Quantum Computation

Stephan Sigg

Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

TU-Braunschweig, 17.03.2017
1985 David Deutsch: *Can a Quantum Computer efficiently solve problems that have no efficient solution on a classical computer?*
Important results in Quantum Computation

1985  David Deutsch: *Can a Quantum Computer efficiently solve problems that have no efficient solution on a classical computer?*

1994  Peter Shor: *Fast factorization / solution to the discrete logarithm problem*
Important results in Quantum Computation

1985  David Deutsch: *Can a Quantum Computer efficiently solve problems that have no efficient solution on a classical computer?*

1994  Pether Shor: *Fast factorization / solution to the discrete logarithm problem*

1995  Lov Grover: *Quadratic speedup on unstructured search space*
Important results in Quantum Computation

1985  David Deutsch: *Can a Quantum Computer efficiently solve problems that have no efficient solution on a classical computer?*

1994  Pether Shor: *Fast factorization / solution to the discrete logarithm problem*

1995  Lov Grover: *Quadratic speedup on unstructured search space*

1990s  *Quantum Computers can efficiently simulate physical systems that can not be efficiently simulated on classical computers*
Important results in Quantum Computation

1985  David Deutsch: *Can a Quantum Computer efficiently solve problems that have no efficient solution on a classical computer?*

1994  Pether Shor: *Fast factorization / solution to the discrete logarithm problem*

1995  Lov Grover: *Quadratic speedup on unstructured search space*

1990s  Quantum Computers can efficiently simulate physical systems that can not be efficiently simulated on classical computers

2009  Harrow, Hassidim, Lloyd: *Exponential speedup in solving linear equations*
Introduction

Qubits

Quantum Computation

Quantum Algorithms
Quantum Bits

Similar to a classical bit, a qubit can take states $|0\rangle$ or $|1\rangle$. In contrast to classical bits, a qubit can be in a linear combination of states:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.
Quantum Bits

- Similar to a classical bit, a qubit can take states $|0\rangle$ or $|1\rangle$
- In contrast to classical bits, a qubit can be in a linear combination of states:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$\alpha, \beta \in \mathbb{C}$$
Quantum bits

Quantum Bits

- Similar to a classical bit, a qubit can take states $|0\rangle$ or $|1\rangle$.
- In contrast to classical bits, a qubit can be in a linear combination of states:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

where $\alpha, \beta \in \mathbb{C}$, and

$$|\alpha|^2 + |\beta|^2 = 1$$

Bloch-sphere representation of a Qubit

$$|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right)$$
Quantum bits

Quantum Bits

- Similar to a classical bit, a qubit can take states $|0\rangle$ or $|1\rangle$
- In contrast to classical bits, a qubit can be in a linear combination of states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$\alpha, \beta \in \mathbb{C}$

$$|\alpha|^2 + |\beta|^2 = 1$$

Bloch-sphere representation of a Qubit

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

(Ignore $e^{i\gamma}$ since it has no observable effect)
Quantum bits

Measurement of qubits

- Infinite number of possible states for a single qubit.

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ |\alpha|^2 \]

\[ |\beta|^2 \]
Quantum bits

Measurement of qubits

- Infinite number of possible states for a single qubit.
- However, measurement of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ yields

  0  with probability $|\alpha|^2$

  1  with probability $|\beta|^2$
Multiple qubits

- Systems of multiple qubits are described accordingly:
  - A 2-qubit system has four computational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ with

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$\sum_{i,j \in 0,1} |\alpha_{ij}|^2 = 1$$
Multiple qubits

- Systems of multiple qubits are described accordingly:
  - A 2-qubit system has four computational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ with
    \[
    |\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle
    \]
    \[
    \sum_{i,j=0,1} |\alpha_{ij}|^2 = 1
    \]

Remark A system of $n$ qubits has computational basis states of the form $|x_1 x_2 \ldots x_n\rangle$ and $2^n$ amplitudes. For larger $n$ it becomes increasingly infeasible for a classical system to keep track of all individual amplitudes.
Introduction

Qubits

Quantum Computation

Quantum Algorithms
Quantum NOT-gate

\[ X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \]

\[ X|\psi\rangle = X(\alpha|0\rangle + \beta|1\rangle) \]
\[ = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \]
\[ = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \]
\[ = \beta|0\rangle + \alpha|1\rangle \]
Requirements for quantum gates

Quantum gates need to be

- **linear**
  
  *(Violation of this rule would lead to paradoxes such as time travel and faster-than-light travel)*

- **Unitary** \( (U^\dagger U = I) \)
  
  *(In order to guarantee \( |\alpha|^2 + |\beta|^2 = 1 \) also after applying the transformation)*
Quantum Computation

Single qubit gates

Requirements for quantum gates

Quantum gates need to be

- **linear**
  
  *(Violation of this rule would lead to paradoxes such as time travel and faster-than-light travel)*

- **Unitary** *(U†U = I)*
  
  *(In order to guarantee |α|^2 + |β|^2 = 1 also after applying the transformation)*

