Quantum Training:

Quantum algorithms for quantum computation and simulation

Benoit.vermersch@lpmmc.cnrs.fr
bvermersch.github.io

TPs with Nicolas Roch
Nicolas.roch@neel.cnrs.fr
Modern supercomputers

Exponential rise of supercomputer power → we may reach soon technological/financial/environmental barriers

Supercomputer Power (FLOPS)
The growth of supercomputer power, measured as the number of floating-point operations carried out per second (FLOPS) by the largest supercomputer in any given year. (FLOPS) is a measure of calculations per second for floating-point operations. Floating-point operations are needed for very large or very small real numbers, or computations that require a large dynamic range. It is therefore a more accurate measure than simply instructions per second.

```
<table>
<thead>
<tr>
<th>Rank</th>
<th>Rmax Speak (PFLOPS)</th>
<th>Name</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>415.530</td>
<td>Fugaku</td>
<td>Supercomputer Fugaku</td>
</tr>
<tr>
<td>2</td>
<td>148.600</td>
<td>Summit</td>
<td>IBM Power System AC922</td>
</tr>
<tr>
<td>3</td>
<td>94.640</td>
<td>Sierra</td>
<td>IBM Power System S922LC</td>
</tr>
<tr>
<td>4</td>
<td>93.015</td>
<td>Sunway TailuLight</td>
<td>Sunway MPP</td>
</tr>
</tbody>
</table>
```

Source: TCPP60 Supercomputer Database

Fugaku: 1 billion USD...
Some tough problems for computers

Integer factorization

Database search

Optimization problems

Quantum chemistry

Strongly correlated quantum materials
What is a quantum computer?

Paul Benioff  Richard Feynman  Yuri Manin  David Deutsch

A quantum machine that could imitate any quantum system, including the physical world
Why can a quantum computer be powerful?

1 classical bit

\[ \psi = |0\rangle \]

1 quantum bit (qubit)

\[ \psi = c_0 |0\rangle + c_1 |1\rangle \]

N classical bits

\[ \psi = |00000000\rangle \]

2^N configurations

N qubits

\[ \psi = c_0 |00000000\rangle + \cdots + c_{2^N-1} |11111111\rangle \]

2^N configurations ‘simultaneously’
The power of quantum parallelism

Example: brute force attack on 4 bit keys

Complexity: \( O(2^N) \)

Credit: EE-Times
The power of quantum parallelism

The quantum way

$$|s\rangle = \sqrt{\frac{1}{2^N}} (|0000\rangle + \cdots + |1111\rangle)$$

Grover’s algorithm: We test all states simultaneously! (see lecture 2)
### The First Era of Quantum Computing

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1925</td>
<td>Dirac, one of the founders of quantum physics, writes that physicists now know all laws necessary to simulate chemical systems.</td>
</tr>
<tr>
<td>1965</td>
<td>Feynman’s theories of quantum-electro-dynamics</td>
</tr>
<tr>
<td>1980</td>
<td>Yuri Manin proposed an idea of Quantum Computing</td>
</tr>
<tr>
<td>1981</td>
<td>Feynman proposes quantum phenomenon to perform computations</td>
</tr>
<tr>
<td>1991</td>
<td>Artur Ekert at the University of Oxford, invents entanglement based secure communication</td>
</tr>
<tr>
<td>1994</td>
<td>Shor’s algorithm for finding prime factors</td>
</tr>
<tr>
<td>1996</td>
<td>Grover’s database search algorithm</td>
</tr>
<tr>
<td>2000</td>
<td>First working 5-qubit NMR computer demonstrated at the Technical University of Munich.</td>
</tr>
<tr>
<td>2001</td>
<td>Using a 7 qubit computer, researchers at IBM/Stanford University factor the number 15.</td>
</tr>
<tr>
<td>2004</td>
<td>First five-photon entanglement demonstrated by Jian-Wei Pan’s group at the University of Science and Technology of China</td>
</tr>
<tr>
<td>2005</td>
<td>The scientist at the Institute of Quantum Optics and Quantum Information at the University of Innsbruck in Austria announce the first quantum byte, or qubyte</td>
</tr>
<tr>
<td>May 2017</td>
<td>IBM announces a 16 qubit machine that will be used as a follow-on to the 5 qubit machine</td>
</tr>
<tr>
<td>Sep 2017</td>
<td>Microsoft reveals an unnamed quantum programming language, integrated with Visual Studio. Programs can be executed locally on a 32-qubit simulator, or a 40-qubit simulator on Azure.</td>
</tr>
<tr>
<td>Oct 2017</td>
<td>Intel announces a 17-qubit superconducting chip</td>
</tr>
<tr>
<td>Oct 2017</td>
<td>Google announces OpenFermion: The Open Source Chemistry Package for Quantum Computers</td>
</tr>
<tr>
<td>Nov 2017</td>
<td>IBM announces 20 qubit quantum computing machine available as a cloud service and next-generation IBM Q system in development with first working 50 qubit processor</td>
</tr>
<tr>
<td>Nov 2017</td>
<td>IBM expands its open-source quantum computing eco-system application development software package QISKit</td>
</tr>
<tr>
<td>2016</td>
<td>IBM makes a five-qubit quantum processor available to developers, researchers and programmers for experimentation via its cloud portal.</td>
</tr>
</tbody>
</table>

