An introduction to Quantum Computing

Antonio Falabella

INFN CNAF

9/6/2023

Overview

Overview

1. Overview
2. Quantum Computing Concepts
3. Quantum Protocols
4. Quantum Computation
5. Tools and other topics

Quantum Computing Concepts

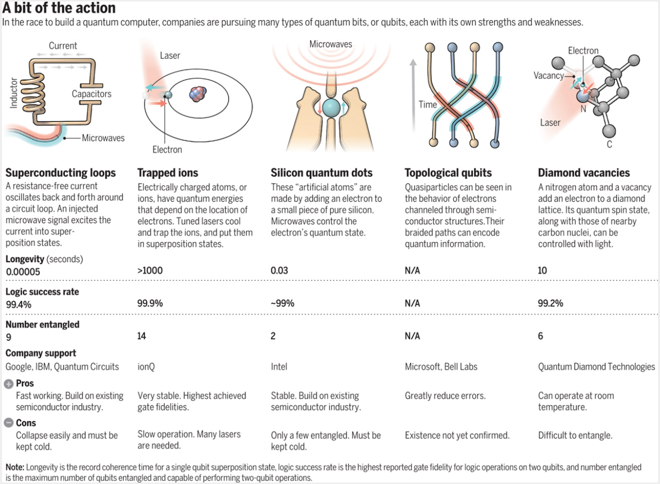
What's Quantum Computing

- Quantum computing is a computing paradigm that exploits quantum mechanical properties to perform some calculations more efficiently than classical computing
- The interactions inside a quantum computer are under the complete control of the programmer
- Interaction with the environment lead to *Decoherence*
- Superposition allows quantum systems to access all of its states simultaneously (quantum parallelism)
- This feature allows some algorithms to outperform classical ones: Grover's algorithm, Shor's Algorithm
- Application:
  - Simulation of quantum systems
  - Optimization problems
  - Machine learning
  - Cryptography
  - Computational Complexity

Models

- Quantum Turing machines
- **Quantum Circuits (Quantum Logic Gates)**
- Measurement based quantum computing
- Adiabatic quantum computing
- Topological quantum computing

Technologies


Current
Inductor
Capacitors
Microwaves
Laser
Electron
Microwaves
Time
Electron
Vacancy
N
Laser
C

A bit of the action

In the race to build a quantum computer, companies are pursuing many types of quantum bits, or qubits, each with its own strengths and weaknesses.

	Superconducting loops	Trapped ions	Silicon quantum dots	Topological qubits	Diamond vacancies
	A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into superposition states.	Electrically charged atoms, or ions, have quantum energies that depend on the location of electrons. Tuned lasers cool and trap the ions, and put them in superposition states.	These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.	Quasiparticles can be seen in the behavior of electrons channeled through semi-conductor structures.Their braided paths can encode quantum information.	A nitrogen atom and a vacancy add an electron to a diamond lattice. Its quantum spin state, along with those of nearby carbon nuclei, can be controlled with light.
Longevity (seconds)	0.00005	>1000	0.03	N/A	10
Logic success rate	99.4%	99.9%	~99%	N/A	99.2%
Number entangled	9	14	2	N/A	6
Company support	Google, IBM, Quantum Circuits	ionQ	Intel	Microsoft, Bell Labs	Quantum Diamond Technologies
⊕ **Pros**	Fast working. Build on existing semiconductor industry.	Very stable. Highest achieved gate fidelities.	Stable. Build on existing semiconductor industry.	Greatly reduce errors.	Can operate at room temperature.
⊖ **Cons**	Collapse easily and must be kept cold.	Slow operation. Many lasers are needed.	Only a few entangled. Must be kept cold.	Existence not yet confirmed.	Difficult to entangle.

Note: Longevity is the record coherence time for a single qubit superposition state, logic success rate is the highest reported gate fidelity for logic operations on two qubits, and number entangled is the maximum number of qubits entangled and capable of performing two-qubit operations.

