Quantum computation as a new scheme for problem-solving

Federico Tomás B. Pérez

Institut Henri Poincaré (París) || Instituto de Física La Plata (Argentina)

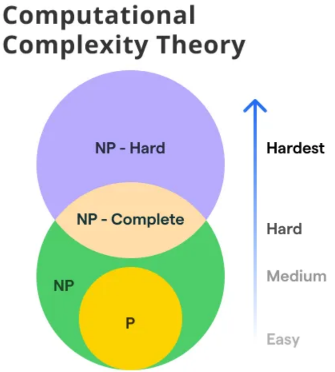
March 8th, 2024

IFLP CONICET UNLP

CIMPA ihp Institut Henri Poincaré SORBONNE UNIVERSITÉ

Computational Complexity

- **P-class** problems: decision problems in polynomial resources.
- **NP-class** problems: decision problems whose proof is verifiable in polynomial resources.
- **NP-Complete**: "Generalizations" of NP problems.
- **NP-Hard**: which are at least as hard as the hardest problems in NP



Computational Complexity

What if there were a way to overcome these problems via another type of computational frameworks?...

Computational Complexity

What if there were a way to overcome these problems via another type of computational frameworks?...
Consider the integer factorization problem...

Computational Complexity

What if there were a way to overcome these problems via another type of computational frameworks?...

Consider the integer factorization problem... It is suspected to be neither **P** nor **NP**-complete.

Computational Complexity

In: Proceedings, 35th Annual Symposium on Foundations of Computer Science,
Santa Fe, NM, November 20–22, 1994, IEEE Computer Society Press, pp. 124–134.

Algorithms for Quantum Computation:
Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Brief History of Quantum Mechanics

Stage: Late 19th. Century Physics:

Brief History of Quantum Mechanics

Late 19th. Century Physics:

1. At the end of the 19th century, classical physics faced challenges in explaining certain phenomena, such as blackbody radiation and the photoelectric effect.

Brief History of Quantum Mechanics

Late 19th. Century Physics:

1. At the end of the 19th century, classical physics faced challenges in explaining certain phenomena, such as *blackbody radiation* and the *photoelectric effect*.

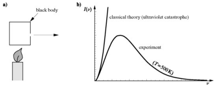


Figure: Classical Mechanics fails to describe blackbody radiation

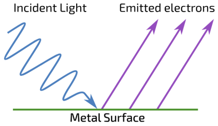


Figure: Electrons are only ejected when there is *enough* light hitting the surface, contrary to classical predictions.

History of Quantum Mechanics

- Max Planck proposed the idea of quantized energy levels to explain blackbody radiation.

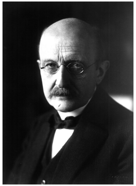


Figure: Max Planck (1858-1947)

History of Quantum Mechanics

- Max Planck proposed the idea of quantized energy levels to explain blackbody radiation.
- Albert Einstein applied the concept of quanta to explain the photoelectric effect, introducing the dual nature of light, suggesting both wave and particle characteristics (superposition)

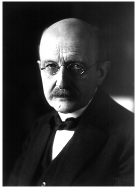


Figure: Max-Planck (1858-1947)

Figure: Einstein in 1905

History of Quantum Mechanics

- Max Planck proposed the idea of quantized energy levels to explain blackbody radiation.
- Albert Einstein applied the concept of quanta to explain the photoelectric effect, introducing the dual nature of light, suggesting both wave and particle characteristics (superposition)

From then on, physicists expanded QM by exploring

Motivation

- What would happen if storing and computation devices became ever so small that quantum effects start to become noticeable?

