Introduction to Quantum Computing

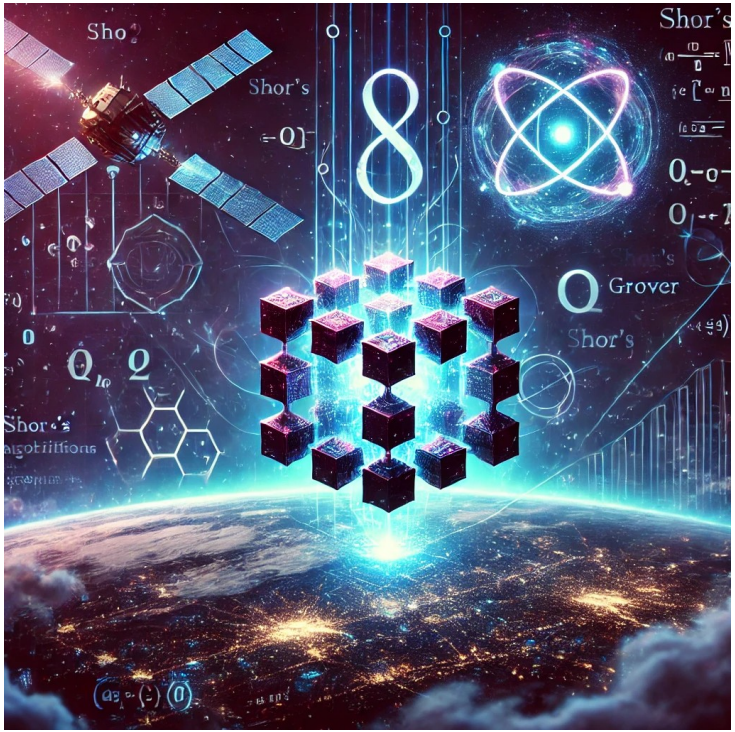
Professor Adrian FLOREA, PhD
adrian.florea@ulbsibiu.ro

- background material in **computer science**, **mathematics** and **physics** necessary to **understand quantum computation and quantum information**

Acknowledgement: "*Romanian National Quantum Communication Infrastructure* (RONAQCI)", project within the Digital Europe programme of the European Commission, call DIGITAL-2021-QCI-01 (EU Secure Quantum Communication Infrastructure), topic DIGITAL-2021-QCI-01-DEPLOY-NATIONAL, https://www.ronaqci.upb.ro/

Quantum computing in the news

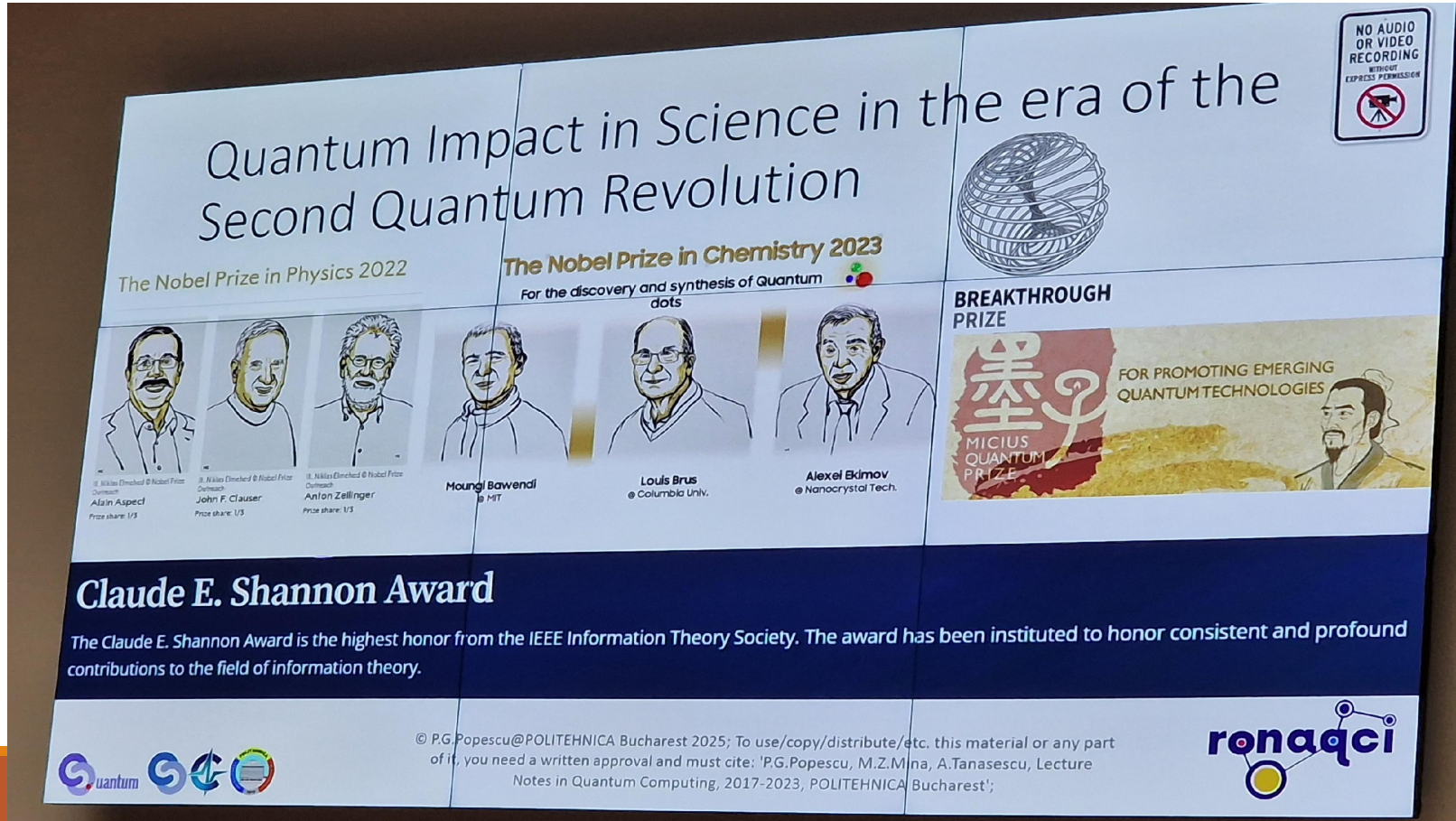
- China **teleported a qubit** from earth to a satellite
- **Shor's algorithm** has put our current encryption methods at risk
- **Quantum Key Distribution** will make encryption safe again
- **Grover's algorithm** will speed up data searches.



- **But what does all this really mean?**
- **How does it all work?**
- **Critical need to integrate quantum computers with classical supercomputing resources** to **build practical quantum solutions**!

- **The Nobel Prize in Physics 2022** was awarded jointly to Alain Aspect, John Clauser and Anton Zeilinger **"*for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science*"**

- **The Nobel Prize in Chemistry 2023** was awarded to Moungi Bawendi, Louis Brus and Aleksey Yekimov **"*for the discovery and synthesis of quantum dots*"**



Syllabus (I)

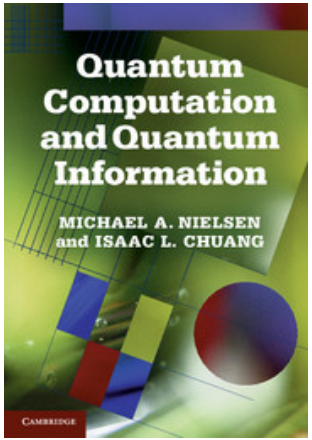
1. **Supporting Literature / Tools**
2. **History of Quantum Theory & Quantum Computing. The 5 postulates**
3. **What is Quantum Computing (QC)? Main concepts: *superposition, entanglement, decoherence*.**
4. **Why Quantum Computing?**
5. **Comparison between classic computing and QC**
6. **Uses of quantum computing across industries: healthcare, finance, industry, agriculture, cybersecurity & national security**
7. **Mathematical background on quantum states and operations. Basic Linear Algebra: Vectors, Matrices, Hermitian/Unitary matrices**

Syllabus (II)

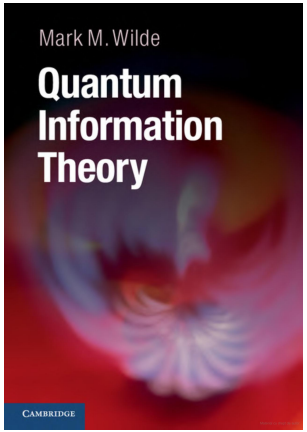
8. Representing 1 q-bit. The <bra| and |ket> notations. Computational basis and Hadamard basis
9. Single q-bit gates: NOT, Hadamard, Pauli
10. Representing 2 q-bits. CNOT, Toffoli, Fredkin gates. Tensor product. Examples
11. Measurement. Entanglement. Teleportation.
12. Quantum Evolutionary Algorithm and its Application
13. Introduction to Qiskit. Quantum Instruction Set.
14. Exercises. Testing in Qiskit
15. The Architecture of Quantum Computers (a layered approach).
16. Quantum Algorithms: Deutsch, Grover, Schor. The BB84 Protocol

Resources and bible books (I)

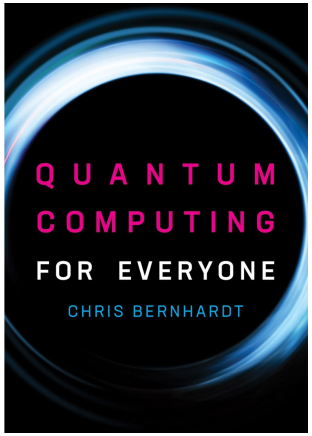
Nielsen, M. A., & Chuang, I. L. (2010). ***Quantum computation and quantum information*****.** Cambridge university press.



Wilde, Mark M (2013). ***Quantum information theory***. Cambridge university press.



Bernhardt, Chris (2019). *Quantum computing for everyone*, Massachusetts Institute of Technology,



Resources and bible books (II)

- **IBM Quantum Platform - https://docs.quantum.ibm.com/start/hello-world**
- **IBM Qiskit SDK - https://www.ibm.com/quantum/qiskit**
- **IBM Quantum Composer - https://quantum.ibm.com/composer**
- **Understanding Quantum Information & Computation - https://www.youtube.com/watch?v=3-c4xJa7Flk&list=PLOFEBzvs-VvqKKMXX4vbi4EB1uaErFMSO&index=3**
- **Quirk: Quantum Circuit Simulator - https://algassert.com/quirk**
- Shuyuan Yang, Min Wang and Licheng Jiao, **A novel quantum evolutionary algorithm and its application**, Proceedings of the 2004 Congress on Evolutionary Computation (IEEE Cat. No.04TH8753), Portland, OR, USA, 2004, pp. 820-826 Vol.1, doi: 10.1109/CEC.2004.1330945.
- Zhang, G. **Quantum-inspired evolutionary algorithms: a survey and empirical study**. J Heuristics 17, 303–351 (2011). https://doi.org/10.1007/s10732-010-9136-0
- Wille, Robert, et al. "The MQT Handbook: A Summary of Design Automation Tools and Software for Quantum Computing." arXiv preprint arXiv:2405.17543 (2024).

History of Quantum Theory & Quantum Computing (I)

"*Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical*."

Richard Feynman, **interested in the relationship between physics and computation**, **1965 Nobel Prize in Physics**

1985: ***Quantum Mechanical Computers*** - focuses on **details of how a quantum computer would work and how quantum algorithms would be designed**.

Quantum mechanics

Fundamental physical theory describing behavior of atoms, electrons and other elementary particles!

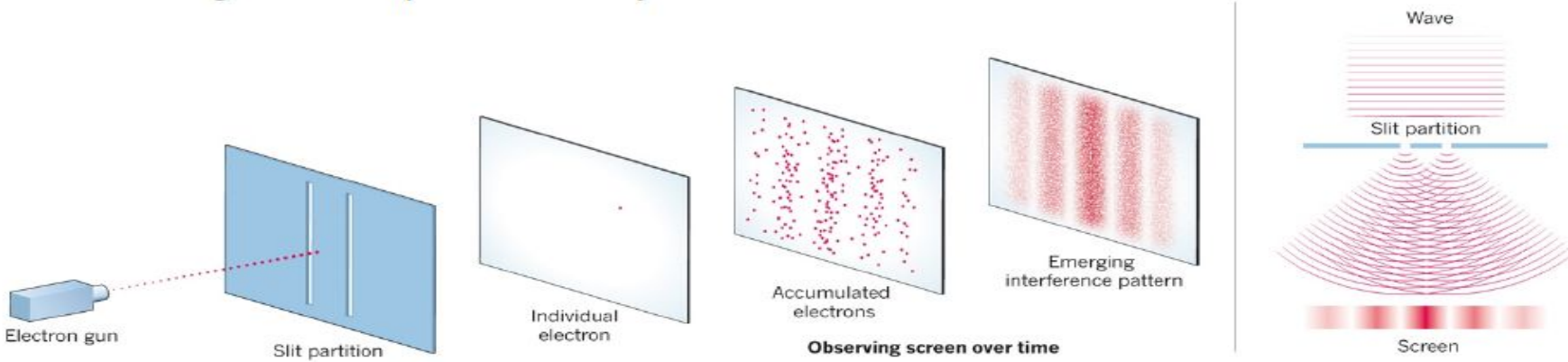
(But: general relativity not taken into account ⇝ area of active research)

History of Quantum Theory & Quantum Computing (II)

- 1900 Max Planck: energy quantization, invented as mathematical tool to describe black body radiation:

$$E = nh\nu, \quad n \in \mathbb{N},\ h\text{: Planck's constant},\ \nu\text{: frequency}$$

- 1905 Albert Einstein: explanation of the photoelectric effect by describing light as composed of discrete quanta (photons)
- 1913 Niels Bohr: Bohr model of atoms: electrons in discrete energy states, Rydberg formula for spectral emission wavelengths of hydrogen
- 1924 Louis de Broglie: wave–particle duality of matter

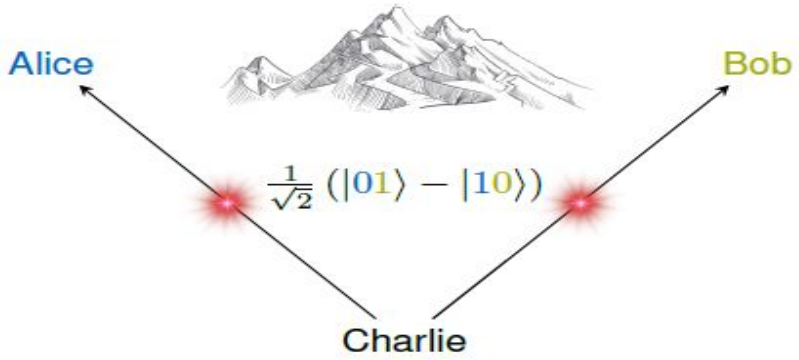


History of Quantum Theory & Quantum Computing (III)

- 1925 Erwin Schrödinger: Schrödinger equation for the wave function Ψ of a quantum-mechanical system:

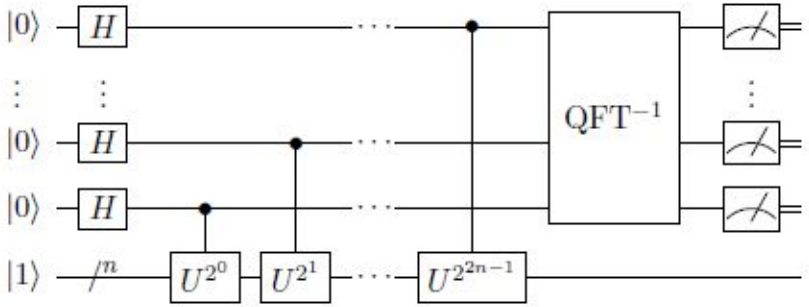
$$i\hbar\frac{\mathrm{d}}{\mathrm{d}t}|\Psi(t)\rangle = \hat{H}\,|\Psi(t)\rangle$$

- 1927 Werner Heisenberg: uncertainty principle
- 1927 Niels Bohr and Werner Heisenberg: Copenhagen interpretation of quantum mechanics
- 1928 Paul Dirac: Dirac equation, combines special relativity and quantum mechanics; first prediction of antimatter
- 1935 Einstein, Podolsky, Rosen: EPR paradox: "spooky action at a distance" due to quantum entanglement (⇝ Bell's inequality)



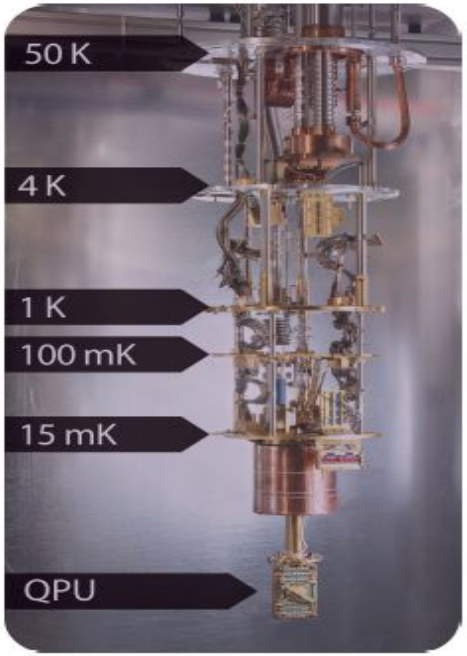
History of Quantum Theory & Quantum Computing (IV)

- 1948 Claude Shannon: "A Mathematical Theory of Communication": foundation of information theory
- 1961 Rolf Landauer: Landauer's principle: logically irreversible manipulation of information is necessarily dissipative
- 1964 John Bell: Bell's inequality: "local realism" violates predictions by quantum mechanics (later experiments agree with quantum mechanics)
- 1982 Richard Feynman: idea of a universal quantum computer
- 1985 David Deutsch: precursor of Deutsch-Jozsa algorithm: exponentially faster than any possible deterministic classical algorithm
- 1993 Bernstein und Vazirani: foundations of quantum complexity theory
- 1994 Peter Shor: Shor's algorithm for integer factorization
  ($\rightsquigarrow$ highly relevant for public-key cryptography)
  threath to RSA cryptosystem

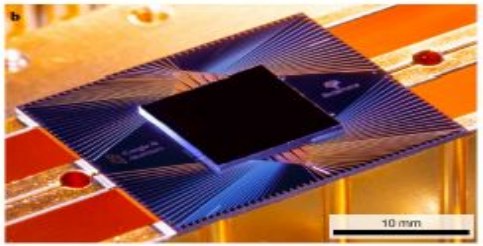


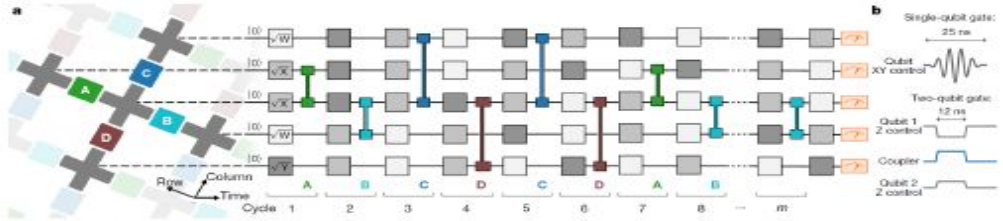
History of Quantum Theory & Quantum Computing (V)

- 1998 2-qubit nuclear spin resonance quantum system
- 2009 Research group of John Martinis: “Josephson-junction superconducting qubit”
- 2015 DWAVE “quantum annealing” system (2048 qubits)



- 2016 IBM quantum computer with 50 qubits
- 2019 Google / Martinis group: “quantum supremacy”, Sycamore processor (53 qubits)





F. Arute, . . . , H. Neven, J. M. Martinis. *Quantum supremacy using a programmable superconducting processor*. Nature 574, 505 (2019)

- 2020 Alpine Quantum Technologies (aqt.eu): ion-trap QC, qubit loss detection and correction

Theoretical basis of Quantum Systems

The 5 postulates form the theoretical basis of quantum systems (including quantum computers) and pertain to qubits, their measurements, and evolution, Schrödinger's law, and more. They were formulated by the early masters of the field, including Dirac, Heisenberg, von Neumann, around the 1930s. The postulates of quantum mechanics also demonstrate the connection between the physical world and the mathematical formalism of quantum mechanics.

POSTULATE 1: "To every isolated quantum system Σ (e.g., electron, photon, atom, ion, particle family, etc.), there is associated a complex Hilbert space $H = H(\Sigma)$, called the **space of states of the system**, and non-zero states ψ of system Σ are represented by vectors $|\psi\rangle$ in H. If $\dim H = 2$, then the states are associated with qubits."

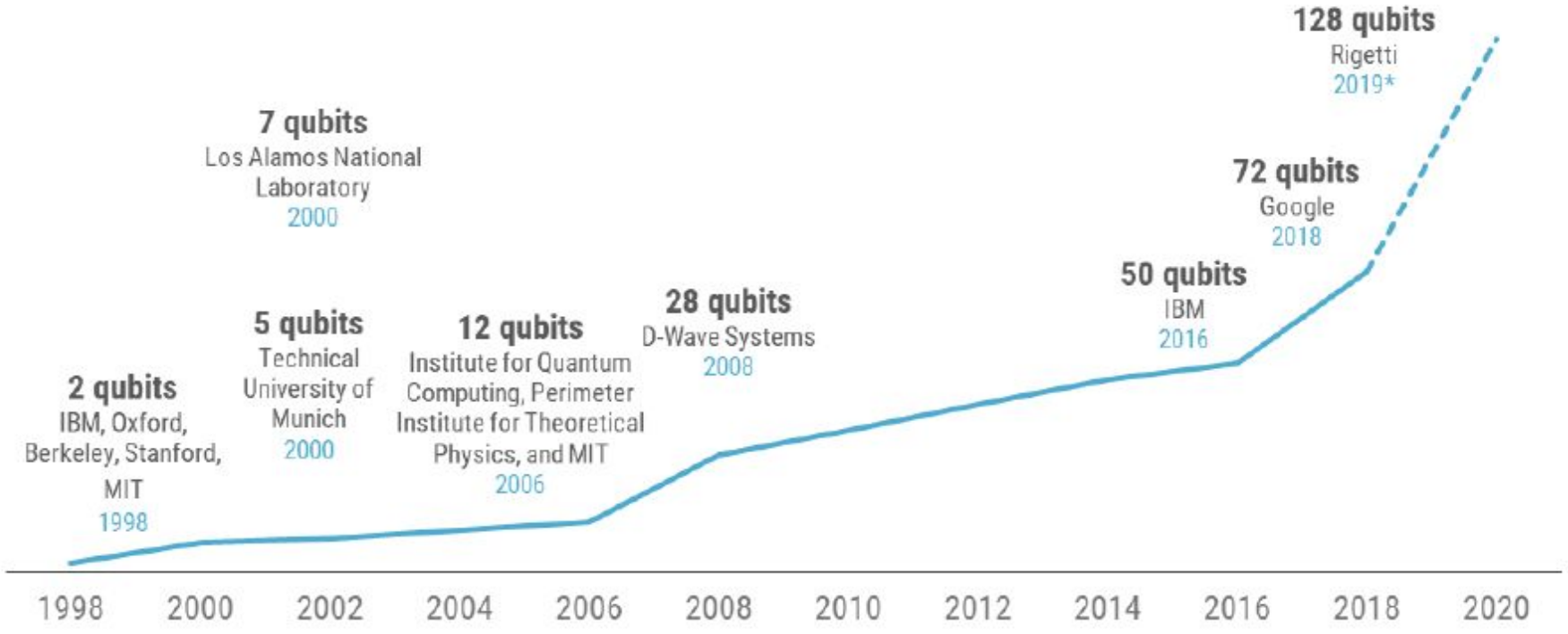
Postulate 1 refers to the Hilbert space associated with any isolated quantum system (including qubits in particular); **Postulate 2 concerns the transformation of qubits**, and **Postulate 3 deals with the effect of measurements**. The **last two postulates summarize the dynamics of states and the composition of quantum systems**.

Quantum Computing: Hardware Technologies

- Superconductors
- Trapped Ions
- Photons
- Neural Atoms
- Silicon Spins/Quantum Dots

Quantum computers are getting more powerful

Number of qubits achieved by date and organization 1998 – 2020*



Source: MIT, Qubit Counter. *Rigetti quantum computer expected by late 2019.

CBINSIGHTS

Association for Computing Machinery

acm Technology Policy Council

TechBriefs

QUANTUM COMPUTING AND SIMULATION

Garfinkel, S. L., & Hoofnagle, C. J. (**2022**). ACM TechBrief: Quantum computing and simulation.

QUANTUM SIMULATION: BY THE NUMBERS	
20,000,000	Estimated number of information units ("qubits") necessary for a quantum computer to defeat the strongest widely used public key encryption.[1]
127	Maximum number of such qubits achieved to date.[2]
10	Minimum estimated number of years for quantum computing to become viable.[3]
40	Maximum estimated number of years for quantum computing to become viable.[3]
2	Maximum estimated number of years for quantum simulation to become widely used.[4]

Association for Computing Machinery
acm Technology Policy Council
TechBriefs

QUANTUM COMPUTING AND SIMULATION

Powerful quantum simulators are nearly a reality

- ✔ quantum simulators refer to specialized **quantum computers tailored to performing simulations of dynamic models of relevant processes** (rather than conventional computers simulating quantum phenomena)
- ✔ **quantum simulators may hasten development of a practical, general-purpose quantum computer**.
- ✔ **Risks of quantum simulators**:
  - could permit clandestine weapons development without threat of detection.
  - have the potential to substantially undermine rights to personal privacy worldwide.

