



HAL
open science

Quantum technologies

Kenneth Maussang

► **To cite this version:**

Kenneth Maussang. Quantum technologies. Master. Introduction to Quantum Computing, France. 2023, pp.80. hal-04423755

HAL Id: hal-04423755

<https://cel.hal.science/hal-04423755>

Submitted on 29 Jan 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Quantum technologies

Introduction to Quantum Computing

Kenneth MAUSSANG

Université de Montpellier

2022 – 2023

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

- 1 Quantum revolution(s)
 - The first quantum revolution
 - The second quantum revolution
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

- 1 Quantum revolution(s)
 - The first quantum revolution
 - The second quantum revolution
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

I.1. The first quantum revolution

Modern physics mainly relies on the development of quantum mechanics theory. Beneath conceptual and philosophical consequences, it has deeply impacted our all-day life with the development of several new technologies

- semiconductors ;
- NMR systems ;
- lasers ;
- atomic clock (GPS).

These devices are sometimes designed as *quantum 1.0*, that is devices which rely on the effects of quantum mechanics.

- 1 Quantum revolution(s)
 - The first quantum revolution
 - The second quantum revolution
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

1.2. The second quantum revolution

Quantum technologies are often described as the *second quantum revolution* or *quantum 2.0*. They are generally regarded as a class of devices that actively create, manipulate and read out quantum states of matter, often using quantum effects of superposition and entanglement.

The field of quantum technology was first outlined in a 1997 book by Gerard J. Milburn. The field of quantum technology has benefited immensely from the influx of new ideas from the field of quantum information processing, particularly quantum computing.

1.2. The second quantum revolution

The Quantum Manifesto was signed by 3,400 scientists and officially released at the 2016 Quantum Europe Conference, calling for a quantum technology initiative to coordinate between academia and industry, to move quantum technologies from the laboratory to industry, and to educate quantum technology professionals in a combination of science, engineering, and business.

The European Commission responded to that manifesto with **the Quantum Technology Flagship**, a €1 Billion, 10-year-long megaproject, similar in size to earlier European Future and Emerging Technologies Flagship projects such as the Graphene Flagship and Human Brain Project. China is building the world's largest quantum research facility with a planned investment of 76 Billion Yuan (approx. €10 Billion). The USA, Canada, Australia, Japan and the UK are also preparing national initiatives.

https://en.wikipedia.org/wiki/Quantum_technology

1.2. The second quantum revolution

Quantum technologies are classified into four applicative domains

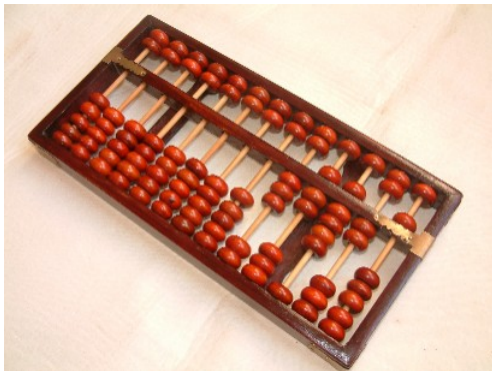
- **Quantum sensing and quantum metrology**
atomic clocks, quantum gravimeters, quantum magnetometers,...
- **Quantum simulators**
modelling in a pure and controlled way the behavior of quantum systems that cannot be calculated
- **Quantum communications**
secured communications that insure the inviolability of the information communicated
- **Quantum computing**
quantum speed-up of calculations

- 1 Quantum revolution(s)
- 2 Classical computer
 - Brief history of classical computers
 - Classical bits
 - Classical electronics
 - Moore's law
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

- 1 Quantum revolution(s)
- 2 **Classical computer**
 - Brief history of classical computers
 - Classical bits
 - Classical electronics
 - Moore's law
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

II.1. Brief history of classical computers

A computer is a calculator.



<https://commons.wikimedia.org/wiki/File:Boulier1.JPG>

The abacus is the oldest form of calculator.

II.1. Brief history of classical computers

The natural basis of calculation is base 10 (10 fingers of the hand).

For a long time, the unit of calculation was the pebble (*le caillou*) (used in the first abacuses).

In Latin pebble = *calculus*.

Analog calculator

An analog calculator is a calculator that **uses continuous physical measurements** (e.g. electrical) to model a problem to be solved. It is more of a simulator than a computer (e.g. for predicting the motion of planets).

Analog computers are (or more accurately were) very well suited to solving ordinary differential equation systems thanks to their integrators that perform true integration as a function of time.

First mechanical calculators



https://commons.wikimedia.org/wiki/File:Arts_et_Metiers_Pascaline_dsc03869.jpg

Musée des Arts et Métiers (Paris). Photo : David Monniaux, 2005.

