Introduction to Quantum Computing

DeiC Conference 2023, Kolding

November 8, 2023

Torben Larsen, tola@cs.aau.dk

Department of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

Agenda

Presenter/Lecturer

Quantum Background

Theory, Companies, and Applications

Brief Primer on States and Qubits

The Core Quantum Principles

Classical and Quantum Computing

Qubits

Classical Bits and Quantum Qubits

Notation and Properties

Quantum Registers

Qgates

Properties

Pauli-X qgate

Selected qgates

Qcircuits

Literature

Presenter/Lecturer

AALBORG UNIVERSITY
DENMARK

Presenter/Lecturer

Dept. of Computer Science
Aalborg University
Denmark

Presenter/Lecturer

Scientific Background

AALBORG UNIVERSITY
DENMARK

My scientific background:

- Telecom engineering degree from 1988 — 35 years academic experience.
- Dr.Techn. in nonlinear noisy networks and systems from 1998.
- Substantial leadership experience – mainly as associate dean.
- After 12 years in leadership positions, I returned to research/teaching by 1 Nov. 2022.
- Since returning to research/teaching I have had 100% focus on quantum computing.

Presenter/Lecturer
Scientific Background

My scientific background:

- Analog measurements
- Compressed sensing
- Microwave techniques
- HPC
- Algorithms
- Numerical techniques
- Fortran
- Signal processing
- Python
- IC design
- Analog circuits
- Quantum computing
- Numerical computations

Presenter/Lecturer
Prerequisites and Objectives

Introduction to Quantum Computing

Torben Larsen

Presentation . . .

- Prequisites:
  - An introduction to the basics of quantum computing.
  - Minimum math and quantum mechanics prerequisites.

Presenter/Lecturer
Prerequisites and Objectives

Presentation . . .

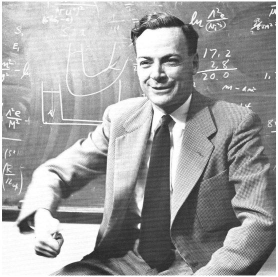
- Prequisites:
  - An introduction to the basics of quantum computing.
  - Minimum math and quantum mechanics prerequisites.
- Objectives:
  - Providing a basic understanding of the key elements in Quantum Computing.
  - Overview of some of the most important vendors of quantum computers and simulators/emulators.
  - Provide examples of places to get low cost access to quantum computers and simulators/emulators.

AALBORG UNIVERSITY
DENMARK

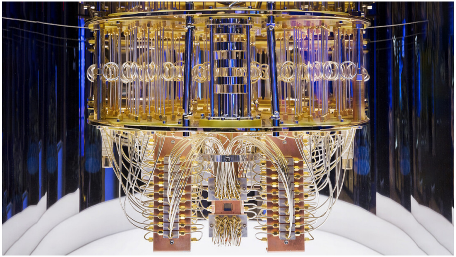
Quantum Background

AALBORG UNIVERSITY
DENMARK

From invention to current implementation:



Feynman, 1958

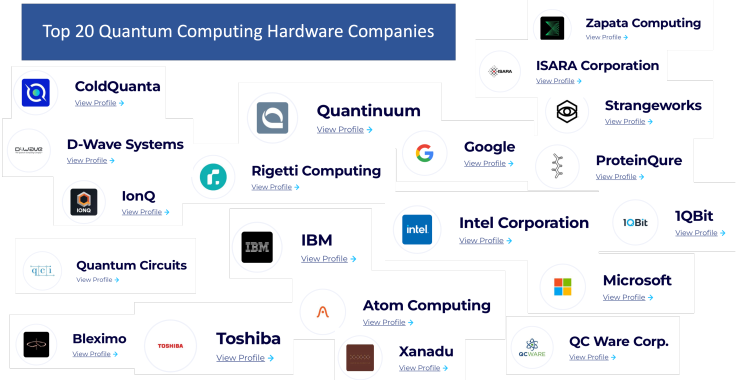


IBM, 2023

Despite the nice looking IBM quantum computer, the area is still highly immature, far from complex and really useful applications → Research area .. but with fast growth, industrial interest, and billions of USD technology advancement is fast.

