

INTRODUCTION TO QUANTUM COMPUTING

History & Panorama

Frédéric Groschans

December 2, 2019,

Journée thématiques IN2P3



BEFORE WE START, SOME LOCAL (=FRENCH) CONTEXT


For the last decades, French physicists and computer scientists have built forums to work together on quantum information

BEFORE WE START, SOME LOCAL (=FRENCH) CONTEXT

For the last decades, French physicists and computer scientists have built forums to work together on quantum information

If interested, join:

Nationally GDR  <http://gdriqfa.unice.fr>

Groupe de travail information quantique of the 
<https://members.loria.fr/SPerdrix/gt-iq/>

in IdF region DIM  <http://www.sirteq.org/>

where you are (?) Several structures are taking form in
Grenoble, Paris-Saclay, Sorbonne Université, etc.

TABLE OF CONTENTS

1. Introduction
2. Architecture of a Quantum Computer
3. Algorithms
4. Hardware

INTRODUCTION



Modelling a quantum system is **hard**:

State of n two-level systems live in a 2^n -dimensional Hilbert space

50 spin $\frac{1}{2}$ particle described by $2^{50} \sim 10^{15}$ complex numbers!

Feynman 1982 I don't want an explosion. I only want the needed **resource** to be **proportional** to the physical system to simulate. Let us build a computer with quantum mechanical elements

Feynman 1982 I don't want an explosion. I only want the needed **resource** to be **proportional** to the physical system to simulate. Let us build a computer with quantum mechanical elements

Deutsch 1985 describes the **quantum Turing machine**

D, Josza, Simon 1992-3 find artificial algorithms solved **exponentially faster** by quantum computers

1994: SHOR'S ALGORITHM CHANGES THE GAME

Shor's algorithm factors a n -bits number $N = p \times q$ into its prime factors in a time $\propto n^3$

It changes **everything**, because

- faster than classical $\exp(Cn^{1/3}(\log n)^{2/3})$
 - factoring is a natural, useful, and well studied problem
 - it does not seem linked to quantum physics at all!
- ⇒ physics and computer science seem deeply linked

ARCHITECTURE OF A QUANTUM COMPUTER

The following models are (almost) equivalent

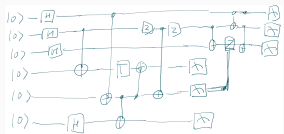
Quantum Circuit

Measurement based QC (MBQC)

Adiabatic QC

MAIN UNIVERSAL QUANTUM COMPUTING MODELS

Quantum Circuit Computation is a series of unitaries (gates) applied to initial state $|0\rangle^{\otimes n}$, followed by $\{|0\rangle, |1\rangle\}$ measurements



- Generalization of the reversible computer
- Universal gate-set :

$$\left\{ H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, Z = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}, T = \begin{bmatrix} 1 & \\ & e^{i\frac{\pi}{4}} \end{bmatrix} \right.$$
$$\left. \text{CNOT} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & & & 1 \end{bmatrix} \right\}$$

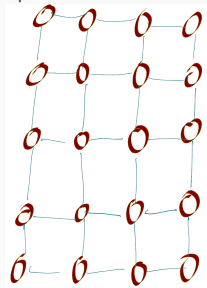
- Basis for most implementations (ions, superconducting qubits, etc.)

Measurement based QC (MBQC)

Adiabatic QC

Quantum Circuit

Measurement based QC (MBQC) A generic multipartite entangled state (cluster state) is prepared. A computation is a measurement pattern



- Proposed in [Raussendorf, Briegel, 2001]
- Quantum and classical computation well distinct
- Basis for verified and/or blind quantum computing
- Useful for photonic implementations

Adiabatic QC

Quantum Circuit

Measurement based QC (MBQC)

Adiabatic QC The well known ground state of Hamiltonian H_0 is prepared. Then the Hamiltonian is slowly evolved s.t.

$$H(t) = (1 - f(t))H_0 + f(t)H_T$$

- Proposed in [Fahri et al. 2000]
- f slow enough \Rightarrow we end in ground state of H_T
- $T = 0 \Rightarrow$ equivalent to circuit QC
- Seems easier to do
- But no known error correction scheme \Rightarrow unclear advantage
- Basis for quantum annealers (D-wave)

Shor and Steane find error quantum correcting codes in 1995

The idea: measuring the error **without** measuring the qubit.

