Introduction to quantum computing

André Chailloux

▶ **To cite this version:**

André Chailloux. Introduction to quantum computing. WAIFI 2020 - International Workshop on the Arithmetic of Finite Fields, Jul 2020, Rennes, France. hal-03138529

HAL Id: hal-03138529

https://inria.hal.science/hal-03138529

Submitted on 20 Jan 2022

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 4.0 International License

Introduction to Quantum Computing

André Chailloux, Inria de Paris

WAIFI'20

Quantum physics and quantum computing

- Quantum physics (beginning. 20th century): physics at a very small scale. Planck, Heisenberg, Schrodinger, Einstein ...

- Particles behave differently
  - Can be in a superposition of physical states.
  - Are modified when observed and quantumness is destroyed (so very fragile)

- In the 1970's : idea to control quantum systems to simulate other quantum systems, and more generally for computing.

From quantum physics to quantum computing

Quantum physics

$$i\hbar\frac{\partial}{\partial t}\Psi = \hat{H}\Psi$$

$$\frac{d}{dt}\hat{A}(t) = \frac{i}{\hbar}[\hat{H}, \hat{A}(t)] + \frac{\partial \hat{A}(t)}{\partial t},$$

$$\vdots$$

Benioff, Deutsch

Quantum computing

- Quantum bits
- Quantum operations
- Quantum gates and quantum computing model.

Goal of today's talk

Quantum computing

- Many promising applications.

- Quantum key distribution (BB84)/quantum cryptography.

- Quantum algorithms
  - Shor's algorithm (1994)
  - Grover's algorithm (1998)
  - ...

- Other things I'm not going to talk about: quantum simulation, quantum sensing.

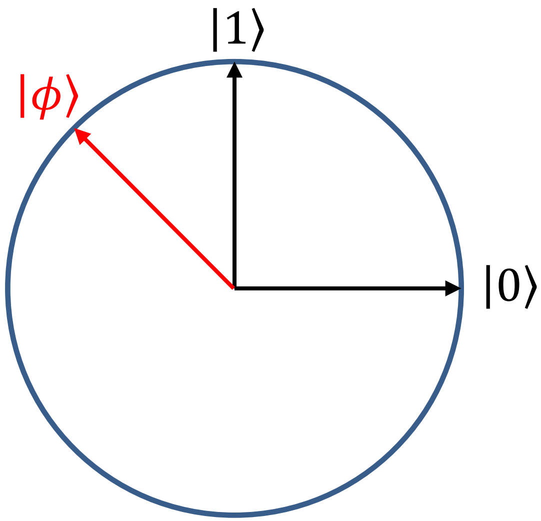
Outline of this talk

- Formalism of quantum computing

- Quantum algorithms

- General perspectives: quantum-secure cryptography, what can we do today from a hardware perspective.

- A quantum bit (or qubit) is a vector of norm 1 of the canonical $\mathbb{C}^2$ Hilbert space.
- Basis: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$; $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$
- $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$; $\alpha, \beta \in \mathbb{C}$
- Graphical representation of $|\phi\rangle$ when $\alpha, \beta \in \mathbb{R}$.



What does it mean to be in a superposition of states?

- Classical bits: 0;1. Unit of information. For eg. whether there is current in a wire (bit 1) ot not (bit 0)

- Qubits: basis = $\{|0\rangle, |1\rangle\}$. These basis elements also correspond to a physical state:
  - Spin of a particle (up = $|0\rangle$; down = $|1\rangle$).
  - Position of a particle (left = $|0\rangle$; right = $|1\rangle$).
  - Current in a wire (off = $|0\rangle$; on = $|1\rangle$).
  - Many other physical states can used to witness quantum effects (fortunately not the life of cats).

What does it mean to be in a superposition of states?

- So say I manage to construct $|\phi\rangle = \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$ that corresponds to the state of an electrical current ($|0\rangle =$ off, $|1\rangle =$ on)

- But say now I measure whether I have some electrical current or not.

- What ouptut do I get? Well 'on' or 'off', not both at the same time.
  - Probabilistic outcome: 'off' wp. 1/3 and 'on' wp. 2/3.

