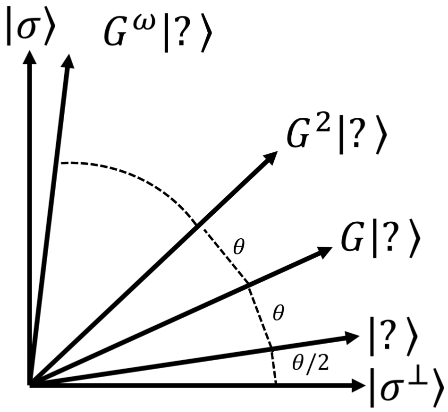
# Grover's rotation illustrated



# Grover's rotation illustrated



# Grover's rotation illustrated



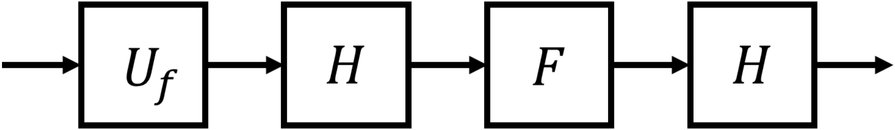



Figure: Quantum circuit for Grover's rotation.

# Putting all together

1. The Grover rotation is implemented as $G \equiv U_f \to H \to F \to H$.
   1. Show that $F$'s matrix representation is $2\,|00\ldots0\rangle\,|00\ldots0\rangle^\top - I$.
   2. Show that $H^\top = H$.
   3. Show that the matrix representation of $HFH$ is $2\,|?\rangle\,|?\rangle^\top - I$.
   4. Show that $U_f$ is a reflection through the qubit array $\left|\sigma^\perp\right\rangle$. Recall that a linear transformation is a reflection through a vector $v$ if its matrix representation is $2vv^\top - I$.
   5. Conclude that $G$ performs a rotation. It can be shown that this rotation is done by an angle of $\theta = 2\arcsin\sqrt{M/N}$ towards $|\sigma\rangle$.
2. Write down the circuit implementing Grover's algorithm and argue why it computes a solution of $f$ with high probability.