Romanian contribution to Quantum Computing paradigme

- **First quantum revolution – 1980 - 1990**
- **Second quantum revolution – 2023 (EU funding for QC). Maintaining the gap between RO and rest of the countries who invest and educate QC – master programs, conferences & research grants**
- **Romanian top contributors:** Sandu Popescu - http://www.sandupopescu.com

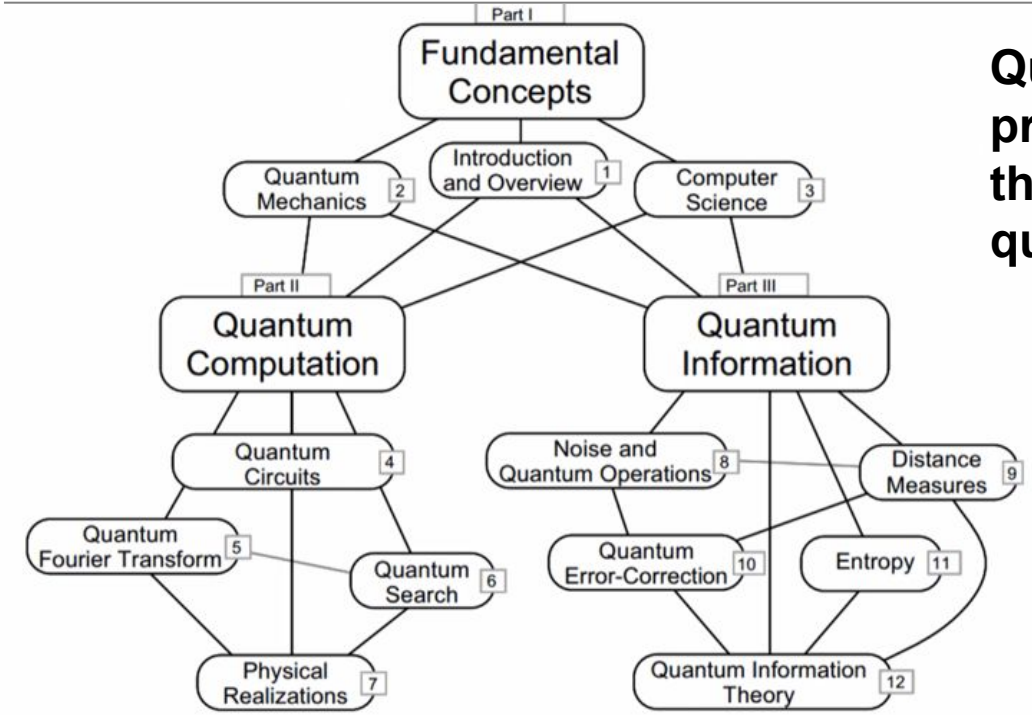
  - A Romanian quantum fundamentalist;
  - "Whilst my work focuses mainly on fundamental, theoretical aspects of quantum theory, I also greatly enjoy engaging with experimentalists. In particular I designed and participated in the first teleportation experiment, one of the most famous experiments in the field of quantum information."

What is Quantum Computing ? (I)

- Quantum computers take a **different approach to computing from traditional digital machines**, one **based on calculating probabilities instead of discrete values**.
- Rather than processing bits that can represent only a 0 or 1, they compute with **qubits (quantum bits)**, which can initially represent many values.
- **Quantum computers then manipulate the qubits** with mechanisms called **quantum gates**, causing **the qubits to change over time**.
- Finally, **each qubit is measured by a conventional computer and converted to a 0 or 1** that the ordinary digital computer can record. This **process may need to be repeated many times for a single quantum computation**.

What is Quantum Computing? (II)

Nielsen & Chuang provide a good structure:

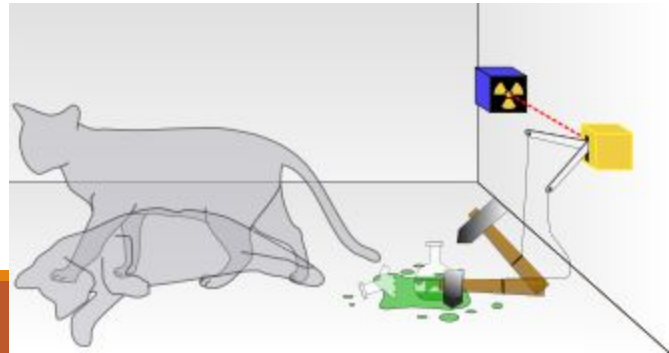


Quantum computing is the processing of information that's represented by special quantum states.

Why Quantum Computing ? (I)

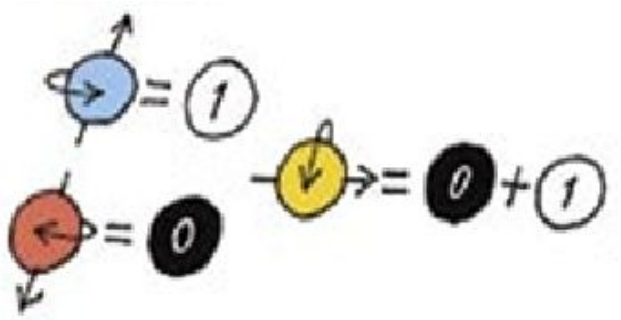
- **Exponentially faster than classic computers** (in some areas)
- In 2019, Google said that it ran a calculation on a **quantum computer in just a few minutes** that would take **a classical computer 10,000 years** to complete *(quantum supremacy).*
- In 2020, a team based in China took this a step further, claiming that it had performed a calculation in 200 seconds that would take an ordinary computer 2.5B years — 100 trillion times faster.

- in contrast to a classic computer it **mimics the way particles work at an atomic level**



Why Quantum Computing ? (II)

- The fundamental feature of a quantum computer is that it uses **qubits** instead of **bits**. A qubit may be a particle such as an electron, with "**spin up**" (***blue***) representing **1**, "**spin down**" (***red***) representing **0**, and quantum states called **superposition** that involve **spin up and spin down simultaneously** (*yellow*).



- **Spinul este o proprietate fundamentală a particulelor în mecanica cuantică**, care joacă un rol important în domeniul informațiilor cuantice.
- Este o proprietate mecanică cuantică a particulelor elementare, cum ar fi **electronii și protonii**, și este adesea descrisă ca o **formă intrinsecă a momentului unghiular**.
- **Starea unui qubit poate fi reprezentată ca o combinație liniară a stărilor spin-up și spin-down**.

Why Quantum Computing ? (III)

- A small number of particles in superposition states can carry an enormous amount of information: a **mere 1,000 particles can be in a superposition that represents every number from 1 to $2^{1,000}$ (about 10^{300})**, and a **quantum computer would manipulate all those numbers in parallel**, for instance, by **hitting the particles with laser pulses**.

- **When the particles' states are measured at the end of the computation**, however, **all but one random version of the 10^{300} parallel states vanish**.
- **Clever manipulation of the particles could nonetheless solve certain problems very rapidly**, such as factoring a large number.

Why Quantum Computing ? (IV)

Between 1970s and 1980s, a few pioneers were inspired to ask whether some of the **fundamental questions of computer science and information theory could be applied to the study of quantum systems**.

Instead of looking at quantum systems purely as phenomena to be explained as they are found in nature, they **looked at them as systems that can be designed**. This seems a small change in perspective, but the implications are profound. No longer is the **quantum world** taken merely as presented, but instead it **can be created**.

⇒ A new perspective that inspired both a resurgence of interest in the fundamentals of quantum mechanics, and also many **new questions combining physics, computer science, and information theory**.

⇒ Research questions:

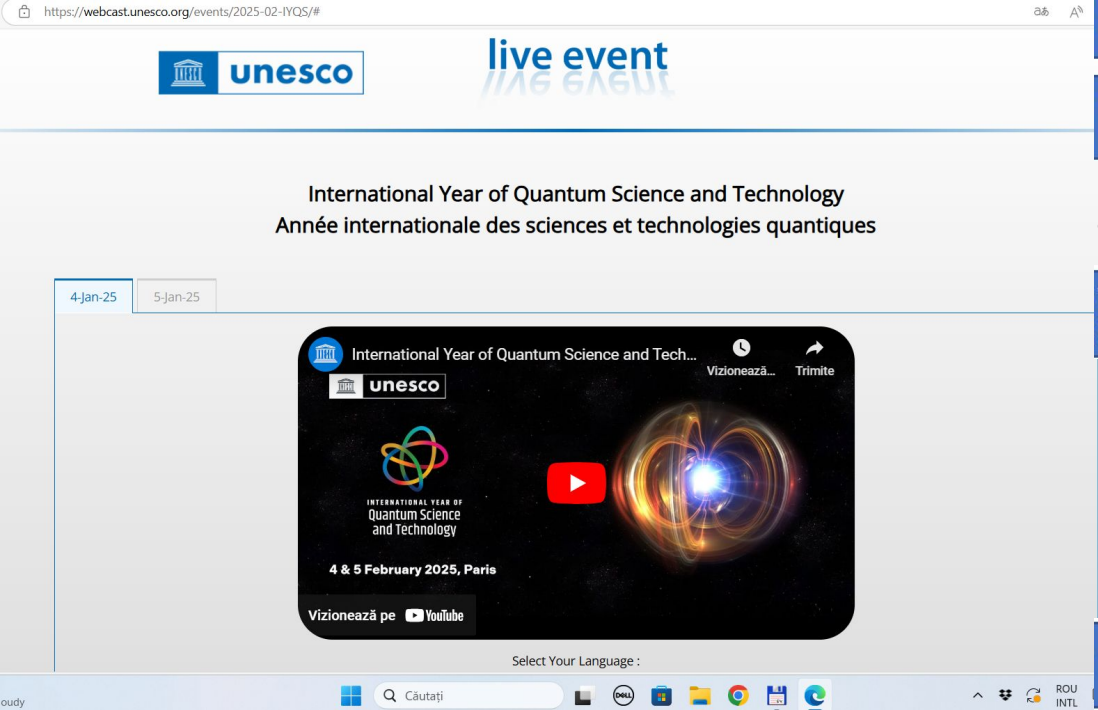
- **What are the fundamental physical limitations on the space and time required to construct a quantum state?**
- **How much time and space are required for a given dynamical operation?**
- **What makes quantum systems difficult to understand and simulate by conventional classical means?**

Why Quantum Computing ? (V)

- On **5 December 2023**, the **EU Council released a declaration that EU Member States are signing** to indicate that they **recognize the strategic importance of quantum technologies for the EU's scientific and industrial competitiveness** and **are committed to working together to develop a world-class quantum technology ecosystem across Europe**, with the **ultimate goal** of **making Europe the 'quantum valley' of the world**, a leading global region for quantum excellence and innovation.
- **Romania is aligning itself with these efforts** – see RONAQCI project (*Romanian National Quantum Communication Infrastructure*), DIGITAL-2021-QCI-01 (EU Secure Quantum Communication Infrastructure), 2023-2025.
- The global **quantum research and innovation effort in quantum science and technology is growing steadily**
  - ✔ **current global investments exceed $36 billion**
  - ✔ the global **quantum technology market is expected to reach $42.4 billion by 2027**.

Why Quantum Computing ? (VI)

- On **4-5 February 2025**, **UNESCO organized International Year of Quantum Science and Technology** for create awareness about importance of Quantum Science and its applications in achieving Agenda 2030 and its 17 Sustainable Development Goals.



Roundtable Discussion: Pushing the Frontiers of Quantum Science and Technology

Panel Discussion: Public Engagement and Education in Quantum Science and Technology

harnessing quantum advancements for climate action, economic growth, and societal well-being.

Voices from the Industry: The Challenge of Developing Quantum at Scale

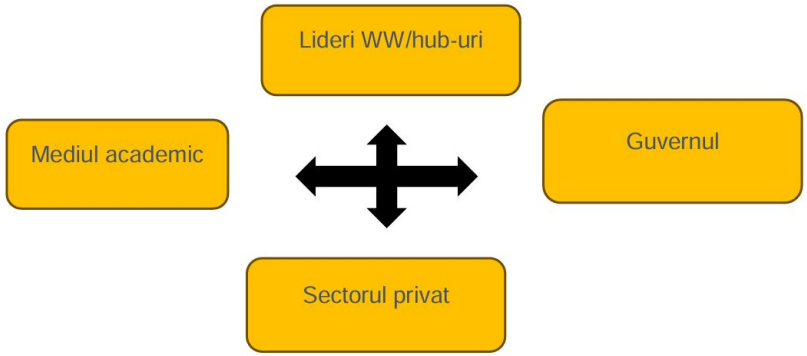
address the challenges and opportunities of scaling quantum technologies for practical use sharing experiences in bringing quantum research to market, showcasing groundbreaking developments in this field

Panel Discussion: Ethics of Quantum Technologies

Romania’s effort for Quantum Computing (I)

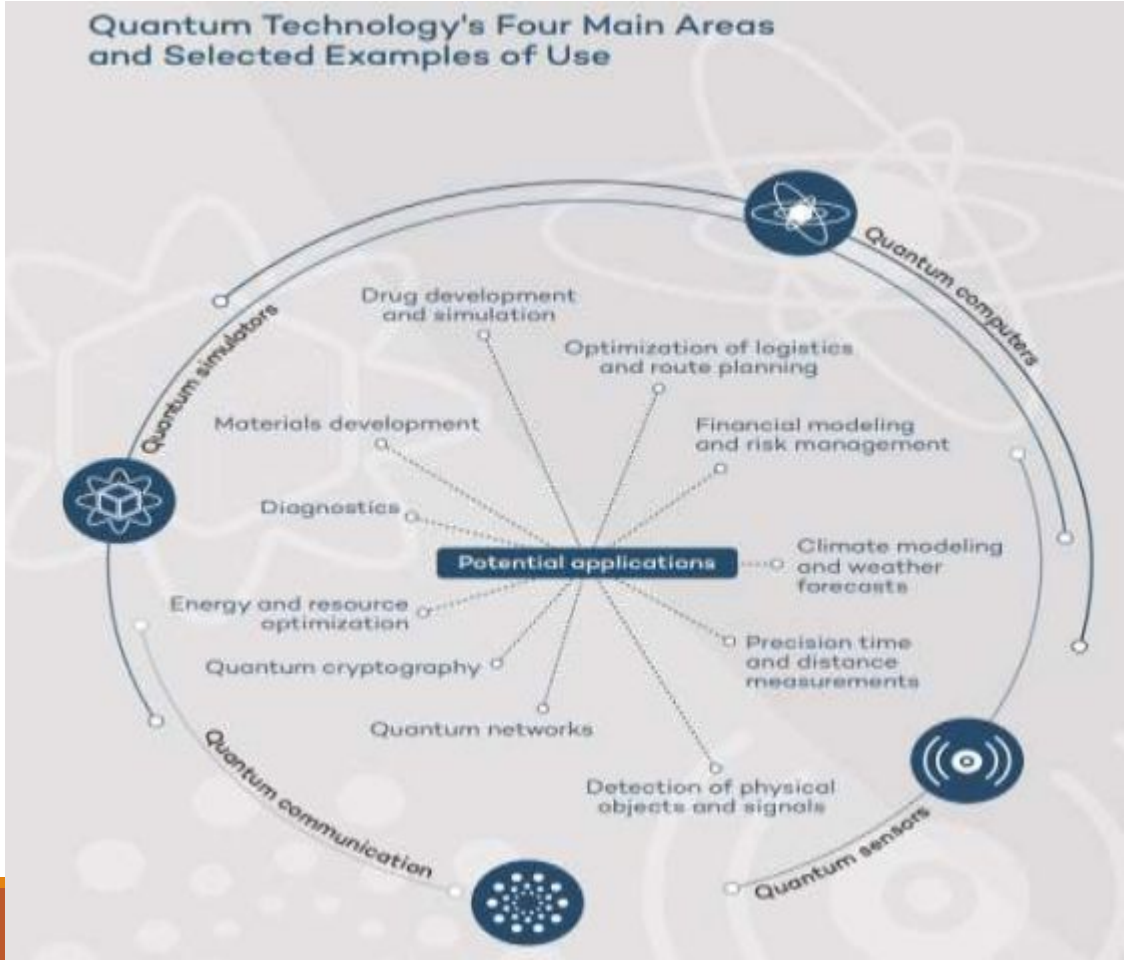
- **National Strategy in the Field of Quantum Technologies** for the period 2024-2029, approved by decision HG no. 1028/2024, published in **Monitorul Oficial**, Part I no. 893 from 04 September 2024. https://www.mcid.gov.ro/programe-nationale/strategia-nationala-in-domeniul-tehnologiilor-cuantice-2024-2029-2/
- **Romania** aims to become a **regional center of excellence** in the **development of applications for quantum technologies**
- Romania can **capitalize on the opportunities offered by quantum technologies through cooperation between public institutions, private entities and academia**

Components of a quantum ecosystem



Romania’s effort for Quantum Computing (II)

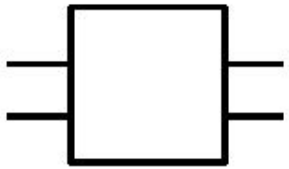
- **Innovation in Industry**
  - ✔ Investments in quantum infrastructure projects (**quantum computing**, **quantum networks**, **quantum sensors**, **quantum cryptography**)
- **Education and Training**
  - ✔ Master in QC at București (2023), Timișoara(2024), Postgraduate program (Cluj)
- **Research and Development**



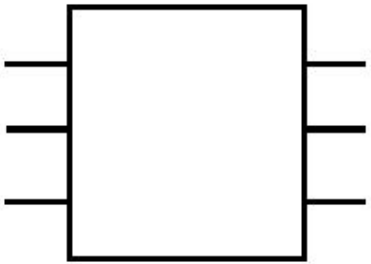
Conventional (clasical) Computing

States of a system

2 Inputs
→ 2^2=4 cases: 00
01
10
11



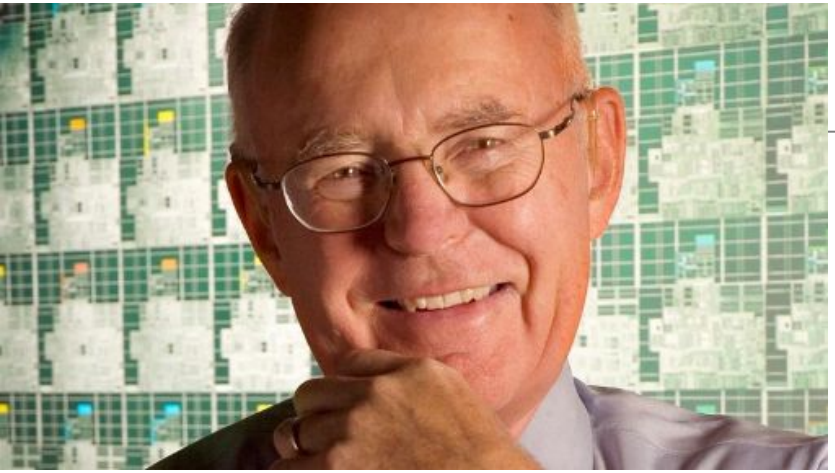
3 Inputs
→ 2^3=8 cases: 000
001
010
011
…



300 Inputs
→ 2^{300}=~10^{90} cases:
00000…00
00000…01
00000…10
00000…11
…

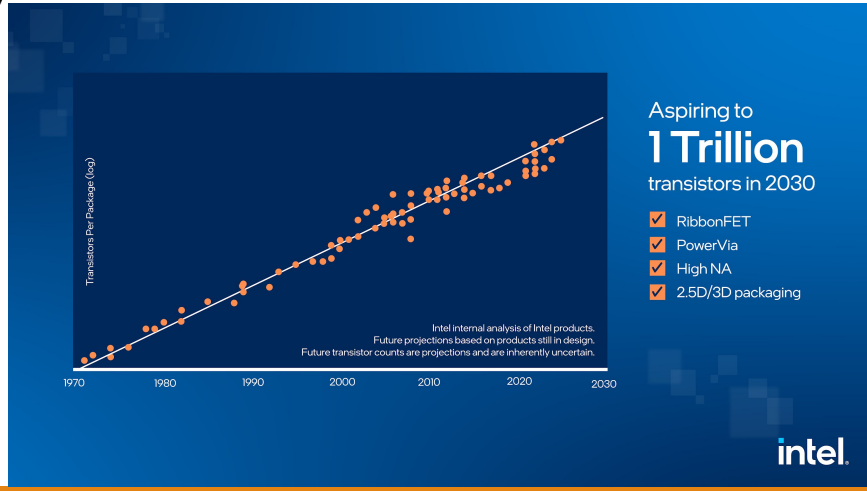
- For comparison: Number of atoms in the universe is approx. ~10^{78}

Past Development in Semiconductors Industry



Exponential growth of integrated circuits! (Moore's Law)

Trend (*log scale*)



Leading to…

Transistors approaching the atomic scale?

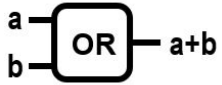
Computer cooling as in nuclear power plants?

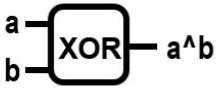
➔ Today‘s technologies are approaching their limits!

Besides that…
Many problems remain hard for today’s computing technologies

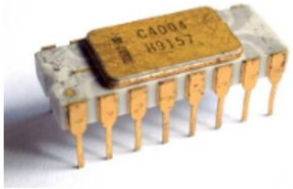
…even with further advancements.

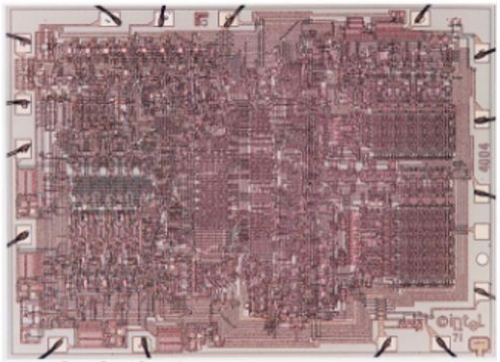
Classical Computing





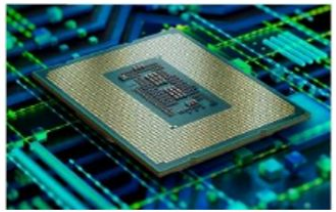
1971
Intel® 4004

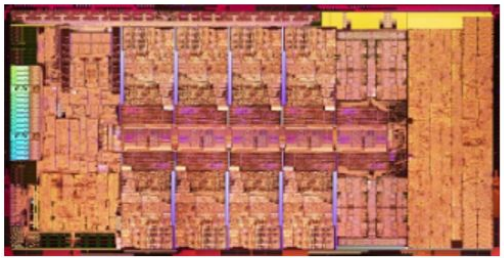




2300	Number of Transistors	Billions
16	Number of Pins	1700
750 kHz	Frequency	5.2 GHz
4-bit	Instruction Set	64-bit
1	Number of Cores	16

2021
12th Generation Intel® Core ™





Conventional vs. Quantum Physics

- Thus far: **Newton‘s Physics**
  - Describe “our world”
  - Based on particles
  - Completely deterministic

$$0 \qquad \text{or} \qquad 1$$

- Now: **Quantum Mechanics**
  - Describe the **smallest „things“** in our Universe (electrons or photons)
  - Described by waves (**wave-particle duality**)

  - Completely probabilistic

$$\alpha_0 \cdot |0\rangle + \alpha_1 \cdot |1\rangle$$
$$\text{with} \quad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

  - **Allows to be in more than on state at one time**
  - Measurement collapses back to single state (back to “classical” world)
  - **True Random**
  - **Entanglement**

Wave-particle duality of matter

- In 1924, **Louis de Broglie (Nobel Prize 1929)** introduced theory of **electron waves s**uggesting that an **electron around a nucleus could be thought of as being a standing wave** and that electrons and all matter could be considered as waves.
- Following de Broglie's proposal of wave-particle duality of electrons, in 1925 **Erwin Schrödinger (Nobel Prize 1933)** developed **the wave equation of motion for electrons** (wave mechanics).
- The **microparticle and its wave function represent the same thing**: the **form of manifestation of the** considered **quantum system** (in this case the microparticle).
- The **wave function represents the probability amplitude of finding the microparticle in the specified position** as a result of observation by an experimenter (measurement).

Conventional vs. Quantum Computing

- **Classical bit:** In basis state 0 or 1

- **Qubit:** Superposition of two basis states
  $\alpha_0 \cdot |0\rangle + \alpha_1 \cdot |1\rangle$ with $|\alpha_0|^2 + |\alpha_1|^2 = 1$
- Measurement leads 0/1 with $|\alpha_0|^2/|\alpha_1|^2$ probability

- Represented in terms of **vectors**

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- **Operations** represented through unitary matrices,
  e.g., $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

- Example

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

- $|0\rangle$ and $|1\rangle$ are **standard computational basis states**
- A 1-qubit system, in general, can be in a state $\boldsymbol{\alpha_0|0\rangle+\alpha_1|1\rangle}$
- $\boldsymbol{\alpha_i}$ **- probability amplitude**, complex number, associated with each computational basis state

Classical Computing

ASM

```
mov r0, #1
mov r1, #1
l:
add r2, r0, r1
str r2, [r3]
add r3, #4
mov r0, r1
mov r1, r2
b l
```

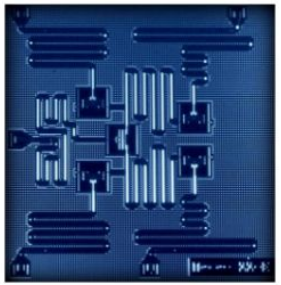
1110
0110
0001
1001

Quantum Computing

QASM

```
OPENQASM 2.0;
include "qelib1.inc";

qreg  q[3];
creg  c[3];
h q[2];
cx q[2], q[1];
cx q[2], q[0];
measure q[2] -> c[2];
```

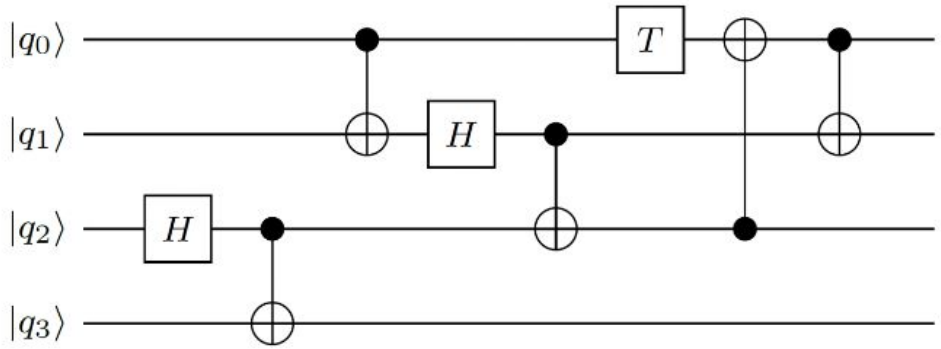


1110
0110
0001
1001

Quantum Circuits / Quantum Software

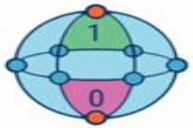
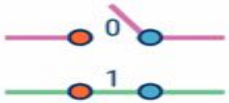
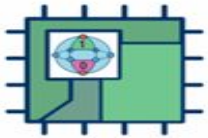
- Cascades of quantum gates working on qubits
- Quantum gates may either be unary gates or working on two gates with a control qubit (black dot) and a target qubit

Quantum assembly (QASM) languages are machine-independent languages that traditionally describe quantum computation in the circuit model.