Source: Quest for Qubits by Gabriel Popkin

`https://www.science.org/doi/10.1126/science.354.6316.1090`

Quantum Mechanics Concepts

- State of quantum mechanical system is completely specified by its state ψ (wave function)
- Every observable *a* has a corresponding hermitian operator *A*
- The state can be in *superposition* of eigenstates with complex numbers as coefficients $\rightarrow$ square module is the probability of measuring each state
- The wave function is governed by the Schröedinger equation $H(t)\psi(t) = i\hbar\frac{\partial\psi(t)}{\partial t}$

Bits vs Qubits

Bits

- In general a voltage level over/under a certain threshold

Qubits

- Spin state of an electron
- Energy level of an atom
- Light polarization (H/V)
- Superconducting current flow (clockwise/counter clockwise)

Qubits

- Classical bit takes discrete values $(0, 1)$
- Qubit $\rightarrow$ two dimensional Hilbert space
- The two states are $|0\rangle$ and $|1\rangle$ represented with *Dirac* notation or in matrix notation $\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- Qubits can also be a combination of the two states

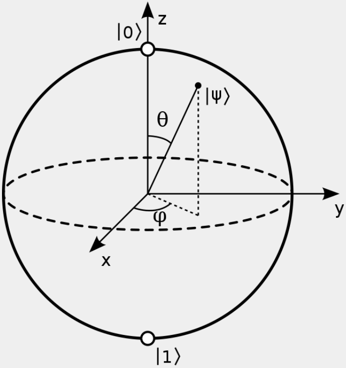
Generic state

$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, α and β complex numbers (contrast wrt classical bits)
$|\alpha|^2 + |\beta|^2 = 1 \rightarrow$ Unitary

Bloch sphere

General two state ket

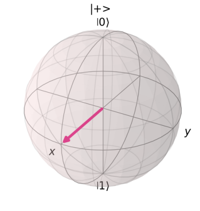
- $|\psi\rangle = e^{i\gamma}(cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle)$
- $0 \le \theta \le \pi$, $0 \le \phi \le 2\pi$
- Representation useful only for single-qubit

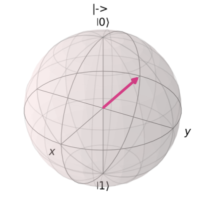


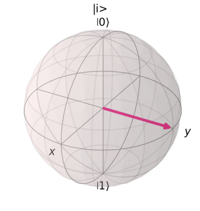
Superposition

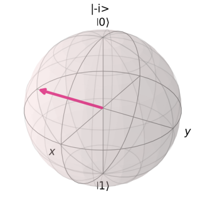
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- $|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$
- $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$



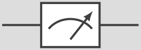




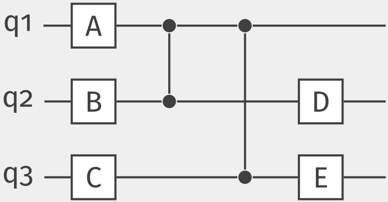


Measurement

General qubit

- In order to know the value of a qubit a measurement must be performed
- The result of the measurement is random
- $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$
- $$Meas(a\,|0\rangle + b\,|1\rangle) = \begin{cases} 0 & \text{with probability } |a|^2 \\ 1 & \text{with probability } |b|^2 \end{cases}$$
- 
- If you perform the same measurement you will obtain $|0\rangle$ or $|1\rangle$ with certainty depending on the previous measure

Quantum Circuits



- Schematic representation of a quantum computation
  - qubits : data (register) are represented on the left
  - gates : acts on single or multiple qubits
  - measurements : results
  - Time progress left to right

Single Qubits - Quantum Gates

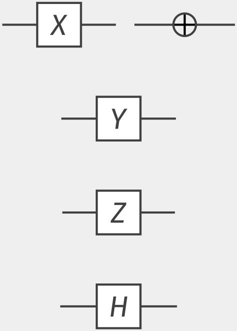
- Quantum gates for two states can be represented bit 2X2 matrices
- In general they are unitary operators $U^\dagger U = I$
- Remember that the possible values of the measurement are the eigenvalues of the operators, the result is a random process!
- Rotation around the three axis