Credit: [https://thetechfool.com/](https://thetechfool.com/)
The NISQ Era and beyond (2018-)

NISQ: noisy intermediate scale quantum

**Qubit Timeline Estimates**

- Crypto-Agility Becomes Important
- Quantum Advantage Meaningful Work
- Transient Quantum Supremacy
- Postquantum Cryptography
- Financial Services Begins to Use QC
- QML Impact to AI
- Greater Business Use Cases
- RSA/ECC Not Used for PKI
- All Historical RSA Encryption Can Be Cracked?

Note: Dates are speculative
ID: 374252

© 2018 Gartner, Inc.

The new challenge...

See lecture 4
The NISQ Era and beyond (2018-)

Cash for qubits
A growing number of quantum technology firms are raising cash from private investors, particularly in the sectors of quantum computing and quantum software.

**TOTAL VALUE OF DEALS**
(US$, millions)

<table>
<thead>
<tr>
<th>Year</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>46</td>
</tr>
<tr>
<td>2013</td>
<td>6</td>
</tr>
<tr>
<td>2014</td>
<td>67</td>
</tr>
<tr>
<td>2015</td>
<td>18</td>
</tr>
<tr>
<td>2016</td>
<td>86</td>
</tr>
<tr>
<td>2017</td>
<td>278</td>
</tr>
<tr>
<td>2018</td>
<td>173</td>
</tr>
</tbody>
</table>

**NUMBER OF DEALS**
- Instrumentation, tools and services
- Communication
- Computing
- Software
- Sensors and materials

**LOCATION OF INVESTMENTS 2012-18**
(US$, millions)

China is heavily commercializing quantum technologies including secure communications. But information on private funding deals is scarce; those disclosed tend not to report amounts.

*Includes unspecified contribution from the Australian government alongside private investors.*
Quantum softwares

→ TPs with Nicolas Roch

```python
[23] circuit = cirq.Circuit()
circuit.append(basic_circuit())
print(circuit)

c (0, 0): X^0.5 \cdot \epsilon \cdot X^0.5 \cdot \mathcal{M}(\text{\textquotesingle\text{alpha}\textquotesingle\text{\textquotesingle}})
(0, 1): X^0.5 \cdot \epsilon \cdot X^0.5 \cdot \mathcal{M}(\text{\textquotesingle\text{beta}\textquotesingle\text{\textquotesingle}})

[24] from cirq import Simulator
simulator = Simulator()
result = simulator.run(circuit)
print(result)

c alpha=0
beta=1
```
Qiskit architecture

« Simulator »