Drawing Paralellisms

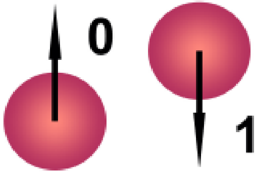
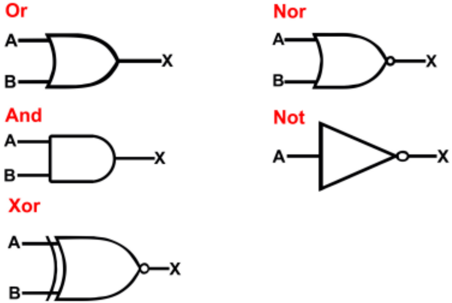
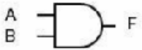


Figure: The classical bit

Drawing Paralellisms



AND



Inputs		Output
A	B	F
0	0	0
1	0	0
0	1	0
1	1	1

OR

Inputs		Output
A	B	F
0	0	0
1	0	1
0	1	1
1	1	1

Figure: Caption

Drawing Paralellisms

Classical Gates can be thought of as functions.

Drawing Paralellisms

Classical Gates can be thought of as functions.
For example:

$$\wedge : \{0,1\}^2 \longrightarrow \{0,1\} \text{ with}$$

$$\wedge(0,0) = 0$$

$$\wedge(0,1) = 0$$

$$\wedge(1,0) = 0$$

$$\wedge(1,1) = 1$$

Figure: Caption

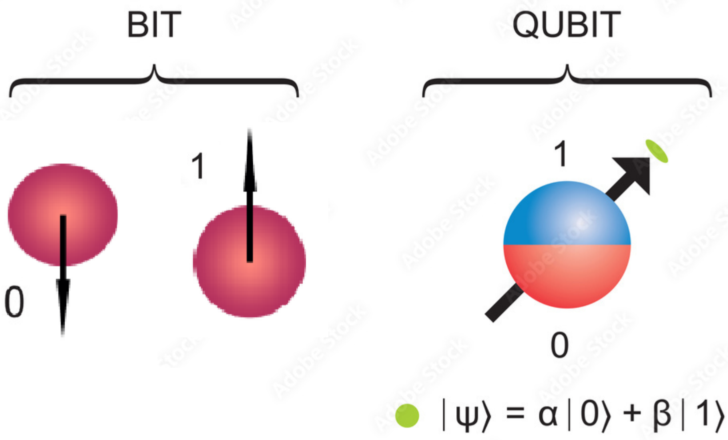
Drawing Paralellisms

An full circuit can then be thought of as a general function

$$F : \{0,1\}^n \to \{0,1\}^m.$$

The Quantum-Bit

Let us present the Quantum Bit or (QuBit)



The Qubit

A question arises...

The Qubit

A question arises... How do we work with Qubits?

The Qubit

A question arises... How do we work with Qubits?

- this leads to the measurement process.

Measuring a Qubit

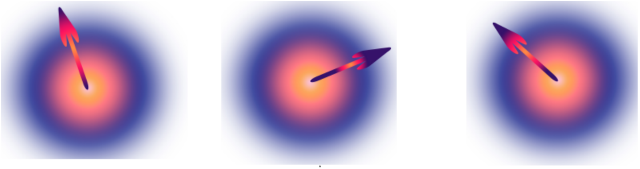


Figure: System of qubits at initial time $t = 0$.

Measuring a Qubit

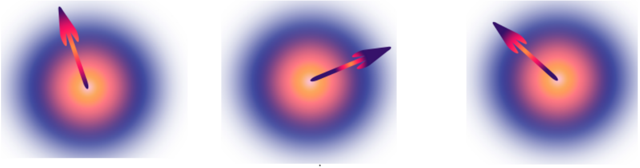


Figure: System of qubits at initial time $t = 0$.

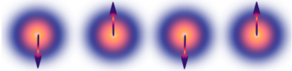


Figure: System of qubits measured at some later time $t > t_0$.

Measuring a Qubit

If we repeat the experiment, we might get...

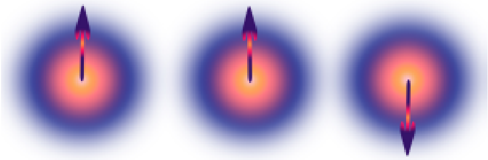


Figure: We might call this state $|\uparrow\uparrow\downarrow\rangle$

Measuring a Qubit

If we repeat the experiment, we might get...