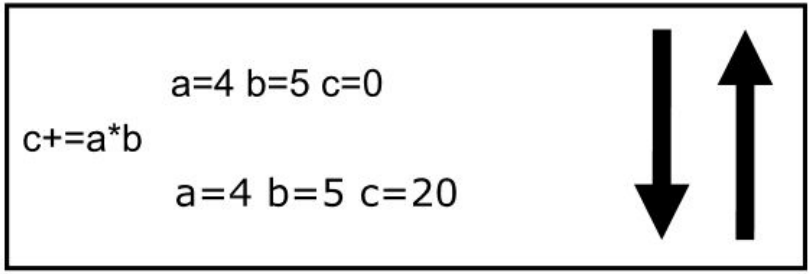

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[4];
h q[2];
cx q[2],q[3];
cx q[0],q[1];
h q[1];
cx q[1],q[2];
t q[0];
cx q[2],q[0];
cx q[0],q[1];
```

Comparison between classic computing and QC

Quantum Computing	Vs.	Classical Computing
 Calculates with qubits, which can represent 0 and 1 at the same time		Calculates with transistors, which can represent either 0 or 1 
 Power increases exponentially in proportion to the number of qubits		Power increases in a 1:1 relationship with the number of transistors 
 Quantum computers have high error rates and need to be kept ultracold		Classical computers have low error rates and can operate at room temp 
 Well suited for tasks like optimization problems, data analysis, and simulations		Most everyday processing is best handled by classical computers 

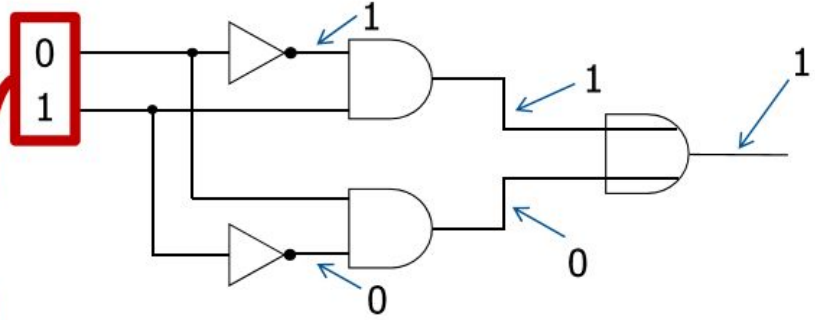
Challenges (examples)

- "Programming" (different paradigms)
- Every quantum operation is inherently reversible



- Not to mention
  - Dealing with "0 and 1 at the same time"
  - Understanding/Handling quantum operations
  - Physical constraints
  - Error correction
  - …

- Simulation



$$|\psi\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix}$$

Exponential complexity

Already simple tasks are substantially harder for quantum computing than for conventional circuits/systems

- Further:
  - Interdisciplinarity
  - Terminology and Formalizations

Complexity (I)

$|\psi\rangle$

$$\begin{bmatrix} \alpha_0 \\ \vdots \\ \vdots \\ \alpha_{N-1} \end{bmatrix}$$

Where is the catch?

$|0 \ldots 0\rangle$ ➡ $N = 2^n$

n qubits

$$\begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \quad \begin{bmatrix} \alpha_{0\ldots0} \\ \vdots \\ 2^{12} \\ \vdots \\ \alpha_{1\ldots1} \end{bmatrix} \quad \begin{bmatrix} \alpha_{0\ldots0} \\ \vdots \\ 2^{22} \\ \vdots \\ \alpha_{1\ldots1} \end{bmatrix} \quad \begin{bmatrix} \alpha_{0\ldots0} \\ \vdots \\ 2^{32} \\ \vdots \\ \alpha_{1\ldots1} \end{bmatrix} \quad \begin{bmatrix} \alpha_{0\ldots0} \\ \vdots \\ 2^{42} \\ \vdots \\ \alpha_{1\ldots1} \end{bmatrix} \quad \begin{bmatrix} \vdots \\ 2^{305} \\ \vdots \\ \alpha_{1\ldots1} \end{bmatrix}$$

#qubits	2	12	22	32	42	305
memory	64B	64KiB	64MiB	64GiB	64TiB	
		L1 cache	L3 cache	RAM	HPC	

Complexity – storage requirements

$$n \text{ qubits} \rightarrow 2^{(n+4)} \text{ Bytes}$$

- **For 1 qubit** there are necessary 2 (**alpha_0** and **alpha_1**) complex coefficients (each having **Real** part and **Imaginary** part) => 4 real values (each represented on 8B – double precision, or depending on the target architecture) => **32B memory requirement**

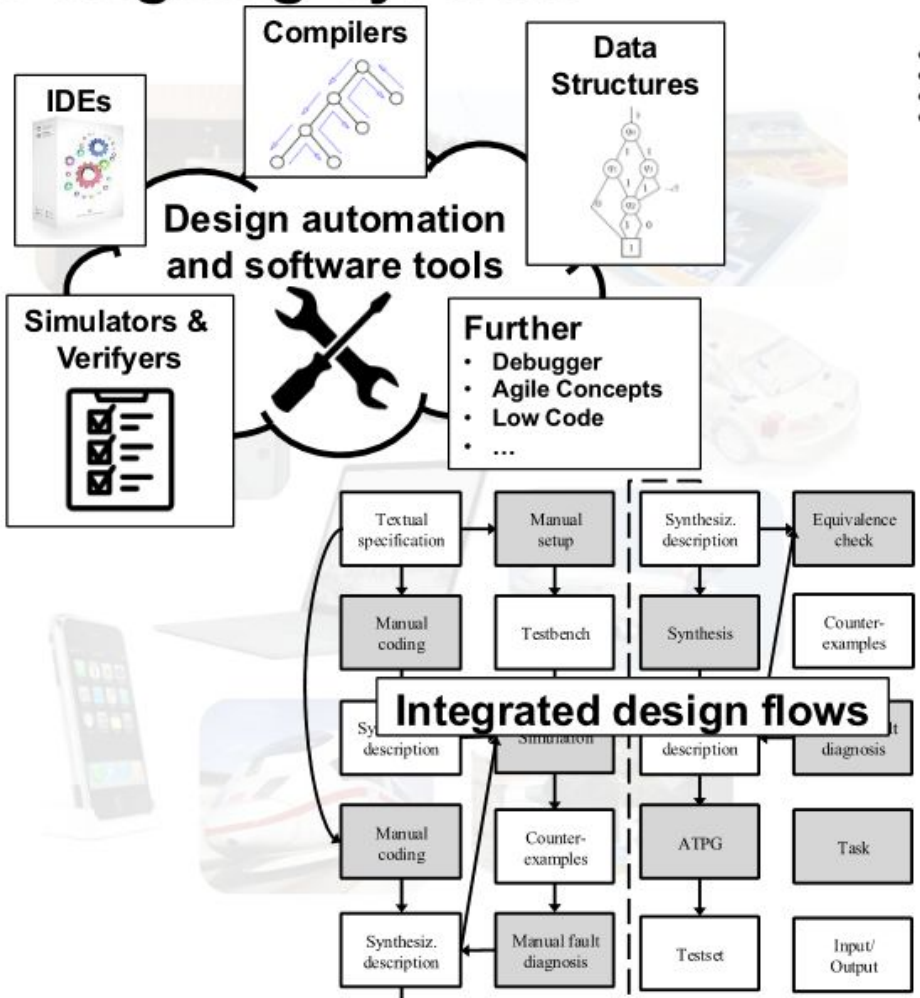
- For **2 qubits** there are necessary 4 (**alpha_00**, **alpha_01, alpha_10**, **alpha_11**)) complex coefficients (each having Real part and Imaginary part) => 8 real values (each represented on 8B – double precision, or depending on the target architecture) => **64B memory requirement**.

- For **n qubits** there are necessary **2^n** (**alpha_00…00**, **alpha_00…01, alpha_00…10**, **alpha_00…11, …, alpha_11…11** – on **n** position) complex coefficients (each having Real part and Imaginary part) => 2***2^n** real values (each represented on 8B – double precision, or depending on the target architecture) => **2^(n+4) Bytes memory requirement**.

Quantum Computing: The 21st century technology

- Huge interest…
  - from big Players: IBM, Google, Microsoft, Amazon, …
  - from Startups: AQT, Rigetti, IonQ, …
- Exponential improvements in the best case
  - Integer factoring in polynomial time
  - Break current internet cryptography
- Various further application domains
  - Nature
  - Optimization
  - Finance
  - Machine Learning
  - …

Designing Systems



- **Classical Systems**
  - Are enormously **complex**
  - Rely on efficient and scalable **design automation methods and software**
  - Integrated into powerful **design flows**
  - Have been developed and optimized **over the past decades**

Designing Quantum Systems

- **Classical Systems**
  - Are enormously **complex**
  - Rely on efficient and scalable **design automation methods and software**
  - Integrated into powerful **design flows**
  - Have been developed and optimized **over the past decades**

- **Quantum Systems**
  - Similar tasks (simulation, compilation, etc.), but **substantially different** paradigm
  - **Initial solutions** are available
  - **Do not** fully exploit the decades of experiences in **design automation**

We may end up in a situation where we have quantum computers but no methods to use them

Overview: Software Tooling for Quantum

- Programming Language: Python
- Different categories of SDK providers
  - Quantum SDK and Quantum Computers (e.g., IBM/Qiskit, Google/Cirq, Quantinuum/Pytket, Xanadu/Pennylane, …)
  - Quantum SDK and platform (e.g., Microsoft Azure, AWS Braket, …)
  - Only Quantum SDK (e.g., MQT, Classiq, …)
- Functionalities of SDKs similar with differences in the details, such as syntax, supported simulators/quantum computers, …
- Simulator vs. actual Quantum Computer
- Some have special foci:
  - Pennylane: Quantum Machine Learning
  - Classiq: High-Level Software Generation
  - …

Qiskit

Cirq

QUANTINUUM

Azure

aws

Amazon Braket

MUNICH QUANTUM TOOLKIT

PENNYLANE

CLASSIQ

The Munich Quantum Toolkit (MQT)

Application

- Workflow from classical problem to quantum solution
- Automated encoding, execution & decoding

Compilation

- Automatic device selection
- Compiler optimization
- Technology-specific compilation
- Reversible synthesis

Error Correction

- Decoding algorithms
- Fault-tolerant state preparation
- Automated code construction and numerical simulations

Application → Simulation → Compilation → Verification → Error Correction → Hardware

Simulation

- Classical simulation of quantum circuits based on decision diagrams
- Includes sampling, noise-aware simulation, Hybrid Schrödinger Feynman approaches, approximation strategies, expectation value computations, etc.

Verification

- Equivalence checking
- Verifying compilation results

Hardware

- Application specific physical design for superconducting platform

Data Structures & Core Methods

- Efficient data structures
- Dedicated core methods (optimal and heuristic)
- Based on C++ and Python

Decision Diagrams · Tensor Networks · ZX-Calculus · SAT/SMT Solvers · Machine Learning · Heuristics

Check it out!

https://mqt.readthedocs.io

All tools are available as open-source repositories on GitHub under the MIT license

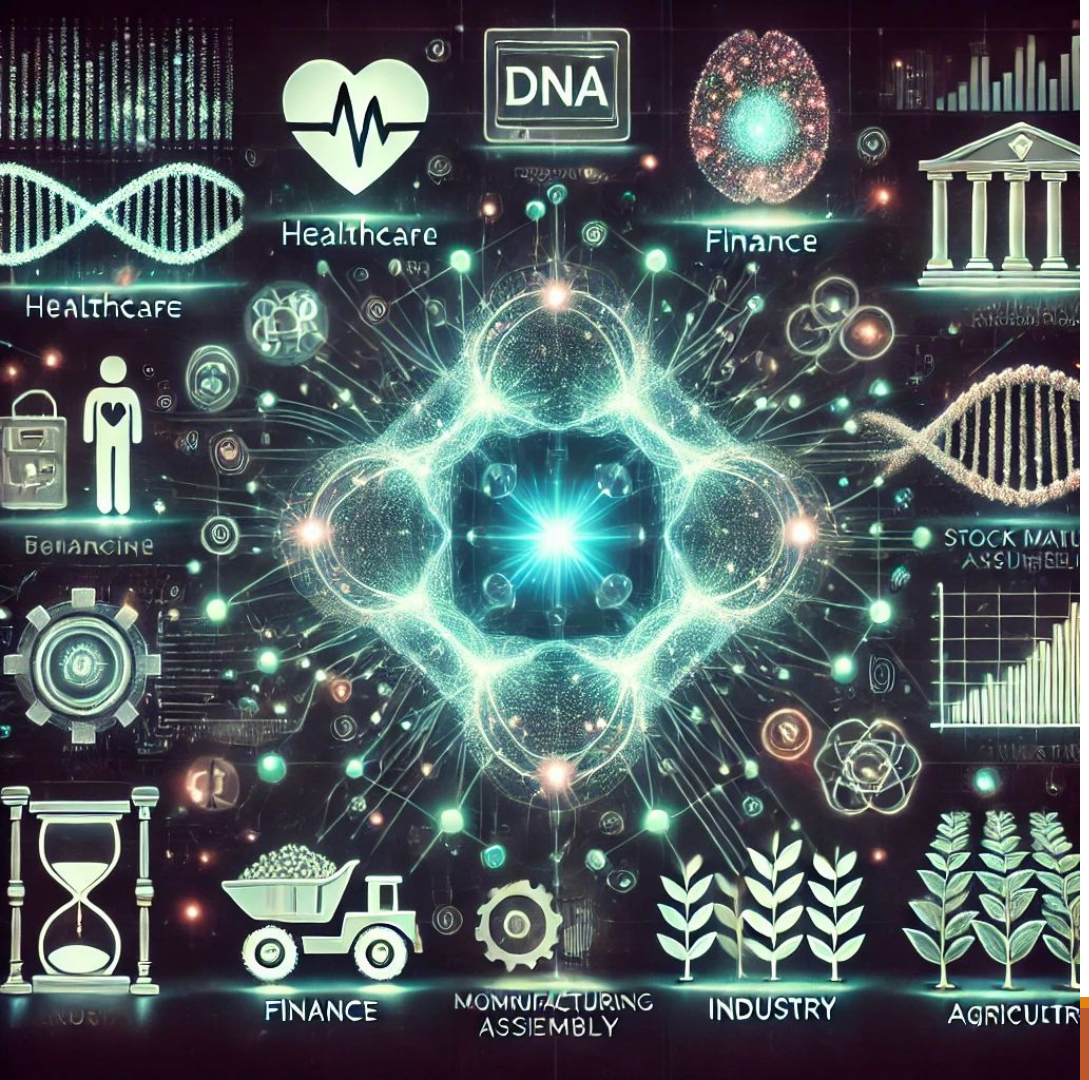
Access to Quantum Computers

- Always using APIs over the internet
- Quantum circuits are created on classical computers,
- sent to the quantum computing provider,
- executed on an actual quantum computer, and
- the results are sent back to the user.

- Like IBM, AWS is offering access to many devices already today:

○	IonQ	IonQ Device	03:07:22	Universelle Gate-Modell-QPU basierend auf gefangenen Ionen
○	Oxford Quantum Circuits	Lucy	00:07:21	Universelle Gate-Modell-QPU basierend auf supraleitenden Qubits
○	QuEra	Aquila	4 days 06:07:22	Analoger Quantenprozessor basierend auf neutralen Atom-Arrays
○	Rigetti	Aspen-11	OFFLINE	Universelle Gate-Modell-QPU basierend auf supraleitenden Qubits
○	Rigetti	Aspen-M-2	05:07:21	Universelle Gate-Modell-QPU basierend auf supraleitenden Qubits
○	Xanadu	Borealis	05:07:22	Gaußsches Boson-Sampling auf einem programmierbaren photonischen Prozessor

- Pricing: Fix costs plus variable costs depending on number of shots
  - Rigetti via AWS: $0.30 / task + $0.00035 / shot
  - IonQ via AWS: $0.30 / task + $0.01 / shot



Uses of *Quantum Computing* across industries: Healthcare, Finance, Cybersecurity, Blockchain, Artificial Intelligence, Industry, Agriculture, National Security

Uses of Quantum Computing across Industries: Healthcare, Finance, Industry, Agriculture

HEALTHCARE

- **Modelling biomolecular and chemical reactions with QC. Google** announced that it had **used a quantum computer to simulate a chemical reaction** (September 4, 2020).
- **Future quantum computers are predicted to be able to simulate complex molecular interactions much more accurately** than classical computers. Within healthcare, this could help **speed up drug discovery efforts** by making it easier to **predict the effects of drug candidates**.
- **Using QC for protein folding** and make **designing powerful protein-based medicines** easier!

Uses of Quantum Computing in Healthcare

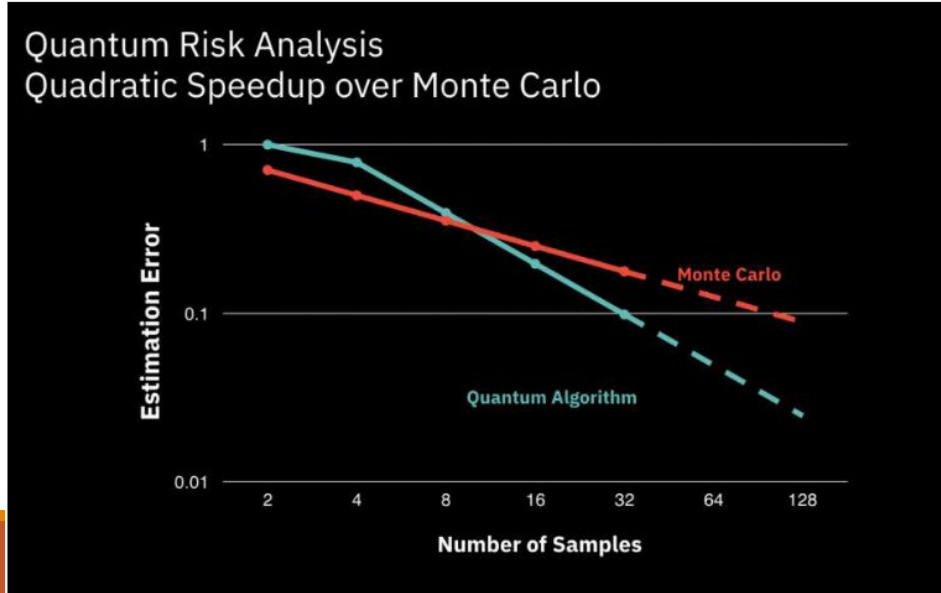
- **Quantum computing** could lead to better approaches to **personalized medicine** by allowing **faster genomic analysis to inform tailored treatment plans specific to every patient!**
- **Sending sensitive information securely** anywhere or **diagnosing diseases faster and more accurately** just by looking inside cells!
- **Genome sequencing creates lots of data**, **meaning** that analysing a person's DNA requires **a lot of computational power**. **Companies are** already **reducing the cost and resources needed to sequence the human genome**; => but a **powerful quantum computer could sift through this data much more quickly**, making genome sequencing more efficient and easier to scale.

Uses of Quantum Computing in Finance (I)

- **Quantum computers could help computational models** that make assumptions about the way markets and portfolios will perform **by parsing through data more quickly, running better forecasting models, and more accurately weighing conflicting possibilities.**
- **QC could solve complex optimization problems** related to tasks **like portfolio risk optimization** and **fraud detection.**
- **Another area of finance that quantum computers could change are Monte Carlo simulations—a probability simulation used to understand the impact of risk and uncertainty in financial forecasting models.**

Uses of Quantum Computing in Finance (II)

- Another area of finance that **quantum computers could change** are **Monte Carlo simulations –** a probability simulation **used to understand the impact of risk and uncertainty in financial forecasting models.**



Source IBM

Uses of Quantum Computing in Cybersecurity (I)

- Cybersecurity could be affected by quantum computing.
- **Powerful quantum computers threaten to break cryptography techniques like RSA encryption**, commonly used today to keep sensitive data and electronic communications secure.
- **Shor's algorithm**, a quantum algorithm theorized in 1994, **describes how a suitably powerful quantum computer** (that could emerge around 2030) **could very quickly find the prime factors of large numbers**, a task that classical computers find extremely difficult. RSA encryption relies on this challenge to protect data being shuttled around online.
- But **several companies (NXP Semiconductors) are emerging to counter this threat by developing new encryption methods**, collectively known as "***post-quantum cryptography***" – creating a problem that even a powerful quantum computer wouldn't be expected to have many advantages in trying to solve.

Adoption by companies of PQC - post-quantum cryptography

Business Wire
https://www.businesswire.com › ... · Traducerea acestei pagini

QuSecure Launches Crypto-Agile Post-Quantum ...

14 mar. 2024 — Leveraging advanced **crypto-agile post-quantum cryptography**, QuProtect Core **Security** offers a seamless and robust **security** layer, delivering best ...

QuSecure

FORBES > INNOVATION > CYBERSECURITY

Google Confirms New Quantum Encryption For Chrome Is Coming Nov. 6

Davey Winder Senior Contributor

Davey Winder is a veteran cybersecurity writer, hacker and analyst.

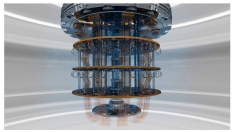
Sep 18, 2024, 03:49am EDT

daily.dev
https://app.daily.dev › posts · Traducerea acestei pagini

IBM adds quantum-resistant controls within new security suite

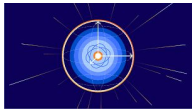
22 oct. 2024 — **IBM** has introduced the Guardian Data **Security** Center to help organizations protect against AI and **quantum**-computing threats.

NXP
Post-Quantum Cryptographic Migration Challenges for Embedded Devices



The Cloudflare Blog
https://blog.cloudflare.com › post-quantum-to-origins

Cloudflare now uses post-quantum cryptography to talk to ...



The Hacker News
https://thehackernews.com › ... · Traducerea acestei pagini

Google Chrome Switches to ML-KEM for Post-Quantum ...

17 sept. 2024 — **Google has announced that it will be switching from KYBER to ML-KEM** in its Chrome web browser as part of its ongoing efforts to defend against the risk posed ...

WIRED
https://www.wired.com › ap... · Traducerea acestei pagini

Apple's iMessage Is Getting Post-Quantum Encryption

21 feb. 2024 — **Apple** is launching its first **post-quantum** protections, one of the biggest deployments of the future-resistant **encryption** technology to date.

Uses of Quantum Computing in Cybersecurity (II)

The quantum paradigm is a "mixed blessing" in such context.

The bad side

Shor's algorithm: severe impact on public-key cryptography
breaks RSA, D-H, ECC in polynomial time

Grover's algorithm: improves brute-force attacks
quadratic speed-up, weakens security of AES

This looks discouraging, however...

The good side

Exploiting quantum phenomena gives us perfect security.

Uses of Quantum Computing in Cybersecurity (III)

- **NIST releases first 3 finalized Post-Quantum encryption standards** (more quantum-resistant public-key cryptographic algorithms) - https://csrc.nist.gov/projects/post-quantum-cryptography.
- Quantum Key Distribution (QKD) technology could offer some respite from quantum computers' code-breaking abilities.
- **QKD works by transferring encryption keys using entangled qubits**. Since quantum systems are altered when measured, it's possible to check if an eavesdropper has intercepted a QKD transmission. Done right, this means that **even quantum computer-equipped hackers would have a hard time stealing information**.
- Though **QKD currently faces practical challenges like the distance over which it is effective** (most of today's QKD networks are pretty small), many are expecting it to soon become a big industry.
- The **RONAQCI** project aims to **develop a 1500 km quantum communications network with QKD**, the largest in Europe, with 36 links, in parallel with the RoEduNet optic fiber network.

Briefly characterize the quantum communication

- Comunicarea cuantică este metoda de transfer a stărilor cuantice dintr-un loc în altul. Ideea generală este că stările cuantice codifică informația cuantică: prin urmare, **comunicarea cuantică implică și transmiterea de informații cuantice și distribuția resurselor cuantice precum inseparabilitatea**.
- Comunicarea cuantică acoperă aspecte care variază de la fizica de bază la aplicații practice care sunt relevante pentru societatea de astăzi. Din punct de vedere aplicativ, un interes major s-a concentrat asupra distribuției cheilor cuantice (QKD), deoarece aceasta oferă o modalitate sigură de a stabili o cheie confidențială între parteneri aflați la distanță. Acest lucru are potențialul de a rezolva problemele de securitate fundamentale și de lungă durată din societatea bazată pe informație, precum și problemele emergente asociate stocării sigure pe termen lung (de exemplu, pentru dosarele de sănătate și infrastructură) și va fi esențială pentru operarea securizată a aplicațiilor care implică Internetul lucrurilor (IoT) și cloud.

What are the methods to quantum secure encryption schemes? (I)

- Broadly speaking, **there are three methods to quantum secure encryption schemes**:
  1. O metodă este să se continue să se utilizeze **criptografia tradițională cu cheie publică**, dar să se dezvolte algoritmi alternativi pentru a rezista atacurilor cuantice. Această metodă este numită criptografie postcuantică (**postquantum cryptography PQC**).
     - Meritul său tehnologic este că poate fi compatibilă cu criptoinfrastructura existentă, și asigură rate ridicate pe distanțe lungi.
     - Un neajuns al PQC este că algoritmii dezvoltați s-au dovedit a fi siguri numai împotriva atacuri cuantice cunoscute. Acest lucru poate duce la vulnerabilități de securitate viitoare cu potențial dezastruos pentru informațiile transmise astăzi.

What are the methods to quantum secure encryption schemes? (II)

2. A doua metodă este comunicarea directă securizată cuantică (**quantum secure direct communication QSDC**). QSDC permite utilizatorilor a transmite direct informații private prin canale cuantice securizate, fără distribuire securizată a cheilor. Datorită pașilor săi de comunicare relativ simpli, QSDC a atras o mare atenție și a cunoscut o dezvoltare rapidă în ultimele două decenii. Cu toate acestea, ratele atinse ale QSDC sunt mai mici decât ale altor scheme de criptare securizată cuantică.

What are the methods to quantum secure encryption schemes? (III)

3. O altă metodă este distribuția cuantică a cheii (**quantum key distribution QKD**). Securitatea necondiționată a QKD a fost riguros dovedită pe baza legilor fundamentale ale cuanticii, cum ar fi inseparabilitatea cuantică și teorema de ne-clonare. Astfel, siguranța sa este independentă de îmbunătățiri viitoare ale capacității de calcul și ale algoritmilor. QKD combinat cu PQC este schema tipică de securitate cuantică a cărei siguranță poate fi în prezent demonstrată teoretic. Această schemă poate descoperi instantaneu comportamente și evenimente care interceptează comunicația și poate realiza securitate ridicată în sisteme de criptare de înaltă performanță..

What are the main approaches in implementing QKD (quantum key distribution)?

- O implementare QKD constă din trei părți:
  - **sursă, canal și detecție** iar diferitele scheme de codificare sau decodificare sunt incorporate în aceste trei părți.
- Există în mod normal **două tipuri de canale în aplicațiile practice**: **spațiu liber** și **fibre optice**. Teoretic, siguranța sistemului nu se bazează pe implementarea fizică a canalelor cuantice.
- Din punct de vedere tehnic, **QKD la nivel metropolitan poate profita de canalele existente și infrastructurile asociate**. Astfel, majoritatea cercetărilor privind QKD integrat s-au concentrat pe surse, modulatori, și circuite. Aici, se acordă în principal atenție dispozitivelor funcționale ale sursei, detecției, codificării și decodării.

Quantum key distribution

Unlike computationally secure schemes, QKD is provably secure [2].

A secret key is established to be used with a symmetric cipher.

BB84 protocol

- first QKD scheme, C. H. Bennett and G. Brassard [3]
- based on the conjugate coding proposal
- relies on the uncertainty principle and no-cloning theorem

Further developments

- B92 [4]
- E91 [5]
- SARG04 [6]

Uses of Quantum Computing in Blockchain & Cryptocurrencies (I)

- **Quantum computing's threat to encryption extends to blockchain tech and cryptocurrencies**—including Bitcoin and Ethereum—which rely upon quantum-susceptible encryption protocols to complete transactions.
- Though **specific quantum threats to blockchain-based projects vary**, the **potential fallout could be severe**.
  - **About 25% of bitcoins** (worth $173B+) **are stored so that they could be easily stolen by a quantum computer-equipped thief** (analysis from Deloitte).
  - **Quantum computers could** eventually become powerful enough to **decrypt and interfere with transactions before they're verified by other participants on the network**, undermining the integrity of the decentralized system.

Uses of Quantum Computing in Blockchain & Cryptocurrencies (II)

- **Blockchain technology is being increasingly used for** applications in **asset trading, supply chains, identity management**, and more. **Worried by the profound risks posed by quantum computers, a number of players are moving to make blockchain tech safer**.
  - **Bitcoin and Ethereum are experimenting with a new blockchain protocol** called the **Quantum Resistant Ledger** that's specifically designed to counter quantum computers.
  - **Quantum-resistant blockchains may not fully emerge until post-quantum cryptography standards are more firmly established** in the coming years.
  - **Startups** including QuSecure and Qaisec **are working on quantum-resistant blockchain tech for enterprises**.

Quantum Inspired Evolutionary Algorithms (I)

