Quantum Computation: circuits and simple algorithms

Raimondas Čiegis

Department of Mathematical Modelling, email: rc@vgtu.lt

September 5, 2026

More restrictions on quantum computations.

Copying an unknown qubit is impossible.

More restrictions on quantum computations.

Copying an unknown qubit is impossible.

Quantum no-cloning theorem. *There does not exist a 2-qubit unitary U that maps*

$$|\phi\rangle\,|0\rangle \to |\phi\rangle\,|\phi\rangle\,.$$

for every qubit $|\phi\rangle$.

Proof. Let's assume that such 2-qubit unitary U exists. Then

$$U: \; |00\rangle \;\to\; |00\rangle\,, \quad |10\rangle \;\to\; |11\rangle\,.$$

Next we consider the qubit $c = \alpha |0\rangle + \beta |1\rangle$. Since U is a linear operator then

$$U: \ |c, 0\rangle \ \rightarrow \ \alpha |00\rangle + \beta |11\rangle .$$

This result is not correct, the correct answer should be

$$U: \ |c, 0\rangle \ \rightarrow \ |c, c\rangle = \alpha^2 |00\rangle + \alpha\beta(|01\rangle + |10\rangle) + \beta^2 |11\rangle .$$

Quantum circuits

A *quantum circuit* generalizes the idea of classical circuits, replacing the *AND*, *OR*, and *NOT* gates by elementary quantum gates.

Quantum circuits

A *quantum circuit* generalizes the idea of classical circuits, replacing the *AND*, *OR*, and *NOT* gates by elementary quantum gates.

As in the classical case, a quantum circuit is a finite directed acyclic graph of input nodes, gates, and output nodes.

There are n nodes that contain the input (exactly as it is for classical bits); in addition we may have some more input nodes that are initially $|0\rangle$ (workspace).

Quantum circuits

A *quantum circuit* generalizes the idea of classical circuits, replacing the *AND*, *OR*, and *NOT* gates by elementary quantum gates.

As in the classical case, a quantum circuit is a finite directed acyclic graph of input nodes, gates, and output nodes.

There are n nodes that contain the input (exactly as it is for classical bits); in addition we may have some more input nodes that are initially $|0\rangle$ (workspace).

Mathematically, elementary quantum gates can be composed into bigger unitary operations by taking tensor products (if gates are applied in parallel to different parts of the register), and ordinary matrix products (if gates are applied sequentially).

Example 1. We want to get the 2-qubits entangled state:

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

The initial state is given by $|A_0\rangle = |00\rangle$.
First apply the Hadamard gate to the first qubit

$$|A_1\rangle = H \otimes I\,|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

then apply $CNOT$ to both qubits, with the first qubit acting as the control

$$|A_2\rangle = CNOT\,|A_1\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

and then Z gate to the last qubit

$$|A\rangle = I \otimes Z\;|A_2\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big).$$

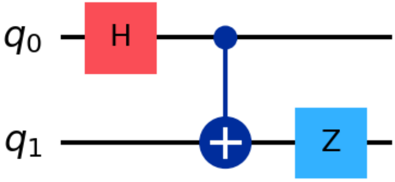

Fig1. Simple circuit for turning $|00\rangle$ into an entangled state

Example 2. Generate a superposition of all states.

Lets assume that we have n qubits, initial states $|0\rangle$.

Then to each qubit apply the H gate (a tensor product of n Hadamard gates)

$$H^{\otimes n} = H \otimes H \otimes \cdots \otimes H,$$

where

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

Example 2. Generate a superposition of all states.

Lets assume that we have n qubits, initial states $|0\rangle$.

Then to each qubit apply the H gate (a tensor product of n Hadamard gates)

$$H^{\otimes n} = H \otimes H \otimes \cdots \otimes H,$$

where

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

If $n = 2$, then the result is

$$\begin{aligned} H^{\otimes 2}\,|00\rangle &= \frac{1}{2}\big(\,|0\rangle + |1\rangle\,\big) \otimes \big(\,|0\rangle + |1\rangle\,\big) \\ &= \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big). \end{aligned}$$

Example 2. Generate a superposition of all states.

Lets assume that we have n qubits, initial states $|0\rangle$.