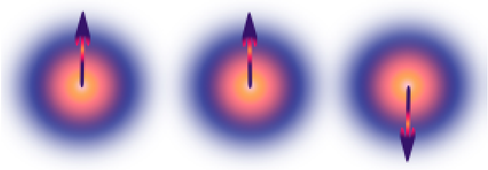


Figure: We might call this state $|\Psi\rangle = |\uparrow\uparrow\downarrow\rangle$

We can build a probability distribution $P_i(a = 0_i, 1_i) = |\langle a|\Psi\rangle|^2$.

Single Qubit Gates

$$X = \sigma_x = \mathrm{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

$$Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Two-Qubit Gates

Of special interest is the CNOT gate, given by

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

Classical and Quantum Computation

Generally, we can combine Quantum and Classical gates for more efficient computation

Classical and Quantum Computation

Generally, we can combine Quantum and Classical gates for more efficient computation

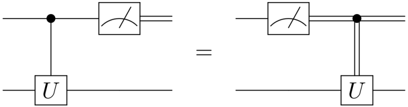


Figure: Deferred measurement

Classical and Quantum Computation

Now, we will study an application: Superdense coding

Secure Quantum Comunications: Superdense Coding

- Consider a situation in which Alice wants to send a qubit to Bob.

Secure Quantum Comunications: Superdense Coding

- Consider a situation in which Alice wants to send a qubit to Bob.
- We wish to send an entangled state (e.g. $|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|{\downarrow_1}{\downarrow_2}\rangle + |{\uparrow_1}{\uparrow_2}\rangle\right)$

Secure Quantum Comunications: Superdense Coding

- Consider a situation in which Alice wants to send a qubit to Bob.
- We wish to send an entangled state (e.g. $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow_1\downarrow_2\rangle + |\uparrow_1\uparrow_2\rangle\right)$

Classical and Quantum Computation

Grover's Search Algorithms

Consider a list of N items,

Grover's Search Algorithms

Consider a list of N items, with an item w of interest...

Consider a list of N items, with an item w of interest...

- On average, we need to check $N/2$ (structured list).

Consider a list of N items, with an item w of interest...

- On average, we need to check $N/2$ (structured list).
- In the worst-case scenario, N (unstructured list).

Consider a list of N items, with an item ω of interest...

- On average, we need to check $N/2$ (structured list).
- In the worst-case scenario, N (unstructured list).

With quantum computation, we need only $\mathcal{O}(\sqrt{N})$ *operations* $\Rightarrow$ Grover's search Algorithm

Grover's search Algorithm

Grover's algorithm can be written as follows:

Grover's search Algorithm

Grover's algorithm can be written as follows:

1. Initialization.

   Repeat until $|\omega\rangle$ is found:

2. We apply a quantum operation called *oracle*.

Grover's search Algorithm

Grover's algorithm can be written as follows:

1. Initialization.

   Repeat until $|\omega\rangle$ is found:

2. We apply a quantum operation called *oracle*.
3. We apply an additional reflection.

   End(Repeat)

Grover: Initialization

There is no knowledge about the state of the system $\rightarrow |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.

Grover: Initialization

There is no knowledge about the state of the system $\rightarrow |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.

On average, we need to try $\mathcal{O}(N/2)$ times to guess right.

Grover: Initialization

There is no knowledge about the state of the system $\rightarrow |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$.

On average, we need to try $\mathcal{O}(N/2)$ times to guess right.