```
begin
    t ← 0
        initialize Q(t)     // Q(t) is population of quantum chromosomes at generation t
        make P(t) by observing Q(t) states // binary solutions P(t) is formed by observing Q(t)
        evaluate P(t)
        store the best solution among P(t)
        while (not termination-condition ) do
        begin
            t ← t+1
            crossover and mutate to update P(t)
            evaluate P(t)
            store the best solution among P(t)
            update Q(t) to get Q'(t)
            make P'(t) by observing Q'(t) states
            select in {P(t) ∪ P'(t)} to get new P(t)
        end
end
```

Quantum Inspired Evolutionary Algorithms (II)

- QEA is a probabilistic algorithm similar to EA. It maintains a population Q(t) = $\{q_1^t, q_2^t, \dots, q_n^t\}$ at generation *t*, where *n* is the size of the population, and q_j^t is a quantum chromosome which is defined as:

  $q_j^t = \begin{pmatrix} \alpha_1^t \alpha_2^t \dots \alpha_m^t \\ \beta_1^t \beta_2^t \dots \beta_m^t \end{pmatrix}$, where $j \in \{1, 2, \dots, n\}$ and *m* is the chromosome length.
- Compared with EA, two steps "*observe Q(t)*" and "*update Q(t)*" are added.
- In "*observe Q(t)*", the binary solutions P(t) is formed by observing Q(t), as is described bellow:
  - For each bit of the chromosome, generate a random real number $p \in [0,1]$.
  - If $p > |\alpha_i|^2$, the corresponding bit in P(t) takes "1"; else "0".

- In the "*update Q(t)*", one can use different methods to evolve *Q(t)*,for example, generate Q(t) in a random way, and generate Q(t) by evolutionary operator, or apply some suitable quantum gates to produce *Q(t)*.
- If a quantum gate is designed, the transform matrix must be a unitary matrix.
- The **most commonly used** matrixes are **Control-not** gate (CNOT), **Rotation** (Rx(θ)) and **Hadamard** (H) gate.

Quantum Machine Learning Algorithms for QC

- Quantum computers have abilities to **parse through massive data sets, simulate complex models, and quickly solve optimization** problems.
- Besides that **QML provides** some commercial advantages, future quantum computers could develop AI even further.
- AI that taps into quantum computing could advance tools like computer vision, pattern recognition, voice recognition, machine translation, and more.
- Quantum computing may even help create AI systems that act in a more human-like way (e.g., enabling robots to make optimized decisions in real-time and more quickly adapt to changing circumstances or new situations).
  - Google develops machine learning tools that combine classical computing with quantum computing and expects these tools to work with near-term quantum computers.
  - Quantum software startup Zapata recently stated that it considers quantum machine learning one of the most promising commercial applications for quantum computers in the short term.

Quantum Computing for Optimization of Logistics (I)

- A **complex optimization problem** that would take **a supercomputer thousands of years** to solve could be handled by **a quantum computer in just a matter of minutes**.
- Given the extreme **complexities and variables involved in international shipping routes** and orchestrating supply chains, **quantum computing** could be well-placed to help tackle **daunting logistics challenges**.
- **DHL is already looking for quantum computers** to help it **more efficiently pack parcels and optimize global delivery routes**. The company is hoping to increase the speed of its service while also making it easier to adapt to changes — such as cancelled orders or rescheduled deliveries.
- Others want to **improve traffic flows using quantum computers**, a capability that could help **delivery vehicles make more stops in less time**.

Quantum Computing for Optimization of Logistics (II)

Source: Volkswagen

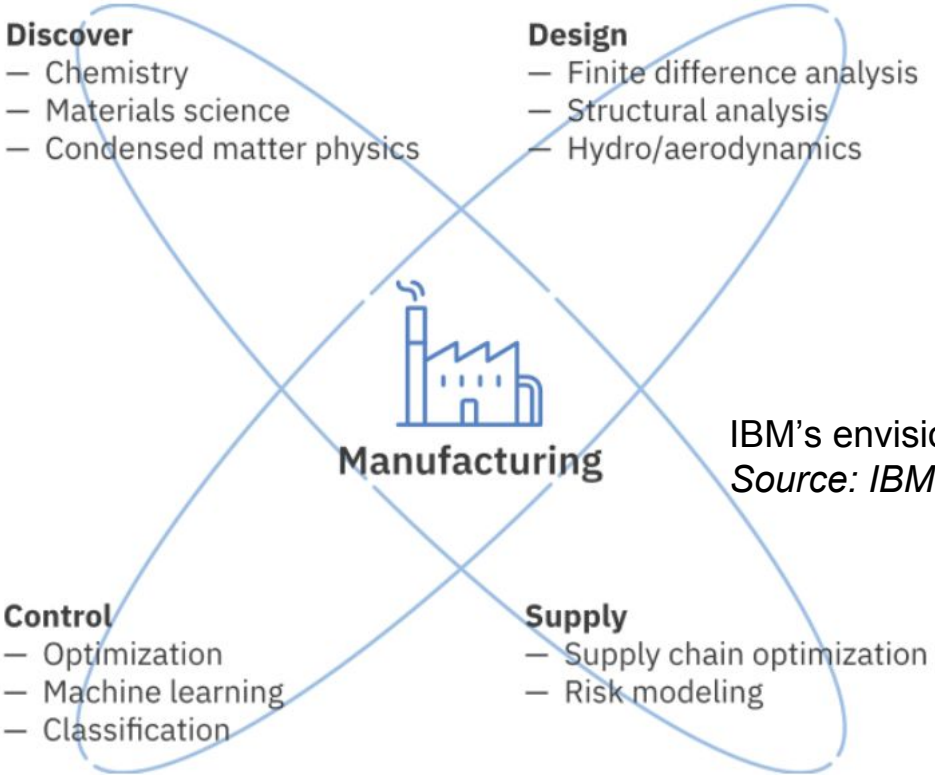
- In the **automotive industry, Volkswagen Group** has led the way, **launching a dedicated team for quantum computing research in 2016**.
- In 2019, the **Volkswagen team worked with D-Wave** to **demonstrate the first live traffic-routing system to rely on quantum computing**. The test used buses in **Lisbon**, Portugal, to **predict traffic volumes and route trips** to **minimize passenger wait times and bus travel times**, avoid traffic jams, and make the traffic flow as efficient as possible.
- Using a new **algorithm powered by quantum computing, designed to maximize the paint shop efficiency without slowing assembly overall**, the shops could now run significantly more vehicles in a row.

- The **Volkswagen** team has also **applied quantum computing** to:
  - **vehicle pricing** to help strike the right balance for customer demand.
  - **developing new materials**
  - **figuring out where new electric vehicle charging stations should be located** to maximize their usefulness.

Quantum Computing for Manufacturing & Industrial Design (I)

- **Airbus** - a global **aerospace corporation - established a quantum computing unit in 2015** and has also invested in **quantum software startup QC Ware** and **quantum computer maker IonQ**.
- Airbus is looking at **quantum annealing for digital modelling and materials sciences**. For instance, **a quantum computer could filter through countless variables in just a few hours to help determine the most efficient wing design for an airplane**.
- **IBM** has also **identified manufacturing as a target market for its quantum computers**, with the company highlighting areas like **materials science, advanced analytics for control processes, and risk modelling** as key applications for the space.

Quantum Computing for Manufacturing & Industrial Design (II)



Though quantum computing will likely be implemented in manufacturing only gradually as more powerful machines emerge over the coming years, some companies — including **machine learning startup Solid State AI is already offering quantum supported services for the industry**.

IBM's envisioned manufacturing applications for quantum computing.
Source: IBM

Quantum Computing for Boosting Agriculture (I)

- **Quantum computers could help to produce fertilizers more efficiently.**
  - ✔ Nearly all of the fertilizers used in agriculture around the world rely on ammonia. **The ability to produce ammonia (or a substitute) more efficiently would mean cheaper and less energy-intensive fertilizers**. In turn, easier access to better fertilizers could **help feed the planet's** growing population. Ammonia is in high demand and is estimated to be a $77B global market by 2025 (CB Insights).
- **Little recent progress** has been made on improving the process to create or replace ammonia **because the number of possible catalyst combinations that could help us do so is extremely large** — meaning that we essentially still rely on an energy-intensive technique from the 1900s.

Quantum Computing for Boosting Agriculture (II)

- **Using today's supercomputers to identify the best catalytic combinations to make ammonia would take centuries to solve**. However, **a powerful quantum computer could be used to much more efficiently analyze different catalyst combinations**—another application of simulating chemical reactions—and help find a better way to create ammonia.

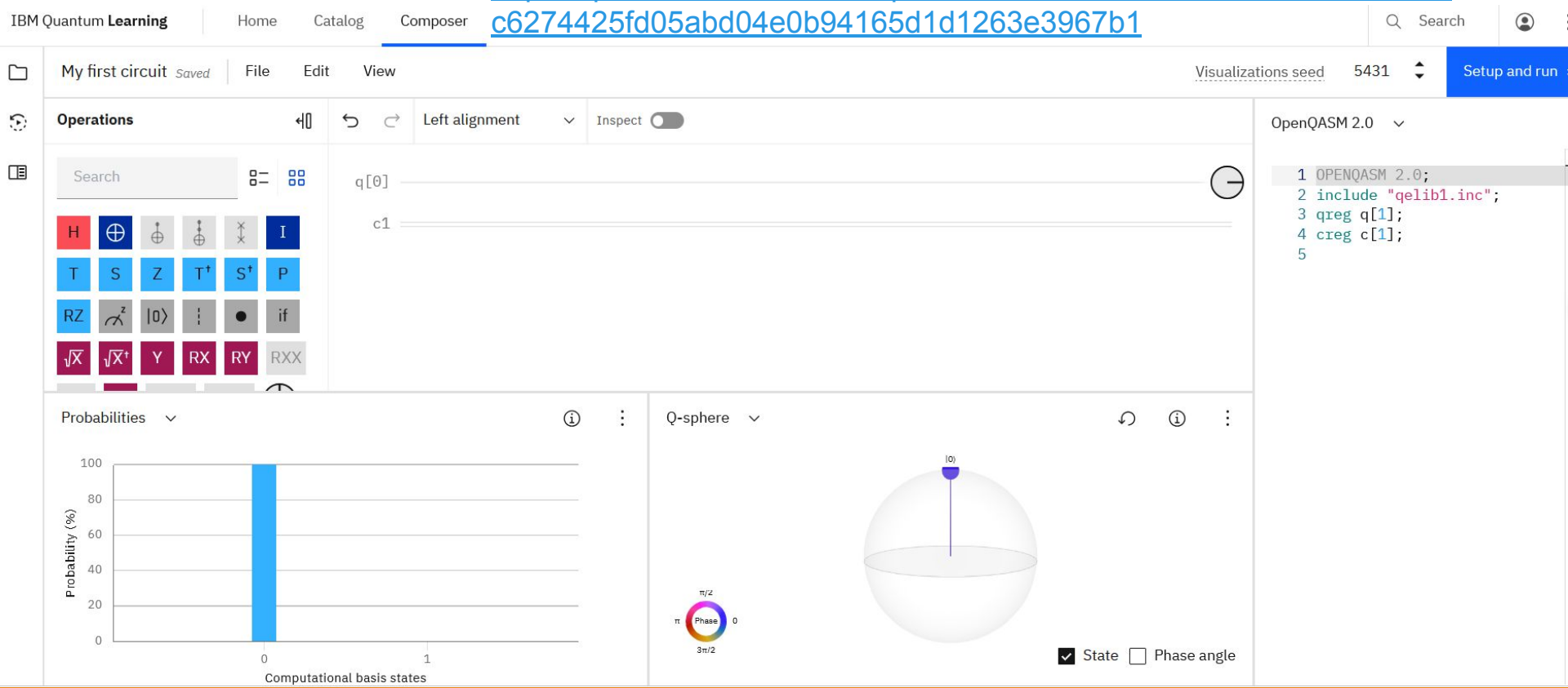
- **Bacteria in the roots of plants make ammonia every day with a very low energy cost using a molecule called nitrogenase**. **This molecule is beyond the abilities of our best supercomputers to simulate and hence better understand**, but it could be within the reach of a future quantum computer.

Quantum Computing for bolstering National Security

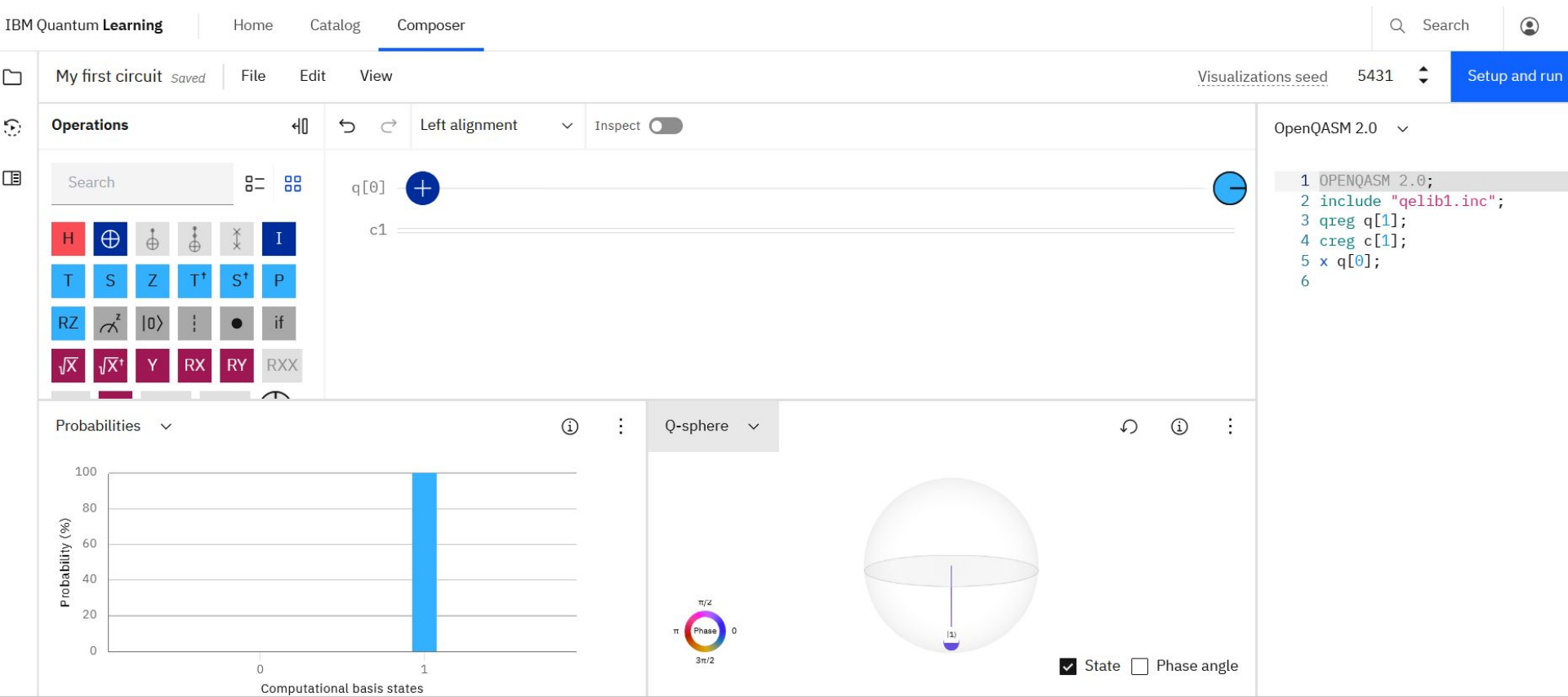
- **Defence applications for quantum computers** could include among many others:
  - **code breaking for spying**
  - **running battlefield simulations**
  - **designing better materials for military vehicles.**
- **US government announced $625M investment in quantum technology research institutes** run by the Department of Energy.
- **China's government has put billions of dollars behind numerous quantum technology projects**, and a team based in the country **recently claimed** to have **achieved a quantum computing breakthrough.**
- **Though it is uncertain when quantum computing may play an active role in national security,** it is beyond doubt that **no country will want to fall behind the capabilities of its rivals.** A new **"arms race"** has already begun.

IBM Quantum Composer (I)

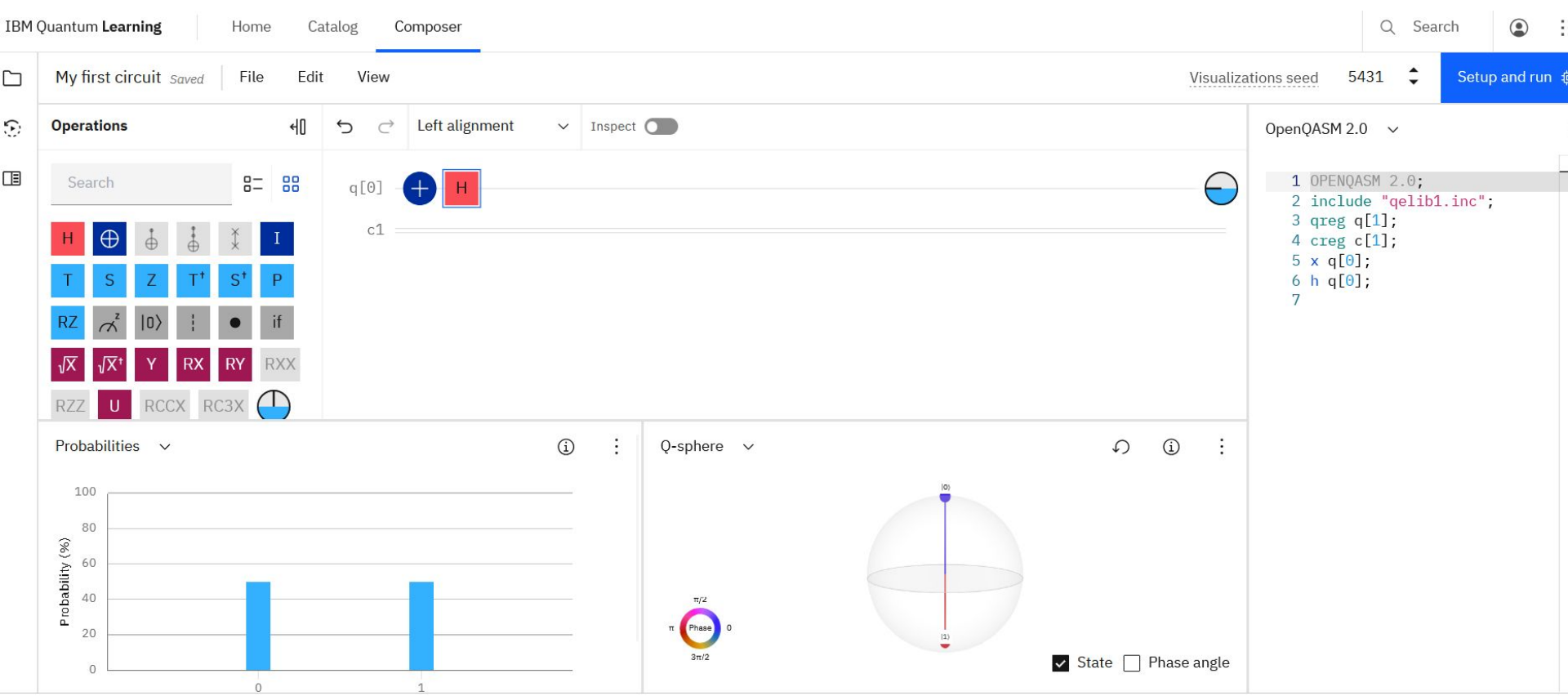
https://quantum.ibm.com/composer/files/3bdca771f37320b9482ea6246c6274425fd05abd04e0b94165d1d1263e3967b1



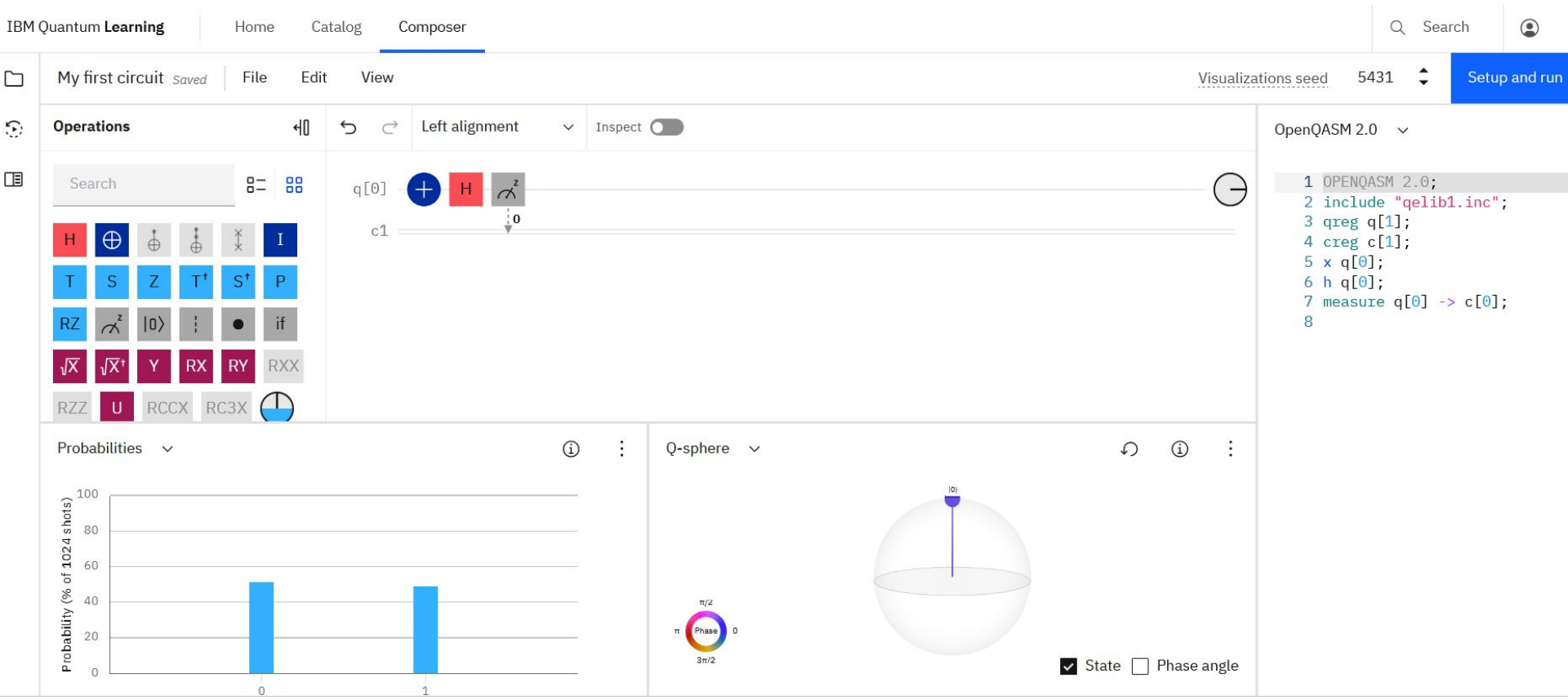
IBM Quantum Composer (II)



IBM Quantum Composer (III)



IBM Quantum Composer (IV)



How to learn about Quantum Information

Simplified description

- Simpler and typically learned first
- Quantum states represented by *vectors*
- Operations are represented by *unitary matrices*
- Sufficient for an understanding of most

General description

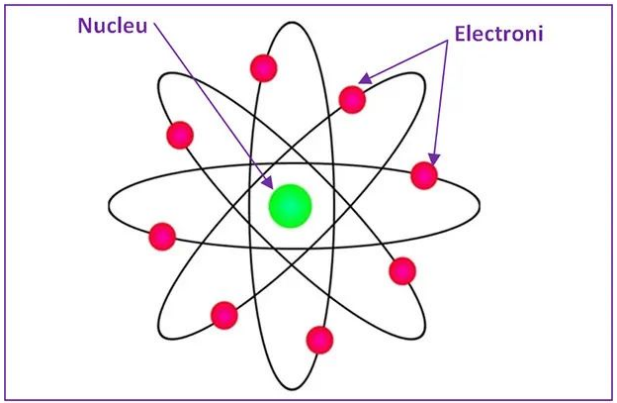
- More general and more broadly applicable
- Quantum states represented by *density matrices*
- Allows for a more general class of measurements and operations
- Included both the *simplified description* & *classical information* as special cases

The Qubit

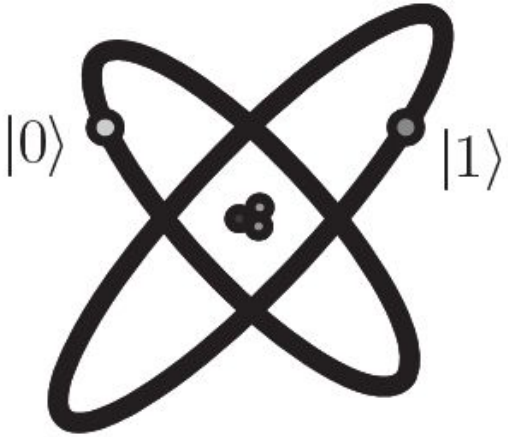
Information Fundamental Unit (Abstract)

- Bit: 0 or 1
  - Voltage;
  - Magnetic fields;
  - Etc…;

- Qubit: Simplest Quantum System
  - Atoms;
  - Photons;
  - Etc…;



Qubits, the quantum version of bits used in classical computing, **are the basic units of information in a quantum computer**.



Qubit represented by two electronic levels in an atom

Dirac notation (first part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $|a\rangle$ the *column vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Example 1

If $\Sigma = \{0, 1\}$, then

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Dirac notation (II)

Example 2

If $\Sigma = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, then we might choose to order these states like this: $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$. This yields

$$|\clubsuit\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |\diamondsuit\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |\heartsuit\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |\spadesuit\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

- Also known as **Bra–ket notation**, is a notation for linear algebra and linear operators on complex vector spaces introduced as an easier way to write quantum mechanical expressions!

Measuring probabilistic states

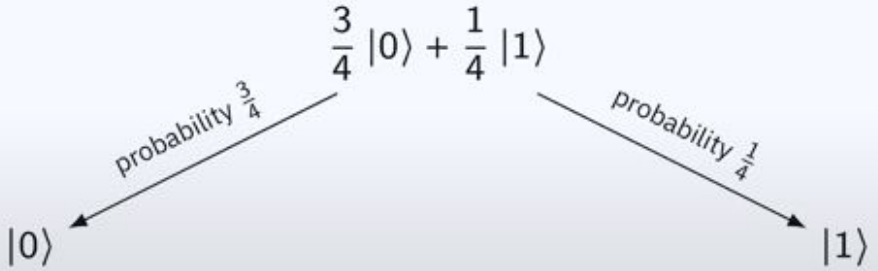
Example

Consider the probabilistic state of a bit X where

$$\Pr(X = 0) = \frac{3}{4} \quad \text{and} \quad \Pr(X = 1) = \frac{1}{4}$$

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} \begin{array}{l} \longleftarrow \text{entry corresponding to 0} \\ \longleftarrow \text{entry corresponding to 1} \end{array}$$

Measuring X selects (or reveals) a transition, chosen at random:



Quantum Information (I)

A ***quantum state*** of a system is represented by a ***column vector*** whose indices are placed in correspondence with the classical states of that system:

- The entries $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ are complex numbers
- The sum of the absolute values squared of the entries must equal 1.

Definition

The *Euclidean norm* for vectors with complex number entries is defined like this:

$$v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \Longrightarrow \quad \|v\| = \sqrt{\sum_{k=1}^{n} |\alpha_k|^2}$$

Quantum state vectors are therefore ***unit vectors*** with respect to this norm $\|v\|$

Quantum Information (II)

Examples of qubit states

- Standard basis states: $|0\rangle$ and $|1\rangle$
- Plus/minus states:

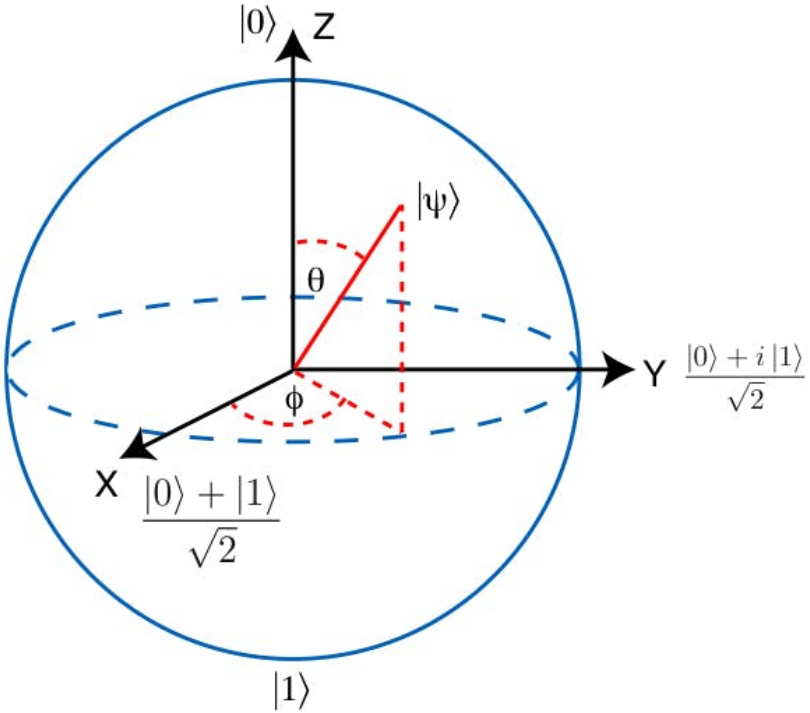
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

- A state without a special name:

$$\frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle$$

- The **two orthogonal Z-basis states** of a qubit are defined as: **|0⟩** and **|1⟩**.
- The **two orthogonal X-basis states** of a qubit are: $|+\rangle$ and $|-\rangle$
- The **two orthogonal Y-basis states** of a qubit are:

$$|R\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \quad |L\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$



Bloch sphere is a geometrical representation of the **pure state** space of a two-level quantum mechanical system (**qubit**)

Quantum Information (III)

Example

A quantum state of a system with classical states ♣, ♦, ♥, and ♠:

$$\frac{1}{2}|\clubsuit\rangle - \frac{i}{2}|\diamondsuit\rangle + \frac{1}{\sqrt{2}}|\spadesuit\rangle = \begin{pmatrix} \frac{1}{2} \\ -\frac{i}{2} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$|\Psi\rangle$ - Ket vector (column vector)

$\langle\Psi|$ - Bra vector (row vector)

For any column vector $|\psi\rangle$, the row vector $\langle\psi|$ is the *conjugate transpose* of $|\psi\rangle$:

$$\langle\psi| = |\psi\rangle^\dagger$$

Mathematical background on quantum states and operations. Basic Linear Algebra: Vectors, Matrices, Hermitian/Unitary matrices

- **Hermitian** matrix (or self-adjoint matrix) is **a complex square matrix that is equal to its own conjugate transpose.**
- Matrix **U** is ***unitary***, that is $U^\dagger U = I_2$, where $U^\dagger$ is the **adjoint of U** (***obtained by transposing and then complex conjugating U***), and I_2 is the two by two **identity matrix.**

Qiskit Fall Fest 2024

One and two-qubit applications on IBM's quantum computers

by Stefan Ataman

Nuclear Physics

Extreme Light Infrastructure - Nuclear Physics (ELI-NP)

October 30, 2024

Hermitian/Unitary matrices

POSTULATE 2: "If the quantum system Σ does not interact with other systems and is in a non-zero state $|\psi_0\rangle$ at a moment t_0, then it transitions to another non-zero state $|\psi_1\rangle$ at time t_1 with a probability equal to the real subunitary number $\cos^2\alpha$, where α is the measure of the angle $\widehat{\psi_0, \psi_1}$ between the states $|\psi_0\rangle$ and $|\psi_1\rangle$; moreover, these two states are connected by a unitary operator $U : H \to H$ $(U^\dagger U = I)$, which depends **only** on the moments t_0, t_1, namely: $|\psi_1\rangle = U(|\psi_0\rangle)$."

The Qubit

Dirac bra-ket notation - the qubit

From the basic ket examples,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

we move to the qubit,

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

with $c_0, c_1 \in \mathbb{C}$ and for **normalization**:

c_0, c_1 – specify the amplitudes of two states

$$|c_0|^2 + |c_1|^2 = 1$$

Normalization: why is that? Let's recall.

$|c_0|^2$ – gives the probability that the qubit will be found in state "0";

$|c_1|^2$ – gives the probability that the qubit will be found in state "1".

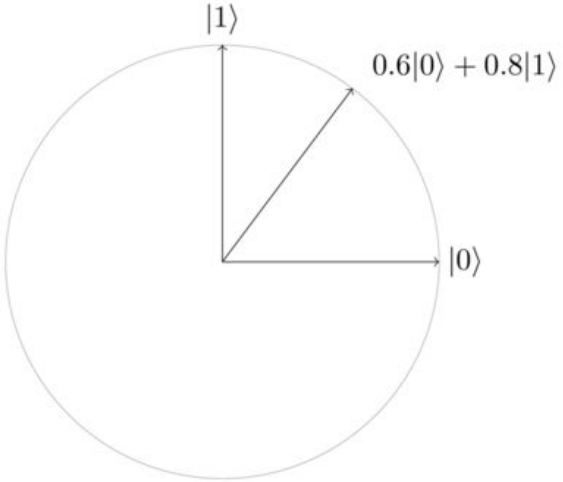
Example of qubit

Bit **Qubit** → **Qubit State**

0 $|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

1 $|1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$$0.6|0\rangle + 0.8|1\rangle = 0.6 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 0.8 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0.6 \\ 0.8 \end{bmatrix}$$



Acting on qubits

How do you act on one qubit?

Answer: with operators (i. e. 2×2 matrices!)

Why is that?
Because a qubit is a 2×1 *matrix*. So matrix multiplications requires

$$\underbrace{\begin{pmatrix} \circ \\ \circ \end{pmatrix}}_{|\psi'\rangle} = \underbrace{\begin{pmatrix} \circ & \circ \\ \circ & \circ \end{pmatrix}}_{\text{operator or quantum gate}} \underbrace{\begin{pmatrix} \circ \\ \circ \end{pmatrix}}_{|\psi\rangle}$$

Here $\circ$ is a *generic* component of the above matrices.

Quantum Logic Gates (I)

Not Gate: Pauli's X matrix

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

$$\begin{aligned} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} (\alpha|0\rangle + \beta|1\rangle) &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \\ &= \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \\ &= \alpha|1\rangle + \beta|0\rangle \\ &= X(\alpha|0\rangle + \beta|1\rangle). \end{aligned}$$

Acting on qubits

First quantum gate: Pauli's σ_x matrix. We call it simply X:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Let's apply X on $|1\rangle$:

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Next, we apply it on $|0\rangle$:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

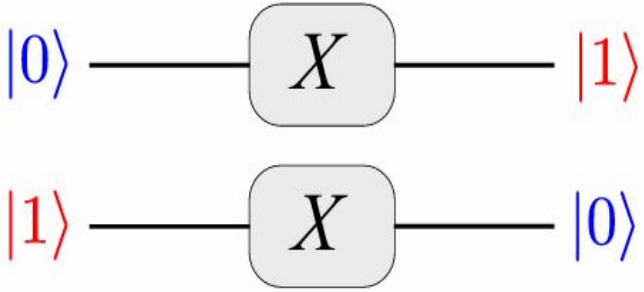
The X gate as a quantum circuit

Similar to digital circuits, we can draw quantum circuits. A single line implies a quantum bit. A double line means a classical bit (coming soon). So we had the X gate:

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

As a quantum circuit this is:

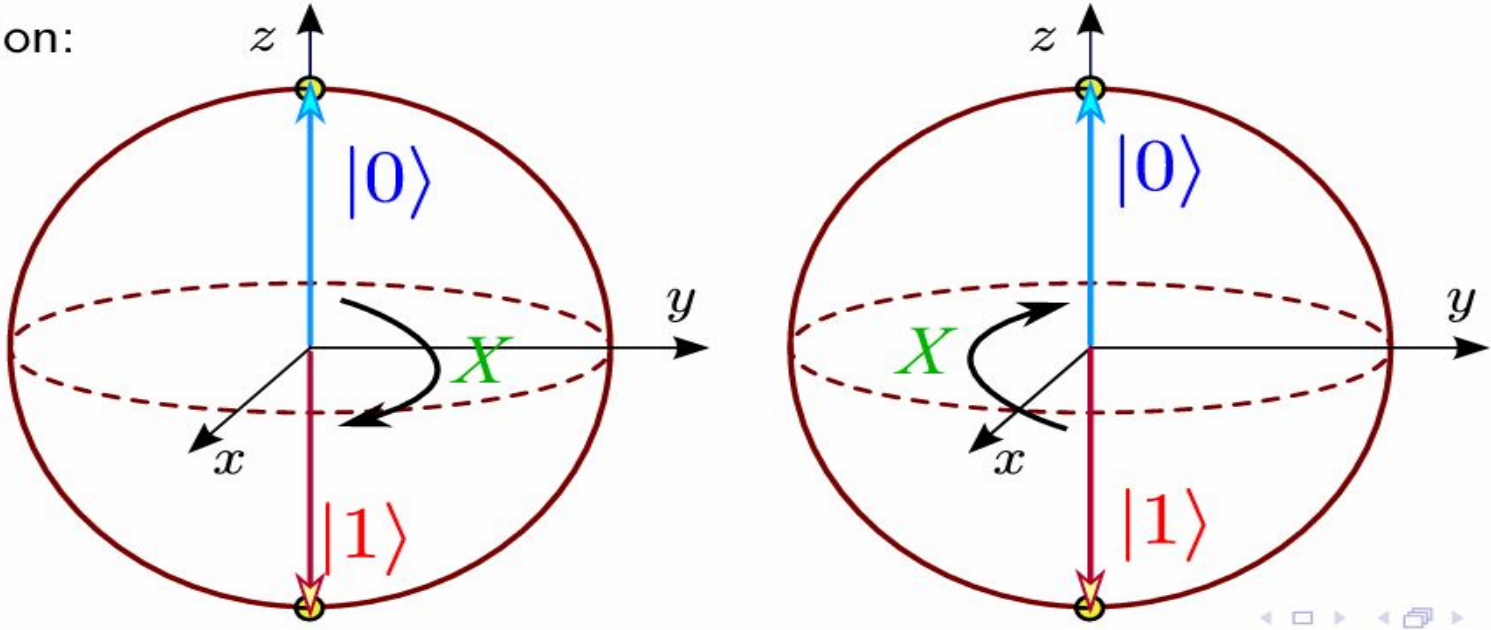


The X gate on the Bloch sphere

In summary, the X gate did this:

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

Graphical depiction:



Quantum Logic Gates (II)

Hadamard Gate: puts a qubit into a superposition

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

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

- The appropriate condition on the **matrix representing the gate** is that the matrix **U** describing the single qubit gate be ***unitary***, that is $U^\dagger U = I_2$, where $U^\dagger$ is the **adjoint of U** (***obtained by transposing and then complex conjugating U***), and I_2 is the two by two **identity matrix**.

- **Unitarity constraint is the only constraint** on quantum gates!

Quantum Logic Gates (III)

The Hadamard gate

You probably know by now the Hadamard (H) gate:

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

Applying H on $|0\rangle$ we get:

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

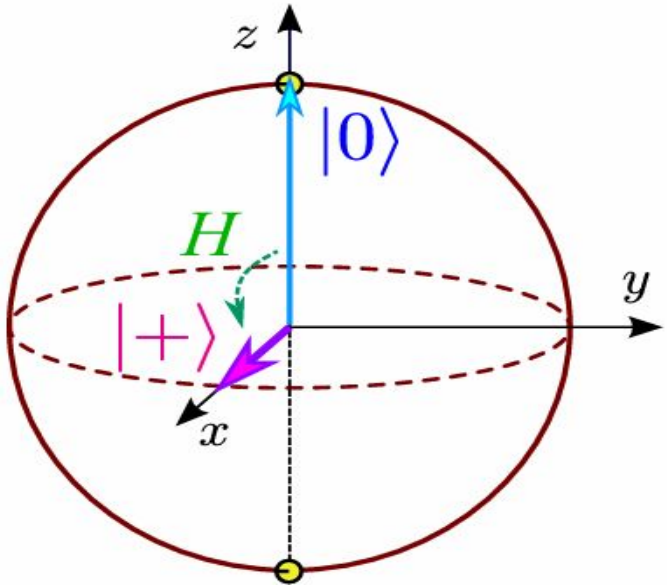
Applies on $|1\rangle$ we have:

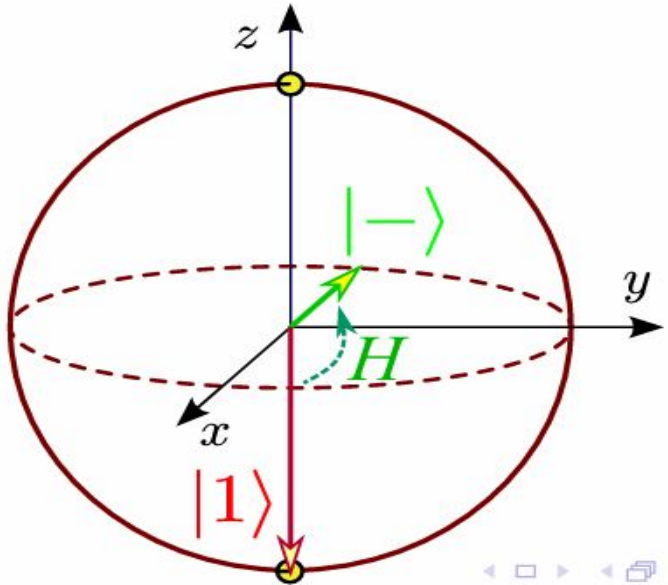
$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle$$

The Hadamard gate

$$|0\rangle \text{ —— } H \text{ —— } \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

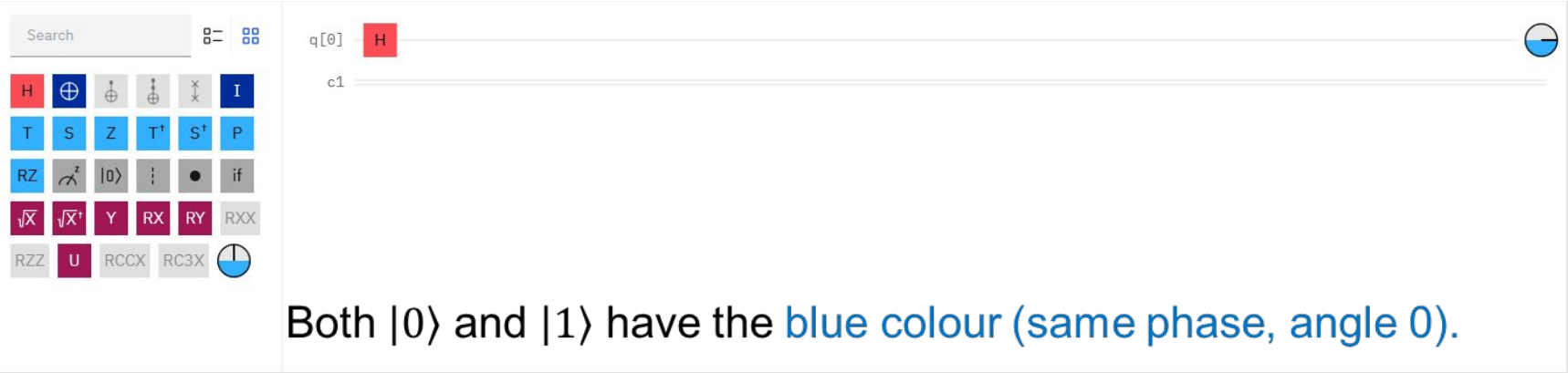
$$|1\rangle \text{ —— } H \text{ —— } \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



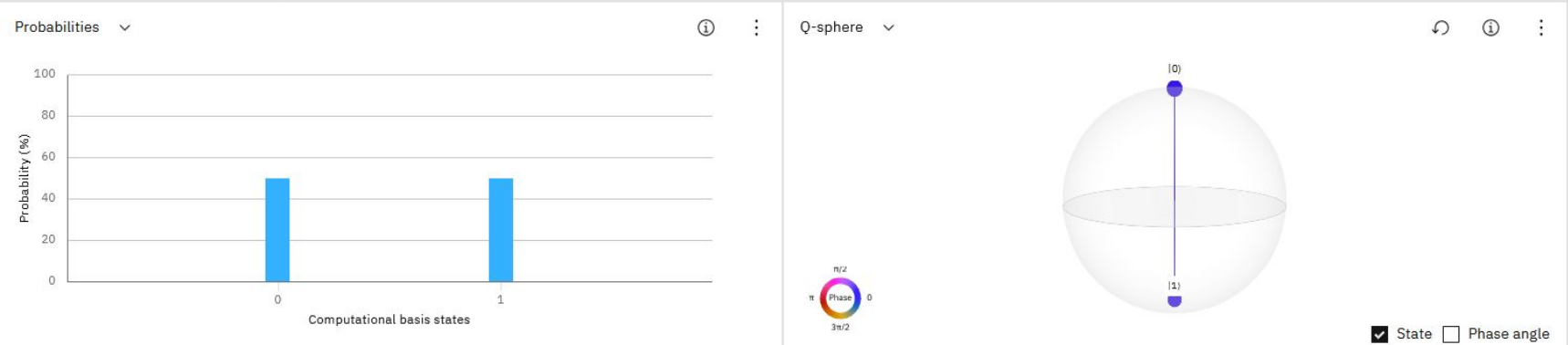


Representation of “plus” state in Quantum Composer

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

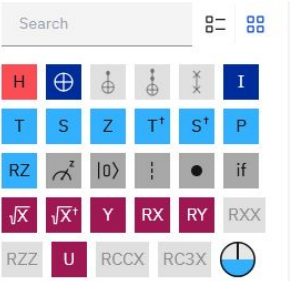


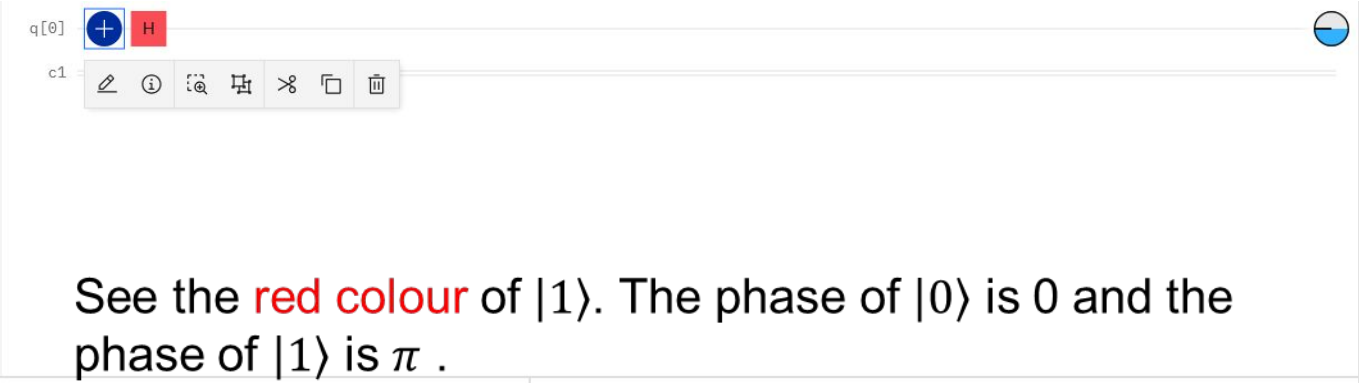

