Quantum Information

Marco Chiani
University of Bologna, Italy
Dept. of Electrical, Electronic, and Information Engineering “Guglielmo Marconi”

Aperitivo con AI: there is plenty of WORK at the bottom!
Bologna, February 17, 2021
Introduction
Quantum Mathematical Tools
Quantum algorithms
Secure quantum communication
Quantum hype? Quantum information technologies: really promising?

**Quantum effort worldwide**

- **Quantum Canada** CA$1b = $766m
- **United Kingdom** £1b = $1.3b
- **Netherlands** 150m € = $177m
- **Germany** 2.6b € = $3.1b
- **China** $10b
- **Russia** ₽50b = $663m
- **Korea** W44.5b = $37m
- **Japan** ¥50b = $470m
- **Taiwan** NT$8b = $282m
- **Australia** A$130m = $94m
- **US National Quantum Initiative** $1.2b
- **France** 1.8b € = $2.2b
- **European Quantum Flagship** 1b € = $1.1b
- **Israel** ₪1.2b = $360m
- **Singapore** S$150m = $109m

Global effort 2021 $22.5b (estimate)

©2021 QURECA Ltd – Confidential and Proprietary
Quantum information applications

- Quantum sensing: use of quantum mechanical phenomena such as entanglement to yield higher statistical precision than purely classical approaches

- Quantum computation: algorithms using quantum mechanical phenomena such as superposition and entanglement

- Quantum communications:
  - to secure communication
  - to move quantum information
  - to improve classical communication
Quantum bits - qubits
Define “state” of a classical/quantum system

... “state” means whatever information is required about a specific system, in addition to physical laws, in order to predict its behavior in future experiments†

- Classical (macroscopic) example: switch “open” or “closed” → state is one classical bit
- Quantum example: spin of an electron. Measured in any direction (Stern-Gerlach), two possible results, “same (+1)” or “opposite (−1)”, with some probabilities.

To predict its behavior we need a two-dimensional unit norm complex $\mathbb{C}^2$ vector $[\alpha, \beta]^T$ (referred to a specific direction, let’s say along $z$)

† Fano, Ugo. "Description of states in quantum mechanics by density matrix and operator techniques." Reviews of Modern Physics (1957)
⇒ Measurements are not gentle: after we measure, the state becomes what has been observed (collapses).
⇒ If we know the spin along z, we know nothing about the spin along x.
Quantum state: spin of an electron / photon polarization

\[ \psi = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \]

\[ |\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (\text{qubit}) \]

The state allows to calculate the probabilities for spin measurements in any possible direction, as well as the behavior in future experiments.

\[ P(\text{measuring “up”}) = |\alpha|^2 \]

\[ \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1 \]

\[ P(\text{measuring “down”}) = |\beta|^2 \]
Some examples of qubit physical implementation (incomplete list)

| Physical support | Name                              | Information support                               | |0)     | |1)     |
|------------------|-----------------------------------|---------------------------------------------------|--------|--------|
| Photon           | Polarization encoding             | Polarization of light                              | Horizontal | Vertical |
|                  | Number of photons                 | Fock state                                         | Vacuum | Single photon state |
|                  | Time-bin encoding                 | Time of arrival                                    | Early | Late    |
| Coherent state of light | Squeezed light | Quadrature                                         | Amplitude-squeezed state | Phase-squeezed state |
| Electrons        | Electron Spin                     | Spin                                              | Up     | Down    |
|                  | Electron number                   | Charge                                            | No electron | One electron |
| Nucleus          | Nuclear spin addressed through NMR| Spin                                              | Up     | Down    |
| Optical lattices | Atomic spin                       | Spin                                              | Up     | Down    |
| Josephson junction | Superconducting charge qubit | Charge                                             | Uncharged superconducting island ($Q = 0$) | Charged superconducting island ($Q = 2e$, one extra Cooper pair) |
|                  | Superconducting flux qubit        | Current                                           | Clockwise current | Counterclockwise current |
|                  | Superconducting phase qubit       | Energy                                            | Ground state | First excited state |
| Singly charged quantum dot pair | Electron localization | Charge                                             | Electron on left dot | Electron on right dot |
| Quantum dot      | Dot spin                          | Spin                                              | Down   | Up      |
| van der Waals heterostructure | Electron localization | Charge                                             | Electron on bottom sheet | Electron on top sheet |

from Wikipedia

M. Chiani, Univ. of Bologna
Introduction to Quantum Information
Quantum computing
Quantum Mechanics: it is possible to act on physical systems to change states according to linear transformations $U$ s.t. $U^\dagger U = I$ (unitary transformations)

- **Single qubit gate** example: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

  $$|\psi\rangle \xrightarrow{X} X |\psi\rangle$$

  $$X(\alpha |0\rangle + \beta |1\rangle) = \alpha |1\rangle + \beta |0\rangle \quad \text{“bit flip”}$$

- **Two-qubits gate** example: controlled-not, CNOT ($a, b \in \{0, 1\}$)

  $|a\rangle \quad |a\rangle$

  $|b\rangle \quad |a \oplus b\rangle$

It is possible to realize an arbitrary $U$ by using single-qubit and CNOT elementary gates.
The state of \( n \) qubits is a complex vector with dimension \( N = 2^n \).