Includes quantum hardware (TPs with N. Roch)
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
<th>Activity/Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday 23/09</td>
<td>2pm-3.30pm</td>
<td>Amphi Mag MdM</td>
<td>Lecture 1 (all students) Benoit Vermersch, Quantum bits, quantum gates</td>
</tr>
<tr>
<td>Wednesday 30/09</td>
<td>2pm-3.30pm</td>
<td>Amphi Mag MdM</td>
<td>Lecture 2 (all students) Benoit Vermersch, Quantum algorithms</td>
</tr>
<tr>
<td>Wednesday 07/10</td>
<td>2pm-4pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 1:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 1</td>
</tr>
<tr>
<td>Wednesday 07/10</td>
<td>2pm-4pm</td>
<td>Mag1 MdM</td>
<td><strong>Group 2:</strong> Benoit Vermersh, Implementation on simulators and quantum computers: 1</td>
</tr>
<tr>
<td>Wednesday 07/10</td>
<td>4pm-6pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 3:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 1</td>
</tr>
<tr>
<td>Wednesday 21/10</td>
<td>2pm-4pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 1:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 2</td>
</tr>
<tr>
<td>Wednesday 21/10</td>
<td>2pm-4pm</td>
<td>Mag1 MdM</td>
<td><strong>Group 2:</strong> Benoit Vermersh, Implementation on simulators and quantum computers: 2</td>
</tr>
<tr>
<td>Wednesday 21/10</td>
<td>4pm-6pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 3:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 2</td>
</tr>
<tr>
<td>Wednesday 04/11</td>
<td>2pm-3.30pm</td>
<td>Amphi Mag MdM</td>
<td>Lecture 3 (all students) Benoit Vermersch, Quantum error correction codes</td>
</tr>
<tr>
<td>Wednesday 18/11</td>
<td>2pm-4pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 1:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 3</td>
</tr>
<tr>
<td>Wednesday 18/11</td>
<td>2pm-4pm</td>
<td>Mag1 MdM</td>
<td><strong>Group 2:</strong> Benoit Vermersh, Implementation on simulators and quantum computers: 3</td>
</tr>
<tr>
<td>Wednesday 18/11</td>
<td>4pm-6pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 3:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 3</td>
</tr>
<tr>
<td>Wednesday 25/11</td>
<td>2pm-3.30pm</td>
<td>Amphi Mag MdM</td>
<td>Lecture 4 (all students) Benoit Vermersch, Quantum Optimization/Simulation - Quantum advantage</td>
</tr>
<tr>
<td>Wednesday 02/12</td>
<td>2pm-4pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 1:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 4</td>
</tr>
<tr>
<td>Wednesday 02/12</td>
<td>2pm-4pm</td>
<td>Mag1 MdM</td>
<td><strong>Group 2:</strong> Benoit Vermersh, Implementation on simulators and quantum computers: 4</td>
</tr>
<tr>
<td>Wednesday 02/12</td>
<td>4pm-6pm</td>
<td>Amphi Mag MdM</td>
<td><strong>Group 3:</strong> Nicolas Roch, Implementation on simulators and quantum computers: 4</td>
</tr>
<tr>
<td>Wednesday 09/12</td>
<td>2pm-6pm</td>
<td>Amphi Mag, MdM</td>
<td>Exam (all students): Oral presentations by the students</td>
</tr>
</tbody>
</table>
Useful references

- Quantum computation and quantum information
  (Nielsen and Chuang)

- John Preskill's quantum information course:
  http://theory.caltech.edu/~preskill/ph219/index.html

- Quantum world II (Zoller and Gardiner)

- Surface code: https://arxiv.org/abs/1208.0928
Lecture 1: Quantum Circuits

- Presentations of a quantum circuit
- Single qubit: structure and operation (gates)
- Multi-qubit case: Universal set of gates
- The Measurement
- Physical realizations
A quantum circuit executes the most common type of quantum algorithms. There exists other types! e.g., quantum annealing/analog quantum simulation (see Lecture 4).
A qubit is a two-level quantum system (e.g., a two-level atom)

\[ |\psi\rangle = c_0 |0\rangle + c_1 |1\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} \]

The state of a pure single qubit state can be represented by a Bloch vector on the Bloch sphere

\[ |\psi\rangle = \cos \left( \frac{\theta}{2} \right) |0\rangle + \sin \left( \frac{\theta}{2} \right) e^{i\phi} |1\rangle \]

Classical bits are limiting cases of a qubit
Single qubit gates

A single qubit gate converts a single qubit state to another single qubit state

\[ q \xrightarrow{X} |\psi'\rangle = X |\psi\rangle \]

It is described by a unitary 2x2 matrix

\[ UU^\dagger = 1 \]

Or, equivalently, by a rotation on the Bloch sphere
Important Single qubit gates

Pauli-X (X) \[ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \]

Pauli-Y (Y) \[ \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \]

Pauli-Z (Z) \[ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]

Hadamard (H) \[ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \]

Phase (S, P) \[ \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \]

\(\pi/8\) (T) \[ \begin{bmatrix} 1 & e^{i\pi/4} \\ 0 & 0 \end{bmatrix} \]

Question: How can I create an equal-weight superposition state from the logical state \(|0\rangle\) ?