A *Pascaline*, a mechanical calculator developed by Blaise Pascal (1652).

II.1. Brief history of classical computers

Binary, octal and hexadecimal systems.

TABLE 86 MEMOIRES DE L'ACADEMIE ROYALE

DES
NOMBRES.

bres entiers au-dessus du double du plus haut degré. Car icy, c'est comme si on disoit, par exemple, que 111 ou 7 est la somme de quatre, de deux & un. Et que 1101 ou 13 est la somme de huit, quatre & un. Cette propriété sert aux Effayeurs pour peser toutes sortes de masses avec peu de poids, & pourroit servir dans les monnoyes pour donner plusieurs valeurs avec peu de pieces.

Cette expression des Nombres étant établie, sert à faire tres-facilement toutes sortes d'operations.

Pour l'Addition par exemple.

Pour la Soustraction.

Pour la Multiplication.

Pour la Division.

Et toutes ces operations sont si aisées, qu'on n'a jamais besoin de rien effayer ni deviner, comme il faut faire dans la division ordinaire. On n'a point besoin non-plus de rien apprendre par cœur icy, comme il faut faire dans le calcul ordinaire, où il faut sçavoir, par exemple, que 6 & 7 pris ensemble font 13; & que 5 multiplié par 3 donne 15, suivant la Table d'une fois au off un, qu'on appelle Pythagorique. Mais icy tout cela se trouve & se prouve de source, comme l'on voit dans les exemples précédens sous les signes ☉ & ⊙.

Simplicity of multiplication and binary division.

Multiply by 2 = add a 0

$$11 \times 2 = 22$$

$$1011 \times 10 = 10110$$

Divide by 2 = remove the last digit corresponding to the rest

$$11 \div 2 = 5 \text{ hold } 1$$

$$1011 \div 10 = 101 \text{ hold } 1$$

https://commons.wikimedia.org/wiki/File:Leibniz_binary_system_1703.png

Explication de l'Arithmétique Binaire,
G. W. Leibniz (1703-1705)

II.1. Brief history of classical computers

Octal : basis $8 = 2^3$.

Each 3-bit packet is the binary writing of a digit in base 8.

$$\begin{aligned} 0_8 &= 000, & 1_8 &= 001, & 2_8 &= 010, & 3_8 &= 011, \\ 4_8 &= 100, & 5_8 &= 101, & 6_8 &= 110, & 7_8 &= 111. \end{aligned}$$

For example,

$$10101101110_2 = 10:101:101:110 = 2556_8.$$

II.1. Brief history of classical computers

Hexadecimal : basis $16 = 2^4$.

0, 1, 2, ..., 9, A, B, C, D, E and F.

Each 4-bit packet is the binary writing of a digit in base 16.

$$A_{16} = 10_{10} = 1010_2, B_{16} = 11_{10} = 1011_2, C_{16} = 12_{10} = 1100_2,$$

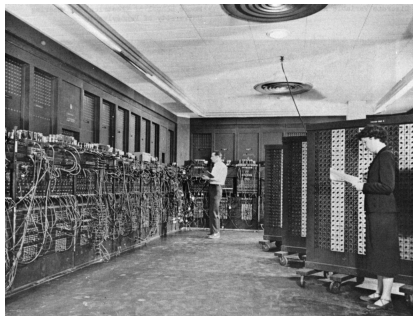
$$D_{16} = 13_{10} = 1101_2, E_{16} = 14_{10} = 1110_2, F_{16} = 15_{10} = 1111_2.$$

For example,

$$10101101110_2 = 101:0110:1110 = 56E_{16}.$$

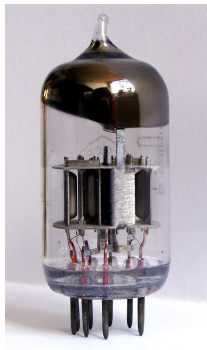
II.1. Brief history of classical computers

First computers



ENIAC (Electronic Numerical Integrator And Computer) in Philadelphia, Pennsylvania, in 1945. Building 328, the Ballistic Research Laboratory (BRL). Photo : US Army.

<https://fr.wikipedia.org/wiki/ENIAC>



ENIAC is based on vacuum tube transistors.

fr.wikipedia.org/wiki/Tube_%C3%A9lectronique

II.1. Brief history of classical computers

ENIAC is one of the first computers built, developed in 1945 by IBM. Before ENIAC, Colossus has been developed in 1943 to decrypt secret messages emitted by Germans. But ENIAC was the **first computer, fully made out of electronics, designed to be *Turing-complet***: it may be reprogrammed to solve any calculation problem (in theory).

The ENIAC weighted 30 tons, with an occupied surface of 72m² and a power consumption of 140 kW !