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

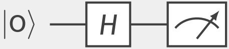
- Hadamard Gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Single Qubits - Quantum Gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Quantum Circuits

- A very simple circuit
- 

- After gate H we have $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
- The measurement will give 0 or 1 with probability 50%
- Perfect random number generator

Reversible Computing

- In classical computing only the NOT gate is *reversible*
- AND, OR and NAND gates are not reversible
- In QC operators are reversible only measurement is not $\rightarrow$ **Reversible Computing**
- $U^{-1} = U^{\dagger}$
- Reversible computing has consequences also on energy consumption (Landauer's principle, 1961)
- Computation can done reversibly

Tensor Products

- Hilbert spaces (i.e. two electrons spaces) can be combined to obtain an higher dimensional spaces
- From example combining multiple 2-states spaces will result in 2^n different states
- $|0\rangle, |1\rangle \rightarrow |0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$
- $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Entanglement

- A state that cannot be represented as a tensor product of other state in lower dimensional spaces is called *entangled*
- i.e. $|\Phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \rightarrow$ superposition of $|00\rangle$ and $|11\rangle$
- if you measure qubit 1 and find 0 then instantaneously qubit 2 will be found on state 1

Bell's states

- $|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $|\Phi^-\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$
- $|\Psi^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$, $|\Psi^-\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$

EPR Paradox

Spin 1/2 particle

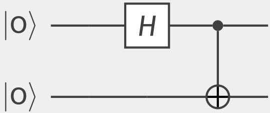
- $|\psi\rangle = \frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{\sqrt{2}}$
- One particle is send to Alice the other Bob
- If Alice measure the spin along the *z* axis (operator σ_z) she gets $+1$
- If Bob measure the *z* component he will obtain $\sigma_z = -1$ with probability 1
- Perfect anticorrelation
- Quantum mechanics → "non-locality" and violates realism (properties of a system independent of the measure)
- Hidden variables → some property that govern these probabilities that we cannot access

Bell Inequalities

Measurement

- Any theory of local hidden variables must satisfy an inequality $\rightarrow$ John Bell (1964)
- Proposed a series of experiments to determine the probabilities of measurements as expected classically (i.e. three entities that have two values with two different probabilities)
- Bell inequalities are violated by QM (because of entanglement)
- QM violates locality

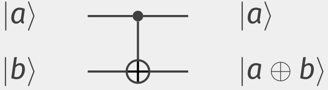
Quantum Circuits

- Bell state circuit → create an entangled pair
- 

- After gate H we have $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
- Combining the two qubits $\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle$
- CNOT $\frac{|00\rangle+|10\rangle}{\sqrt{2}} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$

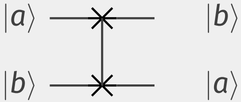
Multiple qubits gates

- CNOT : $|ab\rangle = |a a \oplus b\rangle$



$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

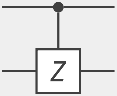
- Theorem : CNOT gate with one-qubit gates are universal for Quantum Computing
- SWAP : $|ab\rangle = |ba\rangle$



$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Multiple qubits gates

- Controlled Z (CZ): flips the phase of the target qubit if the control qubit is in the $|1\rangle$ state (try with $|1\rangle|1\rangle$)



$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

- Other multi-qubits: Toffoli, Fredkin, ...

Quantum Protocols

Superdense coding

What is it?