```
1 OPENQASM 2.0;
2 include "qelib
3 qreg q[1];
4 creg c[1];
5 h q[0];
6
```



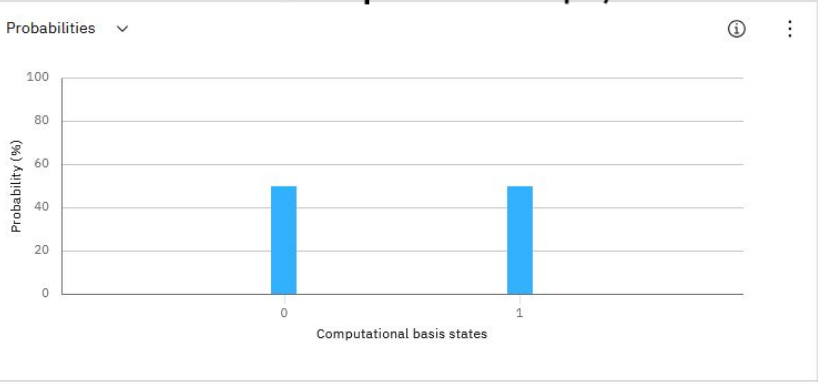
Representation of “minus” state in Quantum Composer

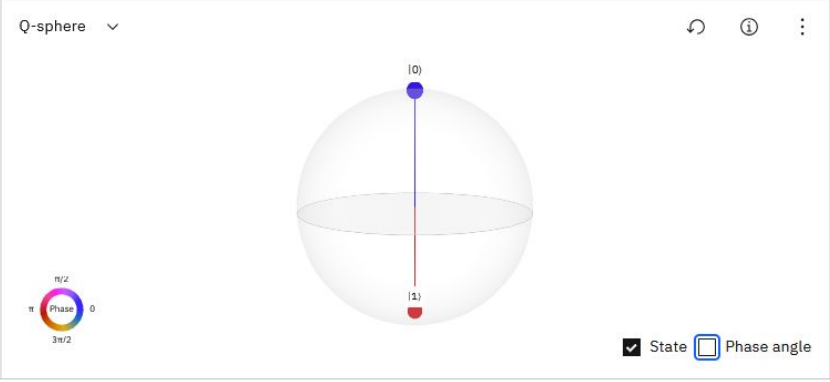
$$|-\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle) = H \cdot |1\rangle$$