Quantum measurements

- More precisely, if I start from $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ and I measure:
  - I get outcome '0' wp. $|\alpha|^2$.
  - I get outcome '1' wp. $|\beta|^2$.

- After the measurement, the state collapses to the measured stated.
  - I get outcome '0' wp. $|\alpha|^2$. The state becomes $|\phi\rangle = |0\rangle$.
  - I get outcome '1' wp. $|\beta|^2$. The state becomes $|\phi\rangle = |1\rangle$.

- When a state is measured, it has to 'choose' in which state he really is.
  - Measurements destroy the 'quantumness' of the underlying physical particle
  - Measuring a quantum state changes it!

Quantum measurements: undetermination

- Measurements are the only way to get information about a quantum state.

- Suppose you are given $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$.
  - The only way to get some information about α and β is to perform a measurement on $|\phi\rangle$.
  - But this gives only 1 bit of information and then destroys all information about α and β (recall $\alpha, \beta \in \mathbb{C}$).

- Qubits can't be fully read. Actually, we can recover a very small amount of information about α, β.

- Measuring qubits destroys their quantum nature.

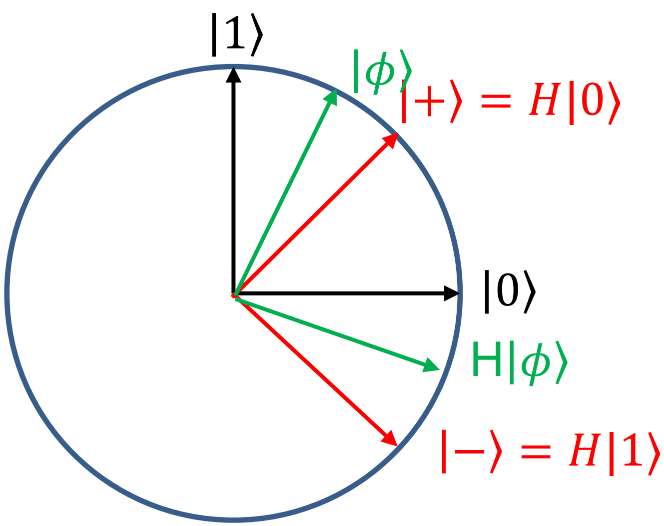
- However, we can perform quantum operations on qubits without destroying their quantum nature.

- Quantum operations are linear and norm preserving. They can be represented by unitary matrices U

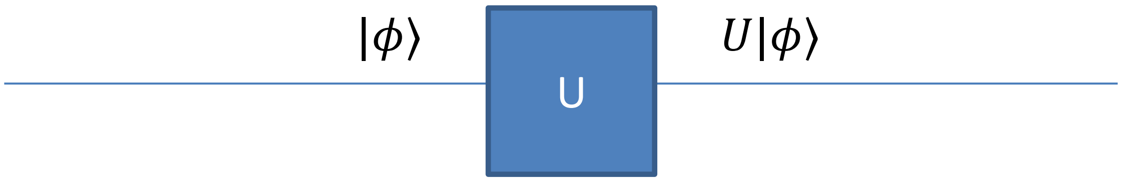
U= $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$: $\begin{pmatrix} a \\ b \end{pmatrix}$;$\begin{pmatrix} c \\ d \end{pmatrix}$ are each of norm 1 and orthogonal.

- Bit flip (BF): $U_{BF} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
  - $U_{BF}|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \quad ; \quad U_{BF}|1\rangle = |0\rangle$
  - $U_{BF}\left(\alpha|0\rangle + \beta|1\rangle\right) = \beta|0\rangle + \alpha|1\rangle$.
- Hadamard gate: $H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$.
  - $H\,|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \coloneqq |+\rangle$.
  - $H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \coloneqq |-\rangle$.

- H gate.


$|1\rangle$
$|\phi\rangle$
$|+\rangle = H|0\rangle$
$|0\rangle$
$H|\phi\rangle$
$|-\rangle = H|1\rangle$

- Any 2 x 2 unitary matrix U is an admissible quantum operation on 1 qubit.



- A quantum unitary doesn't measure the quantum state, and thus preserves its quantumness.
- For eg. a photon going through a crystal, changing its polarity (which is the quantum state of the photon)
- Easy to do experimentally.