- Impossible: Copy qubits
Quantum Computation

Single qubit gates

The Hadamard-gate

\[ H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \]

The H-gate turns a \( |0\rangle \) and \( |1\rangle \) halfway between \( |0\rangle \) and \( |1\rangle \):

\[ H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad ; \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \]
Quantum Computation

Decomposing single qubit operations

\[ U = e^{i\alpha} \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix} \]
Quantum Computation

Decomposing single qubit operations

Any Classical circuit can be simulated with qubit gates
Quantum Computation
Multiple qubit gates

Controlled-NOT (CNOT)
Flip second qubit IFF control qubit is $|1\rangle$:

$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

$U_{CN} = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{bmatrix}$
Quantum Computation

Bell states

<table>
<thead>
<tr>
<th>In</th>
<th>Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>00\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>01\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>10\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>11\rangle$</td>
</tr>
</tbody>
</table>

Example:

$|00\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{CNOT} \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

EPR states

Hadamard gate to put the top qubit in a superposition

CNOT gate superposition acts as control input to CNOT
Quantum teleportation is a technique for moving quantum states around – even in the absence of a quantum communications channel.
Quantum teleportation

Quantum teleportation is a technique for moving quantum states around – even in the absence of a quantum communications channel.
\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]
\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ |\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle \]

\[ = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)] \]
\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ |\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle \]

\[ = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)] \]

\[ |\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)] \]
\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]

\[ |\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle \]
\[ = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)] \]

\[ |\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)] \]

\[ |\psi_2\rangle = \frac{1}{2} [\alpha (|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta (|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \]
\[ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \]

\[ |\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle \]

\[ = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)] \]

\[ |\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)] \]

\[ |\psi_2\rangle = \frac{1}{2} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \]

\[ = \frac{1}{2} [|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \]

\[ + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)] \]
Introduction

Qubits

Quantum Computation

Quantum Algorithms
Quantum algorithms

Quantum parallelism

Evaluating a function for multiple inputs simultaneously

- $f(x) : \{0, 1\} \rightarrow \{0, 1\}$
- $\oplus$: addition modulo 2
Quantum algorithms

Quantum parallelism

Evaluating a function for multiple inputs simultaneously

- $f(x) : \{0, 1\} \rightarrow \{0, 1\}$
- $\oplus$: addition modulo 2

Applying $U_f$ results in

\[ |0, f(0)\rangle + |1, f(1)\rangle \]
\[ \frac{\sqrt{2}}{} \]
Quantum algorithms

Deutsch’s algorithm

\[ |0\rangle \quad H \quad x \quad x \quad H \]

\[ |1\rangle \quad H \quad y \quad y \oplus f(x) \quad H \]

\[ |\psi_0\rangle \quad \uparrow \quad |\psi_1\rangle \quad \uparrow \quad \uparrow \quad \uparrow \quad |\psi_2\rangle \quad |\psi_3\rangle \]
Quantum algorithms

Deutsch’s algorithm

\[ |\psi_0\rangle = |01\rangle \]
Quantum algorithms

Deutsch’s algorithm

\[ |\psi_0\rangle = |01\rangle \]

\[ |\psi_1\rangle = \left[ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \]
Quantum algorithms

Deutsch’s algorithm

If we apply $U_f$ to $\frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle)$ we obtain $(-1)^{f(x)} \frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle)$

$\psi_0 \rangle = |01\rangle$

$\psi_1 \rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

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

Deutsch’s algorithm

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

- $|\psi_1\rangle = \left[ \frac{|0\rangle+|1\rangle}{\sqrt{2}} \right] \left[ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right]$

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

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

Deutsch’s algorithm

\[ |\psi_0\rangle = |01\rangle \]

\[ |\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \]

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

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

\[ = \pm |f(0) \oplus f(1)\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \]

Since

\[ f(0) \oplus f(1) = 0 \]

IFF \( f(0) = f(1) \)
Quantum algorithms

Deutsch’s algorithm

\[ |\psi_0\rangle = |01\rangle \]

\[ |\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \]

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

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

\[ = \pm |f(0) \oplus f(1)\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \]

Measuring the first qubit determines a global property with just a single evaluation of \( f(x) \)
Quantum algorithms – outlook

Deutsch-Jozsa algorithm
Introduction

Qubits

Quantum Computation

Quantum Algorithms
Thank you!

Stephan Sigg
stephan.sigg@aalto.fi
Literature

Further reading

- Childs, van Dam: Quantum algorithms for algebraic problems, Rev. Mod. Phys. 82, 2010
- D. Bacon, W. van Dam: Recent progress in quantum algorithms, Commun. ACM 53, 84-93, 2010
Links

Quantum Algorithm Zoo  http://math.nist.gov/quantum/zoo/
Quantum Computation

Single qubit gates

The Z-gate

\[ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

The Z gate leaves \(|0\rangle\) unchanged and flips \(|1\rangle\) to \(-|1\rangle\)
Quantum Computation

Copying qubits

Is is possible to copy qubits?

- In classical circuits, it is possible to copy bits with the help of a CNOT gate
- Can we use the CNOT qubit gate to copy qubits?