Share classical information between two parties (Alice and Bob). N classical bit sharing M < N QuBits

Preparation

A Third party prepare and entangled state (Bell State) $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Communication

Alice then apply an encoding based on the two classical bits she wants to send and sends back the transformed qubit to Bob to be decoded

Superdense coding - Encoding

Encoding

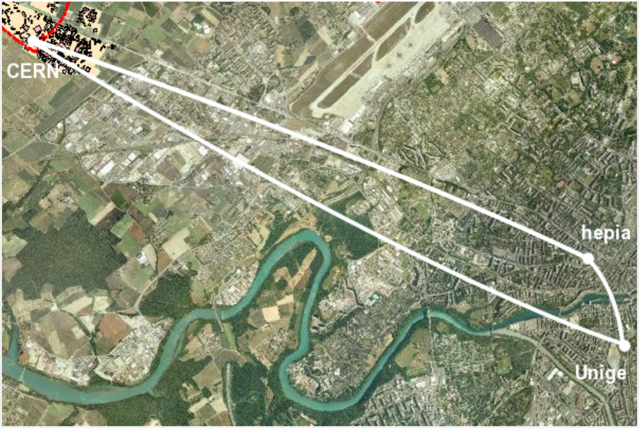
- 00 $\rightarrow$ no modification $\rightarrow \frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- 01 $\rightarrow$ phase flip $Z \rightarrow \frac{|00\rangle-|11\rangle}{\sqrt{2}}$
- 10 $\rightarrow$ NOT gate $X \rightarrow \frac{|10\rangle+|01\rangle}{\sqrt{2}}$
- 11 $\rightarrow$ gate $iY \rightarrow \frac{|01\rangle-|10\rangle}{\sqrt{2}}$
- With the second qubit in possession Bob can determine Alice's choice

QKD

Cryptography

- Classical algorithm based on RSA (Rivest, Shamir and Adleman) → finding prime factors of large number is computationally hard
- RSA can be cracked by Shor's algorithm
- OTP completely secure provided the secret key is truly random
- if a secure communication channel can be established → key distribution
- Possible protocol BB84 (see. F. Amori seminar `https://agenda.infn.it/event/34417/`), E91, B91 ...

QKD

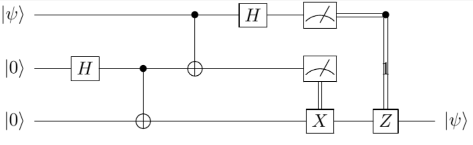


https://arxiv.org/pdf/1203.4940.pdf

No-cloning theorem

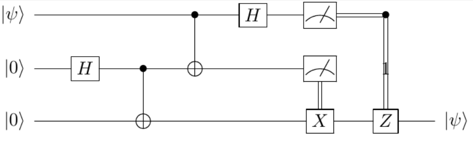
- Copy of a state into another
- Only through unitary evolution not a measurement
- $|a\rangle = \alpha |0\rangle + \beta |1\rangle$
  - $U |a\rangle |0\rangle = |a\rangle |a\rangle$
  - $U |a\rangle |0\rangle = U(\alpha |0\rangle |0\rangle + \beta |1\rangle |0\rangle)$
  - $= \alpha |0\rangle |0\rangle + \beta |1\rangle |1\rangle$
  - but $|a\rangle |a\rangle = \alpha^2 |0\rangle |0\rangle + \alpha\beta |0\rangle |1\rangle + \beta\alpha |1\rangle |0\rangle + \beta^2 |1\rangle |1\rangle$
- Eavesdropper cannot copy the message without destroying it

Quantum Teleportation



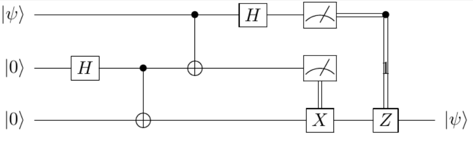
- Alice wants to teleport qubit $|a\rangle = \alpha|0\rangle + \beta|1\rangle$
- Initial state consist of qubit 1, 2 and 3 $|a_1\rangle = |a\rangle|0\rangle|0\rangle = (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle$
- After the first entanglement of the second and third qubit the state become $|a_2\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$
- One the two qubits (2 and 3) is kept with Alice the other with Bob
- Alice than performs a CNOT of qubit 2 using her qubit as control qubit