II.1. Brief history of classical computers

The completed machine was announced to the public the evening of February 14, 1946 and formally dedicated the next day at the University of Pennsylvania, having cost almost \$500,000 (approximately \$6,300,000 today).

The basic machine cycle was 200 microseconds (20 cycles of the 100 kHz clock in the cycling unit), or 5,000 cycles per second for operations on the 10-digit numbers. In one of these cycles, ENIAC could write a number to a register, read a number from a register, or add/subtract two numbers.

Two major technological breakthrough:

- semiconductor transistors ;
- magnetic memories.

It has permits to downsize computers through miniaturization and increased performances of devices.

II.1. Brief history of classical computers

The IBM 305 RAMAC was the first commercial computer that used a moving-head hard disk drive (magnetic disk storage) for secondary storage. The system was publicly announced on September 14, 1956, with test units already installed at the U.S. Navy and at private corporations.

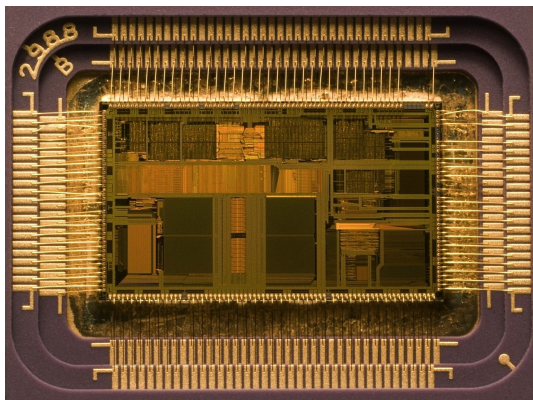


Photo by U. S. Army Red River Arsenal.

commons.wikimedia.org/wiki/File:BRL61-IBM_305_RAMAC.jpeg

II.1. Brief history of classical computers

Miniaturization thanks to advances in microelectronics (integrated circuits from 1960 and microprocessors from 1970).



The Intel 80486, also known as the i486 or 486, introduced in 1989.

https://en.wikipedia.org/wiki/Intel_80486

- 1 Quantum revolution(s)
- 2 **Classical computer**
 - Brief history of classical computers
 - **Classical bits**
 - Classical electronics
 - Moore's law
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

II.2. Classical bits

The elementary block of classical logic is the **bit** (classical bit).

A bit may takes only two values: 0 or 1.

An ensemble of bits is used to "encode" an integer in binary. The information is stored in the form of a succession of bits:

01100101001011100.

The numerical calculation is performed using logic gates: NOT, OR, XOR, CNOT,...

11.2. Classical bits

Numerization (or digitization) is a process that permits to express a decimal integer number into a binary basis. Let $(n, N) \in \mathbb{N}^2$ be two integers such that $n < 2^N - 1$. Then

$$\exists \{a_i\}^N \in \{0, 1\} \text{ such that } n = \sum_{i=0}^N a_i \times 2^i.$$

The ensemble of $\{a_i\}$ is the binary decomposition of the number n on the binary basis, a_0 being units, a_1 being tens, a_2 being hundreds, etc...

Let denote n_2 the expression of n in binary basis, encoded over N bits:

$$n_2 = a_N a_{N-1} a_{N-2} \cdots a_2 a_1 a_0.$$

II.2. Classical bits

Example: coding on 4 bits ($N = 4$)

$$1 = 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 \Rightarrow 0001,$$

$$2 = 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 \Rightarrow 0010,$$

$$3 = 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 \Rightarrow 0011,$$

$$4 = 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0 \Rightarrow 0100,$$

etc...

Only integers are converted into binary numbers. For a real number (a "float"), one may transform it into several integer data.

II.2. Classical bits

Depending on the value of N , a number may or may not be converted to N bits (i.e. N binary digits). Thus, N will define the maximum value of the integer decimal number that can be encoded on N bits (or N binary digits).

The choice of the number of bits used: compromise between the number of values needed, the available memory and the calculation or acquisition speed (Cf. FFT and sampling rate).

II.2. Classical bits

Examples:

Coding on 8 bits (1 octet): from 00000000 to 11111111 (which corresponds to the valeur $2^8 - 1 = 255$).

Coding on 16 bits (1 octet): $2^{16} - 1 = 65,535$ values.

Color scales on 8 bits: 8 bits in RGB system is 8 bits for Red, 8 bits for Green and 8 bits for Blue, that is $3 \times 8 = 24$ bits for a single pixel.

24 bits = 16,777,216 \approx 16 millions of colors.