Concatenation: from left to right
Multi-qubit case

Single qubit gates can act on parallel in a tensor product space

\[ |0\rangle |0\rangle |0\rangle |0\rangle |0\rangle \rightarrow H |0\rangle |0\rangle H |0\rangle H |0\rangle H |0\rangle H |0\rangle \]

However, for a **universal quantum computer**, every global unitary operation of the \(2^N\times2^N\) Hilbert space must be available

\[ \rightarrow \text{Entangling operations required} \]
Multi-qubit case

**Deutsch (1989):**
A universal quantum computer can be realized with a set of single qubit and two qubit gates

The number of gates required to realize a certain operation is not necessarily small

**Efficient algorithms** are the one that a require polynomial number of gates
Important two-qubit gates

**Controlled Not (CNOT, CX)**

- CNOT: Flip the target qubit iff the control qubit is 1

**Controlled Z (CZ)**

- CZ: minus sign if both qubits are 1
Two qubit gates generate entanglement

Creation of a Bell state

Two ingredients: Hadamard and CNOT

\[ |0\rangle |0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]
\[ |0\rangle \rightarrow \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \]

We have created a maximally entangled state!
Universal set of gates

- **Hadamard (H)**: \[ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \]
- **Phase (S, P)**: \[ \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \]
- **\(\pi/8\) (T)**: \[ \begin{bmatrix} 1 & e^{i\pi/4} \\ 0 & e^{-i\pi/4} \end{bmatrix} \]
- **Controlled Not (CNOT, CX)**: \[ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \]

This set is not unique

With one set, I can reach any state up to arbitrary accuracy

Note: phase gate is optional here (but convenient)
Universal set of gates (example)

Build a CZ gate from a CNOT gate and two Hadamard gates

Idea: Change of basis from the Hadamard: \( H X H = Z \)

Exercice: Check the identity
Measurement

The measurement is often the last step of a quantum circuit

Mapping of quantum states to classical information (classical registers)

Very crucial step (readout errors)

Quantum operations based on measurement outcomes are possible (ex: error correction lecture 3)
A measurement is described by a set of $n$ measurement outcomes $(a_i)_{i=1}^n$.

A quantum state is measured (and projected) in the state $|a_i\rangle$ with probability $|\langle a_i | \psi \rangle|^2$.

In a quantum circuit, measurements in the `computational basis',

$$|\langle s | \psi \rangle|^2$$

**Histogram obtained after 1024 repetitions of the circuit**

![Histogram](image)
A single shot is not generically sufficient to characterize a quantum state
A single measurement basis is also not always sufficient
Non-destructive measurement (very important for the next lectures..)

Question:
What is the final state of the first qubit $q_0$ ???

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$ Bell state
Full measurement of a multi qubit state in the computational basis

Can you make sense of this measurement statistics?
Entertainment: Real quantum computers

Ion traps

The physics of these devices can be understood from atomic physics and quantum optics.
Entertainment: Real quantum computers

Superconducting quantum circuits

The physics of these devices can be understood from solid-state physics and quantum optics

Many other platforms: NMR qubits, silicon qubits, Rydberg atoms

Grenoble is an important place: N. Roch, O. Buisson, T. Meunier, M. Vinet,.. https://quantum.univ-grenoble-alpes.fr/
Real quantum computers

Performances

Table 2. Summary of the achieved success probabilities for the implemented circuits, in percentages

<table>
<thead>
<tr>
<th>Connectivity</th>
<th>Star shaped</th>
<th>Fully connected</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware</td>
<td>Superconducting</td>
</tr>
<tr>
<td>Success probability/%</td>
<td>Obs Rand Sys</td>
<td>Obs Rand Sys</td>
</tr>
<tr>
<td>Margolus</td>
<td>74.1(7) 82 75</td>
<td>90.1(2) 91 81</td>
</tr>
<tr>
<td>Toffoli</td>
<td>52.6(8) 78 59</td>
<td>85.0(2) 89 78</td>
</tr>
<tr>
<td>Bernstein–Vazirani</td>
<td>72.8(5) 80 74</td>
<td>85.1(1) 90 77</td>
</tr>
<tr>
<td>Hidden shift</td>
<td>35.1(6) 75 52</td>
<td>77.1(2) 86 57</td>
</tr>
</tbody>
</table>


Performance: Remarkable experimental progressess, quantum computers do exist (since 2005)!

Speed: 1 Hz for trapped ions, ~10 kHz for superconducting circuits
Summary Lecture 1

- **Quantum circuits** are an architecture for developing quantum algorithms.
- Basic ingredients: **qubits**, single qubit **gates** and two qubit gates (sufficient for universal quantum computation), and **measurement**.
- **Different physical platforms** can now implement quantum circuits: trapped ion, superconducting quantum circuits, etc.