```
1 OPENQASM 2.0;
2 include "qelib1.inc";
3 qreg q[1];
4 creg c[1];
5 x q[0];
6 h q[0];
7
```





Basic math stuff

Recall Euler's relation(s):

$$e^{i\theta} = \cos\theta + i\sin\theta \qquad e^{-i\theta} = \cos\theta - i\sin\theta$$

Some important values:

$$e^{i\pi} = \cos\pi + i\sin\pi = -1 \qquad e^{i2\pi} = 1$$

Ans some more values ($\theta = \pi/2$):

$$e^{i\pi/2} = i \qquad e^{-i\pi/2} = -i$$

And finally ($\theta = \pi/4$):

$$e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}} = \frac{1+i}{\sqrt{2}} \qquad e^{-i\pi/4} = \frac{1-i}{\sqrt{2}}$$

The Y and Z gates

Pauli's σ_y / Y gate si defined by

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

And finally, the last Pauli gate is

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

May I recall Pauli's σ_x matrix i .e the X gate,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Maybe as an exercise you computed:

X^2, Y^2 and Z^2. Do you recall the result?

The X, Y and Z gates - squared

You got

$$X^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}_2$$

and then

$$Y^2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}_2$$

and finally

$$Z^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}_2$$

So we have the neat result

$$X^2 = Y^2 = Z^2 = \mathbb{I}_2$$

and as a consequence, for $\forall N \in \mathbb{N}$ we have

$$X^{2N+1} = X, \quad Y^{2N+1} = Y, \quad Z^{2N+1} = Z$$

Quantum Logic Gates (IV)

Other Gates

$$Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

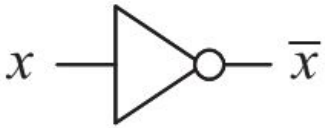
$$\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}$$

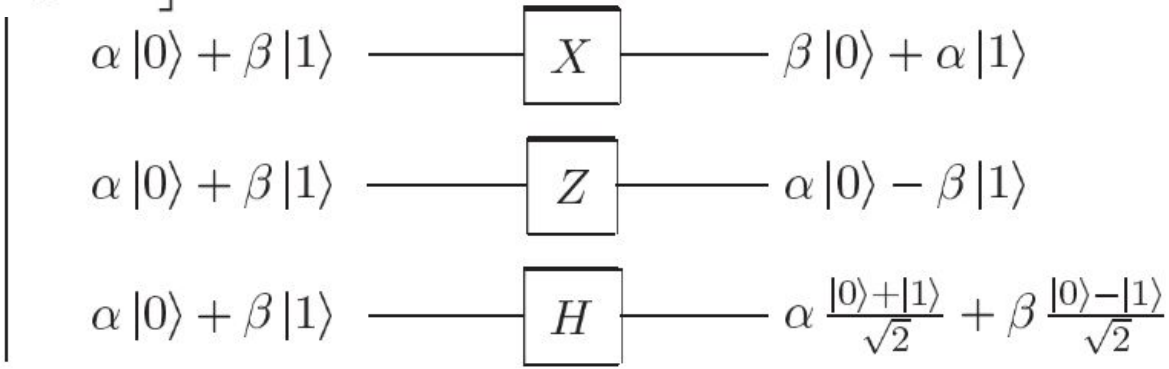
Restrictions

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

- only gates that preserves the “norm” can be used:

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





Check the identities!

The S gate (phase)

Can we have a gate $\square$ such that

$$\square \cdot \square = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

or in other words

$$\square = \sqrt{Z}?$$

Meet the "S gate":

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

I claim that:

The S gate rotates your qubit with $\pi/2$ around the z-axis.

Obviously:

$$S^2 = Z$$

The T or $\pi/8$ gate

Meet the "T gate" (T), also called the "$\pi/8$ gate",

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

Let's rewrite this gate as

$$T = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}$$

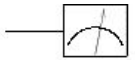
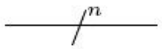
Now you understand the name "$\pi/8$".

I claim that:

The T gate rotated your qubit with $\pi/4$ around the z-axis.

Summary of Single Qubit Gates & Symbols in IBM Quantum Composer

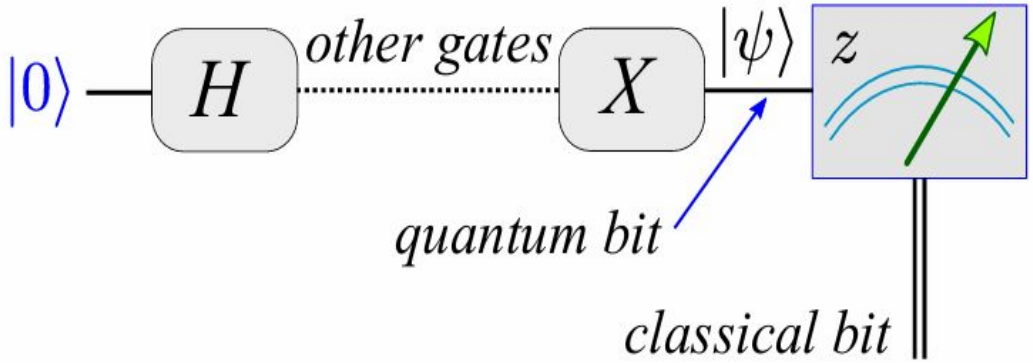
Hadamard	H	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$	H
Pauli-X	X	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$	⊕
Pauli-Y	Y	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$	Y
Pauli-Z	Z	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$	Z
Phase	S	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$	S
$\pi/8$	T	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$	T

measurement		Projection onto $\|0\rangle$ and $\|1\rangle$	
qubit		wire carrying a single qubit (time goes left to right)	
classical bit		wire carrying a single classical bit	
n qubits		wire carrying n qubits	

Measurement of a qubit

Recall Max Born (1926)

Measurement is probabilistic.



Obvious fact:

The measurement of a qubit yields a (single) **classical bit**.

Measurement of a qubit

Recall: Max Born (1926)

(Much to Einstein's dislike.) Measurement is probabilistic.

Specifically, for our qubit:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

The probability to find $|0\rangle$ *i. e.* "0" after a measurement is $p_0 = |c_0|^2$.
The probability to find $|1\rangle$ *i. e.* "1" after a measurement is $p_1 = |c_1|^2$.

Remark:

The total probability is the probability to find $|0\rangle$ plus the probability to find $|1\rangle$. This is $p_0 + p_1 = |c_0|^2 + |c_1|^2 = 1$.

Measurement of a qubit - formalized

Specifically, for our qubit:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$

The probability to find $|0\rangle$ after a measurement is

$$p_0 = |\langle 0|\psi\rangle|^2 = |c_0|^2$$

The probability to find $|1\rangle$ after a measurement is

$$p_1 = |\langle 1|\psi\rangle|^2 = |c_1|^2$$

Multiple Qubits (I)

- A two qubit system has four computational basis states: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
- **A pair of qubits** can also **exist in superpositions of these four states**, so the quantum state of two qubits involves associating a complex coefficient – called an amplitude – with each computational basis state, such that the state vector describing the two qubits is:

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

- Similar to the case for a single qubit, the measurement result x = (00, 01, 10 or 11) occurs with probability $|\alpha_x|^2$, with the state of the qubits after the measurement being $|x\rangle$
- The condition that probabilities sum to one is:

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$$

Multiple Qubits (II)

$$|a\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}, \quad |b\rangle = \begin{bmatrix} b_0 \\ b_1 \end{bmatrix}$$

$$|ba\rangle = |b\rangle \otimes |a\rangle = \begin{bmatrix} b_0 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \\ b_1 \times \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{bmatrix}$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 0 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} =$$

$$\frac{1}{\sqrt{2}} |00\rangle + 0\,|01\rangle + 0\,|10\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

The **Kronecker product**, denoted by $\otimes$, is an operation on two matrices of arbitrary size resulting in a block matrix. It **is a particularization of the tensor product**.

$$a_1|000..00| + a_2|000..01| + \ldots + a_{2^n}|111..11|$$

$$|a_1|^2 + |a_2|^2 + \ldots + |a_{2^n}|^2 = 1$$

The evolution of a discrete quantum system

POSTULATE 5: "If Σ_1, Σ_2 are two independent and isolated quantum systems, then the state space of the **composite** ($\equiv$ **assembled**, **merged**) quantum system Σ is the tensor product of the state spaces of the component systems, meaning:

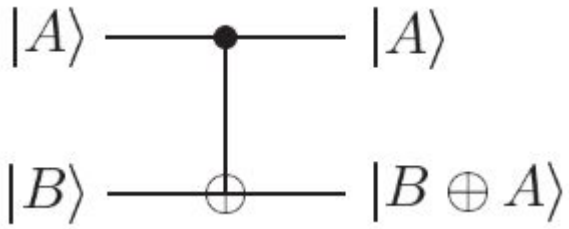
$$H(\Sigma) = H(\Sigma_1) \otimes H(\Sigma_2). \tag{0.31}$$

In addition, if Σ_1 is in the state $|\psi_1\rangle$ while Σ_2 is in state $|\psi_2\rangle$, then Σ will be in the state $|\psi_1\rangle \otimes |\psi_2\rangle$. Relation (0.31) extends to any composite quantum systems $\Sigma_1, \ldots, \Sigma_n$ whose composite system is Σ; specifically,

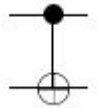
$$H(\Sigma) = H(\Sigma_1) \otimes H(\Sigma_2) \otimes \cdots \otimes H(\Sigma_n)." \tag{0.32}$$

Controlled Not Gate (CNOT)

- This gate has **two input qubits**, known as the **control qubit** ($|A\rangle$) and the **target qubit** ($|B\rangle$), respectively.
- **If the control qubit is set to 0, then the target qubit is left alone (unchanged).**
- **If the control qubit is set to 1, then the target qubit is flipped.**



$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



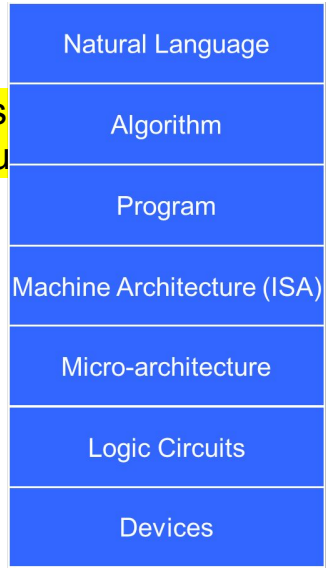
$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$
$$\rightarrow \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle$$

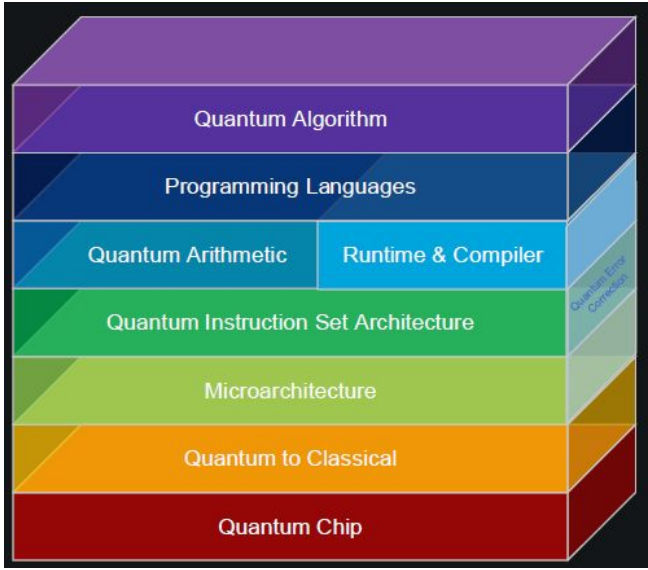
$$CNOT \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{pmatrix} \qquad CNOT = \begin{pmatrix} I_2 & O_2 \\ O_2 & X \end{pmatrix}$$

Overview about QC architecture and the layered approach from algorithm to hardware

- History of Qiskit
- The Architecture of Quantum Computers
- From Quantum Circuit to Quantum Hardware

- Understanding the workflow of quantum computers
- Acquiring a bird's eye view about the QC architectu
- Discovering various qubit types
- Learning about Transpiler stages with Qiskit





The History of Qiskit. Key milestones in Qiskit development

2016: IBM Quantum Experience is launched, making a real quantum computer available over the internet for the first time.

2017: Qiskit is released as an open-source framework for programming quantum computers.

2018:The **transpiler** is released. Qiskit elements (**Terra, Aer, Ignis, Aqua**) are introduced.

2019: Qiskit gains support for third-party hardware, starting with a five-qubit trapped ion device at the University of Innsbruck. The first cohort of Qiskit advocates is also introduced.

2020-Present: Qiskit continues to grow, with a vibrant community of over 550,000 users and contributions leading to more than 2,800 research papers.

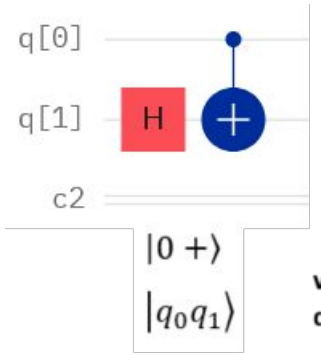
Qiskit Community Highlights

- Open Source & Collaborative
- Community Support
- Slack Channel
- Qiskit Advocates
- Events & Learning Opportunities
- Qiskit Global Summer School
- Workshops, Challenges & Hackathons
- Resources & Learning
- Tutorials, Documentation & Courses

Slides 9-31 Introduction to Qiskit.pdf

Bit-ordering and graphical interpretation in Qiskit SDK

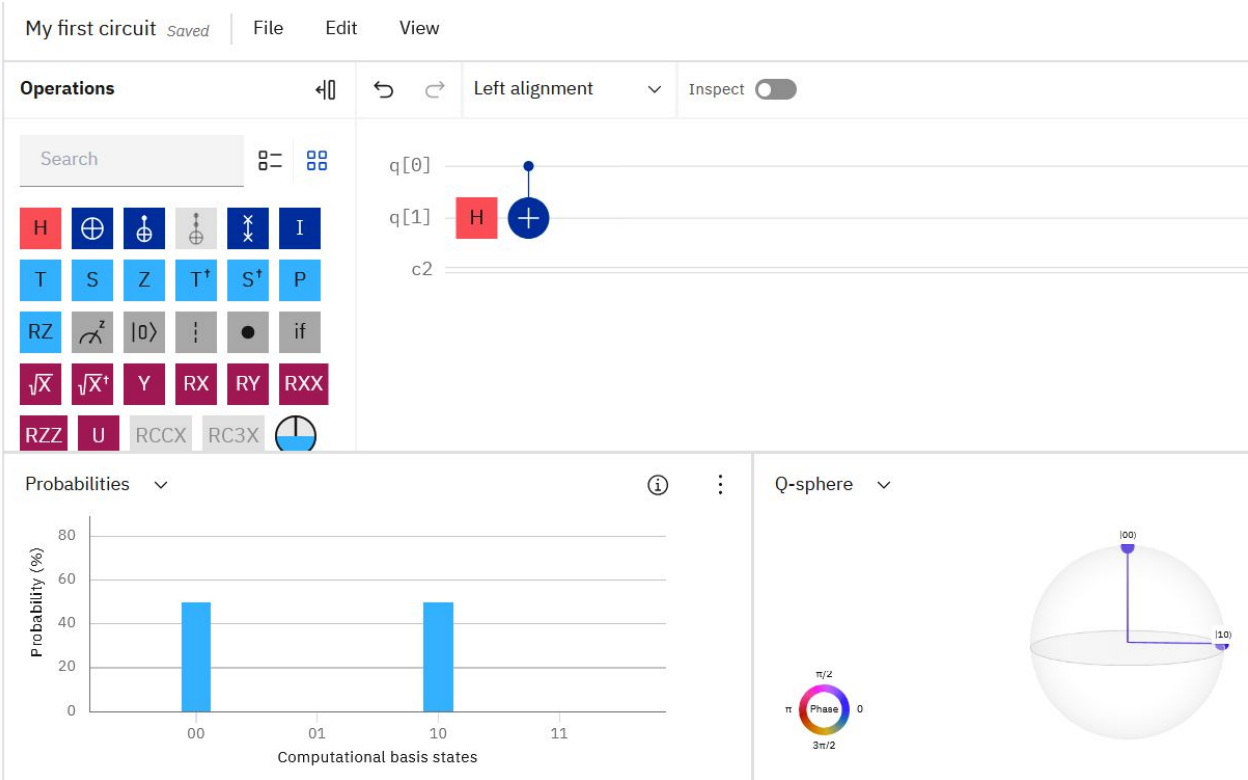
- If you have a set of *n* bits (or qubits), you'll usually label each bit 0→*n*−1. **Different software and resources must choose how they order these bits both in computer memory and when displayed on-screen**.



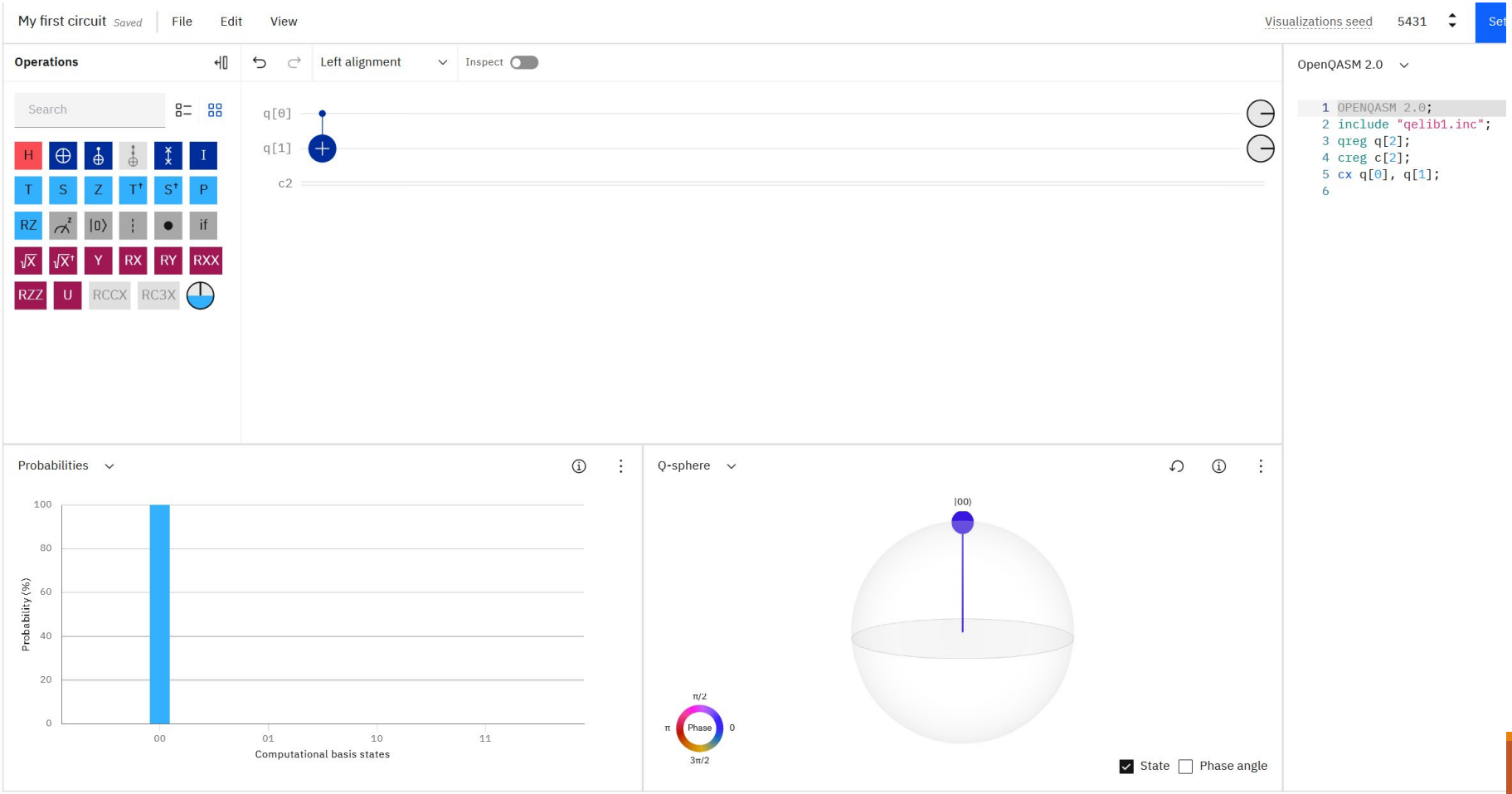
visualization of quantum states

$c_1 c_0 = \{00, 01, 10, 11\}$

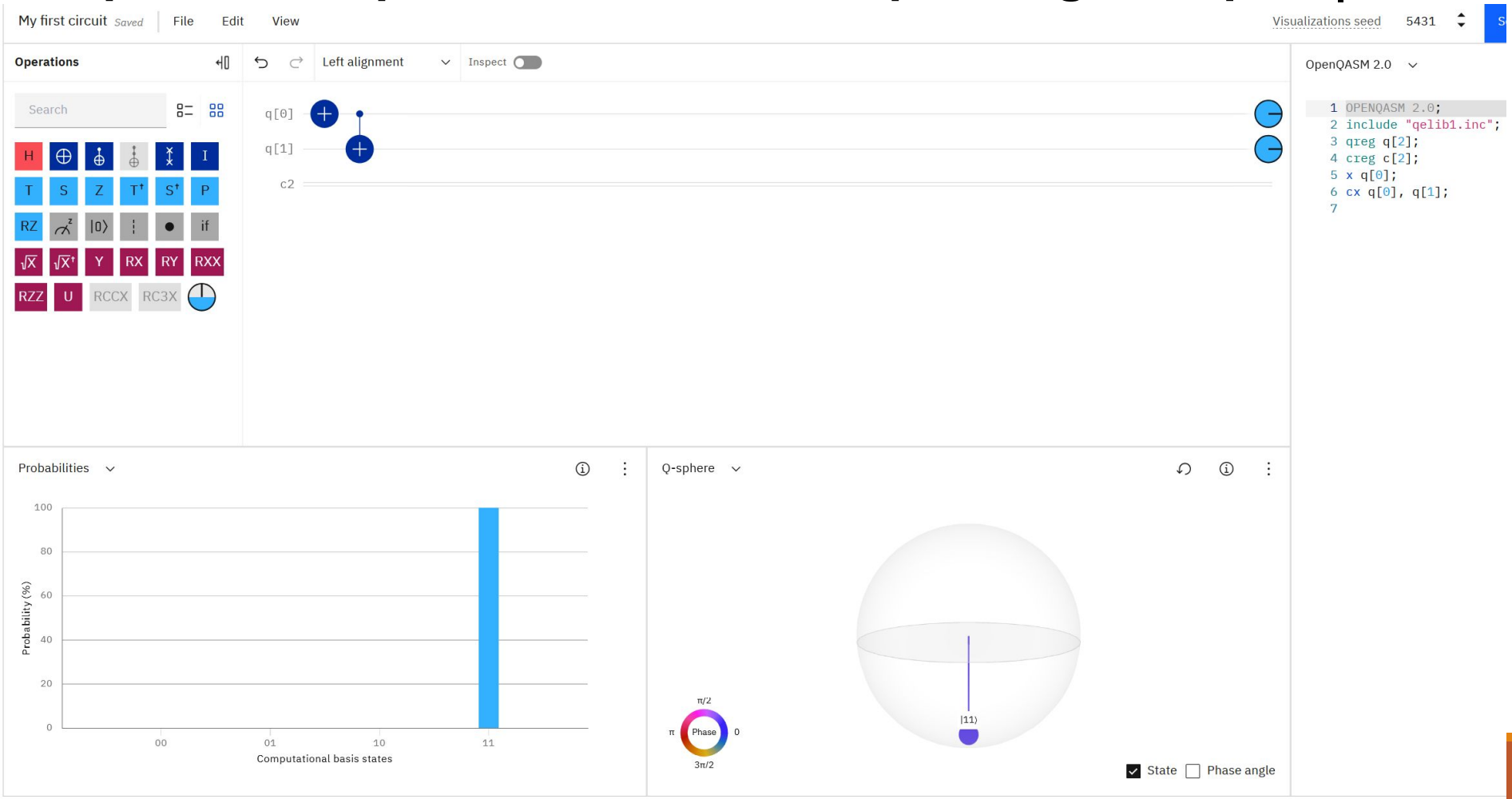
visualization of classical states



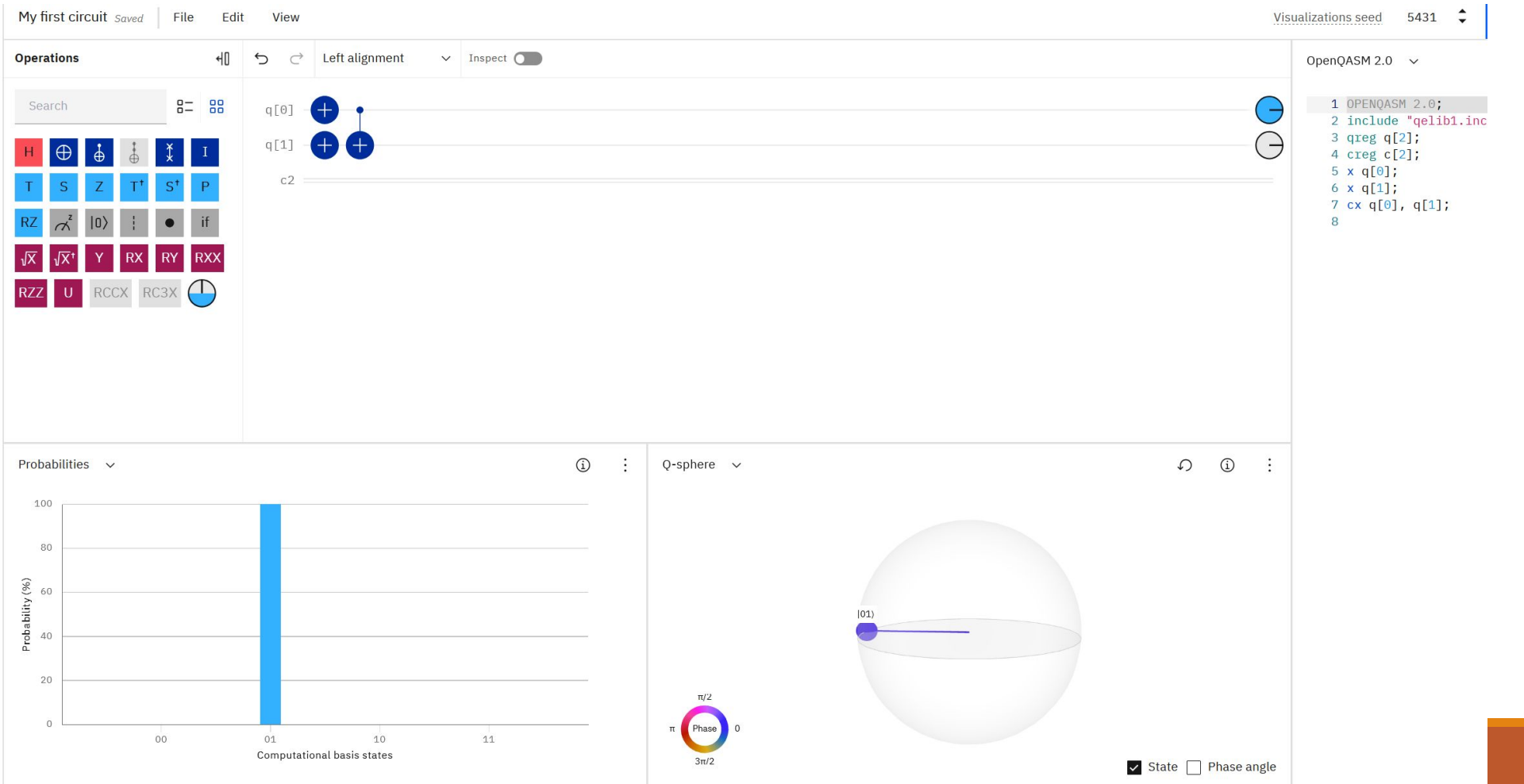
Graphical interpretation of CNOT depending on input: |00>



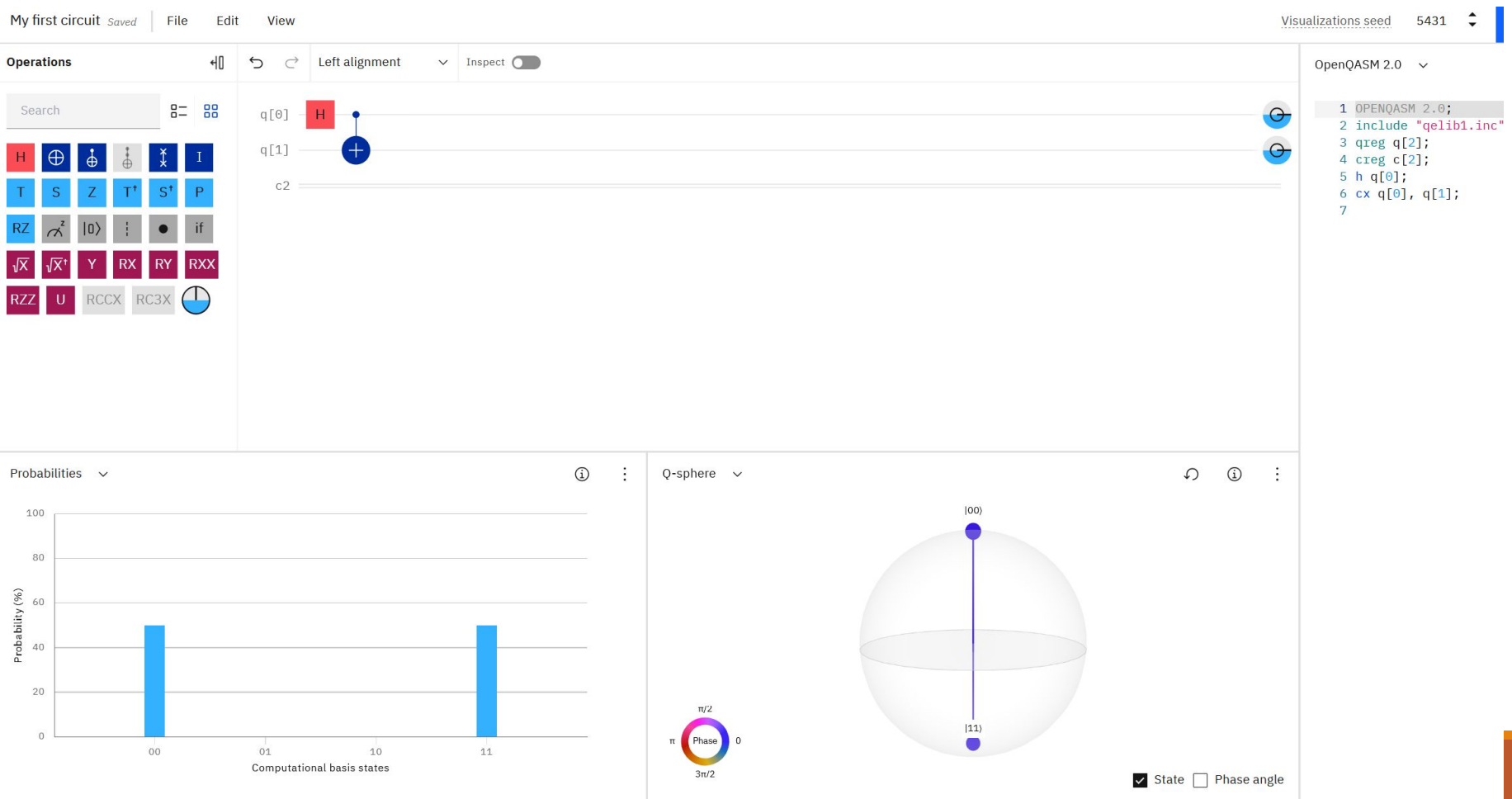
Graphical interpretation of CNOT depending on input: |10>



Graphical interpretation of CNOT depending on input: |11>



Graphical interpretation of CNOT depending on input: |+0> (I)



Graphical interpretation of CNOT depending on input: |+0> (II)

To the entry of CNOT we have:

- the control bit $H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = |+\rangle$
- the target bit $|0\rangle$

$\Rightarrow$ The tensorial product of the input in the CNOT gate is:

$$\Rightarrow |+0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}.$$

Applying CNOT gate to the previous vector:

$$\begin{pmatrix}1000\\0100\\0001\\0010\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\1\\\frac{1}{\sqrt{2}}\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\1\\\frac{1}{\sqrt{2}}\end{pmatrix}$$