Then to each qubit apply the H gate (a tensor product of n Hadamard gates)

$$H^{\otimes n} = H \otimes H \otimes \cdots \otimes H,$$

where

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

If $n = 2$, then the result is

$$\begin{aligned} H^{\otimes 2}\,|00\rangle &= \frac{1}{2}\big(\,|0\rangle + |1\rangle\,\big) \otimes \big(\,|0\rangle + |1\rangle\,\big) \\ &= \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big). \end{aligned}$$

General case:

$$H^{\otimes n}\,|00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} |j\rangle\,.$$

Example 3. Quantum teleportation.

Suppose there are two parties, Alice and Bob.
Alice has a qubit $|A\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ that she wants to send to Bob via a classical channel.
Alice herself does not know the values of the coefficients α_0, α_1.
Let's remember that qubits cannot be copied.

Example 3. Quantum teleportation.

Suppose there are two parties, Alice and Bob.
Alice has a qubit $|A\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ that she wants to send to Bob via a classical channel.
Alice herself does not know the values of the coefficients α_0, α_1.
Let's remember that qubits cannot be copied.

Alice also shares an EPR-pair

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

with Bob.

Initially, their joint state is

$$|A\rangle \otimes |\psi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle \big).$$

The first two qubits belong to Alice, the third to Bob.

After that, they move to stay in different cities (or may be even different planets).

Initially, their joint state is

$$|A\rangle \otimes |\psi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle \big).$$

The first two qubits belong to Alice, the third to Bob.

After that, they move to stay in different cities (or may be even different planets).

First, Alice performs a *CNOT* on her two qubits and then a Hadamard transform on her first qubit:

$$|\psi_1\rangle :=$$

$$CNOT \otimes I \; |A\rangle \otimes |\psi\rangle = \frac{1}{\sqrt{2}}\big(\alpha_0 |000\rangle + \alpha_0 |011\rangle + \alpha_1 |110\rangle + \alpha_1 |101\rangle \big),$$

$$\begin{aligned} H \otimes I \otimes I \; |\psi_1\rangle = & \frac{1}{2}\big(\alpha_0 |000\rangle + \alpha_0 |100\rangle + \alpha_0 |011\rangle + \alpha_0 |111\rangle \\ & + \alpha_1 |010\rangle - \alpha_1 |110\rangle + \alpha_1 |001\rangle - \alpha_1 |101\rangle \big) = |\psi_2\rangle \,. \end{aligned}$$

Their joint 3-qubit state can be written as

$$
\begin{aligned}
|\psi_2\rangle = & \frac{1}{2}\Big(|00\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle\,) + |01\rangle \otimes (\alpha_0 |1\rangle + \alpha_1 |0\rangle\,) \\
& + |10\rangle \otimes (\alpha_0 |0\rangle - \alpha_1 |1\rangle\,) + |11\rangle \otimes (\alpha_0 |1\rangle - \alpha_1 |0\rangle\,)\Big).
\end{aligned}
$$

Now we are ready for teleportation! Alice's two qubits are in a superposition of four possible computational basis states.

Their joint 3-qubit state can be written as

$$
\begin{aligned}
|\psi_2\rangle = & \frac{1}{2}\Big(|00\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) + |01\rangle \otimes (\alpha_0 |1\rangle + \alpha_1 |0\rangle) \\
& + |10\rangle \otimes (\alpha_0 |0\rangle - \alpha_1 |1\rangle) + |11\rangle \otimes (\alpha_0 |1\rangle - \alpha_1 |0\rangle) \Big).
\end{aligned}
$$

Now we are ready for teleportation! Alice's two qubits are in a superposition of four possible computational basis states.

Alice then measures her two qubits in the computational basis and gets one result $0, 1, 2$ or 3 with an equal probability.

When Alice makes a measurement, the state of Bob's qubit also changes, the qubit is projected into a state corresponding to the Alice's measurement result.

Teleportation has occurred!

When Alice makes a measurement, the state of Bob's qubit also changes, the qubit is projected into a state corresponding to the Alice's measurement result.

Teleportation has occurred!

Then Alice sends the result (2 random classical bits a and b) to Bob over a classical channel.

Bob now knows which transformation he must do on his qubit in order to regain the qubit $\alpha_0 |0\rangle + \alpha_1 |1\rangle$.

If $b = 1$ then he applies X gate on his qubit.

If $a = 1$ then he applies Z gate on his qubit.

For instance, if Alice sent $ab = 11$, then Bob knows that his qubit is $\alpha_0 |1\rangle + \alpha_1 |0\rangle$. A X gate followed by a Z will give him Alice's original qubit.

Note that the qubit on Alice's side has been destroyed: teleporting moves a qubit from Alice to Bob, rather than copying it.

In fact, we know that copying an unknown qubit is impossible.