- 1 Quantum revolution(s)
- 2 **Classical computer**
 - Brief history of classical computers
 - Classical bits
 - **Classical electronics**
 - Moore's law
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

II.3. Classical electronics

Key elements of classical microelectronics :

- resistors;
- capacitors;
- inductances;
- diodes;
- **transistors.**

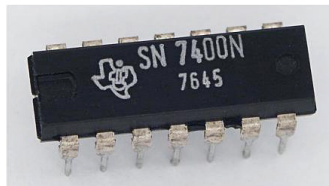
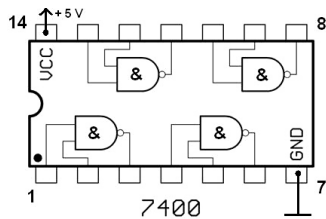
These elements are the basic blocks of modern technologies of information and communication.

II.3. Classical electronics

Properties:

- governed by classical physics law;
- no quantum effects;
- no quantum states superposition;
- no quantum field quantification.

Integrated circuits



The view and element placement of the popular chip 7400 from Texas Instruments. The chip contains four logical elements AND-NOT (NAND). The two additional contacts supply power (+5 V) and connect the ground. This chip was made in the 45th week of 1976.

https://fr.wikipedia.org/wiki/Fonction_logique

Technological breakthrough: the transistor



The invention of the transistor earned researchers at Bell Labs a Nobel prize.

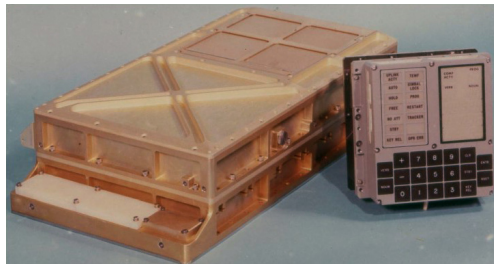
Science Museum/Science & Society.



In 1997 Lucent Technologies created this replica to commemorate the 50th anniversary of the invention of the point-contact transistor at Bell Labs in December 1947.

https://en.wikipedia.org/wiki/History_of_the_transistor
<https://www.nature.com/news/2008/080820/full/454927a.html>

Technological breakthrough: the transistor

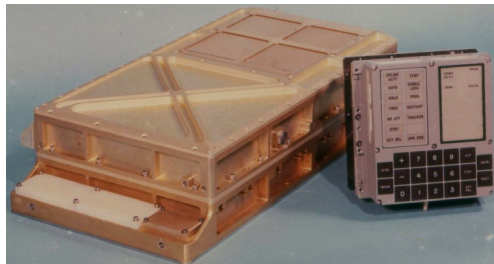


The DSKEY input module (right) shown alongside the Apollo Guidance Computer's main casing (left).

The Apollo Guidance Computer (AGC) is a digital computer produced for the Apollo program that was installed on board each Apollo command module (CM) and Apollo Lunar Module (LM). The AGC provided computation and electronic interfaces for guidance, navigation, and control of the spacecraft.

https://en.wikipedia.org/wiki/Apollo_Guidance_Computer

Technological breakthrough: the transistor

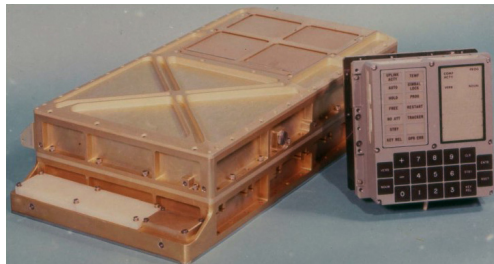


The DSKEY input module (right) shown alongside the Apollo Guidance Computer's main casing (left).

The AGC has a 16-bit word length, with 15 data bits and one parity bit, with a processor made out of **12,300 transistors**. Astronauts communicated with the AGC using a numeric display and keyboard called the DSKY (for "display and keyboard", pronounced "DIS-kee").

https://en.wikipedia.org/wiki/Apollo_Guidance_Computer

Technological breakthrough: the transistor

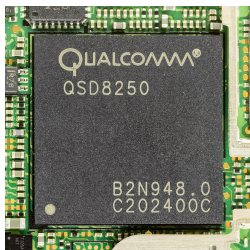


The DSKEY input module (right) shown alongside the Apollo Guidance Computer's main casing (left).

The AGC was the first silicon integrated circuit based computer. The computer's performance was comparable to the first generation of home computers from the late 1970s, such as the Apple II, TRS-80, and Commodore PET.

https://en.wikipedia.org/wiki/Apollo_Guidance_Computer

Technological breakthrough: the transistor



HTC Desire - main board - Qualcomm
QSD8250 - Snapdragon CPU 1GHz
Scorpion.

https://en.wikipedia.org/wiki/Qualcomm_Snapdragon
https://en.wikipedia.org/wiki/Transistor_count

Qualcomm Snapdragon processors might be found in smartphones. The model 8cx / SCX8180 has been released in 2018.

The smallest size of transistors of this chip is **7nm only**.