Graphical interpretation of CNOT depending on input: |+0> (III)

- After applying the Hadamard gate on |0> of the control qubit => 50% probability of having a qubit of value 0 and 50% of having a qubit of value 1 (see slide 90 – “Representation of “plus” state in Quantum Composer”)

- If the control qubit is in |0> => the target qubit (which is initially in |0>) is not changed => will obtain the state |00> with probability of 50%

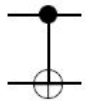
- If the control qubit is in |1> => the target qubit (which is initially in 0) is changed to 1 => will obtain the state |11> with probability of 50%

Controlled U(niversal) Gates

- **A controlled-U operation (gate)** is a two qubit operation, **with a control and a target qubit**.
- **If the control qubit is set then U is applied to the target qubit**, otherwise the target qubit is left alone.
- $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$

controlled-NOT

U = X



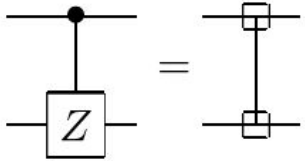
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

swap

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

controlled-Z

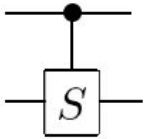
U = Z



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

controlled-phase

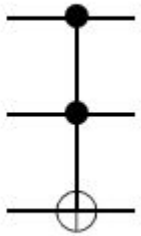
U = S



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

CCNOT Gate - Toffoli

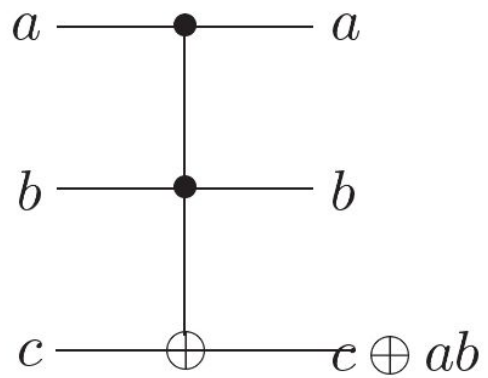
Toffoli



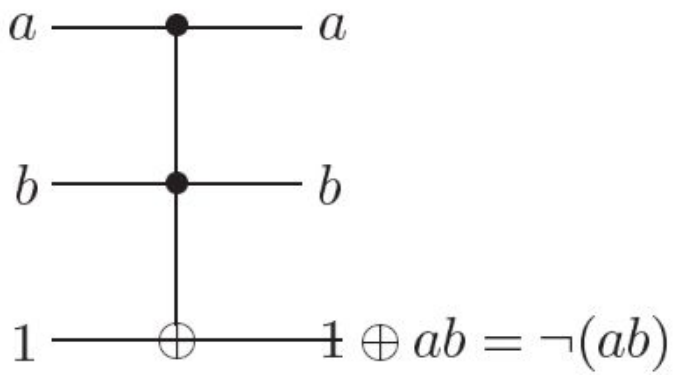
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

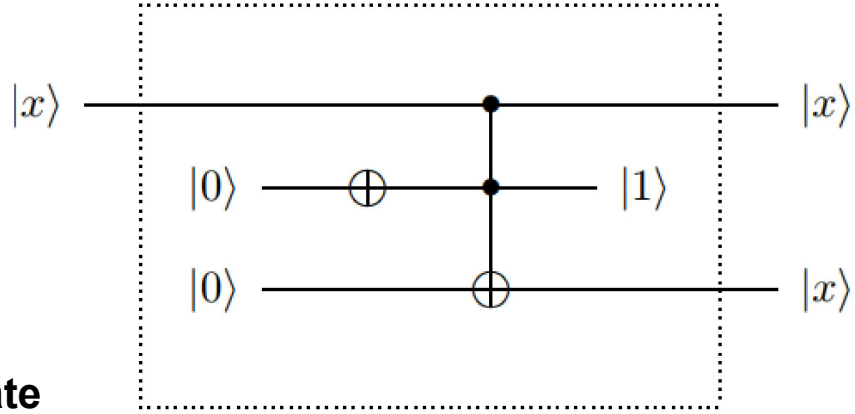
- The Toffoli gate has three input qubits and three output qubits
- **Two of the qubits are control qubits** that are unaffected by the action of the Toffoli gate.
- **The third qubit is a target qubit** that **is flipped if both control bits are set to 1, and otherwise is left alone.**
- **Applying the Toffoli gate twice** to a set of qubits has the effect **(a, b, c) → (a, b, c ⊕ ab) → (a, b, c),** and thus the **Toffoli gate is a reversible gate.**



Implementing Quantum Circuits using Toffoli Gate

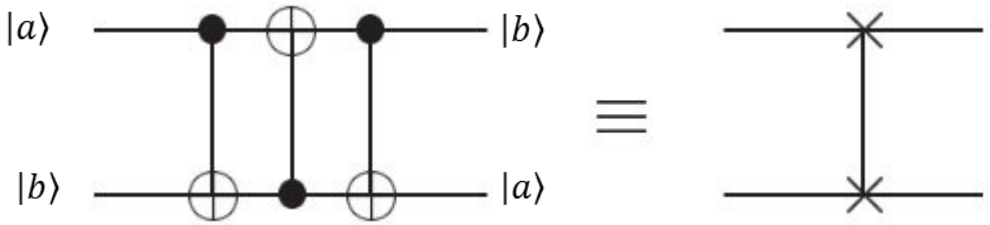


- Classical circuit **implementing a NAND gate using a Toffoli gate**.
- The top two bits represent the input to the NAND, while the third bit is prepared in the standard state 1.



- FANout with the Toffoli gate

Swapping two qubits

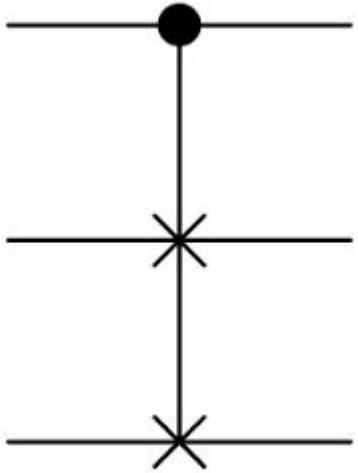


- It swaps the states of the two qubits. To see that this circuit accomplishes the swap operation, note that the sequence of gates has the following sequence of effects on a computational basis state $|a, b\rangle$
- All additions are done modulo 2 (XOR)!

$$|a, b\rangle \rightarrow |a, a \oplus b\rangle \rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle$$

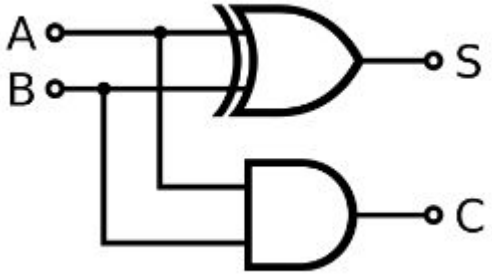
FREDKIN Gate

- To add – truth tabel, explanations and formula

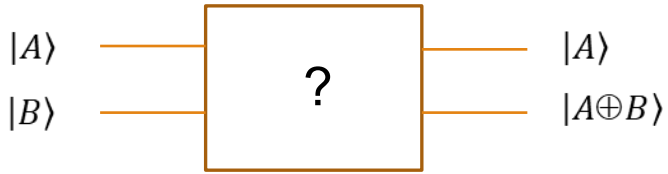


Problem 1

In this problem, you will **build a quantum version of a half adder** – the basic building block of addition on a classical computer. The most important part of such a circuit is the half-adder:

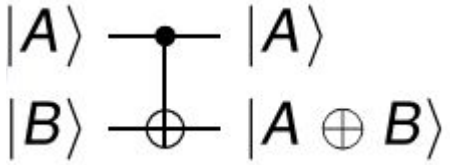


where A and B are classical bits, **S = A ⊕ B** is the sum modulo two and **C = A · B** is ordinary multiplication of A and B called the **carry**. The carry is the part of the summation that adds to the next digit (it is only 1 if both A = 1 and B = 1).

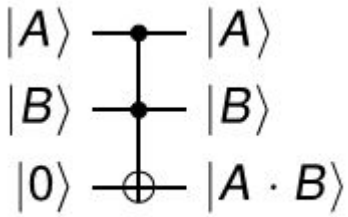


Solution 1

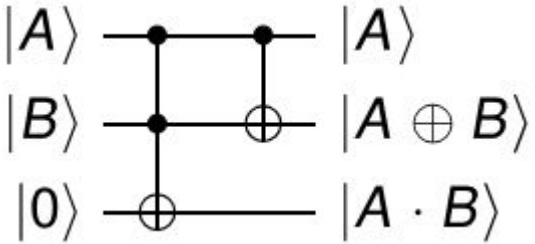
- **S computation**



- **C (carry) computation**



- **The full circuit**



Quantum Superposition

- **One** of the **properties** that sets a **qubit apart from a classical bit** is that it can be in **superposition**.
- **Superposition is one of the fundamental principles of quantum mechanics**. In classical physics, a **wave describing a musical tone can be seen as several waves with different frequencies that are added together, superposed**.
- Similarly, **a quantum state in superposition can be seen as a linear combination of other distinct quantum states**. The **superposition of qubits depends on the chosen basis**.

For example, **when a qubit is in a superposition state of equal weights**, **a measurement will make it collapse to one of its two basis states $|0\rangle$ and $|1\rangle$ with an equal probability of 50%.** $|0\rangle$ is the state that when measured, and therefore collapsed, will always give the result 0. Similarly, $|1\rangle$ will always convert to 1.

Quantum Entanglement – RO (*Inseparabilitatea*). Teleportation

- One of the other counter-intuitive phenomena in quantum physics is entanglement.
- **A pair or group of particles** is **entangled** when **the quantum state of each particle cannot be described independently of the quantum state of the other particle(s)**.
- The **most captivating application of entanglement** is **quantum teleportation**.
- Quantum teleportation is a **process through which the state of a quantum system can be transmitted from one location to another using two entangled particles** and **classical communication**.
- **Please make no mistake**; **we are not talking about the science fiction trope of teleporting matter here**. The process of quantum teleportation offers a **genuine solution solely for transmitting quantum information across vast distances, overcoming classical limitations**.

Quantum Entanglement (II)

Let us consider a two-qubit system whose **Hilbert space** is denoted by $H_A \otimes H_B$.

Definition E.1.
If the state of two qubits can be written as a product state $|\psi_{AB}\rangle = |\xi_A\rangle \otimes |\eta_B\rangle$, then the state is called **separable** or **product**. The two states $|\xi\rangle$ and $|\eta\rangle$ are arbitrary states of a qubit.

Definition E.2.
If the **state of two qubits cannot be written as a product state**, $|\psi_{AB}\rangle \neq |\xi_A\rangle \otimes |\eta_B\rangle$, then **the state is called entangled**.

Practical achievements

Distribution distances have greatly increased over the years.

1989: 32 cm [10]

1998: 1 km [11]

2004: 122 km [12]

2015: 307 km [13]

2016: 404 km [14]

2017: **1,200 km** [15]

2018: 421 km [16]

2020: 509 km [17]

Long-distance QKD using *Micius* satellite

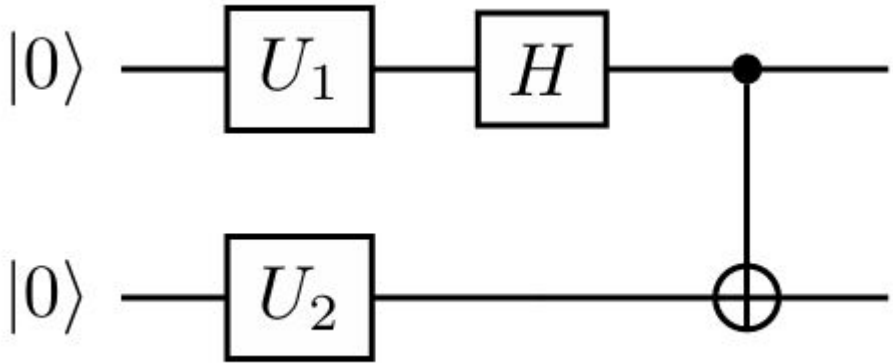
https://www.oeaw.ac.at/fileadmin/NEWS/2018/IMG/quantentelefonat_grafik.jpg

Sep 2017: "Quantum Call" between Vienna and Beijing [18]

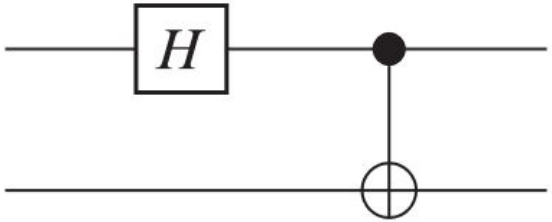
Generation of the Bell states (I)

Pg. 3 of **CNQ-RoNaQCI-Training-C3-Entanglement-QTeleportation.pdf**

- The 4 states: **All the four Bell states are entangled**
- Illustrating the graphics and demonstration



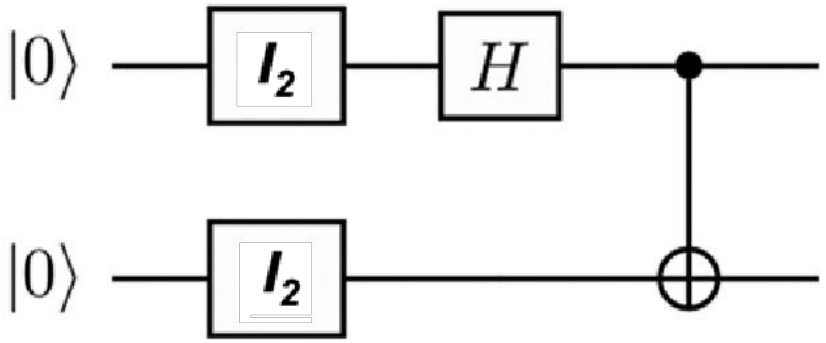
The Bell Circuit

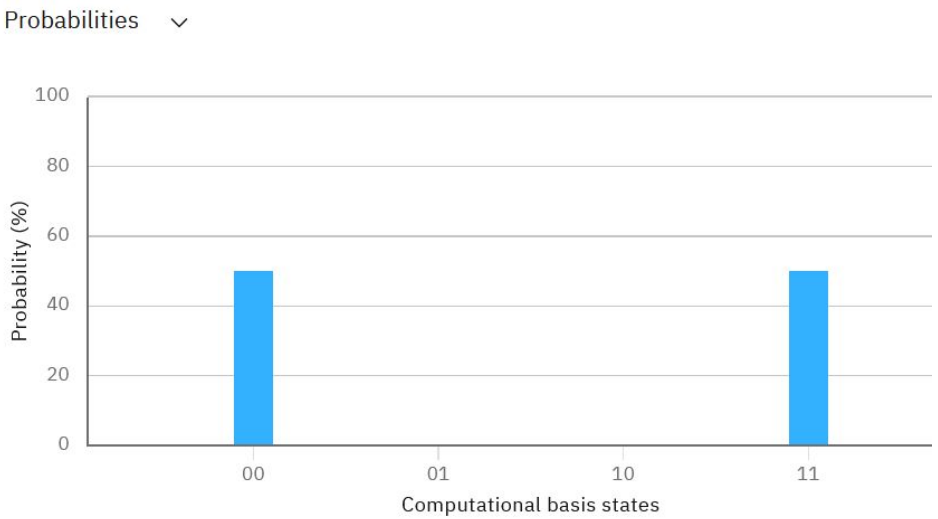


- For generating the state |β00⟩, the unitary operators are U1 = I and U2 = I
- For generating the state |β01⟩, the unitary operators are U1 = I and U2 = X
- …

Generation of the Bell states (II)

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

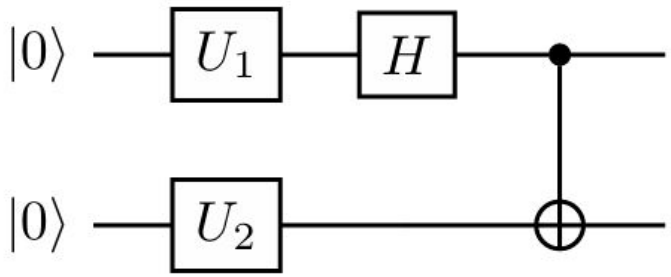


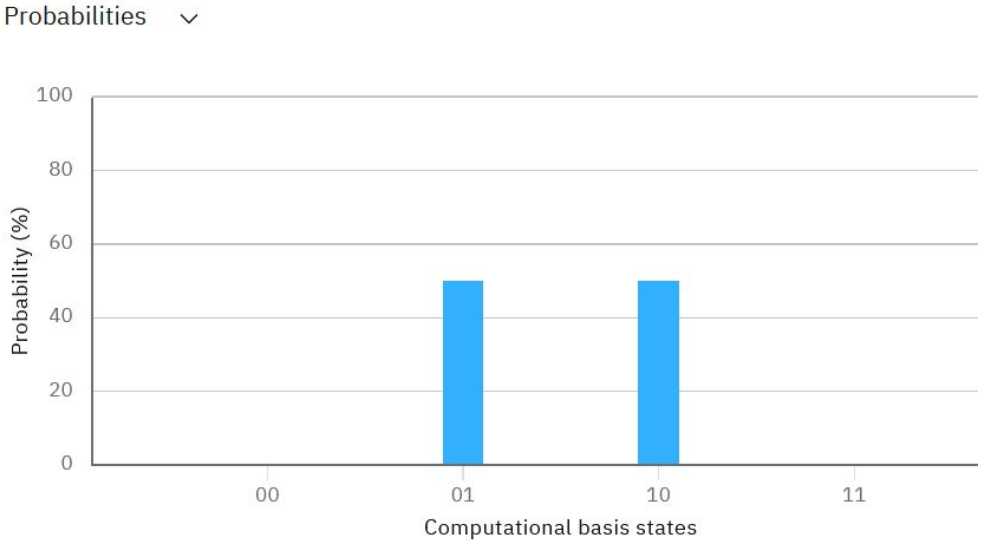


$$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Generation of the Bell states (III)

$$\beta_{01} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$



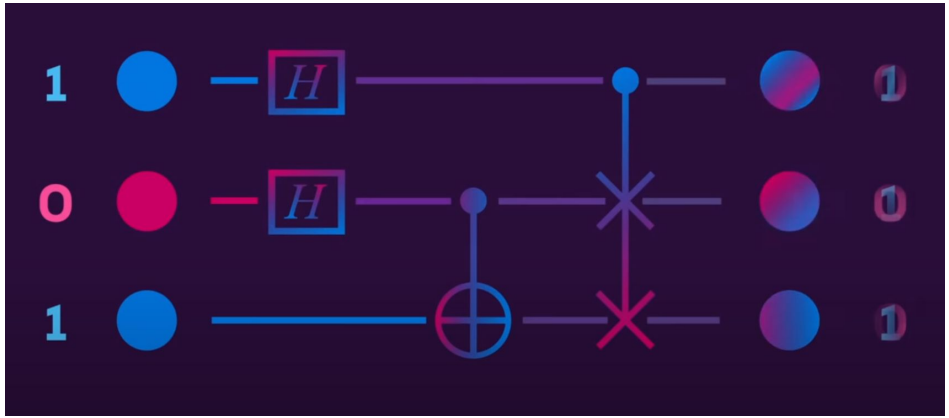


- For generating the state $|\beta_{01}\rangle$, the unitary operators are U_1 = I and U_2 = X

$$|00\rangle \xrightarrow{I\otimes X} |01\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

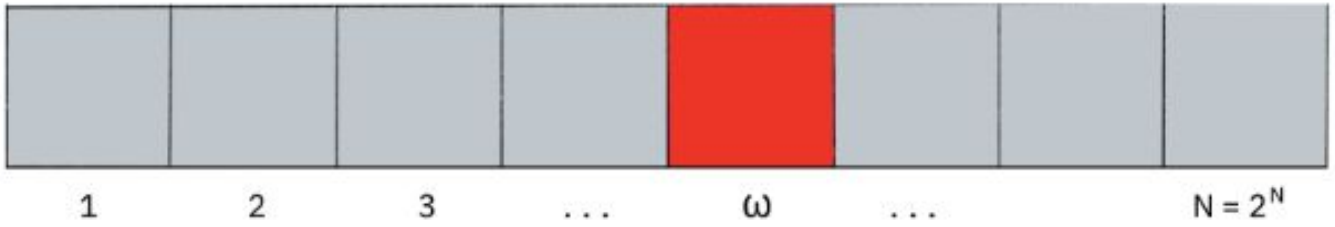
Process of a quantum computer

1. Start in a computational basis state.
2. Apply a sequence of CNOT and single-qubit gates.
3. To obtain the result, measure in the computational basis. The probability of any result, say 00 . . . 0, is just the square of the absolute value of the corresponding amplitude.



Grover's algorithm (1996)

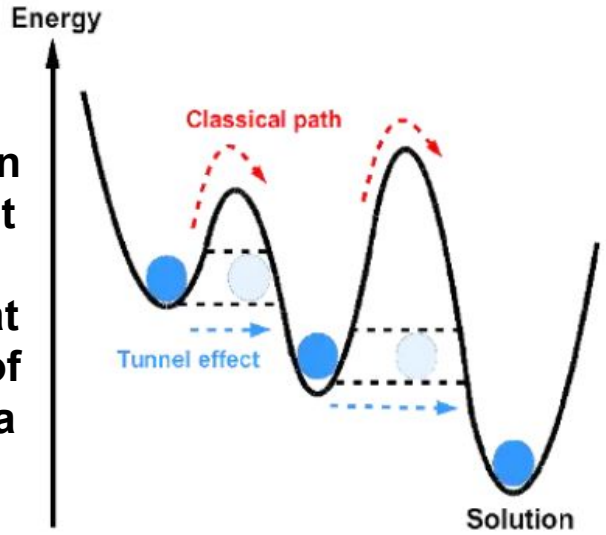
- given a large list of items, we wish to locate a particular item



- in classical computation this is done in O(N)
- in quantum computation there are used just $O(\sqrt{N})$ evaluations

Quantum Annealing

- **physical systems tend to be in the lowest energy state**, called the ground state
- we **encode the information of our optimization problem into a physical system in a way that its ground state is the solution of our problem**
- the program evolves to the ground state naturally, without using quantum gates
- **Quantum annealing is well suited for solving optimization problems**. The approach can quickly **find the most efficient configuration** among many possible combinations of variables.
- D-Wave offers a commercially available **quantum annealer that uses the properties of qubits to find the lowest energy state of a system**, which **corresponds to the optimal solution for a specific problem** that has been mapped against this system.



REFERENCES

1. https://quantum.country/
2. https://quantumcomputing.stackexchange.com/
3. https://quantum-computing.ibm.com/composer/docs/iqx/guide/grovers-algorithm
4. https://www.quantamagazine.org/how-pi-connects-colliding-blocks-to-a-quantum-search-algorithm-20200121/
5. https://quantum-computing.ibm.com/
6. https://www.youtube.com/watch?v=JhHMJCUmq28
7. https://www.youtube.com/watch?v=zvfkXjzzYOo
8. https://medium.com/@quantum_wa/quantum-annealing-cdb129e96601
9. https://defence-industry-space.ec.europa.eu/eu-space/research-development-and-innovation/quantum-technologies_en
10. Ahsan, Usama. "*AutoQP: Genetic Programming for Quantum Programming*." 2020 17th International Bhurban Conference on Applied Sciences and Technology (IBCAST). IEEE, 2020.
11. Spector, L. (2004). *Automatic Quantum Computer Programming: a genetic programming approach* (Vol. 7). Springer Science & Business Media.
12. Mackinnon, Duncan. *Evolving quantum algorithms with genetic programming*. 2017. PhD Thesis. University of Guelph.

Midterm test (I)

Pentru quantum state-ul arbitrar al unui qubit ...

- a. putem face o copie prin entanglement
- b. putem face o copie prin teleportare
- c. nu putem face o copie ✔

Considerand ca intr-un qubit se poate mapa o infinitate de informatie, cati biti de informatie se pot transm

- a. doi biti ✔
- b. foarte multi dar un numar finit de biti