Quantum Background

Theory, Companies, and Applications



AALBORG UNIVERSITY
DENMARK

- **Vendors of Quantum Computer Systems:**
  - IBM. `https://www.ibm.com/quantum`
  - Quantinuum. `https://www.quantinuum.com`
  - Strangeworks. `https://strangeworks.com`
  - D-Wave Systems. `https://www.dwavesys.com`
  - Rigetti Computing. `https://www.rigetti.com`
  - Oxford Ionics. `https://www.oxionics.com`
  - IonQ. `https://ionq.com`
  - 1QBit. `https://1qbit.com`
  - Algorithmic. `https://algorithmiq.fi`
  - Xanadu. `https://www.xanadu.ai`
  - Intel. `https://www.intel.com/content/www/us/en/research/quantum-computing.html?wapkw=quantum`
  - Google. `https://quantumai.google`
  - Microsoft. `https://azure.microsoft.com/en-us/solutions/quantum-computing/`

Dept. of Computer Science
Aalborg University
Denmark

Application industries:

- Defense sector.
- Encryption and data security.
- Weather prediction and climate models.
- Construction and discovery of new materials and medicine.
- Energy sector.
- Logistics.
- Financial sector.
- AI and Neural networks.
- Digital twins.
- Gaming industry.

Dept. of Computer Science
Aalborg University
Denmark

Quantum Computer State Description:

- The smallest unit of information in Quantum Computing is the Quantum-bit or Qubit.
- A Qubit represents the state of the wavefunction $|\phi\rangle$ in Schrödingers equation at a specific time.
- A single Qubit may be in the “on” state ($|1\rangle$) or it may be in the “off” state ($|0\rangle$) **or any linear combination thereof**.
- Schrödingers equation, which describes how the state of a quantum mechanical system evolves in time, is linear. Hence, linear combinations of solutions are also valid solutions.

Quantum Computer State Description:

- If a qubit has the state $|0\rangle$ and $|1\rangle$, a superposition of these also describe the same state. The general superposition form of the state is:

$$|\psi\rangle = \alpha\,|0\rangle \;+\; \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,\; \alpha, \beta \in \mathbb{C}$$

- The two core states $|0\rangle$ (ground state) and $|1\rangle$ (excited state) are orthonormal[1] in Hilbert space.
- The joined state $|\psi\rangle$ is a superposition of the core states each multiplied by a constant complex number at the given time instant.

[1] Two vectors in a inner product space are orthonomal if they are orthogonal unit vectors.

Dept. of Computer Science
Aalborg University
Denmark

- Quantum Computing uses qubits as the basis unit of information.
- Physical quantum computers are based on quantum elements such as photons, ions, electrons, and protons.
- Relevant quantum mechanical concepts:
  - Superposition.
  - Entanglement.
  - Decoherence.
  - Measurement.

AALBORG UNIVERSITY
DENMARK

Superposition:

- A quantum state can be any linear combination of states and follows form:

$$|\psi\rangle = \alpha\,|0\rangle \;+\; \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,\; \alpha, \beta \in \mathbb{C}$$

AALBORG UNIVERSITY
DENMARK

Superposition:

- A quantum state can be any linear combination of states and follows form:

$$|\psi\rangle = \alpha\,|0\rangle\ +\ \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,\ \alpha, \beta \in \mathbb{C}$$

Entanglement:

- A state where particles are so tightly correlated that gaining information about one will give immediate information about the other.

Quantum Background
The Core Quantum Principles

Superposition:

- A quantum state can be any linear combination of states and follows form:

$$|\psi\rangle = \alpha\,|0\rangle \;+\; \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,\; \alpha, \beta \in \mathbb{C}$$

Entanglement:

- A state where particles are so tightly correlated that gaining information about one will give immediate information about the other.

Decoherence:

- Loss of superposition due to the fragile quantum system spontaneously couples to the environment.

AALBORG UNIVERSITY DENMARK

Superposition:

- A quantum state can be any linear combination of states and follows form:

$$|\psi\rangle = \alpha\,|0\rangle \;+\; \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,\; \alpha, \beta \in \mathbb{C}$$

Entanglement:

- A state where particles are so tightly correlated that gaining information about one will give immediate information about the other.