Recap of qubits

- A qubit $|\phi\rangle = \alpha|0\rangle + \beta|0\rangle$ represents a particle which is in a superposition of states (here '0' and '1').
- The laws of quantum mechanics allow to interact with $|\phi\rangle$ in 2 ways:
  - Via quantum unitary operations: preserves the quantumness.
  - Via measurments: destroys the quantumness. Only way to retrieve information about the state.

2 qubit states.

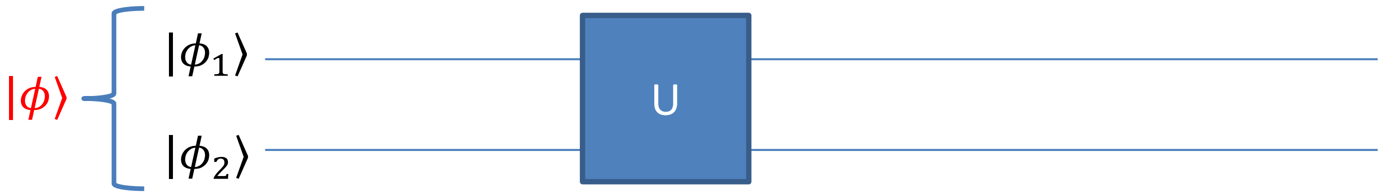
- 2 bits: 00;01;10;11.
- 2 qubit state: $|\phi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$.
  - $\alpha, \beta, \gamma, \delta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.
- $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$; $|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$; $|10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$; $|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
- Again, 2 ways to interact:
  - Quantum operations on 2 qubits, represented by 4 x 4 unitary matrices. Eg.

$$U = \begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 \\ 1/2 & 1/2 & -1/2 & -1/2 \\ 1/2 & -1/2 & -1/2 & 1/2 \\ 1/2 & -1/2 & 1/2 & -1/2 \end{pmatrix} ; U|\phi\rangle = U \cdot \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = 1/2 \begin{pmatrix} \alpha+\beta+\gamma+\delta \\ \alpha+\beta-\gamma-\delta \\ \alpha-\beta-\gamma+\delta \\ \alpha-\beta+\gamma-\delta \end{pmatrix}$$

  - Measurments: get outcome ‘00’ wp. $|\alpha|^2$. Similarly with ’01’, ’10’, ’11’.

2 qubits and entanglement

- Concatenation of 2 qubits



- $|\phi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$; $|\phi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$.
- What is the overall state $|\phi\rangle$ of the system?

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

- Entanglement: not all 2 qubit states $|\phi\rangle$ are of the form $|\phi_1\rangle \otimes |\phi_2\rangle$.
  - Eg. $|\phi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. This is an entangled state.

- [EinsteinPodolskiRosen’35] paradox: ‘spooky action at a distance’.

- Confirmed experimentally by Aspect.
  - Quantum mechanics is non-local as predicted by Bell (1964).
  - Non-locality has a very elegant explanation in terms of computer science concepts and information theory:

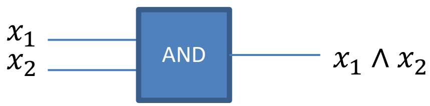
n qubit states

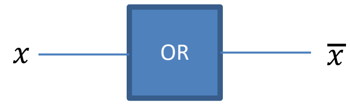
- n qubit state: $|\phi\rangle = \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle$.
  - Each $\alpha_i \in \mathbb{C}, \sum_i |\alpha_i|^2 = 1$.
  - Superposition of 2^n different states.

- Unitary operations: 2^n x 2^n matrices!
  - Even though these are quantum admissible operations: in general, we cannot make them efficiently.

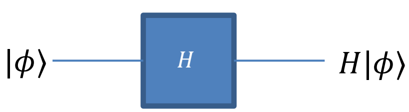
- Notions of complexity for quantum computing?