It results in **8,500,000,000 transistors on a 112 mm² chip**.

- 1 Quantum revolution(s)
- 2 **Classical computer**
 - Brief history of classical computers
 - Classical bits
 - Classical electronics
 - **Moore's law**
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

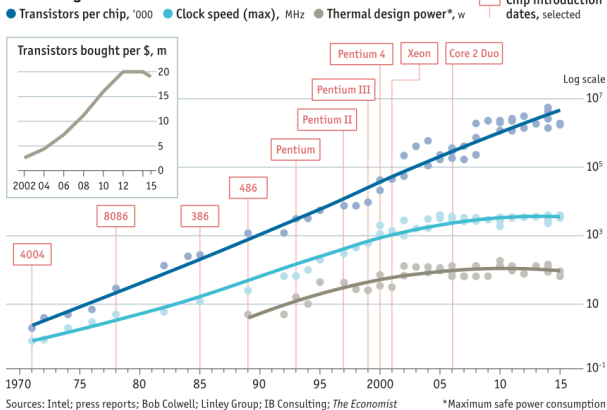
II.4. Moore's law

Moore's Law states that the number of transistors on a microchip doubles about every two years, though the cost of computers is halved. In 1965, Gordon E. Moore, the co-founder of Intel, made this observation that became Moore's Law.

In other words, Moore's Law says that the growth of microprocessors is exponential.

11.4. Moore's law

Stuttering



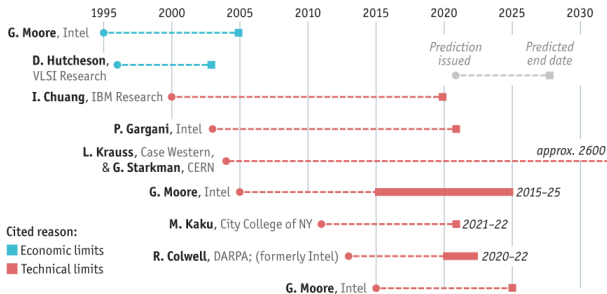
Technology Quarterly After Moore's law, *The Economist* (March, 12th 2016)

<https://www.economist.com/technology-quarterly/2016-03-12/after-moores-law>

11.4. Moore's law

Faith no Moore

Selected predictions for the end of Moore's law



Sources: Intel; press reports; *The Economist*

Technology Quarterly After Moore's law, *The Economist* (March, 12th 2016)

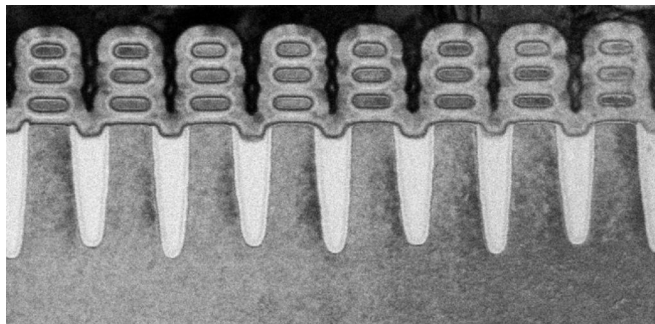
<https://www.economist.com/technology-quarterly/2016-03-12/after-moores-law>

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?**
 - Moore's law and quantum effects
 - IBM's roadmap 2014
 - Benefits from quantum mechanics
- 4 Complexity, algorithms, and quantum computers
- 5 References

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?**
 - Moore's law and quantum effects
 - IBM's roadmap 2014
 - Benefits from quantum mechanics
- 4 Complexity, algorithms, and quantum computers
- 5 References

III.1. Moore's law and quantum effects

June 2017: 5nm transistors reported by IBM research !

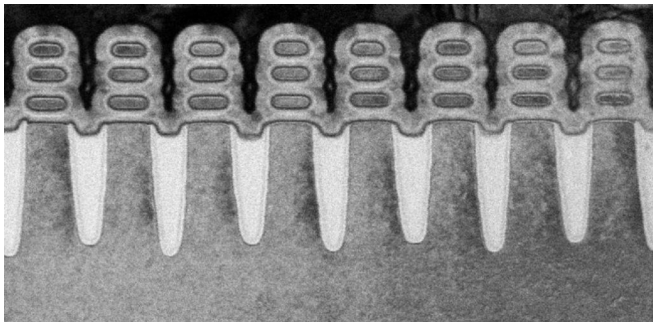


For reference, it takes 10 to 15 years of research and development before a groundbreaking new chip technology proliferates the market.

Today's chips with vertical "fin" transistors, called FinFET, power today's most-powerful 14nm, 10nm and 7nm chips.

III.1. Moore's law and quantum effects

June 2017: 5nm transistors reported by IBM research !