Example \( n = 3 \)

\[
\alpha_0 |000\rangle + \alpha_1 |001\rangle + \cdots + \alpha_7 |111\rangle
\]

Exponential compression:

\[
40 \text{ qubits} \Rightarrow 2^{40} \approx 10^{12}
\]

However, when we measure we see just one configuration, with prob. \( |\alpha_j|^2 \).

Example: \( |\alpha_7|^2 \) is the probability to measure \( |111\rangle \)
Exploiting superposition: input $\sum_x |x\rangle |0\rangle \Rightarrow$ output $\sum_x |x\rangle |f(x)\rangle$
Main quantum algorithms

- Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms (Shor’s algorithm)
- Quantum search, space of $N$ elements. Classical search operations: $O(N)$
  Quantum search $O(\sqrt{N})$ (Grover’s algorithm)
Polynomial-time Algorithm for Prime Factorization on a Quantum Computer (Shor, 1994)

Ingredients:

- Factorization by order-finding
- Period-finding by Quantum Fourier Transform
The integer $N$ as a factor in common with $x - 1$ if $x^2 \mod N = 1$ and $x \mod N \neq \pm 1$.

To find $x$: generate random $y$, then find the period of $y^a \mod N$:

$$y^0 \mod N, y^1 \mod N, ...$$

Factoring $\iff$ period-finding.
Tools from signal analysis: Fourier

(Warning: imprecise statements, just to give the idea)
A function with period $P$ in time has frequency components at frequencies $k/P$. 

\[
\begin{align*}
\text{time} & \quad 0 \quad P \quad P \\
\text{freq} & \quad 0 \quad \frac{N}{P} \quad \frac{2N}{P} \quad N - 1
\end{align*}
\]
Tools from signal analysis: Fourier

(Warning: imprecise, just to give the idea)

Quantum Fourier Transform

\[ |0\rangle \rightarrow |0\rangle \]
\[ |N - 1\rangle \rightarrow |N - 1\rangle \]

\[ |0\rangle \rightarrow |2N/P\rangle \]
\[ |N/P\rangle \rightarrow |N - 1\rangle \]
Quantum order-finding, \( f(a) = f(a + P) \)

(Warning: imprecise, just to give the idea)

\[
U_f = \text{unitary, computes } f(a) \text{ in a register } \Rightarrow \text{output } \sum_x |x\rangle |f(x)\rangle
\]

Measure the second register. For example it turns out \( f(x) = 12 \)
Left in the first reg: superposition of all \( |x\rangle \) with \( x \) giving \( f(x) = 12 \) \( \Rightarrow \) periodic

Then, Quantum Fourier Transform: the measured frequency is some random multiple of \( 1/P \)
By repeating a couple of times, \( P \) can be derived with high probability
Quantum machine learning

The state of $n$ qubits is a complex vector with dimension $N = 2^n$

$$x \in \mathbb{C}^N \iff |x\rangle \text{ of } \log_2 N \text{ qubits}$$

<table>
<thead>
<tr>
<th></th>
<th>Classical</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>FFT</td>
<td>$O(N \log N)$</td>
<td>$O((\log N)^2)$</td>
</tr>
<tr>
<td>Eigenvect, eigenval of sparse matrices</td>
<td>$O(N^2)$</td>
<td>$O((\log N)^2)$</td>
</tr>
<tr>
<td>Matrix inversion</td>
<td>$O(N^3)$</td>
<td>$O((\log N)^3)$</td>
</tr>
</tbody>
</table>

**Table:** Number of operations for basic linear algebra subroutines
Quantum and AI

- ... 
- Quantum deep learning 
- Quantum convolutional neural networks 
- Quantum principal component analysis 
- TensorFlow Quantum 
- Quantum neural networks 
- ...
### Some existing quantum computers