- c. o infinitate de biti

Midterm test (II)

La ce se refera pisica lui Schrodinger?

a. La o superpozitie ✔

b. La pisica pe care Schrodinger efectua experimente cuantice.

c. La pisica pe care o avea Schrodinger si pe care o chema Joey, cea care i-a fost alaturi in ultima par parte din opera sa.

Distanta neintrerupta pentru distributia cuantica de chei criptografice a depasit borna de 1000km?

True ✔

False

Midterm test (III)

La ce se refera initialele EPR ale conceptului 'EPR paradox'?

- a. Einstein, Podolsky, Rosen ✔
- b. Entanglement, Position, Recover
- c. Entanglement, Projections, Rotations

Romania, prin proiectul RoNaQCI, va realiza in 2025, la finele proiectului ...

- a. cea mai mare (ca lungime) retea terestra de QKD din Europa ✔
- b. cea mai mare (ca lungime) retea de QKD din Europa
- c. cea mai mare (ca lungime) retea terestra de comunicatii cuantice din Europa
- d. cea mai mare (ca lungime) retea terestra de QKD din lume

Midterm test (IV)

Ce reprezinta <0|0>?

- a. Un vector
- b. O matrice
- c. Un numar ✔

Lui Sandu Popescu, fizician roman, i se atribuie primul experiment al Teleportarii efectuat cu succes?

- True ✔
- False

Test_2 (I)

Time left 0:29:44

Question 1

Not yet answered

Marked out of 1.00

Flag question

In the quantum teleportation protocol, what is being teleported?

- a. A cat
- b. Entanglement
- c. A quantum state

Clear my choice

Time left 0:27:10

Question 2

Not yet answered

Marked out of 1.00

Flag question

What is a QKD vault?

- a. a Google Drive folder
- b. a software storage structure which aggregates QKD keys obtained from the QKD device
- c. a physical hard drive inside the QKD device

Test_2 (II)

Time left 0:24:44

Question 3

Not yet answered

Marked out of 1.00

Flag question

We can make a copy of an arbitrary unknown quantum state (qubit).

- ○ True
- ◉ False

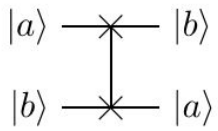
Next page

De adăugat
q4 - q10

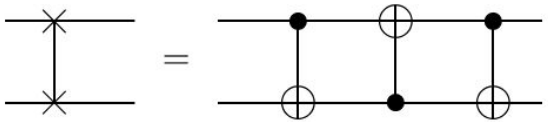
In physics, the no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state, a statement which has profound implications in the field of quantum computing among others.

Exercise 4.1 (Basic quantum circuits)

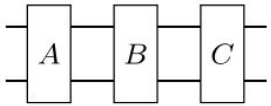
(a) Find the matrix representation (with respect to the computational basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$) of the *swap-gate* $|a, b\rangle \mapsto |b, a\rangle$, which is written in circuit form as



Also show that the swap operation is equivalent to the following sequence of three CNOT gates:



Hint: You can either work directly with basis states, e.g. $|a, b\rangle \overset{\text{CNOT}}{\mapsto} |a, a \oplus b\rangle$, or use matrix representations. In the latter case, note that a sequence of gates like



(with A, B, C unitary 4×4 matrices) corresponds to the matrix product CBA since the circuit is read from left to right, but the input vector in the matrix representation is multiplied from the right.

Test_3 (I)

Question 1

Not yet answered

Marked out of 1.00

Flag question

What is the main goal of post-quantum cryptography?

- a. Use entangled particles in daily messaging
- b. Improve current quantum key distribution
- c. Encrypt quantum bits
- d. Develop classical algorithms resistant to quantum attacks

Test_3 (II)

Question 3

Not yet answered

Marked out of 1.00

Flag question

Who explored the photoelectric effect, further solidifying the idea that light can behave as both a wave and a particle (photons)?

a. Werner Heisenberg

b. Albert Einstein

c. Max Plank

Test_3 (III)

Question 4

Not yet answered

Marked out of 1.00

Flag question

The most particular statement we can make about projector matrices (i.e. satisfying $P^2=P$) is that they are:

- a. Hermitian
- b. square
- c. normal
- d. Unitary

Test_3 (IV)

Question 7

Not yet answered

Marked out of 1.00

Flag question

Which of the following best describes quantum entanglement?

a. A particle being in multiple states at once.

b. A particle transferring energy instantaneously to another.

c. Two particles sharing the same location in space.

d. Two particles whose states remain correlated regardless of the distance between them.

Test_3 (V)

Question 9

Not yet answered

Marked out of 1.00

Flag question

Which of the following gates performs a rotation of π radians on the Z-axis?

a. CNOT

b. Z

c. X

d. Hadamard

Test_3 (VI)

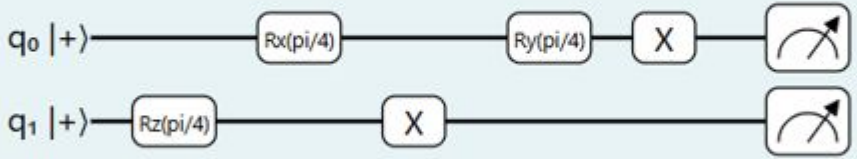
Question 10

Not complete

Marked out of 1.00

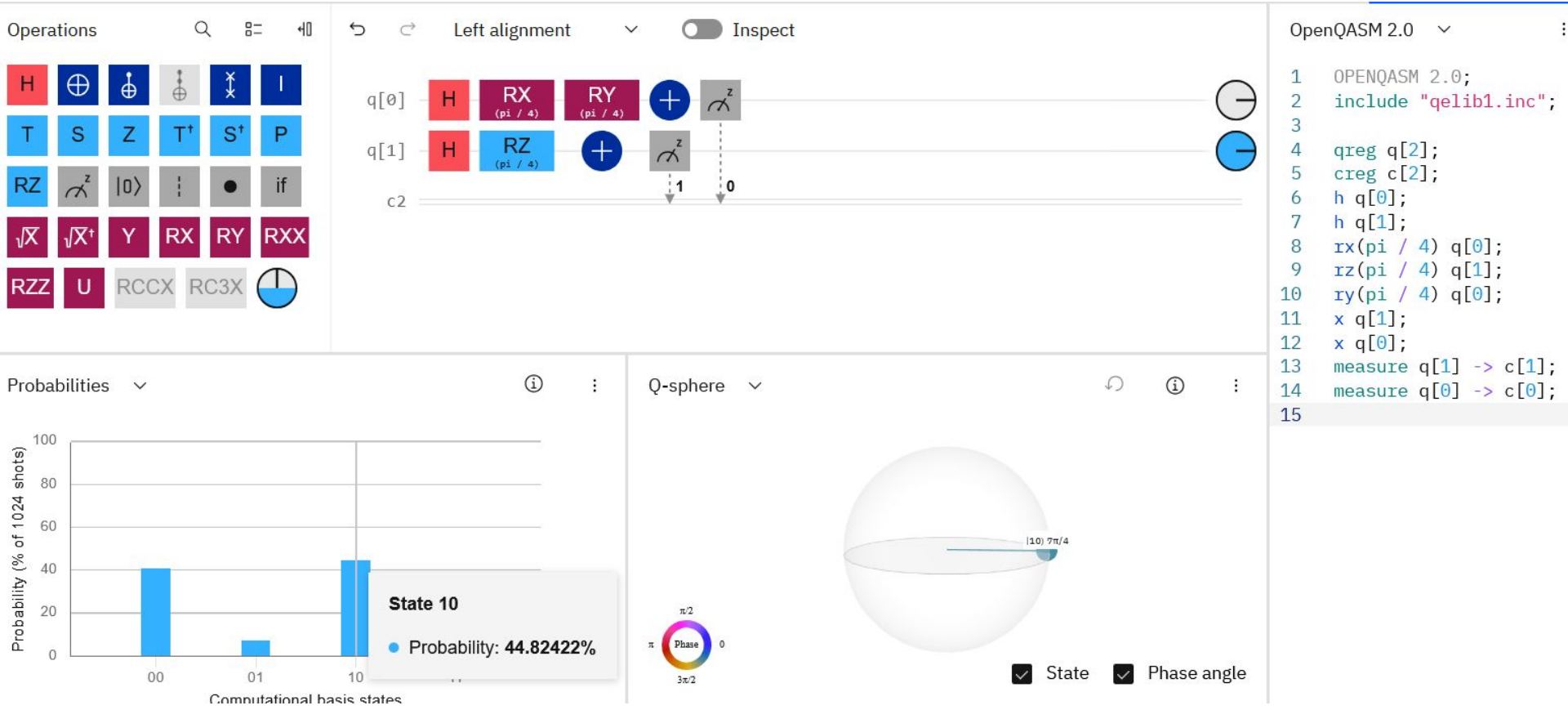
Flag question

2-Qubit Quantum Circuit



What is the probability of measuring $|q_1q_0>$ the state $|10>$ in computational base?

Test_3 (VI) continued



Test_3 (VI) continued..

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}; \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4.1}$$

The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the *rotation operators* about the $\hat{x}$, $\hat{y}$, and $\hat{z}$ axes, defined by the equations:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.4}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.5}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}. \tag{4.6}$$

Test_3 (VII)

Question 2

Not complete

Marked out of 1.00

Flag question

BB84 Protocol

Alice's bits	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0
Alice's bases	X	X	Z	Z	X	X	X	X	Z	Z	Z	X	X	X	Z	Z
Bob's bases	X	Z	X	Z	X	X	X	Z	X	X	Z	X	X	X	Z	X
Bob's measurements	1	0	1	1	0	0	0	0	1	0	0	1	0	0	0	0

Alice and Bob are performing the BB84 quantum key distribution protocol.

After transmitting and measuring the qubits, they publicly disclose their measurement bases and their measurement values

Write the Quantum Bit Error Rate (QBER) value for this run of the protocol:

Test_3 (VIII)

Which of the following kets denotes a pure separable quantum state? Write the digit of the correct answer:

1)

$$\begin{pmatrix} \frac{-16-63i}{130} \\ \frac{33+56i}{130} \\ \frac{-33+56i}{130} \\ \frac{-16+63i}{130} \end{pmatrix}$$

2)

$$\begin{pmatrix} \frac{198-336i}{845} \\ \frac{24-7i}{130} \\ \frac{33-56i}{338} \\ \frac{-144+42i}{325} \end{pmatrix}$$

3)

$$\begin{pmatrix} \frac{-16+63i}{130} \\ -1i \\ \frac{1i}{4} \\ \frac{-16-63i}{130} \end{pmatrix}$$

4)

$$\begin{pmatrix} \frac{1i}{2} \\ \frac{33+56i}{130} \\ \frac{33-56i}{130} \\ \frac{-1i}{2} \end{pmatrix}$$

Test_3 (IX)

Which of the following kets denotes a pure quantum state? Write the digit of the correct answer:

1)

$$\begin{pmatrix} \frac{12 - 5i}{13} \\ \frac{5 + 12i}{13} \end{pmatrix}$$

2)

$$\begin{pmatrix} \frac{5 + 12i}{13} \\ \frac{4 + 3i}{5} \end{pmatrix}$$

3)

$$\begin{pmatrix} \frac{60 + 144i}{169} \\ \frac{109 - 144i}{169} \end{pmatrix}$$

4)

$$\begin{pmatrix} \frac{60 + 144i}{169} \\ \frac{4 + 3i}{13} \end{pmatrix}$$

General Properties of Density Matrices

Consider an observable A in the "pure" state $|\psi\rangle$ with the expectation value given by

$$\langle A \rangle_\psi = \langle \psi | A | \psi \rangle , \tag{9.1}$$

then the following definition is obvious:

Definition 9.1 *The **density matrix** ρ for the pure state $|\psi\rangle$ is given by*

$$\rho := |\psi\rangle\langle\psi|$$

This density matrix has the following properties:

$$\text{I)} \quad \rho^2 = \rho \quad \text{projector} \tag{9.2}$$

$$\text{II)} \quad \rho^\dagger = \rho \quad \text{hermiticity} \tag{9.3}$$

$$\text{III)} \quad \mathrm{Tr}\,\rho = 1 \quad \text{normalization} \tag{9.4}$$

$$\text{IV)} \quad \rho \geq 0 \quad \text{positivity} \tag{9.5}$$

Test_3 (X)

Which of the following matrices denotes a quantum gate? Write the digit of the correct answer:

1)

$$\begin{pmatrix} \frac{21+72i}{125} & \frac{-384-112i}{625} \\ \frac{28+96i}{125} & \frac{216+63i}{625} \end{pmatrix}$$

2)

$$\begin{pmatrix} \frac{21+72i}{125} & \frac{3i}{5} \\ \frac{28+96i}{125} & \frac{4i}{5} \end{pmatrix}$$

3)

$$\begin{pmatrix} \frac{21+72i}{125} & \frac{-4i}{5} \\ \frac{28+96i}{125} & \frac{3i}{5} \end{pmatrix}$$

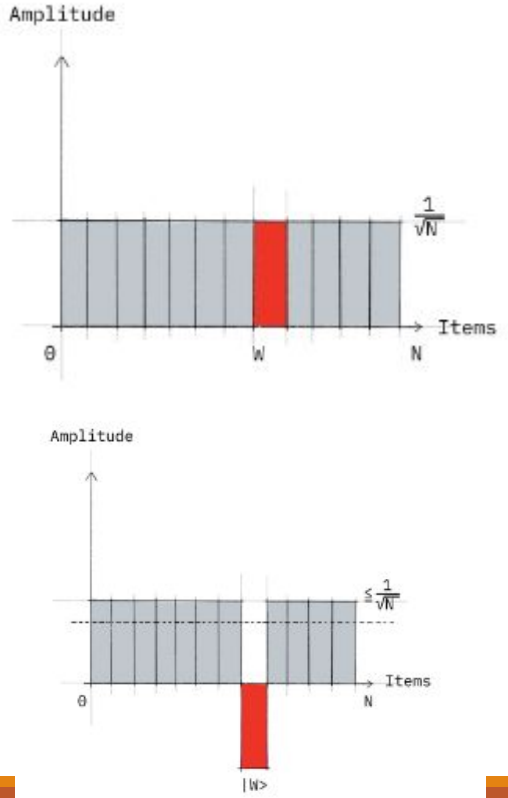
4)

$$\begin{pmatrix} \frac{21+72i}{125} & \frac{-96-28i}{125} \\ \frac{28+96i}{125} & \frac{72+21i}{125} \end{pmatrix}$$

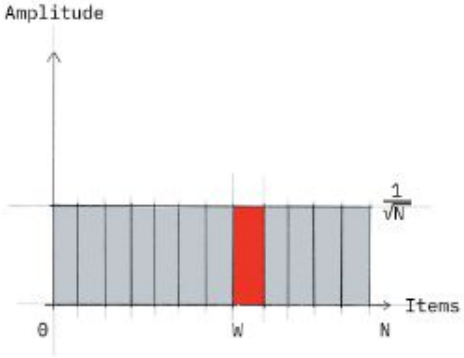
Quantum search

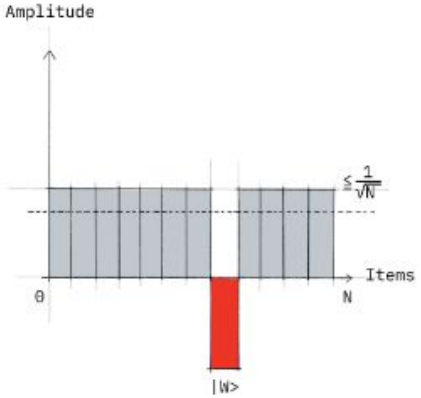
Example of a quantum oracle for w=101

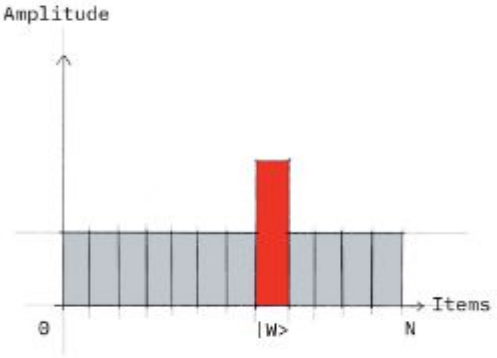
$$U_w = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{-1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

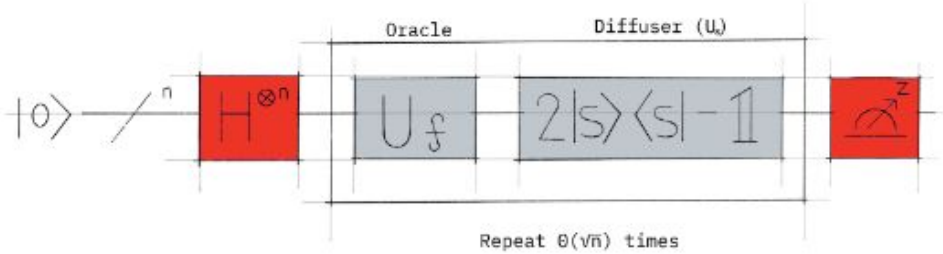


Quantum search





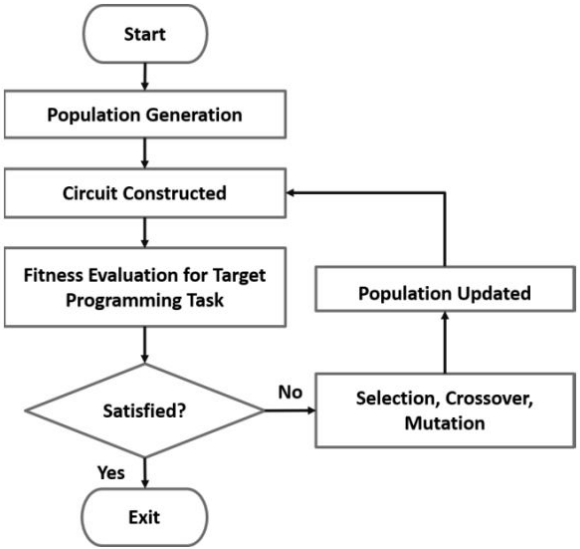




Genetic Programming

- an automated method for creating a working computer program from a high-level problem statement of a problem
- it starts from a high-level statement of “what needs to be done” and automatically creates a computer program to solve the problem
- especially used for symbolic regression
- for Quantum Computing Linear Genetic Programming can be used

Linear Genetic Programming for Quantum Computing



(H, 0)	(CX, 3, 0)	(H, 1)	(X, 0)	(H, 3)	(H, 2)	(X, 2)

Target

- generate a quantum program that performs quantum search for N items
- this program should work for any input function (oracle)

Fitness function

$$\text{fitness}(o_i) = \sum_{i=1}^{N} |o_i - y_i|$$

$o_i = \text{program output}, \quad y_i = \text{desired output}$

Mutation(s)

- index + gate mutation
- index mutation
- gate mutation
- permutation

Crossover

Genetic Algorithms: Uniform Crossover

- In Uniform Crossover, a value of the first parent's gene is assigned to the first offspring and the value of the second parent's gene is to the second offspring with probability 0.5.
- With probability 0.5 the value of the first parent's gene is assigned to the second offspring and the value of the second parent's gene is assigned to the first offspring.

Example:

- Parent 1: **X** X **X** X X **X** X
- Parent 2: Y **Y** Y **Y** **Y** Y **Y**
- Offspring 1: **X** **Y** **X** **Y** **Y** **X** **Y**
- Offspring 2: Y X Y X X Y X

Example of generated programs for 2-qubits

```
:(H(2))
:(H(1))
:(oracle(w))
:(H(1))
:(H(1))
:(H(1))
:(Z(1))
:(CZ(2, 2))
:(H(2))
:(X(1))
:(CZ(2, 1))
:(H(1))
:(H(2))
```

```
:(H(2))
:(H(1))
:(oracle(w))
:(H(1))
:(X(1))
:(H(2))
:(H(1))
:(CNOT(2, 1))
:(CNOT(1, 1))
:(X(1))
:(CZ(1, 1))
:(H(2))
:(Z(1))
```

```
:(X(1))
:(H(1))
:(H(2))
:(Z(1))
:(Z(2))
:(oracle(w))
:(H(2))
:(H(2))
:(Z(1))
:(H(1))
:(CNOT(1, 2))
:(Z(2))
:(H(1))
```