Decoherence:

- Loss of superposition due to the fragile quantum system spontaneously couples to the environment.

Measurement:

- Collapsing a superposition to yield state $|0\rangle$ or $|1\rangle$ based on probabilities $|\alpha|^2$ and $|\beta|^2$, respectively.

AALBORG UNIVERSITY
DENMARK

Noisy Intermediate Scale Quantum (NISQ) computing

- Noisy Intermediate Scale Quantum (NISQ) computing is a term coined by John Preskill in 2018, which noted that current quantum computers at the time (and indeed still in 2023) are prone to considerable error rates and limited in size by the number of logical qubits in the system.

AALBORG UNIVERSITY
DENMARK

Noisy Intermediate Scale Quantum (NISQ) computing

- Noisy Intermediate Scale Quantum (NISQ) computing is a term coined by John Preskill in 2018, which noted that current quantum computers at the time (and indeed still in 2023) are prone to considerable error rates and limited in size by the number of logical qubits in the system.

Towards low-noise and fault tolerant quantum computers

- Noise in quantum gates limits the size of reliable quantum circuits.
- A 100-qubit NISQ quantum computer will not change the world.
- Technology development aims for low-noise and later for fault tolerant quantum computing.

Dept. of Computer Science
Aalborg University
Denmark

Overview of various Quantum Computer simulators:

- https://thequantuminsider.com/2022/06/14/top-63-quantum-computer-simulators-for-2022/
- https://thequantuminsider.com/2022/05/27/quantum-computing-tools/

GitHub Full Stack Libraries and Simulators:

- https://github.com/qosf/awesome-quantum-software

Company → simulator links:

- D-Wave → https://github.com/dwavesystems/dwave-ocean-sdk
- IBM → https://qiskit.org
- Intel → https://github.com/intel/intel-qs
- Rigetti → https://github.com/quil-lang/qvm
- Xanadu (photonic library) → https://github.com/xanaduai/strawberryfields
- Xanadu (Gaussian Boson Sampling) → https://github.com/xanaduAI/thewalrus

Out→

- Moore's law is coming to an end with doubling in transistor density every 18 months.
- Some problems are so large that they can not be computed on even the largest supercomputers that exist.

Dept. of Computer Science
Aalborg University
Denmark

Out→

- Moore's law is coming to an end with doubling in transistor density every 18 months.
- Some problems are so large that they can not be computed on even the largest supercomputers that exist.

→In

- A computer that uses the laws of quantum mechanics to perform massively parallel computing through superposition and entanglement.

AALBORG UNIVERSITY DENMARK
Dept. of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

Out→

- Moore's law is coming to an end with doubling in transistor density every 18 months.
- Some problems are so large that they can not be computed on even the largest supercomputers that exist.

→In

- A computer that uses the laws of quantum mechanics to perform massively parallel computing through superposition and entanglement.

Quantum Computing relies on quantum mechanics and quantum theory. **Possibilities for extreme speed in some areas but lacks the generality of classical computers in other areas.** Well suited for 'combinatorics', optimization, chemistry, AI/ML, statistics, secure communication, ...

Classical Computer:

- A computer that uses voltages/currents across/through circuits and gates, which can be controlled and manipulated entirely by classical mechanics.
- Building blocks: bits, registers, and logic gates.

AALBORG UNIVERSITY
DENMARK

Classical Computer:

- A computer that uses voltages/currents across/through circuits and gates, which can be controlled and manipulated entirely by classical mechanics.
- Building blocks: bits, registers, and logic gates.

Quantum Computer:

- A computer that uses the laws of quantum mechanics to perform massively parallel computing through superposition and entanglement.
- Building blocks: qubits, quantum registers, and reversible gates.

A technology platform is a combination of mathematical quantum processing, a mapping to realizable hardware, and coupling this to a software stack for further processing.

[2] Edited descriptions from: R.L. Amoroso: “Brief Primer on the Fundaments of Quantum Computing”

Dept. of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

A technology platform is a combination of mathematical quantum processing, a mapping to realizable hardware, and coupling this to a software stack for further processing.