After about a decade of studying the idea of putting gates all around the transistor – often referred to as Gate-All-Around (GAA) – stacked nanosheets delivered a GAA transistor for the 5nm node that actually improved density, performance, and power – all built with industry manufacturable tools and processes.

<https://www.ibm.com/blogs/think/2017/06/5-nanometer-transistors/>

III.1. Moore's law and quantum effects

In the context of logic technology scaling, **Moore's Law breaks down into four parts**: density, performance, power and economy.

- Density, or the number of transistors per square inch of a chip, has gone from Gordon Moore's original observation in 1965 of doubling every 12 months, to now taking three years.
- Performance improvements have experienced a similar slowing.
- Power, while less influential at its introduction, has grown in importance due to our battery-hungry mobile devices.
- The economy, or cost per transistor, is the only element of the "law" that's kept similar pace over the last 50 years.

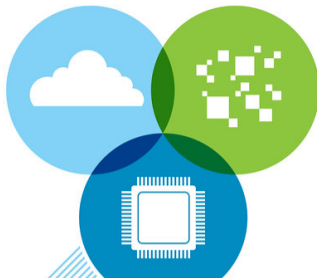
<https://www.ibm.com/blogs/think/2017/06/5-nanometer-transistors/>

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?**
 - Moore's law and quantum effects
 - IBM's roadmap 2014
 - Benefits from quantum mechanics
- 4 Complexity, algorithms, and quantum computers
- 5 References

IBM is investing \$3 billion to push the limits of chip technology

Cloud and big data applications are placing new challenges on systems, just as the underlying chip technology is facing significant physical scaling limits.

IBM is investing **\$3 billion** over the next five years in **two R&D programs** that will push IBM's semiconductor innovations from today's breakthroughs into the advanced technology leadership required for the future.



<https://www-03.ibm.com/press/us/en/pressrelease/44357.wss>

Just how
small is
7nm?

A strand
of human
**DNA is 2.5
nanometers**
in diameter.



<https://www-03.ibm.com/press/us/en/pressrelease/44357.wss>

III.2. IBM's roadmap 2014

7 nanometer and beyond

Serious physical challenges are threatening current semiconductor scaling techniques and will impede the ability to manufacture advanced chips.



Semiconductors show promise to scale from **today's 22 nanometers** down to 14 and then 10 nanometers in the next several years, with scaling to **7 nanometers** and perhaps below by the end of the decade.

Bridge to a post-silicon era

Silicon transistors, tiny switches that carry information on a chip, have been made smaller year after year, but they are approaching a point of **physical limitation**.

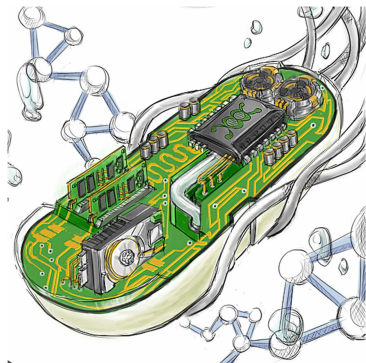


Beyond 7 nanometers, the challenges dramatically increase, requiring a new kind of material to power systems of the future. Potential alternatives include new materials such as **carbon nanotubes**, and computational approaches such as **neuromorphic computing** and **quantum computing**.

<https://www-03.ibm.com/press/us/en/pressrelease/44357.wss>

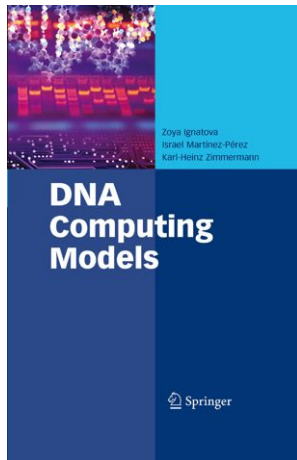
III.2. Rethinking computers

DNA based calculators



Inner Workings: DNA for data storage and computing
PNAS December 29, 2015 112 (52) 15771-15772

<https://www.pnas.org/content/112/52/15771>



<https://link.springer.com/book/10.1007/>

978-0-387-73637-2

DNA based calculators

Report



molecular
systems
biology

Programming *Escherichia coli* to function as a digital display

Jonghyeon Shin, Shuyi Zhang, Bryan S Der, Alec AK Nielsen & Christopher A Voigt* 

<https://www.embopress.org/doi/full/10.15252/msb.20199401>

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?**
 - Moore's law and quantum effects
 - IBM's roadmap 2014
 - Benefits from quantum mechanics**
- 4 Complexity, algorithms, and quantum computers
- 5 References

III.3. Benefits from quantum mechanics

Transistors are getting smaller and smaller: quantum effects are no longer negligible...

Several strategies for *post-silicon* electronics, one of them being *quantum electronics* and *quantum computing*.