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \]
Quantum Computation
Copying qubits

Is it possible to copy qubits?

- In classical circuits, it is possible to copy bits with the help of a CNOT gate
- Can we use the CNOT qubit gate to copy qubits?
- Try to copy $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$a|00\rangle + b|11\rangle$$
Quantum Computation

Copying qubits

Is it possible to copy qubits?

▶ In classical circuits, it is possible to copy bits with the help of a CNOT gate
▶ Can we use the CNOT qubit gate to copy qubits?

▶ Try to copy $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$:
▶ Did we copy $|\psi\rangle$?

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
Quantum Computation

Copying qubits

Is it possible to copy qubits?

- In classical circuits, it is possible to copy bits with the help of a CNOT gate
- Can we use the CNOT qubit gate to copy qubits?

- Try to copy $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:
- Did we copy $|\psi\rangle$?
- Show equation 1.22

$$|\psi\rangle = a|0\rangle + b|1\rangle$$
Quantum Computation

Copying of qubits

No-cloning theorem

Aim

\[ |\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \]

Assume

\[ U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \]

Contradiction

The inner product of these two equations gives

\[ \langle \psi | \psi \rangle = (\langle \psi | \psi \rangle)^2 \]

is only possible for

\[ x \in \{0, 1\} \]
Quantum Computation

Copying of qubits

No-cloning theorem

Aim  \[ |\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \]

Assume

\[
U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \\
U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle
\]
Quantum Computation

Copying of qubits

No-cloning theorem

Aim  \(|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle\)

Assume

\[ U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \]
\[ U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle \]

Contradiction  The inner product of these two equations gives

\[ \langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2 \]

\[ x = x^2 \text{ is only possible for } x \in \{0, 1\} \]
Quantum algorithms
Classical computations on a quantum computer

Simulation of classical circuits

Any classical circuit can be replaced by an equivalent quantum circuit containing only reversible elements by using Toffoli gates

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>a  b  c</td>
<td>a' b' c'</td>
</tr>
<tr>
<td>0  0  0</td>
<td>0  0  0</td>
</tr>
<tr>
<td>0  0  1</td>
<td>0  0  1</td>
</tr>
<tr>
<td>0  1  0</td>
<td>0  1  0</td>
</tr>
<tr>
<td>0  1  1</td>
<td>0  1  1</td>
</tr>
<tr>
<td>1  0  0</td>
<td>1  0  0</td>
</tr>
<tr>
<td>1  0  1</td>
<td>1  0  1</td>
</tr>
<tr>
<td>1  1  0</td>
<td>1  1  1</td>
</tr>
<tr>
<td>1  1  1</td>
<td>1  1  0</td>
</tr>
</tbody>
</table>

\[ a \rightarrow a \]
\[ b \rightarrow b \]
\[ c \rightarrow c \oplus ab \]
Quantum algorithms

Classical computations on a quantum computer

NAND
\[ a \quad \oplus \quad b \quad = \quad \neg(ab) \]

FANOUT
\[ 1 \quad \rightarrow \quad a \]
\[ 0 \quad \rightarrow \quad a \]
Quantum Computation

qubit gates

Restrictions for multiple qubit gates
Most classical gates not directly convertible to qubit gates since they are non-invertible and irreversible (Unitary requirement).
Unitary quantum gates are always invertible

Universality result
Any multiple qubit logic gate may be composed from CNOT and single qubit gates
Quantum algorithms
Deutsch-Jozsa algorithm

\[ |0\rangle \xrightarrow{n} H \otimes n \quad \xrightarrow{x} U_f \quad \xrightarrow{x} H \otimes n \]

\[ |1\rangle \xrightarrow{H} \rightarrow \]

\[ |\psi_0\rangle \quad |\psi_1\rangle \quad |\psi_2\rangle \quad |\psi_3\rangle \]
Quantum algorithms

Deutsch-Jozsa algorithm

$|\psi_0\rangle = |0\rangle \otimes^n |1\rangle$
Quantum algorithms

Deutsch-Jozsa algorithm

\[ |\psi_0\rangle = |0\rangle \otimes^n |1\rangle \]

\[ |\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[ |0\rangle - |1\rangle \right] \]
Quantum algorithms

Deutsch-Jozsa algorithm

\[ |\psi_0\rangle = |0\rangle \otimes^n |1\rangle \]
\[ |\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \]
\[ |\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \]
Quantum algorithms

Deutsch-Jozsa algorithm

\[ |\psi_0\rangle = |0\rangle \otimes^n |1\rangle \]

\[ |\psi_1\rangle = \sum_{x \in \{0,1\}^n} |x\rangle \frac{|x\rangle}{\sqrt{2^n}} \left[ |0\rangle - |1\rangle \right] \]

\[ |\psi_2\rangle = \sum_{x} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[ |0\rangle - |1\rangle \right] \]

\[ |\psi_3\rangle = \sum_{z} \sum_{x} \frac{(-1)^{x \cdot z + f(x)}|z\rangle}{2^n} \left[ |0\rangle - |1\rangle \right] \]