- Quantum Computer Technology Platforms[2]:
  - Trapped Ion-Based Superconductor
    Using ions trapped in magnetic fields and manipulating them using electromagnetic waves and/or lasers.
  - Linear Optical Quantum Computer (LOQC)
    Realization of qubits by processing different modes of light as quantum states (photonic qubits).
  - Quantum Dot Quantum Computer
    A type of nanoscale atomic/molecular structure allowing control of the flow of electrons using small voltages.
  - Topological Quantum Computer (TQC)
    Based on the braiding of anyons (quasi-particles) in a 2D lattice providing a high degree of error protection from decoherence.

[2] Edited descriptions from: R.L. Amoroso: "Brief Primer on the Fundaments of Quantum Computing"

Classical:

- In classical computing, parallelism refers to the computation of multiple calculations across multiple computational units simultaneously.

AALBORG UNIVERSITY
DENMARK

Classical:

- In classical computing, parallelism refers to the computation of multiple calculations across multiple computational units simultaneously.

Quantum:

- Quantum parallelism refers to the ability of quantum computers to evaluate a function for multiple input values simultaneously.
  - This can be achieved by preparing a quantum system in a superposition of input states, and applying a unitary transformation that encodes the function to be evaluated.
  - The resulting state encodes the function's output values for all input values in the superposition, allowing for the computation of multiple outputs simultaneously.
  - This property is key to the speedup of many quantum algorithms.

Number of qubits for IBM quantum computers:

Year	Vendor	Name	qubits
2019	IBM	Falcon	27
2020	IBM	Hummingbird	65
2021	IBM	Eagle	127
2022	IBM	Osprey	433
2023	IBM	Condor	1,121
2024	IBM	Flamingo	$\geq$1,386
2025	IBM	Kookaburra	$\geq$4,158

AALBORG UNIVERSITY DENMARK

Qubits

Classical Computer State Description:

- One classical bit b has one of two states named '0'/'1'.
- Occasionally, the states are named 'LOW'/'HIGH' or 'False'/'True'.
- Say we have N bits $b_0, b_1, \ldots, b_{N-3}, b_{N-2}, b_{N-1}$ – this allows us to represent e.g. 2^N integers:

$$\begin{aligned} \mathcal{B}_0 &: \quad 0, 0, \ldots, 0, 0 \\ \mathcal{B}_1 &: \quad 0, 0, \ldots, 0, 1 \\ \mathcal{B}_2 &: \quad 0, 0, \ldots, 1, 0 \\ &\vdots \\ \mathcal{B}_{2^N-1} &: \quad 1, 1, \ldots, 1, 1 \end{aligned}$$

- For the classical computer we can have any of the states above but only one at any given time.

Quantum Computer State Description (Recap):

- The smallest unit of information in Quantum Computing is the Quantum-bit or Qubit.
- A Qubit represents the state of the wavefunction $|\phi\rangle$ in Schrödingers equation at a specific time.
- A single Qubit may be in the "on" state ($|1\rangle$) or it may be in the "off" state ($|0\rangle$).
- Schrödingers equation, which describes how the state of a quantum mechanical system evolves in time is linear. Hence, linear combinations of solutions are also valid solutions.

Dept. of Computer Science
Aalborg University
Denmark

Quantum Computer State Description (Recap):

- If a qubit has the state $|0\rangle$ and $|1\rangle$, a superposition of these also describe the same state. The general superposition form of the state is:

$$|\psi\rangle = \alpha\,|0\rangle \;+\; \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,\; \alpha, \beta \in \mathbb{C}$$

- The two core states $|0\rangle$ (ground state) and $|1\rangle$ (excited state) are orthonormal[3] in Hilbert space.
- The joined state $|\psi\rangle$ is a superposition of the core states each multiplied by a constant complex number at the given time instant.

[3] Two vectors in a inner product space are orthonomal if they are orthogonal unit vectors.

Dept. of Computer Science
Aalborg University
Denmark

States in a two-state quantum system:

- A qubit is a two-state (or two-level) quantum mechanical system. There are different ways to enter the quantum state – the following two are typical:
- Spin states of an electron/atom:

$$|1\rangle \quad \text{and} \quad |0\rangle \quad \text{as} \quad \uparrow \quad \text{and} \quad \downarrow$$

  The arrows are spin-up and spin-down, respectively.