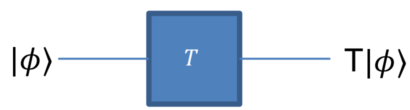
- Following gates are universal for (classical) computing:

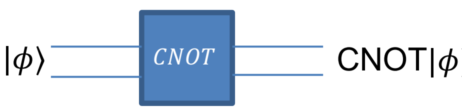




- Any function on n bits can be described using these 2 logical gates.
  - The minimum number of gates required to compute a function f is the circuit complexity of f (in this computational model).
- Quantum circuits, also an (approximate) universal set of gates.







$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{pmatrix} \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Quantum circuit model and complexity

- Any quantum unitary U on n qubits can be approximated by performing only H,T,CNOT unitaires.
  - The minimum number of gates required to compute a unitary U is the quantum circuit complexity of U (in this computational model).

- All universal sets of 1 and 2 qubit gates are equivalent (up to a $\mathrm{polylog}(\frac{1}{\epsilon})$ factor where ϵ is the approximation factor).

Recap

- Quantum computing involves qubits which are in a superposition of bits.
  - 2 operations: unitaries and measurements.

- Unitaries on n qubits involve modifying 2^n complex amplitudes at the same time.
  - At the core of quantum speedups.
  - But operations can be very costly. Also recall that we can gather only n bits of information from the output.

- Computational model: the quantum circuit model.

Quantum error correction

Quantum noise

- As we said, a qubit looses its quantumness when observed.

- Actually, most physical interactions with the environment destroy this quantumness
  - Qubits are extremely fragile.

- This noise is the main problem when considering quantum computation.
  - Is there a way to solve this problem?

- Quantum error correction: we can embed our n working qubits (logical qubits) into n’ > n physical qubits.

- During the computation, we can ensure that our n’ physical qubits remain in our code subspace and correct them if needed.

- This introduces new qubits and new quantum operations, hence new errors.

Threshold theorem: If the noise level per gate is < C (absolute constant), then we can correct errors faster than they arrive.

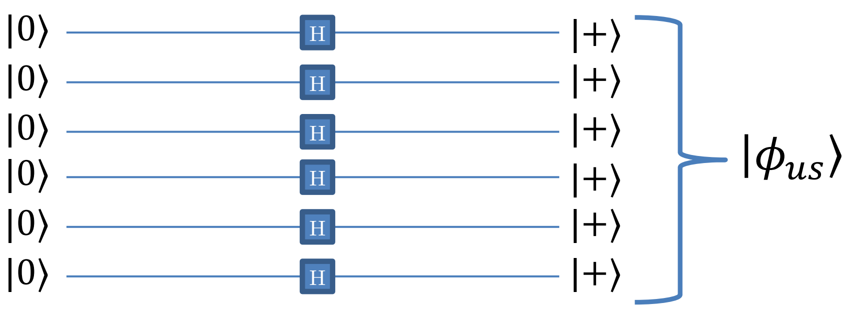
- So there is hope for quantum computing.

Quantum algorithms

- What can we do with quantum computing?

- Toy example 1: given n qubits, construct the uniform superposition $|\phi_{us}\rangle = \sum_{i\in\{0,1\}^n} \frac{1}{2^{n/2}} |i\rangle$.

- By performing basic computation, one can see that $|\phi_{us}\rangle = |+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle = H|0\rangle \otimes H|0\rangle \otimes \cdots \otimes H|0\rangle$



- $|\phi_{us}\rangle$ can be created in time n.

Transforming a classical circuit into a quantum circuit.

- Toy example 2: Quantum access to a classical function.

- We are given a function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ with the description of an circuit computing f.
  - Goal: compute the unitary O_f such that $O_f(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle$.

> Theorem: If the classical circuit for computing f has t gates then the unitary O_f can be constructed (approximately) using O(t) gates.

Shor's algorithm

Factoring problem

Input: a number N of n bits.
Goal: find the decomposition of N in prime numbers $N = \Pi_i p_i^{\alpha_i}$

- Actually, one can reduce this problem to period finding using a bit of number theory.

Period finding problem

Input: a function $f : \mathbb{N} \rightarrow \{0, \dots, N-1\}$ such that $\exists r \in \{0, \dots, N-1\}$ (unknown) st. $f(a) = f(b) \Leftrightarrow a = b \bmod r$
Goal: find r

- Classically, one needs $poly(N)$ time to solve this problem.
  - f can be computed in time $O(log^2(N)polylog(N))$.