We initialize via the operation $|S\rangle = H^{\otimes n}$

Grove: Oracle (first reflection)

Let the oracle be:

$$U_\omega |x\rangle = \begin{cases} |x\rangle \text{ if } x \neq \omega \\ -|x\rangle \text{ if } x = \omega \end{cases}$$

Grove: Oracle (first reflection)

Let the oracle be:

$$U_\omega |x\rangle = \begin{cases} |x\rangle \text{ if } x \neq \omega \\ -|x\rangle \text{ if } x = \omega \end{cases}$$

Then, the new state is

$$|\psi_1\rangle = U_\omega |S\rangle = U_\omega H^{\otimes} |x\rangle \,.$$

Grover: Second Reflection

Then we apply the reflection $U_s = 2\,|S\rangle\langle S| - 1$ onto the previous state,

Grover: Second Reflection

Then we apply the reflection $U_s = 2\,|S\rangle\langle S| - 1$ onto the previous state,

$$|\psi_2\rangle = U_s\,|\psi_1\rangle = U_S U_\omega H^{\otimes}\,|x\rangle\,.$$

Grover: Repetition of these steps

Then, we repeat these steps s.t. the whole operation now reads

$$\left|\psi_i\right\rangle = (U_S U_{\omega)}\left|\psi_{i-1}\right\rangle ,$$

or, more succintly,

$$\left|\psi_{r(N)}\right\rangle = (U_S U_\omega)^{r(N)} H^{\otimes}\left|x\right\rangle ,$$

where $r(N) \approx \frac{\pi}{4}\sqrt{N}$, with N the total number of states.

Example for $N = 4$:

We will show a simple numerical implementation with Qiskit.

Qiskit: Example for $N = 4$:

We will show a simple numerical implementation with Qiskit.

- We want to study a protocol with $N = 4$ states, which we will label $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Qiskit: Example for $N = 4$:

We will show a simple numerical implementation with Qiskit.

- We want to study a protocol with $N = 4$ states, which we will label $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
- Target state: $|\omega\rangle = |11\rangle$

Qiskit: Example for $N = 4$:

We will show a simple numerical implementation with Qiskit.

- We want to study a protocol with $N = 4$ states, which we will label $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
- Target state: $|\omega\rangle = |11\rangle$.
- For $N = 4$, $r(N) \approx 1.57 \approx 2$.

Qiskit: Example for $N = 4$

```
from qiskit import IBMQ, Aer, transpile, execute
from qiskit import QuantumCircuit, ClassicalRegister, QuantumRegister
from qiskit.providers.ibmq import least_busy
```

Qiskit: Example for $N = 4$

```
n = 2
grover_circuit = QuantumCircuit(n)
```

Qiskit: Example for $N = 4$

```
n = 2
grover_circuit = QuantumCircuit(n)

def initialize_s(qc, qubits):
    for q in qubits:
        qc.h(q)
    return qc
```

Qiskit: Example for $N = 4$

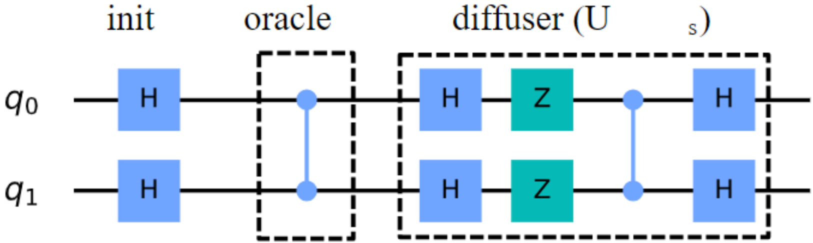
```
n = 2
grover_circuit = QuantumCircuit(n)

def initialize_S(qc, qubits):
    for q in qubits:
        qc.h(q)
    return qc
```

Qiskit: Example for $N = 4$

```
grover_circuit = initalize_s(grover_circuit, [0,1])
grover_circuit.h([0,1])
grover_circuit.z([0,1])
grover_circuit.cz(0,1)
grover_circuit.h([0,1])
grover_circuit.draw()
```

Qiskit: Example for $N = 4$



Qiskit: Example for $N = 4$

```
grover_circuit.measure_all()
qasm_sim = Aer.get_backend('qasm_simulator')
result = qasm_sim.run(grover_circuit).result()
counts = result.get_counts()
plot_histogram(counts)
```

Qiskit: Example for $N = 4$