Quantum circuits to compute values of function

Suppose we have a classical algorithm that computes some function

$$f : \{0,1\}^n \to \{0,1\}^m$$

We want to build a quantum circuit U that maps

$$|z\rangle\,|0\rangle \to |z\rangle\,|f(z)\rangle \quad \forall z \in \{0,1\}^n.$$

Quantum circuits to compute values of function

Suppose we have a classical algorithm that computes some function

$$f : \{0,1\}^n \to \{0,1\}^m$$

We want to build a quantum circuit U that maps

$$|z\rangle\,|0\rangle \to |z\rangle\,|f(z)\rangle \quad \forall z \in \{0,1\}^n.$$

Let's consider 2-qubits operator

$$|x, y\rangle \to |x, y \oplus f(x)\rangle\,,$$

where $\oplus$ denotes exclusive-OR (addition modulo 2).

Then we get an unitary operator

$$U_f : \quad |x, 0\rangle \ \rightarrow \ |x, f(x)\rangle \, .$$

In general case

$$U_f : \quad |x, y\rangle \ \rightarrow \ |x, y \oplus f(x)\rangle \, ,$$

where x is a set of n qubits, and y is set of m qubits.

The property

$$U_f U_f = I,$$

is valid, since $f(x) \oplus f(x) = 0$ (show it).

Now we will test that for Boolean function f_1

$$f_1: \quad 0 \to 0, \qquad 1 \to 0,$$

the operator U_{f_1} is symmetric and unitary.

$$U_{f_1}: \quad |0,0\rangle \to |0,0\rangle, \quad |0,1\rangle \to |0,1\rangle, \quad |1,0\rangle \to |1,0\rangle, \quad |1,1\rangle \to |1,1\rangle,$$

The matrix of this operator:

$$U_{f_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$U_{f_1} = I \otimes I.$$

Exercises.

Find matrix forms of unitary operators of these Boolean functions

$$f_2: \quad \begin{aligned} 0 &\to 1, \\ 1 &\to 0, \end{aligned} \qquad f_3: \quad \begin{aligned} 0 &\to 0, \\ 1 &\to 1, \end{aligned}$$

$$f_4: \quad \begin{aligned} 0 &\to 1, \\ 1 &\to 1, \end{aligned}$$

Test the unitarity of operators.

Consider Boolean function f. We have only a black-box – a code applet to compute the value of $f(x)$.

Our aim is to calculate the value of

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

The classical solver computes two values of function f and finally both values are added.

Deutsch problem

Consider Boolean function f. We have only a black-box – a code applet to compute the value of $f(x)$.

Our aim is to calculate the value of

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

The classical solver computes two values of function f and finally both values are added.

We will see that for the quantum algorithm it is sufficient to apply the quantum function f only once.

Take a 2-qubits vector

$$|\psi_0\rangle = |01\rangle \,.$$

For both qubits apply the Hadamard gates

$$H \otimes H \; |\psi_0\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) := |\psi_1\rangle \,.$$

A quantum unitary operator U_f of function f is defined as

$$U_f : \quad |xy\rangle \quad \to \quad |x, y \oplus f(x)\rangle \,.$$

$$\begin{aligned} U_f : \quad |x\,0\rangle \quad &\to \quad |x, f(x)\rangle \,, \\ U_f : \quad |x\,1\rangle \quad &\to \quad |x, f(x)^*\rangle \,. \end{aligned}$$

Then we get

$$U_f: \quad |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \to \quad |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad \text{if } f(x) = 0,$$
$$U_f: \quad |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \to \quad |x\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}}, \quad \text{if } f(x) = 1.$$

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

Let's compute $|\psi_2\rangle = U_f |\psi_1\rangle$.

We remind that

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right),$$

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

We remind that

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right),$$

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

Then it follows:

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

Now for the first qubit we apply Hadamard gate H

$$|\psi_3\rangle = H \otimes I \, |\psi_2\rangle$$

then

$$|\psi_3\rangle = \begin{cases} \pm\,|0\rangle \otimes \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{if } \; f(0) = f(1), \\ \pm\,|1\rangle \otimes \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}, & \text{if } \; f(0) \neq f(1) \end{cases} .$$

Let's measure the value of the first qubit, then we get

$$\begin{aligned} \pm\,|0\rangle \;&\rightarrow\; f(0) = f(1) \;\rightarrow\; f(0) \oplus f(1) = 0, \\ \pm\,|1\rangle \;&\rightarrow\; f(0) \neq f(1) \;\rightarrow\; f(0) \oplus f(1) = 1. \end{aligned}$$

Now we explain the definition of the query $Q_{x,\pm}$, which is used in many quantum algorithms including the Deutsch-Jozsa algorithm.