Shor's algorithm

Period finding problem

Input: a function $f : \mathbb{N} \to \{0, \ldots, N-1\}$ such that $\exists r \in \{0, \ldots, N-1\}$ (unknown) st. $f(a) = f(b) \Leftrightarrow a = b \bmod r$
Goal: find r

- Shor's quantum algorithm: solves period finding in time $O(log^2(N)polylog(\log(N)))$ for this f.
  - $\Rightarrow$ solves factoring in the same time.

Shor's algorithm: 1 slide sketch

Period finding problem

Input: a function $f : \mathbb{N} \to \{0, \dots, N-1\}$ such that $\exists r \in \{0, \dots, N-1\}$ (unknown) st. $f(a) = f(b) \Leftrightarrow a = b \bmod r$
Goal: find r

- Take $m \approx 2\log(N)$. Construct $|\phi_{us}\rangle \otimes |0\rangle = \sum_{i\in\{0,1\}^m} \frac{1}{2^{m/2}} |i\rangle \otimes |0\rangle$.
- Apply O_f on $|\phi_{us}\rangle \otimes |0\rangle$ to get $|\psi\rangle := \sum_{i\in\{0,1\}^m} \frac{1}{2^{m/2}} |i\rangle \otimes |f(i)\rangle$.
  - Recall that $O_f(|i\rangle|0\rangle) = |i\rangle|f(i)\rangle$
- For a fixed second register ($|f(i_0)\rangle$), we get in the first register a uniform superposition proportional to $\sum_k |i_0 + kr\rangle$.
- The Quantum Fourier Transform allows us to find r in time $O(\log^2(N) polylog(\log(N)))$ for the function f needed for factoring.

Grover's algorithm

- Another iconic algorithm: Grover's algorithm

Search problem

Input: a function $f: \{0,1\}^n \rightarrow \{0,1\}$, with an efficient circuit description
Goal: find $x\ st.\ f(x) = 1$

- In the classical setting:
  - Worst case, a unique solution, need $O(2^n)$ calls to f.

- Quantum setting: Grover's algorithm, needs $O(2^{n/2})$ calls to O_f.

Perspectives

Quantum secure cryptography

- Shor's algorithm
  - Breaks factoring i.e. RSA
  - But also the Discrete Logarithm problem and the elliptic curve discrete log.

- Other problems (for public key crypto) for which we don't have an efficient quantum algorithm:
  - Lattice based crypto
  - Code based crypto
  - Isogeny based crypto
  - Multivariate based crypto
  - Hash based crypto

- Essential for retroactive security.

- Quantum Key Distribution (Quantum Cryptography)
  - Uses quantum communication to encode bits of a secret key.
  - An eavesdropper must observe the qubits and therefore destroy the quantumness: this can be detected.
  - Uses single qubits: we often use photons.
  - Can limit the effects of noise up to a few hundred kilometers: we don't use quantum error correction.

Cerberis^3 QKD System

Quantum Key Distribution for enterprise, government and telco production environments

- Complex network topologies (ring, hub and spoke)
- Interoperability with major Ethernet and OTN encryptors
- Easy integration in any data centre
- Centrally monitored solution
- Multiplexing of all channels on single fibre for metropolitan area

DOWNLOAD BROCHURE

VIEW USE CASES

HOW TO BUY

What can we do today? Quantum Computing

- Many research teams try to construct qubits as robust as possible in order to be highly scalable.
  - At most a few qubits at the same time.

- With recent advances, companies such as IBM or Google construct quantum architecture with around 50 qubits
  - IBM: you can actually go online and run some quantum circuits on their quantum computer: quite noisy.
  - Google: used their computer to perform a task they call Quantum Supremacy: a computational problem that we don't know how to solve classically (but which is veeeery useless and can't be checked).
  - Also no error correction! Not very scalable.

Conclusion

- Quantum computing: a crazy idea.
- A long way to go: especially for Shor's algorithm: a few thousand logical qubits and million/billions physical qubits.
- Other applications that require much less qubits and that can tolerate some noise: constant/polynomial speedups, chemistry/simulation.
- Quantum key distribution works and can have some particular applications coupled with classical crypto.

Thank you for your attention