<table>
<thead>
<tr>
<th>Company</th>
<th>Cloud Access</th>
<th>Technology</th>
<th>Quantum Computer</th>
<th>qubits</th>
<th>SDK/Lang.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM</td>
<td>Yes</td>
<td>Superconducting</td>
<td>IBM Q Montreal</td>
<td>27</td>
<td>QisKit/Python</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IBM Q Manhattan</td>
<td>65</td>
<td>QisKit/Python</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IBM Q Santiago</td>
<td>5</td>
<td>QisKit/Python</td>
</tr>
<tr>
<td>Rigetti</td>
<td>Through AWS</td>
<td>Superconducting</td>
<td>Aspen-8</td>
<td>32</td>
<td>Amazon Braket/Python</td>
</tr>
<tr>
<td>D-Wave</td>
<td>Through AWS</td>
<td>Superconducting, Quant. Annealer*</td>
<td>D-Wave 2000Q</td>
<td>2048*</td>
<td>Amazon Braket/Python</td>
</tr>
<tr>
<td>IonQ</td>
<td>Through AWS</td>
<td>Trapped Ion</td>
<td>-</td>
<td>79</td>
<td>Amazon Braket/Python</td>
</tr>
<tr>
<td>Google</td>
<td>No</td>
<td>Superconducting</td>
<td>Bristlecone</td>
<td>72</td>
<td>Cirq/Python</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sycamore</td>
<td>53</td>
<td>Cirq/Python</td>
</tr>
<tr>
<td>Honeywell</td>
<td>On-demand</td>
<td>Trapped Ion</td>
<td>System Model HØ</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>Xanadu</td>
<td>Yes</td>
<td>Photonic Quantum Computing</td>
<td>-</td>
<td>12</td>
<td>Strawberry Fields/Python</td>
</tr>
<tr>
<td>OriginQ</td>
<td>Yes</td>
<td>Superconducting</td>
<td>Wu Yuan</td>
<td>6</td>
<td>QPanda/C++</td>
</tr>
</tbody>
</table>
TABLE 4.1 Literature-Reported Estimates of Quantum Resilience for Current Cryptosystems, under Various Assumptions of Error Rates and Error-Correcting Codes

<table>
<thead>
<tr>
<th>Cryptosystem</th>
<th>Category</th>
<th>Key Size</th>
<th>Security Parameter</th>
<th>Quantum Algorithm Expected to Defeat Cryptosystem</th>
<th># Logical Qubits Required</th>
<th># Physical Qubits Required</th>
<th>Time Required to Break System</th>
<th>Quantum-Resilient Replacement Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES-GCM$^c$</td>
<td>Symmetric encryption</td>
<td>128</td>
<td>128</td>
<td>Grover’s algorithm</td>
<td>2,953</td>
<td>4,449</td>
<td>4.61 x 10$^6$</td>
<td>2.61 x 10$^{12}$ years</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192</td>
<td>192</td>
<td></td>
<td>4.68 x 10$^7$</td>
<td>3.36 x 10$^7$</td>
<td>1.97 x 10$^{22}$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>256</td>
<td>256</td>
<td></td>
<td>6,681</td>
<td></td>
<td>2.29 x 10$^{32}$</td>
<td></td>
</tr>
<tr>
<td>RSA$^d$</td>
<td>Asymmetric encryption</td>
<td>1024</td>
<td>80</td>
<td>Shor’s algorithm</td>
<td>2,050</td>
<td>8,05 x 10$^6$</td>
<td>8.56 x 10$^6$</td>
<td>Move to NIST-selected PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2048</td>
<td>112</td>
<td></td>
<td>4,098</td>
<td>8.56 x 10$^6$</td>
<td>1.12 x 10$^7$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4096</td>
<td>128</td>
<td></td>
<td>8,194</td>
<td></td>
<td>3.58 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28.63 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>229 hours</td>
<td></td>
</tr>
<tr>
<td>ECC Encryption problem$^g$</td>
<td>Asymmetric encryption</td>
<td>256</td>
<td>128</td>
<td>Shor’s algorithm</td>
<td>2,330</td>
<td>8.56 x 10$^6$</td>
<td>9.05 x 10$^6$</td>
<td>Move to NIST-selected PQC algorithm when available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>384</td>
<td>192</td>
<td></td>
<td>3,484</td>
<td>9.05 x 10$^6$</td>
<td>1.13 x 10$^7$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>521</td>
<td>256</td>
<td></td>
<td>4,719</td>
<td></td>
<td>10.5 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>37.67 hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>55 hours</td>
<td></td>
</tr>
<tr>
<td>SHA256$^h$</td>
<td>Bitcoin mining</td>
<td>N/A</td>
<td>72</td>
<td>Grover’s Algorithm</td>
<td>2,403</td>
<td>2.23 x 10$^6$</td>
<td>1.8 x 10$^4$</td>
<td>Move away from password-based authentication</td>
</tr>
<tr>
<td>PBKDF2 with 10,000 iterations$^i$</td>
<td>Password hashing</td>
<td>N/A</td>
<td>66</td>
<td>Grover’s algorithm</td>
<td>2,403</td>
<td>2.23 x 10$^6$</td>
<td>2.3 x 10$^7$</td>
<td>Move away from password-based authentication</td>
</tr>
</tbody>
</table>

Entanglement-based QKD between two ground stations separated by 1,120 km

Quantum communications: Quantum Internet

- To move and process quantum information
- Most important function: generate long distance quantum entanglement
- Applications:
  - generation of multiparty shared secrets
  - secure private-bid auctions
  - improved sensing
  - blind quantum computing
  - distributed quantum computing
  - quantum-enhanced measurement networks