Quantum computing fully exploits **quantum superposition** and **quantum entanglement**, key elements of quantum algorithms.

Quantum algorithm will outperform classical ones only if they fully exploit quantum superposition and entanglement.

Consequently, it requires to fundamentally rethink algorithms.

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
 - Turing machine
 - Complexity
 - Reversible computing
 - Quantum computers
- 5 References

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers**
 - Turing machine
 - Complexity
 - Reversible computing
 - Quantum computers
- 5 References

IV.1. Turing machine

A Turing machine is a mathematical model of computation that defines an abstract machine, which manipulates symbols on a strip of tape according to a table of rules.

Despite the model's simplicity, given any computer algorithm, a Turing machine capable of simulating that algorithm's logic can be constructed.

https://en.wikipedia.org/wiki/Turing_machine

IV.1. Turing machine

Example of Turing machine.

The machine might be in different states labeled A, B, C, \dots, U and V . The machine read a tape on which each case might be blank or with a finite number of symbols labeled $0, 1, X, Y, \dots$

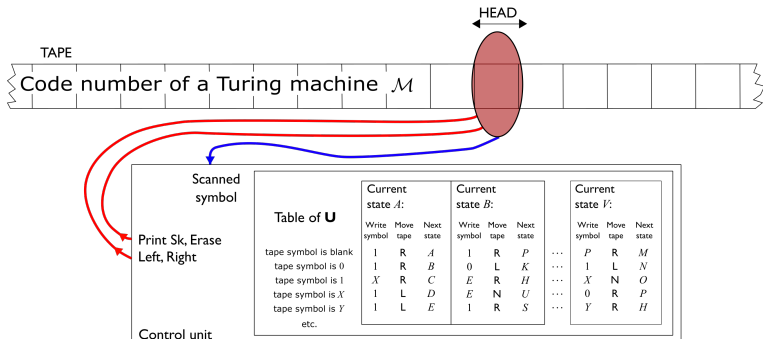


Figure derived from https://commons.wikimedia.org/wiki/File:Universal_Turing_machine.svg,
author: Ch Buckley

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers**
 - Turing machine
 - Complexity**
 - Reversible computing
 - Quantum computers
- 5 References

IV.2. Complexity

In computational complexity theory, NP (nondeterministic polynomial time) is a complexity class used to classify decision problems. NP is the set of decision problems for which the problem instances, where the answer is "yes", have proofs verifiable in polynomial time.

An equivalent definition of NP is the set of decision problems solvable in polynomial time by a non-deterministic Turing machine. This definition is the basis for the abbreviation NP; "nondeterministic, polynomial time."

<https://en.wikipedia.org/wiki/Complexity>

IV.2. Complexity

A problem is said to be NP-hard if everything in NP can be transformed in polynomial time into it, and a problem is NP-complete if it is both in NP and NP-hard. The NP-complete problems represent the hardest problems in NP. If any NP-complete problem has a polynomial time algorithm, all problems in NP do.

It is not known whether every problem in NP can be quickly solved—this is called the P versus NP problem. But if any NP-complete problem can be solved quickly, then every problem in NP can, because the definition of an NP-complete problem states that every problem in NP must be quickly reducible to every NP-complete problem (that is, it can be reduced in polynomial time). Because of this, it is often said that NP-complete problems are harder or more difficult than NP problems in general.

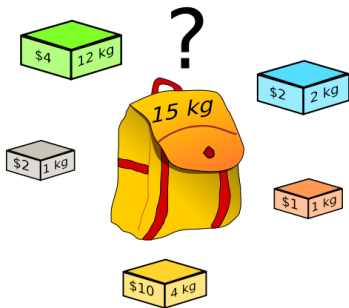
<https://en.wikipedia.org/wiki/NP-completeness>

Examples of NP-complet problems.

- boolean satisfiability problem (sometimes abbreviated SATISFIABILITY or SAT);
- travelling salesman problem;
- minimum k-cut ;
- Knapsack problem.

https://en.wikipedia.org/wiki/List_of_NP-complete_problems

IV.2. Complexity



<https://commons.wikimedia.org/wiki/File:Knapsack.svg>

Example of a one-dimensional (constraint) knapsack problem: which boxes should be chosen to maximize the amount of money while still keeping the overall weight under or equal to 15 kg?

A multiple constrained problem could consider both the weight and volume of the boxes.

https://en.wikipedia.org/wiki/Knapsack_problem

Circuit model: boolean logic, logical gates.

Morgan's theorem: a OR gate might be realized with AND and NOT gates.

Universality of circuit model. But a circuit is not programmable; a circuit is dedicated to a given problem. The number of logical gates is exponential with the number of bits (2^n).

The **von Neumann architecture** permits to solve this problem with programmable computers but computing time remains an issue.