Quantum Teleportation



- After CNOT the state is
  $|a_3\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$
- Alice then applies an Hadamard gate
- $|a_4\rangle = \frac{1}{\sqrt{2}}[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) +$
  $|10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle + \beta|0\rangle)]$

Quantum Teleportation



- Now Alice measures her qubits and send the results to Bob using a classical channel
- Bob uses the received information for a CNOT and a control Z gate
  - $|00\rangle : \alpha|0\rangle + \beta|1\rangle \rightarrow \text{CNOT}\alpha|0\rangle + \beta|1\rangle \rightarrow \text{CZ}\alpha|0\rangle + \beta|1\rangle$
  - $|01\rangle : \alpha|1\rangle + \beta|0\rangle \rightarrow \text{CNOT}\alpha|0\rangle + \beta|1\rangle \rightarrow \text{CZ}\alpha|0\rangle + \beta|1\rangle$
  - $|10\rangle : \alpha|0\rangle - \beta|1\rangle \rightarrow \text{CNOT}\alpha|0\rangle - \beta|1\rangle \rightarrow \text{CZ}\alpha|0\rangle + \beta|1\rangle$
  - $|11\rangle : \alpha|1\rangle - \beta|0\rangle \rightarrow \text{CNOT}\alpha|0\rangle - \beta|1\rangle \rightarrow \text{CZ}\alpha|0\rangle + \beta|1\rangle$

Quantum Computation

Quantum Algorithms

- https://quantumalgorithmzoo.org/
- Quantum search algorithms: Search on unstructured databases (polynomial increase)
- QFT based algorithms : Shor's for (exponential increase)
- Quantum simulation

Quantum advantage

The computational advantage of quantum computers is a measure of how faster a certain task can be done by a quantum computer wrt a classical computer

Quantum supremacy

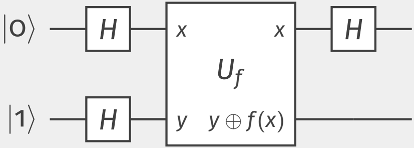
The potential ability of quantum computers to solve problems that classical computers practically cannot

Deutsch's Algorithm

- Univariate function $f : 0, 1 \rightarrow 0, 1$
-
  - $0, 1 \rightarrow 0$ constant
  - $0, 1 \rightarrow 1$ constant
  - $f(0) = 0, f(1) = 1$ balanced
  - $f(0) = 1, f(1) = 0$ balanced
- Classically to decide if the function is constant or balanced you have to query it two times or in general $2^{(n-1)} + 1$ (n being the number of bits)

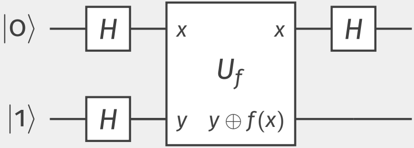
Deutsch's Algorithm - cont'd

- $|x\rangle \to |f(x)\rangle$ won't work (not reversible)
- $|x\rangle\,|y\rangle \to |x\rangle\,|y \oplus f(x)\rangle$
- So let's start with $|01\rangle$
- $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\,|0\rangle\,(|0\rangle - |1\rangle) + \frac{1}{\sqrt{2}}\,|1\rangle\,(|0\rangle - |1\rangle)$
- $\to \frac{1}{\sqrt{2}}\,|0\rangle\,(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + \frac{1}{\sqrt{2}}\,|1 \oplus f(1)\rangle\,(|0\rangle - |1 \oplus f(1)\rangle)$



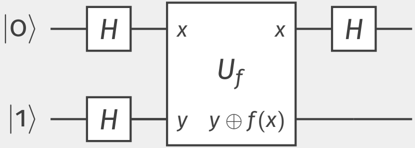
Deutsch's Algorithm - cont'd

- $= (-1)^{f(0)} |0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + (-1)^{f(1)} |1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- if $f(0) = f(1) \rightarrow \pm\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- if $f(0) \neq f(1) \rightarrow \mp\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$