(1) The quantum operation O_x defines a memory access which outputs the bit x_i for input n-bit index i:

$$O_x : \; |i, 0\rangle \to |i, x_i\rangle \, .$$

In order to get the unitary transformation we actually let

$$O_{x,b} : \; |i, b\rangle \to |i, b \oplus x_i\rangle \, .$$

Now we explain the definition of the query $Q_{x,\pm}$, which is used in many quantum algorithms including the Deutsch-Jozsa algorithm.

(1) The quantum operation O_x defines a memory access which outputs the bit x_i for input n-bit index i:

$$O_x : \ |i, 0\rangle \to |i, x_i\rangle \ .$$

In order to get the unitary transformation we actually let

$$O_{x,b} : \ |i, b\rangle \to |i, b \oplus x_i\rangle \ .$$

(2) Given the ability to make a query of the above type, we can also make a new query of the form

$$|i\rangle \to (-1)^{x_i} |i\rangle \ .$$

By setting the target bit to the state

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

we get the required query

$$O_{x,-} = O_x(|i\rangle, |-\rangle) = |i\rangle \frac{1}{\sqrt{2}}\Big(|x_i - (1 - x_i)\rangle \Big)$$
$$= (-1)^{x_i} |i\rangle |-\rangle.$$

Deutsch-Jozsa algorithm

Let's consider a more difficult problem:

For $N = 2^n$, we are given $x \in \{0, 1\}^N$ such that either

(1) all x_i have the same value (constant), or

(2) $N/2$ of the x_i are 0 and $N/2$ are 1 (balanced).

The goal is to find out whether x is constant or balanced.

Deutsch-Jozsa algorithm

Let's consider a more difficult problem:

For $N = 2^n$, we are given $x \in \{0,1\}^N$ such that either

(1) all x_i have the same value (constant), or

(2) $N/2$ of the x_i are 0 and $N/2$ are 1 (balanced).

The goal is to find out whether x is constant or balanced.

It is easy to see that any classical deterministic algorithm needs at least $N/2 + 1$ queries: if it has made only $N/2$ queries and seen only 0s, the correct output is still undetermined.

The algorithm of Deutsch and Jozsa is as follows.

(1) We start in the n-qubit zero state $|0^n\rangle$,

(2) Apply a Hadamard transform to each qubit,

(3) Apply a query $Q_{x,\pm}$,

(4) Apply another Hadamard transform to each qubit,

(5) and then Measure the final state.

The algorithm of Deutsch and Jozsa is as follows.

(1) We start in the n-qubit zero state $|0^n\rangle$,

(2) Apply a Hadamard transform to each qubit,

(3) Apply a query $Q_{x,\pm}$,

(4) Apply another Hadamard transform to each qubit,

(5) and then Measure the final state.

As a unitary transformation, the algorithm can be written as

$$H^{\otimes n} \, O_{x,\pm} \, H^{\otimes n}.$$

Time of the algorithm again progresses from left to right for this formula.

Let us follow the state through these operations.

(1) After the first Hadamard transforms we have obtained the uniform superposition of all i:

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle \, .$$

(2) The $O_{x,\pm}$-query turns this into

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle \, .$$

(3) Applying the second set of Hadamard gates gives the final superposition

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle ,$$

where as before

$$i \cdot j = \sum_{k=1}^{n} i_k j_k .$$

Since $i \cdot 0^n = 0$ for all $i \in \{0,1\}^n$, we see that the amplitude of the $|0^n\rangle$-state in the final superposition is

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} = \begin{cases} 1 & \text{if } \ x_i = 0 \ \ \forall i, \\ -1 & \text{if } \ x_i = 1 \ \ \forall i, \\ 0 & \text{if } \ x \ \text{ balanced.} \end{cases}$$

(4) The final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced.

Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $O(n)$ other operations.

(4) The final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced.

Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $O(n)$ other operations.

Exercises.

1. Is the controlled-NOT operation CX Hermitian?

Determine $(CX)^{-1}$.

2. A SWAP-gate interchanges two qubits: it maps basis state $|a, b\rangle$ to $|b, a\rangle$. Implement a SWAP- gate using a few CX.

When using a CX, you are allowed to use either of the 2 bits as the control, but be explicit about this.