Shor and Steane find error quantum correcting codes in 1995

The idea: measuring the error **without** measuring the qubit.

Here: $Z_1Z_2 = \pm 1, Z_1Z_3 = \pm 1,$

$$|\bar{0}\rangle = |000\rangle \quad |\bar{1}\rangle = |111\rangle \quad \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle = \alpha|000\rangle + \beta|111\rangle$$

Shor and Steane find error quantum correcting codes in 1995

The idea: measuring the error **without** measuring the qubit.

Let there be a bitflip error on qubit 2

Here: $Z_1Z_2 = -1$, $Z_1Z_3 = +1$, \Rightarrow flip bit 2

$$|\bar{0}\rangle = |010\rangle \quad |\bar{1}\rangle = |101\rangle \quad \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle = \alpha|010\rangle + \beta|101\rangle$$

Shor and Steane find error quantum correcting codes in 1995

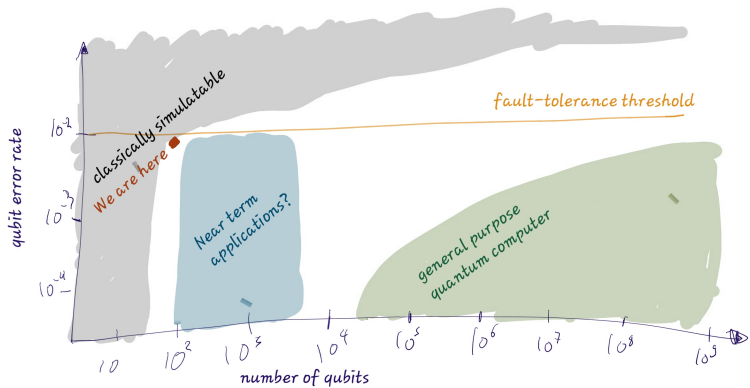
The idea: measuring the error **without** measuring the qubit.

$$|\bar{0}\rangle = (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|\bar{1}\rangle = (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

Combined with fault-tolerant gates acting on these logical qubits ensures the overhead is “reasonable” beyond a finite threshold (10^{-2} – 10^{-3})

YOU ARE HERE



ALGORITHMS

1. Simulation of quantum systems (for physics)
2. Hidden subgroup problems (for cryptography)
3. Search and quantum walks (for combinatorial problems)
4. Linear algebra “solving” (for machine learning)
5. Quantum heuristics (for optimization)
6. Useless but well understood algorithms (sampling problems)

Likely first to be useful

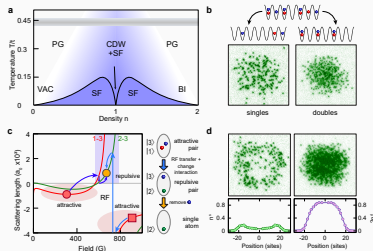
Variants include :

- Analogue vs Digital
- Dynamic vs Static

Already compute things we cannot simulate
 Quantum gas microscopes to investigate
 Bose-Hubbard and Fermi-Hubbard models

Likely first to be useful
 Variants include :

- Analogue vs Digital
- Dynamic vs Static



Mitra et al. arXiv:1705.02039

Ising models with Rydberg atoms in a chain
 Etc.