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers**
 - Turing machine
 - Complexity
 - Reversible computing**
 - Quantum computers
- 5 References

Landauer's principle:

erasing a bit of information requires at least an energy of $k_B T \log 2$.

Irreversibility and heat generation in the computing process, Rolf LANDAUER,
IBM Journal of Research and Development, 5:183 (1961)

Reversible computing:

Reversible computing is a model of computing where the computational process is time-reversible.

In a model of computation that uses deterministic transitions from one state of the abstract machine to another, a necessary condition for reversibility is that the relation of the mapping from states to their successors must be one-to-one.

In other words, if one knows the outputs, it is possible to reconstruct inputs (that is why it is called reversible).

IV.3. Reversible computing

Example of reversible computing with billiard balls:

BBM - Billard Ball Machine, E. Fredkin and T. Toffolin (1982)

<http://jameslin.name/bball/>

https://en.wikipedia.org/wiki/Billiard-ball_computer

Logical boolean gates are NOT reversible, but quantum calculation is reversible (as a results of unitarity properties of operators).

Reversible computing is not submitted to Landauer's limit, and therefore neither is quantum computing.

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
 - Turing machine
 - Complexity
 - Reversible computing
 - Quantum computers
- 5 References

IV.4. Quantum computers

Definition of a quantum machine: **Di Vincenzo criteria**.

Constructing a quantum computer requires five conditions:

- A scalable physical system with well characterized qubit ;
- The ability to initialize the state of the qubits to a simple fiducial state ;
- Long relevant decoherence times ;
- A "universal" set of quantum gates ;
- A qubit-specific measurement capability.

For quantum communications, two additional conditions are required:

- The ability to interconvert stationary and flying qubits ;
- The ability to faithfully transmit flying qubits between specified locations.

https://en.wikipedia.org/wiki/DiVincenzo%27s_criteria



IV.4. Quantum computers

Quantum computers are not a quantum version of a classical computer: there is no OS, no boot, no quantum software.

Hybrid approach: the quantum calculation is delegated to the quantum machine by a classical computer.

Only calculations that could benefit from a quantum algorithm (e.g. quantum speed-up) is realized with a quantum calculation algorithm.

Several NP-hard problem might benefit from quantum speed-up with quantum algorithms.

Potential applications of quantum computers

- chemical simulation ;
- scenario simulation ;
- optimization ;
- AI/ML.

Potential fields of applications of quantum computers

- chemicals and petroleum ;
- distribution and logistics ;
- financial services ;
- health care and life sciences ;
- Manufacturing.

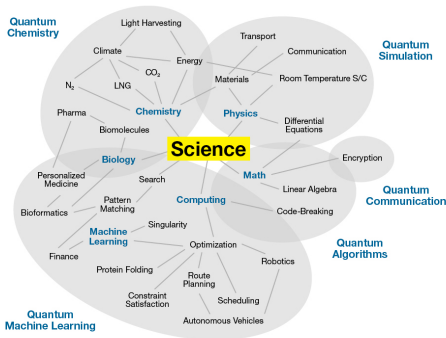
IV.4. Quantum computers



<https://www.gartner.com/smarterwithgartner/the-cio-s-guide-to-quantum-computing>

IV.4. Quantum computers

Quantum Computing Use Cases



gartner.com/SmarterWithGartner

Source: Adapted from Pina Shrobbell and Jeremy O'Brien
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. PR_338248

Gartner.

<http://itango.eu/the-cios-guide-to-quantum-computing/>

- 1 Quantum revolution(s)
- 2 Classical computer
- 3 Why quantum ?
- 4 Complexity, algorithms, and quantum computers
- 5 References

- *UK Quantum Technology Landscape 2014*, Defence Science and Technology Laboratory (UK)
<https://epsrc.ukri.org/newsevents/pubs/dstl-uk-quantum-technology-landscape-2014/>
- *Quantum Technology: The Second Quantum Revolution*, J.P.Dowling and G.J.Milburn (2003)
arXiv:quant-ph/0206091v1
- *Quantum Manifesto for Quantum Technologies* (2016)
<https://ec.europa.eu/futurium/en/content/quantum-manifesto-quantum-technologies>

- www.microsoft.com/en-us/quantum/development-kit
- www.honeywell.com/en-us/newsroom/news/2019/11/the-future-of-quantum-computing
- www.ibm.com/quantum-computing/technology/experience/
- www.dwavesys.com/
- www.rigetti.com/
- aws.amazon.com/fr/quantum-solutions-lab/
- atos.net/fr/vision-et-innovation/atos-quantum
- damo.alibaba.com/labs/quantum
- research.google/teams/applied-science/quantum/
- www.intel.fr/content/www/fr/fr/research/quantum-computing.html