- Polarization states of a photon:

$$|1\rangle \quad \text{and} \quad |0\rangle \quad \text{as} \quad H \quad \text{and} \quad V$$

  The *H* and *V* are horizontal and vertical, respectively.

Dept. of Computer Science
Aalborg University
Denmark

Qubit state description:

- Output state $|\psi\rangle$ from single (two-layer) qubit ...

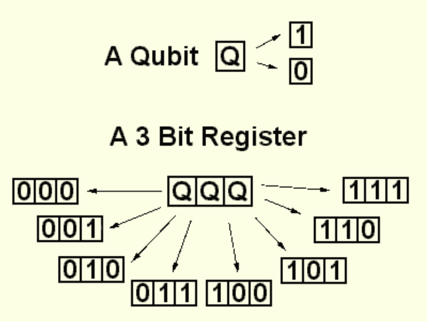
$$|\psi\rangle = \alpha\,|0\rangle \;+\; \beta\,|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1,\; \alpha, \beta \in \mathbb{C} \qquad (1)$$

- The two core states $|0\rangle$ (ground state) and $|1\rangle$ (excited state) are orthonormal in Hilbert space.
- The joined state $|\psi\rangle$ is a superposition of the core states each multiplied by a constant complex number at the given time instant.
- Observing the joint output state $|\psi\rangle$ indicates 4 degrees of freedom. However, the limitation $|\alpha|^2 + |\beta|^2 = 1$ reduces to 3 degrees of freedom.
- $|\alpha|^2$ is the probability of output state $|0\rangle$, and $|\beta|^2$ is the probability of output state $|1\rangle$.

Dept. of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

Register based on:



Dept. of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

Qgates

Dept. of Computer Science
Aalborg University
Denmark

Qgates:

- A quantum gate (quantum logic gate) is a functional unit that transfer input state/states to an output state according to the properties of the quantum gate.

AALBORG UNIVERSITY
DENMARK

Qgates:

- A quantum gate (quantum logic gate) is a functional unit that transfer input state/states to an output state according to the properties of the quantum gate.
- A number of connected (normally different) qgates form a qcircuit that implements an algorithm. This is similar to low-level electronics using connected binary gates (OR, AND, XOR etc.) to achieve a logical desired link between input variables (states) and output variables (states).

Dept. of Computer Science
Aalborg University
Denmark

AALBORG UNIVERSITY
DENMARK

Qgates:

- A quantum gate (quantum logic gate) is a functional unit that transfer input state/states to an output state according to the properties of the quantum gate.
- A number of connected (normally different) qgates form a qcircuit that implements an algorithm. This is similar to low-level electronics using connected binary gates (OR, AND, XOR etc.) to achieve a logical desired link between input variables (states) and output variables (states).
- Due to normalization constraints, any gate operation **U** must be unitary:

$$\mathbf{U}\mathbf{U}^{\dagger} = \mathbf{U}^{\dagger}\mathbf{U} = \mathbf{I}, \quad \mathbf{U} \in \mathbb{C}^{2^N \times 2^N} \tag{2}$$

where **U** is a complex square matrix, $\mathbf{U}^{\dagger}$ is the conjugate transpose of **U**, and **I** is the identity matrix.

Dept. of Computer Science
Aalborg University
Denmark

Qgates:

- To compute the output state we start by defining input base states as vectors:

$$|\mathbf{0}\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |\mathbf{1}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3}$$

- Say we have a unitary transformation described by the unitary transfer matrix **X**:

$$\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{4}$$

Dept. of Computer Science
Aalborg University
Denmark

Qgates:

- Applying the input state $|\mathbf{0}\rangle$ to the transformation matrix $\mathbf{X}$ leads to:

$$|\mathbf{0}\rangle \longrightarrow \mathbf{X}\,|\mathbf{0}\rangle = \mathbf{X}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = |\mathbf{1}\rangle \tag{5}$$

Dept. of Computer Science
Aalborg University
Denmark

Qgates:

- Applying the input state $|\mathbf{0}\rangle$ to the transformation matrix $\mathbf{X}$ leads to:

$$|\mathbf{0}\rangle \longrightarrow \mathbf{X}\,|\mathbf{0}\rangle = \mathbf{X}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = |\mathbf{1}\rangle \tag{5}$$

- Applying the input state $|\mathbf{1}\rangle$ to the transformation matrix $\mathbf{X}$ leads to:

$$|\mathbf{1}\rangle \longrightarrow \mathbf{X}\,|\mathbf{1}\rangle = \mathbf{X}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = |\mathbf{0}\rangle \tag{6}$$

- The **X**-matrix is identical to the Pauli-X matrix, which acts as a quantum state inverter.