Deutsch's Algorithm - cont'd

- After applying the H to just the first qubit
- if $f(0) = f(1) \rightarrow \pm |0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- if $f(0) \neq f(1) \rightarrow \pm |1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$



- So by measuring just the first qubit we can determine if $f(0) = f(1)$ or $f(0) \neq f(1) \rightarrow$ quantum parallelism

Grover's Algorithm

- Search in a database with entries indexed by one index $0, N-1$
- Classic algorithms $\sim O(N)$
- Grover Algorithm $\sim O(\sqrt{N})$ quadratic speed up
- Starts with a combination of 2^N states

$$|x\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \rightarrow \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots \alpha_{N-1} |N-1\rangle$$

Grover's Algorithm

- Initialization $|\psi\rangle = H^{\otimes n}|0\rangle = \sum_{n=0}^{N-1} \alpha_n |n\rangle$
- Oracle: $f(x) = \begin{cases} 1, & \text{if } n = n^* \\ 0, & \text{otherwise} \end{cases}$
- Operator implementation: $O|\psi\rangle = \sum_n \alpha_x (-1)^{f(x)|n\rangle}$ (probability inversion)
- Amplitude amplification : $U\langle n||n\rangle - I$ (diffusion operator)
- Probability approaches 1 after $O(\sqrt{N})$ iterations

Shor's Algorithm

- RSA (Rivest–Shamir–Adleman) is based on the inability to efficiently find the prime factors of large numbers
- For example RSA-2048, key from two large prime numbers (617 digits)
- Cracking RSA-2048 with classical algorithms is not feasible
- Shor's algorithm efficiently find prime factors of large numbers
- polynomial time versus exponential time

Shor's Algorithm - Are we safe?

- `https://arxiv.org/pdf/2212.12372.pdf`
- Factoring integers up to 48 bits with 10 superconducting qubits
- 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048

Quantum Error Correction

NISQ

- Noisy Intermediate-Scale Quantum Computing → quantum advantage without full quantum error correction

- qubits requirement to be isolated conflicts with the need to assess their values
- Leakage(transition to nearby level), relaxation(unwanted transitions to lower-levels)
- As of today on few tens of qubits tested
- Mitigation : qubits isolation, QEC protocols, Topological Quantum Computing

Quantum Error Correction

QEC

- Usually the correction is made using additional redundant qubits based on the assumption that the probability decreases
- Quantum Threshold Theorem $\rightarrow$ QEC works if error rate is kept under a certain threshold
- error 1 every 100/1000 gate operation $\rightarrow$ gate *fidelity* $\simeq 99\% - 99,9\%$
- $\simeq$ 1000 physical qubits every logical qubit

Tools and other topics

Useful tools

- Jupyter Notebooks
- IBM Quantum Experience `https://quantum-computing.ibm.com/`
- Qirk (online simulator) `http://algassert.com/quirk`
- D-Wave `https://www.dwavesys.com/take-leap`

Frameworks and Programming languages

- qasm
- Qiskit
- ProjectQ
- …
- `https://baltig.infn.it/giaco/eqc`

Other topics

- Variational Quantum Computing https://pennylane.ai/qml/glossary/variational_circuit
- Adiabatic Quantum Computing
- Topological Quantum Computing
- Simulation
- Metrology
- Quantum Technologies
- Quantum Machine Learning

References

- A practical introduction to quantum computing - Elias Fernandez-Combarro Alvarez https://indico.cern.ch/event/970903/
- Quantum Computation and Quantum Information, Michael A. Nielsen and Isaac L. Chuang
- Introduction to Classical and Quantum Computing, Thomas G. Wong
- Introduction to Quantum Computing, Ray Lapierre

Qiskit

```
sudo apt install python3-pip python3-dev
sudo -H pip3 install --upgrade pip
sudo -H pip3 install virtualenv
mkdir myProject
source myProject/bin/activate
pip install jupyter
pip install qiskit
pip install numpy
pip install matplotlib
pip install pylatexenc
jupyter notebook
```