Likely first to be useful

Variants include :

- Analogue vs Digital
- Dynamic vs Static

Use a general purpose quantum computer

- exponential improvement over best known classical algorithms
- some gates allow shortcuts R_θ , i SWAP, $XY(\beta, \theta)$
- still interesting with some errors

Likely first to be useful

Variants include :

- Analogue vs Digital
- **Dynamic vs Static**

Dynamic given $|\psi(0)\rangle$ and H compute a quantity of interest for $|\psi(t)\rangle$

Static compute a quantity of interest for the ground state of H

- too hard in generality
- hopefully doable for systems of interests

Shor's algorithm and variants break all public key cryptography actually used until early 21st century

- solves factoring, discrete-log, elliptic curve cryptography
- can be verified
- needs thousands of logical qubits, millions of physical qubits

Shor's algorithm and variants break all public key cryptography actually used until early 21st century

- solves factoring, discrete-log, elliptic curve cryptography
- can be verified
- needs thousands of logical qubits, millions of physical qubits

Sketch of the algorithm (with $f : x \mapsto a^x \pmod N$)

1. Prepare $(H|0\rangle)^{\otimes n} |0\rangle^{\otimes n}$
2. Apply $|x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$ $\sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle = \sum_y \sum_x^{f(x)=y} |x\rangle |y\rangle$
3. measure the 2nd register y $\sum_x^{f(x)=y} |x\rangle$
4. apply a QFT on first register to get the period

Grover's algorithm (1996) and variants can check combination of probability ε in $\propto \frac{1}{\sqrt{\varepsilon}}$ trials

- “only” quadratic improvements
- useful for any unstructured problem (and there are many of them)
- quantum walk variants allow to speedup graph problems (graph coloring, backtracking, etc.)

HHL (Harrow, Hassidim, Lloyd 2009) use the fact that quantum mechanics does linear algebra in large dimensional space for free

- large speedup
- provided one can load large amount of quantum data in a quantum state
- useful for low rank matrices
- useful for machine learning
- unclear if general purpose quantum computer needed

The idea: uses the measurements on a small quantum circuit to optimize over its parameter

- QAOA (Quantum Approximate Optimization algorithm) and VQE (Variational Quantum Eigensolver)
- no theoretical characterization but doable now
- useful for quantum chemistry

Physics experiment on the computational power of nature

HARDWARE

See Daniel Estève's talk this afternoon

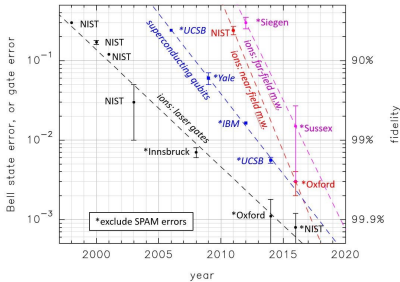


Image NQIT

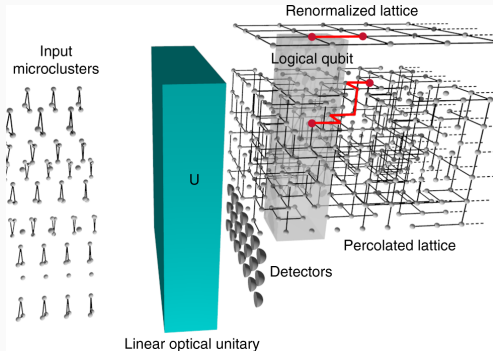
- Useless but classically undoable computation demonstrated with 53 qubits
- Small systems online by Google, IBM, Rigetti
- Academics also develop some systems (CEA Saclay, ETH Zürich, etc.)

A string of ions, trapped by electric fields and manipulated by lasers



- Current performance
 - Single-qubit gate infidelity 10^{-5}
 - Two-qubit gate infidelity 10^{-3}
 - 20 to 50 qubits
- Harder to scale, but can be interconnected
- System online by IonQ
- Many academic develop them (NIST, Innsbruck, Oxford, etc.)

Excellent scaling, but huge overhead: thousands of qubits or nothing



Pant, Towsley, Englund, Guha [arXiv:1701.03775](https://arxiv.org/abs/1701.03775)

- Uses Measurement Based Quantum Computing
- Developed by PsiQuantum, and many academic labs (C2N, La Sapienza, DTU, USTC, etc.)