Dept. of Computer Science
Aalborg University
Denmark

Qgates
Selected qgates

AALBORG UNIVERSITY
DENMARK

Operator	Symbol	Matrix	Comments
Pauli-X	$\mathbf{X}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	Pauli matrices: $\mathbf{X}, \mathbf{Y}, \mathbf{Z} \in \mathbb{C}^{2\times 2}$. All are Hermitian ($\mathbf{M} = \mathbf{M}^\dagger$), involutory ($\mathbf{M}^2 = \mathbf{I}$) and unitary ($\mathbf{M}\mathbf{M}^\dagger = \mathbf{M}^\dagger\mathbf{M} = \mathbf{I}$).[4]
Pauli-Y	$\mathbf{Y}$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	
Pauli-Z	$\mathbf{Z}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	
Hadamard	$\mathbf{H}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	
Phase	$\mathbf{S}$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$	

[4] For more details see Nielsen & Chuang: "Quantum Computation and Quantum Information", Cambridge University Press, 2010.

AALBORG UNIVERSITY
DENMARK

Qcircuits

Dept. of Computer Science
Aalborg University
Denmark

Qcircuits

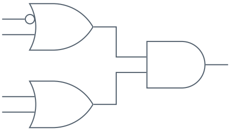
Qcircuits are:

- combinations of correctly connected qgates to provide desired functionalities
- described by their:
  - Input state(s) such as e.g. $|0\rangle$, $|1\rangle$, and $|q_0 q_1 q_2\rangle$.
  - Various transformation matrices that connected correctly provide the desired output state(s) depending on input state(s).
  - Description of the desired output state(s).
    - It is also possible here to use one or more measurement unit(s) remembering that this causes decoherence.

AALBORG UNIVERSITY
DENMARK

Qcircuits
Example from electronics

Electronics circuit based on logical gates (AND, OR, NOT):



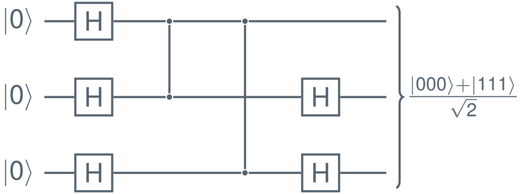
Dept. of Computer Science
Aalborg University
Denmark

Qcircuits

Example from quantum computing

AALBORG UNIVERSITY
DENMARK

Quantum circuit based on Hadamard gates:



A quantum circuit for producing a Greenberger-Horne-Zeilinger (GHZ) state using Hadamard gates and controlled phase gates. The circuit is important for tests of nonlocality.

Literature

Dept. of Computer Science
Aalborg University
Denmark

Literature of general type:

1. Michael A. Nielsen & Isaac L. Chuang: “Quantum Computation and Quantum Information”. Cambridge University Press, 10*th Anniversary Edition*, 2010.
2. Noson S. Yanofsky & Mirco A. Mannucci: “QUANTUM COMPUTING FOR COMPUTER SCIENTISTS”. Cambridge University Press, 2008.
3. N. David Mermin: “Quantum Computer Science – An Introduction”. Cambridge University Press, 2007.
4. Bahman Zohuri and Farhang Mossavar Rahmani: “What is Quantum Computing and How it Works”. Journal of Material Sciences & Manufacturing Research, 2020.

Closure
Contact Information

In case you have any comments, suggestions or have found a bug, please do not hesitate to contact me. You can find my contact details below:

Torben Larsen, `tola@cs.aau.dk`
Selma Lagerlöfs Vej 300, Office 4.2.16
9220 Aalborg
Denmark

Figures:

- Public domain: Slides ..
- Creative commons: Slides ..
- Own creation: Slides ..